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

Sumário

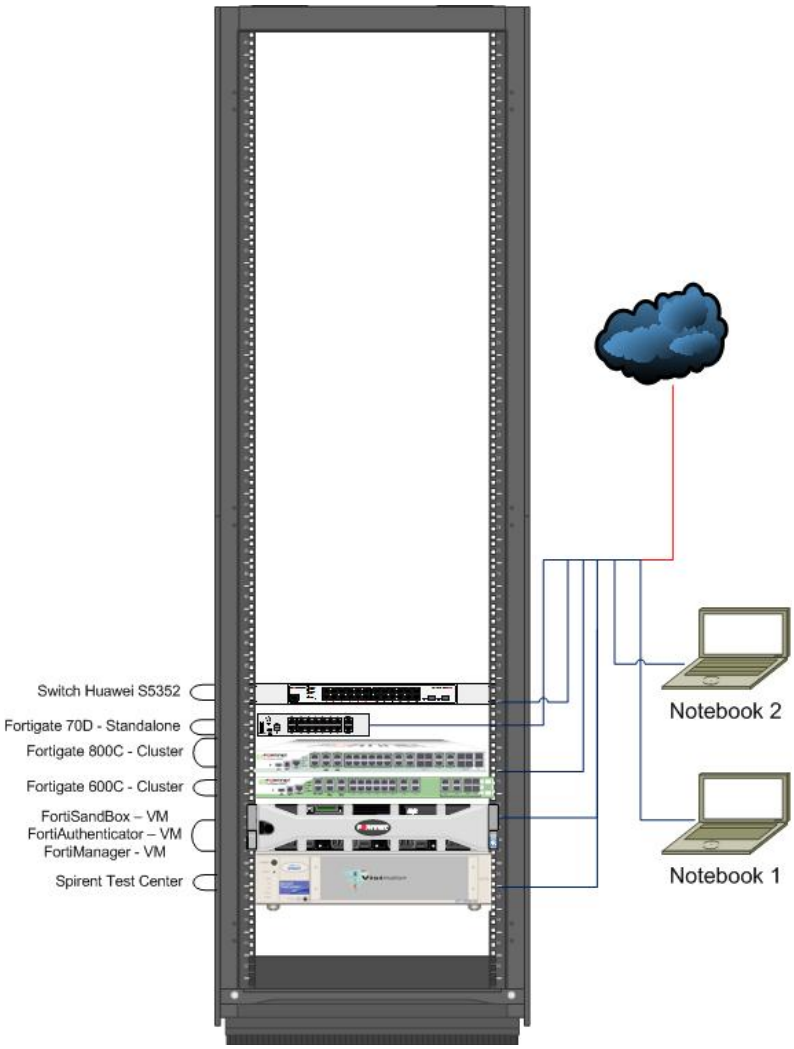
1. OBJETIVO DO CADERNO DE TESTE 3
2. ESTRUTURA FÍSICA 3
3. TABELA DE EQUIPAMENTOS 4
4. CABEAMENTO ESTRUTURADO 7
5. DEMAIS EQUIPAMENTOS 7
6. PERFIL DE TRÁFEGO TESTE 8
7. AMBIENTE DE TESTE 9
8. RELATÓRIO FINAL 10

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.

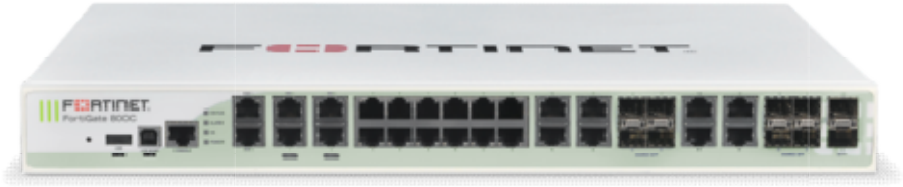
2. ESTRUTURA FÍSICA



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

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

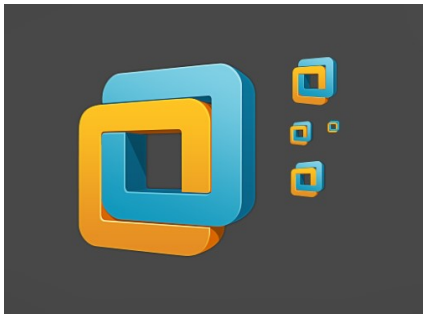
Feature	Ports per module	Connector type	Min/max frame size (w/CRC)	Min/max tx rates	Firmware Instalado
CV-10G-S8	8 x ports -10G (trafego IMIX stateless)	10/100/1000 Base-T copper	58-16384	1 packet per 3.43 seconds to 101% of line rate	4.44
CPU-5003	2x 10G (tráfego statefull	SFP+, 10GBASE-SR/SW	58-16384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

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



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.

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 trafego 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.

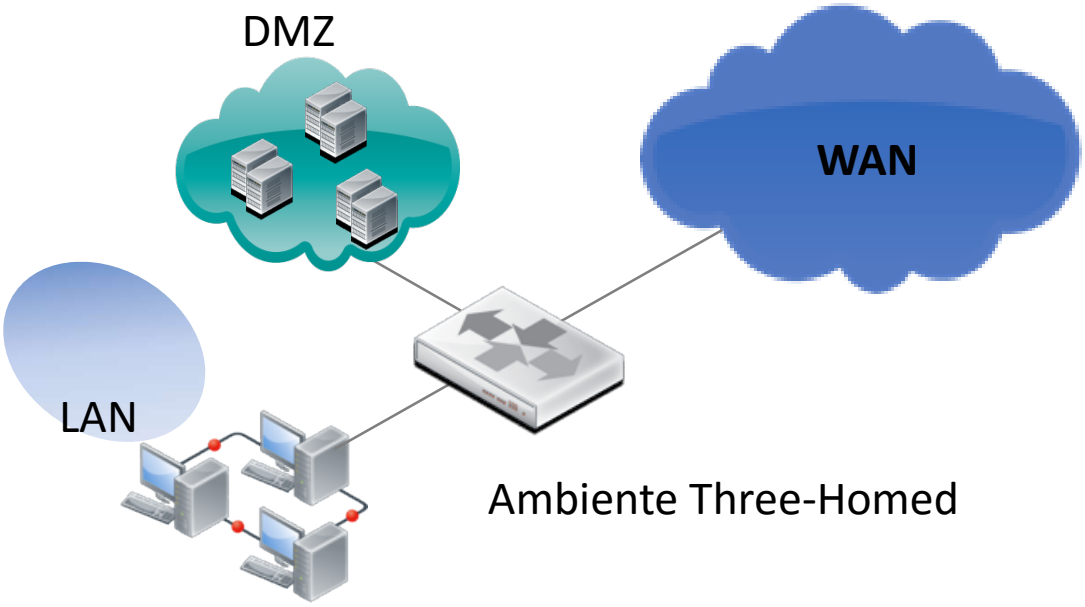
Todo o volume de tráfego mencionado tem por objetivo obter os resultados de cada equipamento NGFW firewall appliance através dos testes gerados pelos equipamentos Spirent baseados em suas respectivas na folha de dados, para cada um dos tipos de equipamentos ofertados.

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.

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

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 Neywork) 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

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:

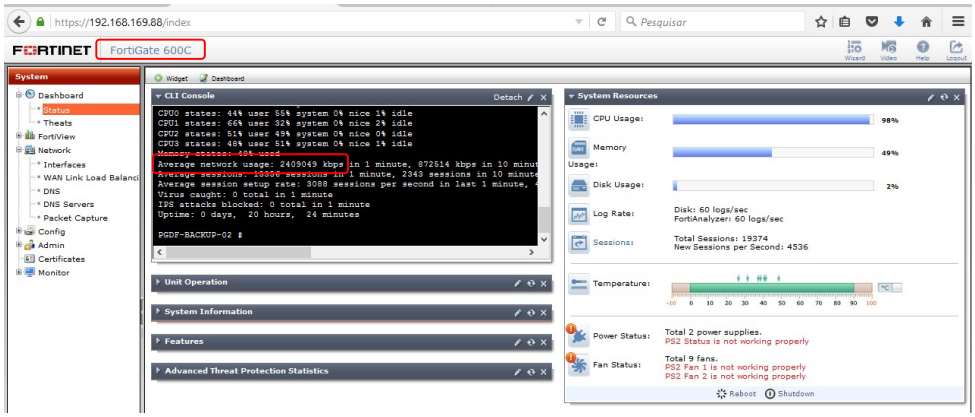
8.1. QUANTO AO DESEMPENHO

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.

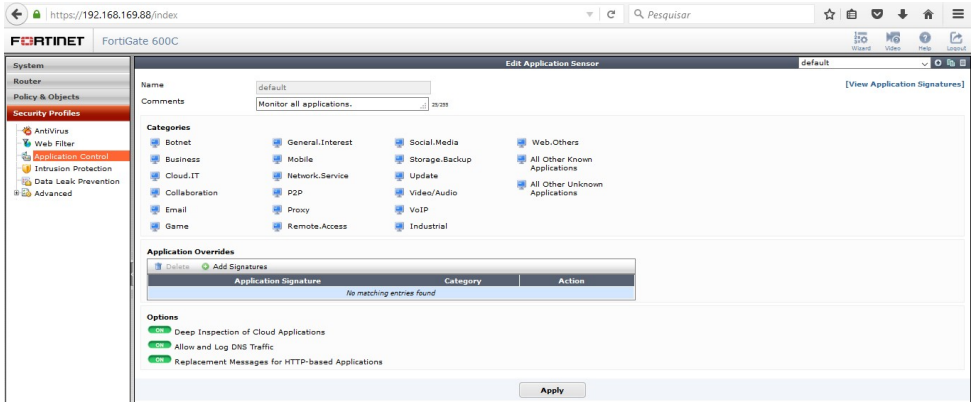
Item 1.6 - CARACTERÍSTICAS ESPECÍFICAS PARA OS 4 (QUATROS) APPLIANCES QUE COMPORÃO O CLUSTER DO SITE PRINCIPAL E DO SITE BACKUP:

Site Backup

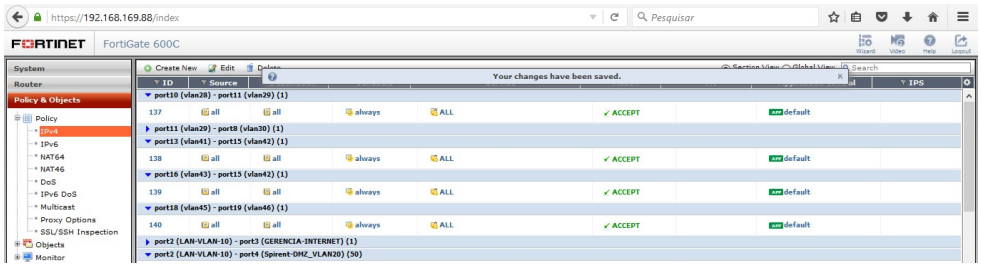
Item de Teste - 1.6.1.1	Os equipamentos que comporão o cluster do Site Backup (Firewall Appliance Tipo 2) deverão possuir um throughput mínimo de 2 (dois) Gbps para as funcionalidades de firewall com controle de aplicação habilitado e throughput mínimo de 1 (um) Gbps para controle de aplicativos, IPS, 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.

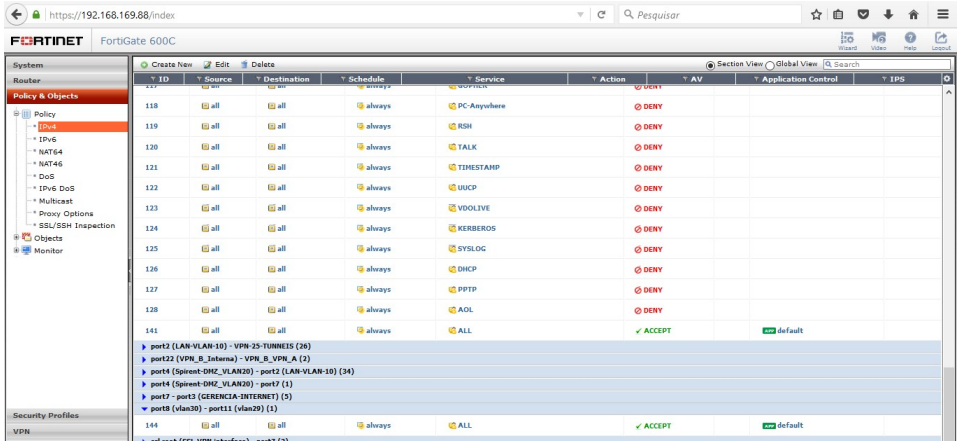


Equipamento alcançando throughput solicitado.



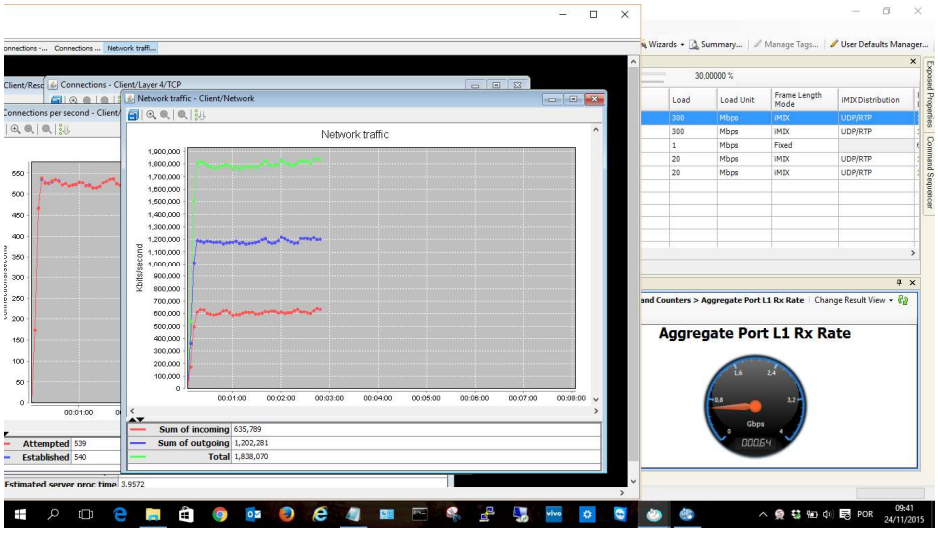
Sensor de APPControl configurado



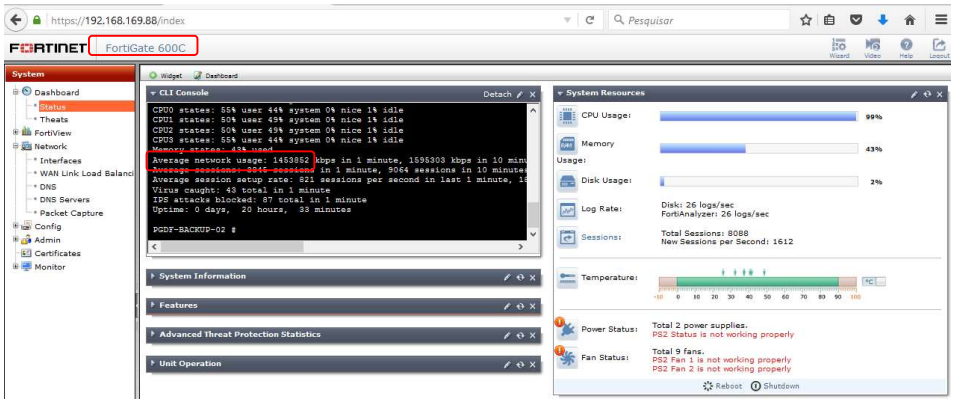


Regras de firewall.

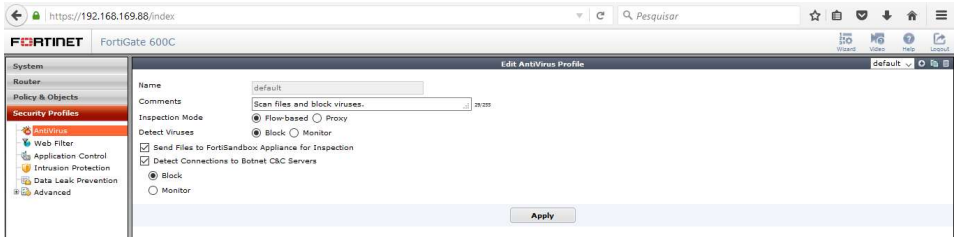
- Spirent



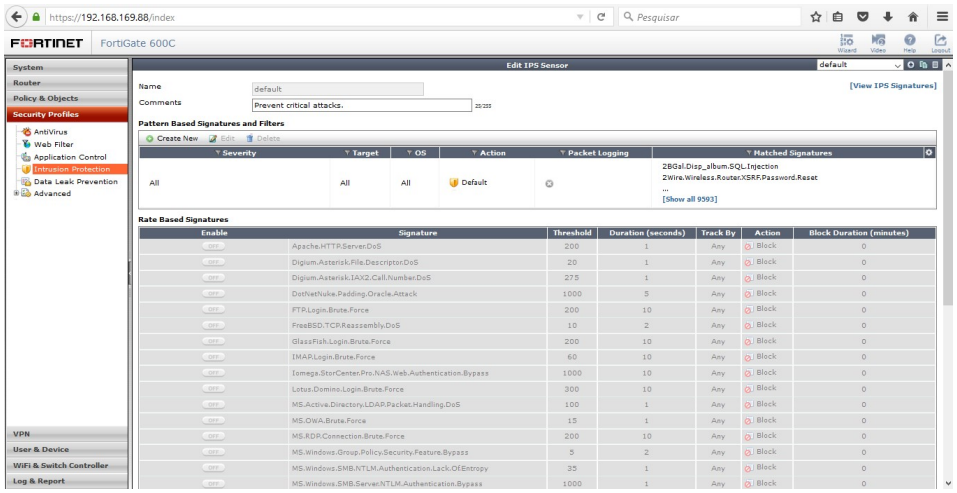
- Teste com APPContrl + AV + IPS



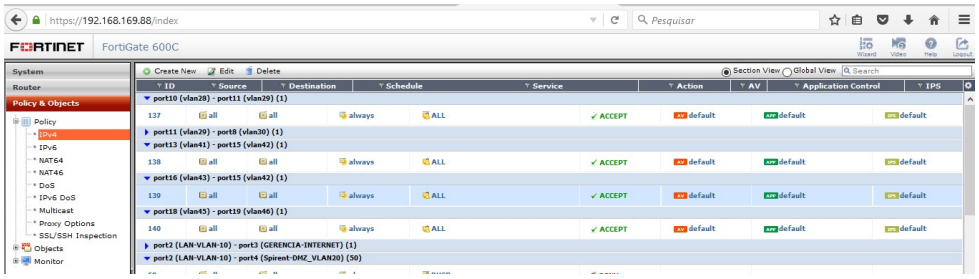
Equipamento alcançando throughput solicitado.

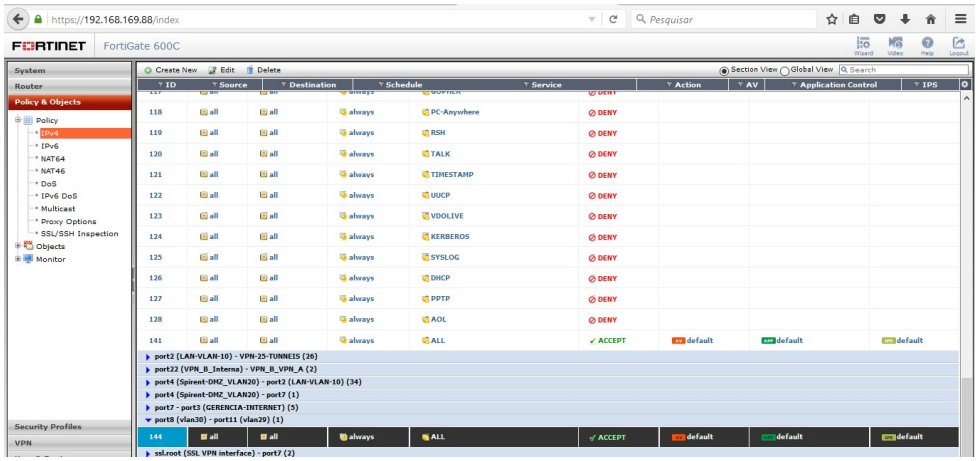


Sensor de AV



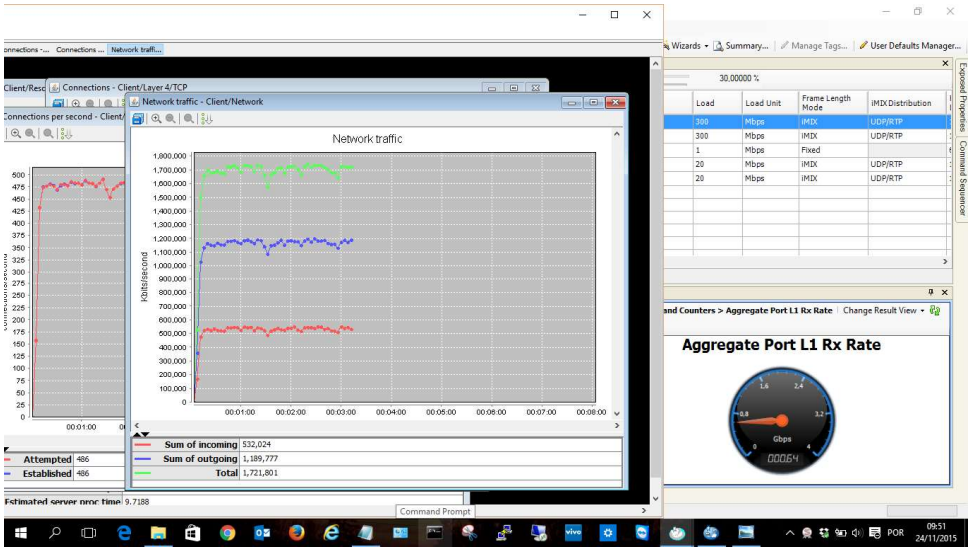
Sensor de IPS





Regras de firewall

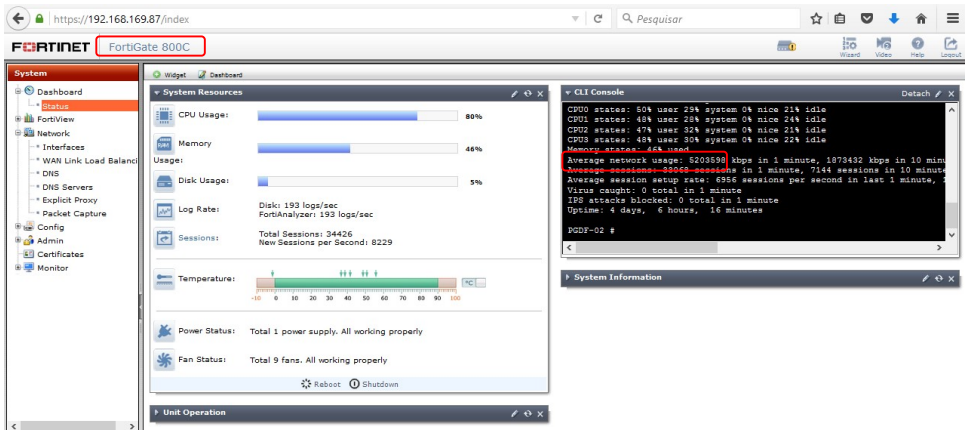
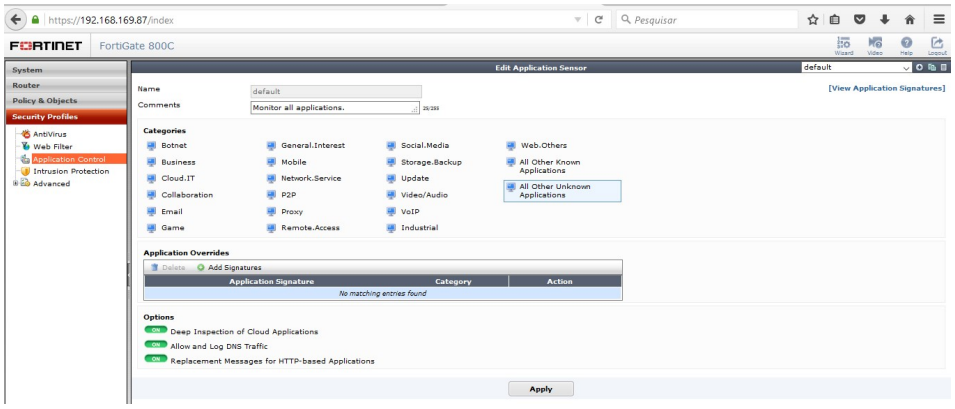
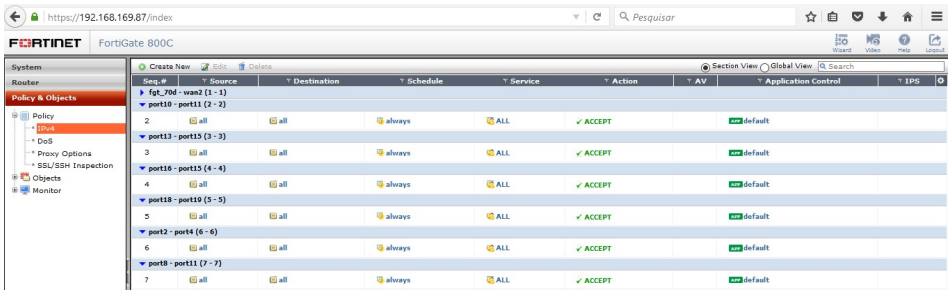
- Spirent

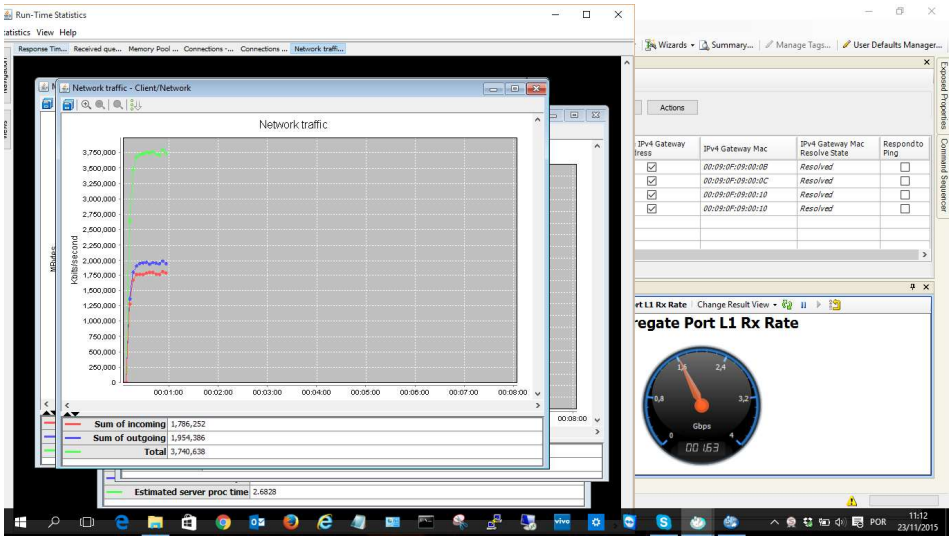


Comentário	Todas as configurações tanto do FGT 600C como do Spirent foram apresentadas/explicadas a todos os presentes na sala de homologação. Maiores detalhes sobre o relatório de tráfego gerado pelo spirent, podem ser encontrados no CD anexo a este caderno.
Assinatura do Cliente	**Assinatura NCT**

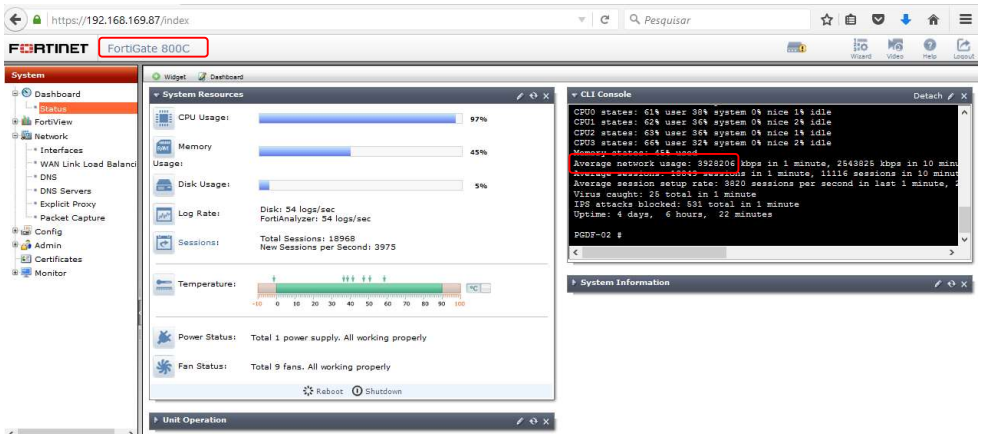
Site principal

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

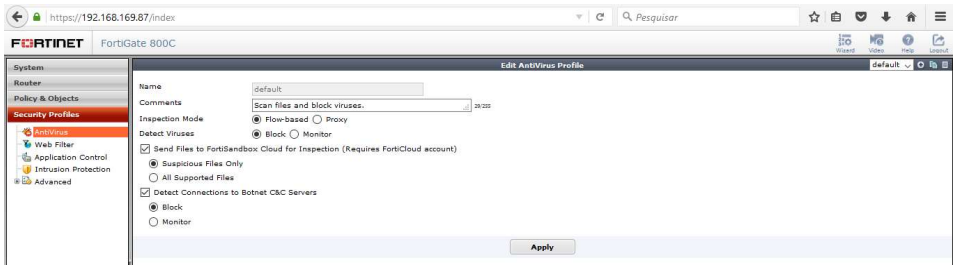
do Teste	solicitados neste edital foram alcançados no equipamento FGT 800C
Evidências	- 800C com APPControl  Equipamento alcançando throughput solicitado.  Sensor de AppControl  Regras de firewall - Spirent



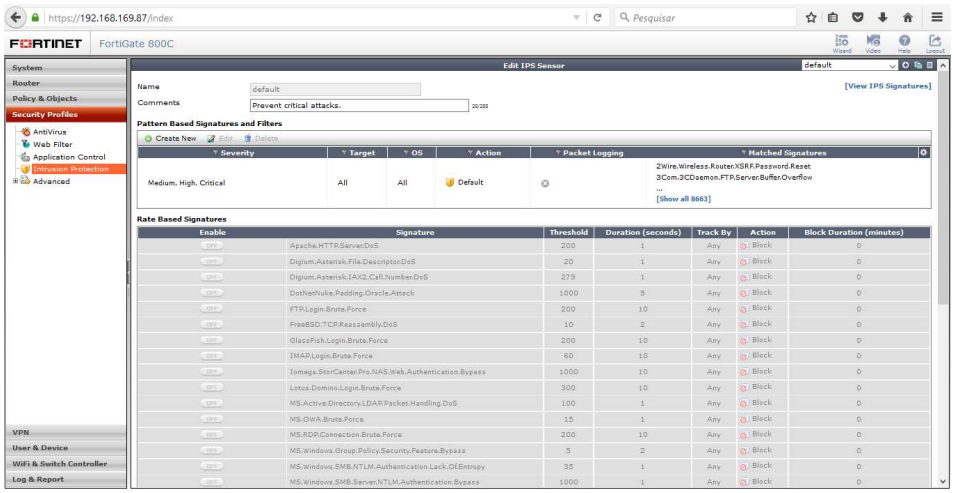
- 800C com AppControl + AV + IPS



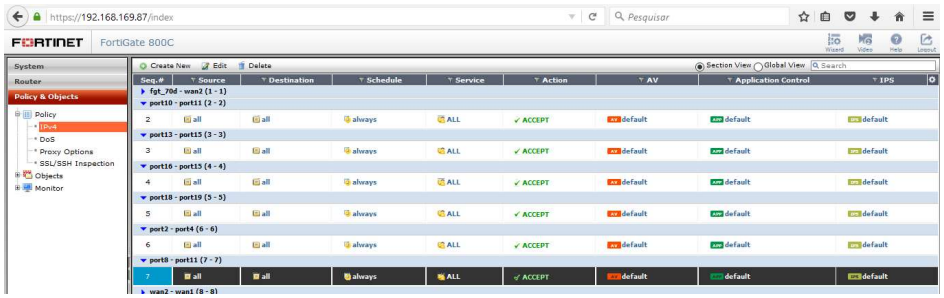
Equipamento alcançando throughput solicitado.



Sensor de AV

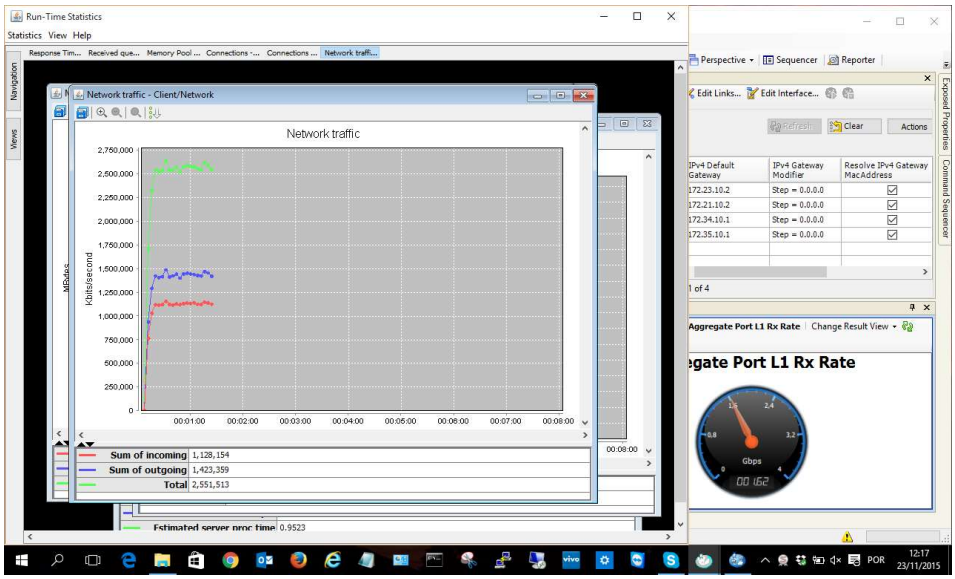


Sensor de IPS



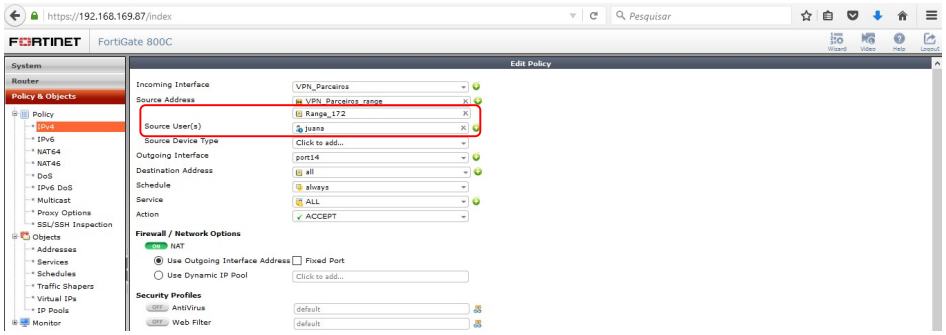
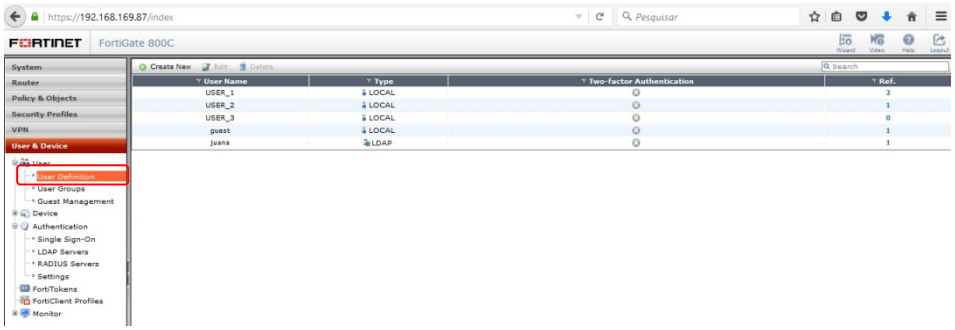
Regras de firewall

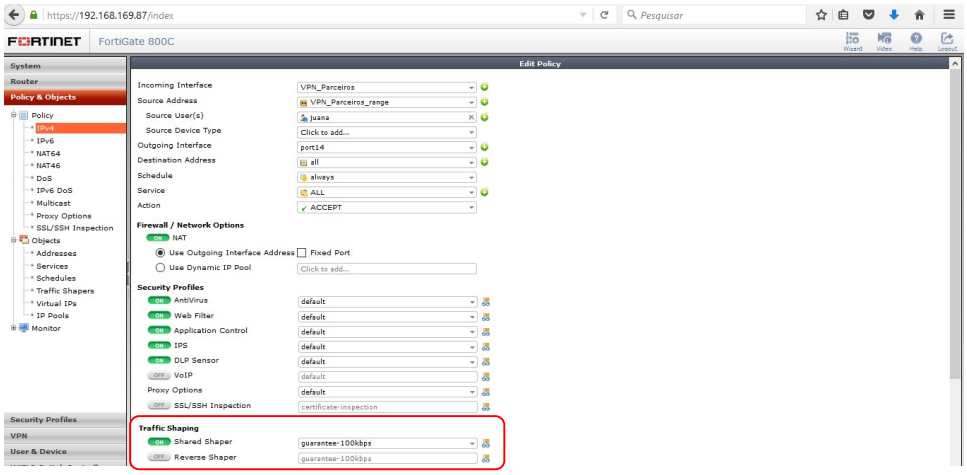
- Spirent

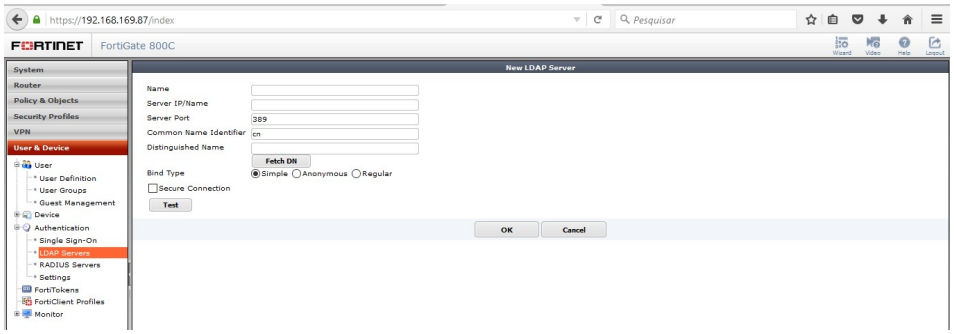


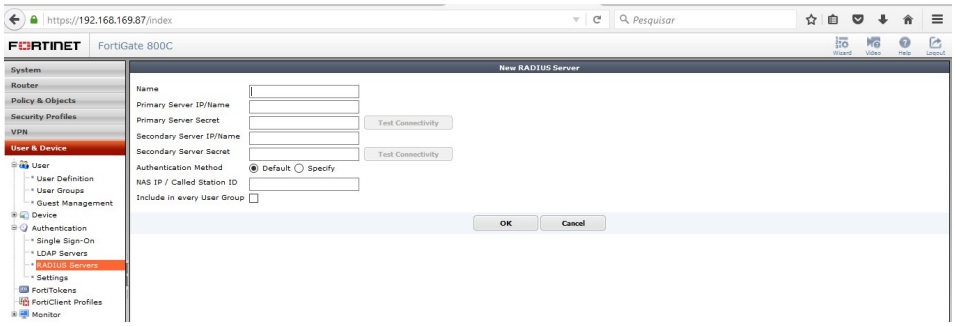
Comentário	Todas as configurações tanto do FGT 800C como do Spirent foram apresentadas/explicadas a todos os presentes na sala de homologação. Maiores detalhes sobre o relatório de trafego gerado pelo spirent, podem ser

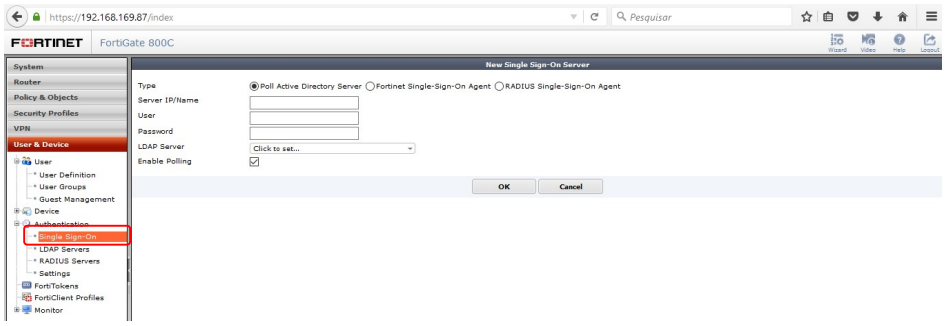
		encontrados no CD anexo a este caderno.	
Assinatura do Cliente		**Assinatura NCT**	

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

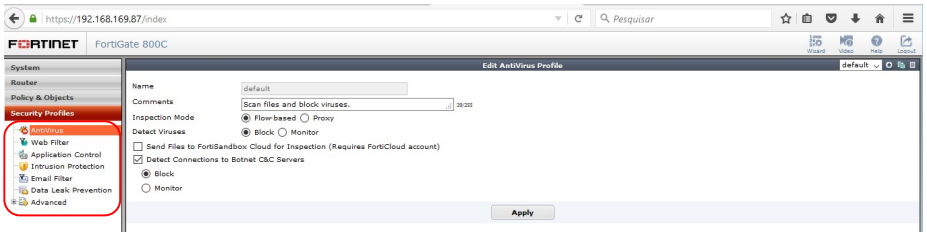


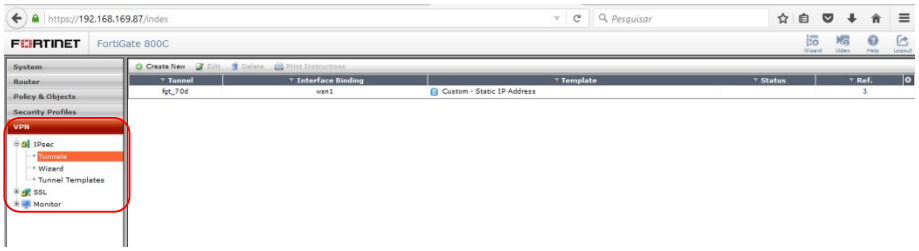


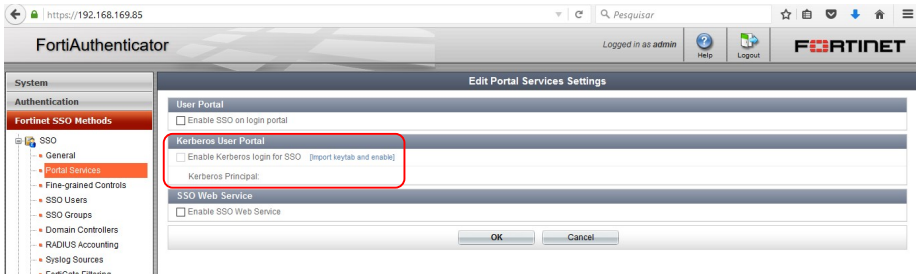




O acesso a microsoft active directory e eDirectory é realizado com a configuração de "single sign-on"

