

AVALIAÇÃO DE PROJETOS BÁSICOS - PB - EDITAIS

ANEXO "D" DO TERMO DE REFERÊNCIA

MODELO DE COMPROVAÇÃO PONTUAL DE ATENDIMENTO À ESPECIFICAÇÃO TÉCNICA

Lote	Item do Lote	Item	Descrição do Item	Atende	Referência/Documento	Página	Observações	Análise do grupo técnico
2	1 a 35	2.1	Requisitos gerais comuns a todos os Firewalls multifuncionais dos lotes 1,2,3,4 e 5					
2	1 a 35	2.1.1	Todos os equipamentos firewall e a solução de gerência integrada devem ser do mesmo fabricante, inclusive os sistemas operacionais executados por esses equipamentos, observado, o disposto no item 2.1.10.	Sim	fortiOS_S4.pdf	1,7	FortiOS 5.4 is an intuitive operative system that can manage all your FortiGate platforms, including the capabilities and services. FortiOS 5.4 provides industry-leading protection, superior visibility and control, and extensive networking capabilities at very high throughput speeds. Central Management and Provisioning Central management support: FortiManager, FortiCloud hosted service, web service APIs Rapid deployment: install wizards, USB auto-install, local and remote script execution	OK
2	1 a 35	2.1.2.	Todos os equipamentos e seus componentes deverão ser novos, sem uso, e entregues em perfeito estado de funcionamento, sem marcas, amassados, arranhões ou outros problemas físicos, acondicionados em suas embalagens originais e acompanhados de todos os acessórios, cabos, conectores, kits de fixação, trilhos, fibras óticas (incluindo sua fusão, se necessário), patchcords, transceivers, etc, necessários às suas instalações e operação em rack de 19" padrão EIA-310. No caso dos lotes 1 e 2, firewall multifuncionais de 100 e 250 Mbps, poderá ser fornecido os insumos como bandejas para colocação dos mesmos em racks.	Sim	De acordo			OK
2	1 a 35	2.1.3.	Não serão aceitos equipamentos em modo End of Support durante a vigência da garantia e que estejam em modo End of Life no ato da assinatura da ata de registro de preços, não deixando de atender ao item 2.1.6 durante toda a vigência da garantia.	Sim	De acordo			OK
2	1 a 35	2.1.3.1.	A exigência acima encontra fundamento na necessidade que a Administração Pública tem de resguardar seus interesses, no sentido de estabelecer exigências mínimas objetivando evitar que ocorra aquisição de equipamentos que tenham o seu ciclo de vida descontinuado em um curto prazo ou para os quais não mais haja suporte técnico e atualizações antes do fim do período de garantia, que é de 60 (sessenta) meses.	Sim	De acordo			OK
2	1 a 35	2.1.3.2.	No ato da assinatura do contrato, caso o equipamento registrado em ata não atenda o disposto no item 2.1.3, poderá ser aceito equipamento de capacidade técnica igual ou superior, da mesma série ou linha ou família, desde que atenda a todos os requisitos técnicos dispostos no presente edital.	Sim	De acordo			OK
2	1 a 35	2.1.4.	O fabricante deverá atualizar firmwares e softwares da solução para novas versões durante toda a vigência da garantia.	Sim	Conforme Proposta			OK
2	1 a 35	2.1.5.	Todas as funcionalidades adquiridas de hardware e software devem operar conforme disposto neste Termo de Referência durante o prazo de garantia dos equipamentos, ou seja, o fornecedor deve garantir a atualização completa das funcionalidades no prazo referido, não sendo permitida a cobrança de quaisquer valores adicionais pelo uso dos hardwares e softwares para esse período. As funcionalidades deverão permanecer ativas, mesmo que não sejam atualizadas após o fim do prazo da garantia.	Sim	De acordo			OK
2	1 a 35	2.1.5.1.	Após o prazo da garantia, os equipamentos deverão permanecer com todas as funcionalidades operacionais, com as atualizações imediatamente anteriores a data final da garantia dos equipamentos.	Sim	De acordo			OK
2	1 a 35	2.1.5.2.	Somente a funcionalidade de filtro de conteúdo web poderá ser desativada ao final do prazo de garantia do equipamento, em razão de sua natureza técnica de acesso on-line as suas bases de dados.	Sim	De acordo			OK
2	1 a 35	2.1.5.3.	A garantia referida no item 2.1.5 terá início com a emissão do termo de recebimento definitivo da solução a ser gerado pela CONTRATANTE conforme disposto no item 12.4.	Sim	De acordo			OK
2	1 a 35	2.1.6.	As licenças de atualização de software (firmware ou drivers) e licenças de atualização de assinaturas deverão ser fornecidas pelo prazo mínimo de 60 (sessenta) meses, a contar da data do recebimento definitivo dos produtos, sem ônus adicional para as atualizações e seu uso.	Sim	De acordo			OK

Lote	Item do Lote	Item	Descrição do Item	Atende	Referência/Documento	Página	Observações	Análise do grupo técnico
2	1 a 35	2.1.7.	Todos os equipamentos devem funcionar com alimentação nominal de 100~120VAC e 210~230VAC e frequência de 50 ou 60 Hz, ou auto-ranging. Deverá vir acompanhado de cabo de alimentação com, no mínimo, 1,80m (6 pés), com plug tripolar 2P+T no padrão ABNT NBR 14136.	Sim	FortiGate_80E_Series.pdf Conforme Proposta	5	Dimensions and Power	OK
2	1 a 35	2.1.8.	O equipamento deve possuir 1 (uma) porta de console para configuração e gerenciamento por interface de linha de comando (CLI).	Sim	FortiGate_80E_Series.pdf	5	GE RJ45 Management	OK
2	1 a 35	2.1.8.1.	Deve ser fornecido pelo menos 1 (um) cabo conversor Serial para USB, compatível com a porta de console do equipamento.	Sim	De acordo			OK
2	1 a 35	2.1.9.	O equipamento deve ser fornecido com todas as suas portas de comunicação, interfaces e afins habilitadas, operacionais e sem custos adicionais, mesmo que para futuras utilizações do órgão ou entidade CONTRATANTE.	Sim	De acordo			OK
2	1 a 35	2.1.9.1.	A CONTRATADA deve entregar a quantidade de transceivers equivalente ao dobro da quantidade mínima de portas exigidas em cada lote conforme os itens 3.15.1.4, 3.22.1.4 e 3.29.1.4.	Sim	FortiGate_80E_Series.pdf Conforme Proposta	6	1 GE SFP RJ45 transceiver module FG-TRAN-GC 1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+ slots. 1 GE SFP SX Transceiver Module FG-TRAN-SX 1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots. 10 GE SFP+ transceiver module, short range FG-TRAN-SFP+SR 10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots.	OK
2	1 a 35	2.1.9.2.	Em caso de defeito ou mau funcionamento dos transceivers, estes devem estar cobertos pela garantia da solução.	Sim	De acordo			OK
2	1 a 35	2.1.10.	O equipamento deve ser fornecido em hardware dedicado tipo appliance ou chassi, com sistema operacional otimizado, do mesmo fabricante, para o uso como firewall corporativo multifuncional.	Sim	fortiOS_54.pdf FortiGate_28E_Series.pdf	15	FortiOS 5.4 is an intuitive operative system that can manage all your FortiGate platforms, including the capabilities and services. FortiOS 5.4 provides industry-leading protection, superior visibility and control, and extensive networking capabilities at very high throughput speeds.	OK
2	1 a 35	2.1.10.1.	Os equipamentos dos lotes 1, 2, 3 e 4 da solução ofertada, não deverão exceder, individualmente, 4 Unidades de Rack, sendo "caixas" únicas, sem empilhamentos.	Sim	FortiGate_80E_Series.pdf	5	Dimensions and Power Form Factor	OK
2	1 a 35	2.1.10.2.	O equipamento do lote 5 da solução ofertada, pode ser baseado em appliance ou chassi, deverá ter atestada, pelo fabricante, a compatibilidade entre os módulos e o chassi e deverá suportar agregação de enlaces multi-chassi (MC-LAG), segundo padrão IEEE 802.1ax.	Sim	De acordo			OK
2	1 a 35	2.1.11.	Deve possuir fonte(s) de energia atendendo aos itens 3.1.1.3, 3.8.1.3, 3.15.1.3, 3.22.1.3 e 3.29.1.3.	Sim	FortiGate_80E_Series.pdf	5	Dimensions and Power	OK
2	1 a 35	2.1.12.	Deve suportar topologias de cluster redundante de alta disponibilidade (failover) no mínimo aos pares, nos modos ativo-ativo e ativo-passivo, com sincronização, em tempo real, de configuração e de estados das sessões. No caso de falha de um dos equipamentos do cluster, não deverá haver perda das configurações e nem das sessões já estabelecidas e a transição entre os equipamentos deverá acontecer de forma transparente para o usuário.	Sim	fortios-handbook-54.pdf	1498-1499	The cluster uses the FGCP to select the primary unit, and to provide device, link and session failover. The FGCP also manages the two HA modes; active-passive (failover HA) and active-active (load balancing HA). Inside the cluster the individual FortiGates are called cluster units. These cluster units share state and configuration information. If one cluster unit fails, the other units in the cluster automatically replace that unit, taking over the work that the failed unit was doing. After the failure, the cluster continues to process network traffic and provide normal FortiGate services with virtually no interruption.	OK
2	1 a 35	2.1.13.	Deve suportar a implementação tanto em modo transparente (camada 2) quanto em modo gateway (camada 3).	Sim	fortios-handbook-54.pdf	234	NAT/Route Mode vs. Transparent Mode A FortiGate can operate in one of two modes: NAT/Route or Transparent. In NAT/Route mode, the most common operating mode, a FortiGate is installed as a gateway or router between two networks. In most cases, it is used between a private network and the Internet. This allows the FortiGate to hide the IP addresses of the private network using network address translation (NAT). NAT/Route mode is also used when two or more Internet service providers (ISPs) will provide the FortiGate with redundant Internet connections. A FortiGate in Transparent mode is installed between the internal network and the router. In this mode, the FortiGate does not make any changes to IP addresses and only applies security scanning to traffic. When a FortiGate is added to a network in Transparent mode, no network changes are required, except to provide the FortiGate with a management IP address. Transparent mode is used primarily when there is a need to increase network protection but changing the configuration of the network itself is impractical.	OK
2	1 a 35	2.1.14.	Possuir filtragem de pacote por endereço IP de origem e destino, por aplicação (independentemente da porta ou protocolo utilizados pela aplicação), por sub-rede e por períodos do dia, permitindo a aplicação de regras por horários e por dias da semana.	Sim	fortios-handbook-54.pdf	1020	Set the Source parameter by selecting the field with the "+" next to the field label. The source in this case is either the source address, source user or source device of the initiating traffic. When the field is selected a window will slide out from the right. Tabs indicating Address, User or Device options are there to help categorize the options along with the option to search. In order to be able to select one of these options it needs to be configured as a firewall object before hand. The "+" icon next to the Search field is a shortcut for creating a new firewall object based on the tab that is currently selected. For the Address and Device tabs, single or multiple options can be selected unless the all option is chosen in which case, it will be the only option. Set the Schedule parameter by using the drop down menu to select a preconfigured schedule. The "+" icon next to the Search field is a shortcut for creating a new schedule object. Set the Destination Address parameter by selecting the field with the "+" next to the field label. This field is similar to the Source field but address objects are the only available options to select. Single or multiple options can be selected unless the all option is chosen in which case, it will be the only option. Set the Service parameter by selecting the field with the "+" next to the field label. (Same mechanics for selection apply as with the other similar fields in this window.) Single or multiple options can be selected unless the ALL option is chosen in which case, it will be the only option.	OK
2	1 a 35	2.1.15.	Permitir criação de serviços por porta ou conjunto de portas para, no mínimo, os protocolos TCP, UDP, ICMP e IP.	Sim	fortios-handbook-54.pdf	952	Protocol Types One of the fundamental aspects of a service is the type of protocol that use used to define it. When a service is defined one of the following categories of protocol needs to be determined: I TCP/UDP/SCTP I ICMP I ICMP6 I IP	OK

Lote	Item do Lote	Item	Descrição do Item	Atende	Referência/Documento	Página	Observações	Análise do grupo técnico
2	1 a 35	2.1.16.	Suportar tags de VLAN;	Sim	fortios-handbook-54.pdf	2176	<p>Adding VLAN subinterfaces</p> <p>A VLAN subinterface, also called a VLAN, is a virtual interface on a physical interface. The subinterface allows routing of VLAN tagged packets using that physical interface, but it is separate from any other traffic on the physical interface.</p> <p>Adding a VLAN subinterface includes configuring:</p> <ul style="list-style-type: none"> Physical interface IP address and netmask VLAN ID VDOM 	OK
2	1 a 35	2.1.17.	Permitir a criação de no mínimo 25 VLANs padrão 802.1q para os firewalls especificados nos lotes 1, no mínimo 50 VLANs padrão 802.1q para os firewalls do lote 2 e no mínimo 500 VLANs padrão 802.1q para os firewalls especificados nos lotes 3, 4 e 5.	Sim	Maximum Values Table 80E.pdf	2	<p>Interfaces (VLAN + physical)</p>	OK
2	1 a 35	2.1.18.	Ser capaz de aceitar comandos de scripts acionados por sistemas externos como, por exemplo, correlacionadores de eventos;	Sim	fortios-handbook-54.pdf	2854-2855	<p>CLI Scripts</p> <p>To upload bulk CLI commands and scripts, go to System > Advanced.</p> <p>Scripts are text files containing CLI command sequences. Scripts can be used to deploy identical configurations to many devices. For example, if all of your devices use identical security policies, you can enter the commands required to create the security policies in a script, and then deploy the script to all the devices which should use those same settings. Use a text editor such as Notepad or other application that creates simple text files. Enter the commands in sequence, with each line as one command, similar to examples throughout the FortiOS documentation set.</p> <p>Uploading script files</p> <p>After you have created a script file, you can then upload it through System > Advanced. When a script is uploaded, it is automatically executed. Commands that require the FortiGate unit to reboot when entered in the command line will also force a reboot if included in a script.</p>	OK
2	1 a 35	2.1.19.	Suportar o bloqueio de tráfego em função da localização geográfica dos IPs de origem e de destino;	Sim	fortios-handbook-54.pdf	1020, 1045	<p>Set the Source parameter by selecting the field with the "+" next to the field label. The source in this case is either the source address, source user or source device of the initiating traffic. When the field is selected a window will slide out from the right. Tabs indicating Address, User or Device options are there to help categorize the options along with the option to search. In order to be able to select one of these options it needs to be configured as a firewall object before hand. The "+" icon next to the Search field is a shortcut for creating a new firewall object based on the tab that is currently selected. For the Address and Device tabs, single or multiple options can be selected unless the all option is chosen in which case, it will be the only option.</p> <p>Set the Destination Address parameter by selecting the field with the "+" next to the field label. This field is similar to the Source field but address objects are the only available options to select. Single or multiple options can be selected unless the all option is chosen in which case, it will be the only option. For more information on addresses, check the Firewall Objects section called Addresses.</p> <p>Geography Based Addresses</p> <p>Geography addresses are those determined by country of origin. This type of address is only available in the IPv4 address category.</p>	OK
2	1 a 35	2.1.20.	Suportar agregação de links, segundo padrão IEEE 802.3ad, nos equipamentos firewall descritos nos lotes 3, 4 e 5.	Sim	fortios-handbook-54.pdf	2148	<p>Aggregate Interfaces</p> <p>Link aggregation (IEEE 802.3ad) enables you to bind two or more physical interfaces together to form an aggregated (combined) link. This new link has the bandwidth of all the links combined. If a link in the group fails, traffic is transferred automatically to the remaining interfaces with the only noticeable effect being a reduced bandwidth.</p>	OK
2	1 a 35	2.1.21.	Possuir ferramenta de diagnóstico do tipo tcpdump.	Sim	fortios-handbook-54.pdf	2190, 3002	<p>Packet Capture</p> <p>When troubleshooting networks, it helps to look inside the header of the packets. This helps to determine if the packets, route, and destination are all what you expect. Packet capture can also be called a network tap, packet sniffing, or logic analyzing.</p> <p>To use the packet capture.</p> <ol style="list-style-type: none"> Go to Network > Packet Capture. Select Create New or select an existing entry if you've already made one that fits your needs. Select the interface to monitor and select the number of packets to keep. Select Enable Filters. Enter the information you want to gather from the packet capture. Select OK. <p>How do you sniff packets</p> <p>The general form of the internal FortiOS packet sniffer command is:</p> <pre>diag sniffer packet <interface_name> <'filter'> <verbose> <count></pre>	OK
2	1 a 35	2.1.21.1.	Suportar e efetuar a captura de pacotes no formato PCAP.	Sim	fortios-handbook-54.pdf	2969	<p>When the packet capture is complete, you can select Download to send the packet capture filter captured packets to your local computer as a *.pcap file.</p>	OK
2	1 a 35	2.1.21.2.	Suportar e efetuar o download dos arquivos PCAP.	Sim	fortios-handbook-54.pdf	2969	<p>When the packet capture is complete, you can select Download to send the packet capture filter captured packets to your local computer as a *.pcap file.</p>	OK
2	1 a 35	2.1.22.	Não deve possuir restrições de licenciamento em relação às características, requisitos e funcionalidades presentes nos subitens do item 2.1, inclusive em relação ao número ou tipo de clientes, usuários, máquinas e endereços IP.	Sim	fortigate-getting-started-54.pdf	70	<p>FortiGate platforms do not impose any limitations on the number or type of customers, users, devices, IP addresses, or number of VPN clients being served by the platform. Such factors are limited solely by the hardware capacity of each given model.</p>	OK
2	1 a 35	2.1.23.	Deve suportar, no próprio firewall, autenticação de usuários locais e integração com serviços de autenticação de diretório LDAP, Microsoft Active Directory e RADIUS, sendo que:	Sim	fortios-handbook-54.pdf	529,538	<p>Server-based password authentication</p> <p>Using external authentication servers is desirable when multiple FortiGate units need to authenticate the same users, or where the FortiGate unit is added to a network that already contains an authentication server. FortiOS supports the use of LDAP, RADIUS, TACACS+, AD or POP3 servers for authentication.</p> <p>Microsoft RADIUS servers</p> <p>Microsoft Windows Server 2000, 2003, and 2008 have RADIUS support built-in. Microsoft specific RADIUS features are defined in RFC 2548. The Microsoft RADIUS implementation can use Active Directory for user credentials.</p>	OK
2	1 a 35	2.1.23.1.	Não deverão existir limitações de licenciamento quanto ao número de usuários, a não ser o limite operacional do equipamento, respeitado o quantitativo mínimo especificado em cada lote;	Sim	fortigate-getting-started-54.pdf	70	<p>FortiGate platforms do not impose any limitations on the number or type of customers, users, devices, IP addresses, or number of VPN clients being served by the platform. Such factors are limited solely by the hardware capacity of each given model.</p>	OK

