Procuradoria Geral do Distrito Federal

GDF

CADERNO DE TESTES

Solução de Segurança de Rede-Firewalls Appliances

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

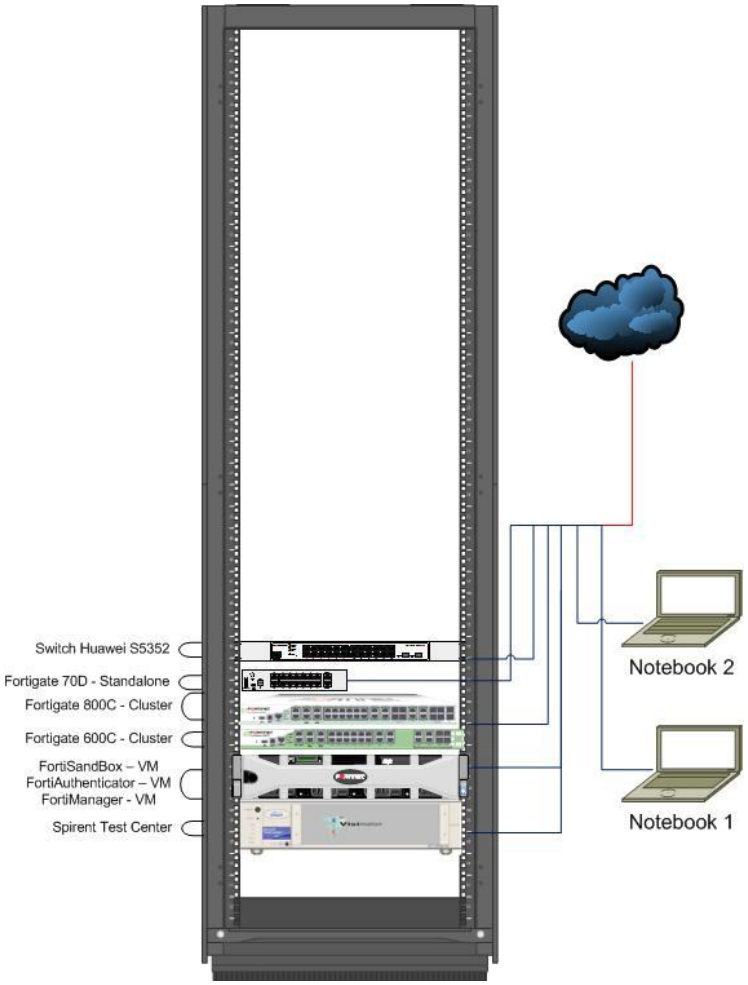
Sumário

1. OBJETIVO DO CADERNO DE TESTE

Este caderno de testes faz referencia 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 especificas aos itens pontualmente indicados no subtópico 9.1.2 e demais outros os quais o PGDF considerar relevantes para homologação dos testes.

O mesmo será realizado 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 25/11/2015.

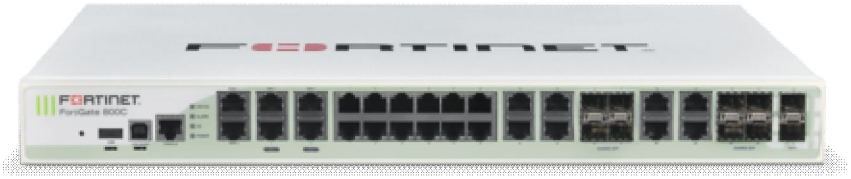
2. ESTRUTURA FÍSICA



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

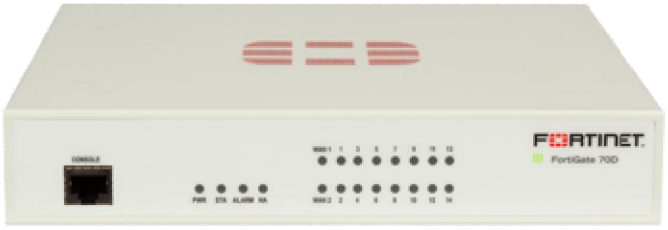


Fortigate 800C

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 600D

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 (trafego stateful	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.

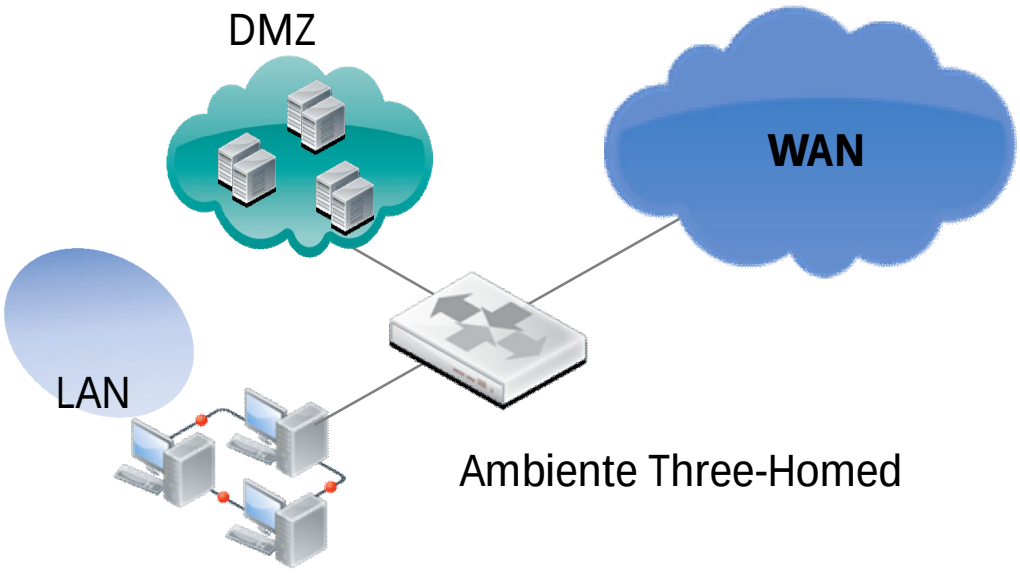
Todo o volume de tráfego mencionado tem por objetivo obter os resultados de cada equipamento NGFW firewall appliance através dos testes gerados pelos equipamentos Spirent baseados em suas respectivas na folha de dados, para cada um dos tipos de equipamentos ofertados.

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, apresentaremos 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 serão testados com todas as funcionalidades ativas, tais como: IPS, Antivírus e Anti-spyware ativados em caráter simultâneo, para se aferido a capacidade de thoughput .

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 das features solicitadas	
Configuração do Teste		Configurado profiles de IPS, APP control, Anti virus com as configurações de base default: -Sensor de IPS : Default com todas as assinaturas da Fortiguard; -Profile de AV : habilitado a monitoração de todos os protocolos ; -Profile de APP control - habilitado todas as aplicações habilitado em uma regra de firewall em caráter simultâneo todos os profiles.	
Procedimento do Teste		Gerar trafego a partir de Spirent para fazer match na regra com qual constam todos os itens de scan habilitados.	
Evidências			
Comentário			
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	Configurado profiles de IPS, APP control, Anti virus com as configurações de base default: -Sensor de IPS : Default com todas as assinaturas da Fortiguard; -Profile de AV : habilitado a monitoração de todos os protocolos ; -Profile de APP control - habilitado todas as aplicações habilitado em uma regra de firewall em caráter simultâneo todos os profiles.
Procedimento do Teste	Gerar trafego a partir de Spirent para fazer match na regra com todos os itens habilitados.
Evidências	
Comentário	
Assinatura do Cliente	**Assinatura NCT**

Item de Teste - 1.6.1.3	Os appliances ofertados deverão possuir em validade a certificação Common Criteria EAL-4 ou ICSA Labs (firewall);
Objetivo do Teste	Evidenciado na documentação oficial do Fabricante
Configuração do Teste	Vide Documentação oficial do fabricante comprovando ICSA Labs
Procedimento do Teste	Vide Documentação oficial do fabricante comprovando ICSA Labs
Evidências	Evidenciado na documentação oficial do Fabricante
Comentário	
Assinatura do Cliente	**Assinatura NCT**

Item de Teste - 1.6.1.6	Os equipamentos fornecidos deverão possuir características de Next Generation Firewall (NGFW) com as seguintes funcionalidades instaladas: filtro de pacotes, controle de aplicações, NAT, PAT, IPS, antivírus, anti-spyware, IDS, DLP (Data Loss Prevention), IPSec VPN site-to-site e cliente-to-site, filtro de URL, QoS e roteamento avançado;
Objetivo do Teste	Mostrar todas as funções solicitadas
Configuração do Teste	Criação de um objeto referente a cada uma das features solicitadas.
Procedimento do Teste	Depois de criados os objetos, demonstrar cada um destes.

Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.1.7	Fonte de alimentação 100-240VAC;		
Objetivo do Teste	Demonstrar Suporte a capacidade de alimentação conforme solicitado		
Configuração do Teste	Conforme validado no Datasheet do equipamento		
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.1.8	Cada appliance deverá possuir, no mínimo, 8 (oito) interfaces ethernet 10/100/1000 e 4 (quatro) interfaces gigabit SFP com transceiver compatível com a infraestrutura da PGDF, de tal forma que o tráfego de sincronismo entre os nós do cluster não seja exclusivo em qualquer das portas;		
Objetivo do Teste	Comprovado conforme no datasheet do equipamento		
Configuração do Teste	Conforme validado no Datasheet do equipamento		
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.1.9	Possuir 1 (uma) interface ethernet dedicada para gerenciamento e monitoramento;		
Objetivo do Teste	Comprovado conforme no datasheet do equipamento		
Configuração do Teste	Conforme validado no Datasheet do equipamento		
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.1.10		Possuir 1 (uma) interface do tipo console ou similar;	
Objetivo do Teste		Comprovado conforme no datasheet do equipamento	
Configuração do Teste		Conforme validado no Datasheet do equipamento	
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.1.11		Suporte a, no mínimo, 10 (dez) roteadores virtuais;	
Objetivo do Teste		Demonstrar funcionalidade solicitada	
Configuração do Teste		Habilitado o modulo de VDOM	
Procedimento do Teste		Criado 10 instâncias de virtualização via interface gráfica	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.1.12		Deve permitir 1.000 (um mil) clientes VPN SSL simultâneos sem a necessidade de licenças adicionais;	
Objetivo do Teste		Demonstrar funcionalidade solicitada	
Configuração do Teste		Criar usuários	
Procedimento do Teste		Autenticação de usuários na VPN	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

1.7- 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	
Objetivo do Teste		Demonstrar funcionalidade conforme solicitado	
Configuração do Teste		Configurar equipamento Spirent para geração de para simulação de trafego para o equipamento Fortigate	
Procedimento do Teste		Validar nos monitores de Throughput da interface o alcance dos índices solicitados .	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.1.2		Os appliances ofertados deverão possuir em validade a certificação Common Criteria EAL-4 ou ICSA Labs (firewall);	
Objetivo do Teste		Conforme demonstrado na documentação oficial fabricante	
Configuração do Teste			
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.1.6		4 (quatro) interfaces de rede 10/100/1000 base-tx;	
Objetivo do Teste		Demonstrar especificação conforme solicitado	
Configuração do Teste		Conforme apresentado no equipamento	
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.1.7		Deve possuir uma interface de rede dedicada para gerenciamento;	
Objetivo do Teste		Demonstrar especificação conforme solicitado	
Configuração do Teste		Conforme apresentado no equipamento	
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.1.8		Deve possuir uma interface do tipo console ou similar;	
Objetivo do Teste		Demonstrar especificação conforme solicitado	
Configuração do Teste		Conforme apresentado no equipamento	
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.1.9	Estar licenciada para suportar sem o uso de licença 25 (vinte e cinco) túneis de VPN IPSec simultâneos;
Objetivo do Teste	Não se aplica
Configuração do Teste	
Procedimento do Teste	

Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

9. ITENS DE FUNCIONALIDADES

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

Item de Teste - 1.6.1.13	Por cada equipamento que compõe a plataforma de segurança, entende-se o hardware e as licenças de softwares necessárias para seu funcionamento;		
Objetivo do Teste	Conforme proposta comercial de modo como solicitado		
Configuração do Teste			
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.1.14	Por console de gerência e monitoramento, entende-se as licenças de software necessárias para as duas funcionalidades, bem como hardware dedicado ou appliances virtual para o funcionamento das mesmas;		
Objetivo do Teste	Conforme proposta comercial de modo como solicitado		
Configuração do Teste			
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.1.15	A console de gerência e monitoramento podem residir no mesmo appliance, desde que possuam recurso de CPU, memória, interface de rede e sistema operacional dedicados para esta função;
Objetivo do Teste	Demonstrar conforme solicitado
Configuração do Teste	Mostrar a interface via GUI no Dashboard

Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.1.16		Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life ou end-of-sale;	
Objetivo do Teste		Conforme proposta comercial de modo como solicitado	
Configuração do Teste			
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.1.17		As funcionalidades de proteção de rede que compõe a plataforma de segurança podem funcionar em múltiplos appliances, desde que obedeçam a todos os requisitos desta especificação;	
Objetivo do Teste		Conforme proposta comercial de modo como solicitado	
Configuração do Teste			
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.1.18		A plataforma deve fazer análise de conteúdo de aplicações em camada 7 do modelo OSI;	
Objetivo do Teste		Demonstrar funcionalidade solicitada	
Configuração do Teste		configurados os modos de APP control e Webfilter, e habilitado o Log.	
Procedimento do Teste		Validar no Log as inspecoes de Webfilter e Application control e demais conteudos de aplicações.	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.1.19		Agregação de links 802.3ad;	
Objetivo do Teste		Demonstrar funcionalidade solicitada	
Configuração do Teste		Configurar nova interface selecionando Type LACP ou Link 802.3ad;	
Procedimento do Teste		Adicionado 2 interfaces em modo de agregação	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.1.20		Permitir a definição de políticas e/ou regras de filtragem baseadas em endereços IP, range, subnets, países, portas, protocolo, aplicação, categoria de aplicações, usuários, grupos, tipos de arquivos (tais como, mas não limitado a: exe, dll, bat, cab, pif, reg) e mecanismos de QoS (traffic shaping, diffserv marking, inclusive por aplicação);	
Objetivo do Teste		Demonstrar funcionalidades solicitadas	
Configuração do Teste		Criação de regra, habilitando filtros conforme solicitados.	
Procedimento do Teste		Demonstrado regra/Política contendo cada um dos filtros mencionados no item.	
Evidências			
Comentário			
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	
Procedimento do Teste		Validar autenticação do usuário à aplicação	
Evidências			
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			
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

CONTROLE POR POLÍTICA DE FIREWALL

Item de Teste - 1.6.2.1	Suportar controle de políticas por porta e protocolo;		
Objetivo do Teste	Demonstrar funcionalidade solicitada		
Configuração do Teste	Criar uma política uma politica habilitando o controle por porta e protocolo		
Procedimento do Teste	Habilitado o count na politica		
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

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.		
Procedimento do Teste	Testado os controles de políticas conforme solicitado.		
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.2.3	Controle, inspeção e de-criptografia SSL por política para tráfego de entrada (inbound) e saída (outbound)
Objetivo do Teste	Demonstrar funcionalidade solicitada
Configuração do Teste	Configurado o modo de Deep Inspection na política de firewall.
Procedimento do Teste	Demonstrado no log do trafego inspecionado sendo ele SSL

Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.2.4	Controle de políticas por usuários, grupos de usuários, IPs e redes;
Objetivo do Teste	Demonstrar funcionalidade solicitada
Configuração do Teste	Configurado uma politica de de controle conforme solicitado
Procedimento do Teste	Demonstrado no log os modos de controle de politicas
Evidências	
Comentário	

Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.2.5	Deve de-criptografar tráfego inbound e outbound em conexões negociadas com TLS 1.2;
Objetivo do Teste	Demonstrar funcionalidade solicitada
Configuração do Teste	Configurar via CLI system global " set gui-https-tls-version " e selecionando o tlsv1-2
Procedimento do Teste	Demonstrar no log do trafego inspecionado sendo este TLS
Evidências	
Comentário	

Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.2.6	É permitido o uso de appliance externo específico para a de-criptografia SSL e TLS com espelhamento do tráfego de-criptografado tanto para o firewall, quanto para as soluções de análise;
Objetivo do Teste	Este item não se aplica visto que o appliance Fortigate efetiva a de-criptografia SSL e TLS.
Configuração do Teste	
Procedimento do Teste	
Evidências	
Comentário	

Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.2.8	QoS baseado em políticas (prioridade, garantia e máximo);
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado
Configuração do Teste	Configurar profile de Traffic Shape
Procedimento do Teste	Mostrar grafico de traffic Shape

Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.2.9		QoS baseado em políticas utilizando marcação de pacotes (diffserv marking), inclusive por aplicações;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar profile de traffic shape habilitando o modulo de marcação de pacote, na politica e por aplicação.	
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.2.10		Suportar objetos e regras IPv6;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar a criação de um objeto IPV6	
Procedimento do Teste		Mostrar um objeto	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.2.11		Suportar objetos e regras multicast;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar uma regra de multicast	
Procedimento do Teste		Validar no log e count da politica	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.2.12		Suportar o agendamento das políticas com o objetivo de habilitar e desabilitá-las em horários pré-definidos;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar perfil de Schedule	
Procedimento do Teste		Validar que nas datas estipuladas e nos períodos marcados a regra deixa de funcionar.	
Evidências			
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		Configurar profile de APP control especificando as aplicações as quais devem serem bloqueadas ou liberadas	
Procedimento do Teste		Habilitar profile de APP em uma política, e validar o acesso a uma aplicação bloqueada e validar este pelo logs.	
Evidências			
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			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.3.1.3		Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Listar a relação de todas as aplicações a partir de um profile default de APP control	
Procedimento do Teste			
Evidências			
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		Via interface grafica Configurar profiles de DLP e APP control com opção de salvar o pacote	
Procedimento do Teste		Validado o Log do match de trafego de DLP e APP control relaciondo as ações habilitadas nos profiles	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.3.1.5		Deve aplicar heurística a fim de detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a: bittorrent criptografado e aplicações VOIP que utilizam criptografia proprietária;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar o profile de APP control habilitando as categorias das aplicações solicitadas sem habilitar Traffic shape	
Procedimento do Teste		Verificar no Log o match no trafego das aplicaçõesk	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.3.1.6		Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e ataques mediante a porta 443.	
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.	
Procedimento do Teste		Efetivar o acesso a uma das aplicacocoes tais como solicitado e verificar no Log o match no trafego das aplicações	
Evidências			
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.		
Procedimento do Teste	Executar um acesso seguro SSL e verificar no Log o match no trafego das aplicações		
Evidências			
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		
Procedimento do Teste	Efetivar um acesso correspondente a aplicação conforme mencionado verificar no Log o match no trafego das aplicações		
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.3.1.9	Identificar o uso de táticas evasivas via comunicações criptografadas;		
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado		
Configuração do Teste	Configurar uma política com o SSL inspection a partir da interface gráfica.		
Procedimento do Teste	Mostrar nos logs match de trafego de conexões criptografadas		
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.3.1.10		Atualizar a base de assinaturas de aplicações automaticamente;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurado em Fortiguard schedule para efetivar o upgrade automático.	
Procedimento do Teste		Mostrar tela do dashboard de informações de licenças e também no menu de Fortiguard status.	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.3.1.11		Reconhecer aplicações em IPv6;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurado feature settings habilitando o serviço de IPV6, para reconhecer aplicações em IPV6.	
Procedimento do Teste		Executar teste de comunicação IPV6 e mostrar no log uma aplicação detectada com endereço em IPV6	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.3.1.12		Limitar a banda (download / upload) usada por aplicações utilizando QoS baseado no IP de origem, usuários e grupos do LDAP / AD;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar profile de APP control, habilitando ação de traffic shape para as aplicações selecionadas, habilitando-os as políticas correspondente aos controles acima citados.	
Procedimento do Teste		Mostrar no log as aplicações fazendo match no profile correspondente ao traffic shape e correspondente aos filtros das regras.	
Evidências			
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	Validado o Fortigate buscando os eventos de Logon do AD, no monitor logon.

Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.3.1.14		Deve ser possível adicionar controle de aplicações através de regras de segurança do dispositivo;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar regra de firewall selecionando o tipo de device e associar o profile de APP control.	
Procedimento do Teste		Validar no Log o match no profile correspondente a política de tipo de device.	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.3.1.15		Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos e análise heurística;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar profile de APP control	
Procedimento do Teste		Validar no Log os tipos de classificação das aplicações.	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.3.1.16		Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar profile de APP control , habilitando ação de bloqueio ou Traffic shape para aplicações desconhecidas	
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.3.1.17	O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado
Configuração do Teste	No Site do Fabricante www.fortiguard.com, no menu APP control-> submeter uma nova aplicação.
Procedimento do Teste	

Evidências			
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" se for o caso de alterar o Default		
Procedimento do Teste	Validar a mensagem de bloqueio por um usuário que fez match em uma aplicação bloqueada e homologar a replecement messages.		
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.3.1.19	Deve possibilitar que o controle de portas seja aplicado para todas as 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			
Evidências			
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.		
Procedimento do Teste	Validar na analise de Logs, as aplicação com ações diferente baseado em cada categoria.		
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.3.1.21	Deve possibilitar a diferenciação e controle de partes das aplicações como, por exemplo, permitir o Gtalk Chat e bloquear seu recurso de transferência de arquivos;

Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar profile de APP control selecionando as aplicações Gtalk transferência de arquivo para aplicar ação de bloqueio.	
Procedimento do Teste		Validar o log o o bloqueio desta aplicação fazendo o match o profile criado.	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.3.1.22		Deve ser possível a criação de grupos estáticos e dinâmicos de aplicações baseados em características das aplicações, tais como:	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar profile de APP control conforme os itens subseqüentes	
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.3.1.22.21		Tecnologia utilizada nas aplicações (cliente-servidor, baseado em navegador, protocolo de rede e etc.);	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar lista de aplicação baseados nos perfis solicitados acima.	
Procedimento do Teste		Validar apos a criação do profile a lista de grupos pelas categorias solicitados.	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.3.1.22.2		Nível de risco da aplicação;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar lista de aplicação baseados nos perfis de risco/severidade	
Procedimento do Teste		Validar apos a criação do profile a lista de grupos pelas categorias solicitados.	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.3.1.22.3	Categoria e subcategoria de aplicações;
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado