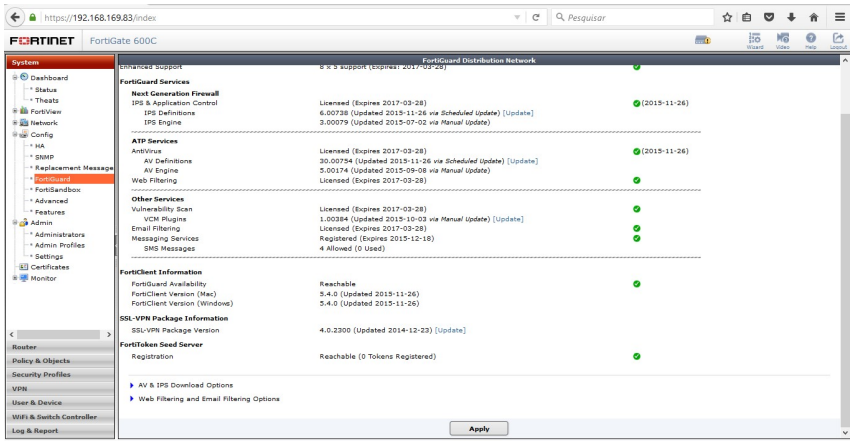


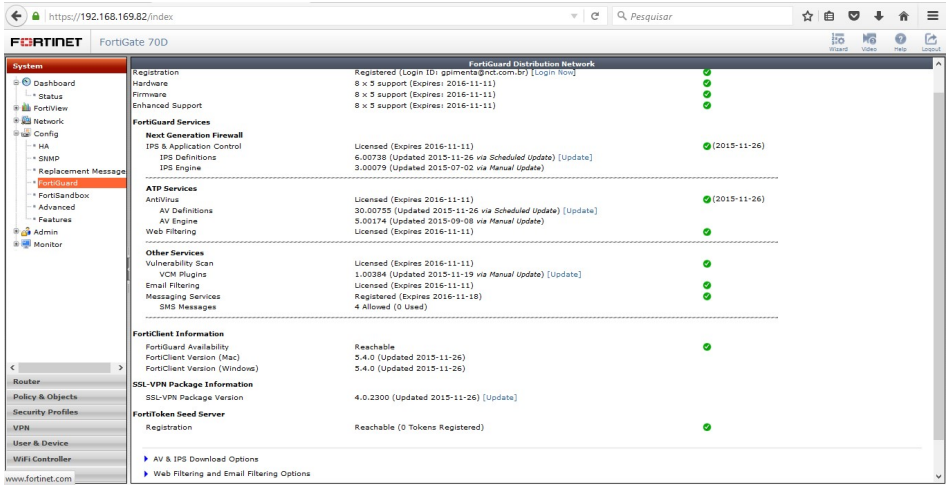


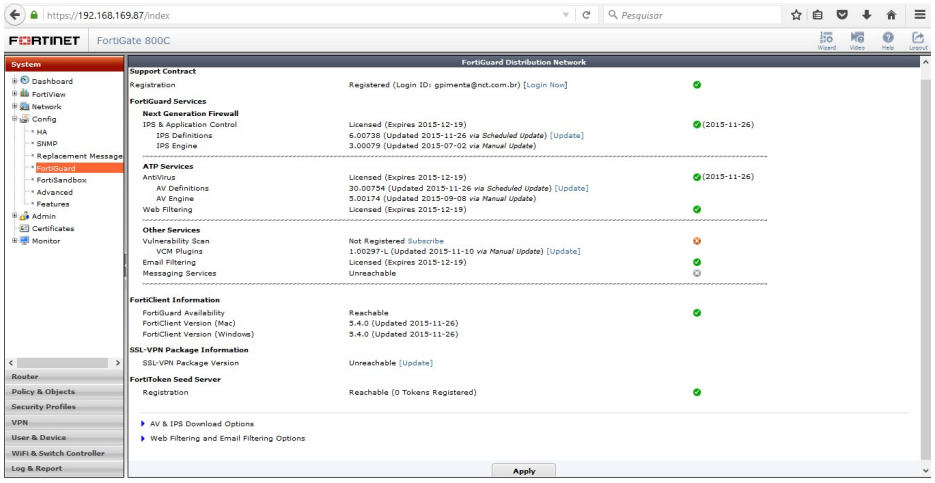


Comentário			
Assinatura do Cliente		**Assinatura NCT**	

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	

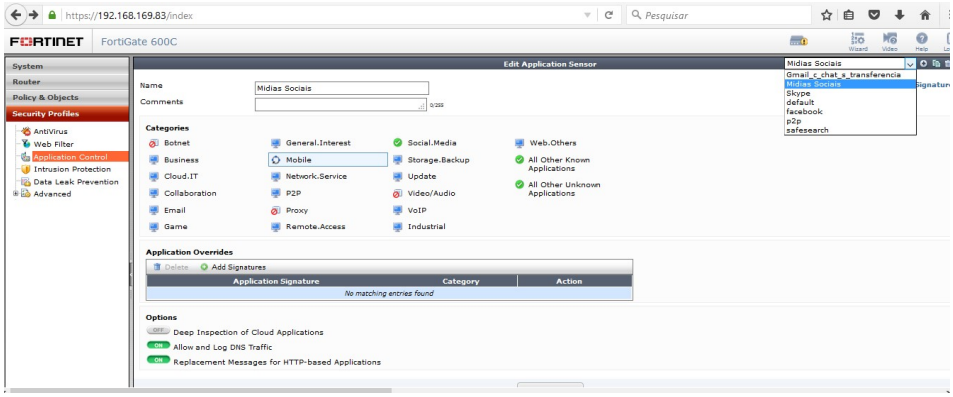
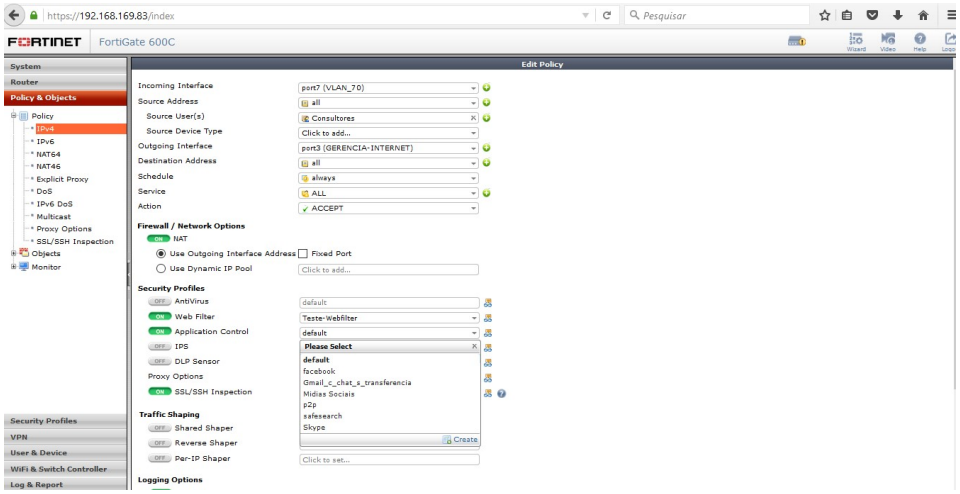






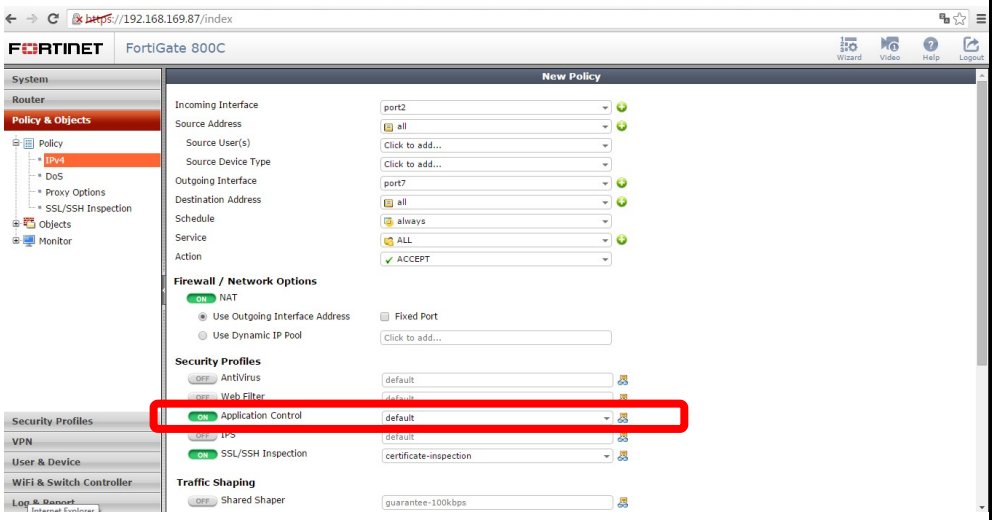
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

CONTROLE POR POLÍTICA DE FIREWALL

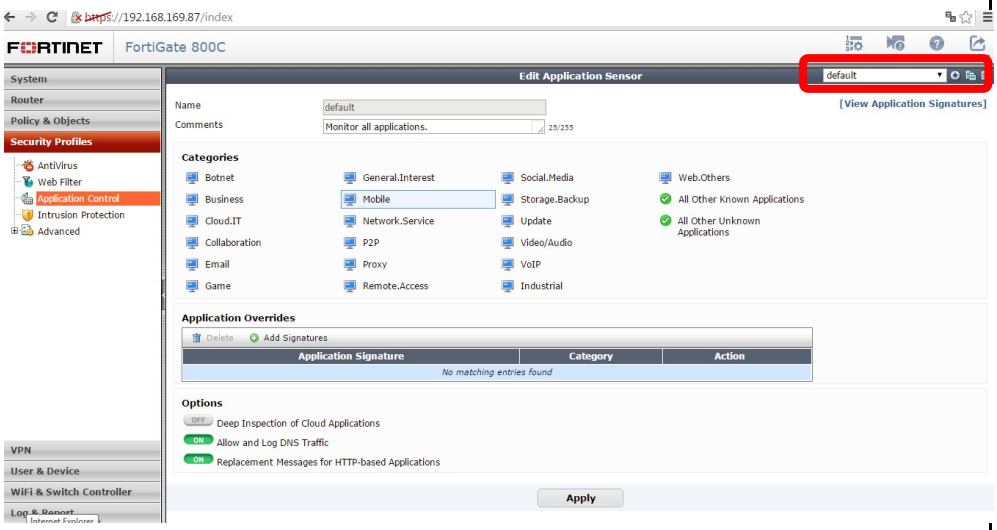
Item de Teste - 1.6.2.2	Controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento) e categorias de aplicações;
Objetivo do Teste	Demonstrar funcionalidade solicitada
Configuração do Teste	Configurado profiles de app 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 apçicações.
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

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:

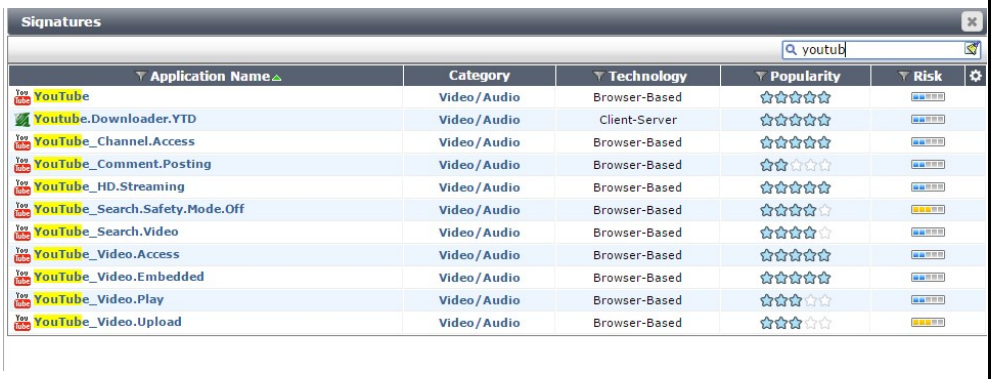


Configurado o perfil default liberando o youtube e todos os demais categorias:

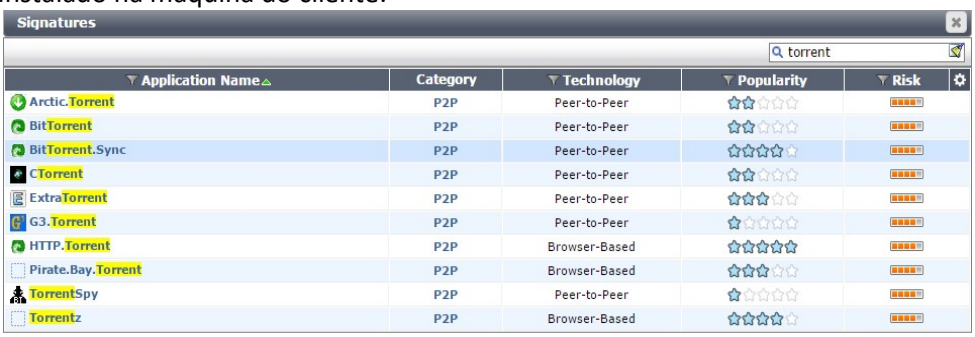


Em seguida selecionado as aplicações correspondente ao youtube para habilitar o

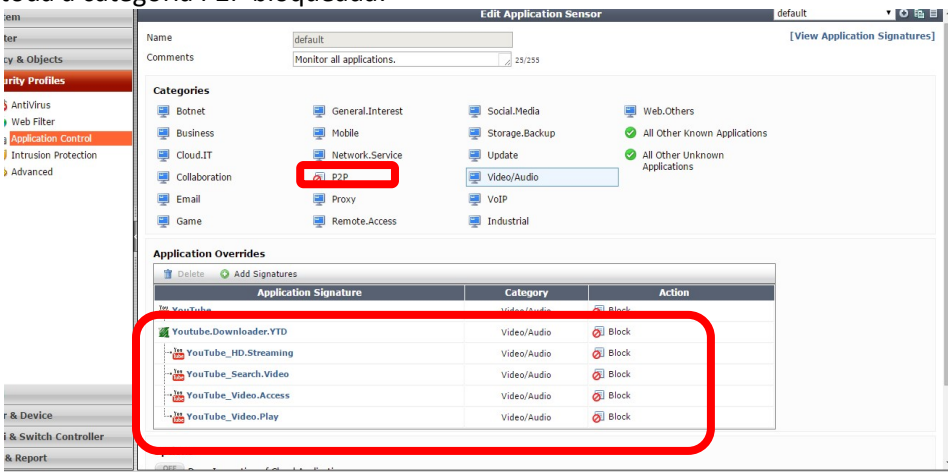
bloqueio apenas para estes:



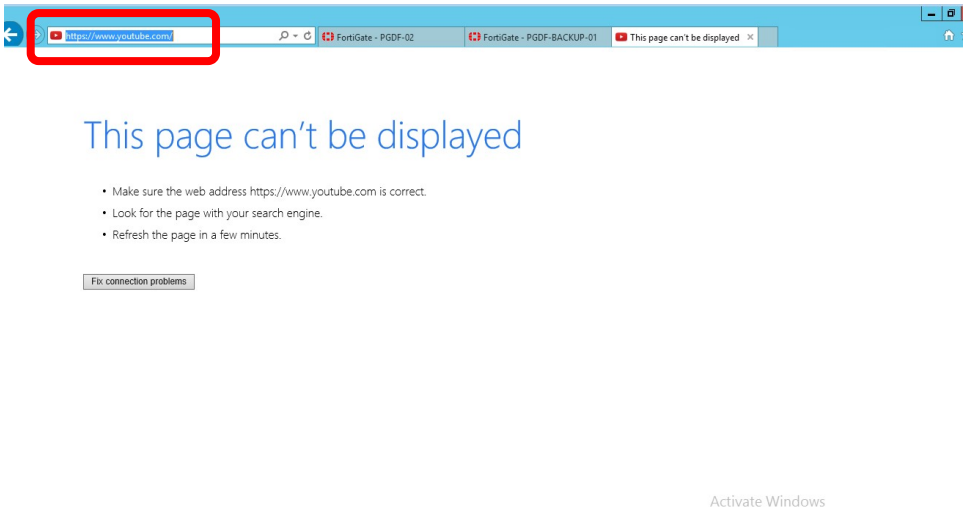
Selecionado o bloqueio de P2P tais como aplicações Bitorrent, que tem tambem instalado na máquina do cliente:



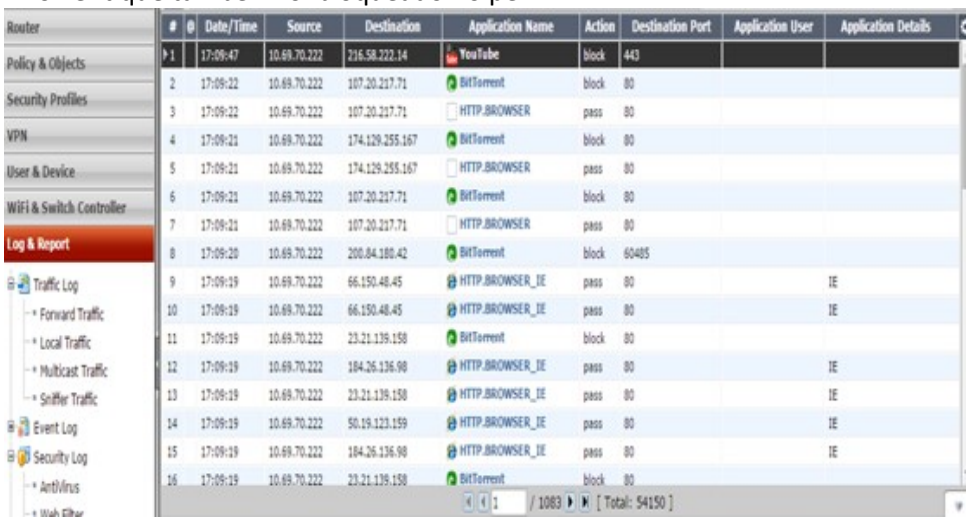
Perfil de controle de aplicação pronto com aplicações de youtube assim como toda a categoria P2P bloqueada:



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:



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



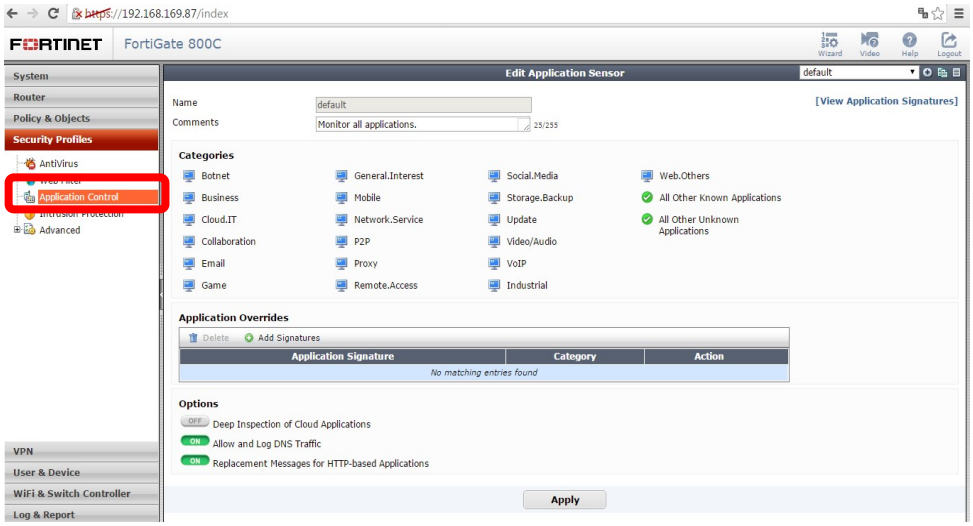
#	Date/Time	Source	Destination	Application Name	Action	Destination Port	Application User	Application Details
1	17:09:47	10.69.70.222	216.58.222.14	YouTube	block	443		
2	17:09:22	10.69.70.222	107.20.217.71	BitTorrent	block	80		
3	17:09:22	10.69.70.222	107.20.217.71	HTTP.BROWSER	pass	80		
4	17:09:21	10.69.70.222	174.129.255.167	BitTorrent	block	80		
5	17:09:21	10.69.70.222	174.129.255.167	HTTP.BROWSER	pass	80		
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		
8	17:09:20	10.69.70.222	200.84.180.42	BitTorrent	block	60485		
9	17:09:19	10.69.70.222	66.150.48.45	HTTP.BROWSER_IE	pass	80		IE
10	17:09:19	10.69.70.222	66.150.48.45	HTTP.BROWSER_IE	pass	80		IE
11	17:09:19	10.69.70.222	23.21.139.158	BitTorrent	block	80		
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
14	17:09:19	10.69.70.222	50.19.123.159	HTTP.BROWSER_IE	pass	80		IE
15	17:09:19	10.69.70.222	184.26.136.98	HTTP.BROWSER_IE	pass	80		IE
16	17:09:19	10.69.70.222	23.21.139.158	BitTorrent	block	80		

Comentário	
Assinatura do Cliente	**Assinatura NCT**

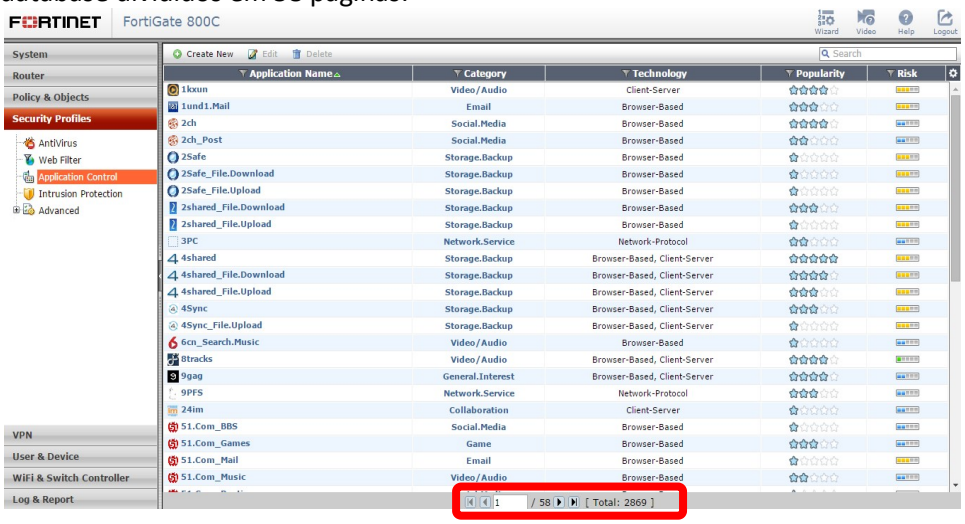
Item de Teste - 1.6.3.1.2	Reconhecer, no mínimo, 1.500 (um mil e quinhentas) aplicações diferentes, incluindo, mas não limitado: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, atualizações de software, protocolos de rede, VOIP, áudio, vídeo, proxies, mensageiros instantâneos, compartilhamento 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	

Evidências

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

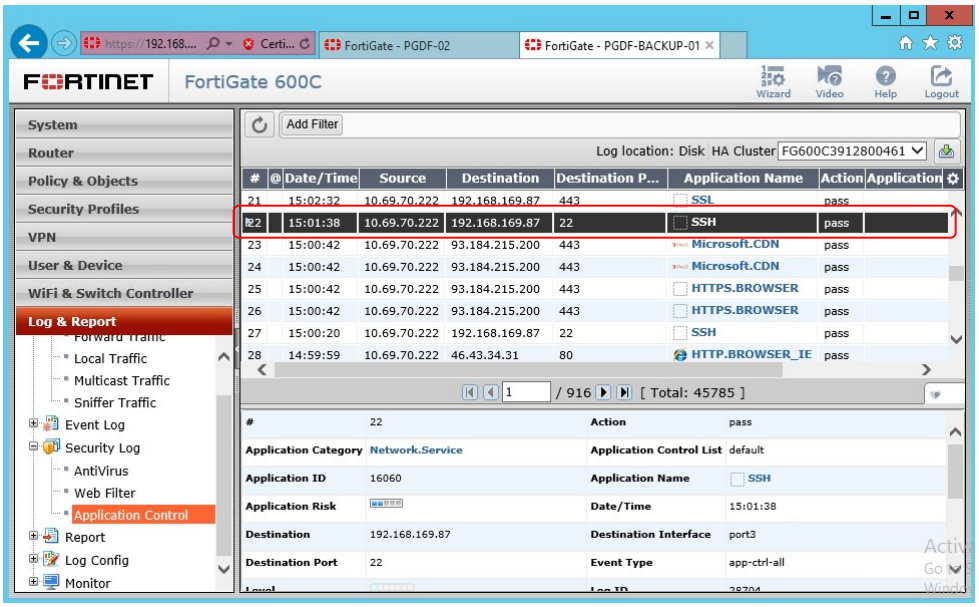
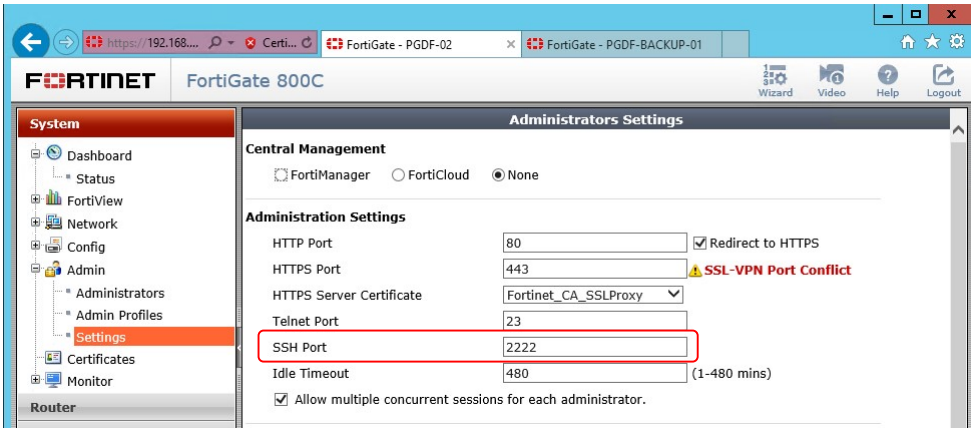


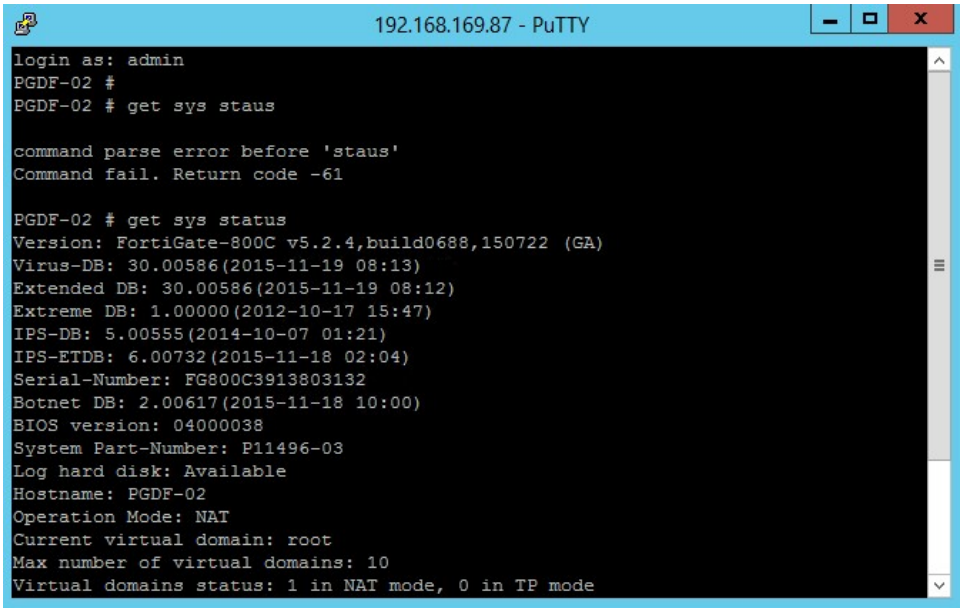
Segue abaixo a tela contendo uma demonstração do "View Application Signatures", o qual é possível observar que há mais de 2000 aplicações no database divididos em 58 páginas:

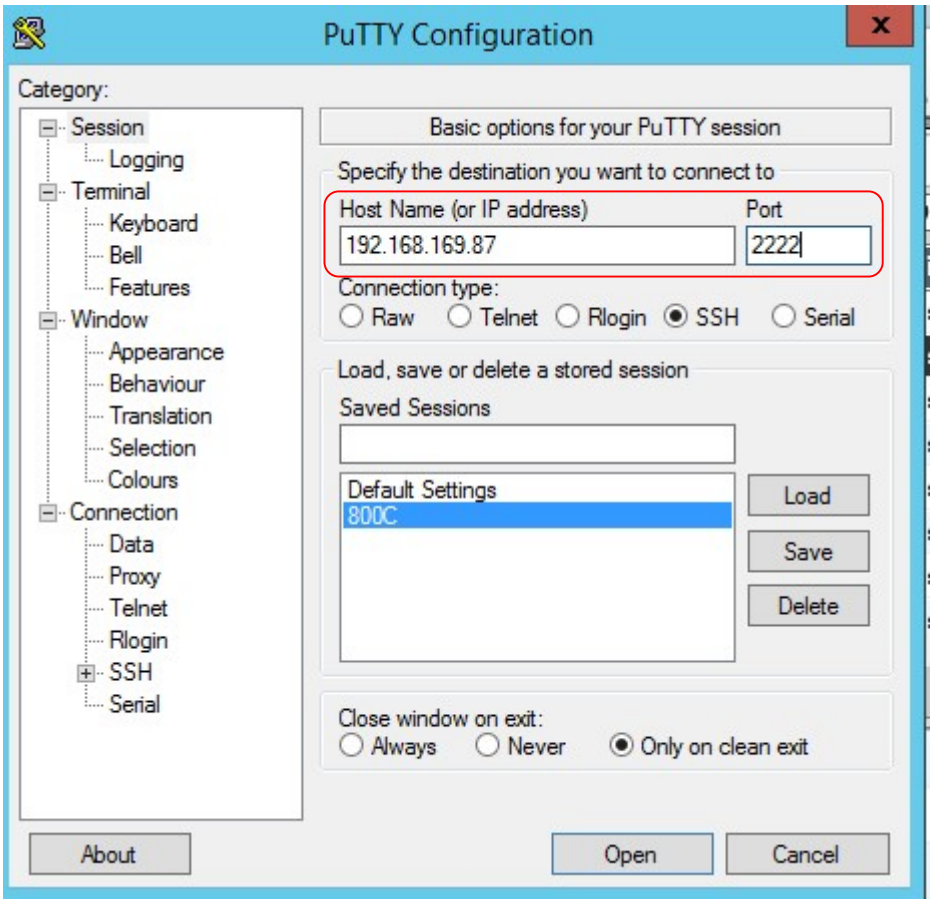


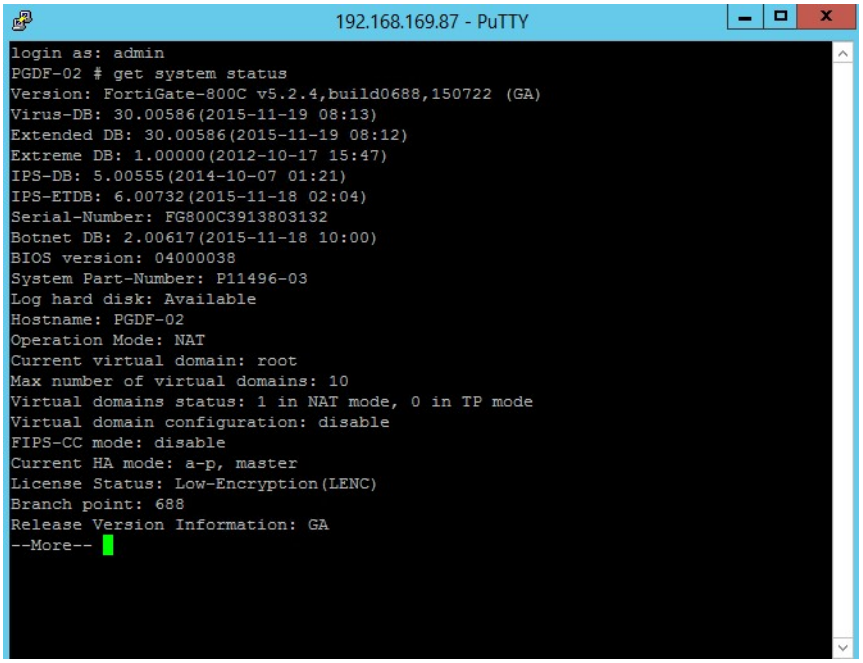
Comentário		
Assinatura do Cliente	**Assinatura NCT**	

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;

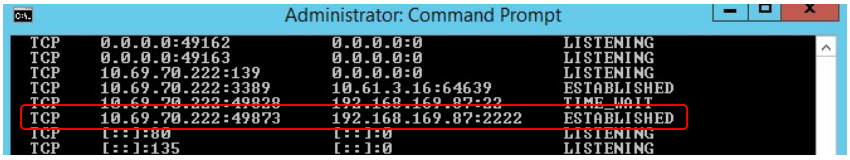
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado
Configuração do Teste	Foi utilizado um teste onde a porta padrão do SSH foi alterada para demonstrar que mesmo em outra porta o equipamento consegue identificar corretamente a aplicação.
Procedimento do Teste	Usar o putty para logar na 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

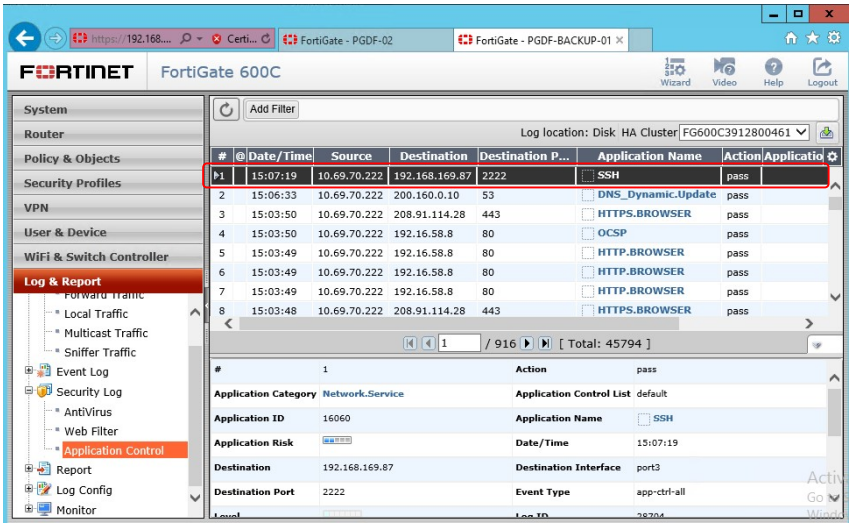

PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Serial
Basic options for your PuTTY session
Specify the destination you want to connect to
Host Name (or IP address)
Port
192.168.169.87
2222
Connection type:
Raw
Telnet
Rlogin
SSH
Serial
Load, save or delete a stored session
Saved Sessions
Default Settings
800C
Load
Save
Delete
Close window on exit:
Always
Never
Only on clean exit
About
Open
Cancel



Acessado pela porta 2222

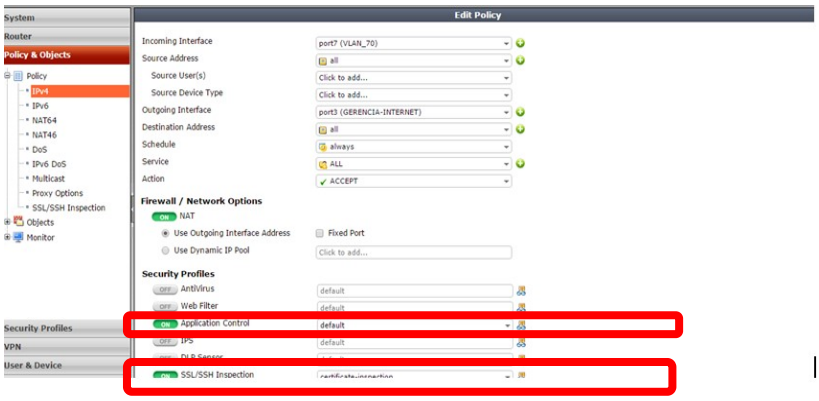


Conexão estabelecida pela porta 2222

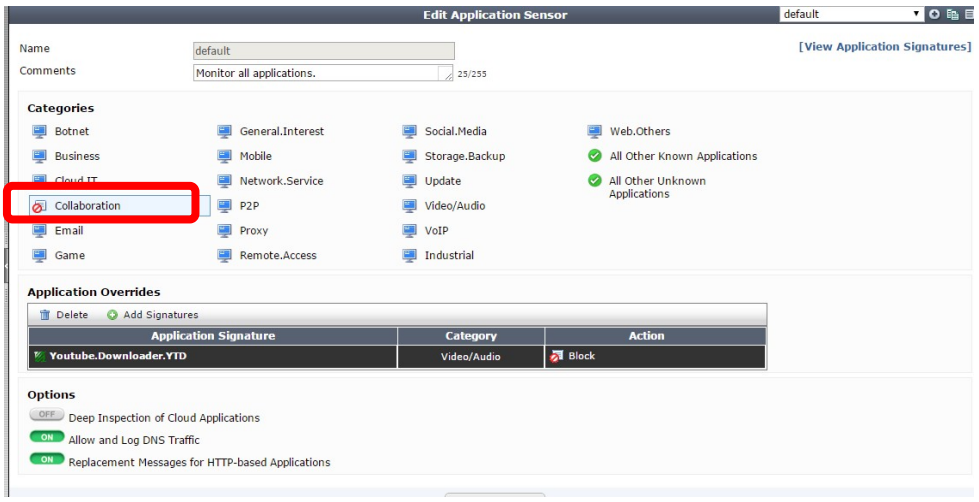


Comentário			
Assinatura do Cliente		**Assinatura NCT**	

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 trafego 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 :

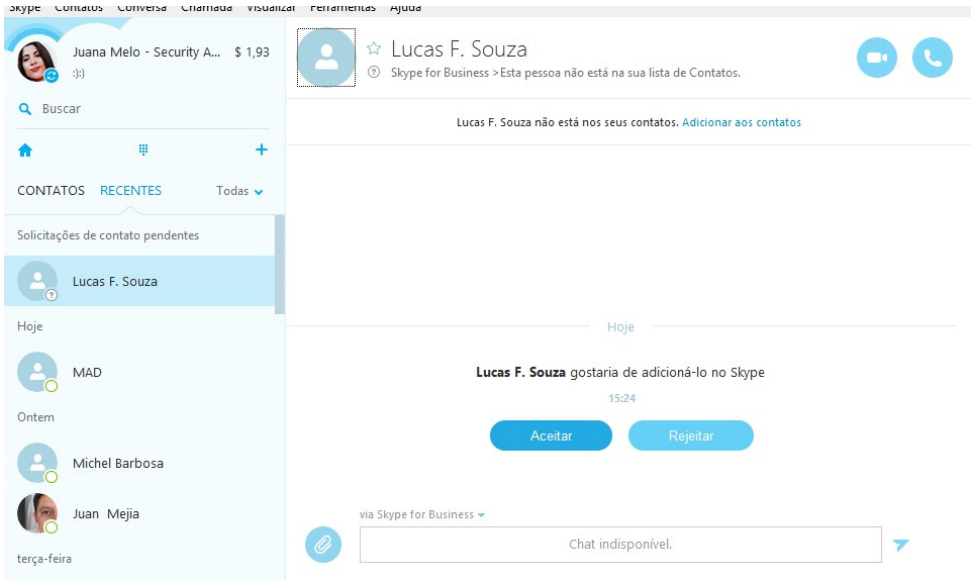


O perfil inserido na regra correspondente ao default onde foi configurado o bloqueio de toda a categoria "collaboration" a qual o Skype esta inserido:

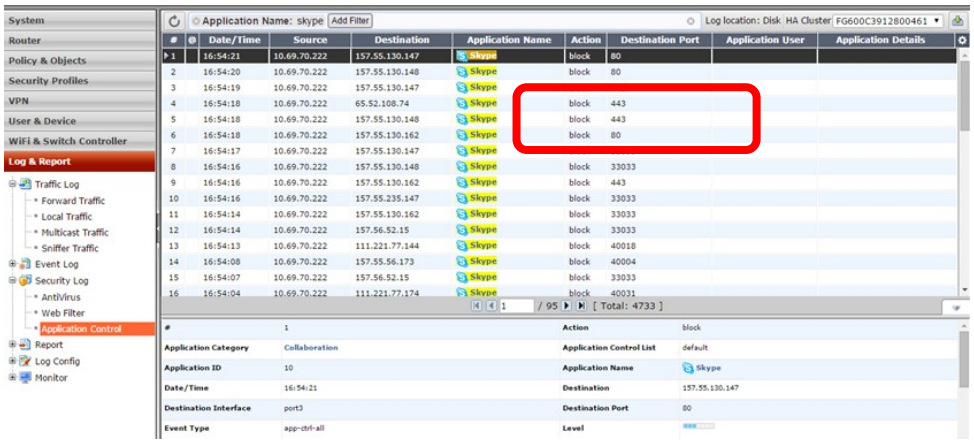


Application Name	Category	Technology
FakeSkype.Botnet	Botnet	Client-Server
Skype	Collaboration	Peer-to-Peer

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:



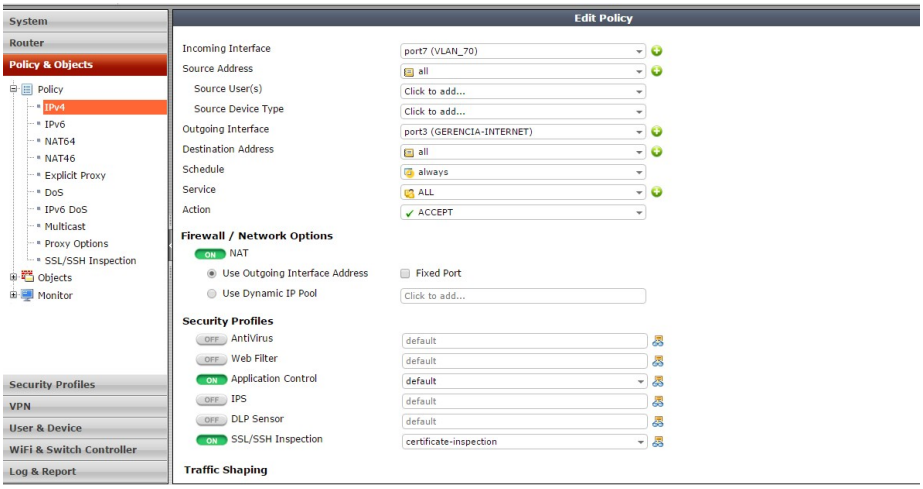
No Log mostra vários eventos de bloqueio do Skype do usuário pela porta 443:



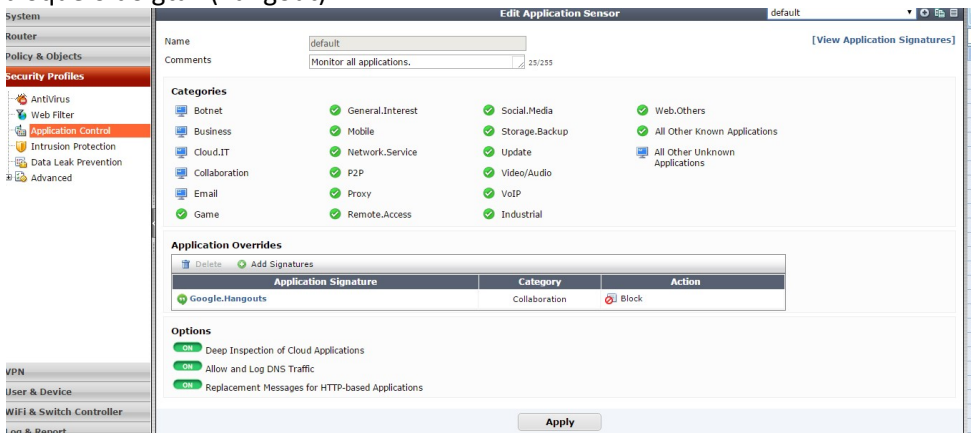
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

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

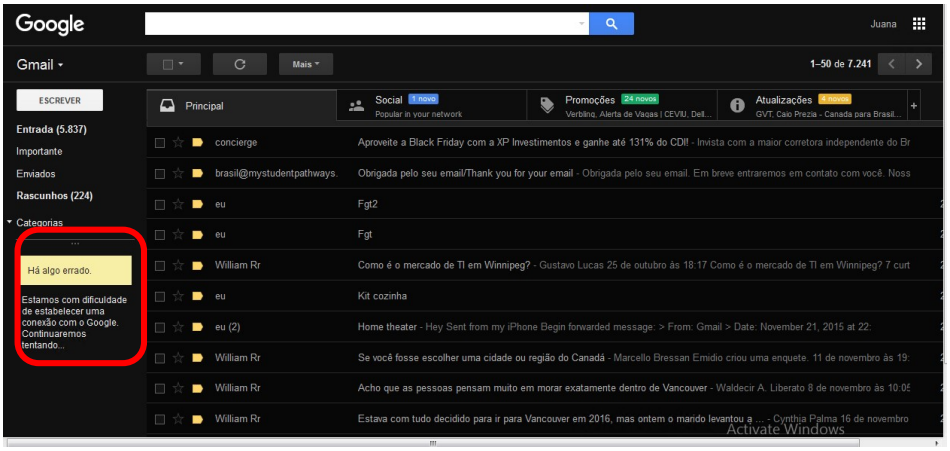
	deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado a: compartilhamento de arquivo dentro do Webex. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas;
Objetivo do Teste	Demonstrar a funcionalidade 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):



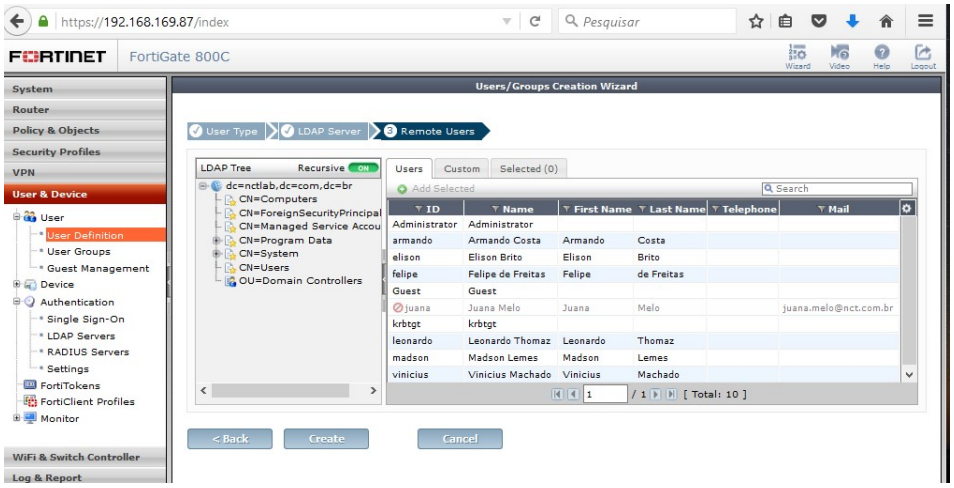
Cliente conseguiu acessar o gmail mais o gtalk (hangout) foi bloqueado, todos conexão segura SSL:



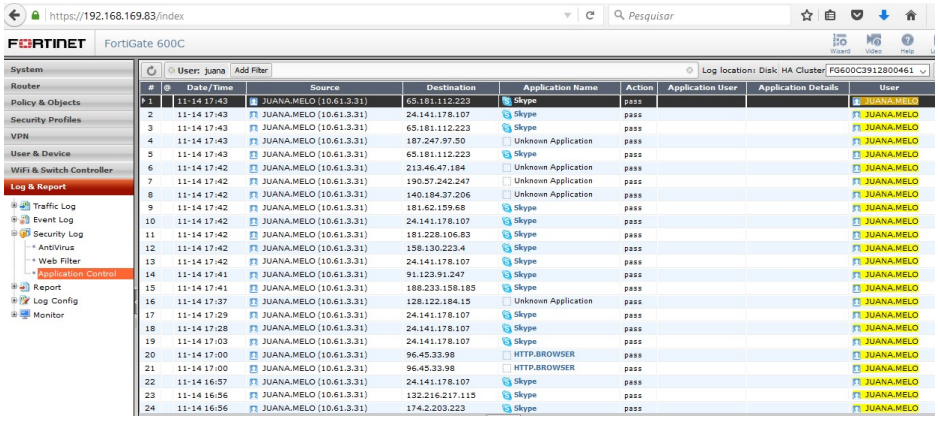
Log no firewall mostrando o acesso normal ao gmail e o block ao hangout na porta 443:

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	

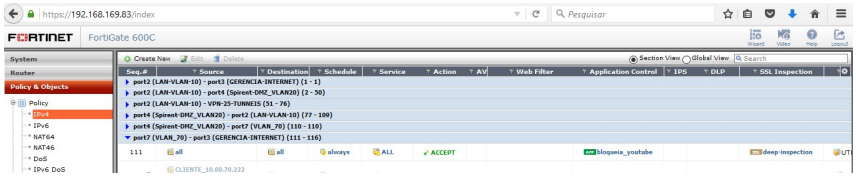


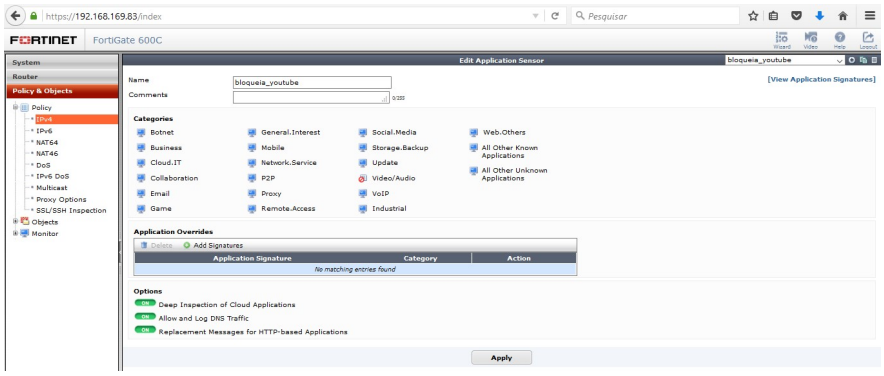
Fortigate integrado com servidor Microsoft AD



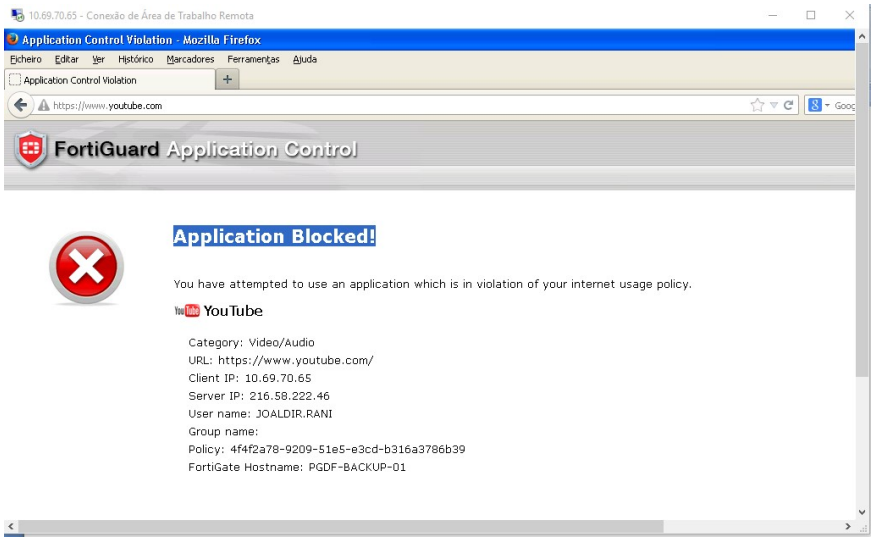
Log de atividade de usuário identificado do Microsoft AD sem agente.