Lote	Item do Lote	Item	Descrição do Item	Atende	Referência/Documento	Página	Observações	Análise do grupo técnico
2	1 a 35	2.1.23.2.	Deve registrar a identificação do usuário em todos os eventos associados gerados pelo equipamento, tais como (mas não restrito a) eventos de autenticação, registros de acesso ou bloqueio e eventos associados a ameaças;	Sim	FortiOS-5.4.4-Log-Reference.pdf	60, 885-886	<p>Event Records system and administrative events, such as downloading a backup copy of the configuration, or daemon activities.</p> <p>I Compliance-check I Endpoint Control I High Availability I Router I System I User I Virtual Private Network (VPN) I WAD I Wireless</p> <p>28721 - LOGID_APP_CTRL_SSH_BLOCK Message ID: 28721 Message Description: LOGID_APP_CTRL_SSH_BLOCK Type: App Category: APP-CTRL-ALL Severity: Warning</p> <p>user User name string 256</p> <p>38031 - LOG_ID_FSSO_LOGON Message ID: Message Description: LOG_ID_FSSO_LOGON Type: Event Category: USER</p>	OK
2	1 a 35	2.1.23.3.	Deve prover identificação de forma transparente aos usuários autentica dos por single signon, no mínimo, por meio dos serviços Microsoft Active Directory e RADIUS;	Sim	fortios-handbook-54.pdf	531	<p>FSSO Fortinet Single Sign on (FSSO) provides seamless authentication support for Microsoft Windows Active Directory (AD) and Novell eDirectory users in a FortiGate environment.</p> <p>RADIUS SSO RADIUS Single Sign-On (RSSO) is a remote authentication method that does not require any local users to be configured, and relies on RADIUS Start records to provide the FortiGate unit with authentication information.</p>	OK
2							<p>16384 - LOGID_ATTCK_SIGNATURE_TCP_UDP Message ID: 16384 Message Description: LOGID_ATTCK_SIGNATURE_TCP_UDP Type: IPS Category: SIGNATURE Severity: Alert</p> <p>attackcontext the trigger patterns and the packetdata with base64 encoding user User name string 256</p>	OK
2	1 a 35	2.1.23.4.	Deve prover portal ou pop-up de login para identificação dos usuários dos demais serviços de LDAP não listados no item anterior;	Sim	fortios-handbook-54.pdf	606	<p>Introduction to Captive portals You can authenticate your users on a web page that requests the user's name and password. Until the user authenticates successfully, the authentication page is returned in response to any HTTP request. This is called a captive portal.</p> <p>After successful authentication, the user accesses the requested URL and can access other web resources, as permitted by security policies. Optionally, the captive portal itself can allow web access to only the members of specified user group.</p> <p>The captive portal can be hosted on the FortiGate unit or on an external authentication server. You can configure captive portal authentication on any network interface, including WiFi and VLAN interfaces.</p>	OK
2	1 a 35	2.1.23.5.	Deve permitir a criação de regras de acesso/bloqueio baseadas em usuários ou grupo de usuários do LDAP e do Microsoft Active Directory;	Sim	fortios-handbook-54.pdf	531,543	<p>FSSO Fortinet Single Sign on (FSSO) provides seamless authentication support for Microsoft Windows Active Directory (AD) and Novell eDirectory users in a FortiGate environment.</p> <p>Supported versions The FortiGate unit supports LDAP protocol functionality defined in RFC 2251: Lightweight Directory AccessProtocol v3, for looking up and validating user names and passwords. FortiGate LDAP supports all LDAP servers compliant with LDAP v3, including FortiAuthenticator. In addition, FortiGate LDAP supports LDAP over SSL/TLS, which can be configured only in the CLI.</p> <p>Set the Source parameter by selecting the field with the "+" next to the field label. The source in this case is either the source address, source user or source device of the initiating traffic.</p> <p>Set the Destination Address parameter by selecting the field with the "+" next to the field label. This field is similar to the Source field but address objects are the only available options to select.</p>	OK
2	1 a 35	2.1.23.6.	Não será permitida a utilização de agentes instalados nos equipamentos dos usuários;	Sim	fortios-handbook-54.pdf	529	<p>You can use external authentication servers in two ways: I Create user accounts on the FortiGate unit, but instead of storing each user's password, specify the server used to authenticate that user. As with accounts that store the password locally, you add these users to appropriate user groups. I Add the authentication server to user groups. Any user who has an account on the server can be authenticated and have the access privileges of the FortiGate user group. Optionally, when an LDAP server is a FortiGate user group member, you can limit access to users who belong to specific groups defined on the LDAP server.</p>	OK
2	1 a 35	2.1.23.7.	Possuir métodos de autenticação de usuários para aplicações executadas sobre os protocolos TCP, tais como (mas não restritos a) aplicações HTTP, HTTPS e FTP;	Sim	fortios-handbook-54.pdf	588-589	<p>Authentication protocols When user authentication is enabled on a security policy, the authentication challenge is normally issued for any of the four protocols, HTTP, HTTPS, FTP, and Telnet, which are dependent on the connection protocol. By making selections in the Protocol Support list, the user controls which protocols support the authentication challenge. The user must connect with a supported protocol first, so that they can subsequently connect with other protocols.</p>	OK

Lote	Item do Lote	Item	Descrição do Item	Atende	Referência/Documento	Página	Observações	Análise do grupo técnico
2	1 a 35	2.1.24.	Suportar Network Address Translation (NAT 1-1, NAT 1-N, NAT N-1) de acordo com a RFC 3022, nos modos estático e dinâmico;	Sim	fortios-handbook-54.pdf SupportedRFCs_FULL.pdf	7-938,94268	<p>Dynamic NAT Dynamic NAT maps the private IP addresses to the first available Public Address from a pool of possible Addresses. In the FortiGate firewall this can be done by using IP Pools.</p> <p>Overloading This is a form of Dynamic NAT that maps multiple private IP address to a single Public IP address but differentiates them by using a different port assignment. This is probably the most widely used version of NAT. This is also referred to as PAT (Port Address Translation) or Masquerading.</p> <p>Static NAT In Static NAT one internal IP address is always mapped to the same public IP address. In FortiGate firewall configurations this is most commonly done with the use of Virtual IP addressing.</p> <p>How FortiOS differentiates sessions when NATING The basics of NAT are fairly simple. Many private addresses get translated into a smaller number of public addresses, often just one. The trick is how the FortiGate keeps track of the return traffic because the web server, or what ever device that was out on the Internet is going to be sending traffic back not to the private address behind the FortiGate but to the IP address of the interface on the public side of the FortiGate.</p> <p>RFC 3022 Description: Traditional IP Network Address Translator (Traditional NAT). Category: VPN (IPsec, PPTP, L2TP) Webpage: http://tools.ietf.org/html/rfc3022 Obsoletes: RFC 1631</p>	OK
2	1 a 35	2.1.25.	Deve suportar no mínimo NAT 64.	Sim	fortios-handbook-54.pdf	941	I To create a NAT64 policy go to Policy > Policy > NAT64 Policy and select Create New.	OK
2	1 a 35	2.1.26.	Possuir a funcionalidade de fazer tradução de endereços dinâmicos um-para-N, PAT (Port Address Translation);	Sim	fortios-handbook-54.pdf	937	<p>Overloading This is a form of Dynamic NAT that maps multiple private IP address to a single Public IP address but differentiates them by using a different port assignment. This is probably the most widely used version of NAT. This is also referred to as PAT (Port Address Translation) or Masquerading.</p>	OK
2	1 a 35	2.1.27.	Suportar nativamente IPv6;	Sim	fortios-handbook-54.pdf	933-934	<p>IPv6 in FortiOS</p> <p>From an administrative point of view IPv6 works almost the same as IPv4 in FortiOS. The primary difference is the use IPv6 format for addresses. There is also no need for NAT if the FortiGate firewall is the interface between IPv6 networks. If the subnets attached to the FortiGate firewall are IPv6 and IPv4 NAT can be configured between the 2 different formats. This will involve either configuring a dual stack routing or IPv4 tunneling configuration. The reason for this is simple. NAT was developed primarily for the purpose of extending the number of usable IPv4 addresses. IPv6's addressing allows for enough available addresses so the NAT is no longer necessary.</p>	OK
2	1 a 35	2.1.27.1.	Suportar, no mínimo, os protocolos de roteamento dinâmico OSPF v3 e BGP, bem como as funcionalidades de roteamento estático e roteamento policy-based	Sim	fortios-handbook-54.pdf	1953, 3053	<p>BGP background and concepts The border gateway protocol contains two distinct subsets — internal BGP (iBGP) and external BGP (eBGP). iBGP is intended for use within your own networks. eBGP is used to connect many different networks together, and is the main routing protocol for the Internet backbone. FortiGate units support iBGP, and eBGP only for communities.</p> <p>OSPFv3 and IPv6 OSPFv3 (OSPF version 3) includes support for IPv6. Generally, all IP addresses are in IPv6 format instead of IPv4. However, OSPFv3 area numbers use the same 32-bit numbering system as OSPFv2, as described in RFC2740. Likewise, the router ID and area ID are in the same format as OSPFv2. As with most advanced routing features on your FortiGate unit, IPv6 settings for dynamic routing protocols must be enabled before they will be visible in the GUI. To enable IPv6 configuration in the GUI, enable it in System > Config > Features.</p> <p>Configuring static routing You need to define the route for traffic leaving the external interface. 1. Go to Network > Static Routes, select Create New. 2. Enter the following information. Destination IP/Mask Leave as 0.0.0.0 0.0.0.0. Device Select the external interface. Gateway Enter the IP address of the next hop router.</p> <p>Unicast Routing / Policy Based routing Yes</p>	OK
2	1 a 35	2.1.28.	Possuir funcionalidades de DHCP client, server e relay;	Sim	fortios-handbook-54.pdf	2151	<p>You can configure one or more DHCP servers on any FortiGate interface. A DHCP server dynamically assigns IP addresses to hosts on the network connected to the interface. The host computers must be configured to obtain their IP addresses using DHCP.</p> <p>You can configure a FortiGate interface as a DHCP relay. The interface forwards DHCP requests from DHCP clients to an external DHCP server and returns the responses to the DHCP clients. The DHCP server must have appropriate routing so that its response packets to the DHCP clients arrive at the unit.</p>	OK
2	1 a 35	2.1.29.	Possuir proteção e suporte a protocolos de Real Time, contemplando no mínimo: Real Time Transport Protocol (RTP), H323 e SIP sobre os protocolos IPV4 ou IPV6.	Sim	fortios-handbook-54.pdf	2,3204,3208	<p>H.323 and RAS session helpers (h323 and ras) The H.323 session helper supports secure H.323 voice over IP (VoIP) sessions between terminal endpoints such as IP phones and multimedia devices. In H.323 VoIP networks, gatekeeper devices manage call registration, admission, and call status for VoIP calls. The FortiOS h323 session helper supports gatekeepers installed on two different networks or on the same network.</p> <p>SIP and RTP/RTCP FortiGates support the Real Time Protocol (RTP) application layer protocol for the VoIP call audio stream. RTP uses dynamically assigned port numbers that can change during a call. SIP control messages that start a call and that are sent during the call inform callers of the port number to use and of port number changes during the call.</p> <p>To add security policies to apply the SIP ALG to SIP sessions 1. Go to Policy & Objects > IPv4 Policy. 2. Add a security policy to allow Phone A to send SIP request messages to Phone B</p>	OK

Lote	Item do Lote	Item	Descrição do Item	Atende	Referência/Documento	Página	Observações	Análise do grupo técnico
2	1 a 35	2.1.30.	Possuir tecnologia de firewall stateful;	Sim	fortios-handbook-54.pdf	926-927	<p>Stateful Firewalls</p> <p>Stateful firewalls retain packets in memory so that they can maintain context about active sessions and make judgments about the state of an incoming packet's connection. This enables Stateful firewalls to determine if a packet is the start of a new connection, a part of an existing connection, or not part of any connection. If a packet is part of an existing connection based on comparison with the firewall's state table, it will be allowed to pass without further processing. If a packet does not match an existing connection, it will be evaluated according to the rules set for new connections. Predetermined rules are used in the same way as a stateless firewall but they can now work with the additional criteria of the state of the connection to the firewall.</p>	OK
2	1 a 35	2.1.31.	Permitir a realização de backup e restore das regras, configurações e políticas, e a transferência desse backup para armazenamento em servidores externos;	Sim	fortios-handbook-54.pdf	301	<p>Configuration Backups</p> <p>Once you successfully configure the FortiGate, it is extremely important that you backup the configuration. In some cases, you may need to reset the FortiGate to factory defaults or perform a TFTP upload of the firmware, which will erase the existing configuration. In these instances, the configuration on the device will have to be recreated, unless a backup can be used to restore it. You should also backup the local certificates, as the unique SSL inspection CA and server certificates that are generated by your FortiGate by default are not saved in a system backup.</p> <p>It is also recommended that you backup the configuration after any future changes are made, to ensure you have the most current configuration available. Also, backup the configuration before any upgrades of the FortiGate's firmware. Should anything happen to the configuration during the upgrade, you can easily restore the saved configuration. Always backup the configuration and store it on the management computer or off-site. You have the option to save the configuration file to various locations including the local PC, USB key, FTP and TFTP site. The last two are configurable through the CLI only.</p>	OK
2	1 a 35	2.1.32.	Possuir funcionalidade de detecção e bloqueio de, no mínimo, os seguintes tipos de ataques: IP Spoofing, SYN Flood, UDP Flood, Port Scanning, ICMP Flood, ICMP sweep, Ataques de Força Bruta ataques Man-in-the-Middle e variações de reflexão;	Sim	fortios-handbook-54.pdf	2,2631,2988	<p>Reverse path lookup</p> <p>Whenever a packet arrives at one of the FortiGate unit's interfaces, the unit determines whether the packet was received on a legitimate interface by doing a reverse lookup using the source IP address in the packet header. This is also called anti-spoofing. If the FortiGate unit cannot communicate with the computer at the source IP address through the interface on which the packet was received, the FortiGate unit drops the packet as it is likely a hacking attempt.</p> <p>Configuring the SYN threshold to prevent SYN floods</p> <p>The preferred primary defence against any type of SYN flood is the DoS anomaly check for tcp_syn_flood threshold. The threshold value sets an upper limit on the number of new incomplete TCP connections allowed per second. If the number of incomplete connections exceeds the threshold value, and the action is set to Pass, the FortiGate unit will allow the SYN packets that exceed the threshold. If the action is set to Block, the FortiGate unit will block the SYN packets that exceed the threshold, but it will allow SYN packets from clients that send another SYN packet.</p> <p>Other flood types</p> <p>UDP and ICMP packets can also be used for DoS attacks, though they are less common. TCP SYN packets are so effective because the target receives them and maintains a session table entry for each until they time out. Attacks using UDP or ICMP packets do not require the same level of attention from a target, rendering them less effective. The target will usually drop the offending packets immediately, closing the session. Use the udp_flood and icmp_flood thresholds to defend against these DoS attacks.</p> <p>Address sweeps</p> <p>An address sweep is a basic network scanning technique to determine which addresses in an address range have active hosts. A typical address sweep involves sending an ICMP ECHO request (a ping) to each address in an address range to attempt to get a response. A response signifies that there is a host at this address that responded to the ping. It then becomes a target for more detailed and potentially invasive attacks. Address sweeps do not always reveal all the hosts in an address range because some systems may be configured to ignore ECHO requests and not respond, and some firewalls and gateways may be configured to prevent ECHO requests from being transmitted to the destination network. Despite this shortcoming, Address sweeps are still used because they are simple to perform with software tools that automate the process. Use the icmp_sweep anomaly in a DoS policy to protect against address sweeps.</p>	OK
2							<p>Rate-based IPS signatures protect networks against application-based DoS and brute force attacks. Administrators can configure nearly 30 rate-based IPS signatures and tune them to their needs. Threshold (incidents per minute) and an action to take when the threshold is reached can be assigned to each signature. If the action is set to block, then a timeout period can be set so that the block is removed after a specified duration.</p> <p>SSL inspection</p> <p>Secure Sockets Layer (SSL) content scanning and inspection allows you to apply antivirus scanning, web filtering, FortiGuard Web Filtering, and email filtering to encrypted traffic. To perform SSL content scanning and inspection, the FortiGate unit does the following:</p> <ul style="list-style-type: none"> Intercepts and decrypts HTTPS, IMAPS, POP3S, SMTPS, and FTPS sessions between clients and servers (FortiGate SSL acceleration speeds up decryption) Applies content inspection to decrypted content, including: <ul style="list-style-type: none"> HTTPS, IMAPS, POP3S, and SMTPS Antivirus, DLP, and DLP archiving HTTPS web filtering and FortiGuard web filtering IMAPS, POP3S, and SMTPS email filtering Encrypts the sessions and forwards them to their destinations. <p>SSL certificates validation</p> <p>Ping is part of Layer-3 on the OSI Networking Model. Ping sends Internet Control Message Protocol (ICMP) "echo request" packets to the destination, and listens for "echo response" packets in reply. However, many public networks block ICMP packets because ping can be used in a denial of service (DoS) attack (such as Ping of Death or a smurf attack), or by an attacker to find active locations on the network. By default, FortiGate units have ping enabled while broadcast-forward is disabled on the external interface.</p>	OK