Configuração do Teste		Configurar lista de aplicação baseados nos perfis de Categoria e subcategoria de aplicações.	
Procedimento do Teste		Validar apos a criação do profile a lista de grupos pelas categorias solicitados	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.3.1.22.4		Aplicações que usem técnicas evasivas utilizadas por malwares, tais como: transferência de arquivos e/ou uso excessivo de banda;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar lista de aplicação baseados nos perfis solicitados	
Procedimento do Teste		Validar apos a criação do profile a lista de grupos dos tipos de perfis solicitados.	
Evidências			
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		Configurar security profiles de IPS e antivirus a partir da interface gráfica.	
Procedimento do Teste		Mostrar os módulos de security profile que representa todos os módulos de scan acima mencionados.	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.4.2		Deve incluir assinaturas de prevenção de IPS e bloqueio de arquivos maliciosos (antivírus e anti spyware);	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar profiles de IPS e Anti-Virus	
Procedimento do Teste		Gerar trafego correspondente a um padrão malicioso e validar a os profiles criados a partir da aba de configuração security policy	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.4.3	As funcionalidades de IPS, antivírus e anti-spyware 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;		
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado		
Configuração do Teste	Desativar a comunicação com a FDN , para que o equipamento nao mais fiquei ativo para a internet. Ou mesmo desaticar o mesmo a internet.		
Procedimento do Teste	Apresentar logs de match de classificação dos filtros e Scans de IPS e Antivírus sendo feita mesmo apos o Fortigate não esta conectado a FDN.		
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.4.4	Deve sincronizar as assinaturas de IPS, antivírus, anti spyware quando implementado em alta disponibilidade ativo/ativo ou ativo/passivo ou ativo/Passivo		
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado		
Configuração do Teste	Acessar via CLI o equipamento Slave e executar o comanado " execute ha manager 0", e em seguida listar o status da eng e a lista de atualização fazendo uma comparação com a do equipamento Master.		
Procedimento do Teste	Validar o output correspondente ao status em ambos os devices validando que as bases estão similares.		
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.4.5	Quando utilizada as funções de IPS, antivírus e anti spyware, o appliance 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	Configurado Profiles de capacidade menina e de capacidade máxima correspondente a cada função mencionada
Procedimento do Teste	Configurado no Spirent gatinho de trafego para avaliar ambos os profiles: de capacidade mínima e os de capacidade máxima.
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		Avaliar o parâmetro de count das políticas criadas especificando as combinações granulares criadas.	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.4.12		Deverá possuir os seguintes mecanismos de inspeção de IPS:	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurado conforme os itens subseqüentes	
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.4.12.1		Análise de padrões de estado de conexões;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		No dashboard selecionar o widget source podendo ser analisado o total de sessões e o total de bytes trafegados.	
Procedimento do Teste		Analisar o grafico com os indices avaliados	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.4.12.2		Análise de decodificação de protocolo;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Ativar o feature de IPS (que é a base para analise) , e configurar em seqüência um profile de APP control	
Procedimento do Teste		Gerar um trafego nao padrão de HTTP, de forma que o fortigate através do LOG de IPS e APP control conseguirá identificar.	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.4.12.3		Análise para detecção de anomalias de protocolo;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configuração de política de DoS, e ajustar os parâmetros conforme indicado pelo cliente	
Procedimento do Teste		Simular trafego para detecção de eventos de anomalia	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.4.12.4		Análise heurística;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar profile de Antivirus	
Procedimento do Teste		Analisar nos Logs os alertas correspondentes ao perfil selecionado	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.4.12.5		IP defragmentation;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar profile de IPS contendo assinaturas de IP defragmentation e ativar em uma regra de firewall.	
Procedimento do Teste		Analisar nos Logs os alertas correspondentes ao perfil selecionado	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.4.12.6		Bloqueio de pacotes malformados;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar profile de IPS e selecionar assinaturas correspondente a pacotes malformados	
Procedimento do Teste		Analise dos logs correspondente a assinaturas de pacotes malformados apos o match do trafego desta assinatura.	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.4.13		Ser imune e capaz de impedir ataques básicos, tais como: syn flood, ICMP flood, UDP flood	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar políticas de DoS, ajustando os parâmetros básicos solicitados	
Procedimento do Teste		Analisar nos Logs de IPS/anomaly e confirmar os alertas correspondentes ao trafego	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.4.14		Detectar e/ou bloquear a origem de um portscan;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar politica de DoS ajustando o parametro de tcp_port_scan e udp_scan	
Procedimento do Teste		Simular o trafego de portscan e validar os alertas no log de IPS/Anomaly	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.4.15		Bloquear ataques efetuados por worms conhecidos;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar profile de Anti-virus	
Procedimento do Teste		Simular trafego de worms e validar os alertas nos logs de anti-virus	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.4.16		Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar perfil de IPS e política de DDoS as assinaturas e parâmetros de anomalia de consideráveis para o ambiente.	
Procedimento do Teste		Mostrar as assinaturas especificas conforme solicitado	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.4.17		Possuir assinaturas para bloqueio de ataques de buffer overflow;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar profile de IPS e selecionar as assinaturas de Buffer overflow	
Procedimento do Teste		Simular a criação da política com as assinaturas conforme solicitado.	
Evidências			
Comentário			
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			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.4.19		É permitido o uso de appliance externo (antivírus de rede), para o bloqueio de vírus e spywares em protocolo SMB de forma a conter malwares se espalhando horizontalmente pela rede;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar no profile de Anti-virus o envio para o Sandbox	
Procedimento do Teste		Validar o envio dos logs no equipamento Fortisandbox vindos do Fortigate	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.4.22	Deve suportar várias técnicas de prevenção, incluindo drop e/ou tcp-rst;
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado
Configuração do Teste	Configurar nos profiles de IPS nas assinaturas ambas as ações mencionadas.
Procedimento do Teste	Validar nos logs de IPS as assinaturas que fizeram match nas ações mencionadas.
Evidências	
Comentário	

Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.4.23		Registrar na console de monitoramento as seguintes informações sobre ameaças identificadas:	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Selecionar o widget para perfil inicial de acesso.	
Procedimento do Teste			
Evidências			
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		Selecionar o Widget de Attack	
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.4.24		Deve suportar a captura de pacotes (pcap), por assinatura de IPS e/ou anti-spyware;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurado no profile de IPS a opção de captura de pacote	
Procedimento do Teste		Fazer uma simulação de uma assinatura habilitada para captura do pacote, em seguida validar no modo de log/archive os pacotes capturados a parti do match pela as assinaturas.	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.4.25		Deve possuir a função de resolução de endereços DNS, para que conexões com destino a domínios maliciosos sejam resolvidas pelo firewall com endereços (IPv4 e IPv6), previamente definidos;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste			
Procedimento do Teste			
Evidências			
Comentário			
Assinatura		**Assinatura NCT**	

do Cliente			

Item de Teste - 1.6.4.26		Permitir o bloqueio de vírus, pelo menos, nos seguintes protocolos: HTTP, FTP, SMB, SMTP;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar um profile de Anti-virus habilitando para inspeção apenas os protocolos mencionados.	
Procedimento do Teste		Validar nos logs os scans realizados referente ao trafego dos protocolos.	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.4.27		Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurado profile de Anti-virus	
Procedimento do Teste		Analisado nos logs a referencias dos tipos de proteção mencionados	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.4.28		Proteção contra downloads de arquivos maliciosos involuntários usando HTTP;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurado profile de Anti-virus	
Procedimento do Teste		Analisado nos logs a referencias dos tipos de proteção mencionados	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.4.29		Rastreamento de vírus em pdf;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar profile de Anti-virus e ativa analise objeto	
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.4.30		Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.);	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar profile de DLP indicando filtro de tipo de arquivo.	
Procedimento do Teste		Validado no perfil log mostrando os scans em zip. gzip, etc	
Evidências			
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			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Analise de malwares modernos - Sandbox

Item de Teste - 1.6.5.2		A solução ofertada dever possuir funcionalidades para análise de malwares não conhecidos incluídas na própria ferramenta ou entregue em composição com outro fabricante;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurado o Equipamento fortiSandbox para o recebimento de amostra para analise de malwares conforme solicitado.	
Procedimento do Teste		Fazer o envio de amostra para ser analisado no Fortisandbox, e validar os logs desta.	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.5.3	O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "in cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado
Configuração do Teste	Configurar o envio o envio das amostras para análise

Procedimento do Teste		Executar uma atividade de envio da amostra, e confirmar a validação do envio da mesma.	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.5.4		Selecionar através de política de firewall quais tipos de arquivos sofrerão esta análise;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar política contendo os arquivos conforme solicitados	
Procedimento do Teste		Validar o teste da atividade da criação da política	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.5.5		A análise deverá considerar, pelo menos, 100 (cem) tipos de comportamentos maliciosos distintos para determinar se o arquivo é malicioso ou não;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		configurar profile de analise de malware para demonstrar os tipos comportamentos maliciosos conforme solicitado	
Procedimento do Teste		Executar um teste de uma amostra para demonstrar o tipo de Scan.	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.5.6		Suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistemas operacionais Windows XP e Windows 7;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar os profiles de emulação de teste nos ambientes conforme solicitado.	
Procedimento do Teste		Executar uma demonstração de analise de amostra em cada ambiente mencionado	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.5.7	Deve suportar o monitoramento de arquivos trafegados na

	internet (HTTP, FTP, HTTP, SMTP) como também arquivos trafegados internamente nos servidores de arquivos usando SMB;		
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado		
Configuração do Teste	Configurar profile de Anti-virus selecionado os tipos de arquivos solicitados e habilitar em uma regra de firewall		
Procedimento do Teste	Executar a adição deste profile em uma politica de firewall e validar teste de trafego destes protocolos para confirmar o scan		
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

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 a aba de summary report e o deteiled report para ter acesso as informações conforme solicitado		
Procedimento do Teste	Gerar um relatório com as informações conforme solicitados		
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.5.10	Deve permitir exportar o resultado das análises de malwares de dia zero em PDF e CSV a partir da própria interface de gerência;		
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado		
Configuração do Teste	Configurar o relatório e exportar conforme solicitado		
Procedimento do Teste	Mostrar o report nos formatos conforme solicitados		
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.5.12	Deve permitir visualizar os resultados das análises de malwares de dia zero nos diferentes sistemas operacionais suportados;
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado
Configuração do Teste	Gerar um relatório de todos as analises
Procedimento do Teste	Apresentar o relatório de todos as analises geradas

Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.5.13		Deve permitir informar ao fabricante quanto a suspeita de ocorrências de falso positivo falso-negativo na análise de malwares de dia zero a partir da própria interface de gerência;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Na aba Fortiview selecionar mark as clear ou mark suspicious, e selecione submit para clound para equipe da fortiguard analisar	
Procedimento do Teste		Executar a demonstração de submit	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.5.14		Suportar a análise de arquivos executáveis, dll, ZIP e criptografados em SSL no ambiente controlado.	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar devices e file type, e selecionar os tipos de extensões conforme solicitado	
Procedimento do Teste		Executar o teste dos tipos de executáveis conforme solicitado	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Filtro de URL

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 testes demonstrando uma política com os filtros solicitados	
Evidências			
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		Configurar política de firewall selecionando controle de acesso por usuários e grupos através dos serviços de integrações solicitados habilitando para cada grupo ou usuários os perfis de web filter	
Procedimento do Teste		Executar teste 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			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.6.1.4		Permite popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar na politica de firewall de autenticação dos grupos de usuário o log de security event	
Procedimento do Teste		Confirmar no painel de log o usuário autenticado mostrando o seu respectivo grupo de acesso.	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.6.1.5		Suporta a capacidade de criação de políticas baseadas no controle por URL e categoria de URL; 50	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar um profile de Web filter e selecionado o modulo de listas locais de URL filter	
Procedimento do Teste		Adicionar a lista de URL filter do profile de Web filter uma especifica URL	
Evidências			
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	Configurar no profile de Web filter e selecionar o safe seach		
Procedimento do Teste	Executar teste de acesso a um destes sites de busca e validar o bloqueio de um objeto de busca classificados como bloqueado no profile.		
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.6.1.7	Suporta base ou cache de URLs local no appliance, evitando delay de comunicação ou validação das URLs;		
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado		
Configuração do Teste	Configurar perfil de Web cache		
Procedimento do Teste	Validar no monitor de cache o volume de cache web armazenado		
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.6.1.8	Possuir pelo menos 60 categorias de URLs;		
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado		
Configuração do Teste	Configurar um profile de web filter , demostrar todas as categorias e sub-categorias existentes		
Procedimento do Teste	Mostrar todas as categorias e sub-categorias		
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.6.1.9	Suportar a criação de categorias de URL customizadas;		
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado		
Configuração do Teste	Configurar uma URL com expressões regulares e com Wildcard.		
Procedimento do Teste	Mostrar os padrões de customização das URLs		
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.6.1.10	Suportar a exclusão de URL do bloqueio, por categoria;
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado
Configuração do Teste	Configurar uma entrada de uma especifica URL na lista de URL

		filter no profile, adicionando ação de allow	
Procedimento do Teste		Mostrar no log de acesso Web que a URL mesmo sendo de uma categoria liberada a mesma foi liberada pela lista de exceção.	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.6.1.11		Permitir a customização de página de bloqueio;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Editar o replacement message	
Procedimento do Teste		Executar teste com uma alteração conforme solicitado pelo cliente.	
Evidências			
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		Configurar políticas selecionando os controles solicitados, adicionar os respectivos profiles de segurança	
Procedimento do Teste		Validar os controles de dados trafegados por estas políticas através dos Logs, mostrando todos os controles habilitados na regra.	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.7.2		Deve possuir integração com Microsoft Active Directory, RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle baseada em usuários e grupos de usuários;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Executar a configuração de FSSO assim como remote servers RADIUS e LDAP.	
Procedimento do Teste		Validar a integração das listas de grupos configurados	
Evidências			