Comentário			
Assinatura do Cliente		**Assinatura NCT**	

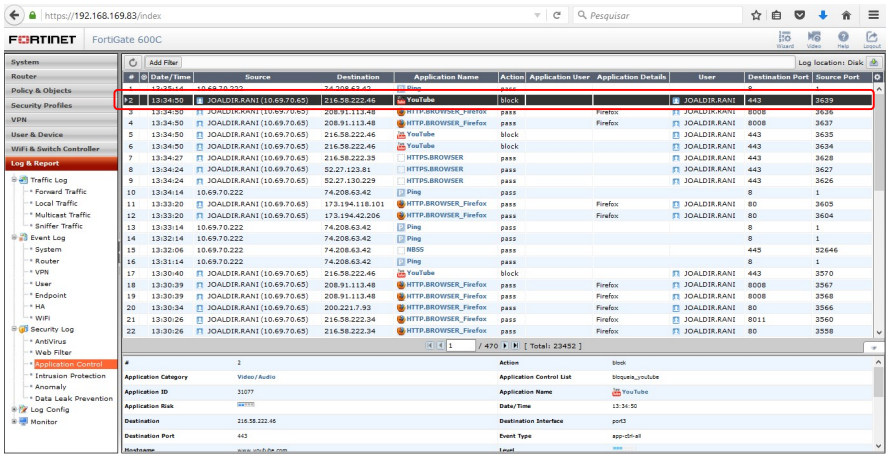
Item de Teste - 1.6.3.1.18	Deve alertar o usuário quando uma aplicação for bloqueada
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado
Configuração do Teste	Configurar replecement messages para " Application Control Block Page"
Procedimento do Teste	Validar a mensagem de bloqueio por um usuário ao acessa uma aplicação bloqueada e homologar a replecement messages.
Evidências	 Regra de firewall



Sensor de AppControl

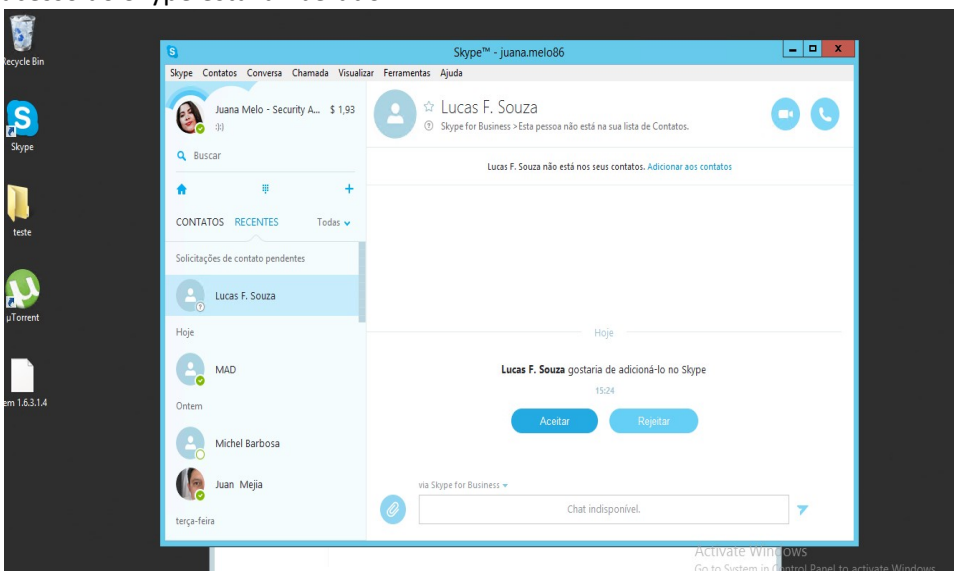
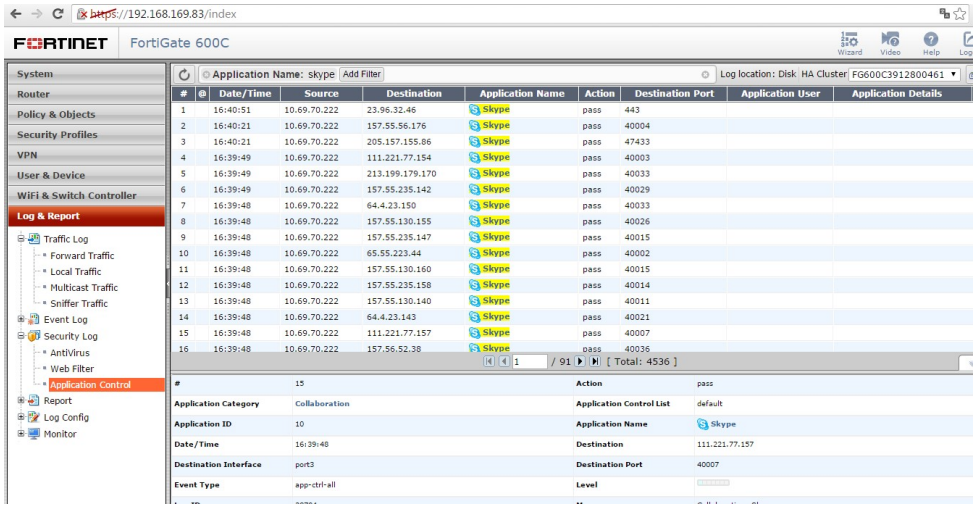


Tela de bloqueio ao acessar aplicação bloqueada.

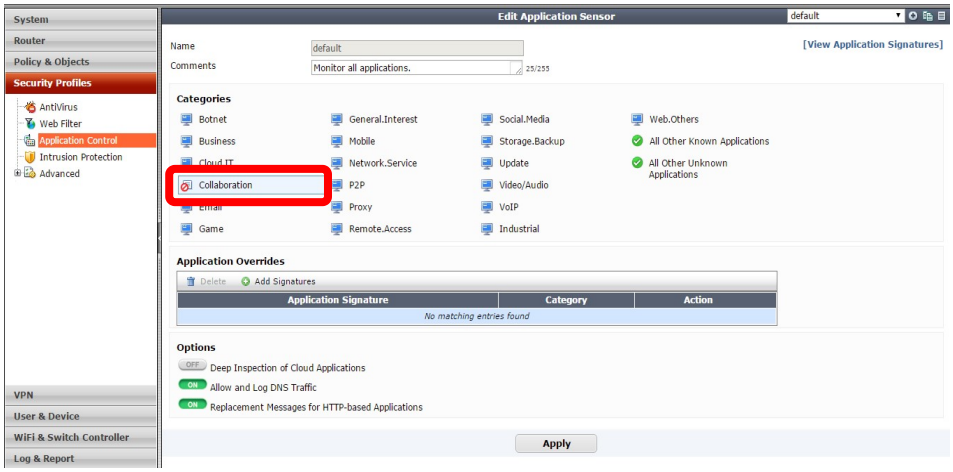


Comentário			
Assinatura do Cliente		**Assinatura NCT**	

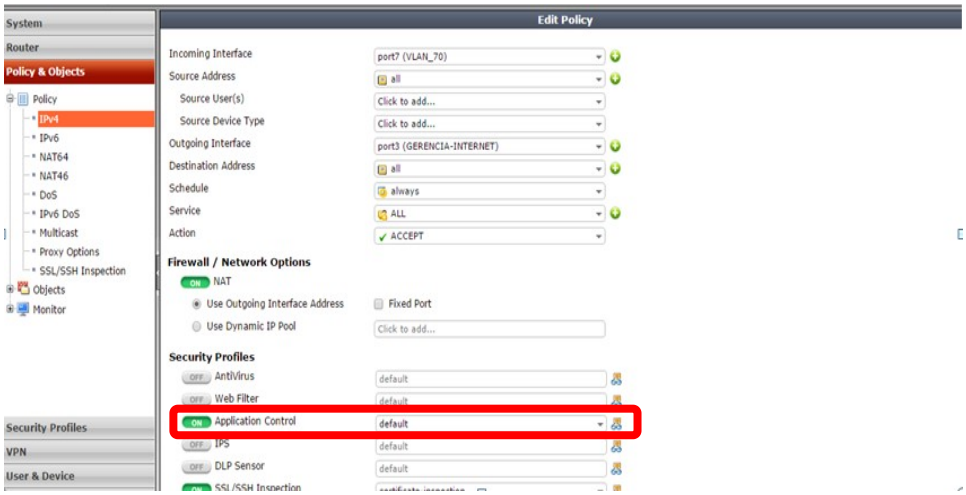
Item de Teste	Deve possibilitar que o controle de portas seja aplicado para todas as

- 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 efetivou 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: 

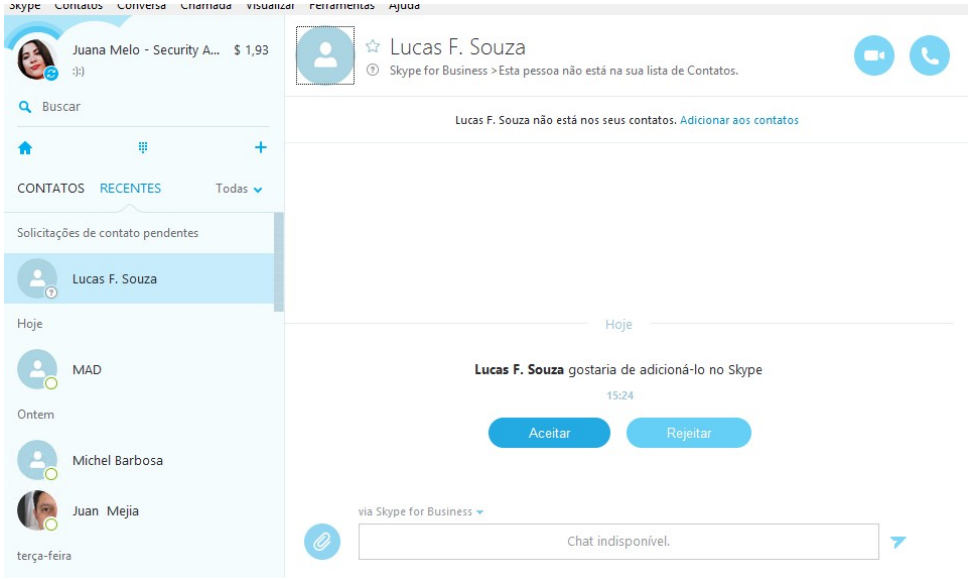
Configurando o perfil de controle de aplicação bloqueando a categoria Collaboration a qual o Skype está inserido:



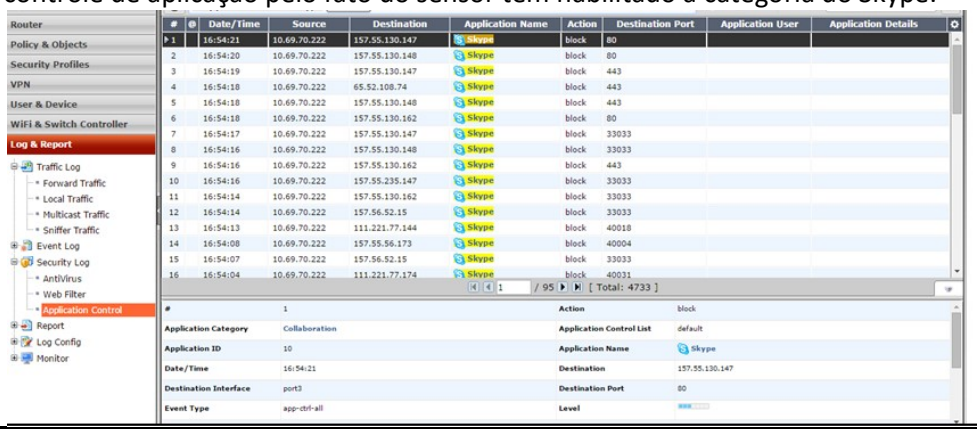
Na regra de Firewall foi inserido o perfil de default de controle de aplicação contendo as especificas configurações conforme executado acima:



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

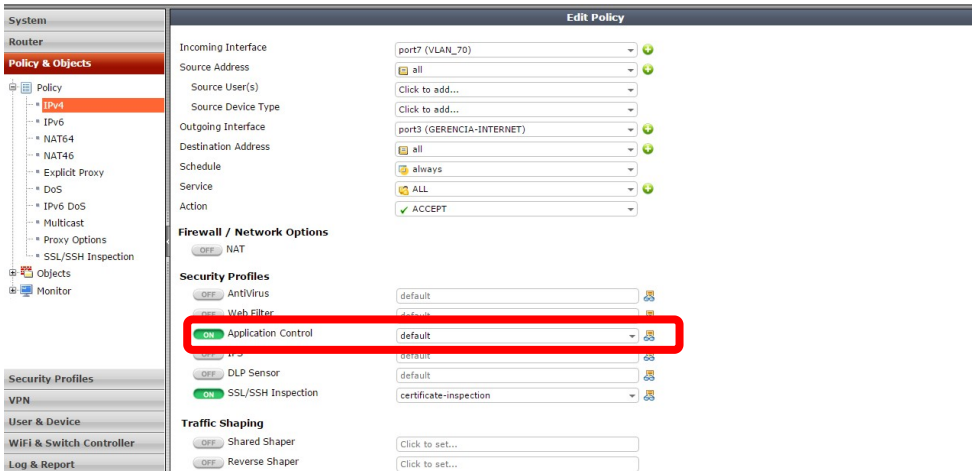


No Log é possivel observar que o usuário esta sendo bloqueado pelo filtro de controle de aplicação pelo fato do sensor tem habilitado a categoria do Skype:

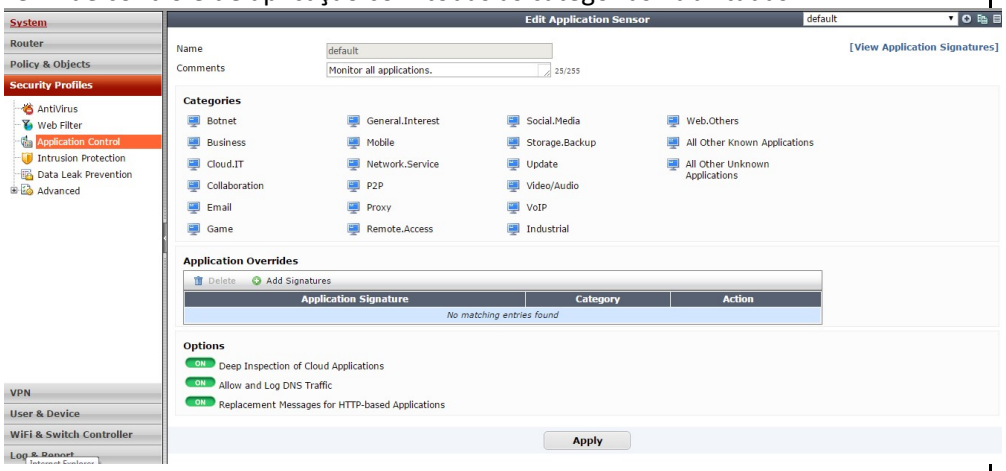


Comentário			
Assinatura do Cliente		**Assinatura NCT**	

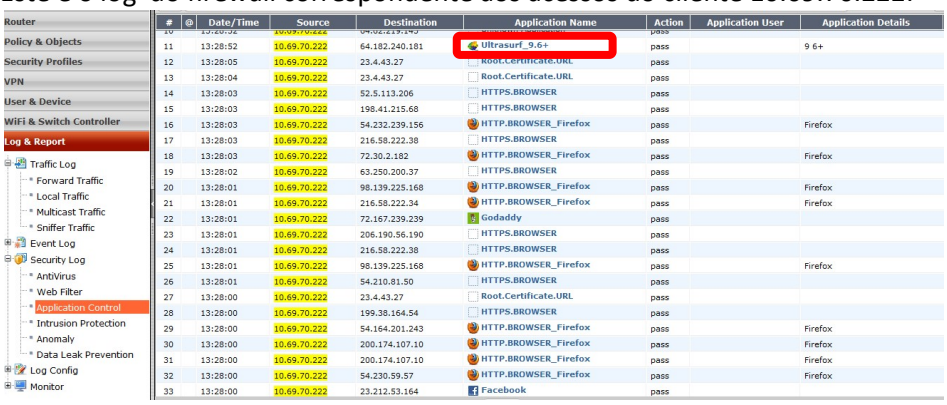
Item de Teste - 1.6.3.1.20	Deve possibilitar a diferenciação de tráfego peer-to-peer (bittorrent, emule, neonet e etc.), proxies (ghostsurf, freegate, ultrasurf e etc.) e Instant Messaging (AIM, Gtalk, Facebook Chat, etc.), permitindo controle granular nas políticas definidas para ambos;
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado
Configuração do Teste	Configurar profile de APP control, especificando ações especificas 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 logo 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:



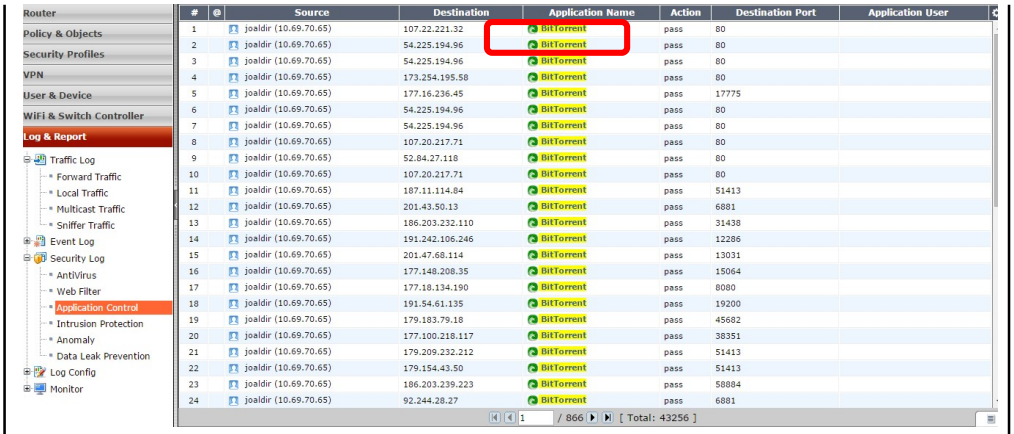
Perfil de controle de aplicação com todas as categorias habilitadas :

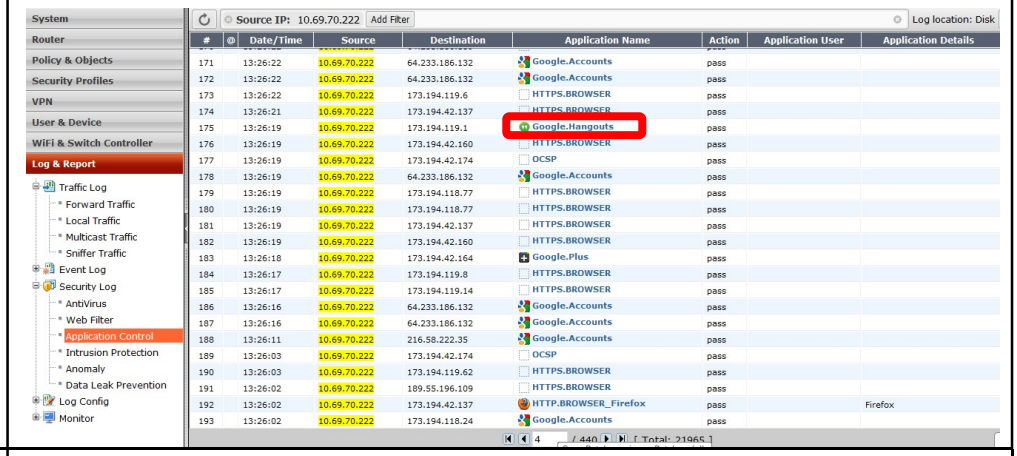


Este é o log do firewall correspondente aos acessos do cliente 10.69.70.222:



#	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	HTTPS.BROWSER	pass		
15	13:28:03	10.69.70.222	198.41.215.68	HTTPS.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	HTTPS.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	HTTPS.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	HTTPS.BROWSER	pass		
24	13:28:01	10.69.70.222	216.58.222.38	HTTPS.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	HTTPS.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	HTTPS.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		

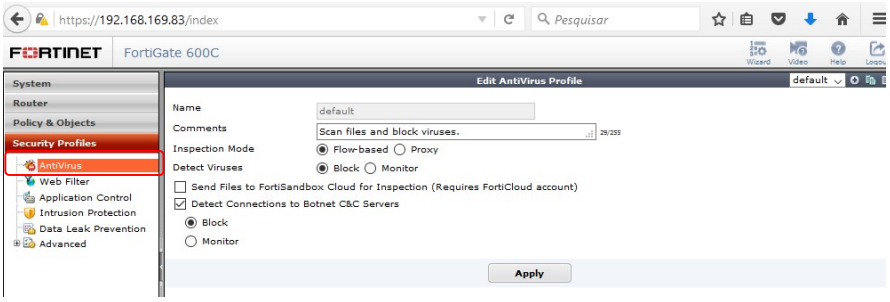




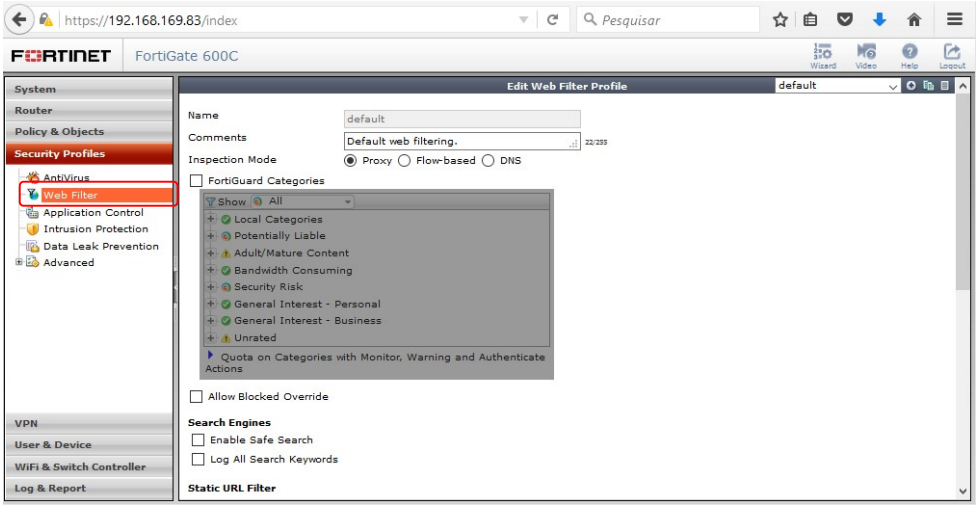
Comentário		
Assinatura do Cliente	**Assinatura NCT**	

PREVENÇÃO DE AMEAÇAS

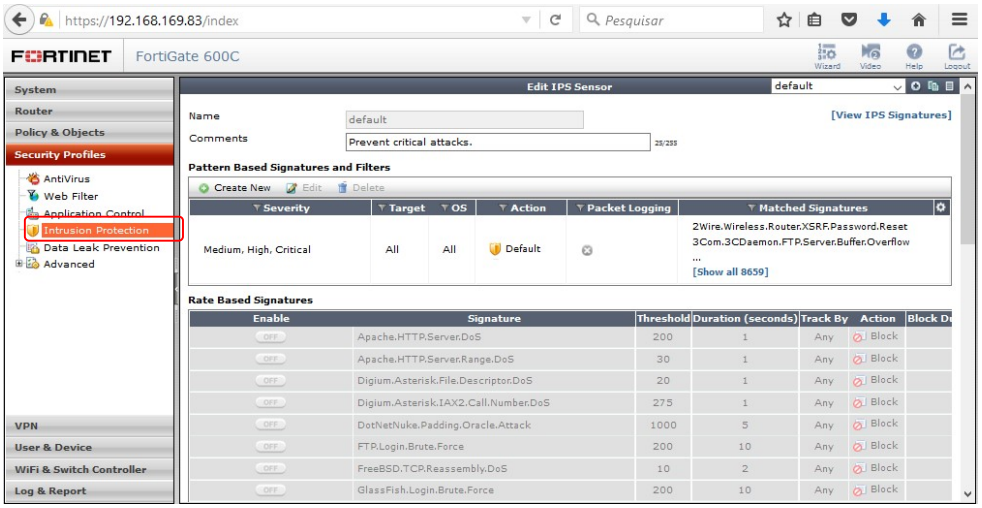
Item de Teste - 1.6.4.1	Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulos de IPS, antivírus e anti-spyware integrados no próprio appliance de firewall;
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado
Configuração do Teste	Demonstrar total disponibilidade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



Módulo de AV



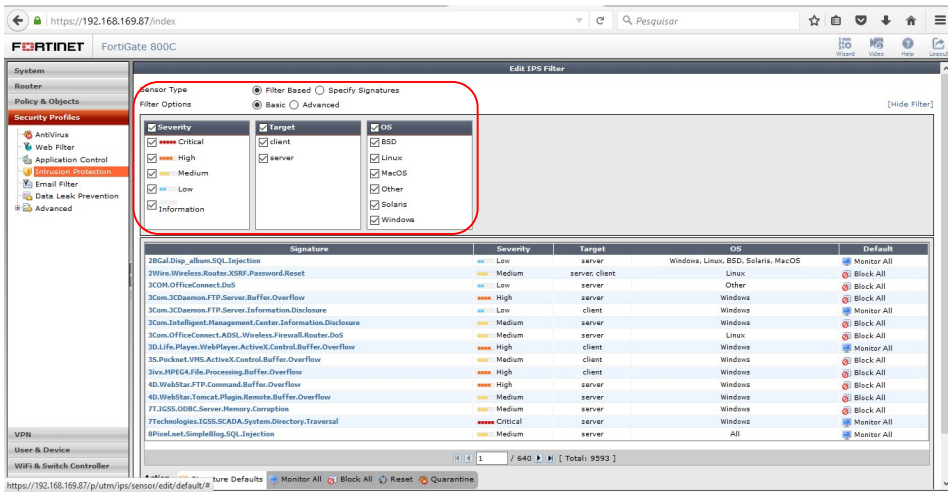
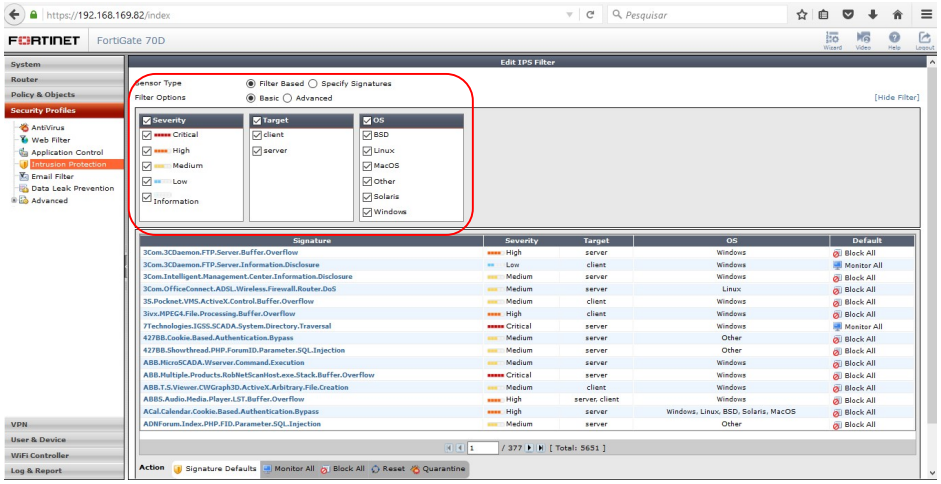
Módulo de web filter

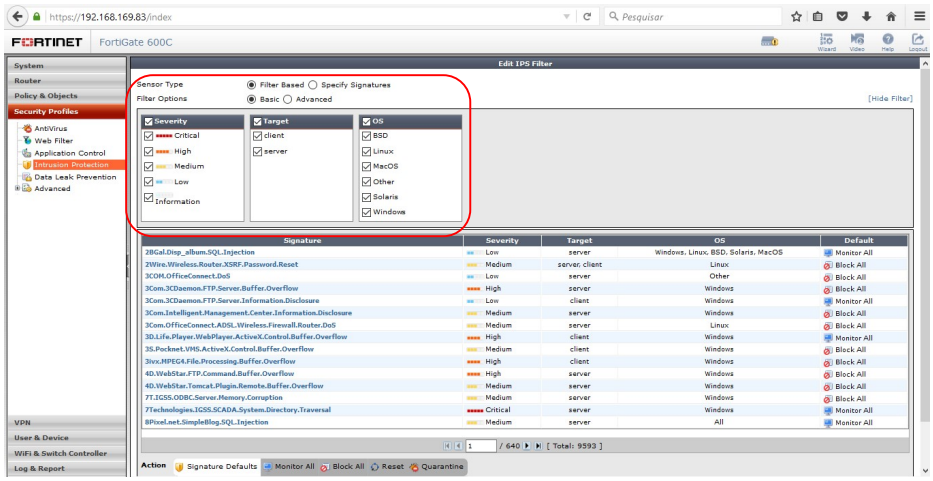


O módulo de anti-spyware esta integrado ao módulo de IPS.

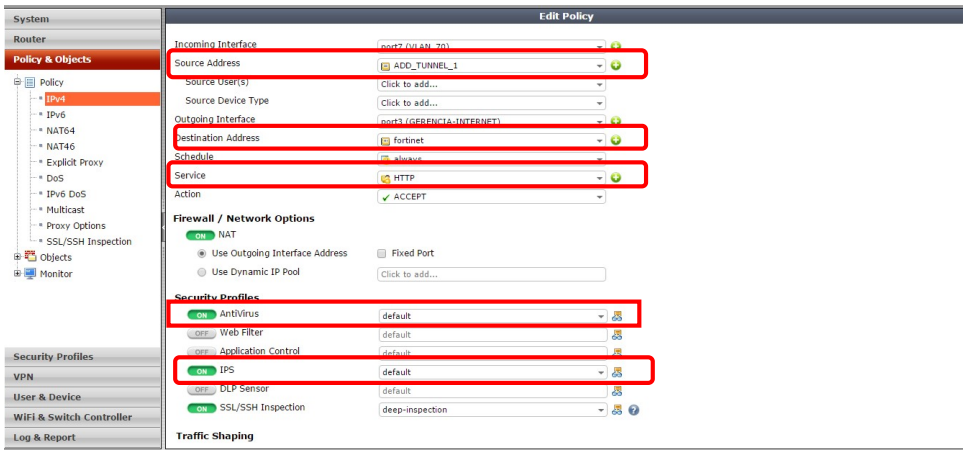
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

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

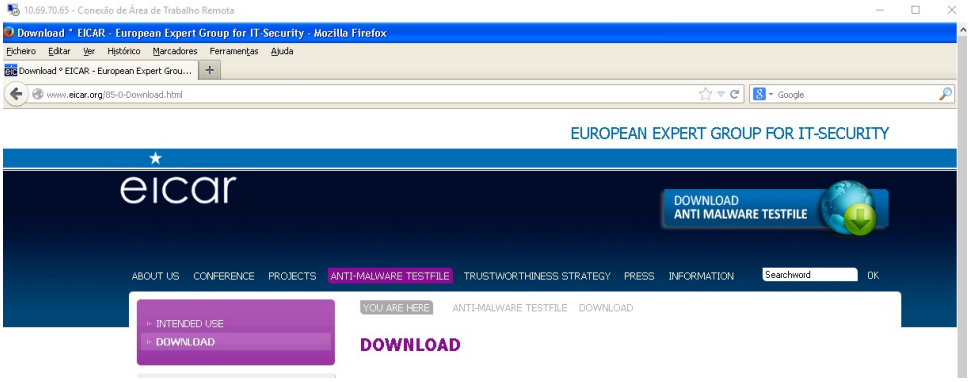
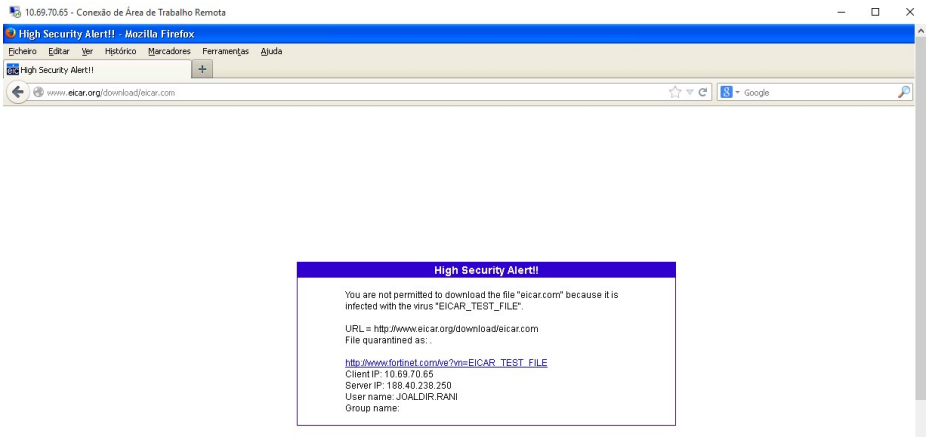
1.6.4.5	deve entregar a performance mínima estabelecida no edital entre ter uma única assinatura de IPS ou ter todas as assinaturas de IPS, antivírus e anti spyware habilitadas simultaneamente;
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado
Configuração do Teste	Todos os testes de 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	 

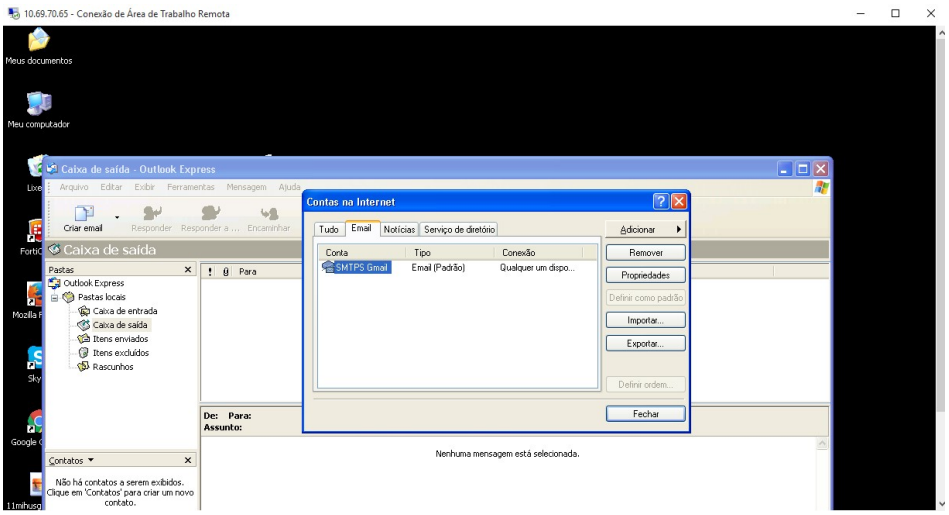


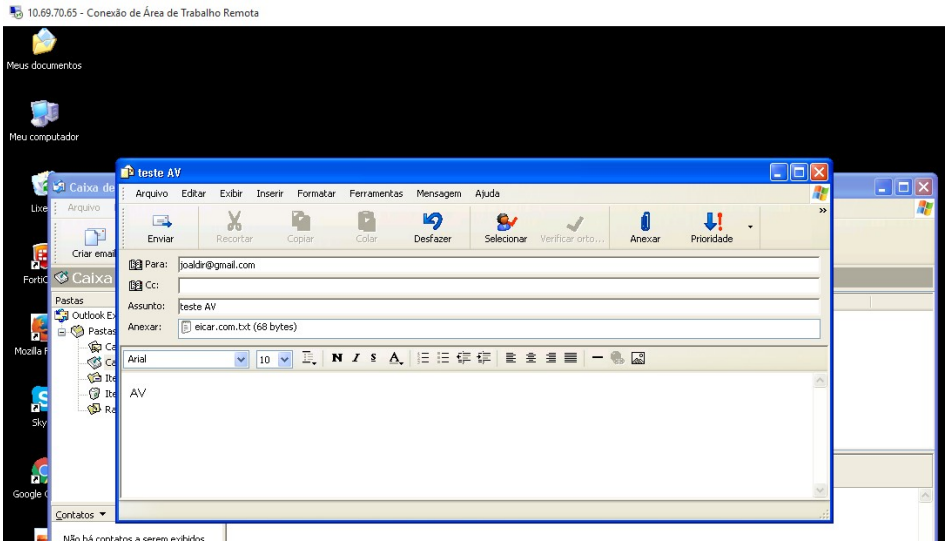
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

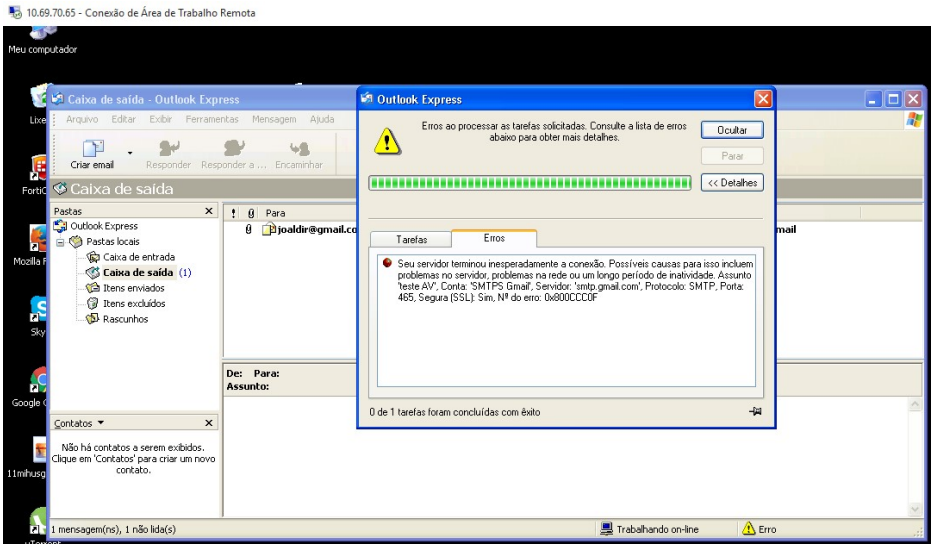
Item de Teste - 1.6.4.8	Deve suportar granularidade nas políticas de IPS, antivírus e anti spyware, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado
Configuração do Teste	Configurar uma política especificando as combinações solicitadas habilitando os profiles 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

		vem com esta habilidade.	
Assinatura do Cliente		**Assinatura NCT**	

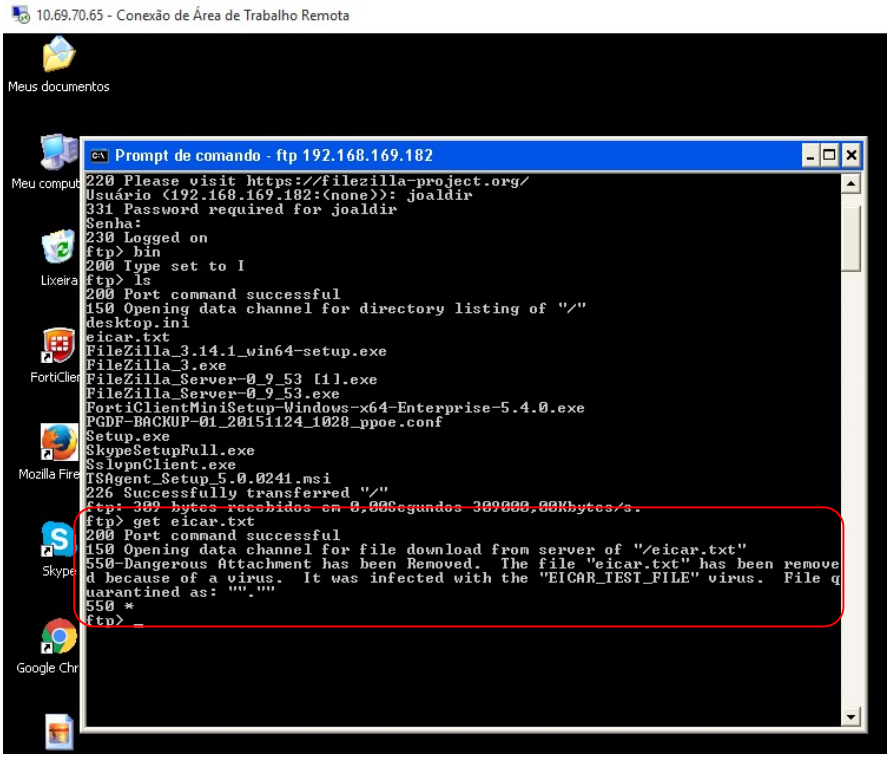
Item de Teste - 1.6.4.18	Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP;
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado
Configuração do Teste	Configurar profiles de Anti-virus selecionado os protocolos mencionado
Procedimento do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