Lote	Item do Lote	Item	Descrição do Item	Atende	Referência/Documento	Página	Observações	Análise do grupo técnico
2	1 a 35	2.1.33.	Suportar sincronização de horário por NTP;	Sim	fortios-handbook-54.pdf	2950-2951	<p>Check date and time</p> <p>The system date and time are important for FortiGuard services, when logging events, and when sending alerts. The wrong time will make the log entries confusing and difficult to use.</p> <p>Use Network Time Protocol (NTP) to set the date and time if possible. This is an automatic method that does not require manual intervention. However, you must ensure the port is allowed through the firewalls on your network.</p> <p>How to check the date and time - web-based manager</p> <ol style="list-style-type: none"> 1. Go to System Information > System Time on the dashboard. <p>Alternately, you can check the date and time using the CLI commands execute date and execute time.</p> <ol style="list-style-type: none"> 2. If required, select Change to adjust the date and time settings. <p>You can set the time zone, date and time, and select NTP usage. In the CLI, use the following commands to change the date and time:</p> <pre>config system global set timezone (use ? to get a list of IDs and descriptions of their timezone) end config system ntp set type custom config ntpserver edit 1 set server "ntp1.fortinet.net" next edit 2 set server "ntp2.fortinet.net" next end set ntpsync enable</pre>	OK
2	1 a 35	2.1.34.	Possuir funcionalidade de geração de relatórios e exportação de logs;	Sim	fortios-handbook-54.pdf	2048	<p>After a log message is recorded, it is stored within a log file which is then stored on a log device. A log device is a central storage location for log messages. The FortiGate unit supports several log devices, such as FortiAnalyzer units, the FortiCloud service, and Syslog servers. A FortiGate unit's system memory and local disk can also be configured to store logs, and because of this, are also considered log devices.</p> <p>When the recorded activity needs to be read in a more human way, the FortiGate unit can generate a Report. A report gathers all the log information that is needed for the report, and presents it in a graphical format, with customizable design and automatically generated charts.</p>	OK
2	1 a 35	2.1.35.	Suportar no mínimo 250 regras ou políticas de firewall para os equipamentos do lote 1 e 1.000 regras ou políticas de firewall para os equipamentos dos lotes 2,3,4 e 5.	Sim	Maximum Values Table 80E.pdf	4	Policies 5000	OK
2	1 a 35	2.1.36.	Permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;	Sim	fortios-handbook-54.pdf	1067,1076	<p>Services</p> <p>While there are a number of services already configured within FortiOS, the firmware allows for administrators to configure there own. The reasons for doing this usually fall into one or more of the following categories:</p> <ul style="list-style-type: none"> ! The service is not common enough to have a standard configuration ! The service is not established enough to have a standard configuration ! The service has a standard port number but there is a reason to use a different one: ! Port is already in use by another service ! For security reasons, want to avoid standard port <p>When looking at the list of preconfigured services it may seem like there are a lot, but keep in mind that the theoretical limit for port numbers is 65,535. This gives a fairly good sized range when you are choosing what port to assign a service but there are a few points to keep in mind.</p> <ul style="list-style-type: none"> ! Most of the well known ports are in the range 0 - 1023 ! Most ports assigned by the Internet Corporation for Assigned Names and Numbers (ICANN) will be in the 1024 -49151 range ! Port numbers between 49,152 and 65,535 are often used for dynamic, private or ephemeral ports. <p>Custom Services that need to be created</p> <p>There are a number of possible services that may need to be added from scratch rather than editing existing ones. While it is possible to create a single custom service that contains all of the open ports needed, it make more sense to make this modular in case only a small subset of the service needs to be added to another policy.</p> <p>Polycom API</p> <ol style="list-style-type: none"> 1. Go to Policy & Objects > Objects > Services. 2. Select Create New. 3. Fill in the fields of the new service with the following information: <p>Name Polycom API Service Type Firewall Category VoIP, Messaging & Other Protocol Type TCP/UDP/SCTP Protocol TCP/UDP/SCTP</p>	OK
2	1 a 35	2.1.37.	Possuir mecanismo de anti-spoofing;	Sim	fortios-handbook-54.pdf	355	<p>Reverse path lookup</p> <p>Whenever a packet arrives at one of the FortiGate unit's interfaces, the unit determines whether the packet was received on a legitimate interface by doing a reverse lookup using the source IP address in the packet header. This is also called anti-spoofing. If the FortiGate unit cannot communicate with the computer at the source IP address through the interface on which the packet was received, the FortiGate unit drops the packet as it is likely a hacking attempt.</p>	OK

Lote	Item do Lote	Item	Descrição do Item	Atende	Referência/Documento	Página	Observações	Análise do grupo técnico
2	1 a 35	2.1.38.	Possuir funcionalidade de exceção em SSL Inspection para sites e aplicações bancárias, não decriptando o tráfego dessas sessões.	Sim	fortios-handbook-54.pdf	2632	<p>Inspection Exemption</p> <p>When you are using a browser to visit SSL encrypted sites and we are using a certificate that does not match the certificate of the site, we are presented with a warning message and the option of continuing, using the untrusted certificate, or terminating the session. However, there are a number of applications that use SSL encrypted traffic. If the application detects SSL traffic that wasn't signed with a certificate that it trusts it will not allow the traffic. The applications do not give the option to manually indicate that we trust the certificate or the site. If the option is available, the customer may choose to import needed SSL certificates into Local Certificates and configure a policy for communication for that application. The assist in preventing loss of access to these site but still enabling the SSL inspection of the rest of the internet traffic, a method of exempting either Website categories or specific sites has been developed. To exempt a large group of sites the profile can be configure to exempt FortiGuard Categories. There are 3 of these categories preselected due to the high likelihood of issues with associated applications with the type of websites included in these categories.</p> <p>I Heath and Wellness I Personal Privacy I Finance and Banking</p>	OK
2	1 a 35	2.1.39.	Possuir inspeção profunda de pacotes para tráfego criptografado (no mínimo em tráfego VPN e HTTPS);	Sim	fortios-handbook-54.pdf	991,2406	<p>Deep Inspection works along the following lines. If your FortiGate unit has the correct chipset it will be able to scan SSL encrypted traffic in the same way that regular traffic can be scanned. The FortiGate firewall will essentially receive the traffic on behalf of the client and open up the encrypted traffic. Once it is finished it reencrypts the traffic and sends it on to its intended recipient. It is very similar to a man-in-the-middle attack. By enabling this feature, it allows the FortiGate firewall to filter on traffic that is using the SSL encrypted protocol.</p> <p>The encrypted protocols that can be inspected are:</p> <p>I HTTPS I SMTPS I POP3S I IMAPS I FTPS</p> <p>SSL VPN</p> <p>Local SSL VPN traffic is treated like special management traffic as determined by the SSL VPN destination port. Packets are decrypted and are routed to an SSL VPN interface. Policy lookup is then used to control how packets are forwarded to their destination outside the FortiGate. SSL encryption and decryption is offloaded to and accelerated by CP8 or CP9 processors.</p>	OK
2	1 a 35	2.1.40.	Possuir, no mínimo, suporte a SNMP v2 e v3;	Sim	fortios-handbook-54.pdf	2808	<p>The FortiGate SNMP implementation is read-only. SNMP v1, v2c, and v3 compliant SNMP managers have readonly access to FortiGate system information through queries and can receive trap messages from the FortiGate unit.</p>	OK
2	1 a 35	2.1.41.	Deve possuir MIB própria contemplando, no mínimo, indicadores de estado do hardware e de performance do equipamento;	Sim	fortios-handbook-54.pdf	2813-2814	<p>To get CPU, memory, and network usage of each cluster unit using the reserved management IP addresses From the command line of an SNMP manager, you can use the following SNMP commands to get CPU, memory and network usage information for each cluster unit. In the examples, the community name is Community. The commands use the MIB field names and OIDs listed below. Enter the following commands to get CPU, memory and network usage information for the primary unit with reserved management IP address 10.11.101.101 using the MIB fields:</p> <pre>snmpget -v2c -c Community 10.11.101.101 fgHaStatsCpuUsage snmpget -v2c -c Community 10.11.101.101 fgHaStatsMemUsage snmpget -v2c -c Community 10.11.101.101 fgHaStatsNetUsage</pre> <p>Fortinet MIBs</p> <p>The FortiGate SNMP agent supports Fortinet proprietary MIBs as well as standard RFC 1213 and RFC 2665 MIBs. RFC support includes support for the parts of RFC 2665 (Ethernet-like MIB) and the parts of RFC 1213 (MIB II) that apply to FortiGate unit configuration. There are two MIB files for FortiGate units - the Fortinet MIB, and the FortiGate MIB. The Fortinet MIB contains traps, fields and information that is common to all Fortinet products. The FortiGate MIB contains traps, fields and information that is specific to FortiGate units. Each Fortinet product has its own MIB.</p>	OK
2	1 a 35	2.1.42.	Deve identificar os países de origem e destino de todas as sessões estabelecidas através do equipamento, exceto para sessões no âmbito da rede interna (não roteadas).	Sim	fortios-handbook-54.pdf	61,63	<p>FortiView Countries console</p> <p>A new Countries console has been introduced to allow administrators to filter traffic according to source and destination countries. This console includes the option to view the Country Map visualization.</p>	OK
2	1 a 35	2.1.43.	Deve permitir a criação de políticas de segurança baseadas em geolocalização, permitindo o bloqueio de tráfego com origem ou destino a determinado país ou grupo de países.	Sim	fortios-handbook-54.pdf	1045,1056	<p>Geography Based Addresses</p> <p>Geography addresses are those determined by country of origin. This type of address is only available in the IPv4 address category.</p> <p>Creating a Geography address</p> <ol style="list-style-type: none"> 1. Go to Policy & Objects > Addresses. 2. Select Create New. A drop down menu is displayed. Select Address. 3. In the Category field, chose Address. (This is for IPv4 addresses.) 4. Input a Name for the address object. 5. In the Type field, select Geography from the drop down menu. 6. In the Country field, select a single country from the drop down menu. 7. In the Interface field, leave as the default any or select a specific interface from the drop down menu. 8. Select the desired on/off toggle setting for Show in Address List. If the setting is enabled the address will appear in drop down menus where it is an option. 9. Input any additional information in the Comments field. 10. Press OK. <p>Address Groups</p> <p>Address groups are designed for ease of use in the administration of the device. If you have a number of addresses or address ranges that will commonly be treated the same or require the same security policies, you can put them into address groups, rather than entering multiple individual addresses in each policy refers to them.</p>	OK
2	1 a 35	2.1.44.	Deve possibilitar a visualização dos países de origem e destino nos logs de eventos, de acessos e ameaças.	Sim	2.1.44_Print.png	1		OK
2	1 a 35	2.1.45.	Deve prover interface de gerência local do firewall ou do cluster (virtual ou físico) do qual o firewall faz parte, por meio de interface gráfica (GUI) e linha de comando – (CLI) ou via SSH. Especificamente a interface gráfica (GUI) deve atender as funcionalidades gerenciais previstas nos subitens 2.1.45.1 ao 2.1.45.14.	Sim	fortios-handbook-54.pdf	83,259	<p>GUI Refresh</p> <p>The FortiGate GUI now uses a new flat GUI design and framework that incorporates a simplified and modern look and feel. In addition to the new look, options have been moved around on the GUI menus.</p> <p>Using the CLI</p> <p>The command line interface (CLI) is an alternative configuration tool to the web-based manager. While the configuration of the GUI uses a point-and-click method, the CLI requires typing commands or uploading batches of commands from a text file, like a configuration script.</p>	OK