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 - 1.6.7.4		Suporte a autenticação Kerberos;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configuração no equipamento Fortiautenticator, adicionando os parâmetros de autenticação Kerberos.	
Procedimento do Teste		Mostrar a integração com o servico de autenticação Kerberos	
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		Configurar FSSO TS agent para Citrix	
Procedimento do Teste		Executar teste de múltiplos usuários por TS sendo autenticados.	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.7.6	Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em servidores acessados remotamente, mesmo que não sejam servidores Windows;
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado
Configuração do Teste	Acessar a aba de User-devices-> monitor->Firewall

Procedimento do Teste		Visualizar no monitor todos os usuários autenticados	
Evidências			
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		Validar o gráfico de traffic shaping por política, e testar video com traffic shaping e sem o traffic shaping.	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.8.2		Suportar a criação de políticas de QoS por:	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configuração conforme os demais itens subseqüentes	
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.8.2.1		Endereço de origem;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar politica de firewall especificando a origem e habilitando nesta o profile de traffic shaping escolhido	
Procedimento do Teste		Validar no Log que o acesso esta sendo feito match pela políticas com traffic shaping.	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.8.2.2		Endereço de destino;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar politica de firewall especificando o destination e habilitando nesta o profile de traffic shaping escolhido	
Procedimento do Teste		Validar no Log que o acesso esta sendo feito match pela políticas com traffic shaping.	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.8.2.3		Por usuário e grupo do LDAP/AD;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Habilitar o profile de traffic shaping na política associados aos grupos dos diretórios mencionados.	
Procedimento do Teste		Validar profile do usuários associado a regra contendo traffic shaping	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.8.2.4		Por aplicações, incluindo, mas não limitado a: Skype, Bittorrent, YouTube e Azureus;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Habilitar profile de traffic shaping nas configurações de APP control associando como ação um dos profiles de traffic shaping as especificas aplicações mencionadas neste item	
Procedimento do Teste		Validar shaping associado por aplicação	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.8.2.5		Por porta;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar regra de firewall especificando uma porta especifica e associar profile de traffic Shaping à esta	
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.8.3		O QoS deve possibilitar a definição de classes por:	
Objetivo do Teste		demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurados as definições conforme os itens subseqüentes	
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		Assinatura NCT	

Item de Teste - 1.6.8.3.1		Banda garantida;	
Objetivo do Teste		demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar profile de traffic shaping selecionado a opção de garantia de banda conforme solicitado	
Procedimento do Teste		Executar preenchimento do valor máximo	
Evidências			
Comentário			
Assinatura do Cliente		Assinatura NCT	

Item de Teste - 1.6.8.3.2		Banda máxima;	
Objetivo do Teste		demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar profile de traffic shaping selecionado a opção de banda máxima conforme solicitado	
Procedimento do Teste		Executar preenchimento do valor de banda máxima	
Evidências			
Comentário			
Assinatura do Cliente		Assinatura NCT	

Item de Teste - 1.6.8.3.3		Fila de prioridade;	
Objetivo do Teste		demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar profile de traffic shaping selecionado uma das opções de prioridade	
Procedimento do Teste		Validar a seleção da opção de prioridade	
Evidências			
Comentário			
Assinatura do Cliente		Assinatura NCT	

Item de Teste - 1.6.8.4	Suportar priorização de tempo real de protocolos de voz (VOIP), tais como: H.323, SIP, SCCP, MGCP e aplicações como Skype;
Objetivo do Teste	demonstrar a funcionalidade conforme solicitado
Configuração do Teste	Configurar no profile de traffic shaping habilitando DSCP, e

		associado à uma regra de firewall contendo tais protocolos de serviços mencionados	
Procedimento do Teste		Validar a seleção da opção de prioridade	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.8.5		Suportar marcação de pacotes Diffserv, inclusive por aplicação;	
Objetivo do Teste		demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar profile de Traffic Shaping, e habilitar o DSCP, em seguida habilitar na regra de firewall correspondente via CLI Diffserv	
Procedimento do Teste		Selecionar um profile de APP control e habilitando o Traffic shaping criado com as especificações de DSCP , em seguida adicioná-lo na regra.	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.8.5		Suportar marcação de pacotes Diffserv, inclusive por aplicação;	
Objetivo do Teste		demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Associar o profile de traffic shaping habilitado ao diffserv a uma ação especifica de uma aplicação	
Procedimento do Teste		Validar a criação desta configuração dentro da aba de APP control	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.8.6		Disponibilizar estatísticas de tempo real para classes de QoS;	
Objetivo do Teste		demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Executar o comando de debug flow para a sessão com QoS	
Procedimento do Teste		Mostrar o output do comando de diagnostico	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.8.7		Deverá permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e usuário.	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Apresentar o painel de App Control monitor	
Procedimento do Teste		Mostrar os resultados no monitor conforme solicitado	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.9.1		Permitir a criação de filtros para arquivos e dados pré-definidos;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar um profile de DLP pré-definindo os tipos de arquivos e dados	
Procedimento do Teste		Mostrar tela de Log de DLP destacando os arquivos pré-definidos	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.9.2		Os arquivos devem ser identificados por extensão e assinaturas;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar profile de DLP especificando is tipos de extensões de arquivo	
Procedimento do Teste		Mostrar o modo de configuração selecionando os tipos de arquivos a ser selecionado no profile	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.9.3		Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, dentre outros) identificados sobre aplicações (P2P, Instant Messaging, SMB, dentre outros);	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar profile de DLP especificando os tipos de filtros por aplicação e padrões de arquivos	
Procedimento do Teste		Mostrar o padrão de configuração do profile, assim como homologar teste de trafego chegando o log passante pela politica de firewall contendo este profile	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.9.4		Suportar identificação de arquivos compactados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar um profile de DLP contendo filtro por arquivos de extensão de compactavel (zip,GZIP,etc)	
Procedimento do Teste		Validar o mecanismos de filtro de tipos de arquivos compactados	
Evidências			
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 a opção de Fingerprinting	
Procedimento do Teste		Validar a criação de informações sensíveis conforme solicitado neste item	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.9.6		Permitir listar o número de aplicações suportadas para controle de dados;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar um profile de DLP na opção de manipulação do sensor, via CLI pode ser listado todos os protocolos suportados.	
Procedimento do Teste		Mostrar a lista de todos os protocolos suportados executando o comando via CLI "set-summary-protocol"	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.9.7	Permitir listar o número de tipos de arquivos suportados para controle de dados.
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado
Configuração do Teste	Configurar um profile de DLP especificando no sensor a opção de Watermark Sensitivity, e selecionar a lista de arquivos suportados.
Procedimento do Teste	Mostrar habilidade de criação de todos estes tipos de arquivos suportados
Evidências	

Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.10.1		Suportar a criação de políticas por geolocalização, permitindo que o tráfego de determinados países seja bloqueado;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar objeto de firewall por geolocalização, em seguida especifica este objeto em uma regra de firewall, habilitar ação de bloqueio para uma lista especifica de países.	
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.10.3		Deve possibilitar a criação de regiões geográficas pela interface gráfica, tornando possível sua utilização em políticas de firewall.	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Criar regra de firewall utilizando o objeto de geolocalização	
Procedimento do Teste		Validar um acesso requisitando um destino não permitido pelo filtro da regra de geolocalização.	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.11.1		Suportar VPN site-to-site e cliente-to-site;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar VPNs dos padrões conforme solicitados	
Procedimento do Teste		Mostrar passos de configuração de ambos os tipos de VPN	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.11.2		Suportar IPSec VPN;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar VPN IPSec do padrão conforme solicitados	
Procedimento do Teste		Mostrar passos de configuração VPN IPSec	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.11.3		Suportar SSL VPN;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar VPN do padrão conforme solicitados	
Procedimento do Teste		Mostrar passos de configuração VPN SSL	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.11.4		A VPN IPSec deve suportar:	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		Configurar conforme solicitados nos itens subseqüentes	
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.11.4.1		3DES;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		No painel de configuração da fase 1 da IPSec VPN, selecionar o modo de encryption conforme solicitado	
Procedimento do Teste		Validar a partir da tela de configuração do modo de encryption 3DES	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.11.4.2		Autenticação MD5 e SHA-1;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		No painel de configuração da fase 1 da IPSec VPN, selecionar o parâmetro de autenticação conforme solicitado.	
Procedimento do Teste		Validar a partir da tela de configuração do modo de autenticação os padrões solicitados.	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.11.4.3	Diffie-Hellman group 1, group 2, group 5 e group 14;
Objetivo do Teste	Demonstrar a funcionalidade conforme solicitado
Configuração do Teste	No painel de configuração da fase 1 da IPSec, selecionar os grupos de DH conforme solicitado

Procedimento do Teste		Validar a partir da tela de configuração os grupos de DH disponíveis para configuração	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.11.4.4		Algoritmo Internet Key Exchange (IKE);	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		No painel de configuração da fase 1 da IPSec, há a opção de IKE em versões 1 e 2.	
Procedimento do Teste		Validar a partir da tela de configuração de IKE e suas opções	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.11.4.5		AES (Advanced Encryption Standard); 128 e 256;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		No painel de configuração da fase 1 da IPSec, selecionar um dos itens de encryption avançado conforme solicitado	
Procedimento do Teste		Validar a partir da tela de configuração referente ao método de encryption avançada , selecionando as opções solicitadas.	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.11.4.6		Autenticação via certificado IKE PKI;	
Objetivo do Teste		Demonstrar a funcionalidade conforme solicitado	
Configuração do Teste		No painel de configuração da fase 1 da IPSec, selecionar o método de autenticação via certificado , em seguida selecionado o tipo de certificado.	
Procedimento do Teste		Mostrar a habilidade de haver a autenticação via certificado	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.11.5	Deve possuir interoperabilidade com os seguintes fabricantes:
Objetivo do Teste	N/A - Possui padrão RFC IPSEC
Configuração do Teste	
Procedimento do Teste	
Evidências	
Comentário	

Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.11.5.1	Cisco;		
Objetivo do Teste	N/A - Possui padrão RFC IPSEC		
Configuração do Teste			
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.11.5.2	Checkpoint;		
Objetivo do Teste	N/A- Possui padrão RFC IPSEC		
Configuração do Teste			
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.11.5.3	Juniper;		
Objetivo do Teste	N/A- Possui padrão RFC IPSEC		
Configuração do Teste			
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.11.5.4	Palo Alto Networks;		
Objetivo do Teste	N/A- Possui padrão RFC IPSEC		
Configuração do Teste			
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.11.5.5	Fortinet;
Objetivo do Teste	N/A- Possui padrão RFC IPSEC
Configuração do Teste	
Procedimento do Teste	
Evidências	
Comentário	

Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.11.5.6		Sonic Wall;	
Objetivo do Teste		N/A- Possui padrão RFC IPSEC	
Configuração do Teste			
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.11.6		A VPN SSL deve suportar:	
Objetivo do Teste		Demonstrar funcionalidade conforme solicitado	
Configuração do Teste			
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.11.6.1.1		Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface Web;	
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			
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			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.11.6.1.3	Atribuição de endereço IP nos clientes remotos de VPN;		
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado		
Configuração do Teste	Configurar as informação de remote gateway da VPN e Realizar o acesso a SSL VPN utilizando a modalidade tunnel mode.		
Procedimento do Teste	Realizar o acesso a VPN e confirmar na placa de rede local o ip do Tunnel.		
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.11.6.1.4	Atribuição de DNS nos clientes remotos de VPN;		
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado		
Configuração do Teste	Configurar os parâmetros de DNS no painel de SSL VPN no firewall Fortigate		
Procedimento do Teste	Executar após a VPN conectada a validação na placa de rede do usuário as definições de DNS atribuidas ao tunnel.		
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.11.6.1.5	Deve haver a opção de ocultar o agente de VPN instalado no cliente remoto, tornando o mesmo invisível para o usuário;		
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado		
Configuração do Teste	Demonstrar ocultação de cliente de vpn		
Procedimento do Teste	Demonstrar cliente oculto no s.o.		
Evidências			
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 VPN		
Evidências			

Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.11.6.1.7	A VPN SSL deve suportar proxy ARP e uso de interfaces PPPoE;		
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado		
Configuração do Teste	Configurar interface PPoE		
Procedimento do Teste	Validar a configuração conforme solicitado		
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.11.6.1.8	Suportar autenticação via AD/LDAP, Secure ID, certificado e base local de usuários;		
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado		
Configuração do Teste	Executar a configuração dos parâmetros de autenticação conforme solicitado.		
Procedimento do Teste	Configurar os parametros conforme solicitado		
Evidências			
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	Configurar uma VPN no padrão client-to-client, especificando a autenticação do cliente com integração como suas credencias do windows da maneira solicitado		
Procedimento do Teste	Executar um teste de conexão de VPN SSL client-to-client conforme solicitado.		
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.11.6.1.10	Suportar a leitura e verificação de CRL (Certificate Revocation List);
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado
Configuração do Teste	Configurar a inserção de lista de certificado revogados na aba de "certificate".
Procedimento do Teste	Executar a importação da lista CRL
Evidências	

Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.11.6.1.11	Permitir a aplicação de políticas de segurança e dispor de visibilidade para as aplicações que circulam dentro dos túneis SSL;		
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado		
Configuração do Teste	Criar uma política de firewall limitando o acesso a aplicações especificas por dentro do tunnel		
Procedimento do Teste	Mostrar a habilidade de visibilidade a parti dos acessos pelo tunnel pela debilitação de políticas de acesso.		
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.11.6.1.12	O agente de VPN a ser instalado nos equipamentos desktop e laptops deve ser capaz de ser distribuído de maneira automática via Microsoft SMS, Active Directory e ser descarregado diretamente desde o seu próprio portal, o qual residirá no centralizador de VPN;		
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado		
Configuração do Teste	Gerar .msi e demonstrar download de cliente		
Procedimento do Teste	Verificar arquivo .msi e realizar download do cliente no portal.		
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.11.6.1.13	O agente deverá comunicar-se com o portal para determinar as políticas de segurança do usuário;		
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado		
Configuração do Teste	Configurar um portal para um especifico grupo de usuário		
Procedimento do Teste	Validar o acesso do usuário ao portal configurado para o mesmo		
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.11.7	Deve permitir que a conexão com a VPN SSL seja estabelecida das seguintes formas:
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado
Configuração do Teste	
Procedimento do Teste	

Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.11.7.1.1	Antes do usuário autenticar na estação;		
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado		
Configuração do Teste	Configurar previsionamento de VPN via client		
Procedimento do Teste	Mostrar autenticação de um usuário que contenha o cliente e mostrar a conexão automática à VPN		
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.11.7.1.2	Após autenticação do usuário na estação;		
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado		
Configuração do Teste	Configurar VPN SSL padrão para acesso de usuário		
Procedimento do Teste	Mostrar autenticação de um usuário que contenha o cliente e mostrar a conexão após o mesmo executar a solicitação de autenticação .		
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.11.7.1.3	Sob demanda do usuário;		
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado		
Configuração do Teste	Configurar VPN SSL padrão para acesso de usuário		
Procedimento do Teste	Executar um acesso sob demanda		
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.11.8	Deverá manter uma conexão segura com o portal durante a sessão;		
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado		
Configuração do Teste	Configurar VPN SSL padrão para acesso ao portal SSL		
Procedimento do Teste	Mostra que o portal esta estabelecido em uma conexão segura SSL.		
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.11.9		O agente de VPN SSL client-to-site deve ser compatível com pelo menos os seguintes sistemas operacionais: Windows XP, Windows Vista, Windows 7, Windows 8 e Mac OSx;	
Objetivo do Teste		Demonstrar funcionalidade conforme solicitado	
Configuração do Teste		Configurar VPN SSL client-to-site	
Procedimento do Teste		Executar testes de acesso nos SO conforme solicitados	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Gerenciamento centralizado e monitoramento

Item de Teste - 1.6.12.1		Centralizar administração de regras e políticas dos equipamentos fornecidos, usando uma única interface de a gerenciamento;	
Objetivo do Teste		Demonstrar funcionalidade conforme solicitado	
Configuração do Teste		Configurar um pacote de política a partir Fortimanager	
Procedimento do Teste		Mostrar a criação de uma política no Fortimanager e aplicar appliance.	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.12.3		O gerenciamento da solução deve suportar acesso via SSH, cliente remoto e/ou web por HTTPS;	
Objetivo do Teste		Demonstrar funcionalidade conforme solicitado	
Configuração do Teste		Configurar na interface os modos de acesso administrativo solicitados neste item	
Procedimento do Teste		Executar o acesso ao equipamento conforme os métodos solicitados.	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

O gerenciamento deve permitir ou possuir:

Item de Teste - 1.6.12.5.1		Criação e administração de políticas de firewall e controle de aplicação;	
Objetivo do Teste		Demonstrar funcionalidade conforme solicitado	
Configuração do Teste		Executar a configuração de pacote de políticas de firewall e profiles de APP control a partir da interface de gerencia do	

		Fortimanager	
Procedimento do Teste		Executar a instalação de pacote de políticas no appliance Fortigate a partir do Foirtimanager.	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.12.5.2		Criação e administração de políticas de IPS, antivírus e antispyware;	
Objetivo do Teste		Demonstrar funcionalidade conforme solicitado	
Configuração do Teste		Configurar as políticas de segurança citadas no item a partir da interface de administração do fortimanager	
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.12.5.3		Criação e administração de políticas de filtro de URL;	
Objetivo do Teste		Demonstrar funcionalidade conforme solicitado	
Configuração do Teste		Configurar as políticas citadas no item a partir da interface de administração do fortimanager	
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.12.5.4		Monitoramento de logs;	
Objetivo do Teste		Demonstrar funcionalidade conforme solicitado	
Configuração do Teste		Acessar o painel Fortiview	
Procedimento do Teste		Visualizar a aba de Log view para obter as informações de logs	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.12.5.5		Ferramentas de investigação de logs;	
Objetivo do Teste		Demonstrar funcionalidade conforme solicitado	
Configuração do Teste		Acessar o painel Fortiview	
Procedimento do Teste		Visualizar a aba de Log view para obter as informações de logs	
Evidências			
Comentário			

Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.12.5.6		Recursos para troubleshooting;	
Objetivo do Teste		Demonstrar funcionalidade conforme solicitado	
Configuração do Teste		Acessar o painel Fortiview e Logs	
Procedimento do Teste		Executar analise de log de trafego e segurança	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.12.5.7		Captura de pacotes;	
Objetivo do Teste		Demonstrar funcionalidade conforme solicitado	
Configuração do Teste		Configurar o filtro de captura de pacotes a partir da interface gráfica	
Procedimento do Teste		Mostrar o arquivo capturado	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.12.5.8		Acesso concorrente de administradores;	
Objetivo do Teste		Demonstrar funcionalidade conforme solicitado	
Configuração do Teste		Configurar múltiplos acessos de administradores	
Procedimento do Teste		Executar acessos de múltiplos administradores simultâneo	
Evidências			
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			
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	Configurar Cores, tags e comentários		
Procedimento do Teste	Mostrar a marcação de cores, tags e comentarios		
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.12.5.11	Deve permitir monitorar via SNMP falhas de hardware, inserção ou remoção de fontes de alimentação, discos e coolers, uso de recursos por número elevado de sessões, número de túneis estabelecidos na VPN cliente-to-site e número de sessões estabelecidas;		
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado		
Configuração do Teste	Configurar comunidade SNMP assim como selecionar este protocolo na interface .		
Procedimento do Teste	Mostrar o modo de configuração de SNMP e a seleção dos itens de monitoramento solicitados neste item		
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.12.5.12	Bloqueio de "commit" das configurações do firewall, no caso de acesso simultâneo de dois ou mais administradores;		
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado		
Configuração do Teste	Configurar a opção de Lock no pacote de política		
Procedimento do Teste	Executar teste de manipulação de política em simultâneo a um outro administrador que selecionou a opção lock		
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.12.5.13	Definição de perfis de acesso na console com permissões granulares, tais como: acesso de escrita, acesso de leitura, criação de usuários e alteração de configurações;		
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado		
Configuração do Teste	Configurar perfis de acesso conforme as granularidades acima mencionadas		
Procedimento do Teste	Executar acessos de vários usuários correspondente a cada perfil de acesso criado.		
Evidências			
Comentário			
Assinatura		**Assinatura NCT**	

do Cliente			

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			
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 - 1.6.12.5.16		Deve atribuir seqüencialmente um número a cada regra de firewall, NAT, QoS e regras de DOS;	
Objetivo do Teste		Demonstrar funcionalidade conforme solicitado	
Configuração do Teste		Automaticamente ao criar uma regra o mesmo já atribui um numero seqüencial.	
Procedimento do Teste		Efetivar a criação de uma regra e validar o numero de seqüência em seguida.	
Evidências			
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		**Assinatura NCT**	

do Cliente			

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	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.12.5.22		Validação de regras antes da aplicação;	
Objetivo do Teste		Demonstrar funcionalidade conforme solicitado	
Configuração do Teste		Executar a aplicação de uma regra	
Procedimento do Teste		Demonstrar aplicação de uma regra e a mensagem de validação da mesma.	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.12.5.23	É permitido o uso de appliance externo para realizar a validação

		de regras antes da aplicação;	
Objetivo do Teste		Não se aplica	
Configuração do Teste			
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.12.5.24		Validação das políticas, avisando quando houver regras que ofusquem ou conflitem com outras (shadowing). É permitida a utilização de appliance externo;	
Objetivo do Teste		Demonstrar funcionalidade conforme solicitado	
Configuração do Teste		Executar o check policy	
Procedimento do Teste		Mostrar o resultado do check policy	
Evidências			
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 - 1.6.12.5.26		Deve possibilitar a integração com soluções de SIEM de mercado;	
Objetivo do Teste		Demonstrar funcionalidade conforme solicitado	
Configuração do Teste		Configurar via CLI o parâmetro de configuração com SIEM	
Procedimento do Teste		Executar testes de comunicação e envio de dados para o SIEM	
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			
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		
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		Gerar relatório e executar o download para mostra
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
Evidências		
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		No dashboad é exibido a quantidade de logs por device	
Procedimento do Teste		Analisar o widget de estatística de logs por device	
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			
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			
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 em qualquer uma dos módulos de sumarização clicar com o botão direito para executar um drill-down, para várias instancias de analise.	
Procedimento do Teste		Executar uma demonstração de drill-down conforme solicitado	
Evidências			
Comentário			
Assinatura		**Assinatura NCT**	

do Cliente			

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		Executar o teste conforme o solicitado	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.12.15		Exibição das seguintes informações, de forma histórica e em tempo real (atualizado de forma automática e contínua a cada 1 minuto):	
Objetivo do Teste		Demonstrar funcionalidade conforme solicitado	
Configuração do Teste		Exigir os dados conforme solicitado nos itens subseqüentes	
Procedimento do Teste			
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		Habilitar no Dashboard o widget "Operation unit"	
Procedimento do Teste		Demonstrar o status dos equipamentos no widget	
Evidências			
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		Habilitar no Dashboard o widget "Advanced threat Protection"	
Procedimento do Teste		Demonstrar o widget "Advanced threat Protection"	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.12.15.4		Administradores autenticados na gerência da plataforma de segurança;	
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			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.12.15.7	Uso de CPU;
Objetivo do Teste	Demonstrar funcionalidade conforme solicitado
Configuração do Teste	No dashboard no widget " system resource"
Procedimento do Teste	Mostrar o status do consumo de memória
Evidências	
Comentário	

Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.12.16		Geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:	
Objetivo do Teste		Demonstrar funcionalidade conforme solicitado	
Configuração do Teste		Configurar os itens conforme solicitado nos itens subseqüentes.	
Procedimento do Teste			
Evidências			
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		Configurar no modulo de "report" o relatório correspondente "application"	
Procedimento do Teste		Gerar o relatório	
Evidências			
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		Configurar no modulo de "report" o relatório correspondente a controle de banda conforme solicitado	
Procedimento do Teste		Gerar o relatório	
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	
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	
Evidências			
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			
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	
Evidências			
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		Configurar no modulo de geração de relatório filtros específicos conforme solicitado neste item	
Procedimento do Teste		Gerar o relatório com os filtros solicitados	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.12.18		Gerar alertas automáticos via:	
Objetivo do Teste		Demonstrar funcionalidade conforme solicitado	
Configuração do Teste		Configurar os alertas conforme o solicitado nos itens subseqüentes	
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.12.18.1		E-mail;	
Objetivo do Teste		Demonstrar funcionalidade conforme solicitado	
Configuração do Teste		Configurar na aba de "alert mail"	
Procedimento do Teste		Mostrar alerta	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.6.12.18.2		SNMP;	
Objetivo do Teste		Demonstrar funcionalidade conforme solicitado	
Configuração do Teste		Configurar alertas via SNMP	
Procedimento do Teste		Mostrar alerta via SNMP	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

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

Item de Teste - 1.7.2.1		A solução deve consistir de appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoramento;	
Objetivo do Teste		Demonstrar especificação conforme solicitado	
Configuração do Teste		Conforme apresentado no equipamento	
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.2.5		A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;	
Objetivo do Teste		Demonstrar especificação conforme solicitado	
Configuração do Teste		Conforme apresentado no equipamento	
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.2.5		O hardware e software que executem as funcionalidades de proteção de rede, bem como a console de gerência e monitoramento, devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;	
Objetivo do Teste		Conforme proposta comércial.	
Configuração do Teste			
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.2.6		Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:	
Objetivo do Teste		Demonstrar conforme solicitado.	
Configuração do Teste			
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.2.6.1		Suporte a 1024 VLAN tags 802.1q;	
Objetivo do Teste		Demonstrar suporte de vlan ao item	
Configuração do Teste		Demonstrar suporte vlan	
Procedimento do Teste		System -> network -> interfaces	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.2.6.2		Suporte a PBR (Policy Based Routing) ou PBF (Policy Based Forwarding);	
Objetivo do Teste		Demonstrar suporte a PBR e PBF	
Configuração do Teste		Demonstrar policicy router	
Procedimento do Teste		Router -> policy router	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.2.6.3		Roteamento multicast (PIM-SM);	
Objetivo do Teste		Demonstrar suporte a multicast	
Configuração do Teste		Demonstrar pim-sm	
Procedimento do Teste		Acessar via CLI o equipamento e demonstrar o suporte a PIM-SM	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.2.6.4		DHCP relay;	
Objetivo do Teste		Demonstrar configuração de DHCP	
Configuração do Teste		Demonstrar DHCP relay	
Procedimento do Teste		System -> network-> interface	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.2.6.5		DHCP server;	
Objetivo do Teste		Demonstrar configuração de DHCP	
Configuração do Teste		Demonstrar DHCP server	
Procedimento do Teste		System -> network-> interface	
Evidências			
Comentário			
Assinatura		**Assinatura NCT**	

do Cliente			

Item de Teste - 1.7.2.6.6		Suporte à criação de objetos de rede que possam ser utilizados como endereço IP de interfaces L3;	
Objetivo do Teste		Demonstrar criação de objetos para uso em L3	
Configuração do Teste		Demonstrar criação de objetos	
Procedimento do Teste		Firewall objects -> address	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.2.7		Suportar subinterfaces ethernet lógicas.	
Objetivo do Teste		Demonstrar sub interfaces lógicas	
Configuração do Teste		Demonstrar vlan	
Procedimento do Teste		System -> network -> interfaces	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.2.8		Deve suportar os seguintes tipos de NAT:	
Objetivo do Teste		Demonstrar conforme solicitado.	
Configuração do Teste			
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.2.8.1		Nat dinâmico (n:1);	
Objetivo do Teste		Demonstrar uso de nat no equipamento	
Configuração do Teste		Demonstrar vip e ip pool	
Procedimento do Teste		Firewall objects -> virtual IPs	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.2.8.2		Nat dinâmico (n:n);	
Objetivo do Teste		Demonstrar uso de nat no equipamento	
Configuração do Teste		Demonstrar vip e ip pool	
Procedimento do Teste		Firewall objects -> virtual IPs	
Evidências			
Comentário			

Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.2.8.3		Nat estático (1:1);	
Objetivo do Teste		Demonstrar uso de nat no equipamento	
Configuração do Teste		Demonstrar vip e ip pool	
Procedimento do Teste		Firewall objects -> virtual IPs	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.2.8.4		NAT estático (n:n)	
Objetivo do Teste		Demonstrar uso de nat no equipamento	
Configuração do Teste		Demonstrar vip e ip pool	
Procedimento do Teste		Firewall objects -> virtual IPs	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.2.8.5		Nat estático bidirecional (1:1);	
Objetivo do Teste		Demonstrar uso de nat no equipamento	
Configuração do Teste		Demonstrar vip e ip pool	
Procedimento do Teste		Firewall objects -> virtual IPs	
Evidências			
Comentário			
Assinatura do Cliente		Assinatura NCT	

Item de Teste - 1.7.2.8.6		Tradução de porta (PAT);	
Objetivo do Teste		Demonstrar uso de nat no equipamento	
Configuração do Teste		Demonstrar ip pool	
Procedimento do Teste		Firewall objects -> virtual IPs ->Port Forwarding	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.2.8.7		NAT de origem;	
Objetivo do Teste		Demonstrar uso de nat no equipamento	
Configuração do Teste		Demonstrar ip pool	
Procedimento do Teste		Firewall objects -> virtual IPs	
Evidências			
Comentário			

Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.2.8.8		NAT de destino;	
Objetivo do Teste		Demonstrar uso de nat no equipamento	
Configuração do Teste		Demonstrar vip	
Procedimento do Teste		Firewall objects -> virtual IPs	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.2.8.9		Suportar NAT de origem e NAT de destino simultaneamente;	
Objetivo do Teste		Demonstrar uso de nat no equipamento	
Configuração do Teste		Demonstrar vip e ip pool	
Procedimento do Teste		Firewall objects -> virtual IPs	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.2.9		Enviar log para um ou mais sistemas de monitoramento de maneira simultânea	
Objetivo do Teste		Demonstrar envio de logs para monitoramento externo para mais de um servidor	
Configuração do Teste		Demonstrar syslog e opções de envio	
Procedimento do Teste		Repetir o procedimento para mais de um servidor de log	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.2.10		Deve haver a opção de enviar logs para os sistemas de monitoramento externos via protocolo TCP e SSL;	
Objetivo do Teste		Demonstrar envio de logs para monitoramento externo	
Configuração do Teste		Demonstrar syslog e opções de envio	
Procedimento do Teste		Demonstrar opções da configuração de syslog	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.2.12	Proteção contra anti-spoofing;
Objetivo do Teste	Demonstrar proteção solicitada
Configuração do Teste	Demonstrar mecanismo de anti-spoofing

Procedimento do Teste		Firewall object, policy	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.2.13		Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);	
Objetivo do Teste		Demonstrar suporte a roteamento dinâmico conforme solicitado no item	
Configuração do Teste		Demonstrar dynamic no fortigate	
Procedimento do Teste		Router -> dynamix -> ospf	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.2.14		Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);	
Objetivo do Teste		Demonstrar suporte a OSPF v6	
Configuração do Teste		Demonstrar suporte a OSPF v6	
Procedimento do Teste		Demonstrar configurações de OSPF com IPv6	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.2.15		Suportar a OSPF graceful restart;	
Objetivo do Teste		Demonstrar suporte a OSPF gracefull	
Configuração do Teste		Demonstrar suporte a OSPF gracefull	
Procedimento do Teste		Demonstrar configuralções de OSPF	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.2.16	Suportar, no mínimo, as seguintes funcionalidades em IPv6: SLAAC (Address Auto Configuration), NAT64, identificação de usuários a partir do LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, regras de proteção contra DoS (Denial of Service), decriptografia SSL, PBF (Policy Based Forwarding), QoS, DHCPv6 relay, SNMP, NTP, SYSLOG, DNS e controle de aplicação;
Objetivo do Teste	Demonstrar suporte aos itens solicitados em ipv6
Configuração do Teste	Demonstrar suporte aos itens solicitados em ipv6
Procedimento do Teste	Demonstrar suporte aos itens solicitados em ipv6

Evidências			
Comentário			
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		**Assinatura NCT**	

do Cliente			

Item de Teste - 1.7.2.21		As funcionalidades de controle de aplicações, VPN IPSec e SSL, QoS, SSL decryptione protocolos de 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.	
Objetivo do Teste		Conforme proposta técnica.	
Configuração do Teste			
Procedimento do Teste			
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 - 1.7.3.3		Controle de políticas por usuários, grupos de usuários, IPs e redes;	
Objetivo do Teste		Demonstrar possibilidade de administração de usuários, grupo, ips e redes	
Configuração do Teste		Demonstrar formas de administração do firewall	
Procedimento do Teste		Firewall objects, address, policy	
Evidências			
Comentário			

Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.3.4		Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (inbound) e saída (outbound).	
Objetivo do Teste		Demonstrar decriptografia de dados	
Configuração do Teste		Demonstrar decriptografia de dados ssl	
Procedimento do Teste		Demonstrar uso de ssl inspection	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.3.5		Deve de-criptografar tráfego inbound e outbound em conexões negociadas com TLS 1.2;	
Objetivo do Teste		Demonstrar decriptogrfia de dados	
Configuração do Teste		Demonstrar decriptogravia de TLS	
Procedimento do Teste		Demonstrar uso de dee p inspection	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.3.6		Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, pif, e reg;	
Objetivo do Teste		Demonstrar bloqueio de arquivos.	
Configuração do Teste		Demonstrar funcionalidades de antitivus	
Procedimento do Teste		Security profile -> antivirus	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.3.7		QoS baseado em políticas (prioridade, garantia e máximo);	
Objetivo do Teste		Demonstrar uso de QoS	
Configuração do Teste		Demonstrar uso de diffserv	
Procedimento do Teste		Demonstrar diffserv	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.3.8	QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações;
Objetivo do Teste	Demonstrar uso de QoS

Configuração do Teste		Demonstrar uso de diffserv	
Procedimento do Teste		Demonstrar diffserv	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.3.9		Suporte a objetos e regras IPv6;	
Objetivo do Teste		Demonstrar suporte a ipv6	
Configuração do Teste		Demonstrar suporte a ipv6	
Procedimento do Teste		Demonstrar suporte a ipv6	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.3.10		Suporte a objetos e regras multicast;	
Objetivo do Teste		Demonstrar suporte a regras multicast	
Configuração do Teste		Demonstrar suporte a regras multicast	
Procedimento do Teste		Policy -> multicast policy	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.3.11		Suportar o agendamento de políticas para que sejam habilitadas ou desabilitadas conforme horário pré-definido;	
Objetivo do Teste		Demonstrar controle de regras por horários	
Configuração do Teste		Demonstrar schedule	
Procedimento do Teste		Firewall object -> schedule	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.4.1.	Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:
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		Demonstrar application control	
Procedimento do Teste		Security profiles -> application control	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.4.1.3		Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, msrdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;	
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 - 1.7.4.1.4	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	Demonstrar application control