10.69.70.65 - Conexão de Área de Trabalho Remota
Meus documentos
Meu computador
Caixa de saída - Outlook Express
Arquivo Editar Exibir Ferramentas Mensagem Ajuda
Criar email
Responder
Responder a ...
Encaminhar
Caixa de saída
Pastas
Outlook Express
Pastas locais
Caixa de entrada
Caixa de saída
Itens enviados
Itens excluídos
Rascunhos
Para
De: Para:
Assunto:
Contatos
Não há contatos a serem exibidos. Clique em 'Contatos' para criar um novo contato.
Nenhuma mensagem está selecionada.
Contas na Internet
Tudo
Email
Notícias
Serviço de diretório
Conta
Tipo
Conexão
SMTPS Gmail
Email (Padrão)
Qualquer um dispo...
Adicionar
Remover
Propriedades
Definir como padrão
Importar...
Exportar...
Definir ordem...
Fechar

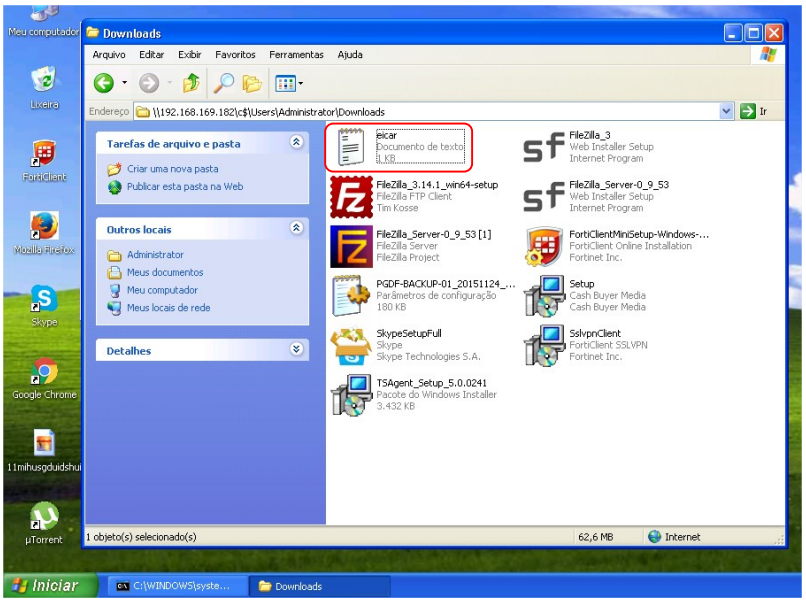

10.69.70.65 - Conexão de Área de Trabalho Remota
Meus documentos
Meu computador
teste AV
Arquivo Editar Exibir Inserir Formatar Ferramentas Mensagem Ajuda
Enviar
Recortar
Copiar
Colar
Desfazer
Selecionar
Verificar orto...
Anexar
Prioridade
Para: joaldir@gmail.com
Cc:
Assunto: teste AV
Anexar: eicar.com.txt (68 bytes)
Arial
10
AV
Contatos

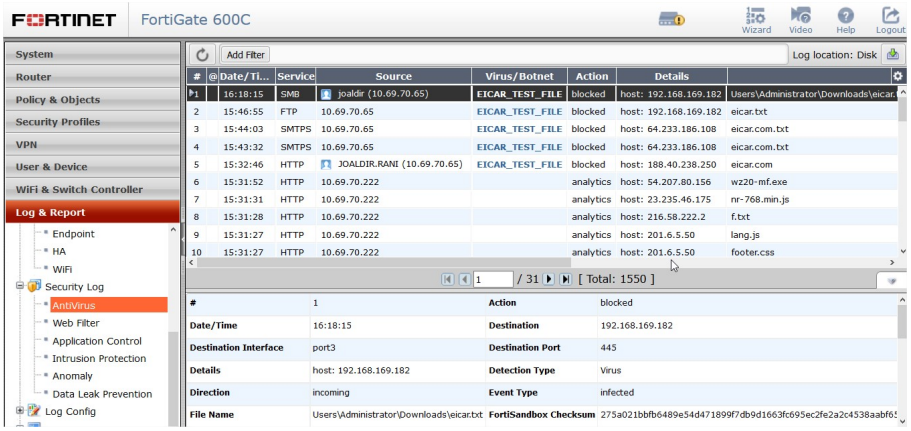

10.69.70.65 - Conexão de Área de Trabalho Remota
Meu computador
Caixa de saída - Outlook Express
Arquivo Editar Exibir Ferramentas Mensagem Ajuda
Criar email
Responder
Responder a ...
Encaminhar
Caixa de saída
Pastas
Outlook Express
Pastas locais
Caixa de entrada
Caixa de saída (1)
Itens enviados
Itens excluídos
Rascunhos
Para
joaldir@gmail.co
De: Para:
Assunto:
Contatos
Não há contatos a serem exibidos. Clique em 'Contatos' para criar um novo contato.
Outlook Express
Erros ao processar as tarefas solicitadas. Consulte a lista de erros abaixo para obter mais detalhes.
Ocultar
Parar
<< Detalhes
Tarefas
Erros
Seu servidor terminou inesperadamente a conexão. Possíveis causas para isso incluem problemas no servidor, problemas na rede ou um longo período de inatividade. Assunto 'teste AV', Conta: 'SMTPS Gmail', Servidor: 'smtp.gmail.com', Protocolo: SMTP, Porta: 465, Segura (SSL): Sim, Nº do erro: 0x800CCC0F
0 de 1 tarefas foram concluídas com êxito
1 mensagem(ns), 1 não lida(s)
Trabalhando on-line
Erro

-FTP

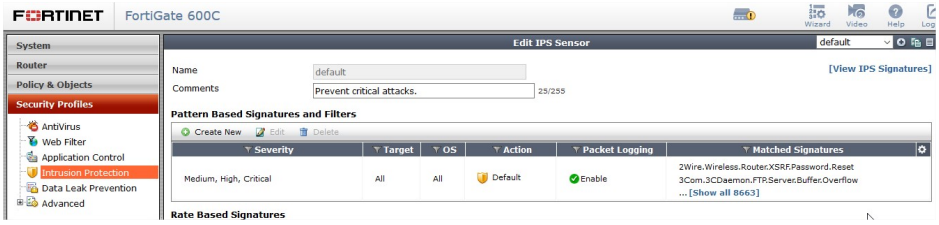
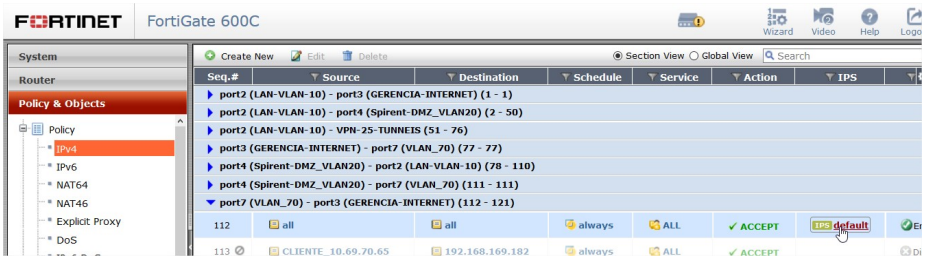

10.69.70.65 - Conexão de Área de Trabalho Remota
Meus documentos
Meu computa
Lixeira
FortiClien
Mozilla Fire
Skype
Google Chr
Prompt de comando - ftp 192.168.169.182
220 Please visit https://filezilla-project.org/
Usuário (192.168.169.182:(none)): joaldir
331 Password required for joaldir
Senha:
230 Logged on
ftp> bin
200 Type set to I
ftp> ls
200 Port command successful
150 Opening data channel for directory listing of "/"
desktop.ini
eicar.txt
FileZilla_3.14.1_win64-setup.exe
FileZilla_3.exe
FileZilla_Server-0_9_53 [1].exe
FileZilla_Server-0_9_53.exe
FortiClientMiniSetup-Windows-x64-Enterprise-5.4.0.exe
PGDF-BACKUP-01_20151124_1028_ppoe.conf
Setup.exe
SkypeSetupFull.exe
SslvpnClient.exe
TSAgent_Setup_5.0.0241.msi
226 Successfully transferred "/"
ftp> get eicar.txt
200 Port command successful
150 Opening data channel for file download from server of "/eicar.txt"
550-Dangerous Attachment has been Removed. The file "eicar.txt" has been remove
d because of a virus. It was infected with the "EICAR_TEST_FILE" virus. File q
uarantined as: "".""
550 *
ftp> _

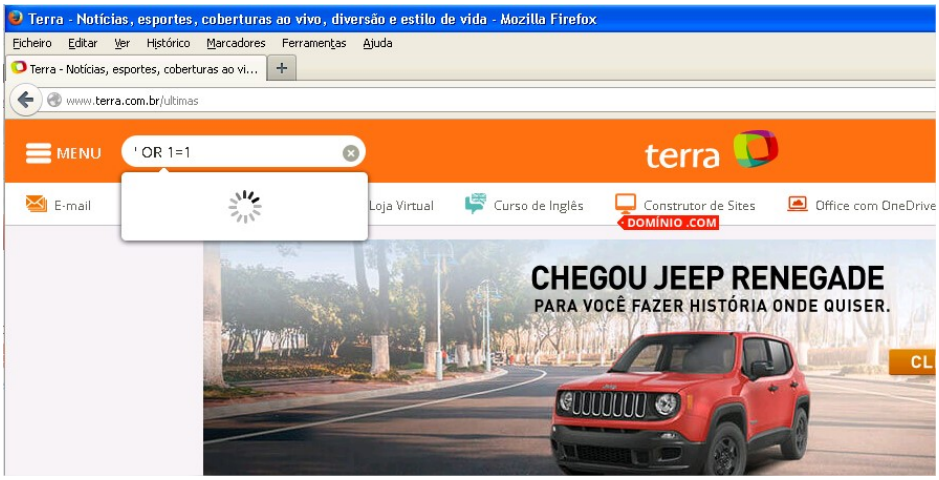
-SMB


Downloads
Arquivo Editar Exibir Favoritos Ferramentas Ajuda
Endereço \\192.168.169.182\c$\Users\Administrator\Downloads
Tarefas de arquivo e pasta
Criar uma nova pasta
Publicar esta pasta na Web
Outros locais
Administrator
Meus documentos
Meu computador
Meus locais de rede
Detalhes
eicar
Documento de texto
1 KB
FileZilla_3.14.1_win64-setup
FileZilla FTP Client
Tim Kosse
FileZilla_Server-0_9_53 [1]
FileZilla Server
FileZilla Project
PGDF-BACKUP-01_20151124_...
Parâmetros de configuração
180 KB
SkypeSetupFull
Skype
Skype Technologies S.A.
TSAgent_Setup_5.0.0241
Pacote do Windows Installer
3.432 KB
FileZilla_3
Web Installer Setup
Internet Program
FileZilla_Server-0_9_53
Web Installer Setup
Internet Program
FortiClientMiniSetup-Windows-...
FortiClient Online Installation
Fortinet Inc.
Setup
Cash Buyer Media
Cash Buyer Media
SslvpnClient
FortiClient SSLVPN
Fortinet Inc.
1 objeto(s) selecionado(s)
62,6 MB
Internet
Iniciar
C:\WINDOWS\syste...
Downloads

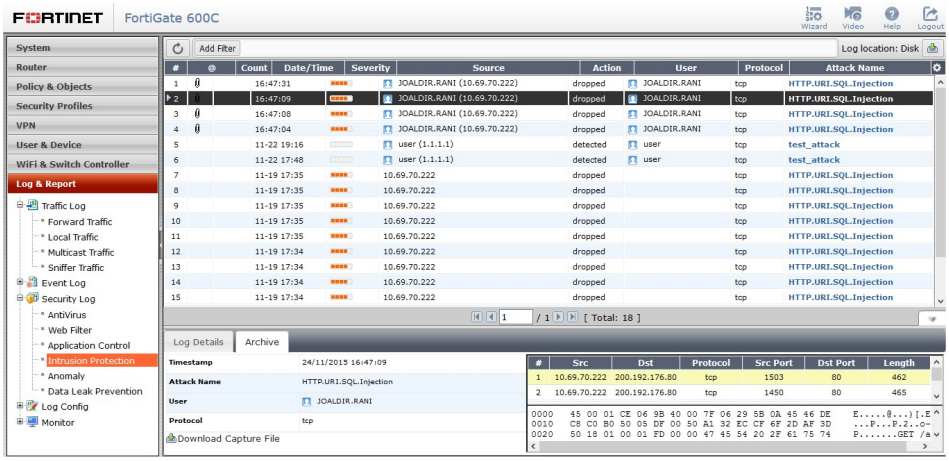


Comentário			
Assinatura do Cliente		**Assinatura NCT**	

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 sintax ' OR 1=1. Foi demonstrado log com as informações e a captura do pacote do ataque.
Evidências	 Sensor IPS  Regra de Firewall



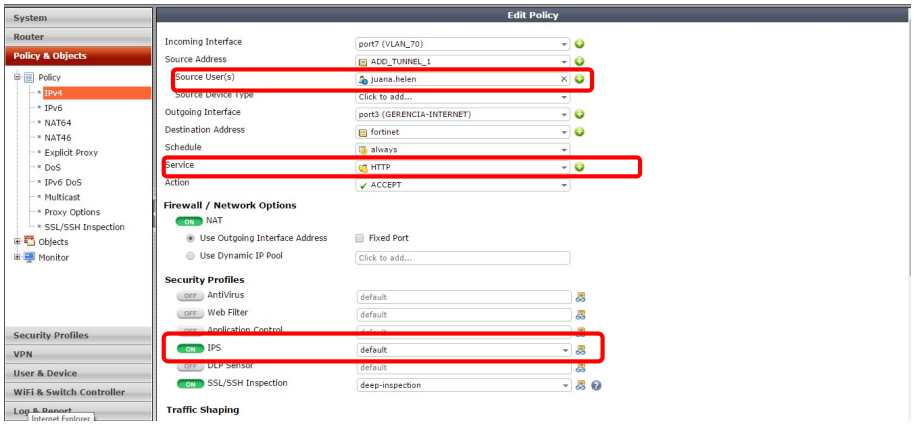
Browser do atacante



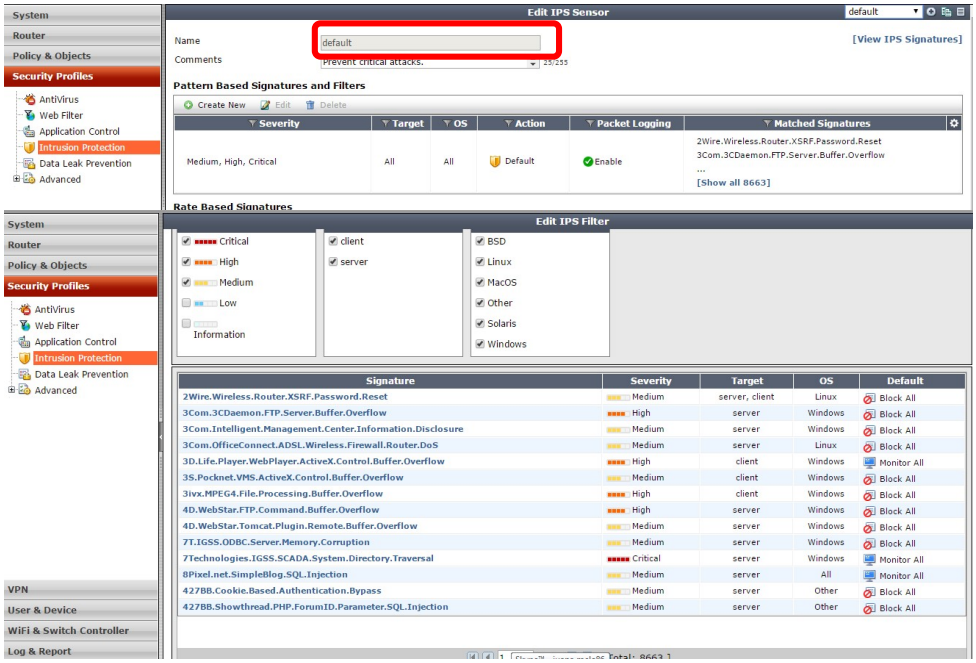
Informações de captura

Comentário	
Assinatura do Cliente	**Assinatura NCT**

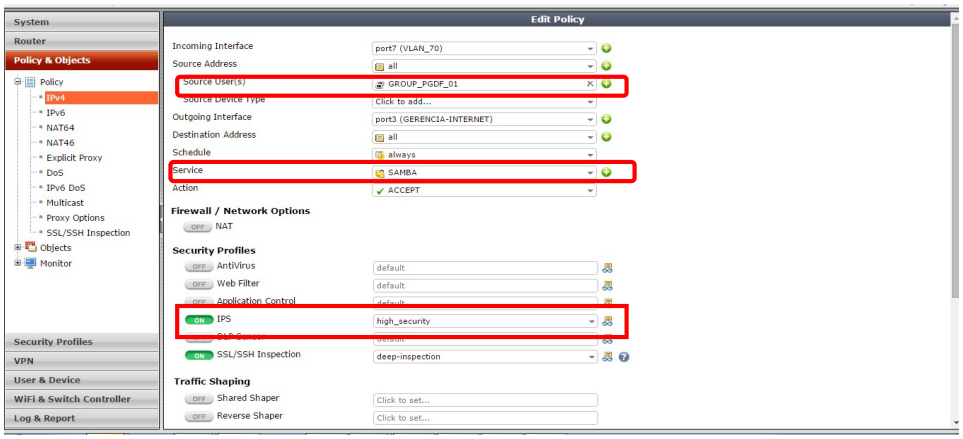
Item de Teste - 1.6.4.31	Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques, baseando-se em políticas de firewall que considere usuários, grupos de usuários, origem e destino;
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado
Configuração do Teste	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 especifico com um perfil de IPS default:



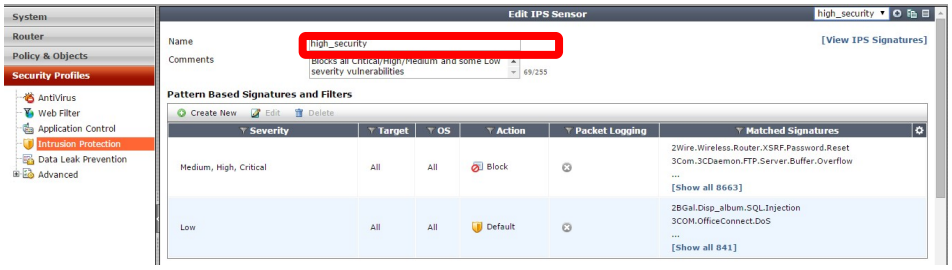
Configuração de perfil default que foi habilitado na regra acima :



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



Configuração de perfil default que foi habilitado na regra acima :

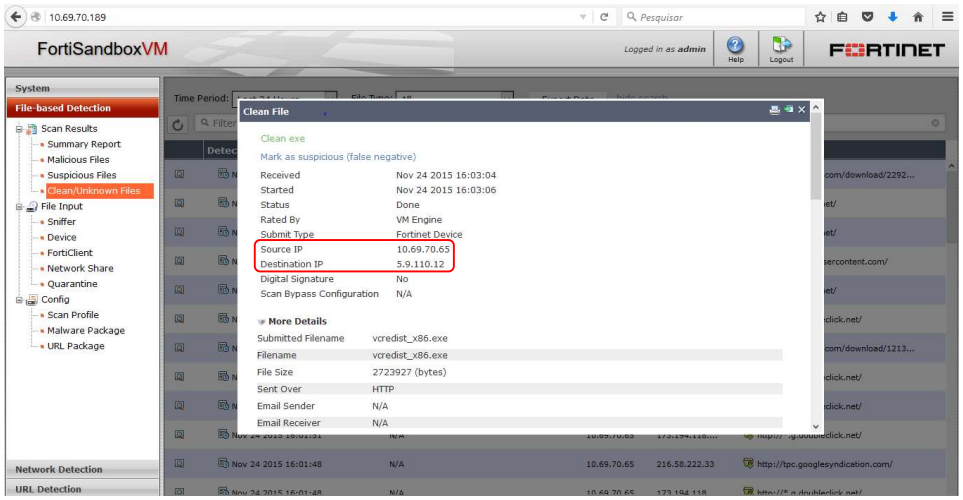


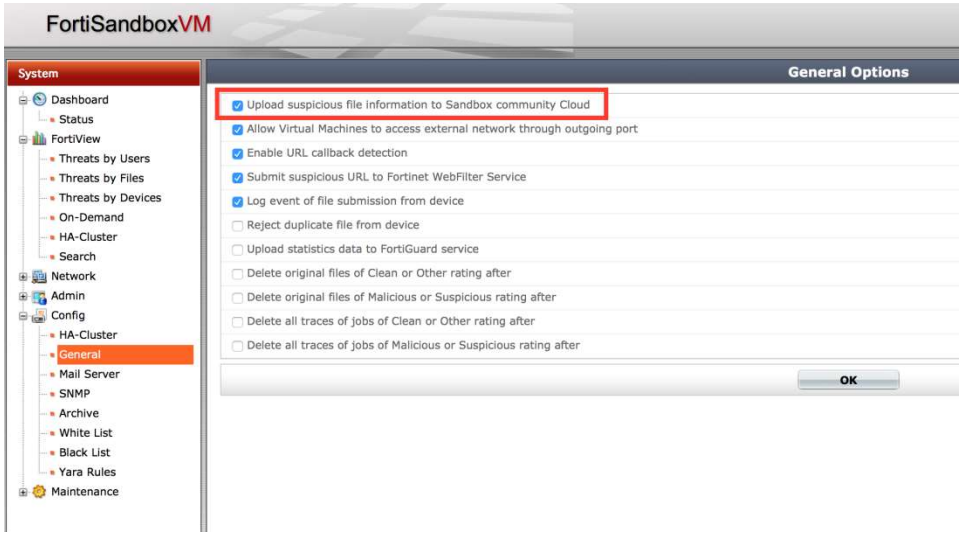
Evidências	
Comentário	
Assinatura do Cliente	**Assinatura NCT**

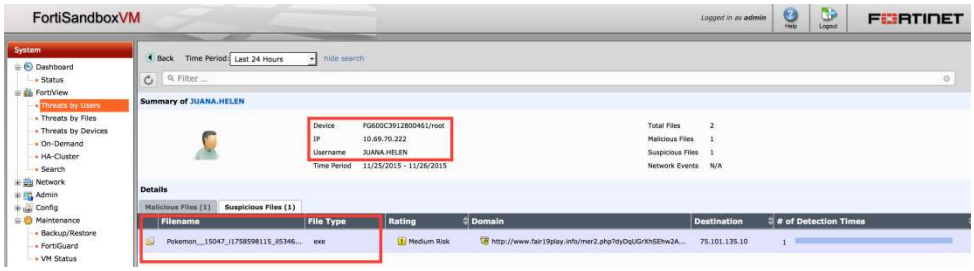
Analise de malwares modernos - Sandbox

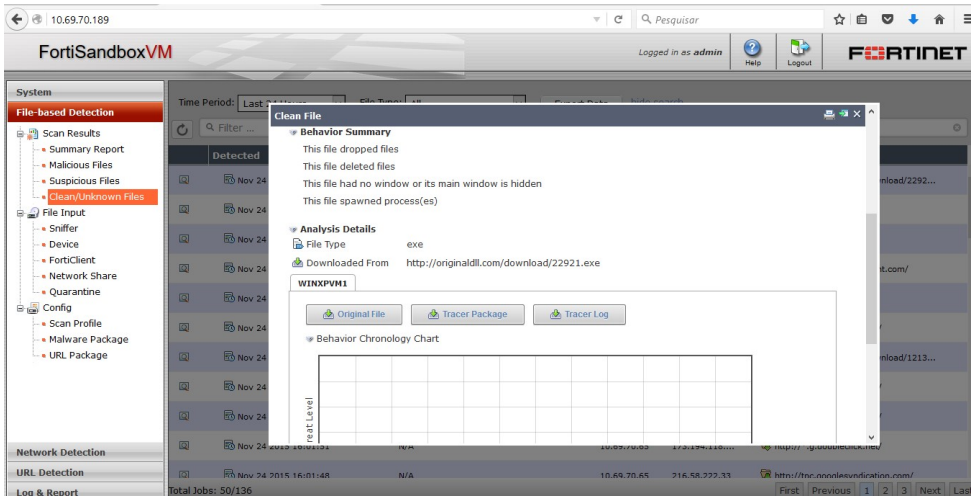
Item de Teste - 1.6.5.8	O sistema de análise "in cloud" ou local deve prover informações sobre as ações do malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar ou propagar a infecção, detectar aplicações não confiáveis utilizadas pelo malware, gerar assinaturas 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	

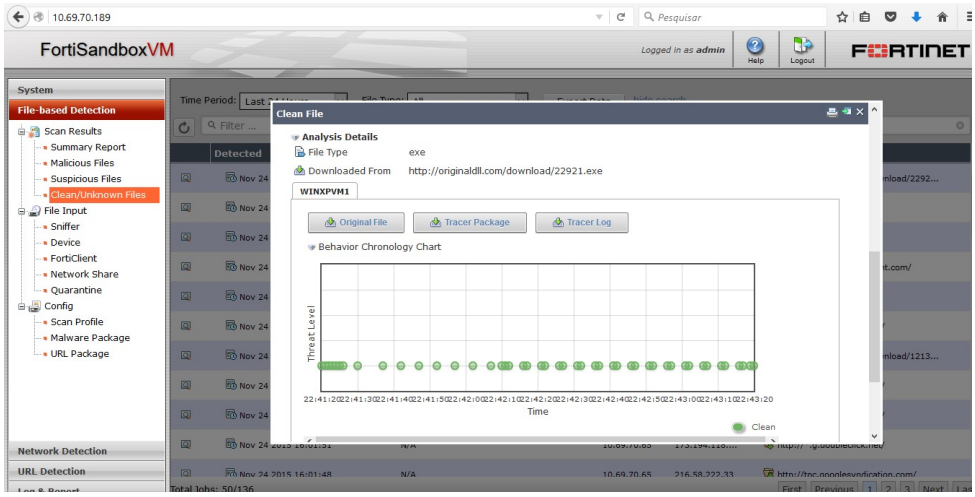
do Teste

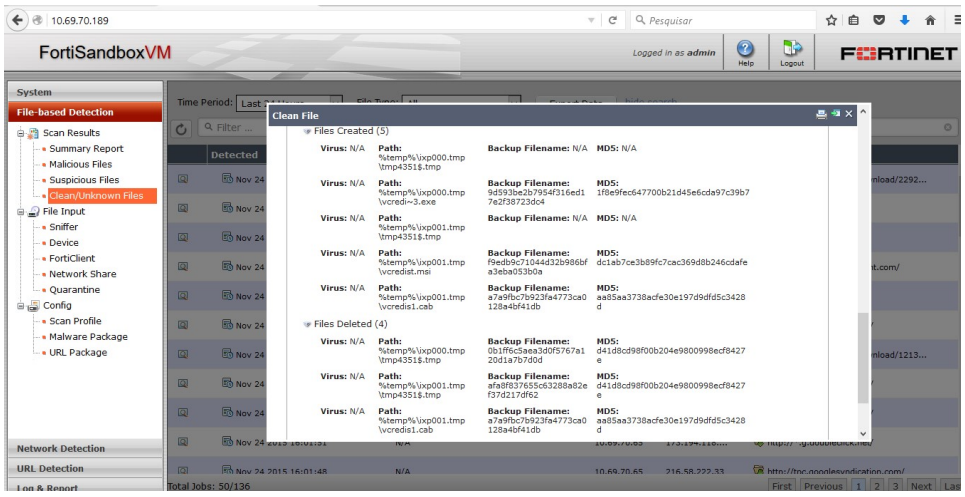

FortiSandboxVM
Clean File
Clean exe
Mark as suspicious (false negative)
Received Nov 24 2015 16:03:04
Started Nov 24 2015 16:03:06
Status Done
Rated By VM Engine
Submit Type Fortinet Device
Source IP 10.69.70.65
Destination IP 5.9.110.12
Digital Signature No
Scan Bypass Configuration N/A
More Details
Submitted Filename vcredist_x86.exe
Filename vcredist_x86.exe
File Size 2723927 (bytes)
Sent Over HTTP
Email Sender N/A
Email Receiver N/A

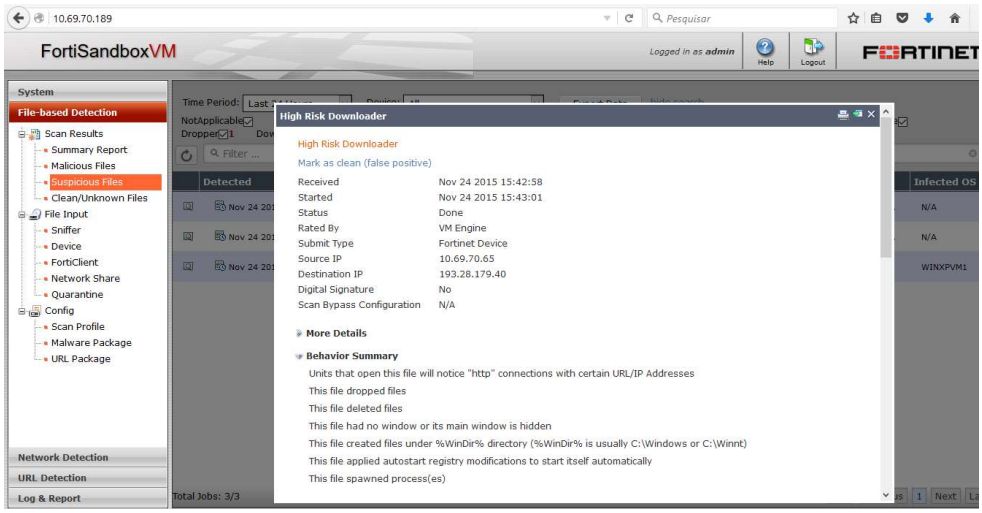

FortiSandboxVM
System
General Options
Upload suspicious file information to Sandbox community Cloud
Allow Virtual Machines to access external network through outgoing port
Enable URL callback detection
Submit suspicious URL to Fortinet WebFilter Service
Log event of file submission from device
Reject 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

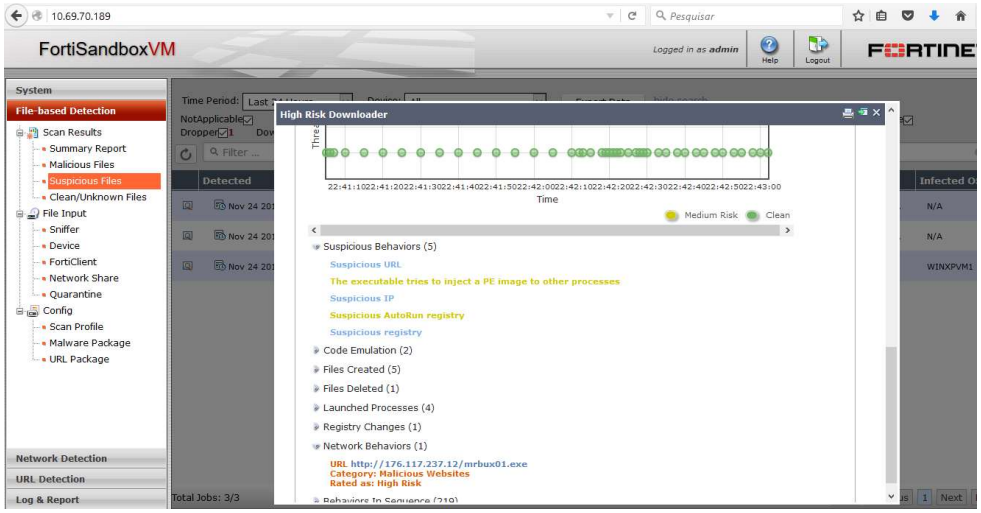

FortiSandboxVM
Summary of JUANA.HELEN
Details

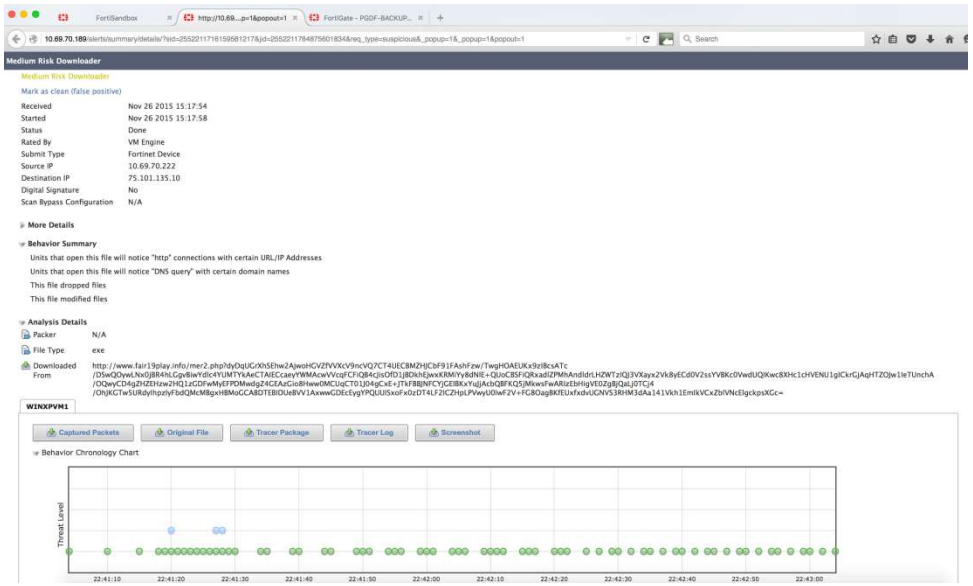

10.69.70.189
FortiSandboxVM
Logged in as admin
Help
Logout
FORTINET
System
File-based Detection
Scan Results
Summary Report
Malicious Files
Suspicious Files
Clean/Unknown Files
File Input
Sniffer
Device
FortiClient
Network Share
Quarantine
Config
Scan Profile
Malware Package
URL Package
Network Detection
URL Detection
Log & Report
Time Period:
Detected
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
WINXPVM1
Original File
Tracer Package
Tracer Log
Behavior Chronology Chart
Total Jobs: 50/136


10.69.70.189
FortiSandboxVM
Logged in as admin
Help
Logout
FORTINET
System
File-based Detection
Scan Results
Summary Report
Malicious Files
Suspicious Files
Clean/Unknown Files
File Input
Sniffer
Device
FortiClient
Network Share
Quarantine
Config
Scan Profile
Malware Package
URL Package
Network Detection
URL Detection
Clean File
Analysis Details
File Type exe
Downloaded From http://originaldll.com/download/22921.exe
WINXPVM1
Original File
Tracer Package
Tracer Log
Behavior Chronology Chart
Threat Level
Time
Clean


10.69.70.189
FortiSandboxVM
Logged in as admin
Help
Logout
FORTINET
System
File-based Detection
Scan Results
Summary Report
Malicious Files
Suspicious Files
Clean/Unknown Files
File Input
Sniffer
Device
FortiClient
Network Share
Quarantine
Config
Scan Profile
Malware Package
URL Package
Network Detection
URL Detection
Clean File
Files Created (5)
Virus: N/A
Path:
Backup Filename:
MD5:
Files Deleted (4)

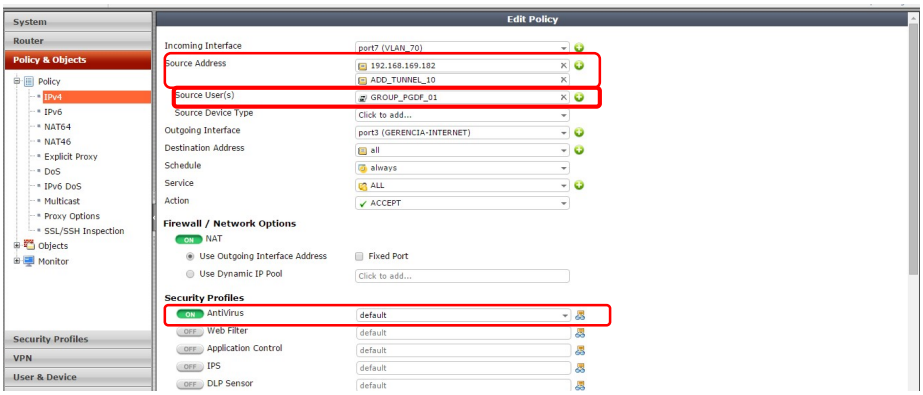

10.69.70.189
FortiSandboxVM
Logged in as admin
Help
Logout
FORTINET
System
File-based Detection
Scan Results
Summary Report
Malicious Files
Suspicious Files
Clean/Unknown Files
File Input
Sniffer
Device
FortiClient
Network Share
Quarantine
Config
Scan Profile
Malware Package
URL Package
Network Detection
URL Detection
Log & Report
High Risk Downloader
High Risk Downloader
Mark as clean (false positive)
Received Nov 24 2015 15:42:58
Started Nov 24 2015 15:43:01
Status Done
Rated By VM Engine
Submit Type Fortinet Device
Source IP 10.69.70.65
Destination IP 193.28.179.40
Digital Signature No
Scan Bypass Configuration N/A
More Details
Behavior Summary
Units that open this file will notice "http" connections with certain URL/IP Addresses
This file dropped files
This file deleted files
This file had no window or its main window is hidden
This file created files under %WinDir% directory (%WinDir% is usually C:\Windows or C:\Winnt)
This file applied autostart registry modifications to start itself automatically
This file spawned process(es)
Total Jobs: 3/3

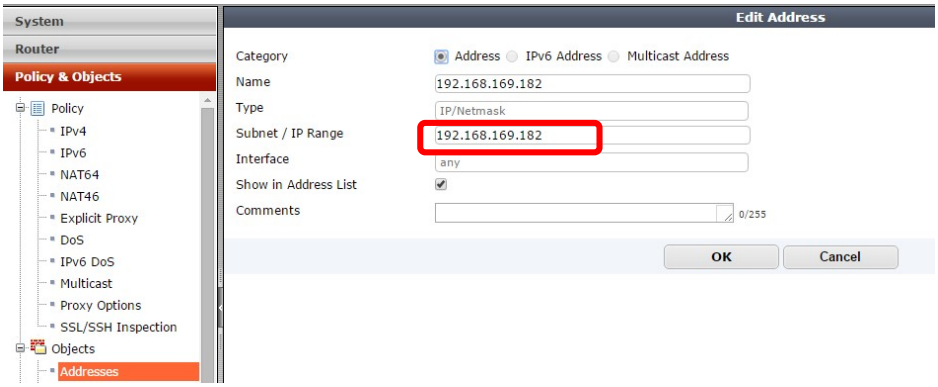

10.69.70.189
FortiSandboxVM
Logged in as admin
Help
Logout
System
File-based Detection
Scan Results
Summary Report
Malicious Files
Suspicious Files
Clean/Unknown Files
File Input
Sniffer
Device
FortiClient
Network Share
Quarantine
Config
Scan Profile
Malware Package
URL Package
Network Detection
URL Detection
Log & Report
High Risk Downloader
Time
Medium Risk
Clean
Suspicious Behaviors (5)
Suspicious URL
The executable tries to inject a PE image to other processes
Suspicious IP
Suspicious AutoRun registry
Suspicious registry
Code Emulation (2)
Files Created (5)
Files Deleted (1)
Launched Processes (4)
Registry Changes (1)
Network Behaviors (1)
URL http://176.117.237.12/mrbux01.exe
Category: Malicious Websites
Rated as: High Risk
Total Jobs: 3/3


Medium Risk Downloader
Mark as clean (false positive)
Received Nov 26 2015 15:17:54
Started Nov 26 2015 15:17:58
Status Done
Rated By VM Engine
Submit Type Fortinet Device
Source IP 10.69.70.222
Destination IP 75.101.135.10
Digital Signature No
Scan Bypass Configuration N/A
More Details
Behavior Summary
Units that open this file will notice "http" connections with certain URL/IP Addresses
Units that open this file will notice "DNS query" with certain domain names
This file dropped files
This file modified files
Analysis Details
Packer N/A
File Type exe
Downloaded From
WINXPVM1
Captured Packets
Original File
Tracer Package
Tracer Log
Screenshot
Behavior Chronology Chart
Threat Level

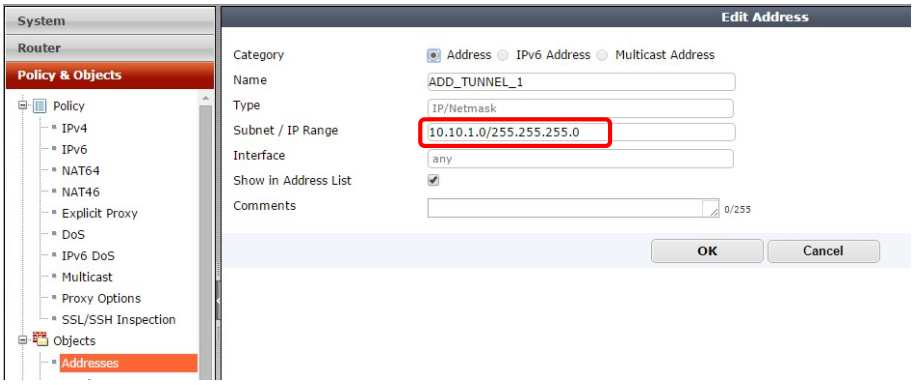
Evidências	

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 antivirus :  Grupo de usuário: Endreços por IP:

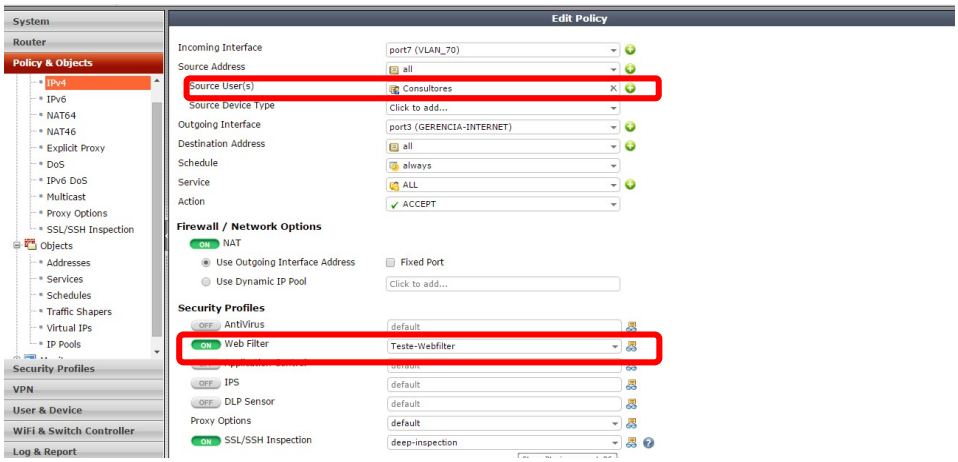


Endereço Rede:



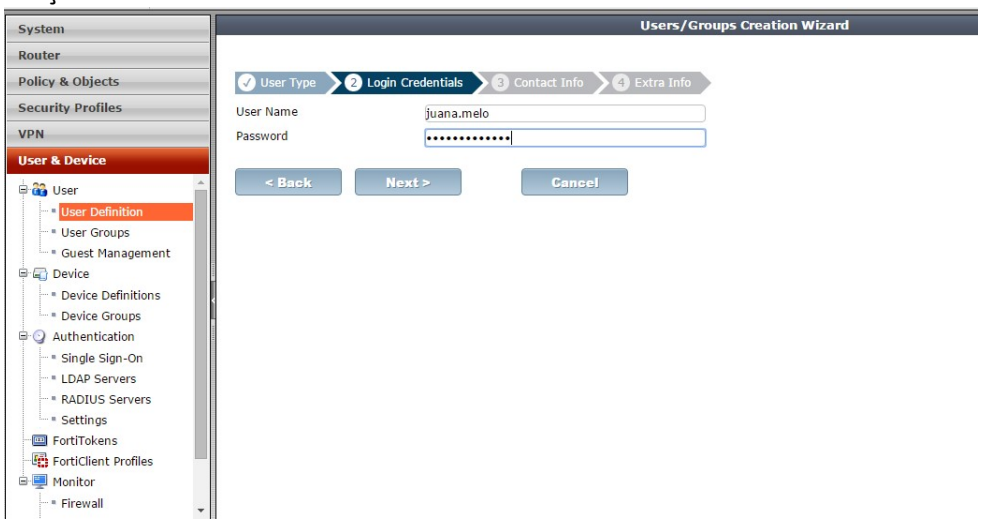
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

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:



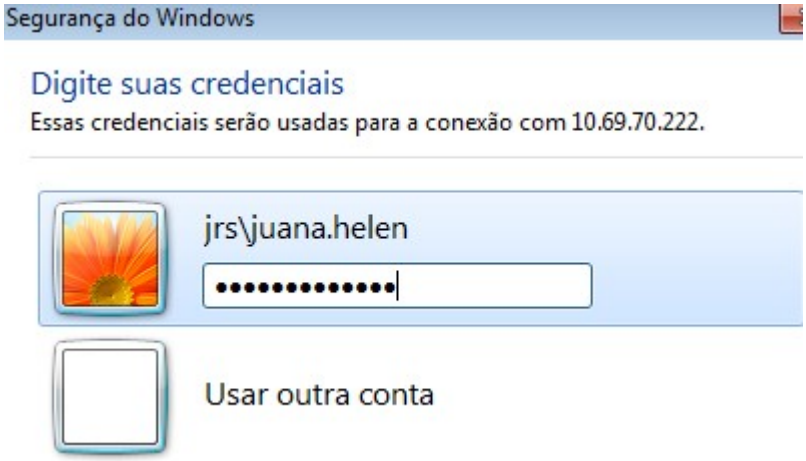
Grupo de acesso do usuário foi feito com a integração com o AD fazendo uma consulta LDAP que também é compatível com e-directory:

Criação de usuário de base local:



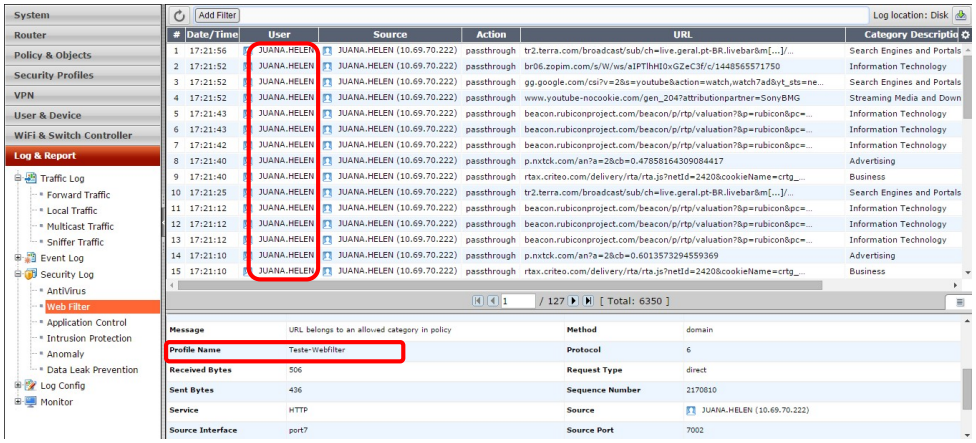
O cliente que acessou no PC RDP 10.69.70.222, autenticou com seu usuário da

rede:



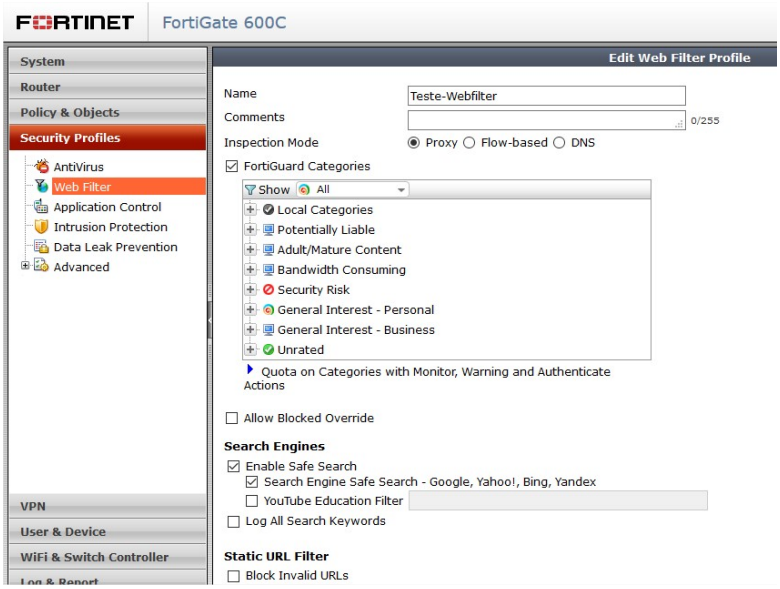
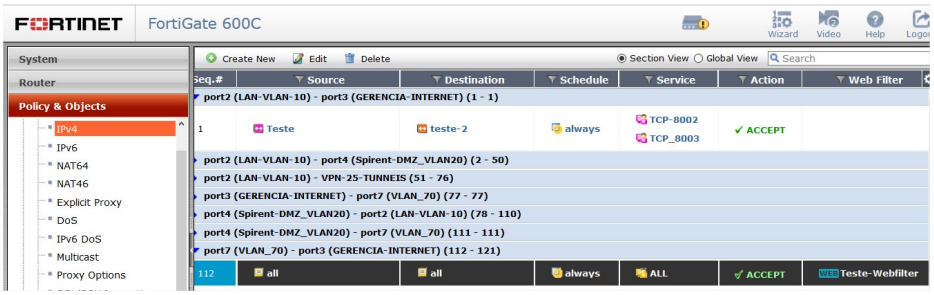
Na tela de monitor do firewall ja foi possível detectar o evento de autenticação do usuário que faz parte do perfil consultores:

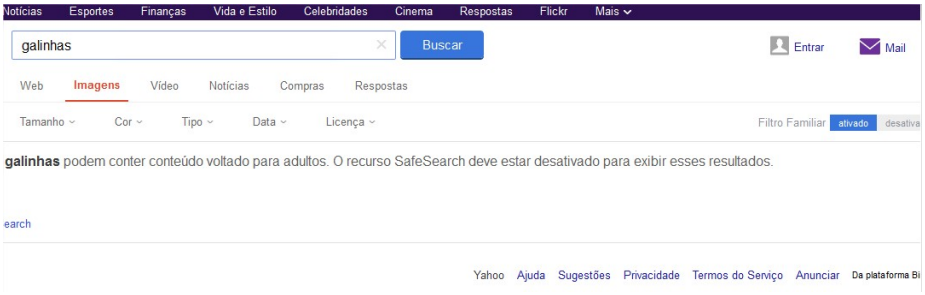
Log de acesso web do usuário autenticado o match no perfil Teste-Webfilter :

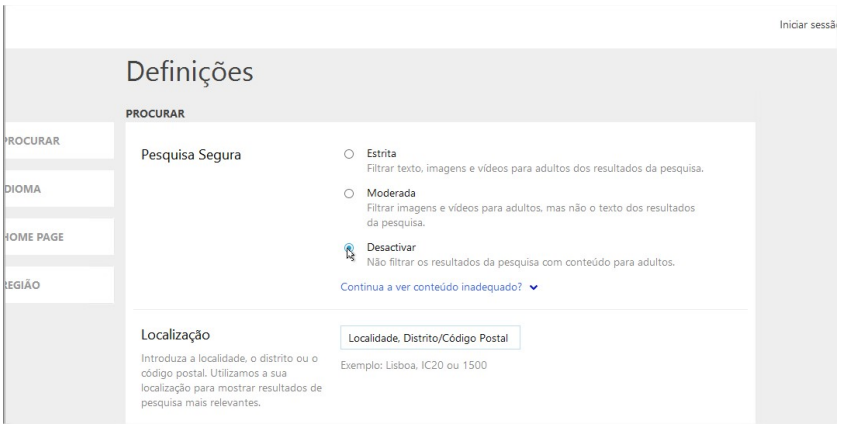


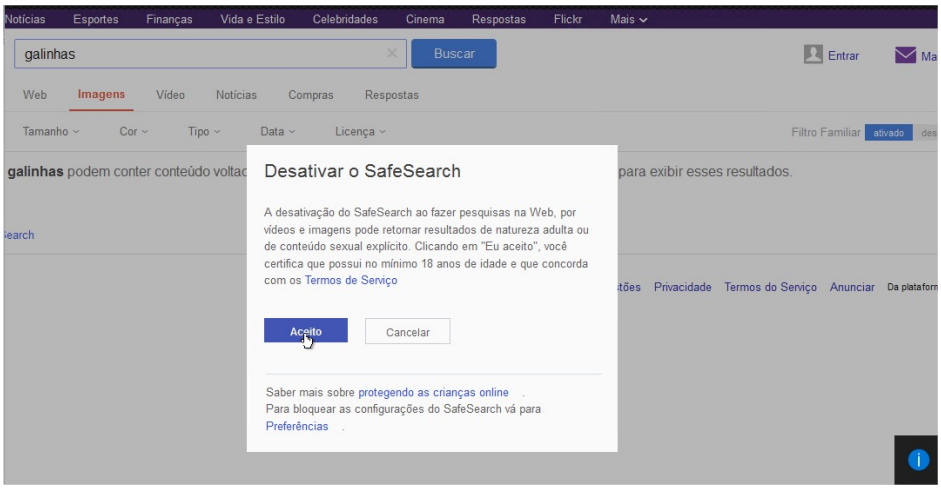
Comentário	
Assinatura do Cliente	**Assinatura NCT**

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;

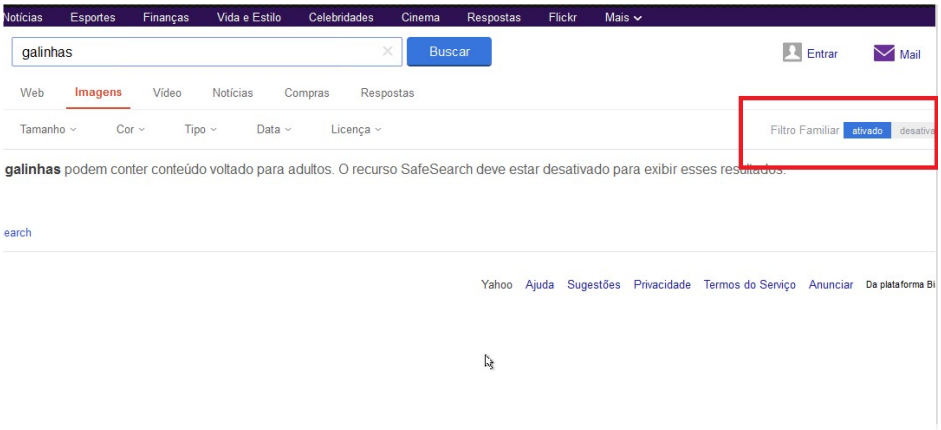
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado
Configuração do Teste	Configurado um perfil de filtro de conteúdo Teste-WebFilter com a funcionalidade Enable Safe Search e Search Engine Search. Configurado uma regra e atribuído o perfil web. Criado um perfil de filtro de aplicação para 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 montra 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



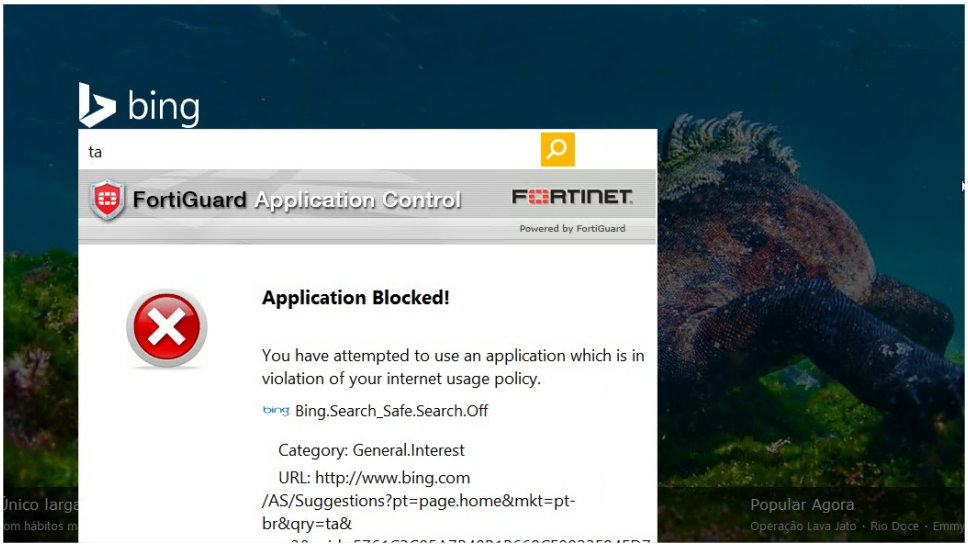




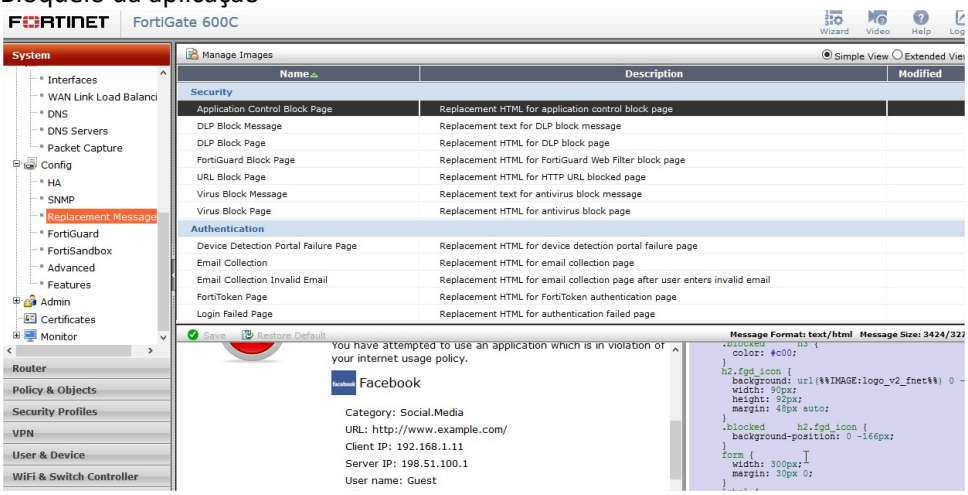
Tentativa de desativar o safe search



Falha na tentativa de desabilitar o safe search



Bloqueio da aplicação

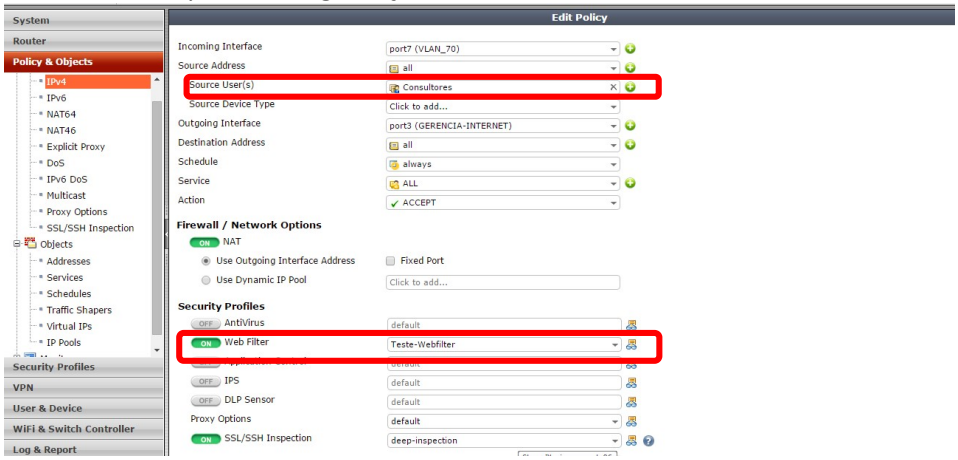


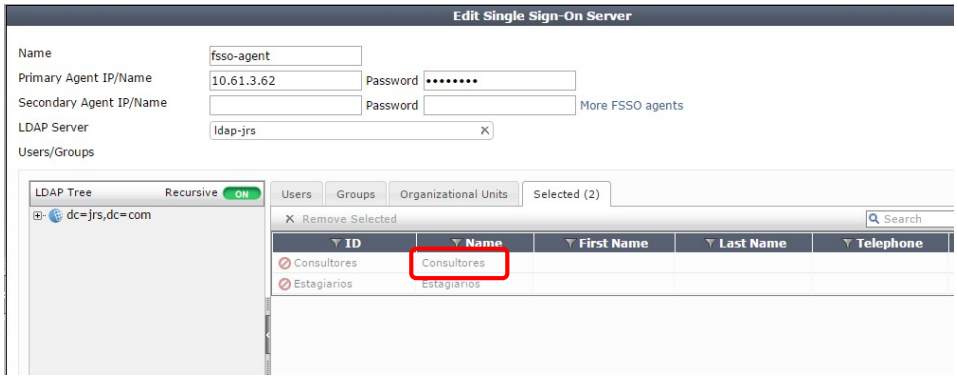
Customização de pagina de bloqueio.

Comentário	

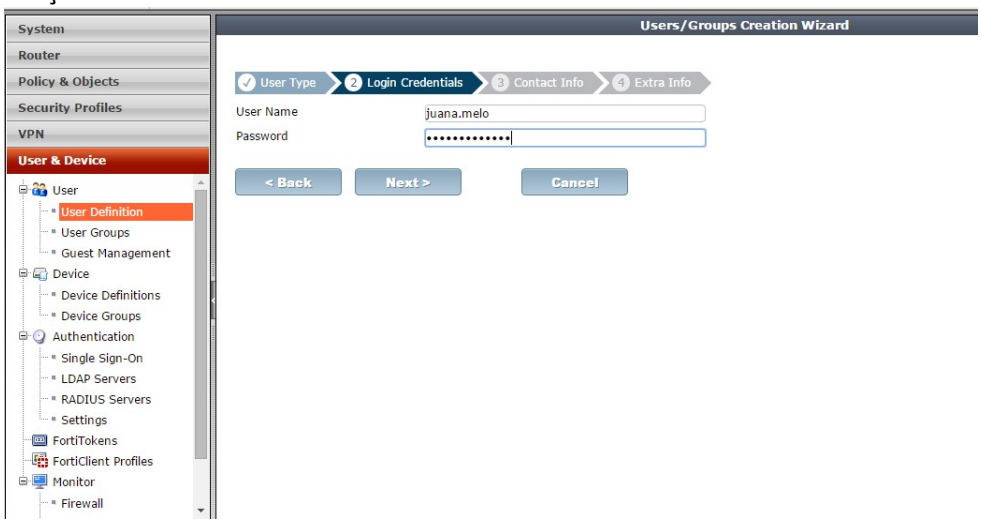
Assinatura do Cliente		**Assinatura NCT**	

Identificação de usuários

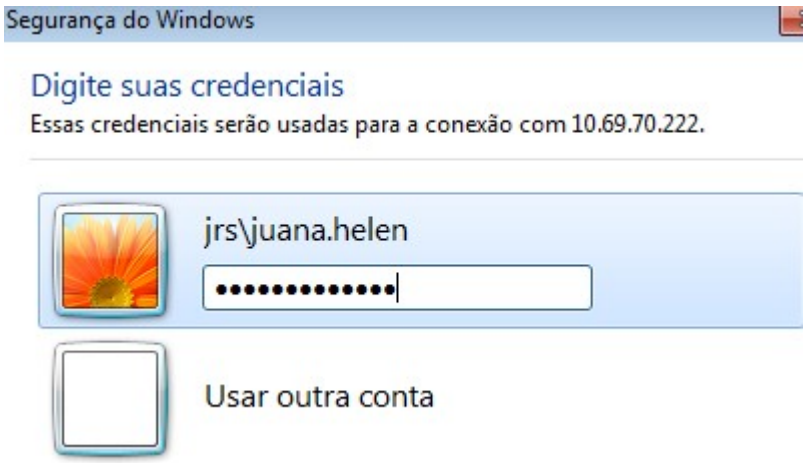
Item de Teste - 1.6.7.1	Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-Directory e base de dados local;
Objetivo do Teste	Demonstrar 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 compativel com e-directory:



Criação de usuário de base local:



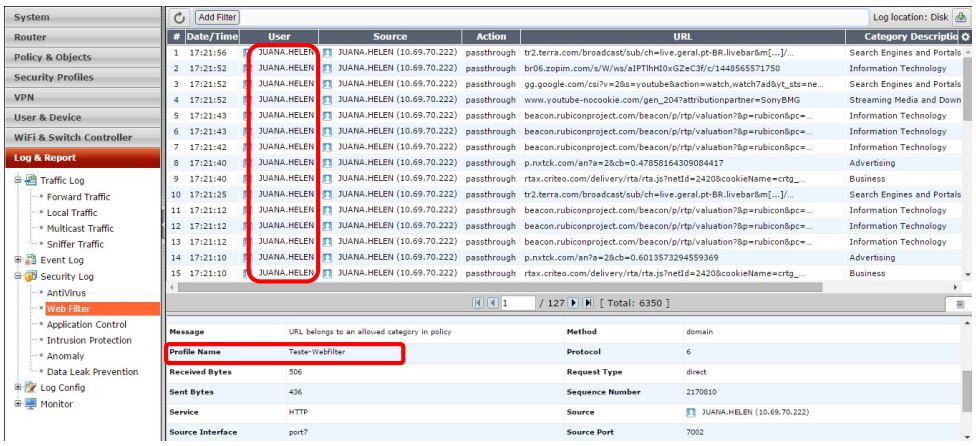
O cliente que acessou no PC RDP 10.69.70.222, autenticou com seu usuário da rede:



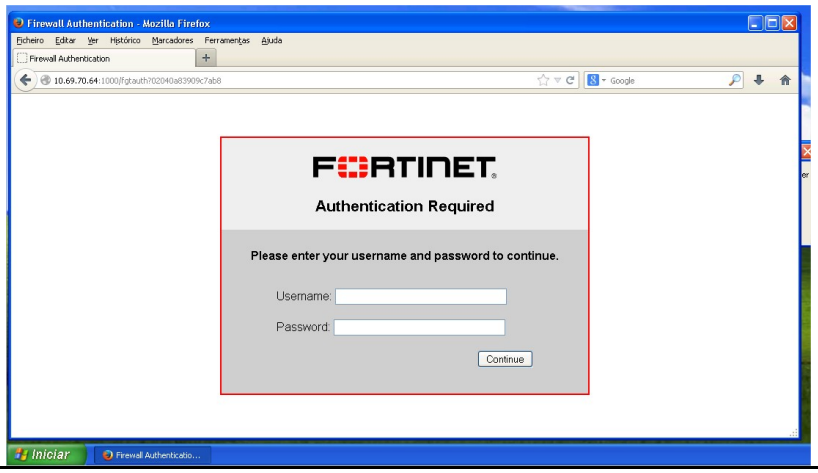
Na tela de monitor do firewall ja foi possível detectar o evento de autenticação

do usuário que faz parte do perfil consultores:

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

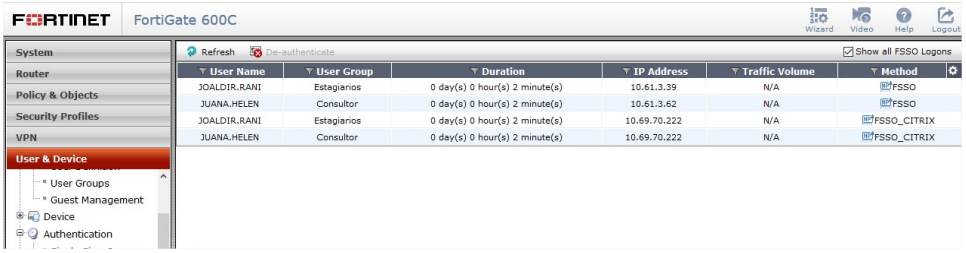


Comentário		
Assinatura do Cliente	**Assinatura NCT**	

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	

Comentário			
Assinatura do Cliente		**Assinatura NCT**	

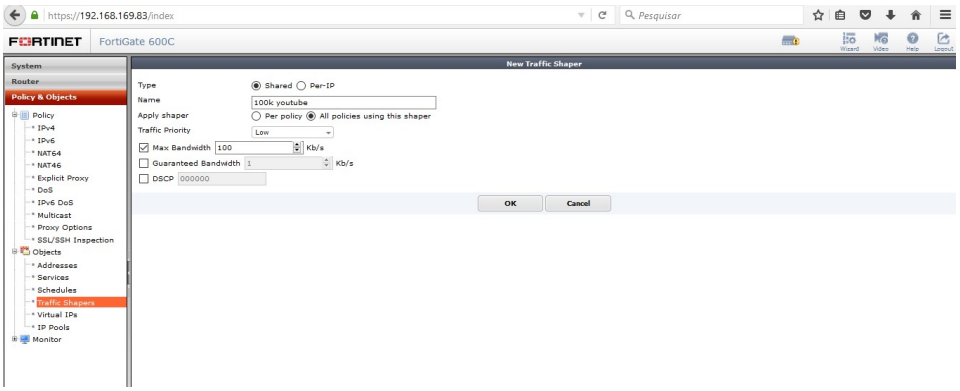
Item de Teste - 1.6.7.5	Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
Objetivo do Teste	Demonstrar 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	

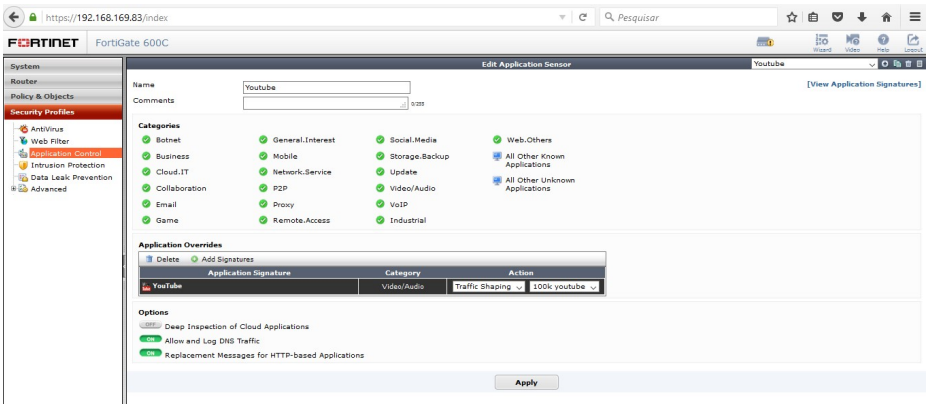


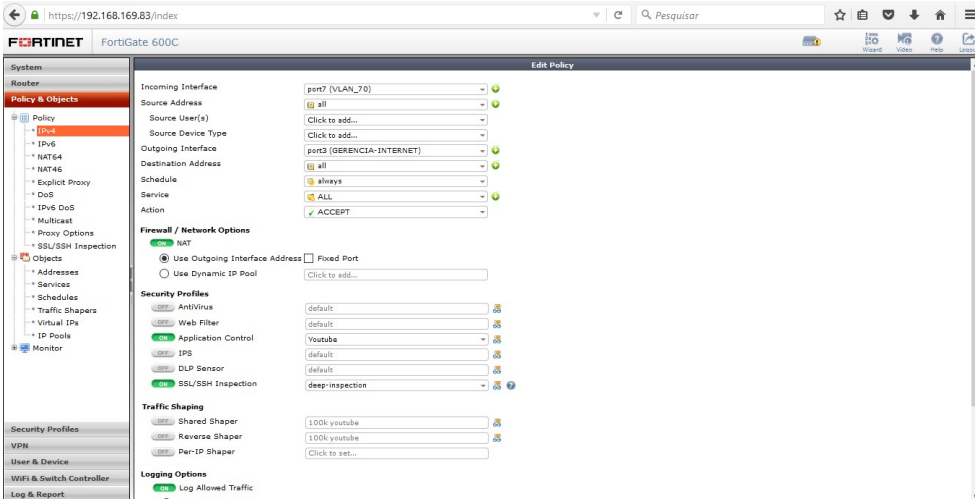
Tela de usuários com o mesmo ip.

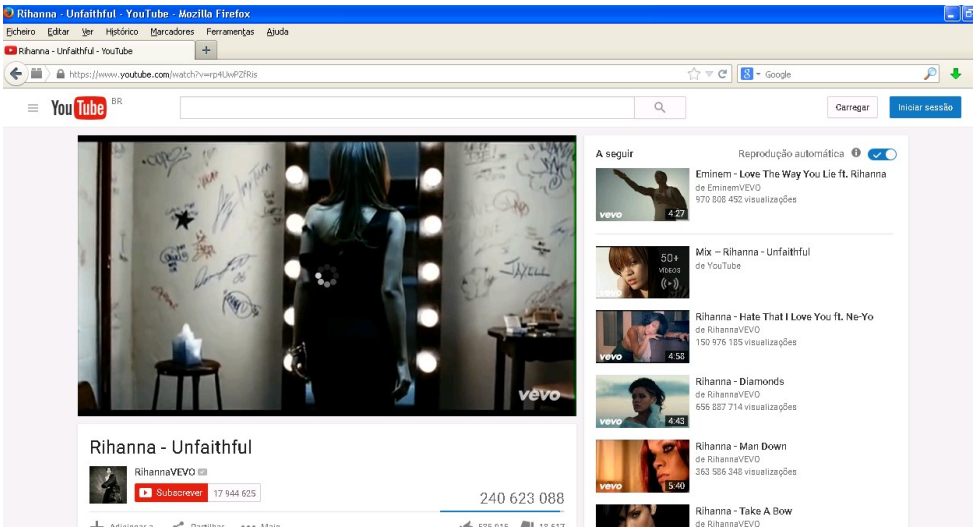
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

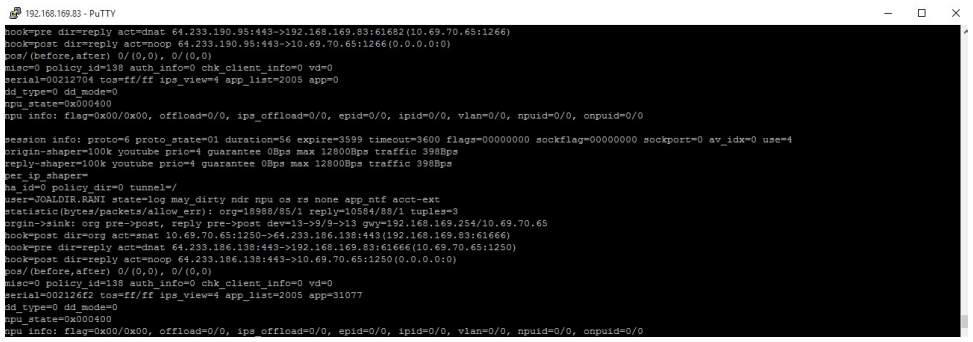
QOS

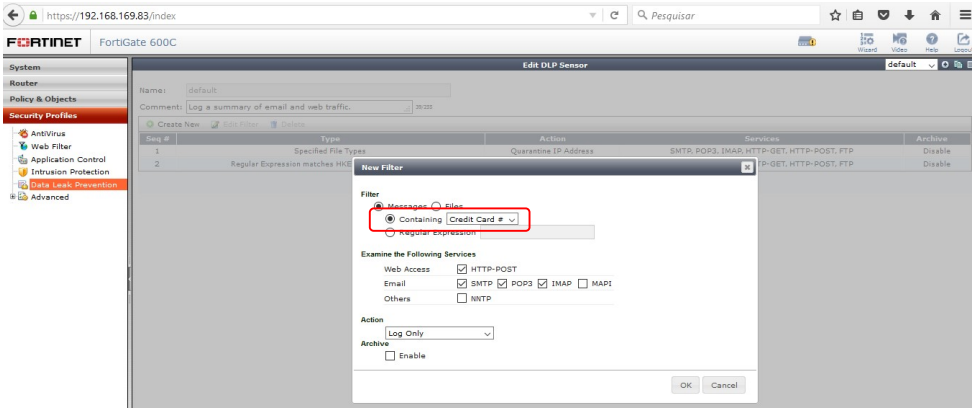
Item de Teste - 1.6.8.1	Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo (youtube, ustream e etc.) e ter um alto consumo de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, tenha a capacidade de controlá-las por políticas de máximo 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	

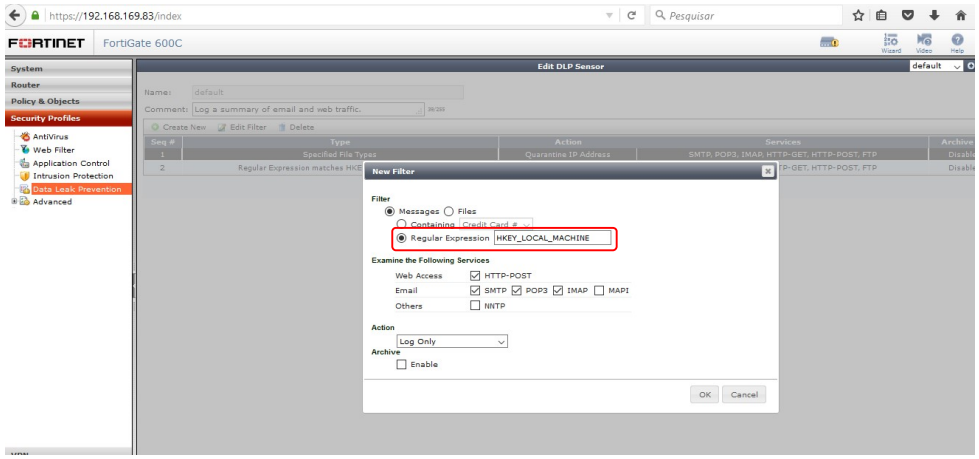

https://192.168.169.83/index
FORTINET
FortiGate 600C
Edit Application Sensor
Youtube
Name
Comments
[View Application Signatures]
Categories
Botnet
General.Interest
Social.Media
Web.Others
Business
Mobile
Storage.Backup
All Other Known Applications
Cloud.IT
Network.Service
Update
All Other Unknown Applications
Collaboration
P2P
Video/Audio
Email
Proxy
VoIP
Game
Remote.Access
Industrial
Application Overrides
Delete
Add Signatures
Application Signature
Category
Action
YouTube
Video/Audio
Traffic Shaping
100k youtube
Options
Deep Inspection of Cloud Applications
Allow and Log DNS Traffic
Replacement Messages for HTTP-based Applications
Apply

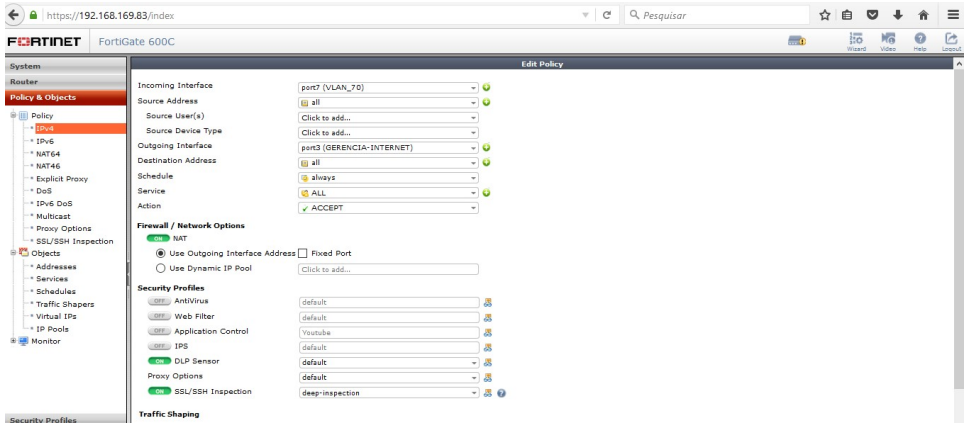

https://192.168.169.83/index
FORTINET
FortiGate 600C
Edit Policy
Incoming Interface
port7 (VLAN_70)
Source Address
all
Source User(s)
Source Device Type
Outgoing Interface
port3 (GERENCIA-INTERNET)
Destination Address
Schedule
always
Service
ALL
Action
ACCEPT
Firewall / Network Options
NAT
Use Outgoing Interface Address
Fixed Port
Use Dynamic IP Pool
Security Profiles
AntiVirus
Web Filter
Application Control
Youtube
IPS
DLP Sensor
SSL/SSH Inspection
deep-inspection
Traffic Shaping
Shared Shaper
100k youtube
Reverse Shaper
Per-IP Shaper
Logging Options
Log Allowed Traffic


Rihanna - Unfaithful - YouTube - Mozilla Firefox
Rihanna - Unfaithful - YouTube
Carregar
Iniciar sessão
A seguir
Reprodução automática
Eminem - Love The Way You Lie ft. Rihanna
Mix – Rihanna - Unfaithful
Rihanna - Hate That I Love You ft. Ne-Yo
Rihanna - Diamonds
Rihanna - Man Down
Rihanna - Take A Bow
Rihanna - Unfaithful
RihannaVEVO
Subscrever
240 623 088

			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

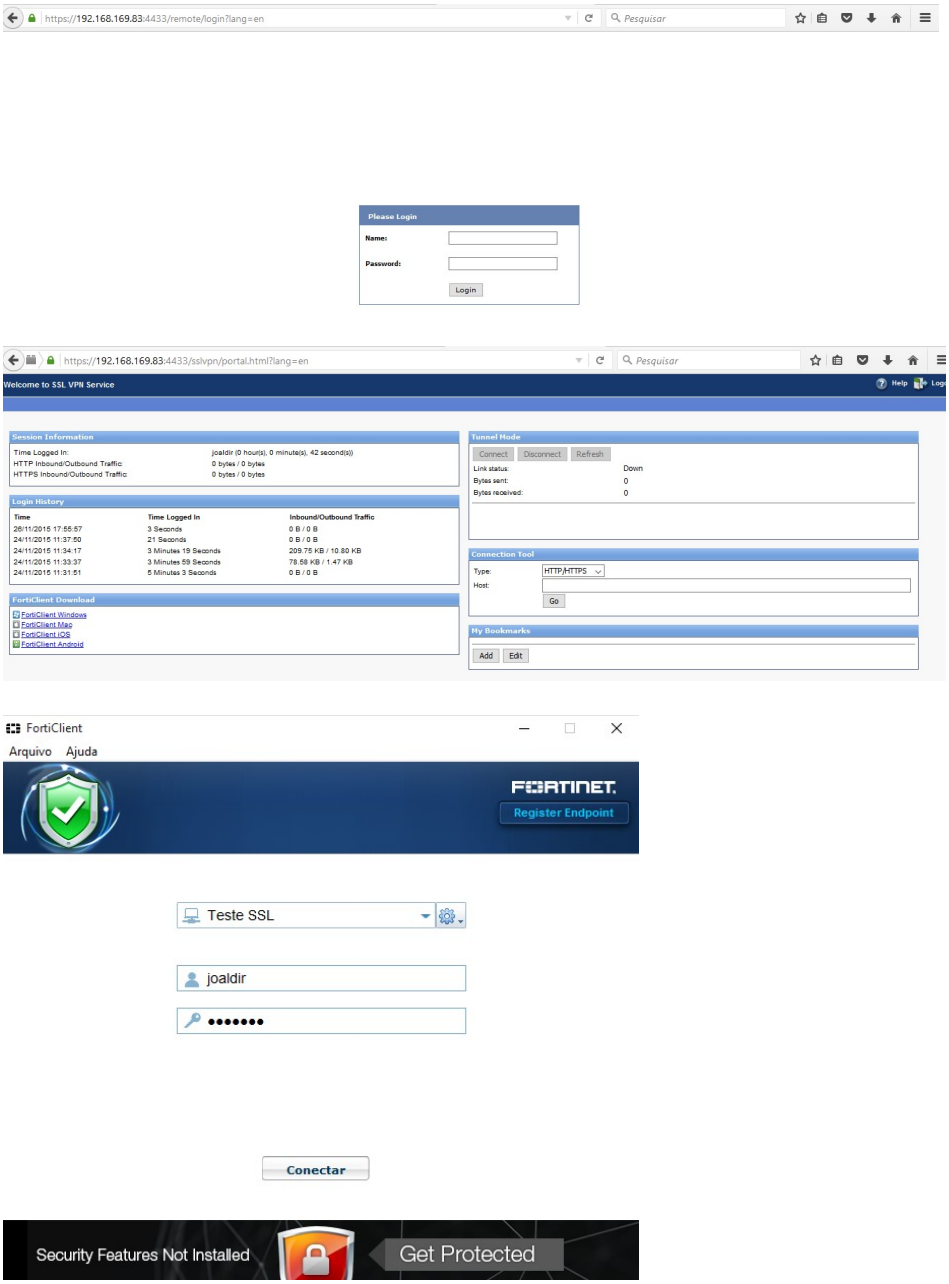
Item de Teste - 1.6.9.5	Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a: número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado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

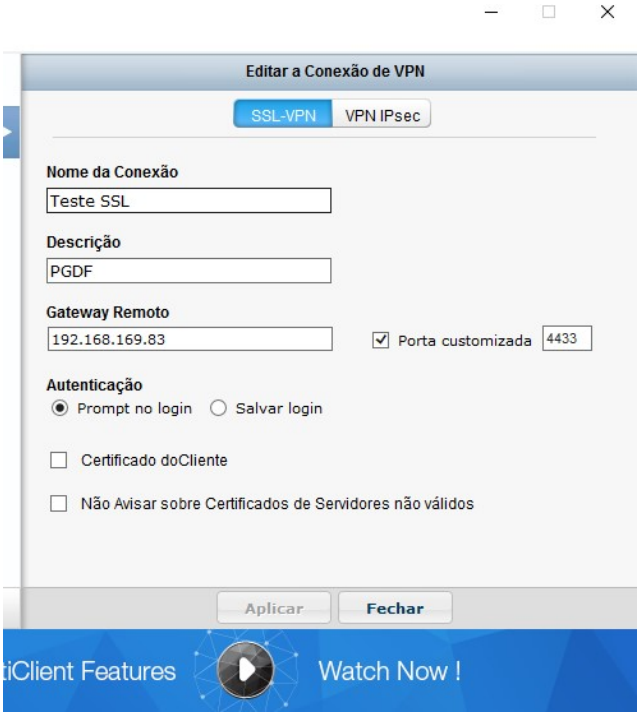




Comentário			
Assinatura do Cliente		**Assinatura NCT**	

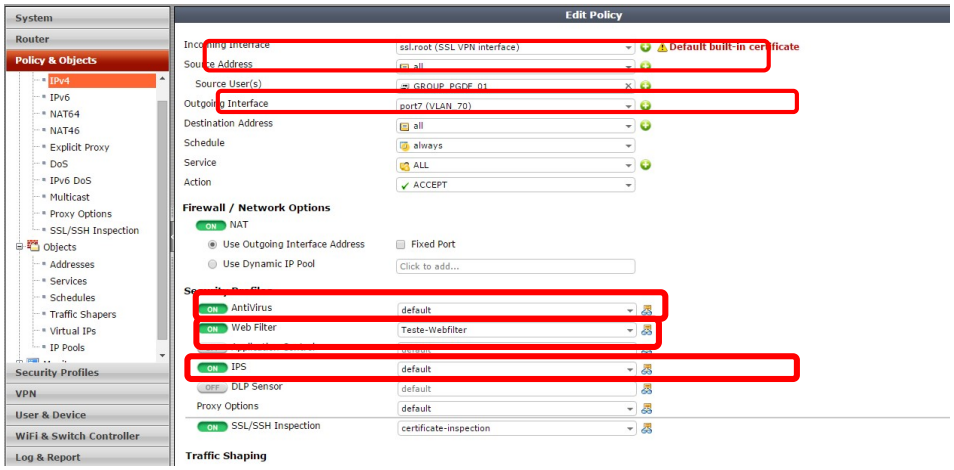
Item de Teste - 1.6.11.6.1.2	A funcionalidade de VPN SSL deve ser atendida com ou sem o uso de agente;
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado
Configuração do Teste	Instalar forticlient SSL VPN em uma estação de trabalho de um usuário assim como efetivar um acesso, em seguida 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
Please Login
Name:
Password:
Login
https://192.168.169.83:4433/sslvpn/portal.html?lang=en
Welcome to SSL VPN Service
Session Information
Tunnel Mode
Connect
Disconnect
Refresh
Login History
Connection Tool
FortiClient Download
My Bookmarks
Add
Edit
FortiClient
Arquivo
Ajuda
FORTINET
Register Endpoint
Teste SSL
joaldir
Conectar
Security Features Not Installed
Get Protected