Lote	Item do Lote	Item	Descrição do Item	Atende	Referência/Documento	Página	Observações	Análise do grupo técnico
2	1 a 35	2.1.45.1.	Deve possuir a capacidade de definir administradores com diferentes perfis de acesso. Os perfis de acesso devem ser, no mínimo, de leitura/escrita e somente leitura.D66	Sim	fortios-handbook-54.pdf	1369	<p>Add new administrator accounts</p> <p>Rather than allowing all administrators to access the FortiGate unit with the admin administrator account you should create administrator accounts for each person that requires administrative access. That way you can track who has made configuration changes and performed other administrative activities. Keep the number of administrative accounts to a minimum to keep better control on who can access the device.</p> <p>To add administrators go to System > Admin Profiles and select Create New.</p> <p>If you want administrators to have access to all FortiGate configuration options, their accounts should have the prof_admin admin profile.</p> <p>Administrators with this profile can do anything except add new administrator accounts.</p> <p>At least one account should always have the super_admin profile as this profile is required to add and remove administrators. To improve security only a very few administrators (usually one) should be able to add new administrators.</p> <p>If you want some administrator accounts to have limited access to the FortiGate configuration you can create custom admin profiles that only allow access to selected parts of the configuration. To add custom admin profiles, go to System > Admin Profiles and select Create New.</p> <p>For example, if you want to add an admin profile that does not allow changing firewall policies, when you configure the admin profile set Firewall Configuration to None or Read Only.</p>	OK
2	1 a 35	2.1.45.2.	Deve permitir a delegação de funções de administração.	Sim	fortios-handbook-54.pdf	2795	<p>Segregated administrative roles</p> <p>To minimize the effect of an administrator causing errors to the FortiGate configuration and possibly jeopardizing the network, create individual administrative roles where none of the administrators have super_admin permissions. For example, one account is used solely to create security policies, another for users and groups, another for VPN, and so on.</p>	OK
2	1 a 35	2.1.45.3.	Deve registrar em log as ações dos usuários administradores.	Sim	fortios-handbook-54.pdf	2794	<p>Monitoring administrators</p> <p>You can view the administrators logged in using the System Information widget on the Dashboard. The Current Administrator row that shows the administrator logged in and the total number of administrators logged in. Selecting Details displays the administrators, where they are logging in from and how (CLI, GUI) and when they logged in. You are also able to monitor the activities the administrators perform on the FortiGate using the event logging. Event logs include a number of options to track configuration changes.</p>	OK
2	1 a 35	2.1.45.4.	Deve suportar a identificação e utilização de usuários nas políticas de segurança.	Sim	fortios-handbook-54.pdf	1020	<p>Set the Source parameter by selecting the field with the "+" next to the field label. The source in this case is either the source address, source user or source device of the initiating traffic. When the field is selected a window will slide out from the right. Tabs indicating Address, User or Device options are there to help categorize the options along with the option to search.</p>	OK
2	1 a 35	2.1.45.5.	Deve suportar agrupamento lógico de objetos ("object grouping") para criação de regras.	Sim	fortios-handbook-54.pdf	246,1039	<p>Policy & Objects</p> <p>Configure firewall policies, protocol options, and supporting content for policies, including schedules, firewall addresses, and traffic shapers.</p> <p>Firewall objects</p> <p>As was mentioned earlier, the components of the FortiGate firewall go together like interlocking building blocks. The Firewall objects are a prime example of those building blocks. They are something that can be configured once and then used over and over again to build what you need. They can assist in making the administration of the FortiGate unit easier and more intuitive as well as easier to change. By configuring these objects with their future use in mind as well as building in accurate descriptions the firewall will become almost self documenting. That way, months later when a situation changes, you can take a look at a policy that needs to change and use a different firewall object to adapt to the new situation rather than build everything new from the ground up to accommodate the change. This chapter includes information about the following Firewall objects:</p> <ul style="list-style-type: none"> Addresses Services and TCP ports Firewall schedules Security profiles 	OK
2	1 a 35	2.1.45.6.	Deve possibilitar o gerenciamento (incluindo a criação, alteração, monitoramento e exclusão) de objetos de rede. Deverá ainda permitir detectar se e onde, na base de regras, está sendo utilizado determinado objeto de rede. Os tipos de objetos deverão permitir especificar de forma distinta grupos e objetos de rede e serviços, diferenciando-os e agrupando-os conforme suas características ou descrição de maneira a permitir o reaproveitamento dos mesmos em diferentes políticas.	Sim	fortios-handbook-54.pdf	1039,1041,1042,1056-1057	<p>Firewall objects</p> <p>As was mentioned earlier, the components of the FortiGate firewall go together like interlocking building blocks. The Firewall objects are a prime example of those building blocks. They are something that can be configured once and then used over and over again to build what you need. They can assist in making the administration of the FortiGate unit easier and more intuitive as well as easier to change. By configuring these objects with their future use in mind as well as building in accurate descriptions the firewall will become almost self documenting. That way, months later when a situation changes, you can take a look at a policy that needs to change and use a different firewall object to adapt to the new situation rather than build everything new from the ground up to accommodate the change.</p> <p>This chapter includes information about the following Firewall objects:</p> <ul style="list-style-type: none"> Addresses Services and TCP ports Firewall schedules Security profiles <p>Addresses</p> <p>Firewall addresses define sources and destinations of network traffic and are used when creating policies. When properly set up these firewall objects can be used with great flexibility to make the configuration of firewall policies simpler and more intuitive. The FortiGate unit compares the IP addresses contained in packet headers with a security policy's source and destination addresses to determine if the security policy matches the traffic.</p>	OK
2							<p>Addresses, address groups, and virtual IPs must have unique names to avoid confusion in firewall policies. If an address is selected in a policy, the address cannot be deleted until it is deselected from the policy</p> <p>Address Groups</p> <p>Address groups are designed for ease of use in the administration of the device. If you have a number of addresses or address ranges that will commonly be treated the same or require the same security policies, you can put them into address groups, rather than entering multiple individual addresses in each policy refers to them.</p> <p>Creating an Address Group</p> <ol style="list-style-type: none"> 1. Go to Policy & Objects > Addresses. 2. Select the down arrow next to Create New, select Address Group. 3. Choose the Category, that is applicable to the proposed selection of addresses. 4. Input a Group Name for the address object. Depending on which Category has been chosen the configurations will differ slightly 	OK
2	1 a 35	2.1.45.7.	Deve contabilizar a utilização ("hit counts") ou o volume de dados trafegados correspondente a cada regra de filtragem individualmente.	Sim	fortios-handbook-54.pdf	922	<p>Policy counter improvements (277555 260743 172125)</p> <ul style="list-style-type: none"> Implicit deny policy counter added first-hit time tracked for each policy "Hit count" is tracked for each policy (total number of new sessions since last reset) Most counters now persist across reboots 	OK

Lote	Item do Lote	Item	Descrição do Item	Atende	Referência/Documento	Página	Observações	Análise do grupo técnico
2	1 a 35	2.1.45.8.	Deve possibilitar a especificação de política por tempo, ou seja, permitir a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora).	Sim	fortios-handbook-54.pdf	1081	<p>Firewall schedules</p> <p>Firewall schedules control when policies are in effect. When you add a security policy on a FortiGate unit you need to set a schedule to determine the time frame in which that the policy will be functioning. While it is not set by default, the normal schedule would be always. This would mean that the policy that has been created is always function and always policing the traffic going through the FortiGate. The time component of the schedule is based on a 24 hour clock notation or military time as some people would say.</p> <p>Creating a recurring schedule object</p> <ol style="list-style-type: none"> 1. Go to Policy & Objects > Schedules. 2. Select Create New. A drop down menu is displayed. Select Schedule. 3. From the Type options, choose Recurring. 4. Input a Name for the schedule object. 5. From the Days options, choose the day of the week that you would like this schedule to apply to. The schedule will be in effect on the days of the week that have a check mark in the checkbox to the left of the name of the weekday. 6. Choose a Start Time. <p>The Start Time is composed of two fields, Hour and Minute. Think of setting the time for a digital clock in 24 hour mode. The Hour value can be an integer from 0 and 23. The Minute value can be from 0 to 59. 0 and 0 would be midnight at the start of the day and 23 and 59 would be one minute to midnight at the end of the day. The value can be entered by keyboard or by using the up and down arrows in the field to select the value.</p> <ol style="list-style-type: none"> 7. Choose a Stop Time. <p>Configuration is the same as Start Time.</p> <ol style="list-style-type: none"> 8. Press OK. 	OK
2	1 a 35	2.1.45.9.	Deve suportar a geração de alertas automáticos via email, SNMP e Syslog.	Sim	fortios-handbook-54.pdf	2806-2808	<p>To configure a Syslog server in the web-based manager, go to Log & Report > Log Settings.</p> <p>To configure alert email - web-based manager</p> <ol style="list-style-type: none"> 1. Go to Log & Report > Log Config > Alert E-mail. <p>SNMP traps alert you to events that occur such as a full log disk or a virus detected.</p> <p>To configure SNMP settings, go to System > SNMP.</p>	OK
2	1 a 35	2.1.45.10.	Deve permitir a exportação de logs via SCP ou FTP.	Sim	fortios-handbook-54.pdf http://help.fortinet.com/fadc/4-5-0/cli/Content/FortiADC/cli-ref/execute_backup_.htm	83	<p>The new administrator's menu (upper right) provides quick access to change the administrator's password, backup the FortiGate configuration, access the CLI console and log out.</p> <p>Syntax</p> <pre>execute backup config tftp <filename> <ipaddress> execute backup full-config tftp <filename> <ipaddress> execute backup full-config-file tftp <filename> <ipaddress> execute backup isp-address tftp <filename> <ipaddress> [<password>] execute backup log ftp <ipaddress>[:port] <ftp_user> <ftp_password> {event attack traffic all} [dir] <filename></pre> <p>Name of the file to be used for the backup file, such as FortiADC_backup.conf.</p> <pre><ipaddress></pre> <p>IP address of the FTP/TFTP server.</p> <pre><password></pre> <p>Password for use when encrypting the backup file using 128-bit AES.</p> <p>If you do not provide a password, the backup file will be stored as clear text.</p> <pre><ipaddress>[:port]</pre> <p>IP address and optional port of the FTP server.</p> <pre><ftp_user> <ftp_password></pre> <p>FTP username and password.</p> <pre>{event attack traffic all}</pre> <p>Specify the type of logs to back up.</p> <pre>[dir]</pre> <p>Optionally, specify a directory on the FTP server to copy the file.</p>	OK
2	1 a 35	2.1.45.11.	Deve informar a utilização dos recursos de CPU, memória, armazenamento interno e atividade de rede dos equipamentos gerenciados.	Sim	fortios-handbook-54.pdf	252-253	<p>System Resources</p> <p>The System Resources widget displays basic FortiGate resource usage. This widget displays the information for CPU and memory in either real-time or historical data. For FortiGates with multiple CPUs, you can view the CPU usage as an average of all CPUs or each one individually.</p> <p>Unit Operation</p> <p>The Unit Operation widget is an illustrated version of the FortiGate's front panel that shows the status of the FortiGate's network interfaces. Interfaces appears green when connected. Hover the mouse pointer over an interface to view further details.</p>	OK
2	1 a 35	2.1.45.12.	Deve informar o número de sessões simultâneas e de novas sessões por segundo dos equipamentos gerenciados.	Sim	2.1.45.12_Print.png	1		OK

Lote	Item do Lote	Item	Descrição do Item	Atende	Referência/Documento	Página	Observações	Análise do grupo técnico
2	1 a 35	2.1.45.13.	Deve possuir visualização mínima sumarizada de: aplicações, ameaças, URLs, endereços de origem, endereços de destino, levando-se em conta o quantitativo de sessões, de consumo de banda e categorização.	Sim	fortios-handbook-54.pdf	1090,1091,1121,1123,1124	<p>I Place your cursor over any object in the visualization to display the device name, the IP address, Sessions, sent and received Bytes and Packets, Bandwidth, and Dropped Bytes.</p> <p>New bandwidth column added to realtime FortiView pages The FortiView console provides a new bandwidth column that displays information for bandwidth calculated on a per-session level, providing administrators the ability to sort realtime bandwidth usage in descending order.</p> <p>Destination IP - Filter by the IP address used by the destination. Source Interface - Filter by the interface type used by the source user, e.g. wan1. Threat - Filter by threat name and/or URL Threat Type - Filter by threat category, e.g. Illegal/Unethical or P2P.</p> <p>Source Interfaces Select to drill down by source interface, including bytes sent and received, and bandwidth used. You can sort entries by selecting the column header.</p> <p>Destination Interfaces - Select to drill down by destination interface, including bytes sent and received, and bandwidth used. You can sort entries by selecting the column header. Threats Select to drill down by threat to view threat-related information, including the threat name, category, threat level, threat score, and number of sessions blocked and allowed. You can sort entries by selecting the column header.</p> <p>Categories - Select to drill down by category to view category-related information, including category name, browsing time, threat score, number of sessions blocked/allowed, and bytes sent/received. You can sort entries by selecting the column header.</p> <p>Sessions - Select to drill down by sessions to view session-related information, including date/time, source, destination IP address and geographic region, application name, security action, security event, and bytes sent/received. You can sort entries by selecting the column header.</p>	OK
2	1 a 35	2.1.45.14.	Deverá suportar gerência remota (via rede local ou WAN) ou por meio da gerência centralizada, sendo que:	Sim	FortiManager-5.4.3-Administration-Guide.pdf	41	<p>Administrative access can be configured in IPv4 or IPv6 and includes the following settings:</p> <p>HTTPS HTTP PING SSH TELNET SNMP Web Service</p>	OK
2	1 a 35	2.1.45.14.1.	A comunicação entre a estação ou sistema de gerência e o firewall ou cluster local deverá ser criptografada e autenticada;	Sim	FortiManager-5.4.3-Administration-Guide.pdf http://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-ports-and-protocols-54/03-FGFM.htm	24	<p>Device Manager Device Manager contains all devices that are managed by the FortiManager unit. You can create new device groups, provision and add devices, and install policy packages and device settings. Device Manager communicates with devices by using the FortiGate-FortiManager (FGFM) protocol.</p> <p>Configuring an SSL connection</p> <p>The default encryption automatically sets high and medium encryption algorithms. Algorithms used for High, Medium, and Low follow the openssl definitions below</p>	OK
2	1 a 35	2.1.46.	Deve permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound) através da classificação dos pacotes (shaping);	Sim	fortios-handbook-54.pdf	2861-2862,2873	<p>The purpose of traffic shaping Traffic shaping, or traffic management, controls the bandwidth available and sets the priority of traffic processed by the policy to control the volume of traffic for a specific period (bandwidth throttling) or rate the traffic is sent (rate limiting).</p> <p>Quality of Service Quality of Service (QoS) is the capability to adjust some quality aspects of your overall network traffic. This can include such techniques as priority-based queuing and traffic policing. Because bandwidth is finite and because some types of traffic are slow, jitter or packet loss sensitive, bandwidth intensive, or operation critical, QoS can be a useful tool for optimizing the performance of the various applications on your network.</p> <p>Shared Shaper Choose one of the default shared shapers: guarantee-100kbps, high-priority, medium-priority, low-priority, shared-1M-pipe or create your own under Policy & Objects > Traffic Shapers. Shared Shapers share the allotted bandwidth with any security policies using them (unless they are set to perpolicy in the CLI). This affects uploads or outbound traffic.</p> <p>Reverse Shaper Choose one of the default shared shapers: guarantee-100kbps, high-priority, medium-priority, low-priority, shared-1M-pipe, or create your own under Policy & Objects > Traffic Shapers. This affects downloads or inbound traffic.</p>	OK
2	1 a 35	2.1.47.	Deve possuir gerenciamento gráfico centralizado das funcionalidades de QoS/Traffic Shaping integrado tanto com a gerência local do equipamento, quanto com a gerência centralizada da solução;	Sim	fortios-handbook-54.pdf	2858-2862	<p>Central management Administering one or two FortiGate units is fairly simple enough, especially when they are in the same room or building. However, if you are administering many FortiGate units that may be located in locations in a large geographical area, or in the world, you will need a more efficient method of maintaining firmware upgrades, configuration changes, and updates. The FortiManager family of appliances supply the tools needed to effectively manage any size Fortinet security infrastructure, from a few devices to thousands of appliances. FortiManager appliances provide centralized policy-based provisioning, configuration, and update management, as well as end-to-end network monitoring for added control. Managers can control administrative access and simplify policy deployment using role-based administration to define user privileges for specific management domains and functions by aggregating collections of Fortinet appliances and agents into independent management domains. By locally hosting security content updates for managed devices and agents, FortiManager appliances minimize web filtering rating request response time and maximize network protection.</p> <p>New Traffic Shaper Policy Configuration Method (269943) Previously, traffic shapers were configured in Policy & Objects > Objects > Traffic Shapers and then applied in security policies under Policy & Objects > Policy > IPv4 . In FortiOS 5.4, traffic shapers are now configured in a new traffic shaping section in Policy & Objects > Traffic Shapers. The way that traffic shapers are applied to policies has changed significantly in 5.4, because there is now a specific section for traffic shaping policies in Policy & Objects > Traffic Shaping Policy. In the new traffic shaping policies, you must ensure that the Matching Criteria is the same as the security policy or policies you want to apply shaping to. The screen shot below shows the new 5.4 GUI interface</p>	OK