Procedimento do Teste		Security profiles -> application control	
Evidências			
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		Demonstrar uso de ips com analise comportamental	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.4.1.6		Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que se utilizam de táticas evasivas via comunicações criptografadas, tais como Skype e ataques mediante a porta 443;	
Objetivo do Teste		Demonstrar uso de decriptografia de dados	
Configuração do Teste		Demonstrar uso de ssl inspection	
Procedimento do Teste		Demonstrar ssl inspection em regra de firewall	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.4.1.7		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 uso de decriptografia de dados	
Configuração do Teste		Demonstrar uso de ssl inspection	
Procedimento do Teste		Demonstrar ssl inspection em regra de firewall	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.4.1.8	Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do mesmo, validando se o tráfego atende às suas especificações, 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 possibilidade de mitigação de trafego	
Configuração do Teste		Demonstrar uso de deep inspection no application control	
Procedimento do Teste		Demonstrar application control com deep inspection em regra de firewall.	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.4.1.9		Identificar o uso de táticas evasivas via comunicações criptografadas;	
Objetivo do Teste		Demonstrar possibilidade de mitigação de trafego criptografado	
Configuração do Teste		Demonstrar uso de ssl inspection	
Procedimento do Teste		Demonstrar uso de ssl inspection em regra de firewall	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.4.1.10		Atualizar a base de assinaturas de aplicações automaticamente;	
Objetivo do Teste		Demonstrar atualização de base de assinaturas	
Configuração do Teste		Demonstrar base da fortiguard	
Procedimento do Teste		System -> config -> fortiguard	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.4.1.12		Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseando-se no IP de origem, usuários e grupos do LDAP/AD;	
Objetivo do Teste		Demonstrar controle de aplicação com traffic shaper	
Configuração do Teste		Demonstrar traffic shaper com autenticação em regra de firewall	
Procedimento do Teste		Demonstrar criação de traffic shaper mais autenticação mais regra de firewall.	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.4.1.16	Para manter a segurança da rede eficiente, deve suportar o

	controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;		
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 - 1.7.4.1.19	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	Demonstrar application control		
Procedimento do Teste	Security profiles -> application control		
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.4.1.20	Deve ser possível a criação de grupos estáticos e dinâmicos de aplicações, baseando-se em suas características, tais como:		
Objetivo do Teste	Demonstrar conforme solicitado.		
Configuração do Teste			
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.4.1.21	Tecnologia utilizada nas aplicações (client-server, browser based, Network Protocol e etc.);		
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 - 1.7.4.1.21.2	Nível de risco da aplicação;
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 - 1.7.4.1.21.3		Categoria e subcategoria 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 - 1.7.4.1.21.4		Aplicações que usem técnicas evasivas, utilizadas por malwares, como transferência de arquivos e/ou uso excessivo de banda.	
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 - 1.7.5.1		Suportar VPN site-to-site e client-to-site;	
Objetivo do Teste		Demonstrar suporte a vpn site-to-site e client-to-site	
Configuração do Teste		Demonstrar configuração de vpn site-to-site e client-to-site	
Procedimento do Teste		Demonstrar criação de vpn site-to-site e client-to-site	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.5.2		Suportar IPSec VPN;	
Objetivo do Teste		Demonstrar suporte a vpn ipsec	
Configuração do Teste		Demonstrar configuração de vpn ipsec	
Procedimento do Teste		Demonstrar criação de vpn ipsec	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.5.3	Suportar SSL VPN;

Objetivo do Teste		Demonstrar suporte a vpn ssl	
Configuração do Teste		Demonstrar configuração de vpn ssl	
Procedimento do Teste		Demonstrar criação de vpn ssl	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.5.4		A VPN IPSec deve suportar:	
Objetivo do Teste		Demonstrar conforme solicitado.	
Configuração do Teste			
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.5.4.1		3DES;	
Objetivo do Teste		Demonstrar criptografia	
Configuração do Teste		Demonstrar uso de criptografia na VPN	
Procedimento do Teste		Criar configuração de criptografia na VPN	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.5.4.2		Autenticação MD5 e SHA1;	
Objetivo do Teste		Demonstrar modos de autenticação	
Configuração do Teste		Demonstrar o uso de autenticação MD5 e SHA1	
Procedimento do Teste		Criar configuração de autenticação da VPN	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.5.4.3		Diffie-Hellman grupo 1, grupo 2, grupo 5 e grupo 14;	
Objetivo do Teste		Demonstrar criptografia	
Configuração do Teste		Demonstrar uso de criptografia na VPN	
Procedimento do Teste		Criar configuração de criptografia na VPN	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.5.4.4	Algoritmo Internet Key Exchange (IKE);

Objetivo do Teste		Demonstrar o uso de chaves IKE	
Configuração do Teste		Demonstrar uso de chaves IKE na VPN	
Procedimento do Teste		Demonstrar uso de chaves IKE na VPN	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.5.4.5		AES 128 e 256 (Advanced Encryption Standard)	
Objetivo do Teste		Demonstrar criptografia	
Configuração do Teste		Demonstrar uso de AES 128 e 256	
Procedimento do Teste		Demonstrar uso de AES 128 e 256 na VPN	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.5.4.6		Autenticação via certificado IKE PKI;	
Objetivo do Teste		Demonstrar uso de autenticação com certificados	
Configuração do Teste		Demonstrar uso de certificados	
Procedimento do Teste		Demonstrar uso de certificados na VPN	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.5.5		Deve possuir interoperabilidade com os seguintes fabricantes:	
Objetivo do Teste		Demonstrar conforme solicitado.	
Configuração do Teste			
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.5.5.1		Cisco	
Objetivo do Teste		Não se aplica - equipamento segue RFCs	
Configuração do Teste			
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.5.5.2	Checkpoint

Objetivo do Teste		Não se aplica - equipamento segue RFCs	
Configuração do Teste			
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.5.5.3		Juniper;	
Objetivo do Teste		Não se aplica - equipamento segue RFCs	
Configuração do Teste			
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.5.5.4		Palo Alto Networks;	
Objetivo do Teste		Não se aplica - equipamento segue RFCs	
Configuração do Teste			
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.5.5.5		Fortinet;	
Objetivo do Teste		Não se aplica - equipamento segue RFCs	
Configuração do Teste			
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.5.5.6		Sonic Wall;	
Objetivo do Teste		Não se aplica - equipamento segue RFCs	
Configuração do Teste			
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.5.6	A VPN SSL deve suportar

Objetivo do Teste		Demonstrar conforme solicitado.	
Configuração do Teste			
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.5.6.1		Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface web;	
Objetivo do Teste		Demonstrar opção de uso de vpn com e sem agente	
Configuração do Teste		Demonstrar cliente de vpn instalado e no browser	
Procedimento do Teste		Demonstrar cliente de vpn instalado e no browser	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.5.6.2		As funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;	
Objetivo do Teste		Demonstrar opção de uso de ssl vpn com e sem agente	
Configuração do Teste		Demonstrar opção de uso de ssl vpn com e sem agente	
Procedimento do Teste		Demonstrar cliente ssl instalado e no browser	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.5.6.3		Atribuição de endereço IP nos clientes remotos de VPN;	
Objetivo do Teste		Demonstrar atribuição de IP aos clientes de vpn	
Configuração do Teste		Configurar um cliente de vpn	
Procedimento do Teste		Demonstrar as configurações no cliente de vpn	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.5.6.4		Atribuição de DNS nos clientes remotos de VPN;	
Objetivo do Teste		Demonstrar atribuição de dns aos clientes de vpn	
Configuração do Teste		Configurar um cliente de vpn	
Procedimento do Teste		Demonstrar as configurações no cliente de vpn	
Evidências			
Comentário			
Assinatura		**Assinatura NCT**	

do Cliente			

Item de Teste - 1.7.5.6.5		Deve haver a opção de ocultar o agente de VPN instalado no cliente remoto, tornando o mesmo invisível para o usuário;	
Objetivo do Teste		Demonstrar ocultação de cliente de vpn	
Configuração do Teste		Demonstrar ocultação de cliente de vpn	
Procedimento do Teste		Demonstrar cliente oculto no s.o.	
Evidências			
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		Demonstrar como as regras de firewall estão integradas as features de UTM e VPN	
Procedimento do Teste		Demonstrar habilitação de features de UTM nas regras de VPN	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.5.6.7		A VPN SSL deve suportar proxy ARP e uso de interfaces PPPoE;	
Objetivo do Teste		Demonstrar os itens solicitados	
Configuração do Teste		Demonstrar o suporte ao uso de arp e PPPoE	
Procedimento do Teste		Demonstrar o suporte ao uso de arp e PPPoE	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.5.6.8		Suportar autenticação via AD/LDAP, Secure ID, certificado e base de usuários local;	
Objetivo do Teste		Demonstrar diferentes formas de autenticação externa	
Configuração do Teste		Demonstrar diferentes formas de autenticação externa	
Procedimento do Teste		Demonstrar a configuração de conexão atraves de ldap certificados e base local	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.5.6.9	Permitir que se estabeleça um túnel VPN client-to-site do cliente

		com a plataforma de segurança, fornecendo uma solução de single-signon aos usuários, integrando-se com as ferramentas de WindowsLogon;	
Objetivo do Teste		Demonstrar integração de login de usuários	
Configuração do Teste		Demonstrar single signon em uso	
Procedimento do Teste		Demonstrar single signon em uso	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.5.6.10	Suporta leitura e verificação de CRL (Certificate Revocation List);	
Objetivo do Teste	Demonstrar a possibilidade de leitura de CRLs	
Configuração do Teste	Demonstrar a opção de certificates do fortigate	
Procedimento do Teste	Demonstrar a opção de leitura de listas de revogação de certificados.	
Evidências		
Comentário		
Assinatura do Cliente	**Assinatura NCT**	

Item de Teste - 1.7.5.6.11	Permite a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;	
Objetivo do Teste	Demonstrar opção de ssl inspection	
Configuração do Teste	Demonstrar ssl inspection	
Procedimento do Teste	Habilitar ssl inspection em regra de firewall	
Evidências		
Comentário		
Assinatura do Cliente	**Assinatura NCT**	

Item de Teste - 1.7.5.6.12	O agente de VPN a ser instalado nos equipamentos desktop e laptops, deve ser capaz de ser distribuído de maneira automática via Microsoft SMS, Active Directory e ser descarregado diretamente desde o seu próprio portal, o qual residirá no centralizador de VPN;	
Objetivo do Teste	Gerar .msi e demonstrar download de cliente	
Configuração do Teste	Gerar .msi e demonstrar download de cliente	
Procedimento do Teste	Verificar arquivo .msi e realizar download do cliente no portal.	
Evidências		
Comentário		
Assinatura do Cliente	**Assinatura NCT**	

Item de Teste - 1.7.5.6.13	O agente deverá comunicar-se com o portal para determinar

		as políticas de segurança do usuário;	
Objetivo do Teste		Demonstrar controle de políticas entre o clientes vpn e concentrador de vpn	
Configuração do Teste		Demonstrar como são construidas as regras de acesso vpn	
Procedimento do Teste		Firewall -> criar nova regra para vpn	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.5.6.14		Deve permitir que a conexão com a VPN SSL seja estabelecida das seguintes formas:	
Objetivo do Teste		Demonstrar conforme solicitado.	
Configuração do Teste			
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.5.6.14.1		Antes do usuário autenticar na estação;	
Objetivo do Teste		Demonstrar conexão automática do cliente de vpn	
Configuração do Teste		Instalar cliente de VPN no S.O.	
Procedimento do Teste		Após instalação o cliente deve se conectar automaticamente a VPN sem o usuário logar na estação de trabalho.	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.5.6.14.2		Após autenticação do usuário na estação	
Objetivo do Teste		Demonstrar conexão automática do cliente de vpn	
Configuração do Teste		Instalar cliente de VPN no S.O.	
Procedimento do Teste		Após instalação o cliente deve se conectar automaticamente a VPN quando o usuário logar na estação de trabalho.	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.5.6.14.3	Sob demanda do usuário;
Objetivo do Teste	Demonstrar conexão do cliente de vpn
Configuração do Teste	Instalar cliente de VPN no S.O.
Procedimento do Teste	Após instalação o cliente deve se conectar a VPN quando for solicitado pelo usuário.

Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.5.6.15		Deverá manter uma conexão segura com o portal durante a sessão;	
Objetivo do Teste		Demonstrar conexão segura	
Configuração do Teste		Acessar via browser o fortimanager	
Procedimento do Teste		Visualizar o certificado emitido e assinado	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.6.3		O gerenciamento deve permitir ou possuir:	
Objetivo do Teste		Demonstrar conforme solicitado.	
Configuração do Teste			
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.6.3.1		Criação e administração de políticas de firewall e controle de aplicação;	
Objetivo do Teste		Demonstrar opção de manipular regras de firewall e controle de aplicações	
Configuração do Teste		Acessar policy e objects	
Procedimento do Teste		Demonstrar manipulação do pacote de regras.	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.6.3.2		Criação e administração de políticas de IPS, antivírus e anti-spyware;	
Objetivo do Teste		Demonstrar opção de manipular regras de ips e antivirus	
Configuração do Teste		Acessar policy e objects	
Procedimento do Teste		Demonstrar manipulação do pacote de regras.	
Evidências			
Comentário			
Assinatura		**Assinatura NCT**	

do Cliente			

Item de Teste - 1.7.6.3.3		Criação e administração de políticas de filtro de URL;	
Objetivo do Teste		Demonstrar opção de manipular regras de filtragem web	
Configuração do Teste		Acessar policy e objects	
Procedimento do Teste		Demonstrar manipulação do pacote de regras.	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.6.3.4		Monitoramento de logs;	
Objetivo do Teste		Demonstrar logs de auditoria do fortimanager	
Configuração do Teste		Acessar system settings	
Procedimento do Teste		Explorar os logs	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.6.3.5		Ferramentas de investigação de logs;	
Objetivo do Teste		Demonstrar logs de auditoria do fortimanager	
Configuração do Teste		Acessar system settings	
Procedimento do Teste		Explorar os logs	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.6.3.6		Recursos para troubleshooting;	
Objetivo do Teste		Demonstrar sniffer	
Configuração do Teste		Acessar os logs e cli do equipamento	
Procedimento do Teste		Demonstrar uso do comando diagnose	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.6.3.7		Captura de pacotes;	
Objetivo do Teste		Demonstrar captura de pacotes	
Configuração do Teste		Acessar o equipamento e demonstrar capture packet	
Procedimento do Teste		Abrir o arquivo .pcap	
Evidências			
Comentário			
Assinatura		**Assinatura NCT**	

do Cliente			

Item de Teste - 1.7.6.3.8		Acesso concorrente de administradores	
Objetivo do Teste		Demonstrar a possibilidade de mais de um administrador logar no equipamento ao mesmo tempo	
Configuração do Teste		Abrir duas estâncias no fortimanager	
Procedimento do Teste		Demonstrar mais de um administrador logado	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.6.3.9		Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;	
Objetivo do Teste		Demonstrar auto help do cli	
Configuração do Teste		Acessar device manager	
Procedimento do Teste		Acessar confurations -> cli	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.6.3.10		Deve permitir usar palavras-chave e cores para facilitar a identificação de regras;	
Objetivo do Teste		Criar objeto com os itens solicitados	
Configuração do Teste		Acessar policy e objects no fortimanager	
Procedimento do Teste		Firewall object -> address	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.6.3.11		Deve permitir monitorar via SNMP falhas de hardware, inserção ou remoção de fontes de alimentação, discos e coolers, uso de recursos por número elevado de sessões, número de túneis estabelecidos na VPN cliente-to-site e número de sessões estabelecidas;	
Objetivo do Teste		Demonstrar monitoramento ativo	
Configuração do Teste		Acessar system settings	
Procedimento do Teste		System settings -> advanced -> snmp	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.6.3.12		Bloqueio de "commit" das configurações do firewall, no caso de acesso simultâneo de dois ou mais administradores;	
Objetivo do Teste		Demonstrar possibilidade de bloquear a gerencia para apenas 1 administrador	
Configuração do Teste		Acessar device manager	
Procedimento do Teste		Colocar objeto em estado de lock	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.6.3.13		Definição de perfis de acesso na console com permissões granulares, tais como: acesso de escrita, acesso de leitura, criação de usuários e alteração de configurações;	
Objetivo do Teste		Demonstrar granularidade de profiles para acesso	
Configuração do Teste		Acessar system settings no fortimanager	
Procedimento do Teste		System settings -> admin -> profile	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.6.3.14		Autenticação integrada ao Microsoft Active Directory e servidor RADIUS;	
Objetivo do Teste		Demonstrar autenticação com base externa	
Configuração do Teste		Acessar o system manager do fortimanager	
Procedimento do Teste		Admin -> remote auth server	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.6.3.15		Localização de em quais regras um endereço IP, IP range, subnet ou objetos estão sendo utilizados;	
Objetivo do Teste		Localizar objetos criados	
Configuração do Teste		Fazer uso do reference de objetos	
Procedimento do Teste		Objects -> busca	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.6.3.16	Deve atribuir sequencialmente um número a cada regra de firewall, NAT, QoS e regras de DOS;
Objetivo do Teste	Demonstrar possibilidades de visualizações dos itens solicitados

Configuração do Teste		Acessar policy objects no fortimanager	
Procedimento do Teste		Demonstrar policy em policy e objects	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.6.3.17		Criação de regras que fiquem ativas em horário definido;	
Objetivo do Teste		Demonstrar schedule de regra	
Configuração do Teste		Acessar policy e objects no fortimanager	
Procedimento do Teste		Criar nova regra com schedule	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.6.3.18		Criação de regras com data de expiração;	
Objetivo do Teste		Demonstrar schedule de regra	
Configuração do Teste		Acessar policy e objects no fortimanager	
Procedimento do Teste		Criar nova regra com schedule	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.6.3.19		Backup das configurações e rollback de configuração para a última configuração salva;	
Objetivo do Teste		Demonstrar rollback de configurações	
Configuração do Teste		Demonstrar revision de configurações	
Procedimento do Teste		Device manager -> configurations	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.6.3.20		Suportar rollback de sistema operacional para a última versão local;	
Objetivo do Teste		Demonstrar a possibilidade de rollback	
Configuração do Teste		Apresentar device manager no fortimanager	
Procedimento do Teste		Demonstrar o firmware management	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.6.3.21		Habilidade de upgrade via SCP, TFTP e interface de gerenciamento;	
Objetivo do Teste		Demonstrar formas de upgrade de firmware	
Configuração do Teste		Realizar upgrade de firmware	
Procedimento do Teste		Utilizar os métodos solicitados para upgrade de firmware	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.6.3.22		Validação de regras antes da aplicação;	
Objetivo do Teste		Demonstrar validação de regras	
Configuração do Teste		Acessar policy e objects	
Procedimento do Teste		Usar policy check no pacote de regras	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.6.10		Geração de relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego gerado;	
Objetivo do Teste		Demonstrar mapas com visualização de trafégo	
Configuração do Teste		Demonstrar mapas com visualização de trafégo	
Procedimento do Teste		Demonstrar mapa de ameaças	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.6.11		Deve prover relatórios com visão correlacionada de aplicações, e filtro de arquivos, para melhor diagnóstico e resposta a incidentes;	
Objetivo do Teste		Demonstrar relatórios	
Configuração do Teste		Acessar reports no fortimanager	
Procedimento do Teste		Acessar reports no fortimanager criar relatório customizado	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.6.12	O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelo dispositivo de segurança;

Objetivo do Teste		Demonstrar logs acumulados	
Configuração do Teste		Apresentar a visualização do fortiview	
Procedimento do Teste		Fortiview->log view	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.6.13		Deve possuir relatórios de utilização dos recursos por aplicações, filtro de arquivos, etc.;	
Objetivo do Teste		Demonstrar relatórios	
Configuração do Teste		Acessar reports no fortimanager	
Procedimento do Teste		Acessar reports no fortimanager criar relatório customizado	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.6.14		Prover uma visualização sumarizada de todas as aplicações, que passaram pela solução;	
Objetivo do Teste		Demonstrar visão de aplicações	
Configuração do Teste		Acessar fortiview no fortiamanger	
Procedimento do Teste		Acessar fortiview -> application e websites -> top applications	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.6.20		Exibição das seguintes informações, de forma histórica e em tempo real (atualizado de forma automática e contínua a cada 1 minuto):	
Objetivo do Teste		Demonstrar conforme solicitado.	
Configuração do Teste			
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.6.20.1	Situação do dispositivo e do cluster;
Objetivo do Teste	Demonstrar status de cluster
Configuração do Teste	Acessar device manager do fortimanager
Procedimento do Teste	Acessar device manager
Evidências	
Comentário	

Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.6.20.2		Principais aplicações;	
Objetivo do Teste		Demonstrar informações de aplicações	
Configuração do Teste		Acessar fortiview no fortimanger	
Procedimento do Teste		Acessar applications	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.6.20.3		Principais aplicações por risco;	
Objetivo do Teste		Demonstrar informações de aplicações	
Configuração do Teste		Acessar fortiview no fortimanger	
Procedimento do Teste		Acessar threats	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.6.20.4		Administradores autenticados na gerência da plataforma de segurança;	
Objetivo do Teste		Demonstrar informações de usuários	
Configuração do Teste		Acessar system settings no fortimanager	
Procedimento do Teste		Acessar system settings -> event log -> filtrar se necessário.	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.6.20.5		Número de sessões simultâneas;	
Objetivo do Teste		Demonstrar número de sessões	
Configuração do Teste		Acessar fortiview no fortimanager	
Procedimento do Teste		Acessar traffic	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.6.20.6	Status das interfaces;
Objetivo do Teste	Demonstrar status de interface.
Configuração do Teste	Acessar device manager
Procedimento do Teste	Verificar status de interfaces em devices e groups
Evidências	

Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.6.20.7		Uso de CPU;	
Objetivo do Teste		Demonstrar uso de CPU	
Configuração do Teste		Acessar fortiview no fortimanager	
Procedimento do Teste		Acessar fortiview -> system -> resource usage	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.6.21		Geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:	
Objetivo do Teste		Demonstrar conforme solicitado.	
Configuração do Teste			
Procedimento do Teste			
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.6.21.1		Resumo gráfico de aplicações utilizadas;	
Objetivo do Teste		Demonstrar relatório de aplicações	
Configuração do Teste		Acessar o a aba report do Fortiamanger	
Procedimento do Teste		Gerar relatório de application	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.6.21.2		Principais aplicações por utilização de largura de banda de entrada e saída;	
Objetivo do Teste		Demonstrar relatório de aplicações	
Configuração do Teste		Acessar o a aba report do Fortiamanger	
Procedimento do Teste		Gerar relatório de application e usage	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.6.21.3	Principais aplicações por taxa de transferência de bytes;
Objetivo do Teste	Demonstrar relatório de aplicações
Configuração do Teste	Acessar o a aba report do Fortiamanger

Procedimento do Teste		Gerar relatório de application e bandwidh	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.6.21.4		Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas;	
Objetivo do Teste		Demonstrar relatório de usuários e aplicações	
Configuração do Teste		Acessar o a aba report do Fortiamanger	
Procedimento do Teste		Gerar relatório customizado	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.6.21.5		Deve permitir a criação de relatórios personalizados;	
Objetivo do Teste		Demonstrar relatório	
Configuração do Teste		Acessar o a aba report do Fortiamanger	
Procedimento do Teste		Gerar relatório customizado	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.6.22		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 filtragem em logs	
Configuração do Teste		Acessar fortiview no fortimanager	
Procedimento do Teste		Acessar o log view e filtrar entradas.	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.6.23		Gerar alertas automáticos via:	
Objetivo do Teste		Demonstrar conforme solicitado.	
Configuração do Teste			
Procedimento do Teste			
Evidências			
Comentário			
Assinatura		**Assinatura NCT**	

do Cliente			

Item de Teste - 1.7.6.23.1		E-mail;	
Objetivo do Teste		Demonstrar envio de email como alerta	
Configuração do Teste		Configurar o Demonstrar alert mail	
Procedimento do Teste		Demonstrar alert mail	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.6.23.2		SNMP;	
Objetivo do Teste		Demonstrar opção de configuração de SNMP	
Configuração do Teste		Acessar system settings do fortimanager	
Procedimento do Teste		Acessar advanced -> snmp	
Evidências			
Comentário			
Assinatura do Cliente		**Assinatura NCT**	

Item de Teste - 1.7.6.23.3	Syslog;
Objetivo do Teste	Demonstrar opção de configuração de syslog
Configuração do Teste	Acessar system settings do fortimanager
Procedimento do Teste	Acessar advanced -> syslog server
Evidências	
Comentário	