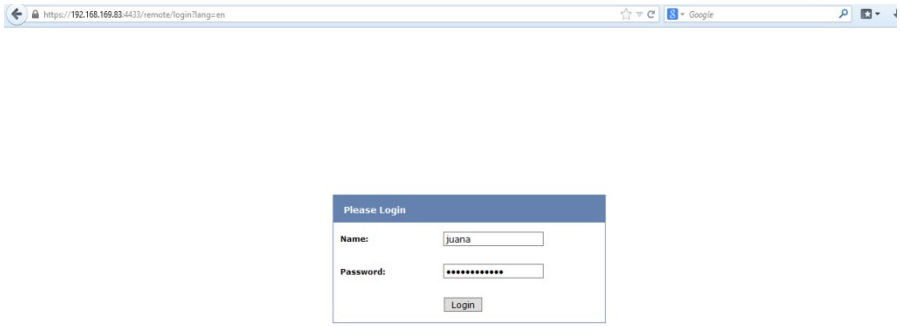


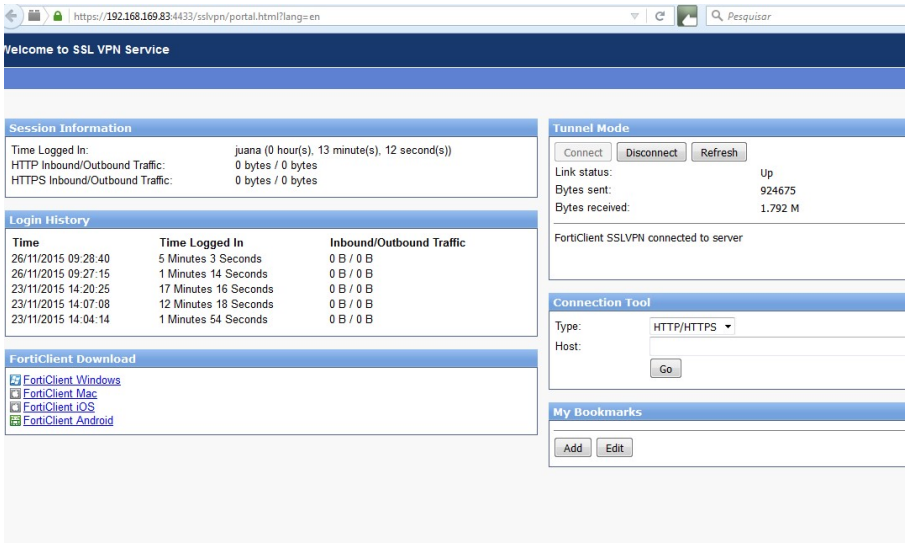
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

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:



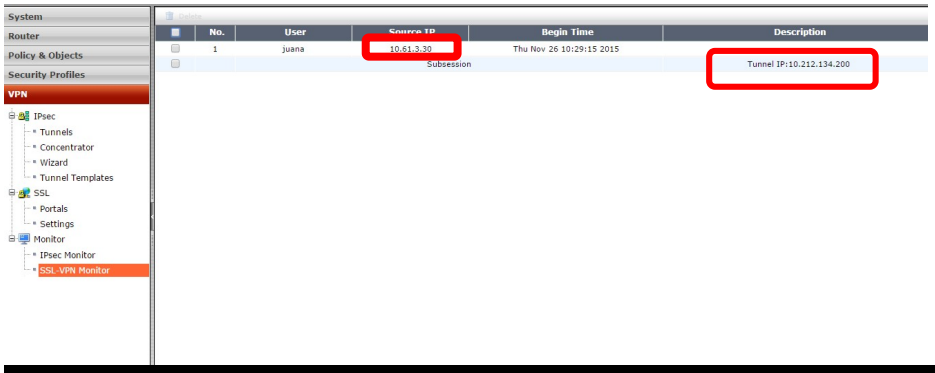
Usuário conectou-se a VPN com a credencial "juana":





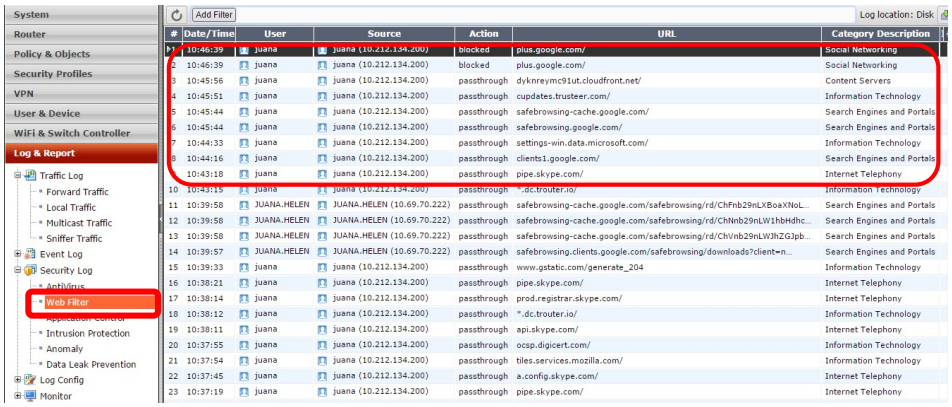
Monitor no firewall dos usuários conectados na VPN, onde é possível observar

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

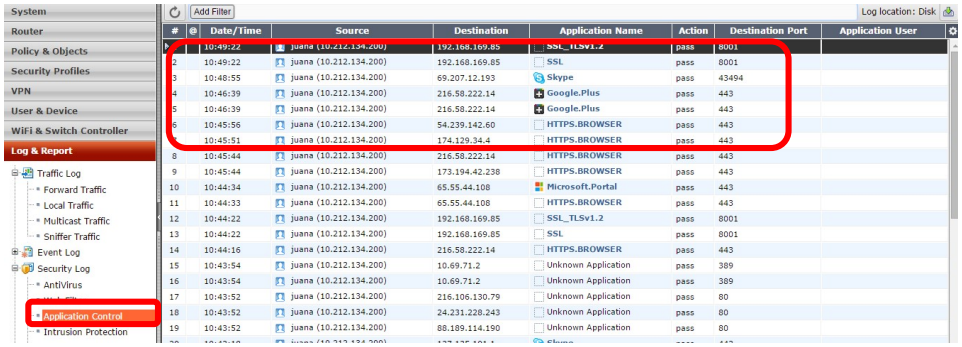



```
Adaptador PPP fortissl:

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

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:
```

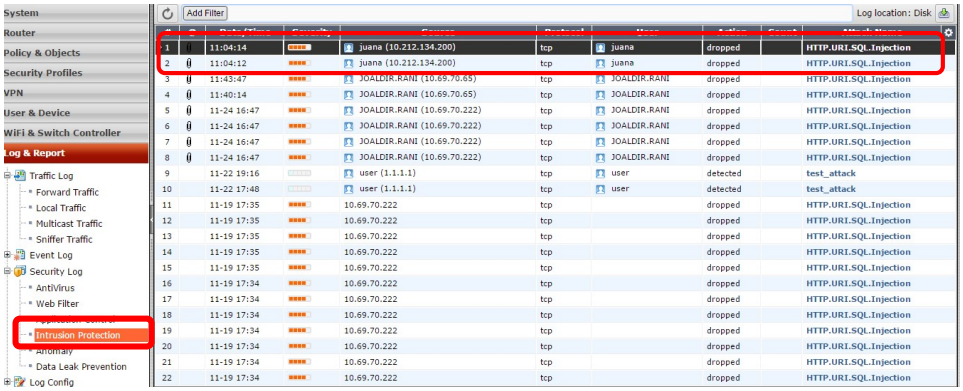
No log do Fortigate é possivel observar vários eventos de webfilter :



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

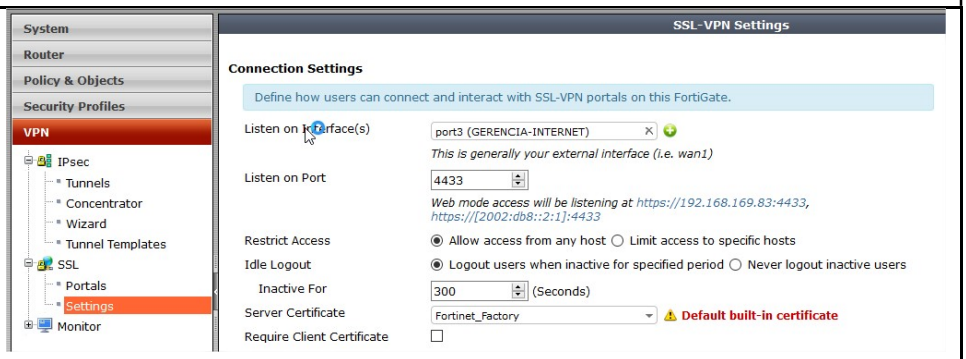
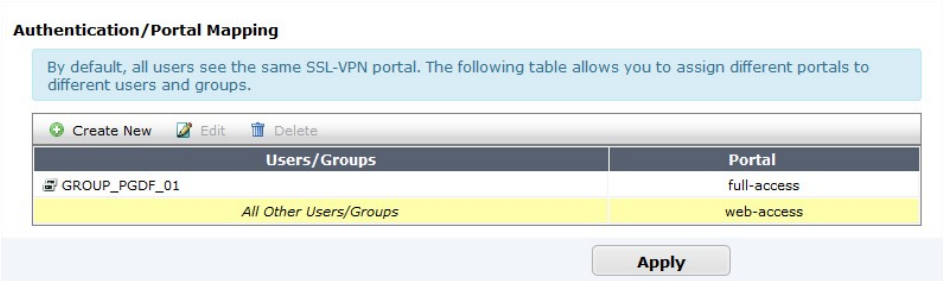
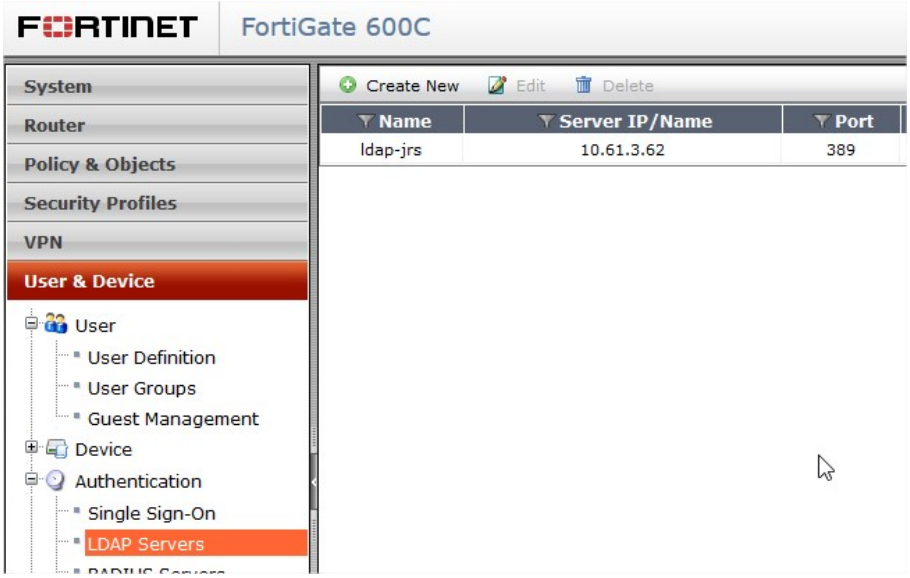


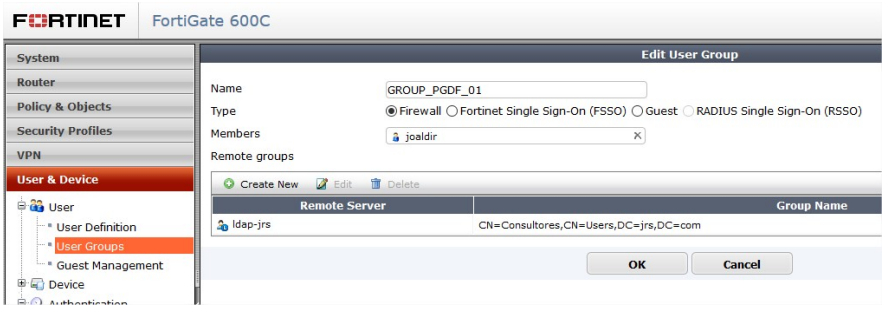
No log do Fortigate é possivel observar vários eventos de IPS :



Comentário	
Assinatura do Cliente	**Assinatura NCT**

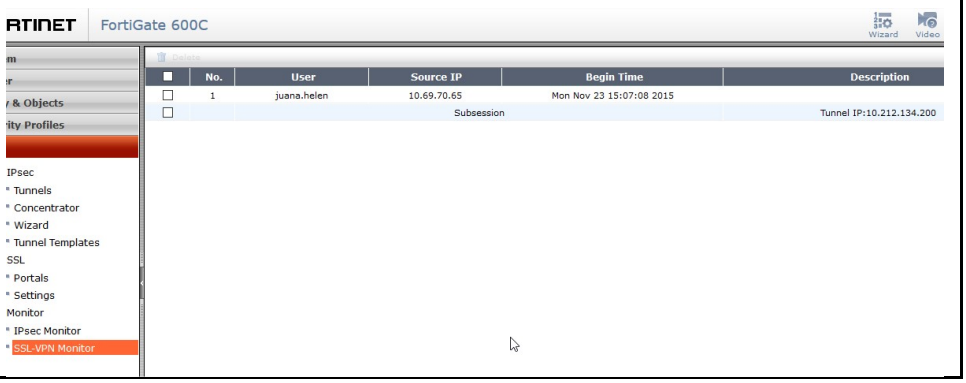
Item de Teste - 1.6.11.6.1.9	Permitir estabelecer um túnel VPN client-to-site do cliente à plataforma de segurança, fornecendo uma solução de single-sign-on aos usuários, integrando-se com as ferramentas de Windows-logon;
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado
Configuração do 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

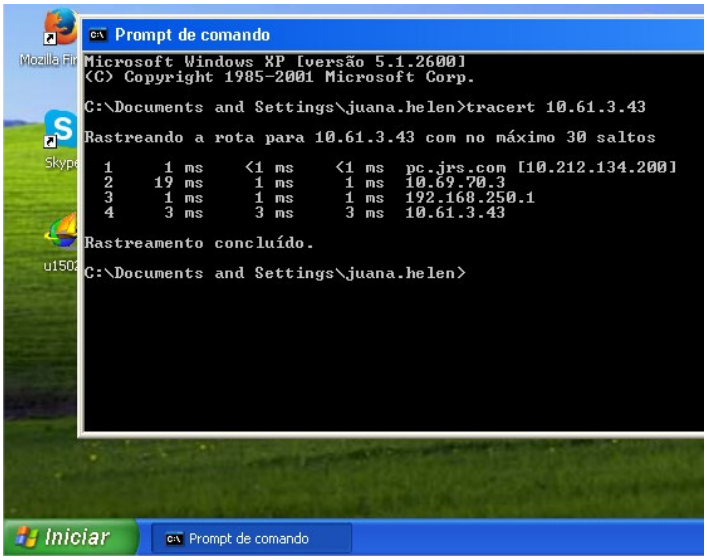
	caminho do cliente ao servidor demonstrando que o trafego passava pelo tunel. Foi aberto uma sessão de compartilhamento de arquivos no servidor de arquivos 10.61.1.43 para demonstrar acesso as recursos.
Evidências	  


FORTINET
FortiGate 600C
System
Router
Policy & Objects
Security Profiles
VPN
User & Device
User
User Definition
User Groups
Guest Management
Device
Edit User Group
Name
GROUP_PGDF_01
Type
Firewall
Fortinet Single Sign-On (FSSO)
Guest
RADIUS Single Sign-On (RSSO)
Members
joaldir
Remote groups
Create New
Edit
Delete
Remote Server
Group Name
ldap-jrs
CN=Consultores,CN=Users,DC=jrs,DC=com
OK
Cancel

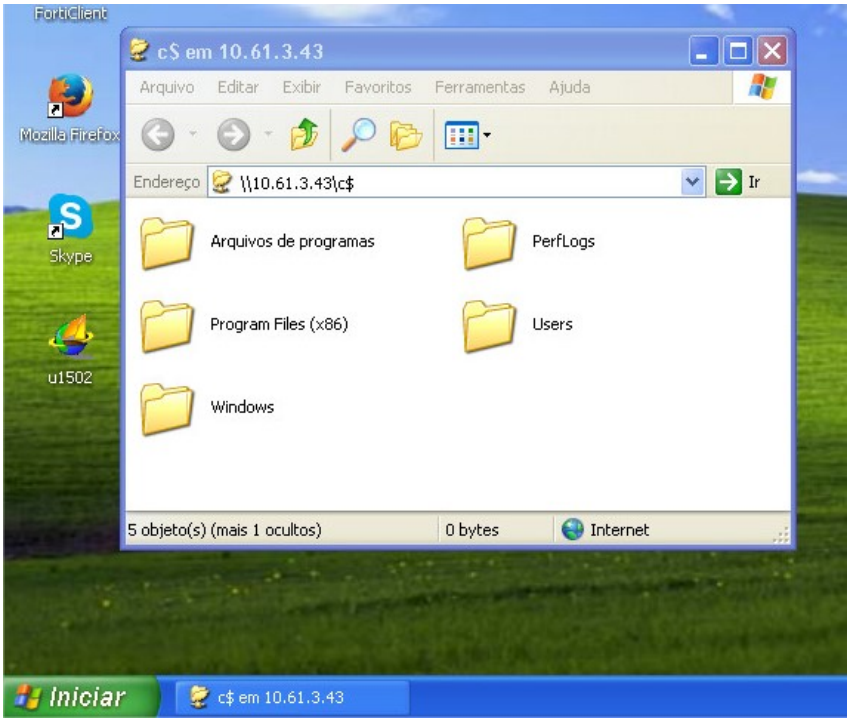
Logon no Windows
Windows XP
Lite 4.0
Nome de usuário:
juana.helen
Senha:
Fazer logon em:
JRS
Fazer logon usando uma conexão dial-up
PT
OK
Cancelar
Desligar...
Opções <<
VPN antes do
pgdf_lab
Minhas credenciais de VPN credentials são as mesmas crede
Usuário da
Senha da VPN:

FortiClient
Windows XP
Lite 4.0
Conectando no tunel VPN (pgdf_lab)...


RTINET
FortiGate 600C
Wizard
Video
IPsec
Tunnels
Concentrator
Wizard
Tunnel Templates
SSL
Portals
Settings
Monitor
IPsec Monitor
SSL-VPN Monitor
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


Prompt de comando
Microsoft Windows XP [versão 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\juana.helen>tracert 10.61.3.43
Rastreando a rota para 10.61.3.43 com no máximo 30 saltos
1 1 ms <1 ms <1 ms pc.jrs.com [10.212.134.200]
2 19 ms 1 ms 1 ms 10.69.70.3
3 1 ms 1 ms 1 ms 192.168.250.1
4 3 ms 3 ms 3 ms 10.61.3.43
Rastreamento concluído.
C:\Documents and Settings\juana.helen>
Iniciar
Prompt de comando

FortiClient
Mozilla Firefox
Skype
u1502
Executar
Digite o nome de um programa, pasta, documento ou recurso da Internet e o Windows o abrirá para você.
Abrir:
\\10.61.3.43\c$
OK
Cancelar
Procurar...
Iniciar



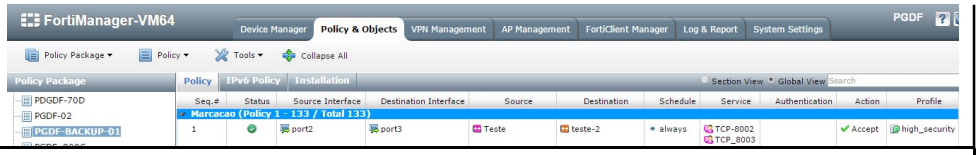
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

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:

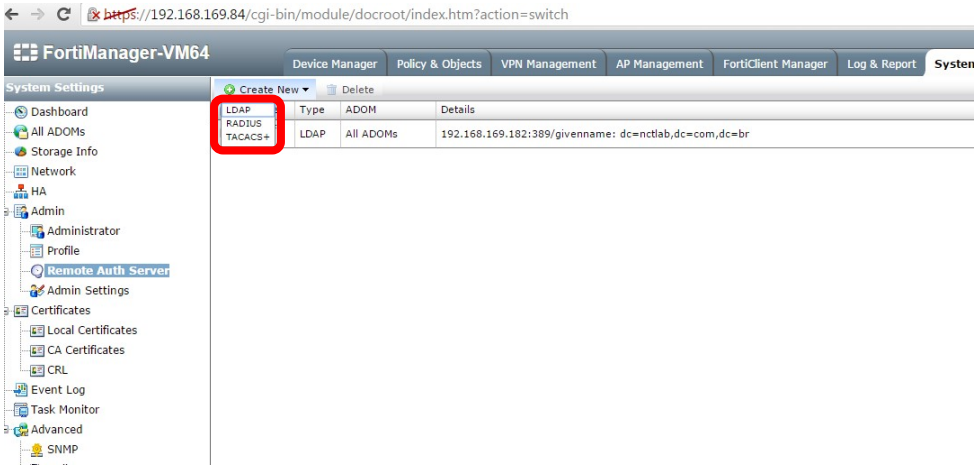
```
PGDF-BACKUP-01 # config system
3g-modem                Configure 3G modem.
accprofile              Configure system admin access group.
admin                   Configure admin users.
arp-table               Configure ARP table.
auto-install            Configure USB auto installation.
autoupdate              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 addre
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--
```

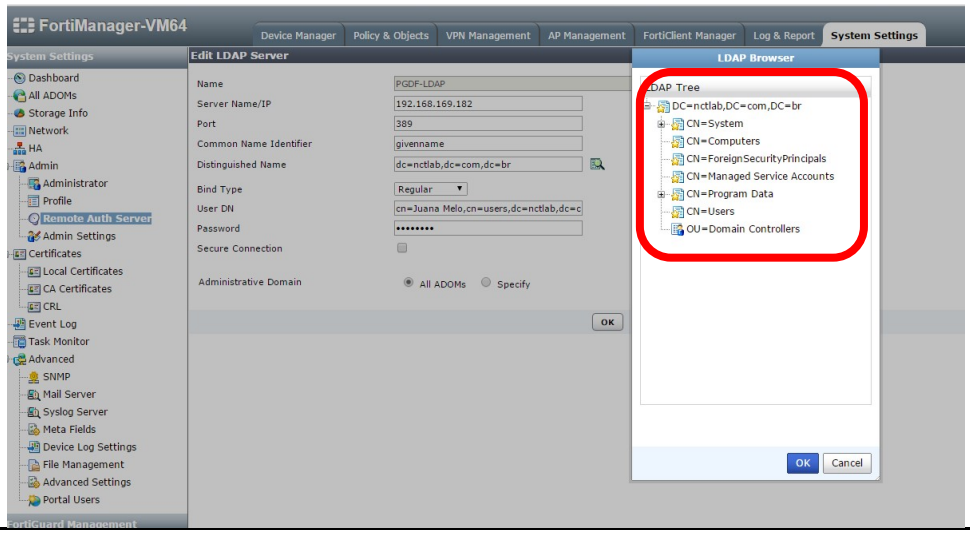
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

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 difereciados 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:



Comentário			
Assinatura do Cliente		**Assinatura NCT**	

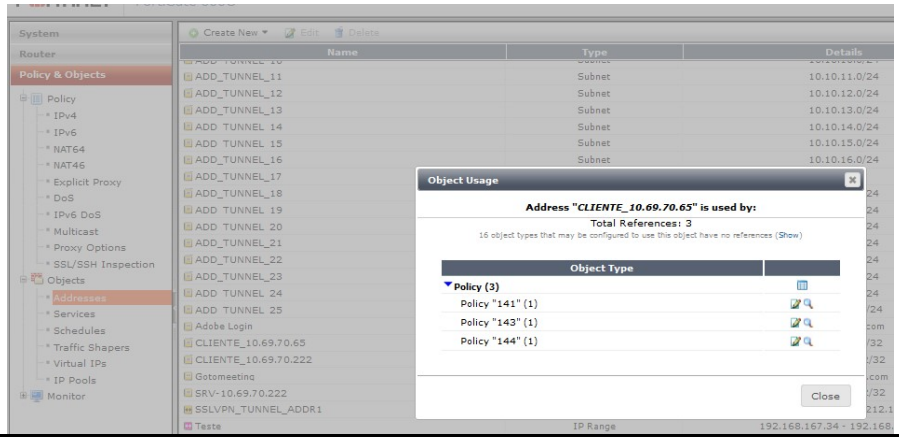
Item de Teste - 1.6.12.5.14	Autenticação integrada ao Microsoft Active Directory e servidor RADIUS;
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado
Configuração do Teste	Configurar servidores de autenticação remoto e integração com o AD conforme solicitado neste item
Procedimento do Teste	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 arvore do AD:



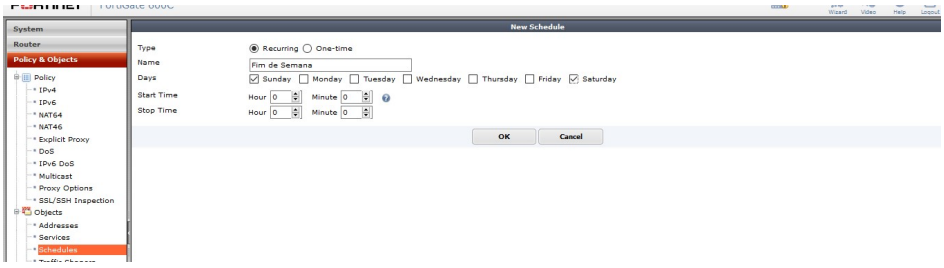
Comentário	
Assinatura do Cliente	**Assinatura NCT**

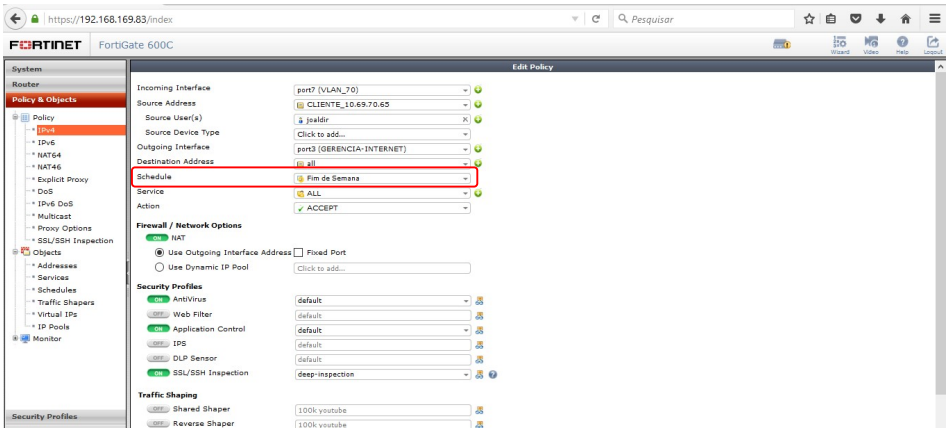
Item de Teste - 1.6.12.5.15	Localização de em quais regras um endereço IP, IP range, subnet ou objetos estão sendo utilizados;
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado
Configuração do Teste	Automaticamente ao configurar um objeto e sendo este inserido em uma regra, perfil ou group, 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:

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

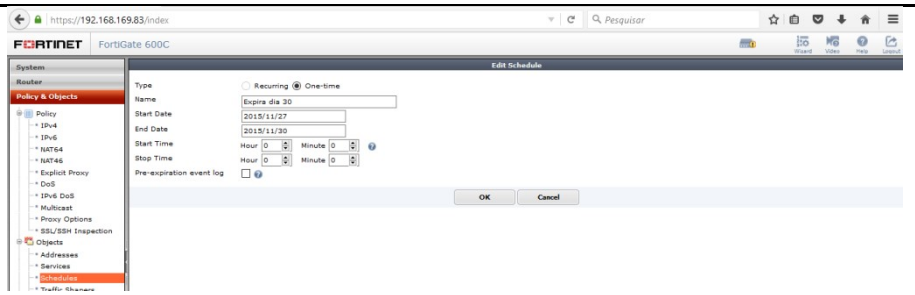
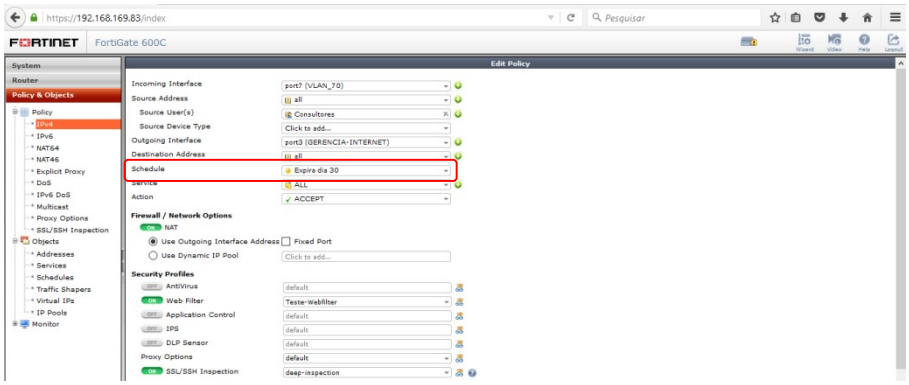


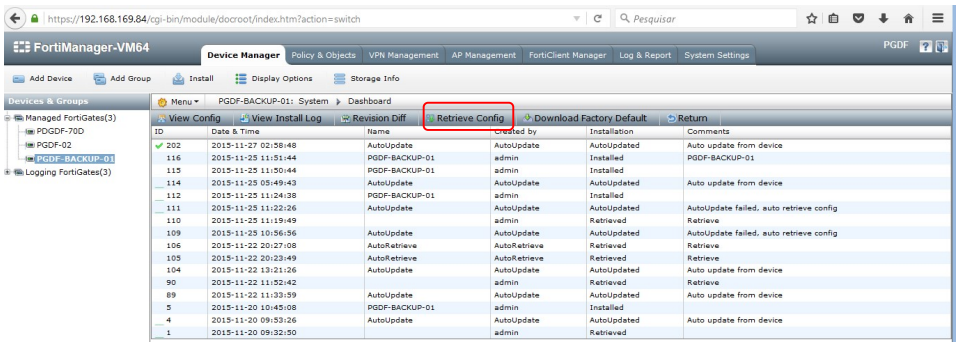
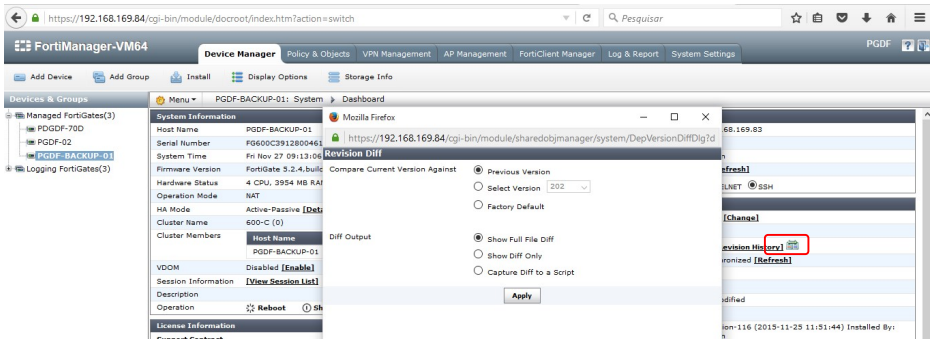
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

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	



Comentário			
Assinatura do Cliente		**Assinatura NCT**	

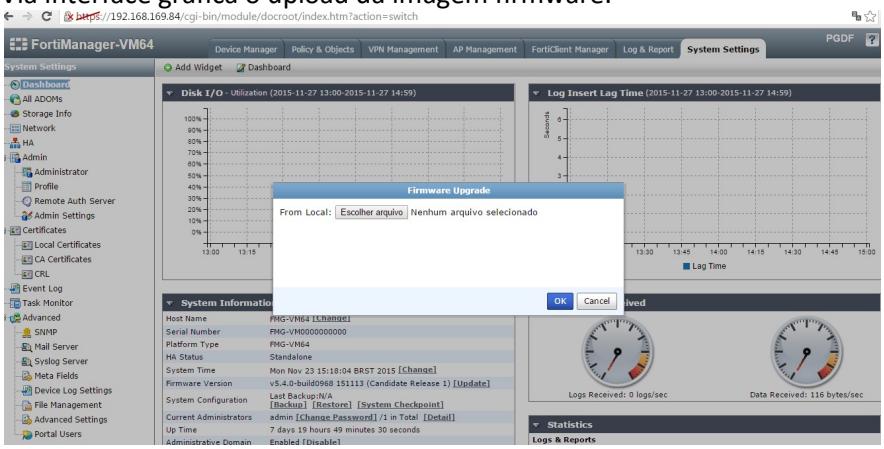
Item de Teste - 1.6.12.5.18	Criação de regras com data de expiração;
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado
Configuração do Teste	Configurar um schedule de período de expiração determinado
Procedimento do Teste	Executar teste de expiração da regra no horário conforme definido.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

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 retrievie manual de configuração e salvar
Procedimento do Teste	Executar teste de backup e de rollback
Evidências	 
Comentário	
Assinatura do Cliente	**Assinatura NCT**

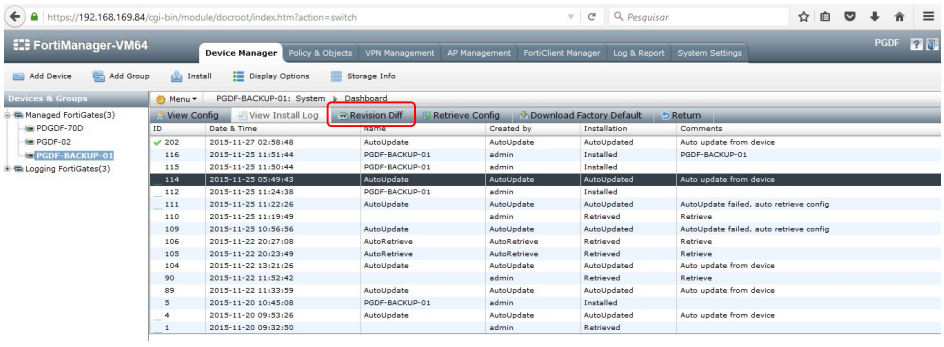
Item de Teste - 1.6.12.5.21	Habilidade de upgrade via SCP, TFTP e interface de gerenciamento;
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado
Configuração do Teste	Iniciar upgrade conforme solicitado
Procedimento do Teste	Mostrar processo de upgrade pela interface de gerenciamento, CLI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

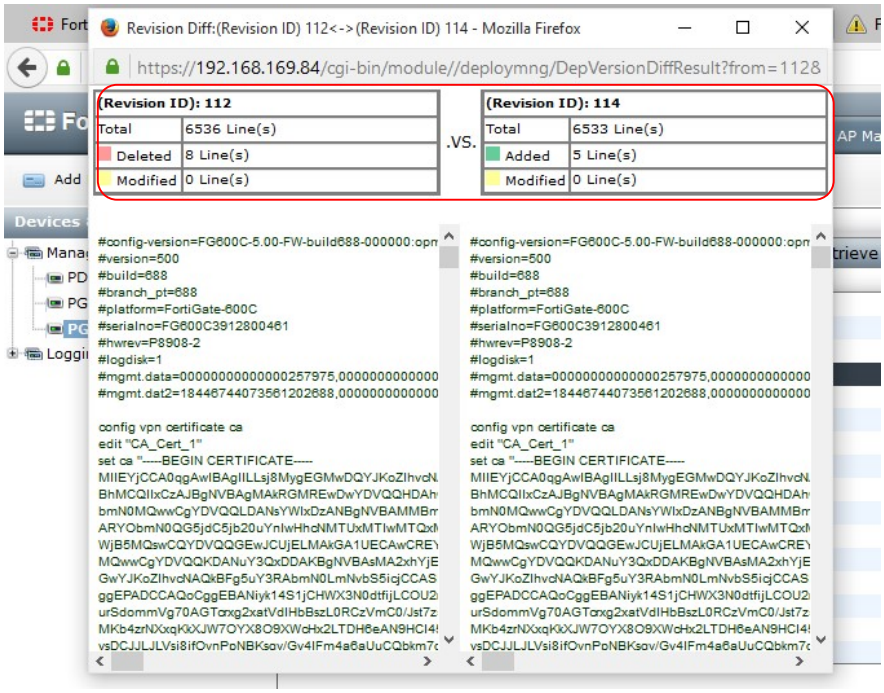
```
FMG-VM64 # execute upload image
ftp      Load image from FTP server.
tftp     Load image from TFTP server to local disk.
usb      Load image from USB to local disk.
```

Via interface gráfica o upload da imagem firmware:



Comentário			
Assinatura do Cliente		**Assinatura NCT**	

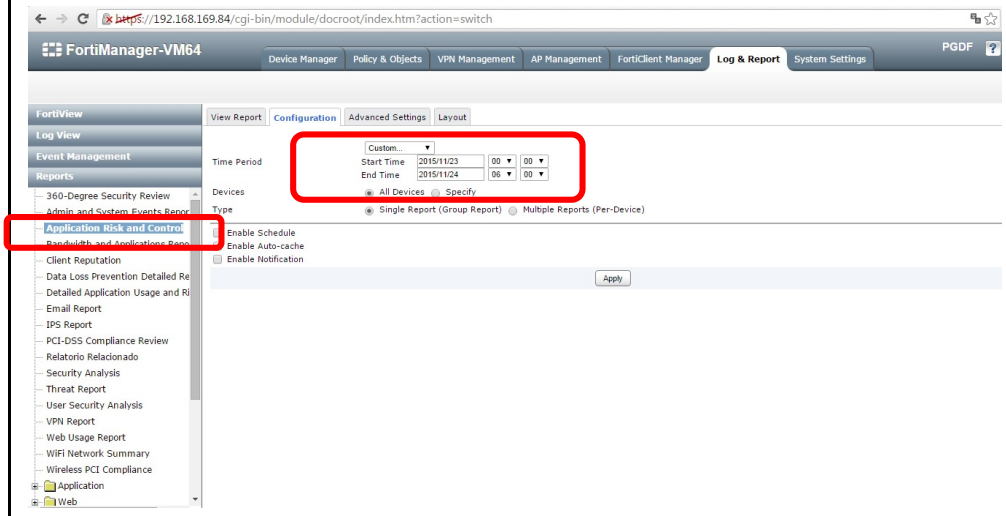
Item de Teste - 1.6.12.5.25	Deve possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas;
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado
Configuração do Teste	Clicar na opção de diff-policy e revision para efetivar um deparar das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



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:

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:

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.Portal	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	Activesync	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

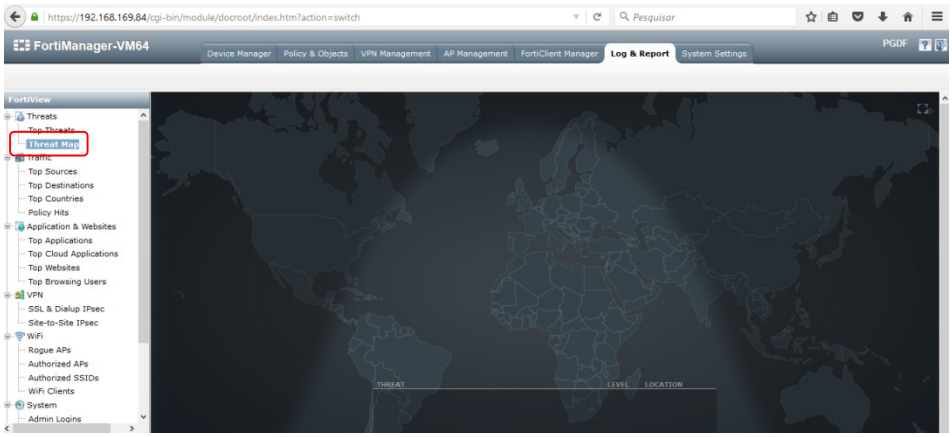
Top 20 high risk applications are listed below. These applications have the risk rating of 5 (critical risk) or 4(high risk). Each application is listed with its respective category, technology, number of users, bandwidth and sessions.

#	Risk	Application Name	Category	Technology	User	Bandwidth	Session
1	5	Ultrasurf_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

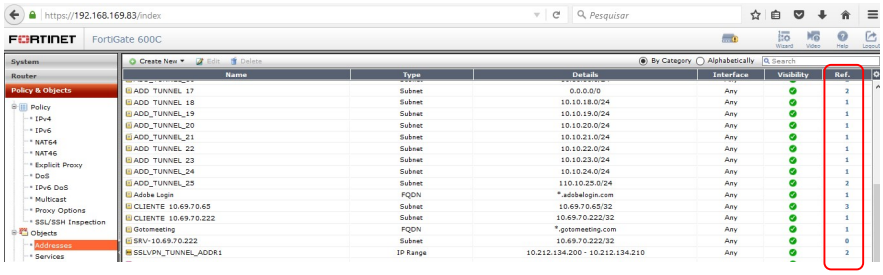
Figure 2: High risk applications (rating of 4 or 5) that are traversing the network.