Lote	Item do Lote	Item	Descrição do Item	Atende	Referência/Documento	Página	Observações	Análise do grupo técnico
2							<p>You can implement QoS on FortiGate units using the following techniques:</p> <p>Traffic policing - Drops packets that do not conform to bandwidth limitations.</p> <p>Traffic shaping - Ensures that the traffic may consume bandwidth at least at the guaranteed rate by assigning a greater priority queue if the guarantee is not being met. Also ensures that the traffic cannot consume bandwidth greater than the maximum at any given instance in time. Flows greater than the maximum rate are subject to traffic policing.</p> <p>Queueing - Transmits packets in order of their assigned priority queue for that physical interface. All traffic in a higher priority traffic queue must be completely transmitted before traffic in lower priority queues will be transmitted.</p>	OK
2	1 a 35	2.1.48.	Deve suportar a criação de políticas de controle de uso de largura de banda, limitando ou expandido individualmente, baseadas em: porta ou protocolo, endereço IP de origem ou destino, grupo de usuários do Microsoft Active Directory e LDAP e aplicações (por exemplo, Youtube e WhatsApp).	Sim	fortios-handbook-54.pdf	2859,2873	<p>There is also added Traffic Shaper support based on the following:</p> <p>I Source (Address, Local Users, Groups)</p> <p>I Destination (Address, FQDN, URL or category)</p> <p>I Service (General, Web Access, File Access, Email and Network services, Authentication, Remote Access, Tunneling, VoIP, Messaging and other Applications, Web Proxy)</p> <p>I Application</p> <p>I Application Category</p> <p>I URL Category</p> <p>Application - Choose an application to specify which applications you wish to apply traffic shaping to. For example, YouTube, Vimeo, or Facebook.</p>	OK
2	1 a 35	2.1.49.	As funcionalidades de VPN não podem possuir qualquer restrição de licenciamento, inclusive em relação ao número de clientes, aos softwares instalados nos clientes, IPs e máquinas, limitado apenas à capacidade de throughput do equipamento para VPN.	Sim	De acordo fortiOS_54.pdf FortiGate_80E_Series.pdf fortigate-getting-started-54.pdf	5570	<p>Concurrent SSL-VPN Users</p> <p>FortiGate platforms do not impose any limitations on the number or type of customers, users, devices, IP addresses, or number of VPN clients being served by the platform. Such factors are limited solely by the hardware capacity of each given model.</p>	OK
2	1 a 35	2.1.50.	Deve permitir a arquitetura de VPN hub and spoke IPSec, tanto para topologias site-to-site ("Full Meshed" e "Estrela") como para client-to-site (remote access);	Sim	fortios-handbook-54.pdf FortiOS_ADVPN_v2_2017-02-01.pdf	1785,1841,1843,1857	<p>VPN Type - Remote Access</p> <p>Remote Device Type - FortiClient VPN for OS X, Windows and Android</p> <p>Description - On-demand tunnel for users using the FortiClient software.</p> <p>You can set up a fully meshed or partially meshed configuration</p> <p>Gateway-to-gateway</p> <p>3 This section explains how to set up a basic gateway-to-gateway (site-to-site) IPsec VPN.</p> <p>Hub-and-spoke configurations</p> <p>This section describes how to set up hub-and-spoke IPsec VPNs.</p> <p>Hub nodes concentrate Spoke nodes in a Star topology</p>	OK
2	1 a 35	2.1.51.	Deve permitir a criação de túneis VPN SSL/TLS;	Sim	fortios-handbook-54.pdf	2728	<p>Tunnel mode</p> <p>In Tunnel mode, remote clients connect to a FortiGate unit that acts as a secure HTTP/HTTPS gateway and authenticates remote users as members of a user group. The SSL VPN client encrypts all traffic from the remote client computer and sends it to the FortiGate unit through an SSL VPN tunnel over the HTTPS link between the user and the FortiGate unit. Another option is split tunneling, which ensures that only the traffic for the private network is sent to the SSL VPN gateway. Internet traffic is sent through the usual unencrypted route. This conserves bandwidth and alleviates bottlenecks.</p> <p>A VPN tunnel is a non-application oriented tunnel that allows the users and networks to exchange a wide range of traffic regardless of application or protocol.</p> <p>FortiOS supports the SSL and TLS versions defined below:</p> <p>SSL and TLS version support table</p> <p>Version RFC</p> <p>SSL 2.0 RFC 6176</p> <p>SSL 3.0 RFC 6101</p> <p>TLS 1.0 RFC 2246</p> <p>TLS 1.1 RFC 4346</p> <p>TLS 1.2 RFC 5246</p>	OK
2	1 a 35	2.1.52.	Deve permitir a criação de túneis VPN SSL/TLS;	Sim	fortios-handbook-54.pdf	1783-1784	<p>VPN tunnels</p> <p>The data path between a user's computer and a private network through a VPN is referred to as a tunnel. Like a physical tunnel, the data path is accessible only at both ends. In the telecommuting scenario, the tunnel runs between the FortiClient application on the user's PC, or a FortiGate unit or other network device and the FortiGate unit on the office private network. Encapsulation makes this possible. IPsec packets pass from one end of the tunnel to the other and contain data packets that are exchanged between the local user and the remote private network. Encryption of the data packets ensures that any third-party who intercepts the IPsec packets can not access the data.</p> <p>You can create a VPN tunnel between:</p> <p>I A PC equipped with the FortiClient application and a FortiGate unit</p> <p>I Two FortiGate units</p> <p>I Third-party VPN software and a FortiGate unit</p>	OK
2	1 a 35	2.1.53.	A funcionalidade de VPN prevista no item anterior poderá ser atendida por meio de dispositivo standalone, caso o appliance do firewall não possua tal funcionalidade, sem prejuízo do gerenciamento centralizado da solução previsto nos itens 2.1.69 e 2.2;	Sim	fortiOS_54.pdf FortiGate_80E_Series.pdf	5 e 9, 5,		OK

Lote	Item do Lote	Item	Descrição do Item	Atende	Referência/Documento	Página	Observações	Análise do grupo técnico
2	1 a 35	2.1.54.	Deve permitir que o usuário realize a conexão VPN por meio de cliente instalado no sistema operacional do seu equipamento ou por meio de interface Web do tipo portal.	Sim	fortios-handbook-54.pdf	1785, 2727	<p>VPN Type - Remote Access</p> <p>Remote Device Type - FortiClient VPN for OS X, Windows, and Android</p> <p>NAT Options - N/A Description - On-demand tunnel for users using the FortiClient software.</p> <p>Web-only mode</p> <p>Web-only mode provides remote users with a fast and efficient way to access server applications from any thin client computer equipped with a web browser. Web-only mode offers true clientless network access using any web browser that has built-in SSL encryption and the Sun Java Runtime Environment (note that there is no minimum Java/JRE version requirement—any version of Java/JRE currently supported by the supplier of the Java/JRE for the operating system should work).</p> <p>Support for SSL VPN web-only mode is built into FortiOS. The feature comprises of an SSL daemon running on the FortiGate unit, and a web portal, which provides users with access to network services and resources including HTTP/HTTPS, Telnet, FTP, SMB/CIFS, VNC, RDP, and SSH.</p>	OK
2	1 a 35	2.1.54.1.	Caso seja por meio de cliente instalado, deverá estar disponível, no mínimo, para os sistemas operacionais Windows (Vista, 7, 8 e 10). Caso não existam clientes (softwares) dos próprios fabricantes instaláveis para os sistemas operacionais: Linux, Mac OS X, Apple iOS e Google Android, deverá a Licitante fornecer gratuitamente softwares de terceiros que sejam totalmente compatíveis com os sistemas operacionais referidos.	Sim	forticlient-v5.0.11-release-notes.pdf FortiClient.pdf	134	<p>Operating System I Microsoft Windows XP (32-bit)</p> <p>I Microsoft Windows Vista (32-bit and 64-bit)</p> <p>I Microsoft Windows 7 (32-bit and 64-bit)</p> <p>I Microsoft Windows 8 (32-bit and 64-bit)</p> <p>I Microsoft Windows 8.1 (32-bit and 64-bit)</p> <p>Operating System Supported:</p> <p>Microsoft Windows 10, 8.1, 7,</p> <p>Windows Server 2008 R2 and</p> <p>Windows Server 2012, 2012 R2, 2016</p> <p>Mac OS X v10.12, v10.11, v10.10, v10.9, v10.8</p> <p>iOS 5.1 or later (iPhone, iPad, iPod Touch)</p> <p>Android OS 4.4.4 or later (phone and tablet)</p>	OK
2	1 a 35	2.1.54.2.	O acesso por meio da interface Web deverá ser compatível com, no mínimo, os navegadores Internet Explorer 9 ou superior e Firefox 4.0 ou superior.	Sim	fortios-handbook-54.pdf	2727	<p>Web Browser - I Microsoft Internet Explorer version 11</p> <p>I Mozilla Firefox version 46</p>	OK
2	1 a 35	2.1.55.	Deve suportar a customização da interface Web para acesso a VPN pelos administradores do sistema, incluindo quais aplicativos, servidores e sistemas estarão acessíveis via portal;	Sim	fortios-handbook-54.pdf	2738	<p>Portal configuration</p> <p>The portal configuration determines what the remote user sees when they log in to the portal. Both the system administrator and the user have the ability to customize the SSL VPN portal.</p> <p>To view the portals settings page, go to VPN > SSL-VPN Portals.</p>	OK
2	1 a 35	2.1.56.	Suportar algoritmos de criptografia para túneis VPN AES-128 e AES-256;	Sim	fortios-handbook-54.pdf	1788	<p>Encryption</p> <p>Encryption mathematically transforms data to appear as meaningless random numbers. The original data is called plaintext and the encrypted data is called ciphertext. The opposite process, called decryption, performs the inverse operation to recover the original plaintext from the ciphertext.</p> <p>The process by which the plaintext is transformed to ciphertext and back again is called an algorithm. All algorithms use a small piece of information, a key, in the arithmetic process of converted plaintext to ciphertext, or vice-versa. IPsec uses symmetrical algorithms, in which the same key is used to both encrypt and decrypt the data. The security of an encryption algorithm is determined by the length of the key that it uses. FortiGate IPsec VPNs offer the following encryption algorithms, in descending order of security:</p> <p>AES-GCM Galois/Counter Mode (GCM), a block cipher mode of operation providing both confidentiality and data origin authentication.</p> <p>AES256 A 128-bit block algorithm that uses a 256-bit key.</p> <p>AES192 A 128-bit block algorithm that uses a 192-bit key.</p> <p>AES128 A 128-bit block algorithm that uses a 128-bit key.</p> <p>3DES Triple-DES, in which plain text is DES-encrypted three times by three keys.</p> <p>DES Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key</p>	OK
2	1 a 35	2.1.57.	Suportar os algoritmos para definição de chave de cifração 3DES e AES;	Sim	fortios-handbook-54.pdf	1788	<p>Encryption</p> <p>Encryption mathematically transforms data to appear as meaningless random numbers. The original data is called plaintext and the encrypted data is called ciphertext. The opposite process, called decryption, performs the inverse operation to recover the original plaintext from the ciphertext.</p> <p>The process by which the plaintext is transformed to ciphertext and back again is called an algorithm. All algorithms use a small piece of information, a key, in the arithmetic process of converted plaintext to ciphertext, or vice-versa. IPsec uses symmetrical algorithms, in which the same key is used to both encrypt and decrypt the data. The security of an encryption algorithm is determined by the length of the key that it uses. FortiGate IPsec VPNs offer the following encryption algorithms, in descending order of security:</p> <p>AES-GCM Galois/Counter Mode (GCM), a block cipher mode of operation providing both confidentiality and data origin authentication.</p> <p>AES256 A 128-bit block algorithm that uses a 256-bit key.</p> <p>AES192 A 128-bit block algorithm that uses a 192-bit key.</p> <p>AES128 A 128-bit block algorithm that uses a 128-bit key.</p> <p>3DES Triple-DES, in which plain text is DES-encrypted three times by three keys.</p> <p>DES Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key</p>	OK
2	1 a 35	2.1.58.	Suportar os algoritmos RSA, Diffie-Hellman/RSA;	Sim	fortios-handbook-54.pdf	555,1802	<p>Configuring the SecurID system</p> <p>To use SecurID with a FortiGate unit, you need:</p> <p>I to configure the RSA server and the RADIUS server to work with each other (see RSA server documentation)</p> <p>I to configure the RSA SecurID 130 Appliance</p> <p>or</p> <p>I to configure the FortiGate unit as an Agent Host on the RSA ACE/Server</p> <p>I to configure the FortiGate unit to use the RADIUS server</p> <p>I to create a SecurID user group</p> <p>I to configure a security policy with SecurID authentication</p> <p>Diffie-Hellman Group Select one or more Diffie-Hellman groups from DH groups 1, 2, 5, and 14 through 21. At least one of the Diffie-Hellman Group settings on the remote peer or client must match one the selections on the FortiGate unit.</p> <p>Failure to match one or more DH groups will result in failed negotiations.</p>	OK

Lote	Item do Lote	Item	Descrição do Item	Atende	Referência/Documento	Página	Observações	Análise do grupo técnico
2	1 a 35	2.1.59.	Suportar Certificado Digital X.509 v3;	Sim	fortios-handbook-54.pdf	614	FortiGate units use X.509 certificates to authenticate single sign-on (SSO) for users. The X.509 standard has been in use since before 2000, but has gained popularity with the Internet's increased popularity. X.509 v3 is defined in RFC 5280 and specifies standard formats for public key certificates, certificate revocation lists, and a certification path validation algorithm. The unused earlier X.509 version 1 was defined in RFC 1422.	OK
2	1 a 35	2.1.60.	Suportar a inclusão (enrollment) de autoridades certificadoras;	Sim	fortios-handbook-54.pdf	621	Obtaining and installing a signed server certificate from an external CA To obtain a signed server certificate for a FortiGate unit, you must send a request to a CA that provides digital certificates that adhere to the X.509 standard. The FortiGate unit provides a way for you to generate the request. To submit the certificate signing request (file-based enrollment): 1. Using the web browser on the management computer, browse to the CA web site. 2. Follow the CA instructions for a base-64 encoded PKCS#10 certificate request and upload your certificate request. 3. Follow the CA instructions to download their root certificate and CRL. When you receive the signed server certificate from the CA, install the certificate on the FortiGate unit.	OK
2	1 a 35	2.1.61.	Permitir alteração dos algoritmos criptográficos das VPNs;	Sim	fortios-handbook-54.pdf	1823	Defining IKE negotiation parameters 1. Go to VPN > IPsec Tunnels and create the new custom tunnel or edit an existing tunnel. 2. Edit the Phase 1 Proposal (if it is not available, you may need to click the Convert to Custom Tunnel button). 3. Select Phase 1 Proposal and include the appropriate entries as follows: Encryption Select a symmetric-key algorithms: NULL — Do not use an encryption algorithm. DES — Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key. 3DES — Triple-DES; plain text is encrypted three times by three keys. AES128 — A 128-bit block algorithm that uses a 128-bit key. AES192 — A 128-bit block algorithm that uses a 192-bit key. AES256 — A 128-bit block algorithm that uses a 256-bit key.	OK
2	1 a 35	2.1.62.	Suportar IKE – Internet Key Exchange, fases I e II;	Sim	fortios-handbook-54.pdf	1798	The FortiGate unit implements the Encapsulated Security Payload (ESP) protocol. Internet Key Exchange (IKE) is performed automatically based on pre-shared keys or X.509 digital certificates. Interface mode, supported in NAT mode only, creates a virtual interface for the local end of a VPN tunnel. This chapter contains the following sections: Phase 1 configuration Phase 2 configuration	OK
2	1 a 35	2.1.63.	Suportar os protocolos de roteamento RIPv2, OSPFv2 ou OSPFv3 para as funcionalidades de VPN;	Sim	fortios-handbook-54.pdf	9, 463, 1972	RIP v2 In 1993, RIP version 2 was developed to deal with the limitations of RIP v1. It was not standardized until 1998. This new version supports classless routing, and subnets of various sizes. OSPFv3 and IPv6 OSPFv3 (OSPF version 3) includes support for IPv6. Generally, all IP addresses are in IPv6 format instead of IPv4. However, OSPFv3 area numbers use the same 32-bit numbering system as OSPFv2, as described in RFC 2740. Likewise, the router ID and area ID are in the same format as OSPFv2. RIP (for simplicity, you could use OSPF or BGP) is then configured to run on the IPsec interface and on the Chicago subnet (you could use redistribute connected, but we'll allow for the fact that there may be other subnets learned from another router on the 10.0.4.0/24 subnet)	OK
2	1 a 35	2.1.64.	Implementar autenticação de usuários utilizando LDAP, Microsoft Active Directory, RADIUS e certificados digitais e suportar, no mínimo, autenticação two-way com certificado digital e LDAP ou Microsoft Active Directory ou RADIUS	Sim	fortios-handbook-54.pdf	564,614,620	Microsoft RADIUS servers Microsoft Windows Server 2000, 2003, and 2008 have RADIUS support built-in. Microsoft specific RADIUS features are defined in RFC 2548. The Microsoft RADIUS implementation can use Active Directory for user credentials. LDAP servers Lightweight Directory Access Protocol (LDAP) is an Internet protocol used to maintain authentication data that may include departments, people, groups of people, passwords, email addresses, and printers. LDAP consists of a data-representation scheme, a set of defined operations, and a request/response network. Two-factor authentication The standard logon requires a username and password. This is one factor authentication—your password is one piece of information you need to know to gain access to the system. Two factor authentication adds the requirement for another piece of information for your logon. Generally the two factors are something you know (password) and something you have (certificate, token, etc.). This makes it harder for a hacker to steal your logon information. For example if you have a FortiToken device, the hacker would need to both use it and know your password to gain entry to your account.	OK
2							Certificate-based authentication This section provides an overview of how the FortiGate unit verifies the identities of administrators, SSL VPN users, or IPsec VPN peers using X.509 security certificates. Generating certificates with CA software CA software allows you to generate unmanaged certificates and CA certificates for managing other certificates locally without using an external CA service. Examples of CA software include ssl-ca from OpenSSL (available for Linux, Windows, and Mac) or gencslicert from SuSE, MS Windows Server 2000 and 2003 come with a CA as part of their certificate services, and in MS Windows 2008 CA software can be installed as part of the Active Directory installation. See Example — Generate and Import CA certificate with private key pair on OpenSSL on page 629.	OK