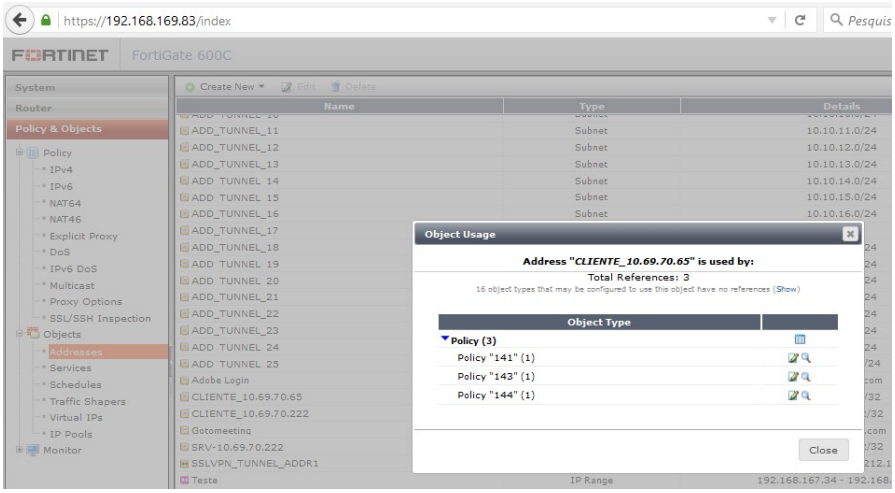
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

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	



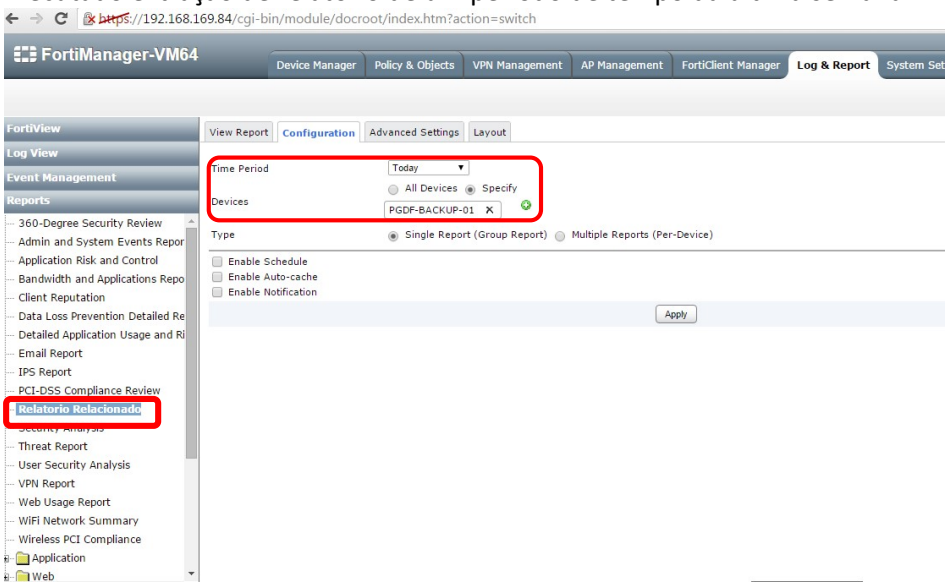
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

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	



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	Executado extração de relatório de um período de tempo da ultima semana:



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

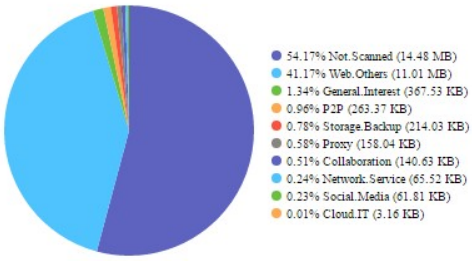
App Categories

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

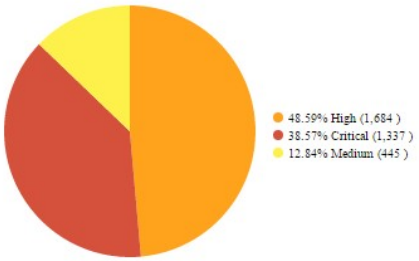
Top 20 Viruses

#	Virus Name	Occurrences
1	Riskware/UltraReach	1

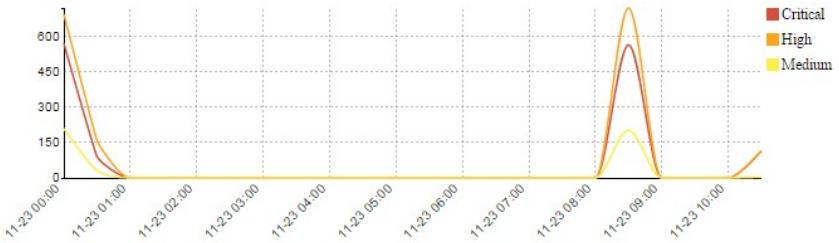
Top 20 Web Domains by Visits

#	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.mxtck.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	akhtm.nspmotion.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



Intrusions

Intrusions Detected

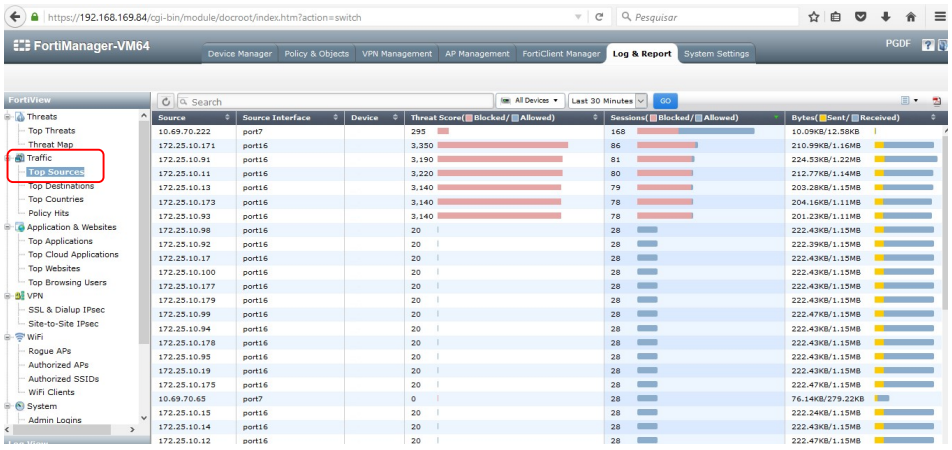
#	Attack Name	Severity	CVE-ID	Counts
1	MS.Word.Linked.Objects.Memory.Corruption	Critical	CVE-2010-1903	80
2	MS.Publisher.Pubconv.dll.Pointer.Overwrite.Memory.Corruption	Critical	CVE-2011-1508	40
3	MS.Visio.Invalid.Tag.Handling.Remote.Code.Execution	Critical	CVE-2009-0096	40
4	MS.Windows.MPEG4.Codec.ASF.Parsing.Code.Execution	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-2010-3231	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

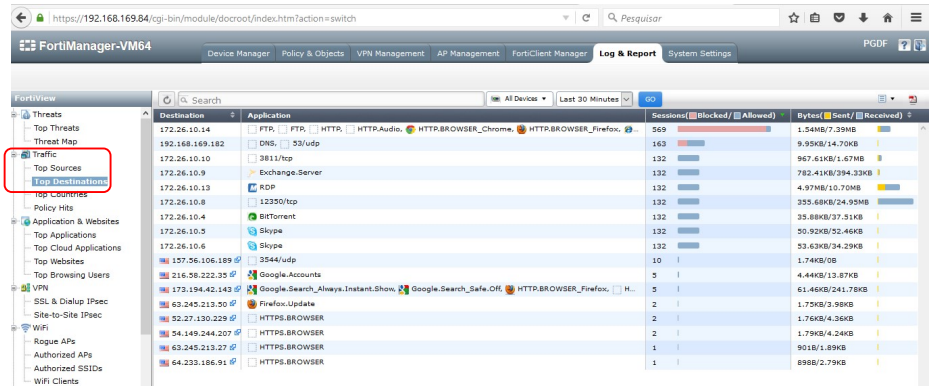
Malware

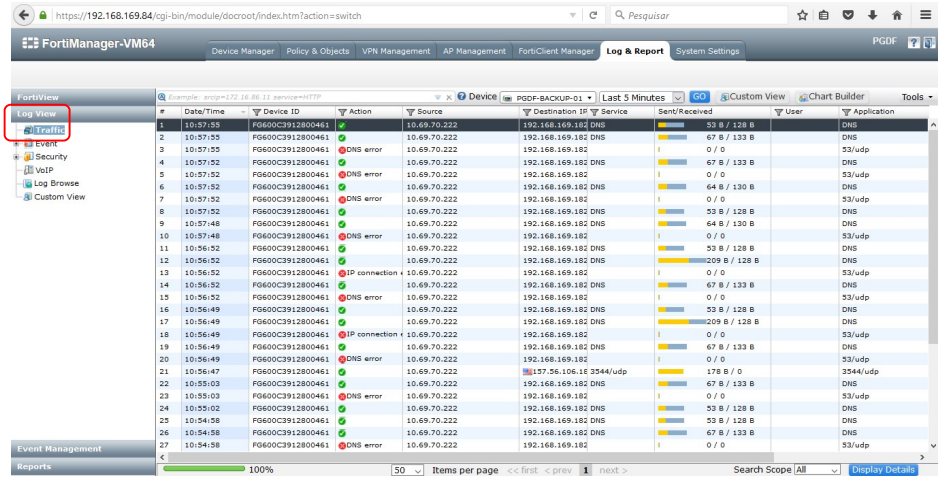
Malware Detected

#	Malware Name	Malware Type	Counts
1	MSOffice/CVE_2013_3906.B!exploit	Virus	60
2	MSWord/CVE20103333.A!exploit	Virus	40
3	PDF/Shellkode.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

Comentário			
Assinatura do Cliente		**Assinatura NCT**	

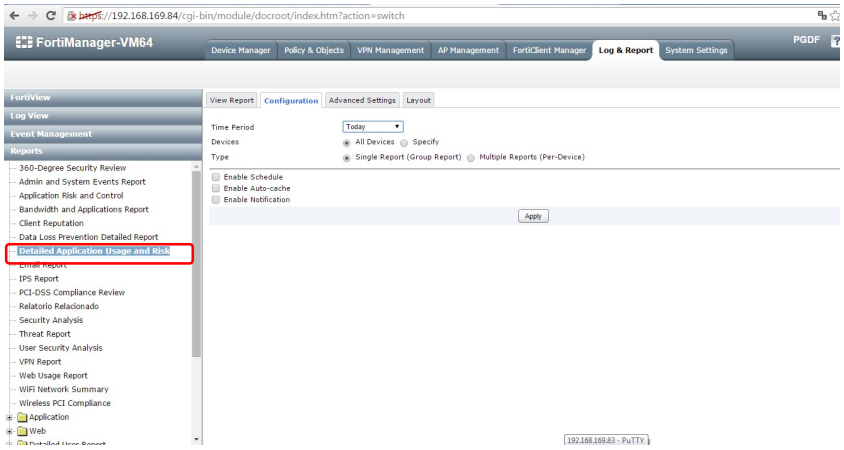
Item de Teste - 1.6.12.7	O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelo dispositivo de segurança;
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado
Configuração do Teste	Apresentar Log & Report
Procedimento do Teste	Demonstrar Log 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 especifico para detalhado recurso de aplicações:



Alguns resultados extraídos do relatório de recursos de aplicação:

Application Bandwidth Usage

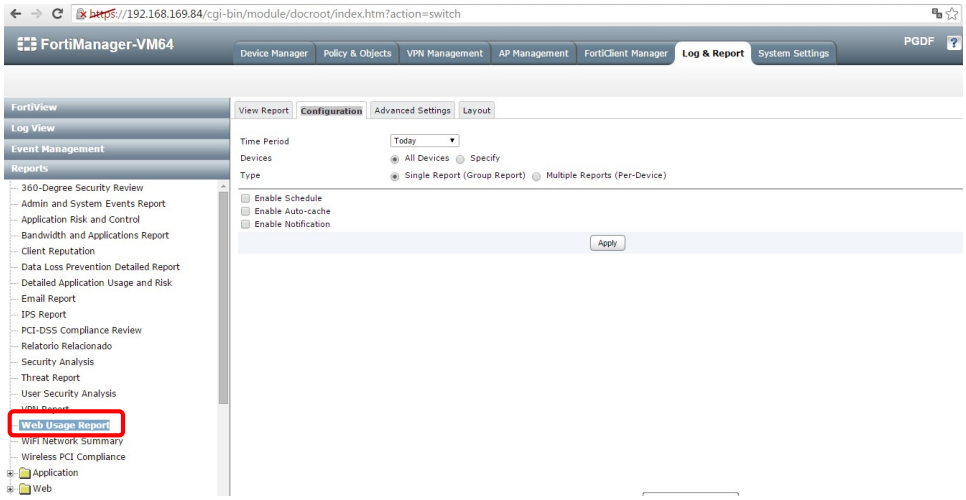
#	Application	Action	Bandwidth	Session Count
1	BitTorrent	Allowed	749.69 KB	1,517
2	BitTorrent	Blocked	260.36 KB	930
3	Bitcomet.HTTP.Seed	Blocked	3.91 KB	149
4	Bitcomet.HTTP.Seed	Allowed	880 B	6

*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.Portal	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 especifico 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

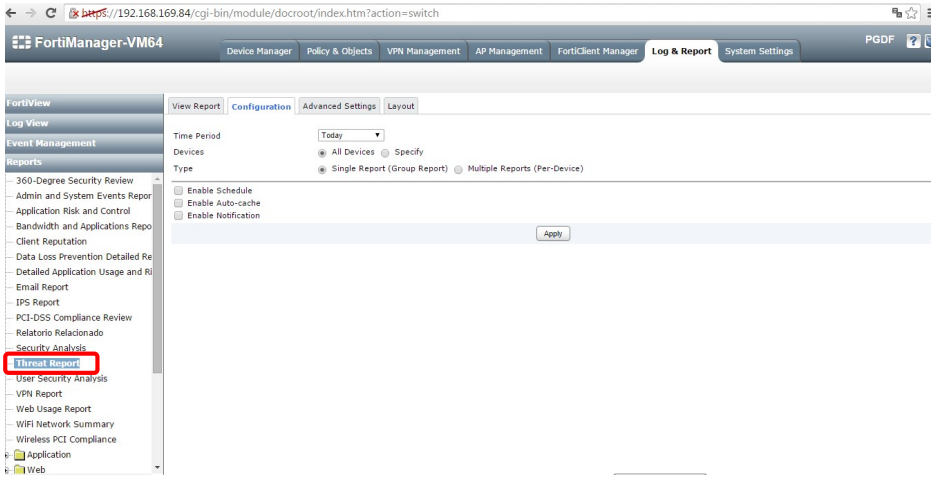
Top 20 Most Visited Categories

#	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.googlesyndication.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.googlesyndication.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.mxtck.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.bitmedianetwork.com	Advertising	24
29	userdmp.com	Meaningless Content	19
30	akhtm.nspmotion.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.mathtag.com	Content Servers	15
34	b.scorecardresearch.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 especifico para detalhado de ameaça:



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/Shellkode.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

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.Overwrite.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-2010-3231	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

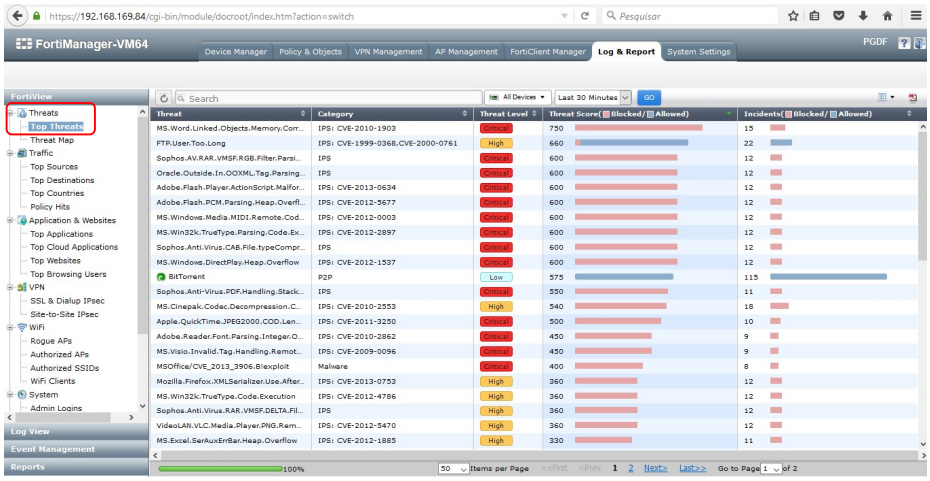
#	Attack Victim	Counts
1	172.26.10.14	370
2	172.25.10.13	39
3	172.25.10.43	39
4	172.25.10.137	39
5	172.25.10.115	39
6	172.25.10.139	39
7	172.25.10.76	39
8	172.25.10.196	39
9	172.25.10.17	39
10	172.25.10.138	39

Intrusion Sources

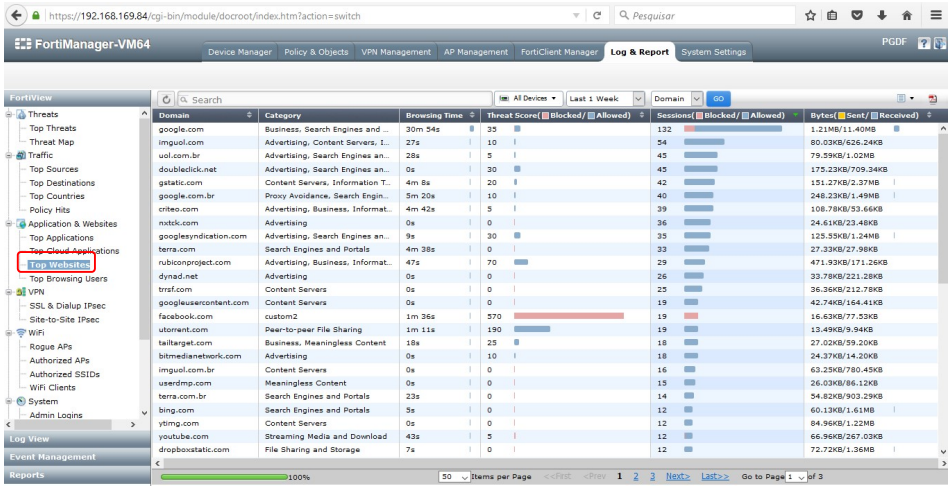
#	Attack Source	Counts
1	172.26.10.14	1,384
2	172.25.10.115	12
3	172.25.10.195	12
4	172.25.10.194	12
5	172.25.10.77	12
6	172.25.10.175	12
7	172.25.10.95	12
8	172.25.10.196	12
9	172.25.10.114	12
10	172.25.10.91	12

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	



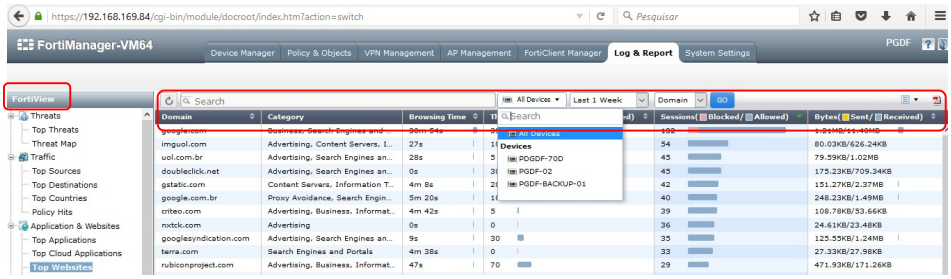
Sumário de ameaças

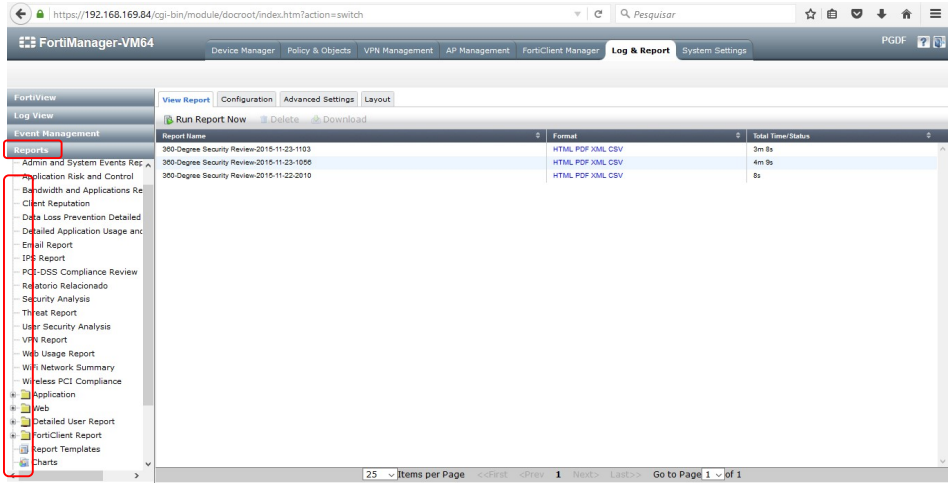


Sumário web

Comentário			
Assinatura do Cliente		**Assinatura NCT**	

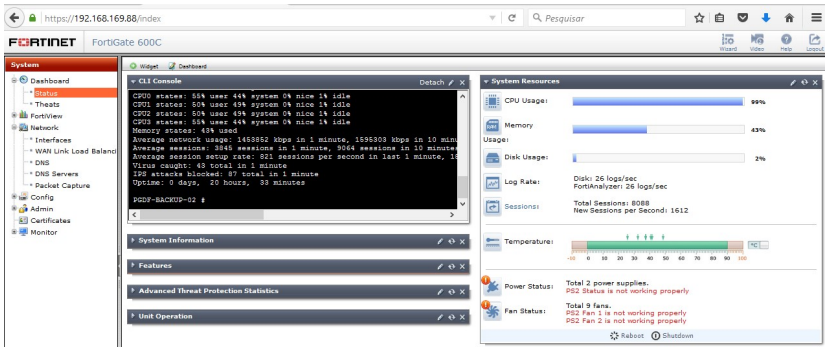
Item de Teste - 1.6.12.10	Deve possuir mecanismo "drill-down" para navegação nos relatórios em tempo real;
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado
Configuração do Teste	A partir aba Fortiview e Log&Report em qualquer uma dos módulos de sumarização clicar com o botão direito para 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	

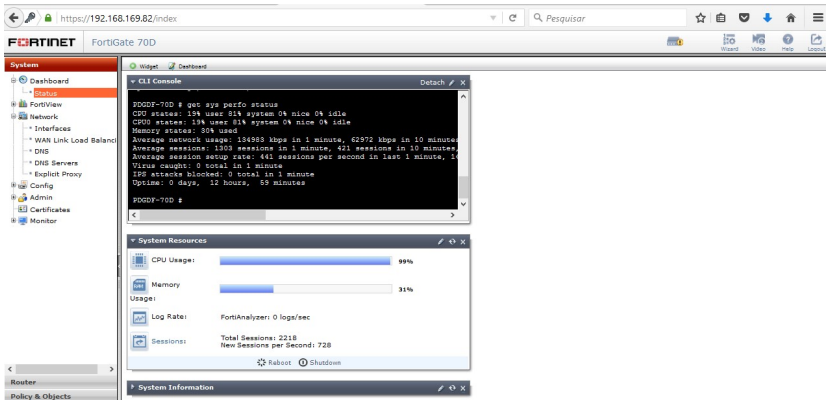


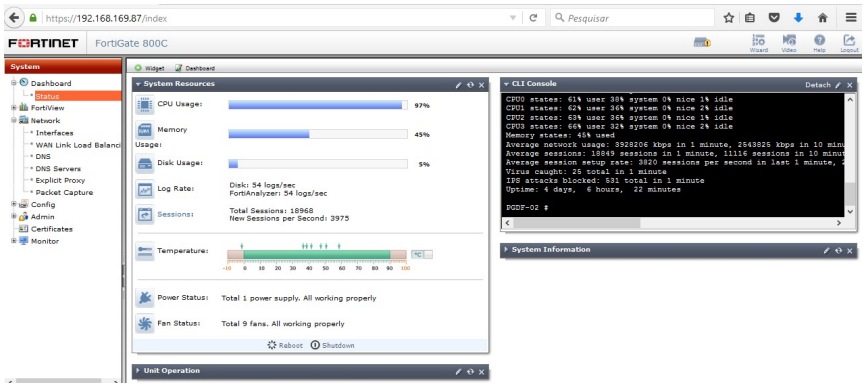


Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.12.13	Deverá ser possível acessar a gerencia para visualizar ou aplicar configurações durante os momentos onde o trafego 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	





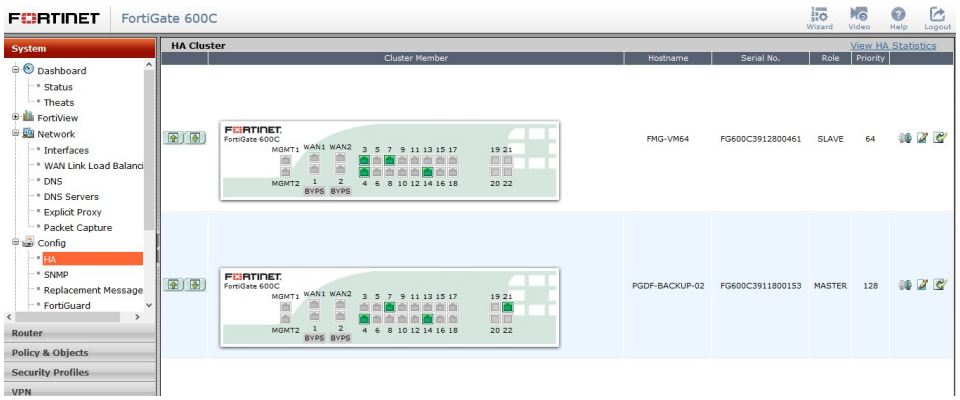


Comentário			
Assinatura do Cliente		**Assinatura NCT**	

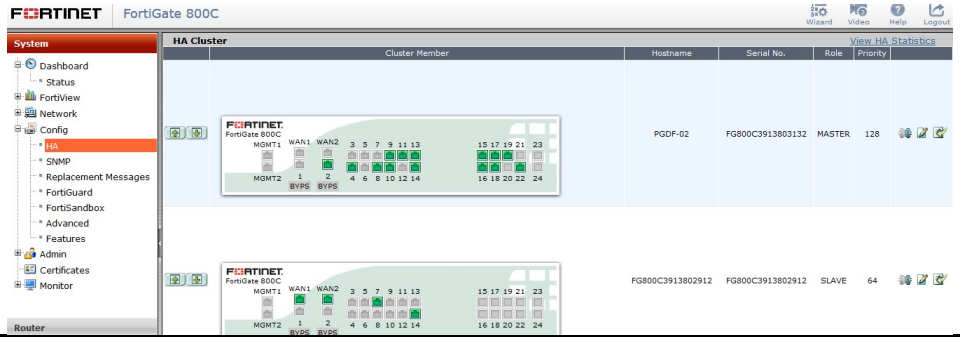
Item de Teste - 1.6.12.15.1	Situação do dispositivo e do cluster;
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado
Configuração do Teste	Equipamentos em HA
Procedimento do Teste	Demonstrar o status dos equipamentos na tela de monitor HA em ambos os cluster 600c e 800c

Evidências

600C

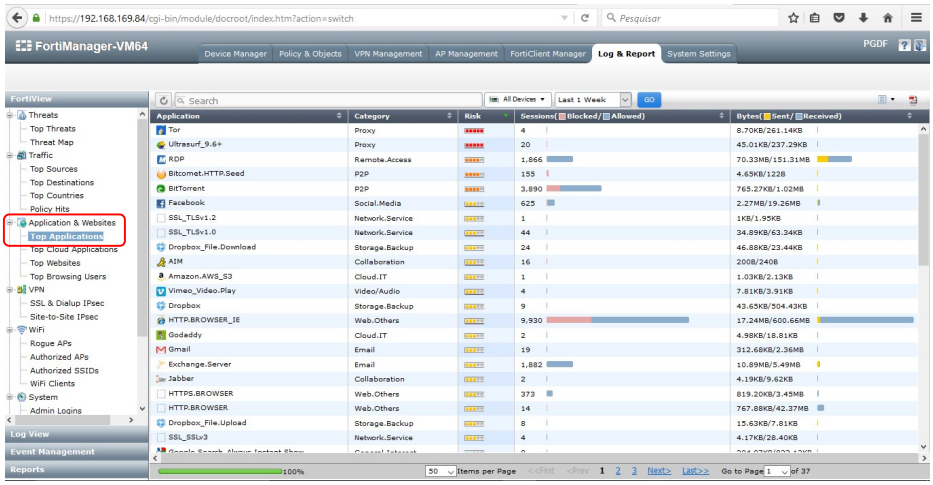


800c

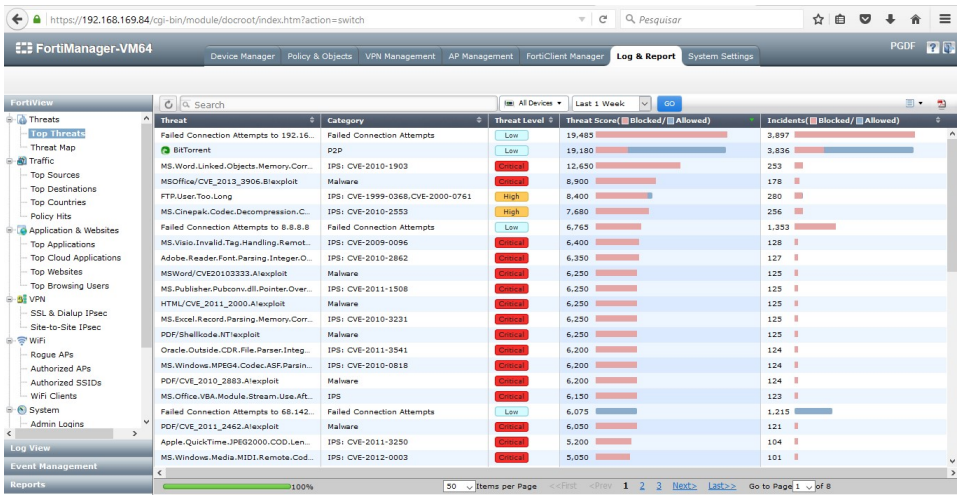


Comentário			
Assinatura do Cliente		**Assinatura NCT**	

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	

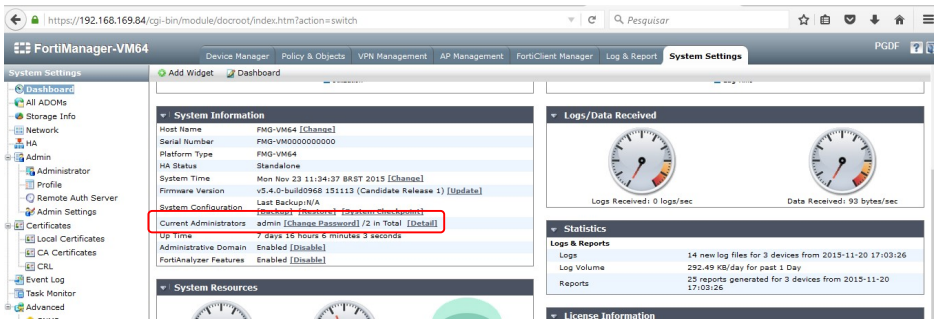


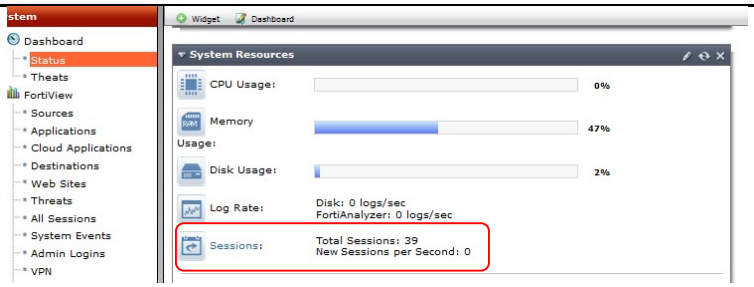
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

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	

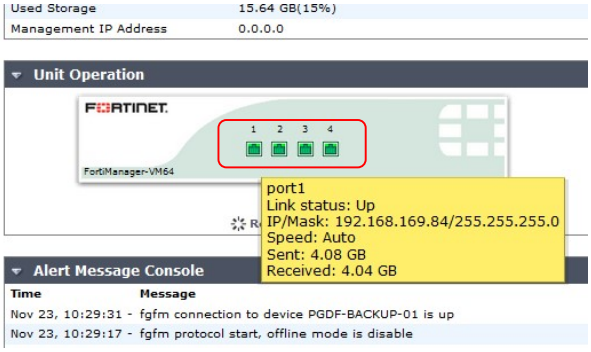
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

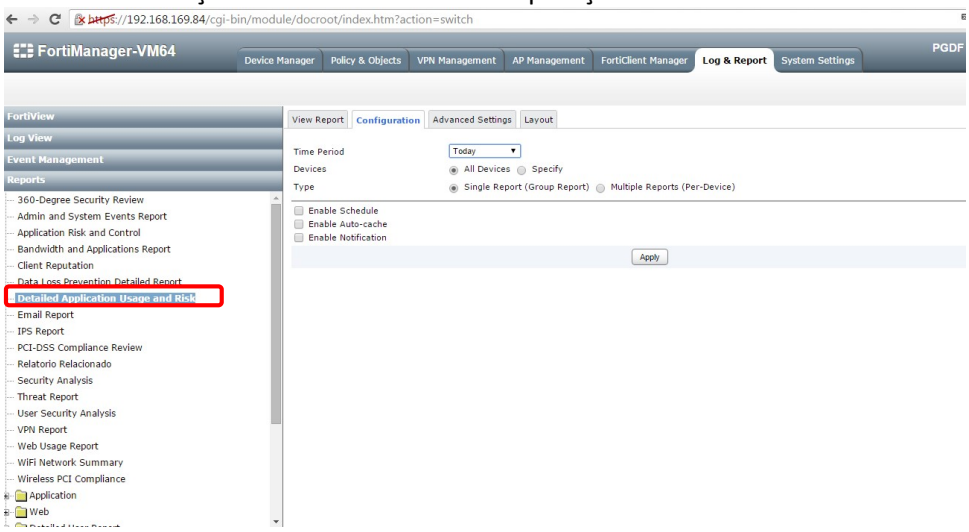
Item de Teste -	Administradores autenticados na gerência da plataforma de segurança;

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	

		[redacted] 	
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 desde relatório correspondente ao uso de aplicação por consumo de banda:

Key Applications Crossing The Network

The section below shows the top 30 applications crossing the network based on the amount of bandwidth they are using, sorted by application category and technology. The risk rating is also listed for each application along with its session count. This provides a more complete view for the applications running on the network and results in better decision-making for overall application control policies and business risk management.

#	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_IE	Web.Client	Browser-Based	1	179.72 KB	79
6	5	Ultrasurf_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

Figure 4: Top applications that are consuming the most bandwidth, sorted by category and technology

Application Categories

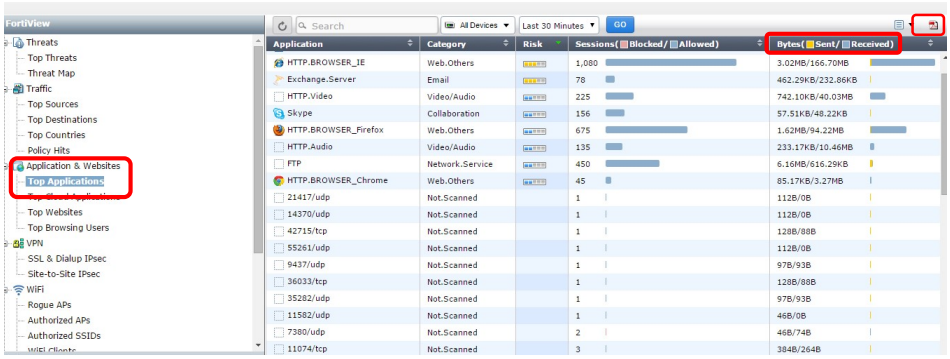
The FortiGuard research team categorizes applications into different categories based on the application behavioral characteristics, underlying technology, and the related traffic transaction characteristics. The categories allow for better application management. For application category details, see: http://www.fortiguard.com/encyclopedia/applications

The following section shows the application category breakdown of all the applications on the network, sorted by bandwidth. This information helps network administrators to identify where the bandwidth is used, and how many applications use it. Armed with this information, the administrators can effectively prioritize the applications based on the business needs: for example, allow business applications but traffic shape the applications for personal use.

Web.Others	90.40%
General.Interest	3.14%
Storage.Backup	1.83%
Proxy	1.35%
P2P	1.14%
Collaboration	1.01%
Social.Media	0.53%
Network.Service	0.52%
Cloud.IT	0.03%
Video/Audio	0.03%
Others	0.03%

Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.12.16.2	Principais aplicações por utilização de largura de banda de entrada e saída;
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado
Configuração do Teste	Selecionar no modulo de "Fortiview" a extração de um relatório correspondente a controle de banda conforme solicitado e extrair um PDF
Procedimento do Teste	Gerar o relatório de utilização de aplicação por consumo de banda de saída e entrada:



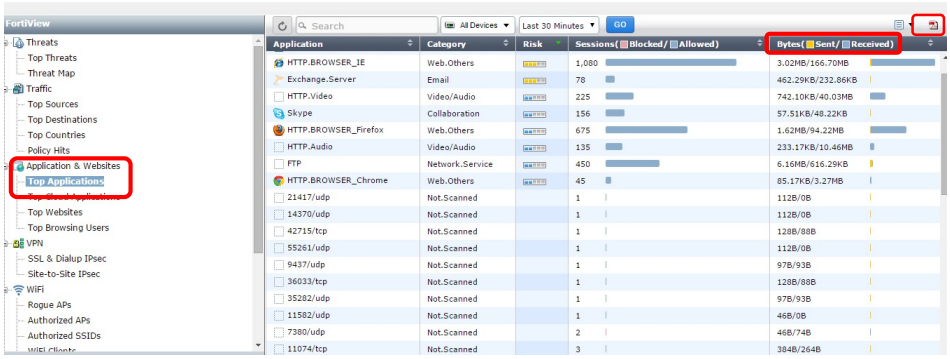
Resultado do relatório extraído do Fortiview:

Top Application

Application	Category	Risk	Sessions(Blocked/Allowed)	Bytes(Sent/Received)
BitTorrent	P2P		78	21.18KB/22.17KB
RDP	Remote.Access		78	2.94MB/6.32MB
HTTP.BROWSER_IE	Web.Others		1,080	3.02MB/166.70MB
Exchange.Server	Email		78	462.29KB/232.86KB
HTTP.Video	Video/Audio		225	742.10KB/40.03MB
Skype	Collaboration		156	57.51KB/48.22KB
HTTP.BROWSER_Firefox	Web.Others		675	1.62MB/94.22MB
HTTP.Audio	Video/Audio		135	233.17KB/10.46MB
FTP	Network.Service		450	6.16MB/616.29KB
HTTP.BROWSER_Chrome	Web.Others		45	85.17KB/3.27MB
21417/udp	Not.Scanned		1	112B/0B
14370/udp	Not.Scanned		1	112B/0B
42715/tcp	Not.Scanned		1	128B/88B
55261/udp	Not.Scanned		1	112B/0B
9437/udp	Not.Scanned		1	97B/93B
36033/tcp	Not.Scanned		1	128B/88B
35282/udp	Not.Scanned		1	97B/93B
11582/udp	Not.Scanned		1	46B/0B
7380/udp	Not.Scanned		2	46B/74B
11074/tcp	Not.Scanned		3	384B/264B
3958/tcp	Not.Scanned		1	128B/88B
32709/udp	Not.Scanned		1	112B/0B
36513/tcp	Not.Scanned		5	240B/200B
14359/udp	Not.Scanned		1	112B/0B
31201/udp	Not.Scanned		1	112B/0B
14736/tcp	Not.Scanned		1	128B/88B
53571/tcp	Not.Scanned		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:



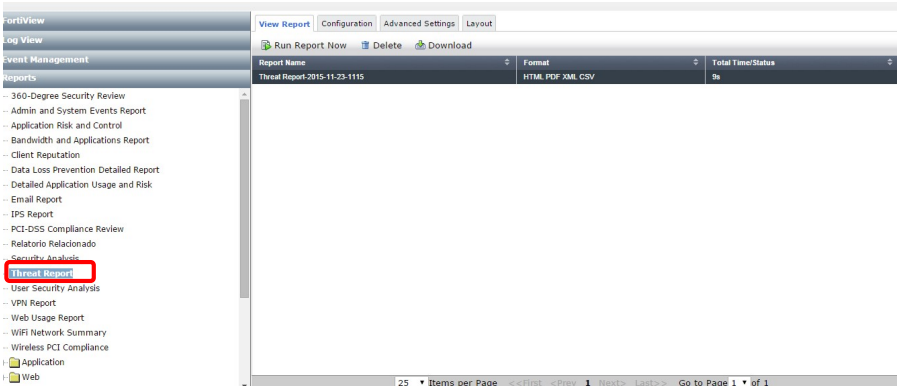
Resultado do relatório extraído do Fortiview:

Top Application

Application	Category	Risk	Sessions(Blocked/Allowed)	Bytes(Sent/Received)
BitTorrent	P2P		78	21.18KB/22.17KB
RDP	Remote.Access		78	2.94MB/6.32MB
HTTP.BROWSER_IE	Web.Others		1,080	3.02MB/166.70MB
Exchange.Server	Email		78	462.29KB/232.86KB
HTTP.Video	Video/Audio		225	742.10KB/40.03MB
Skype	Collaboration		156	57.51KB/48.22KB
HTTP.BROWSER_Firefox	Web.Others		675	1.62MB/94.22MB
HTTP.Audio	Video/Audio		135	233.17KB/10.46MB
FTP	Network.Service		450	6.16MB/616.29KB
HTTP.BROWSER_Chrome	Web.Others		45	85.17KB/3.27MB
21417/udp	Not.Scanned		1	112B/0B
14370/udp	Not.Scanned		1	112B/0B
42715/tcp	Not.Scanned		1	128B/88B
55261/udp	Not.Scanned		1	112B/0B
9437/udp	Not.Scanned		1	97B/93B
36033/tcp	Not.Scanned		1	128B/88B
35282/udp	Not.Scanned		1	97B/93B
11582/udp	Not.Scanned		1	46B/0B
7380/udp	Not.Scanned		2	46B/74B
11074/tcp	Not.Scanned		3	384B/264B
3958/tcp	Not.Scanned		1	128B/88B
32709/udp	Not.Scanned		1	112B/0B
36513/tcp	Not.Scanned		5	240B/200B
14359/udp	Not.Scanned		1	112B/0B
31201/udp	Not.Scanned		1	112B/0B
14736/tcp	Not.Scanned		1	128B/88B
53571/tcp	Not.Scanned		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:



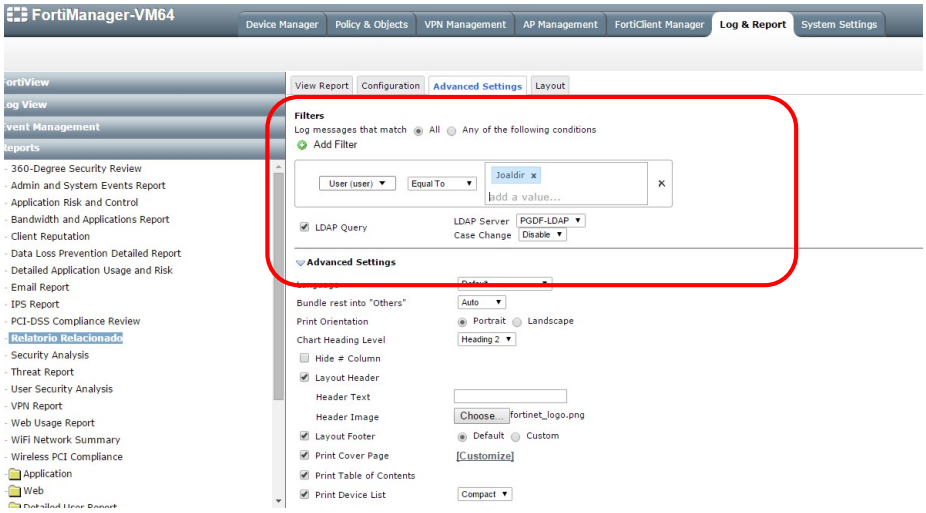
Resultado extraído do relatório:

Malware Victims

#	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 especifico 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

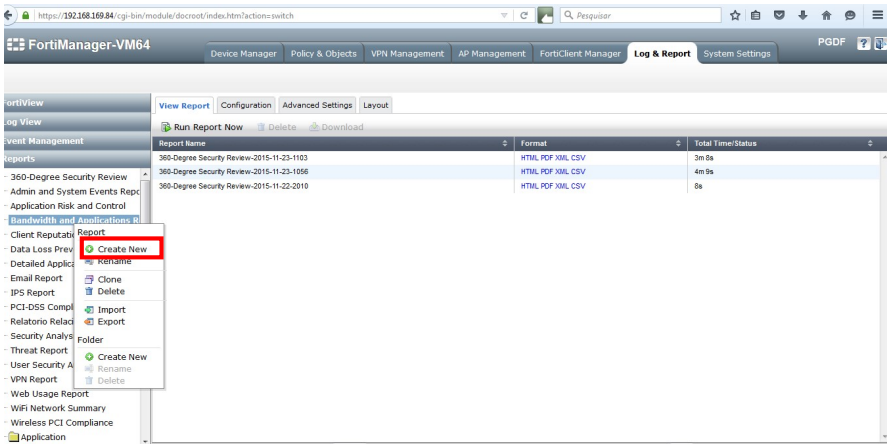
Report Filters(Logic: All)

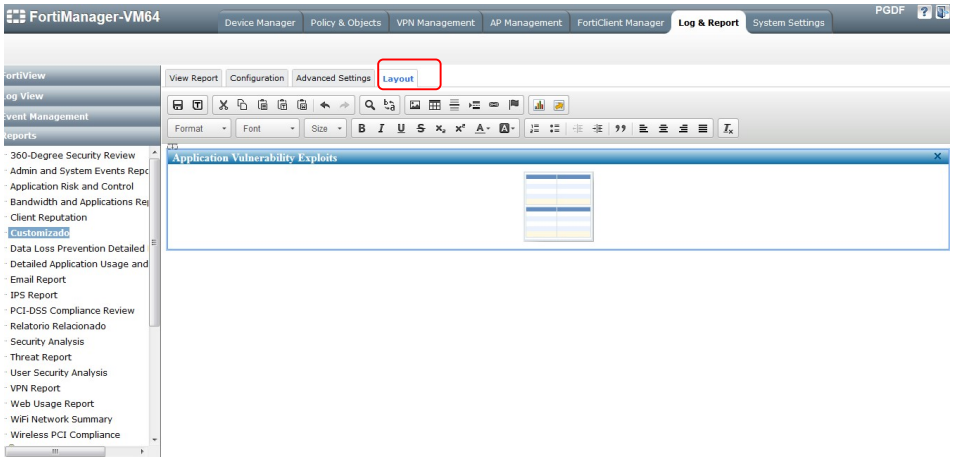
#	Filter name	Value
1	User	include (joaldir)

#	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	hp.imguol.com.br	Content Servers	843.70 KB
7	www.uol.com.br	Search Engines and Portals	792.93 KB
8	tpc.googlesyndication.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.imguol.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.googlesyndication.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	imguol.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	akhtm.nspmotion.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-channel.google.com	Search Engines and Portals	94.17 KB

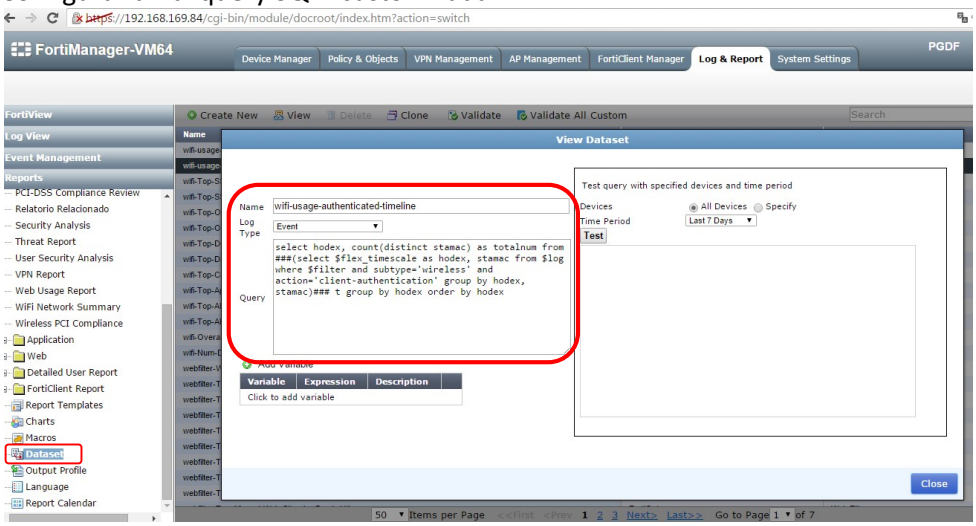
#	Risk	Application Name	Category	Technology	User	Bandwidth	Session
1	2	HTTP.BROWSER_Firefox	Web.Client	Browser-Based	1	9.89 MB	404
2	3	HTTPS.BROWSER	Web.Client	Network-Protocol	1	263.60 KB	59
3	2	Google.Search_Safe.Off	General.Interest	Browser-Based	1	255.87 KB	2
4	3	Dropbox	Storage.Backup	Browser-Based	1	214.03 KB	3
5	3	HTTP.BROWSER_IE	Web.Client	Browser-Based	1	179.72 KB	79
6	5	Ultrasurf_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 relaório:  Editando um novo layout:

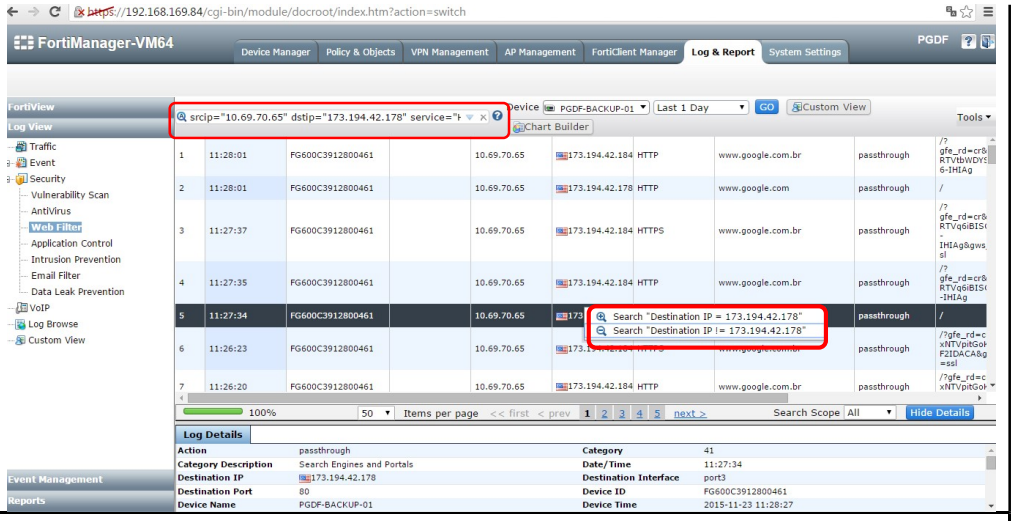


Configurar uma query SQL customizada :



Comentário	
Assinatura do Cliente	**Assinatura NCT**

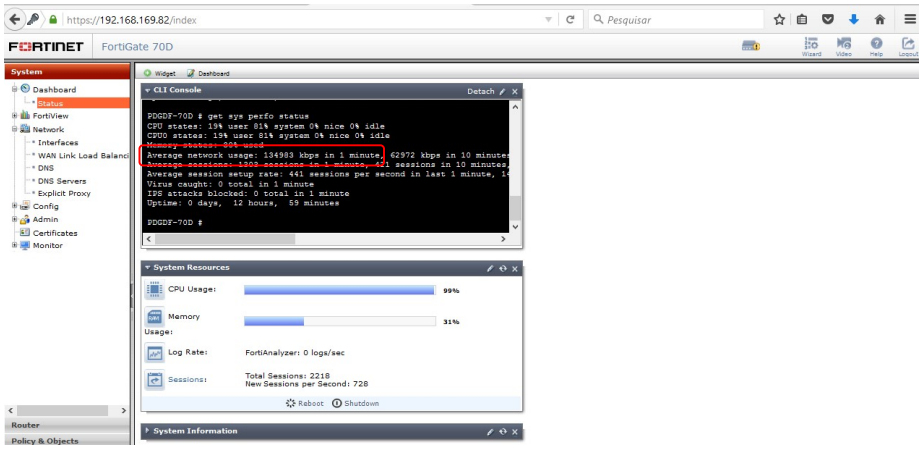
Item de Teste - 1.6.12.17	Em cada critério de pesquisa do log, deve ser possível incluir múltiplas entradas (por exemplo, 10 redes e IPs distintos, serviços HTTP, HTTPS e SMTP), exceto no campo horário, onde deve ser possível definir um faixa de tempo como critério de pesquisa;
Objetivo do Teste	Demonstrar 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"



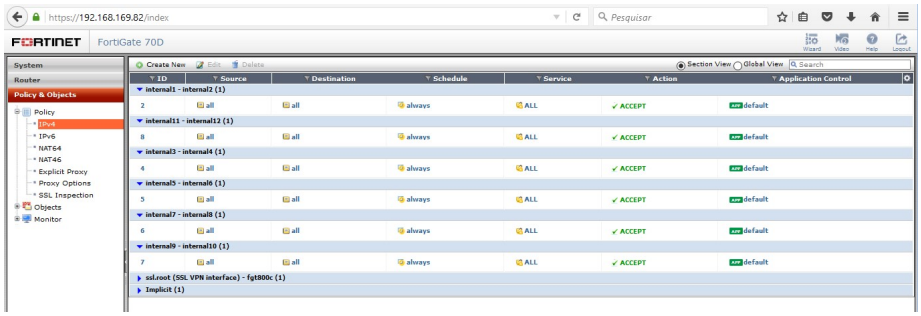
Evidências	
Comentário	
Assinatura do Cliente	**Assinatura NCT**

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

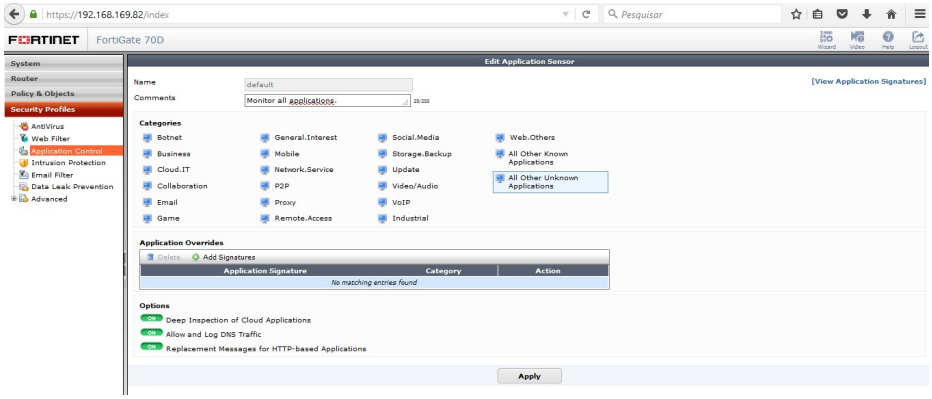
Item de Teste - 1.7.1.1	Throughput mínimo de 100 Mbps com a funcionalidade de controle de aplicação habilitada para todas as assinaturas que o fabricante possuir
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado
Configuração do Teste	Foi configurado sensor de APP control as configurações 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.

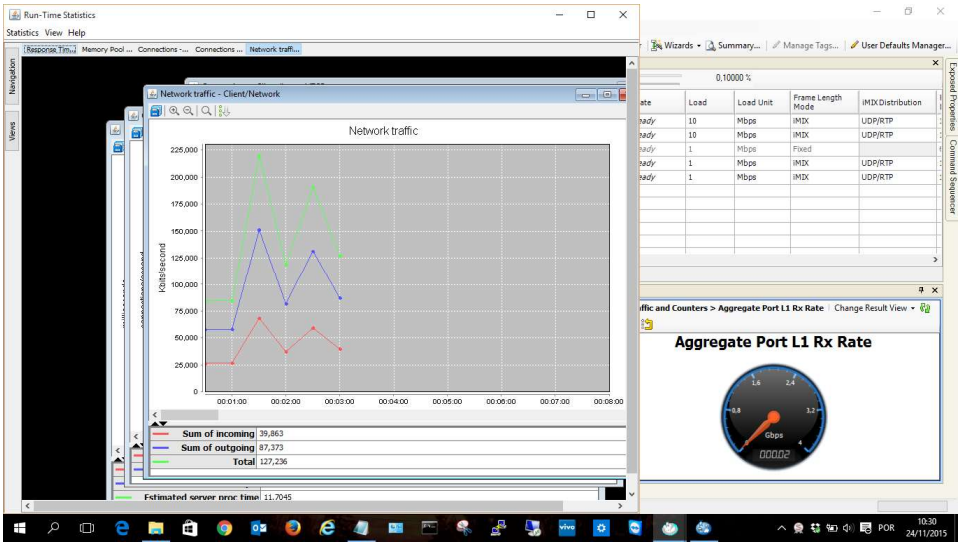


Regra de firewall

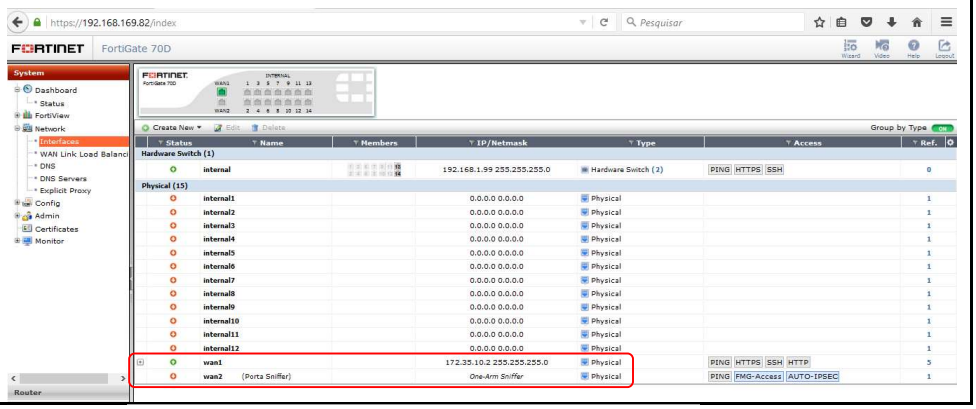


Sensor de APPControl configurado

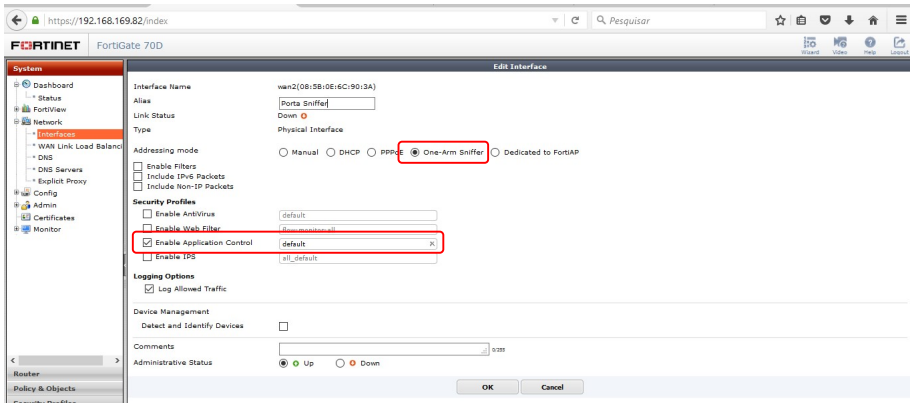
- Spirent

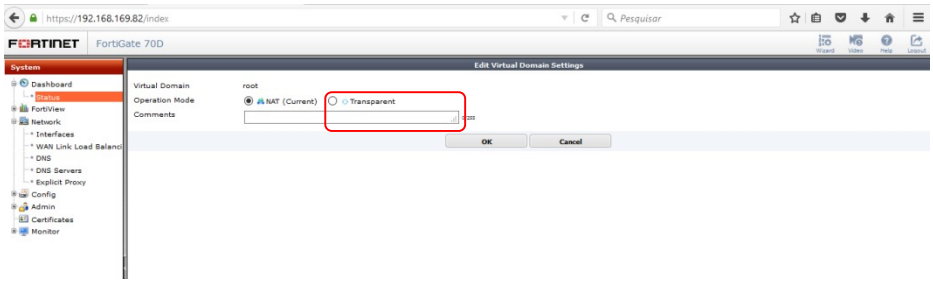


Comentário	Todas as configurações tanto do FGT 70D como do Spirent foram apresentadas/explicadas a todos os presentes na sala de homologação. Maiores detalhes sobre o relatório de trafego gerado pelo spirent, podem ser encontrados no CD anexo a este caderno.
Assinatura do Cliente	**Assinatura NCT**

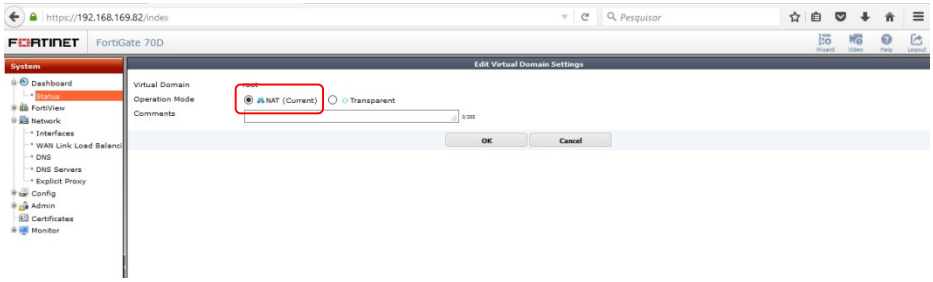
Item de Teste - 1.7.2.17	Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea mediante o uso de suas interfaces físicas nos seguintes modos: modo sniffer(monitoramento e análise do tráfego), camada 2 (L2) e camada 3 (L3);
Objetivo do Teste	Demonstrar funcionalidade de modo 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	

Comentário			
Assinatura do Cliente		**Assinatura NCT**	

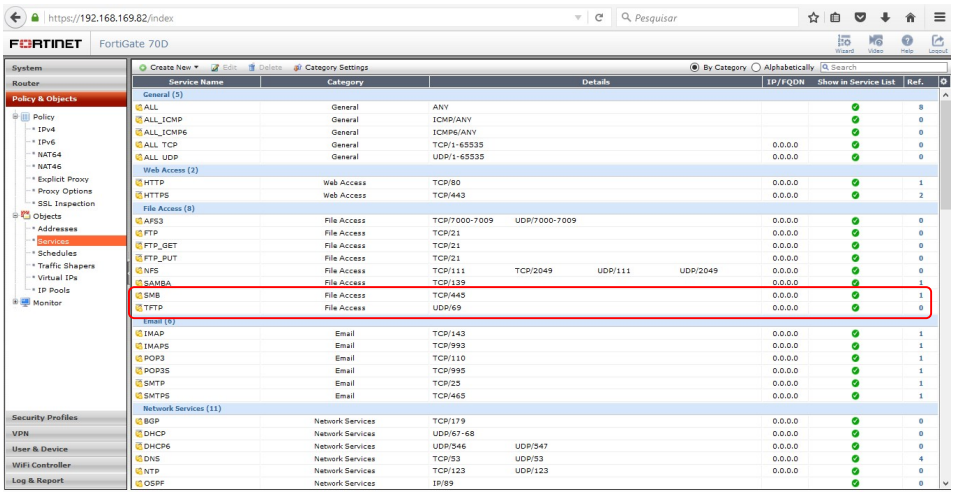
Item de Teste - 1.7.2.18	Modo sniffer, para inspeção via porta espelhada;		
Objetivo do Teste	Demonstrar funcionalidade de modo sniffer		
Configuração do Teste	Demonstrar modo one-arm-sniffer		
Procedimento do Teste	System -> network -> interfaces		
Evidências			
Comentário			
Assinatura do Cliente	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

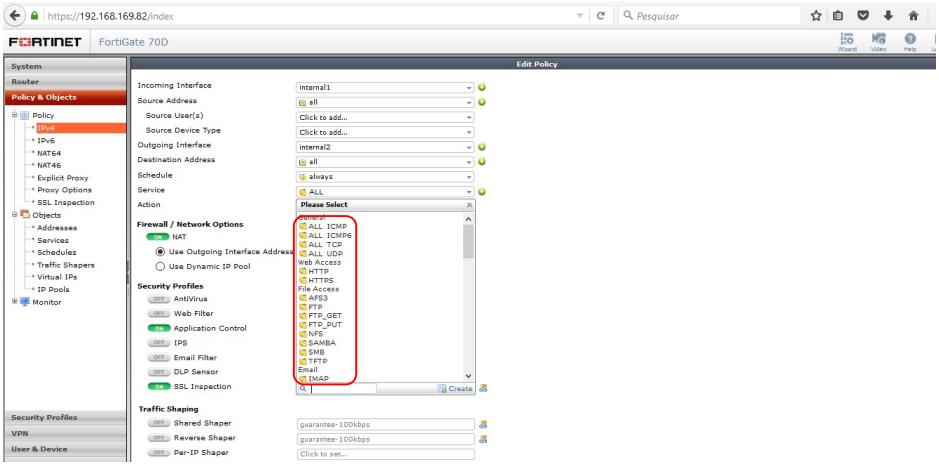
Item de Teste - 1.7.2.19	Modo L2, para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
Objetivo do Teste	Demonstrar funcionalidade de L2 do equipamento
Configuração do Teste	Demonstrar modo transparent
Procedimento do Teste	Status -> operation mode
Evidências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

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**	

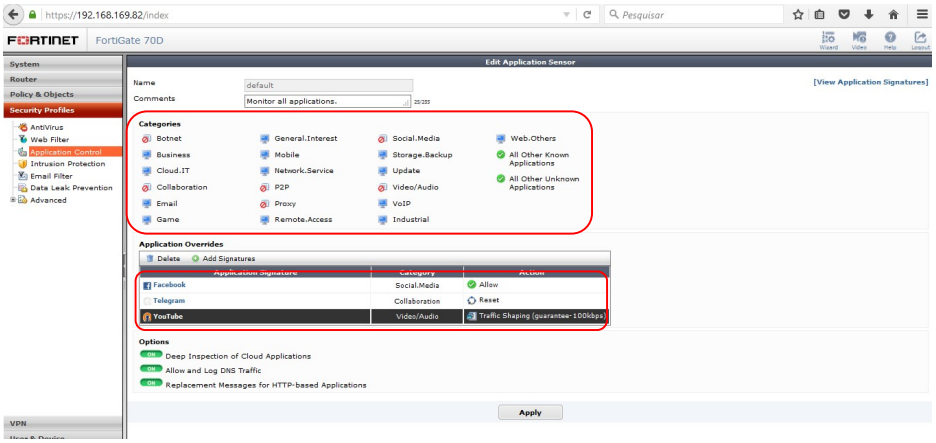
Item de Teste - 1.7.3.1	Controles de políticas por porta e protocolo;
Objetivo do Teste	Demonstrar possibilidade de administração de portas e protocolos
Configuração do Teste	Demonstrar formas de administração do firewall
Procedimento do Teste	Firewall objects, address, service, policy
Evidências	

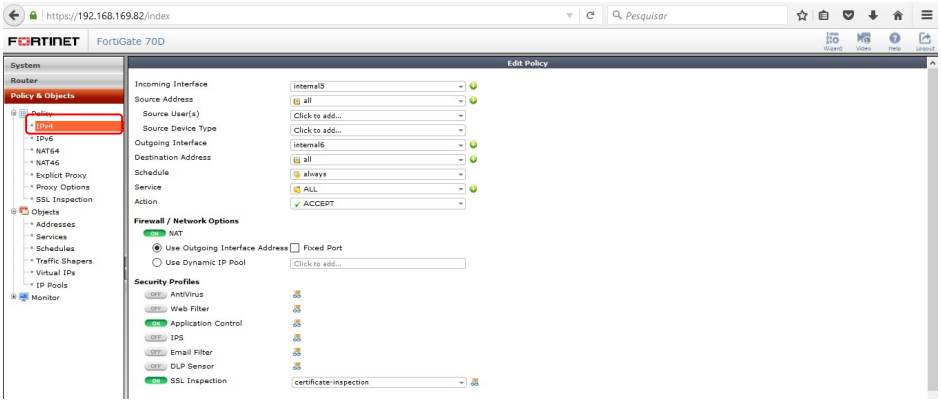


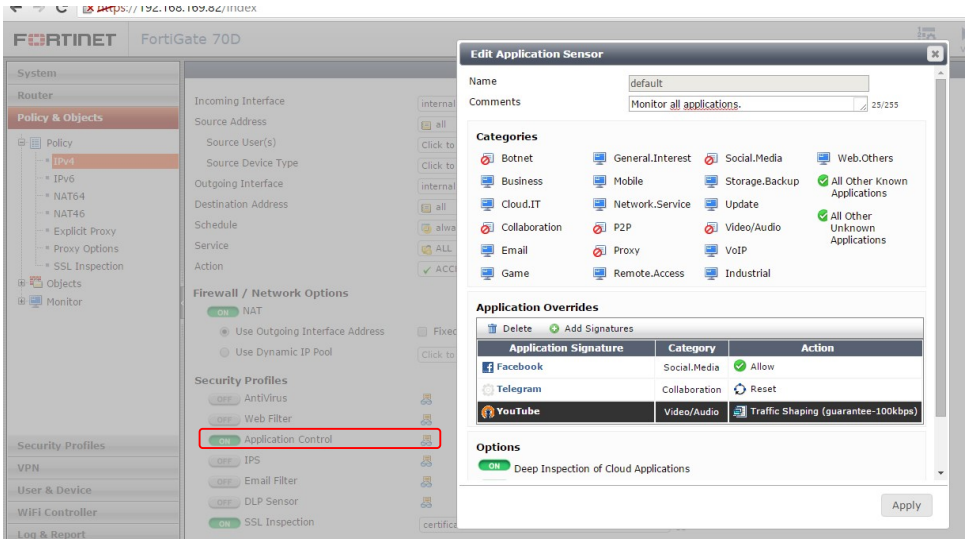


Comentário			
Assinatura do Cliente		**Assinatura NCT**	

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	

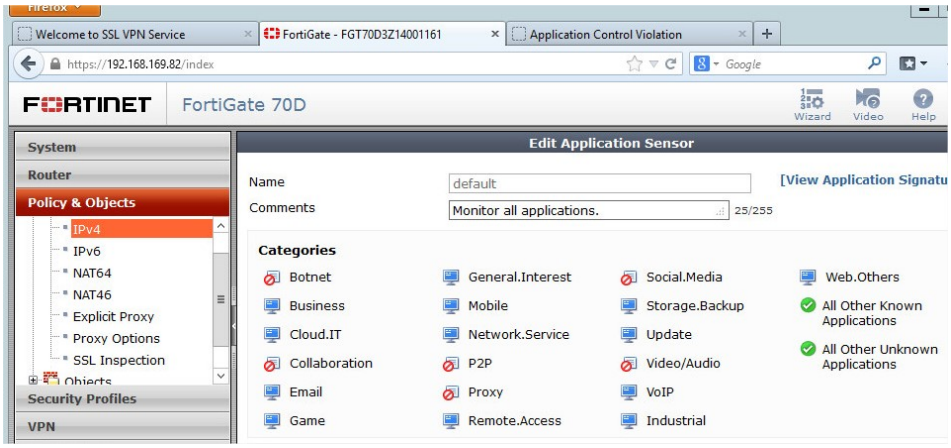
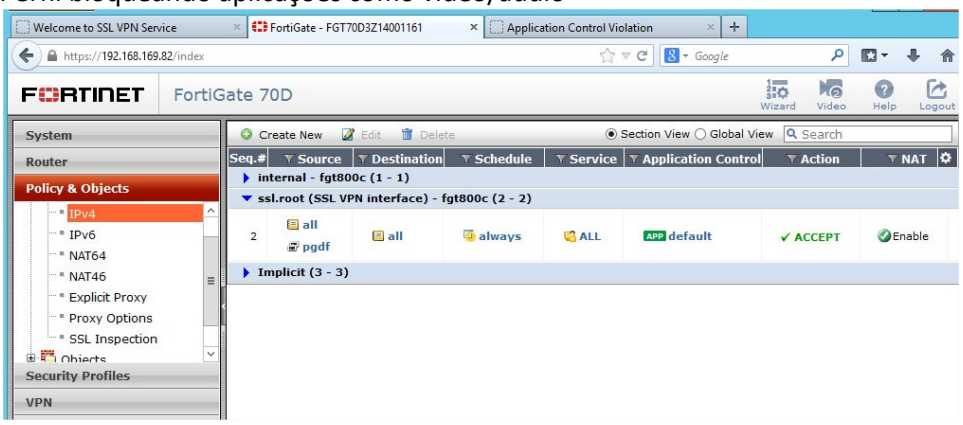


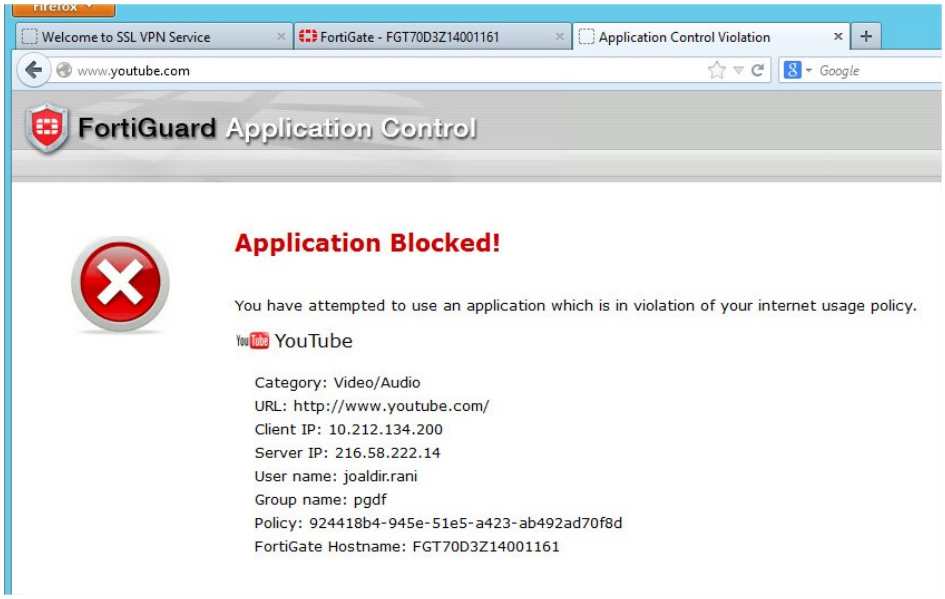




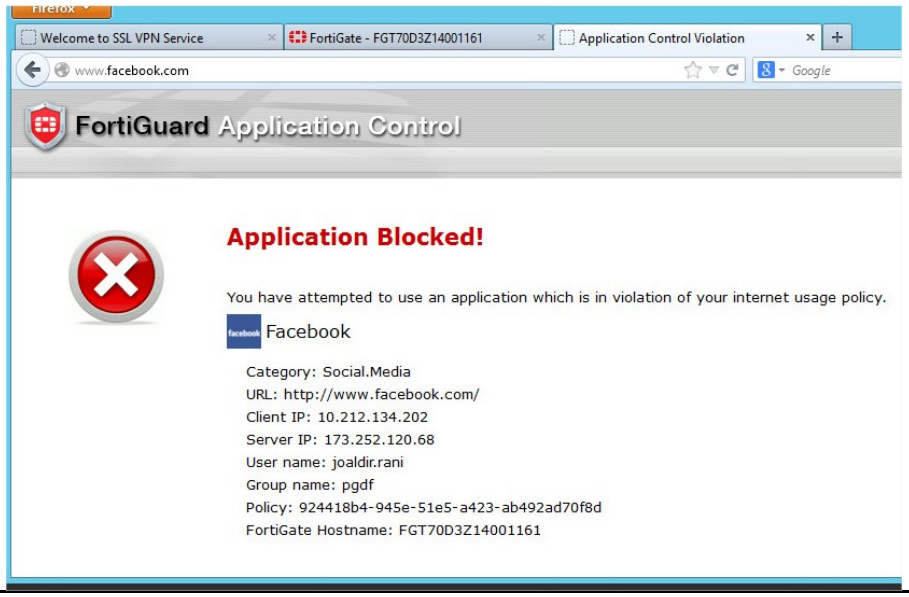
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

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;

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.

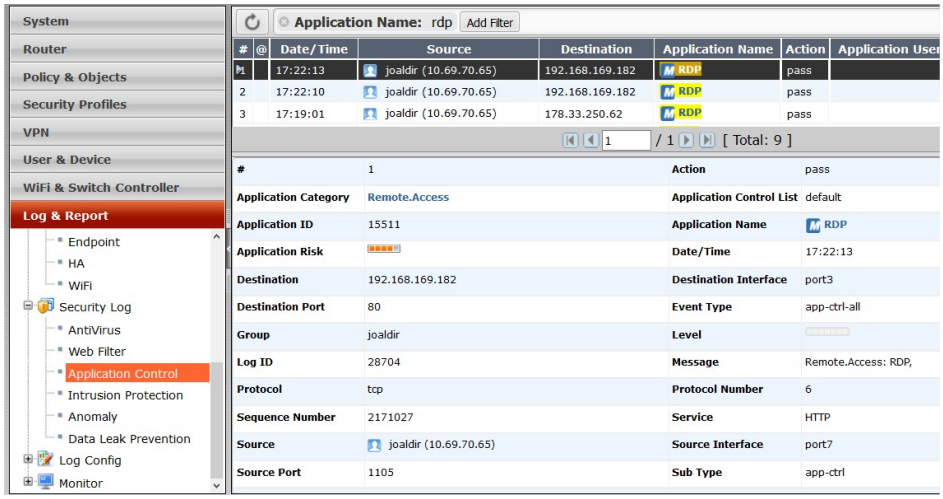
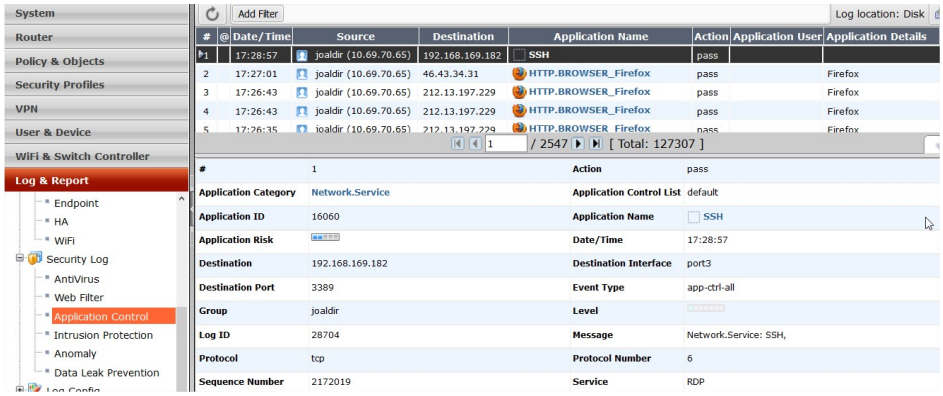
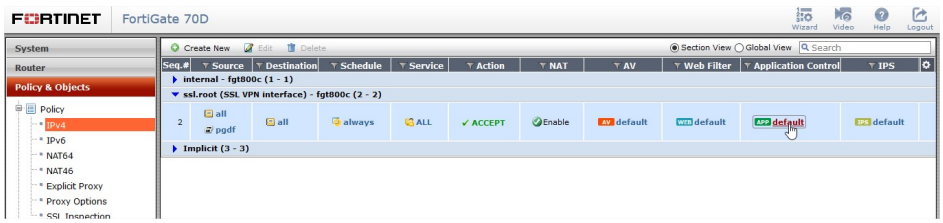


Tela demonstra o bloqueio pela aplicação e não pela web.

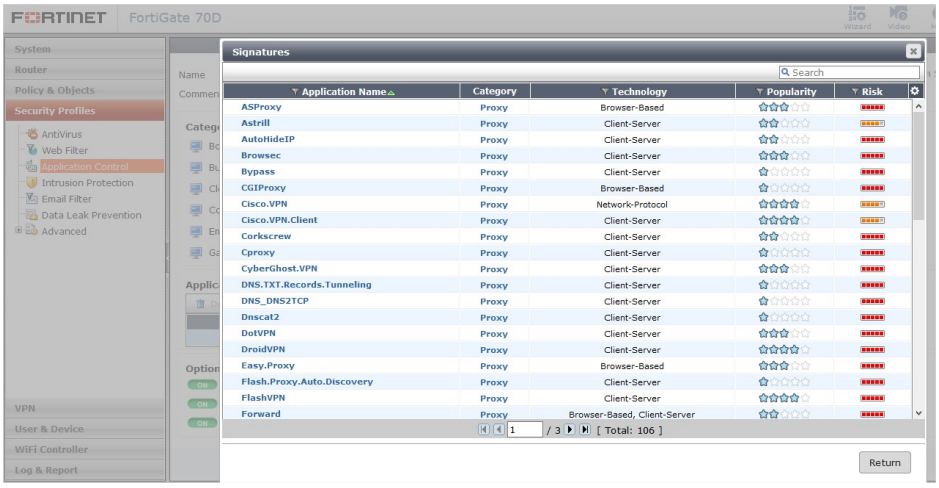


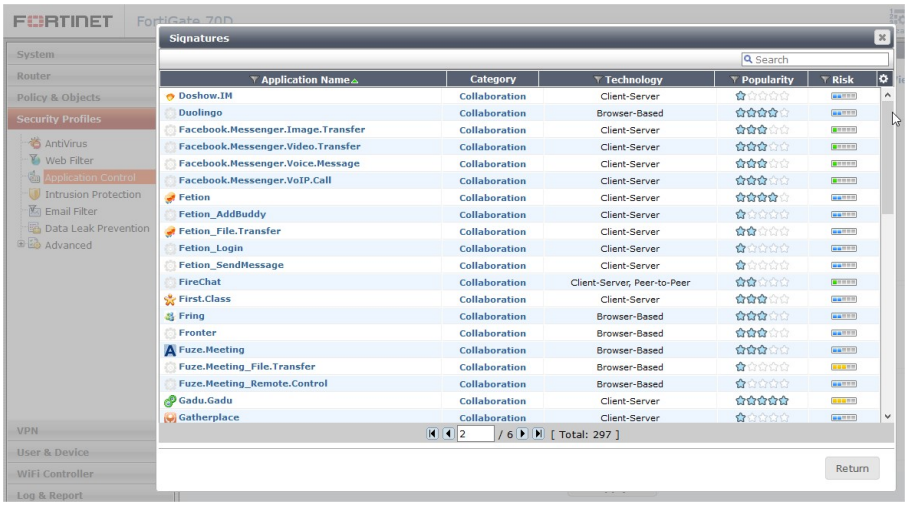
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

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

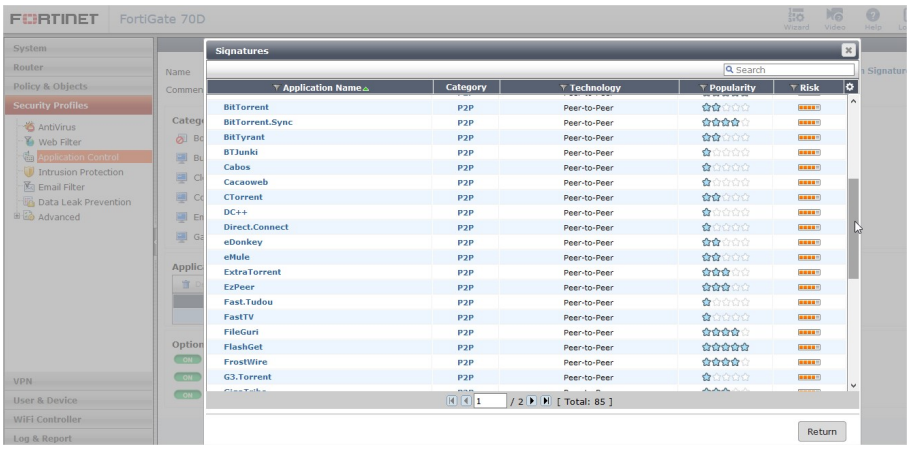
Configuração do Teste	Configurado o perfil de controle de aplicação default. Configurado uma regra de firewall com o perfil de controle de aplicação default.
Procedimento do Teste	De um cliente remote desktop tentou conexão 192.168.169.182:80 para a aplicação passar pela porta 80. De um cliente ssh(putty) colocou o ip 192.168.169.182:3389 para passar a aplicação na porta do remote desktop.
Evidências	 Detecção do Remote Desktop na porta 80  Detecção de SSH sobre a porta 3389.  Regra de firewall
Comentário	
Assinatura do Cliente	**Assinatura NCT**

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**	

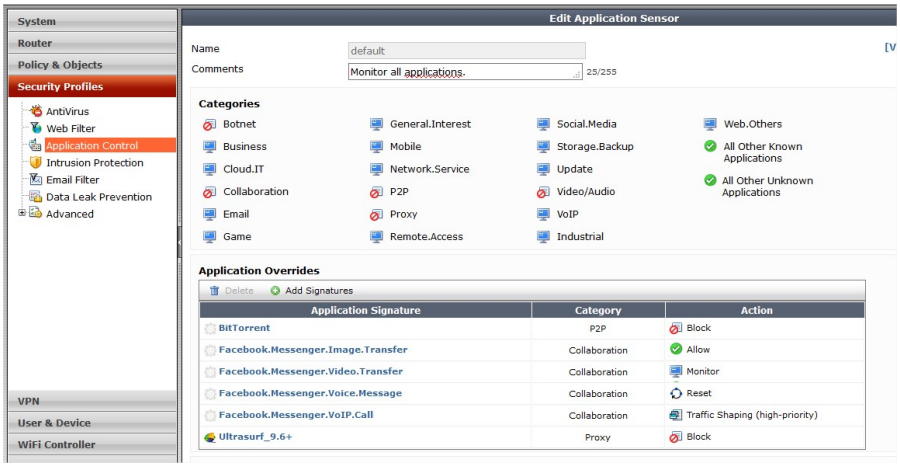
Item de Teste - 1.7.4.1.19	Deve possibilitar a diferenciação de aplicações proxies (ghostsurf, freegate, dentre outros), Instant Messaging (AIM, Gtalk, Facebook Chat, dentre outros), peer-to-peer (Bittorrent, emule, neonet, dentre outros) permitindo um controle granular na configuração de políticas;
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



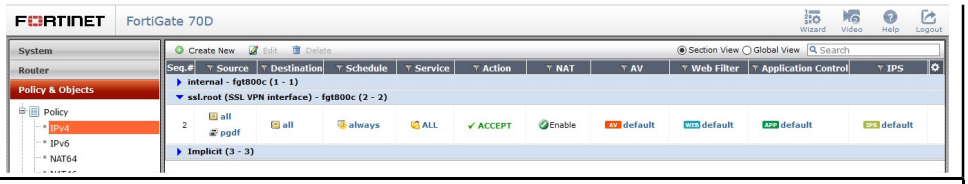
Collaboration (Instant Messenger)

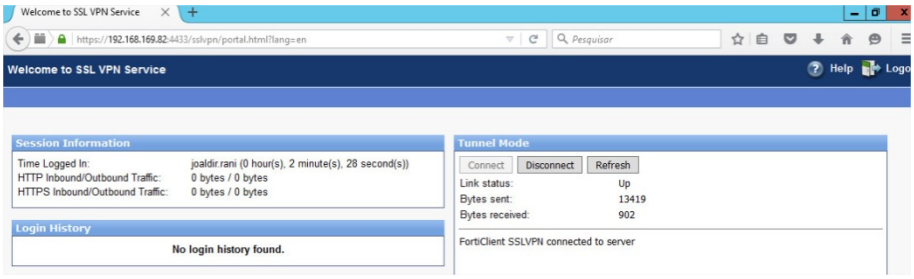


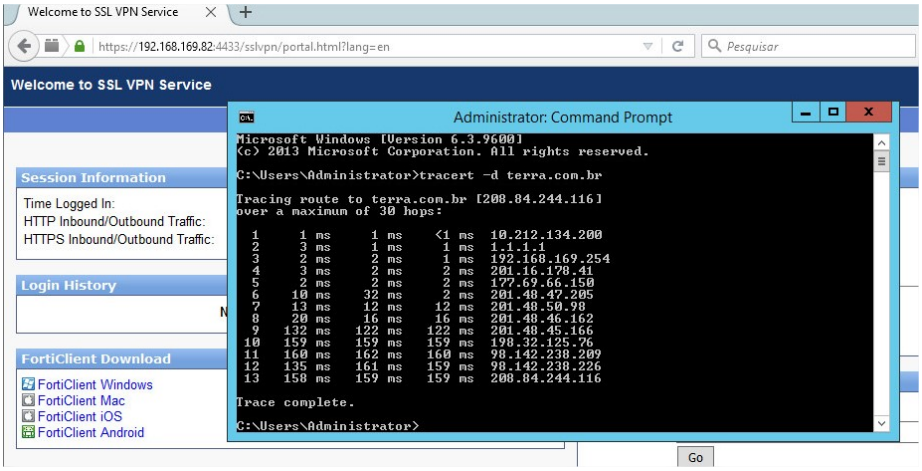
Pee-to-Peer



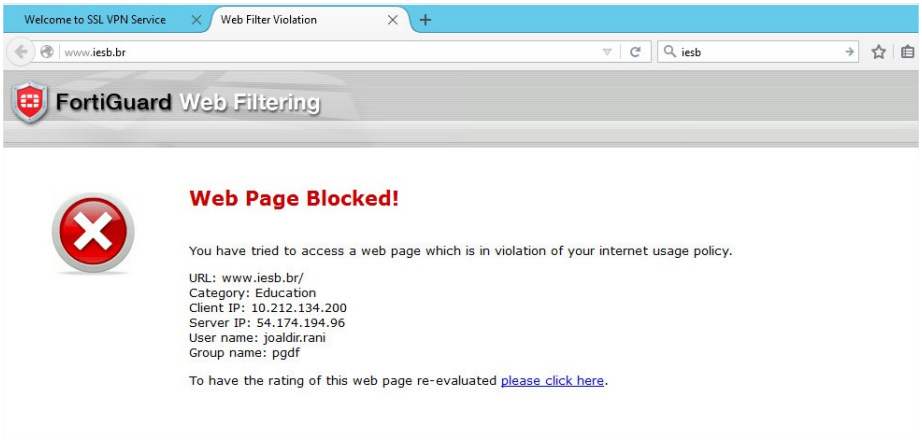
Perfil de controle de aplicação

			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

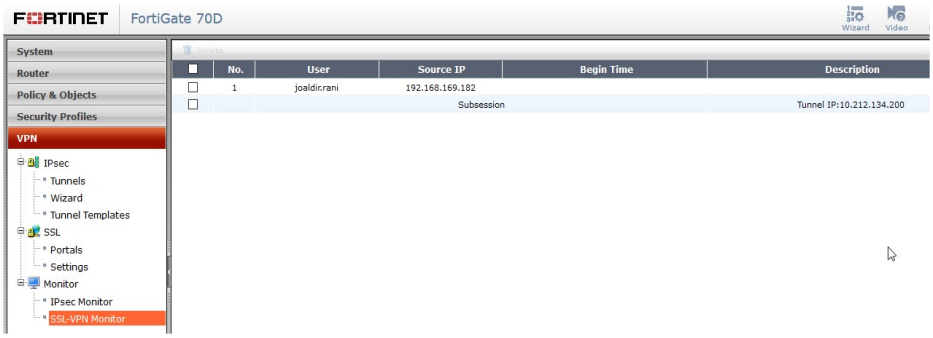
Item de Teste - 1.7.5.6.6	Dever permitir criar políticas de controle de aplicações, IPS, antivírus, anti-spyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
Objetivo do Teste	Demonstrar regras de segurança
Configuração do Teste	Configurado um perfil de controle de aplicação, filtro de conteúdo, antivirus (função de spware encorporada) 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



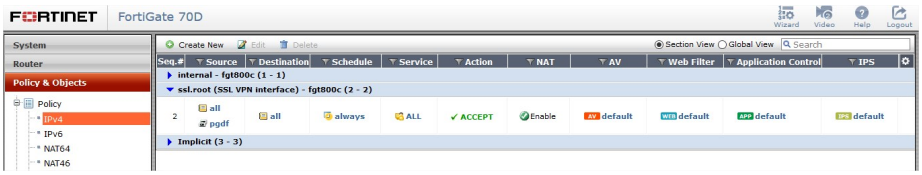
Tracert



Pagina de bloqueio



Informações do tunel



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

Comentário			
Assinatura do Cliente		**Assinatura NCT**	