Lote	Item do Lote	Item	Descrição do Item	Atende	Referência/Documento	Página	Observações	Análise do grupo técnico
2	1 a 35	2.1.65.	Suportar certificados emitidos por autoridade certificadora no padrão ICP-Brasil;	Sim	fortios-handbook-54.pdf	529-530, 618	<p>Certificate authorities A certificate authority can be:</p> <ul style="list-style-type: none"> an organization, such as VeriSign Inc., that provides certificate services a software application, such as Microsoft Certificate Services or OpenSSH <p>For a company web portal or customer-facing SSL VPN, a third-party certificate service has some advantages.</p> <p>The CA certificates are already included in popular web browsers and customers trust the third-party. On the other hand, third-party services have a cost. For administrators and for employee VPN users, the local CA based on a software application provides the required security at low cost. You can generate and distribute certificates as needed. If an employee leaves the organization, you can simply revoke their certificate.</p> <p>Managing X.509 certificates Managing security certificates is required due to the number of steps involved in both having a certificate request signed, and then distributing the correct files for use. You use the FortiGate unit or CA software such as OpenSSL to generate a certificate request. That request is a text file that you send to the CA for verification, or alternately you use CA software to self-validate. Once validated, the certificate file is generated and must be imported to the FortiGate unit before it can be used. These steps are explained in more detail later in this section.</p> <p>This section provides procedures for generating certificate requests, installing signed server certificates, and importing CA root certificates and CRLs to the FortiGate unit.</p>	OK
2	1 a 35	2.1.66.	Suportar leitura e verificação de Certificate Revocation List (CRL);	Sim	fortios-handbook-54.pdf	529	To protect against compromised or misused certificates, CAs can revoke any certificate by adding it to a Certificate Revocation List (CRL). Certificate status can also be checked online using Online Certificate Status Protocol (OCSP).	OK
2	1 a 35	2.1.67.	Suportar NAT Transversal Tunneling (NAT-T);	Sim	fortios-handbook-54.pdf	1824	<p>Nat-traversal Enable this option if a NAT device exists between the local FortiGate unit and the VPN peer or client. The local FortiGate unit and the VPN peer or client must have the same NAT traversal setting (both selected or both cleared). When in doubt, enable NAT-traversal. See NAT traversal on page 1825.</p> <p>Gui refresh - tela do Fortigate - VPN</p>	OK
2	1 a 35	2.1.68.	Possuir gerenciamento gráfico das funcionalidades de VPN e monitoramento de seus eventos de forma integrada tanto com a gerência local do equipamento ou do cluster quanto com a gerência centralizada da solução.	Sim	fortios-handbook-54.pdf	83,149, 279	<p>Updates and enhancements to the IPsec VPN wizard (222339 290377 287021 289251) The IPsec VPN wizard has been simplified to more clearly identify tunnel template types, remote device types, and NAT configuration requirements. Example topological diagrams are now also included.</p> <p>Central management Administering one or two FortiGate units is fairly simple enough, especially when they are in the same room or building. However, if you are administering many FortiGate units that may be located in locations in a large geographical area, or in the world, you will need a more efficient method of maintaining firmware upgrades, configuration changes, and updates.</p> <p>The FortiManager family of appliances supply the tools needed to effectively manage any size Fortinet security infrastructure, from a few devices to thousands of appliances. FortiManager appliances provide centralized policy-based provisioning, configuration, and update management, as well as end-to-end network monitoring for added control. Managers can control administrative access and simplify policy deployment using role-based administration to define user privileges for specific management domains and functions by aggregating collections of Fortinet appliances and agents into independent management domains. By locally hosting security content updates for managed devices and agents, FortiManager appliances minimize web filtering rating request response time and maximize network protection.</p>	OK
2	1 a 35	2.1.69.	VPN gateway-a-gateway deverá possuir interoperabilidade com os gateways de VPN pelo menos dos seguintes fabricantes: Cisco, Checkpoint, Juniper, Palo Alto Networks, Fortinet, AKER, BluePEX, PFSense e SonicWall.	Sim	fortios-handbook-54.pdf	1841	<p>This section explains how to set up a basic gateway-to-gateway (site-to-site) IPsec VPN.</p> <p>In a gateway-to-gateway configuration, two FortiGate units create a VPN tunnel between two separate private networks. All traffic between the two networks is encrypted and protected by FortiGate security policies.</p>	OK
2	1 a 35	2.1.70.	Deve permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis de SSL.	Sim	fortios-handbook-54.pdf	2750,2767	<p>Monitoring active SSL VPN sessions You can go to User & Device > Monitor to view a list of active SSL VPN sessions. The list displays the user name of the remote user, the IP address of the remote client, and the time the connection was made. You can also see which services are being provided, and delete an active web session from the FortiGate unit.</p> <p>Creating security policies Create an SSL VPN security policy with SSL VPN user authentication to allow SSL VPN traffic to enter the FortiGate unit. Create a normal security policy from ssl.root to wan1 to allow SSL VPN traffic to connect to the Internet.</p> <ol style="list-style-type: none"> 1. Go to Policy & Objects > IPv4 Policy and select Create New. 2. Add an SSL VPN security policy as below, and click OK. 	OK
2	1 a 35	2.1.71.	O equipamento deve ser apropriado para o uso em ambiente tropical com umidade relativa na faixa de 20 a 85% (sem condensação) e temperatura ambiente na faixa de 5 a 40°C.	Sim	FortiGate_80E_Series.pdf	5	<p>Operating Temperature</p> <p>Humidity</p>	OK
2	1 a 35	2.2	Solução de gerência centralizada					
2	1 a 35	2.2.1.	Deverá ser fornecida solução de gerência centralizada dos firewalls, do mesmo fabricante e independente (externa) em relação aos equipamentos, sendo que:	Sim	FortiManager.pdf	1	<p>Full Control of Your Security Fabric Dynamic security updates and end-to-end security management for your Fortinet firewalls, wireless access points, switches, endpoints and remote VPN access to provide complete protection.</p>	OK
2	1 a 35	2.2.1.1.	A solução poderá ser fornecida baseada em “appliance especializado” – equipamento especializado para gerência centralizada, ou “appliance virtual” - solução de software executada em máquina virtual que possa ser instalado e executado em ambientes virtuais ou componentes de software instaláveis em sistemas operacionais padrão servidor;	Sim	FortiManager.pdf	2,6	<p>FortiManager 200F, 300E, 400E, 2000E, 3000F, 3900E and VM</p> <p>FortiManager/FortiManager VM licenses</p>	OK
2	1 a 35	2.2.1.2.	Quando a solução for baseada em “appliance especializado”, ou quando quaisquer outros equipamentos forem fornecidos para compor a solução, deverão:					
2	1 a 35	a)	ser compatíveis com rack padrão 19 polegadas;	Sim	FortiManager.pdf	4	Hardware Form Factor	OK
2	1 a 35	b)	possuir, no mínimo, duas interfaces de rede Gigabit Ethernet;	Sim	FortiManager.pdf	4	Total Interfaces	OK
2	1 a 35	c)	possuir fonte de energia com os mesmos parâmetros definidos no item 2.1.7;e	Sim	FortiManager.pdf	4	AC Power Supply	OK
2	1 a 35	d)	possuir, no mínimo, o espaço de armazenamento solicitado no respectivo item 7 de cada um dos lotes do item 3;	Sim	De acordo			A ser validado em testes

Lote	Item do Lote	Item	Descrição do Item	Atende	Referência/Documento	Página	Observações	Análise do grupo técnico
2	1 a 35	2.2.1.3.	Quando a solução for baseada em appliance virtual, deverá ser capaz de ser executada em pelo menos uma das seguintes plataformas virtualizadoras: VMware ESXi, Xen, KVM ou Microsoft Hyper-V, cujo ambiente será fornecido pela CONTRATANTE, não sendo necessário o fornecimento da licença da plataforma virtualizadora. Caso o equipamento ou ambiente virtualizado disponibilizado pela CONTRATANTE seja incompatível com os requisitos mínimos necessários para execução completa da solução baseada em appliance virtual, a ponto de inviabilizar ou prejudicar o seu funcionamento e a fabricante da solução não possua outra alternativa de fornecimento dentre aquelas dispostas nos itens 2.2.1.1, 2.2.1.2 e 2.2.1.4, deverá ser fornecido equipamento com ambiente virtual compatível, observado o disposto no item 2.2.1.2;	Sim	FortiManager.pdf, conforme proposta	5	Hypervisor Support VMware ESX/ESXi 4.0/4.1/5.0/5.1/5.5/6.0, Microsoft Hyper-V 2008 R2/2012/2012 R2 /2016, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure	OK
2	1 a 35	2.2.1.4.	Quando a solução for baseada em componentes de software, deverão ser fornecidas e implantadas, em caráter perpétuo, todas as licenças dos softwares e sistemas operacionais necessários ao funcionamento da solução, em versões para servidor, sendo que a versão fornecida de sistema operacional não poderá entrar em modo End of Support nos 60 (sessenta) meses a contar da data de assinatura do contrato.	Sim	Conforme Proposta e Carta_Fabricante_Fortinet_2.pdf,	1		OK
2	1 a 35	2.2.2.	Deve permitir a gerência centralizada dos equipamentos e contextos virtuais que compõem a solução de alta disponibilidade, devendo ser dimensionada e devidamente licenciada para atender, no mínimo, o número total de equipamentos físicos gerenciados e o número total de contextos virtuais possíveis, compatível com o limite operacional dos equipamentos e clusters gerenciados.	Sim	FortiManager.pdf	2,5	Full control of your network using Security Fabric Ability to manage end-to-end Fortinet devices including FortiGate, FortiAP, FortiSwitch and FortiClient to provide single pane of glass for extended enterprise. CAPACITY AND PERFORMANCE Devices/VDOMs (Maximum)1 1,200 4,000 10,000 CAPACITY Devices/VDOMs (Maximum)1 10 +10 +100 +1,000 +5,000 +10,000	OK
2	1 a 35	2.2.3.	Deve ser licenciada de forma a não limitar número de usuários, objetos, regras de segurança, NAT e endereços IP.	Sim	Carta_Fabricante_Fortinet_1.pdf, fortigate-getting-started-54.pdf	70	FortiGate platforms do not impose any limitations on the number or type of customers, users, devices, IP addresses, or number of VPN clients being served by the platform. Such factors are limited solely by the hardware capacity of each given model.	OK
2	1 a 35	2.2.4.	Deve ser licenciada de forma a permitir a captura e filtragem de todos os eventos gerados por todos os equipamentos e contextos virtuais que compõe a solução de alta disponibilidade.	Sim	FortiAnalyzer-5.6.0-Administration-Guide.pdf FortiAnalyzer.pdf	125	You can deploy FortiAnalyzer physical or virtual appliances to collect, correlate, and analyze geographically and chronologically diverse security data. Alerts and log information from Fortinet appliances and third-party devices are aggregated in a single location, providing a simplified, consolidated view of your security posture. In addition, FortiAnalyzer platforms provide detailed data capture for forensic purposes to comply with policies regarding privacy and disclosure of information security breaches. CAPACITY AND PERFORMANCE GB/Day of Logs 3,000 5,000 8,300 4,000 CAPACITY AND PERFORMANCE GB/Day of Logs 1 incl.* +1 +5 +25 +100 +500 +2,000	OK
2	1 a 35	2.2.5.	Deve permitir a criação e distribuição de políticas de segurança e de objetos de rede de forma centralizada.	Sim	FortiManager-5.4.3-Administration-Guide.pdf	183	Policy & Objects The Policy & Objects pane enables you to centrally manage and configure the devices that are managed by the FortiManager unit. This includes the basic network settings to connect the device to the corporate network, antivirus definitions, intrusion protection signatures, access rules, and managing and updating firmware for the devices. All changes related to policies and objects should be made on the FortiManager device, and not on the managed devices.	OK
2	1 a 35	2.2.6.	Deve permitir a criação de relatórios customizados.	Sim	FortiManager-5.4.3-Administration-Guide.pdf FortiAnalyzer-5.6.0-Administration-Guide.pdf	35132	Reports Configure and generate reports for logging devices. This tab can be hidden by disabling the FortiAnalyzer feature set. Reports You can generate data reports from logs by using the Reports feature. You can do the following: I Use predefined reports. Predefined report templates, charts, and macros are available to help you create new reports. I Create customize reports	OK

Lote	Item do Lote	Item	Descrição do Item	Atende	Referência/Documento	Página	Observações	Análise do grupo técnico
2	1 a 35	2.2.7.	Deve possibilitar a filtragem dos logs do equipamento por, no mínimo: aplicação, endereço IP de origem e destino, país de origem e destino, usuário e horário.	Sim	FortiAnalyzer-5.6.0-Administration-Guide.pdf FortiOS-5.4.4-Log-Reference	111-11211	<p>You can view log information by device or by log group.</p> <p>Filtering log messages You can filter log messages using filters in the toolbar or by using the right-click menu. Filters are not case-sensitive by default. To use case-sensitive filters, select Tools > Case Sensitive Search. To filter log messages using filters in the toolbar:</p> <ol style="list-style-type: none"> 1. Go to the log view you want. 2. Click Add Filter. 3. In the Device list, select a device. 4. In the Time list, select a time period. <p>Then if you type "Skype" in the Add Filter box, FortiAnalyzer searches for "Skype" within these indexed fields: app,dstip,proto,service,srcip,user, and utmaction.</p> <p>Find log entries containing any of the search terms. Separate the terms with "or" or a comma ",". Examples: 1) user=henry or srcip=10.1.0.15</p> <p>Following is an example of traffic log message in raw format. The body fields are highlighted in bold.</p> <pre>date=2014-07-04 time=14:26:59 logid=0001000014 type=traffic subtype=local level=notice vd=vdom1 srcip=10.6.30.254 srcport=54705 srcintf="mgmt1" dstip=10.6.30.1 dstport=80 dstintf="vdom1" sessionid=350696 status=close policyid=0 dstcountry="Reserved" srccountry="Reserved"trandisp=noop service=HTTP proto=6 app="Web Management" duration=13 sentbyte=1948 rcvbyte=3553 sentpkt=9 rcvdpkt=9 devtype="Fortinet Device" osname="Fortinet OS" mastersrcmac=00:09:0f:67:6c:31</pre>	OK
2	1 a 35	2.2.8.	Deve possuir relatórios com informações consolidadas sobre: as mais frequentes fontes de sessões bloqueadas com seus destinos e serviços, os mais frequentes ataques e ameaças de segurança detectadas com suas origens e destinos, os serviços de rede mais utilizados, as aplicações maiores consumidoras de banda de Internet, os usuários que consomem mais banda de Internet, os sites na Internet mais visitados.	Sim	fortios-handbook-54.pdf FortiAnalyzer - Bandwidth and Applications Report.pdf FortiAnalyzer - Threat Report.pdf FortiAnalyzer - Top 20 Category and Websites.pdf FortiAnalyzer - User Security Analysis.pdf FortiAnalyzer - Top Allowed and Blocked	32-62-52-15	<p>Exporting filtered summaries You can export filtered FortiView summaries or any level of the drilldowns to PDF and report charts. Filtered summaries are always exported in table format.</p> <p>Traffic Top Sources Displays the highest network traffic by source IP address and interface, device, threat score (blocked and allowed), sessions (blocked and allowed), and bytes (sent and received).</p> <p>Top Destinations Displays the highest network traffic by destination IP addresses, the applications used to access the destination, sessions, and bytes.</p> <p>Application Traffic Top 30 Applications by Bandwidth and Sessions</p> <p>Users Top 30 Users by Bandwidth and Sessions</p> <p>Top 20 Category and Websites (Session)</p> <p>User Security Analysis</p> <p>Top 500 Allowed Applications by Bandwidth Top 500 Blocked Applications by Session</p>	OK
2	1 a 35	2.2.9.	Deve permitir a geração automática e agendada dos relatórios.	Sim	FortiAnalyzer-5.6.0-Administration-Guide.pdf	154	<p>Managing report schedules You can manage report schedules in Reports > Advanced > Report Calendar. To edit a report schedule:</p> <ol style="list-style-type: none"> 1. In Report Calendar, right-click an upcoming calendar entry, and select Edit. 2. In the Settings tab of the report that opens, edit the corresponding report schedule. <p>To disable a report schedule: In Report Calendar, right-click an upcoming calendar entry, and select Disable. All scheduled instances of the report are removed from the report calendar. Completed reports remain in the report calendar.</p> <p>To delete or download a completed report: In Report Calendar, right-click a past calendar entry, and select Delete or Download. The corresponding completed report will be deleted or downloaded.</p>	OK

Lote	Item do Lote	Item	Descrição do Item	Atende	Referência/Documento	Página	Observações	Análise do grupo técnico
2	1 a 35	2.2.10.	Deve ser capaz de automatizar a aplicação das regras, objetos e políticas desejadas em tempo real a todos os equipamentos e contextos virtuais administrados.	Sim	FortiManager-5.4.3-Administration-Guide.pdf	14,139-141	<p>l Script and automate device provisioning, policy pushing, etc. with JSON APIs or build custom web portals with the XML API,</p> <p>FortiManager scripts enable you to create, execute, and view the results of scripts executed on FortiGate devices, policy packages, the ADOM database, the global policy package, or the DB. Scripts can also be filtered based on different device information, such as OS type and platform.</p> <p>Configuring scripts To configure, import, export, or run scripts, go to Device Manager > Scripts. The script list for your current ADOM will be displayed.</p> <p>Run a script You can select to enable automatic script execution or create a recurring schedule for the script. To run a script: 1. Go to Device Manager > Scripts. 2. Select the script, then right-click and select Run from the menu. 3. Select a device group or devices. 4. Select OK to run the script. The Run Script dialog box will open, showing the progress of the operation and providing information on its success or failure.</p> <p>Syntax applicable for address and address6 config firewall address edit xxxx ...regular FOS command here... config dynamic_mapping edit "<dev_name>:"- "<vdom_name>" set subnet x.x.x.x.x.x.x.x next end</p>	OK
2	1 a 35	2.2.11.	Deverá utilizar comunicação segura criptografada entre a solução de gerência e os equipamentos gerenciados.	Sim	FortiManager-5.4.3-Administration-Guide.pdf http://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-ports-and-protocols-54/03-FGFM.htm	24	<p>Device Manager Device Manager contains all devices that are managed by the FortiManager unit. You can create new device groups, provision and add devices, and install policy packages and device settings. Device Manager communicates with devices by using the FortiGate-FortiManager (FGFM) protocol.</p> <p>Configuring an SSL connection The default encryption automatically sets high and medium encryption algorithms. Algorithms used for High, Medium, and Low follow the openssl definitions below</p>	OK
2	1 a 35	2.2.12.	Deverá manter o histórico de configurações enviadas aos equipamentos e deverá permitir o rollback das configurações.	Sim	FortiManager-5.4.3-Administration-Guide.pdf	124-125	<p>Managing configuration revision history In the Device Manager > Device & Groups pane, select a device group, and then select a device in the lower tree menu. In the device dashboard Configuration and Installation Status widget, select Revision History in the Total Revisions row, to view the FortiManager repository. The repository stores all configuration revisions for the devices, and tags each revision with a version/ID number. You can view the version history, inspect configuration changes, import files from a local computer, view configuration settings, compare different revisions, revert to previous settings, and download configuration files to a local computer.</p>	OK
2	1 a 35	2.2.13.	Deve permitir distribuição centralizada de pacotes de atualização.	Sim	FortiManager-5.4.3-Administration-Guide.pdf	129-130	<p>Upgrade firmware for device groups The firmware of the devices within a group can also be updated as a group. To update device group firmware: 1. Go to Device Manager. 2. In the tree menu, select the device group name, for example, Managed FortiGates. 3. Click the Firmware tab. 4. Locate an applicable firmware image in the Available Upgrade list, then click Upgrade to upgrade all of the devices in the group to that image. The upgrade history is also shown, and can be viewed in more detail by selecting the All History icon.</p>	OK
2	1 a 35	2.2.14.	Deve permitir validar as regras antes, durante ou depois de aplicações.	Sim	FortiManager-5.4.3-Administration-Guide.pdf	58-65	<p>Workflow Mode Workflow mode is used to control the creation, configuration, and installation of policies and objects. It helps to ensure that all changes are reviewed and approved before they are applied.</p> <p>Workflow sessions Administrators use workflow sessions to make changes to policies and objects. The session is then submitted for review and approval or rejection by the administrators defined in the ADOMs workflow approval matrix.</p> <p>Continue Session in Progress Select to continue a session that was previously saved or is already in progress. This option is only available when a session is in progress or saved.</p>	OK
2	1 a 35	2.2.15.	Deve ser capaz de testar a conectividade dos equipamentos gerenciados.	Sim	FortiManager-5.4.3-Administration-Guide.pdf	112	<p>Connectivity - The device connectivity status and the time it was last checked. A green arrow means that the connection between the device and the FortiManager system is up; a red arrow means that the connection is down. Select Refresh to test the connection between the device and the FortiManager system.</p>	OK
2	1 a 35	2.2.16.	Deve prover funcionalidade de detecção de regras conflitantes ou regras equivalentes.	Sim	FortiManager-5.4.3-Administration-Guide.pdf	191	<p>Perform a policy consistency check The policy check tool allows you to check all policy packages within an ADOM to ensure consistency and eliminate conflicts that may prevent your devices from passing traffic. This allows you to optimize your policy sets and potentially reduce the size of your databases.</p>	OK
2	2,9,16,23,30	2.3	Conjunto de funcionalidades IPS/IDS					
2	2,9,16,23,30	2.3.1.	Possuir tecnologia de detecção e prevenção de ataques e intrusões baseada em assinatura;	Sim	fortios-handbook-54.pdf	2575	<p>Intrusion protection The FortiOS Intrusion Protection system combines signature detection and prevention with low latency and excellent reliability. With intrusion protection, you can create multiple IPS sensors, each containing a complete configuration based on signatures. Then, you can apply any IPS sensor to any security policy.</p>	OK
2	2,9,16,23,30	2.3.2.	Possuir, no mínimo, um conjunto de 2.000 (duas mil) assinaturas de detecção e prevenção de ataques, devendo também detectar ataques baseados em anomalias;	Sim	fortiOS_54.pdf	5	IPS and DoS	OK
2	2,9,16,23,30	2.3.3.	Decodificar múltiplos formatos de Unicode;	Sim	http://www.fortiguard.com/search?q=unicode&engine=1 http://www.fortiguard.com/search?q=utf-8&engine=1			OK

Lote	Item do Lote	Item	Descrição do Item	Atende	Referência/Documento	Página	Observações	Análise do grupo técnico
2	2,9,16,23,30	2.3.4.	Suportar fragmentação e desfragmentação IP;	Sim	fortios-handbook-54.pdf	953,1009	<p>SCTP Stream Control Transmission Protocol (SCTP) is part of the Transport Layer of the OSI Model just like TCP and UDP and provides some of the features of both of those protocols. It is message or datagram orientated like UDP but it also ensures reliable sequential transport of data with congestion control like TCP. SCTP provides the following services: Acknowledged error-free non-duplicated transfer of user data Data fragmentation to conform to discovered path MTU size</p> <p>The FortiGate unit automatically reassembles fragmented packets before processing them because fragmented packets can evade security measures. Both IP packets and TCP packets are reassembled by the IPS engine before examination.</p>	OK
2	2,9,16,23,30	2.3.5.	Detectar protocolos independentemente da porta utilizada, identificando aplicações conhecidas em portas não-padrão;	Sim	fortios-handbook-54.pdf	2576	<p>Protocol decoders Before examining network traffic for attacks, the IPS engine uses protocol decoders to identify each protocol appearing in the traffic. Attacks are protocol-specific, so your FortiGate unit conserves resources by looking for attacks only in the protocols used to transmit them. For example, the FortiGate unit will only examine HTTP traffic for the presence of a signature describing an HTTP attack.</p>	OK
2	2,9,16,23,30	2.3.6.	Detectar e Proteger contra, no mínimo, ataques de RPC (Remote Procedure Call), Windows ou NetBios, SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol), DNS (Domain Name System), FTP, SSH , Telnet, ICMP (Internet Control Message Protocol), SIP, SNMP, SSDP ou CHARGEN, RDP (Remote Desktop Protocol), DoS (Denial of Service) e ataques com assinaturas complexas, tais como ataques TCP hijacking.	Sim	<p>https://fortiguard.com/search?q=rpc&type=ips&engine=1 https://fortiguard.com/search?q=smt&type=ips&engine=1 https://fortiguard.com/search?q=imap&type=ips&engine=1 https://fortiguard.com/search?q=pop&type=ips&engine=1 https://fortiguard.com/search?q=dns&type=ips&engine=1 https://fortiguard.com/search?q=ftp&type=ips&engine=1 https://fortiguard.com/search?q=ssh&type=ips&engine=1 https://fortiguard.com/search?q=telnet&type=ips&engine=1 https://fortiguard.com/search?q=icmp&type=ips&engine=1 https://fortiguard.com/search?q=sip&type=ips&engine=1 https://fortiguard.com/search?q=snmp&type=ips&engine=1 https://fortiguard.com/search?q=ssdp&type=ips&engine=1 https://fortiguard.com/search?q=rdp&type=ips&engine=1 https://fortiguard.com/search?q=dos&type=ips&engine=1</p>		OK	
2	2,9,16,23,30	2.3.7.	Possuir proteção contra os ataques como, mas não restringindo-se aos mesmos : 1) Ataques de Worm, Trojan, Backdoors, Portscans, IP Spoofing, DoS, Spywares, Botnets e malwares em geral; 2) Ataques e utilização de tecnologia P2P; 3) Ataques de estouro de pilha (buffer overflow); 5) Tráfego mal formado; 6) Cabeçalhos inválidos de protocolo; 6) Ataques de injeção (SQL Injection, LDAP Injection) e de Cross-Site Scripting; 7) Elevação de privilégio e 8) Exploits - Web Server, Web Browser ActiveX, JavaScript, Browser Plug-ins/Add-nos.	Sim	<p>fortios-handbook-54.pdf http://www.fortiguard.com/search?q=worm&type=ips&engine=1 http://www.fortiguard.com/search?q=trojan&engine=1 https://fortiguard.com/search?q=backdoor&type=ips&engine=1 https://fortiguard.com/search?q=portscan&type=ips&engine=1 https://fortiguard.com/search?q=dos&type=ips&engine=1 https://fortiguard.com/search?q=spyware&type=ips&engine=1 https://fortiguard.com/search?q=botnet&type=ips&engine=1 https://fortiguard.com/search?q=malware&type=ips&engine=1 https://fortiguard.com/search?q=p2p&type=ips&engine=1 https://fortiguard.com/search?q=buffer%20overflow&type=ips&engine=1 https://fortiguard.com/search?q=sql%20injection&type=ips&engine=1 https://fortiguard.com/search?q=ldap%20injection&type=ips&engine=1 https://fortiguard.com/search?q=cross%20site%20scripting&type=ips&engine=1</p>	355,2404,2473	<p>Reverse path lookup Whenever a packet arrives at one of the FortiGate unit's interfaces, the unit determines whether the packet was received on a legitimate interface by doing a reverse lookup using the source IP address in the packet header. This is also called anti-spoofing. If the FortiGate unit cannot communicate with the computer at the source IP address through the interface on which the packet was received, the FortiGate unit drops the packet as it is likely a hacking attempt.</p> <p>IP integrity header checking reads the packet headers to verify if the packet is a valid TCP, UDP, ICMP, SCTP or GRE packet. The only verification that is done at this step to ensure that the protocol header is the correct length. If it is, the packet is allowed to carry on to the next step. If not, the packet is dropped.</p> <p>Network interfaces associated with a port attached to a Network Processor (NP) can be configured to offload anomaly checking, further offloading the CPU for greater performance. Some of the anomaly traffic dropped includes LAND attacks, IP protocol with malformed options, and WinNukes.</p>	OK

Lote	Item do Lote	Item	Descrição do Item	Atende	Referência/Documento	Página	Observações	Análise do grupo técnico
2	2,9,16,23,30	2.3.8.	Emitir alarmes na console de administração integrada, alertas via correio eletrônico, syslog e traps SNMP;	Sim	FortiManager-5.4.3-Administration-Guide.pdf	135,350,355	Alert Email SMTP Server settings including server, authentication, SMTP user, and password. Configure in the system template or import settings from a specific device. Select Apply to save the setting. Hover over the widget heading to select the following options: I Import: Import alert email settings from a specific device. Select the device in the drop-down list. Select OK to import settings. Select Apply to save the settings. I Close: Close the widget and remove it from the system template. Configuring a SNMPv3 user The FortiManager SNMPv3 implementation includes support for queries, traps, authentication, and privacy. Select Create New in the SNMPv3 toolbar to open the New SNMP User page, where you can configure a new SNMP user. You can also edit and delete existing SNMPv3 users. Syslog server Configure syslog server settings for alerts, edit existing settings, or delete syslog servers.	OK
2	2,9,16,23,30	2.3.9.	Permitir monitoração do comportamento do equipamento mediante o protocolo SNMP;	Sim	FortiManager-5.4.3-Administration-Guide.pdf	346	SNMP SNMP is a method for a FortiManager system to monitor and report on FortiGate devices. It also can allow you to monitor a FortiManager system on your local computer. You will need an SNMP agent on your computer to read the SNMP information.	OK
2	2,9,16,23,30	2.3.10.	Atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;	Sim	fortios-handbook-54.pdf	2472,2481	Real-Time & Zero-day Protection The FortiGuard Intrusion Prevention Service (IPS) provides customers with the latest defenses against stealthy network-level threats through a constantly updated database of known threats and behavior-based signatures. FortiGuard IPS service quick facts I Over 10,000 signatures consisting of 18,000 rules I Approximately 470,000 network intrusion attempts resisted per minute I About 1,000 rules are updated or added per week I Over 300 Zero-day vulnerabilities discovered to date This update service is backed by a team of threat experts and a close relationship with major application vendors. The best-in-class team also uncovers significant zero-day vulnerabilities continuously, providing FortiGate units with advanced protection ahead of vendor patches. I Subscribe to FortiGuard IPS Updates and configure your FortiGate unit to receive push updates. This will ensure you receive new IPS signatures as soon as they are available.	OK
2	2,9,16,23,30	2.3.11.	Permitir filtros de anomalias de tráfego estatístico de flooding, scan e source session limits;	Sim	fortios-handbook-54.pdf	1032,1033	The listing of anomaly profiles includes: L3 Anomalies I ip_src_session I ip_dst_session L4 Anomalies I tcp_syn_flood I tcp_port_scan I tcp_src_session I tcp_dst_session I udp_flood I udp_scan I udp_src_session I udp_dst_session I icmp_flood I icmp_sweep I icmp_src_session I sctp_flood I sctp_scan I sctp_src_session I sctp_dst_session	OK
2	2,9,16,23,30	2.3.12.	Permitir filtros de anomalias de protocolos, inclusive protocolos de aplicação (ex.: HTTP, SMTP, NTP, NetBIOS, HTTPS, FTP, DNS, SMB, RPC, SSH e Telnet);	Sim	2.3.12_Print.png	1		OK
2	2,9,16,23,30	2.3.13.	Deve resistir a técnicas de evasão ou ataques direcionados ao próprio equipamento, suportando, no mínimo, as técnicas: IP Packet Fragmentation, Stream Segmentation, RPC Fragmentation, URL Obfuscation, HTML Obfuscation, Payload Encoding, FTP Evasion e Layered Evasions.	Sim	fortios-handbook-54.pdf http://www.fortiguard.com/encyclopedia/ips/12631/chunked-transferencoding http://www.fortiguard.com/encyclopedia/ips/12654/ftp-protocol-bounce-attack	2476	Resistant Against Evasions Evasion techniques attempt to fool the protocol decoders in IPS products by crafting exotic network streams that would not be handled or reconstructed by the decoders, yet still be valid enough for the target recipient to process. Robust IPS engine is capable of handling both common evasions and sophisticated AETs (Advanced Evasion Techniques) deployed by hackers such as IP Packet Fragmentation, TCP Stream Segmentation, RPC Fragmentation, URL & HTML Obfuscation, and other protocolspecific evasion techniques.	OK
2	2,9,16,23,30	2.3.14.	Possuir funcionalidade que permita desativar a análise de assinaturas e protocolos;	Sim	fortios-handbook-54.pdf	2476	Rating Override At times, administrators may have to allow approved people to access what they need during periods when an exception to the normal rules is required, while still having enough control that the organization's web usage policies are not compromised. FortiOS can provide such setup by using alternate profiles.	OK

Lote	Item do Lote	Item	Descrição do Item	Atende	Referência/Documento	Página	Observações	Análise do grupo técnico
2	2,9,16,23,30	2.3.15.	Possuir funcionalidade que permita desativar a análise de ataques a partir de endereços/faixa IP específicos;	Sim	fortigate-cli-ref-54.pdf http://kb.fortinet.com/kb/microsites/search.do?cmd=displayKC&docType=kc&externalId=FD40588&silcId=1&docTypeId=DT_KCARTICLE_1_1&dialogID=114892324&statId=0%200%20114890947	129	config exempt-ip This subcommand is available after rule has been set. edit <exempt-ip_id> Enter the ID number of an exempt-ip entry. For a list of the exempt-ip entries in the IPS sensor, enter ? instead of an ID. Enter a new ID to create a new exempt-ip. dst-ip <ip4mask> Enter destination IP address and netmask to exempt. src-ip <ip4mask> Enter source IP address and netmask to exempt. Technical Note: Exempting IP addresses from IPS sensor scanning	OK
2	2,9,16,23,30	2.3.16.	Permitir o funcionamento mínimo do engine de IPS mesmo que a comunicação com o site do fabricante esteja fora de operação;	Sim	fortios-handbook-54.pdf	250,307	When a new FortiGate is powered on, it automatically searches for FortiGuard services. If the FortiGate is configured for central management, it will look for FortiGuard services on the configured FortiManager system. The FortiGate sends its serial number to the FortiGuard service provider, which then determines whether the FortiGate is registered and has valid contracts for FortiGuard subscriptions and FortiCare support services. If the FortiGate is registered and has a valid contract, the License Information is updated. The FortiGuard team can be found around the globe, monitoring virus, spyware and vulnerability activities. As vulnerabilities are found, signatures are created and pushed to the subscribed FortiGates. Intrusion Prevention System (IPS) - The FortiGuard Intrusion Prevention System (IPS) uses a customizable database of more than 4000 known threats to stop attacks that evade conventional firewall defenses. It also provides behavior-based heuristics, enabling the system to recognize threats when no signature has yet been developed. It also provides more than 1000 application identity signatures for complete application control.	OK
2	2,9,16,23,30	2.3.17.	Possuir as estratégias de bloqueio e liberação selecionáveis, tanto por conjuntos de assinaturas quanto por cada assinatura;	Sim	fortios-handbook-54.pdf http://cookbook.fortinet.com/protecting-web-server/	2474,2577,2579-2580	Edit IPS Sensor (Imagem) Adding Rate Based Signatures These are a subset of the signatures that are found in the database that are normally set to monitor. This group of signatures is for vulnerabilities that are normally only considered a serious threat when the targeted connections come in multiples, a little like DoS attacks. Adding a rate based signature is straight forward. Select the enable button in the Rate Based Signature table that corresponds with the desired signature. Customized signatures Customized signatures must be created before they can be added to the sensor. To get more details on customized signatures check the Custom Application & IPS Signatures chapter. Custom/predefined signature entries Signature entries allow you to add an individual custom or predefined IPS signature. If you need only one signature, adding a signature entry to an IPS sensor is the easiest way. Signature entries are also the only way to include custom signatures in an IPS sensor. Another use for signature entries is to change the settings of individual signatures that are already included in a filter within the same IPS sensor. Add a signature entry with the required settings above the filter, and the signature entry will take priority.	OK
2	2,9,16,23,30	2.3.18.	Suportar a verificação de ataques na camada de aplicação;	Sim	fortios-handbook-54.pdf	2472	Pattern & Rate-Based Signatures The pattern signature matching technique is essential in IPS implementation due to its high level of precision and accuracy. FortiOS offers administrators robust pattern signature selection using filters based on severity, target, operating system, application, and protocol. Each of the 10,000+ signatures has a direct link to its detailed entry on the threat encyclopedia and CVE-ID references. After selection, administrators are able to assign associated actions such as monitoring, blocking, or resetting the session.	OK
2	2,9,16,23,30	2.3.19.	Possuir gerenciamento gráfico centralizado das funcionalidades de IPS/IDS e monitoramento de seus eventos de forma integrada com a gerência local e a gerência centralizada da solução.	Sim	fortios-handbook-54.pdf	2472,2474,2798	Pattern & Rate-Based Signatures The pattern signature matching technique is essential in IPS implementation due to its high level of precision and accuracy. FortiOS offers administrators robust pattern signature selection using filters based on severity, target, operating system, application, and protocol. Each of the 10,000+ signatures has a direct link to its detailed entry on the threat encyclopedia and CVE-ID references. After selection, administrators are able to assign associated actions such as monitoring, blocking, or resetting the session. Edit IPS Sensor The FortiManager family of appliances supply the tools needed to effectively manage any size Fortinet security infrastructure, from a few devices to thousands of appliances.	OK
2	2,9,16,23,30	2.3.20.	Reconhecer assinaturas seletivas e filtros de ataque que devem proteger contra ataques de negação de serviços automatizados, worms e vulnerabilidades conhecidas.	Sim	http://www.fortiguard.com/search?q=dos&type=ips&engine=1 http://www.fortiguard.com/search?q=ddos&type=ips&engine=1 http://www.fortiguard.com/search?q=worm&type=ips&engine=1 http://www.fortiguard.com/search?q=vulnerability&type=ips&engine=1			OK

Lote	Item do Lote	Item	Descrição do Item	Atende	Referência/Documento	Página	Observações	Análise do grupo técnico
2	2,9,16,23,30	2.3.21.	Caso o IPS/IDS não trate parcialmente ou totalmente DoS, será aceito funcionalidade específica complementar.	Sim	fortios-handbook-54.pdf	1010-1014 2472	Defending against DoS attacks Pattern & Rate-Based Signatures The pattern signature matching technique is essential in IPS implementation due to its high level of precision and accuracy. FortiOS offers administrators robust pattern signature selection using filters based on severity, target, operating system, application, and protocol. Each of the 10,000+ signatures has a direct link to its detailed entry on the threat encyclopedia and CVE-ID references. After selection, administrators are able to assign associated actions such as monitoring, blocking, or resetting the session. Rate-based IPS signatures protect networks against applicationbased DoS and brute force attacks. Administrators can configure nearly 30 rate-based IPS signatures and tune them to their needs. Threshold (incidents per minute) and an action to take when the threshold is reached can be assigned to each signature. If the action is set to block, then a timeout period can be set so that the block is removed after a specified duration.	OK
2	3,10,17,24,31	2.4	Conjunto de funcionalidades antivírus e anti-malware					
2	3,10,17,24,31	2.4.1.	Possuir módulo de proteção de antivírus, anti-malware e anti-bot no mesmo equipamento do firewall;	Sim	fortios-handbook-54.pdf	2496	Antivirus / Antivirus concepts	OK
2	3,10,17,24,31	2.4.2.	Possuir funcionalidade de varredura contra vírus e malwares em tráfego nos seguintes protocolos: HTTPS, HTTP e pelo menos dois dos seguintes: FTP, POP3, IMAP e SMTP;	Sim	fortios-handbook-54.pdf	2496	AntiVirus This section describes how to configure the antivirus options. From an antivirus profile you can configure the FortiGate unit to apply antivirus protection to HTTP, FTP, IMAP, POP3, SMTP, and NNTP sessions. If your FortiGate unit supports SSL/SSH content scanning and inspection, you can also configure antivirus protection for HTTPS, IMAPS, POP3S, SMTPS, and FTPS sessions.	OK
2	3,10,17,24,31	2.4.3.	Deve ser capaz de, se houver algum atraso ou falha na realização da atualização automática, o equipamento deve ter a capacidade de alertar imediatamente o administrador através de logs, e-mail ou outros meios de alerta;	Sim	FortiOS-5.4.4-Log-Reference.pdf	253,390.	20113 - LOG_ID_IPSA_DOWNLOAD_FAIL 32116 - LOG_ID_UPD_SIGN_AVPKG_FAILURE	OK
2	3,10,17,24,31	2.4.4.	Deve possuir serviço de atualização automática e manual de assinaturas com o fabricante;	Sim	fortios-handbook-54.pdf	311	Manual updates / Automatic updates	OK
2	3,10,17,24,31	2.4.5.	Suportar funcionamento mínimo da engine de antivírus e anti-malwares mesmo que a comunicação com o site do fabricante esteja fora de operação;	Sim	fortios-handbook-54.pdf	250,307	When a new FortiGate is powered on, it automatically searches for FortiGuard services. If the FortiGate is configured for central management, it will look for FortiGuard services on the configured FortiManager system. The FortiGate sends its serial number to the FortiGuard service provider, which then determines whether the FortiGate is registered and has valid contracts for FortiGuard subscriptions and FortiCare support services. If the FortiGate is registered and has a valid contract, the License Information is updated. The FortiGuard team can be found around the globe, monitoring virus, spyware and vulnerability activities. As vulnerabilities are found, signatures are created and pushed to the subscribed FortiGates. AntiVirus -The FortiGuard AntiVirus Service provides fully automated updates to ensure protection against the latest content level threats. It employs advanced virus, spyware, and heuristic detection engines to prevent both new and evolving threats from gaining access to your network and protects against vulnerabilities.	OK
2	3,10,17,24,31	2.4.6.	Possuir gerenciamento gráfico centralizado das funcionalidades de antivírus e anti-malware integrado com a gerência local e a gerência centralizada da solução.	Sim	fortios-handbook-54.pdf	2463,2798	Inside FortiOS: AntiVirus AntiVirus uses a suite of integrated security technologies to provide against a variety of threats, including both known and unknown malicious codes (Malware), plus Advanced Targeted Attacks (ATA), also known as Advanced Persistent Threats (APT). The FortiManager family of appliances supply the tools needed to effectively manage any size Fortinet security infrastructure, from a few devices to thousands of appliances. FortiManager appliances provide centralized policy-based provisioning, configuration, and update management, as well as end-to-end network monitoring for added control. Managers can control administrative access and simplify policy deployment using role-based administration to define user privileges for specific management domains and functions by aggregating collections of Fortinet appliances and agents into independent management domains. By locally hosting security content updates for managed devices and agents, FortiManager appliances minimize web filtering rating request response time and maximize network protection.	OK
2	3,10,17,24,31	2.4.7.	Identificação, classificação e bloqueio de malwares, contemplando no mínimo, Trojan, Spywares, Backdoors, Worms e Vírus;	Sim	fortios-handbook-54.pdf	2497	Malware threats Malware is the general term covering all the different types of threats to your computer safety such as: I Viruses I Worms I Trojan horses I Ransomware I Scareware I Spyware I Adware I Botnets FortiOS Handbook for FortiOS 5.4.4 Fortinet Technologies Inc. 2496 AntiVirus I Phishing I Grayware	OK
2	4,11,18,25,32	2.5	Conjunto de funcionalidades para tratamento de conteúdo web					
2	4,11,18,25,32	2.5.1.	Deve possuir funcionalidades de tratamento de conteúdo web, devendo sua base de dados conter, no mínimo, 10 (dez) milhões de sites internet web já registrados e classificados, distribuídos em, no mínimo, 40 (quarenta) categorias ou subcategorias pré-definidas;	Sim	fortios-handbook-54.pdf	2476	Superior Coverage FortiGuard Web Filter ratings are performed by a combination of proprietary methods including text analysis, exploitation of the web structure, and human raters. This service currently rates more than 250 million sites covering billions of URLs with each site able to be rated in multiple categories. The FortiGuard database provides a truly international service with support for 70 languages. Extensive and Flexible Categorization Rated URLs are assigned into one of the 98 categories (including 20 user defined ones) which administrators can then easily manage and control. Administrators can configure and populate local categories or place specific URLs in existing categories should the FortiGuard rating not be in agreement with an organization's policies and practices.	OK
2	4,11,18,25,32	2.5.2.	Permitir a criação de categorias personalizadas;	Sim	fortios-handbook-54.pdf	252	Local categories Users can define custom or local categories. See Overriding FortiGuard Website Categorization for details	OK
2	4,11,18,25,32	2.5.3.	Permitir a categorização e reclassificação de sites web por URL;	Sim	fortios-handbook-54.pdf	2528	The different methods of override There are actually two different ways to override web filtering behavior based on FortiGuard categorization of a websites. The second method has two variations in implementation and each of the three has a different level of granularity.	OK

Lote	Item do Lote	Item	Descrição do Item	Atende	Referência/Documento	Página	Observações	Análise do grupo técnico
2	4,11,18,25,32	2.5.4.	Suportar filtragem e categorização das URLs;	Sim	fortios-handbook-54.pdf	2518	Web filter This section describes FortiGate web filtering for HTTP traffic. The three main parts of the web filtering function, the Web Content Filter, the URL Filter, and the FortiGuard Web Filtering Service interact with each other to provide maximum control over what users on your network can view as well as protection to your network from many Internet content threats. Web Content Filter blocks web pages containing words or patterns that you specify. URL filtering uses URLs and URL patterns to block or exempt web pages from specific sources. FortiGuard Web Filtering provides many additional categories you can use to filter web traffic.	OK
2	4,11,18,25,32	2.5.5.	Possuir integração com serviços de diretório LDAP e Microsoft Active Directory para autenticação de usuários;	Sim	fortios-handbook-54.pdf	529	Server-based password authentication Using external authentication servers is desirable when multiple FortiGate units need to authenticate the same users, or where the FortiGate unit is added to a network that already contains an authentication server. FortiOS supports the use of LDAP, RADIUS, TACACS+, AD or POP3 servers for authentication.	OK
2	4,11,18,25,32	2.5.6.	Permitir a criação de regras de acesso/bloqueio baseadas em usuários ou grupo de usuários do LDAP e do Microsoft Active Directory;	Sim	fortios-handbook-54.pdf	1019,1020	Server-based password authentication To configure a IPv4 policy in the GUI Set the Source parameter by selecting the field with the "+" next to the field label. The source in this case is either the source address, source user or source device of the initiating traffic. When the field is selected a window will slide out from the right. Tabs indicating Address, User or Device options are there to help categorize the options along with the option to search. In order to be able to select one of these options it needs to be configured as a firewall object before hand. The "+" icon next to the Search field is a shortcut for creating a new firewall object based on the tab that is currently selected. For the Address and Device tabs, single or multiple options can be selected unless the all option is chosen in which case, it will be the only option.	OK
2	4,11,18,25,32	2.5.7.	Permitir a criação de regras para acesso/bloqueio por endereço IP de origem e sub-rede de origem;	Sim	fortios-handbook-54.pdf	1019-1020	To configure a IPv4 policy in the GUI Set the Source parameter by selecting the field with the "+" next to the field label. The source in this case is either the source address, source user or source device of the initiating traffic. When the field is selected a window will slide out from the right. Tabs indicating Address, User or Device options are there to help categorize the options along with the option to search. In order to be able to select one of these options it needs to be configured as a firewall object before hand. The "+" icon next to the Search field is a shortcut for creating a new firewall object based on the tab that is currently selected. For the Address and Device tabs, single or multiple options can be selected unless the all option is chosen in which case, it will be the only option.	OK
2	4,11,18,25,32	2.5.8.	Permitir a criação de quotas de utilização por horário, ou por categorias, ou por aplicações;	Sim	fortios-handbook-54.pdf	2527	FortiGuard Web Filtering usage quotas In addition to using category and classification blocks and overrides to limit user access to URLs, you can set a daily quota by category, category group, or classification. Quotas allow access for a specified length of time or a specific bandwidth, calculated separately for each user. Quotas are reset every day at midnight.	OK
2	4,11,18,25,32	2.5.9.	Deve ser capaz de exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários, na tentativa de acesso a recursos proibidos ou restringidos pela política de segurança do órgão;	Sim	fortios-handbook-54.pdf	2816-2817	Replacement messages The replacement message list in System > Replacement Messages. The replacement messages list enables you to view and customize replacement messages. Highlight the e replacement messages you wish to edit and customize the message content to your requirements. Hit Save when done.	OK
2	4,11,18,25,32	2.5.10.	Permitir o bloqueio de páginas web por meio da construção de filtros específicos com mecanismo de busca textual;	Sim	fortios-handbook-54.pdf	2538	Static URL Filter You can allow or block access to specific URLs by adding them to the Static URL Filter list. You add the URLs by using patterns containing text and regular expressions. The FortiGate unit allows or blocks web pages matching any specified URLs or patterns and displays a replacement message instead.	OK
2	4,11,18,25,32	2.5.10.1.	O item 2.5.10 pode ser atendido através da criação de aplicações em camada 7 customizadas.	Sim	De acordo	N/A		OK
2	4,11,18,25,32	2.5.11.	Permitir o bloqueio de URLs cujo campo CN ou DN não contém um domínio válido para o certificado SSL;	Sim	fortios-handbook-54.pdf	2633	Allow Invalid SSL Certificate This setting was something that used to be part of the Proxy Options, but now that SSL inspection has it's own configuration setting it is configured with those. It might seem like a straightforward decision that the allowing of invalid SSL certificates must be bad and therefore should not be allowed, but there can be some reasons that should be considered. The issues at hand are the reasons to use a SSL certificate and the reasons that a certificate will be considered invalid.	OK
2	4,11,18,25,32	2.5.12.	Permitir o bloqueio de páginas web por classificação, tais como páginas de streaming, rádio e tv online, P2P, URLs originadas de spam, sites de proxy anônimos, entre outros.	Sim	fortios-handbook-54.pdf	2525-2526	FortiGuard Web Filtering categories ID Category 25 Streaming Media and Download 75 Internet Radio and TV 72 Peer-to-peer File Sharing 86 Spam URLs 59 Proxy Avoidance	OK
2	4,11,18,25,32	2.5.13.	Permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueadas – lista negra;	Sim	fortios-handbook-54.pdf	2538	Static URL Filter You can allow or block access to specific URLs by adding them to the Static URL Filter list. You add the URLs by using patterns containing text and regular expressions. The FortiGate unit allows or blocks web pages matching any specified URLs or patterns and displays a replacement message instead	OK
2	4,11,18,25,32	2.5.14.	Possuir categorização de sites governamentais nacionais, mesmo não tendo domínio “.gov” ou “.gov.br.”	Sim	fortios-handbook-54.pdf http://www.fortiguard.com/webfilter?q=www12.senado.leg.br http://www.fortiguard.com/webfilter?q=https%3A%2F%2Fwww.congresso.nacional.leg.br%2Fportal	2527	51 Government and Legal Organizations	OK
2	4,11,18,25,32	2.5.15.	Categorizar as URLs com taxa de acerto mínima de 80% (oitenta por cento), não sendo consideradas neste percentual categorização genérica ou similar.	Sim	Será aferido no “Teste de Assertividade” como exigido pelo item 5.2.6 do Anexo E do Termo de Referência			A ser validado em testes
2	4,11,18,25,32	2.5.16.	Suportar e forçar pesquisas seguras em pelo menos dois sistemas de buscas, contemplando Google e/ou Bing e/ou Yahoo.	Sim	fortios-handbook-54.pdf	2535	SafeSearch SafeSearch is a feature of popular search sites that prevents explicit web sites and images from appearing in search results. Although SafeSearch is a useful tool, especially in educational environments, the resourceful user may be able to simply turn it off. Enabling SafeSearch for the supported search sites enforces its use by rewriting the search URL to include the code to indicate the use of the SafeSearch feature. For example, on a Google search it would mean adding the string “&safe=active” to the URL in the search.	OK
2	5,12,19,26,33	2.6.	Conjunto de funcionalidades para controle de aplicações e análise profunda					

Lote	Item do Lote	Item	Descrição do Item	Atende	Referência/Documento	Página	Observações	Análise do grupo técnico
2	5,12,19,26,33	2.6.1.	Possuir módulo de filtro de aplicações e de conteúdo desenvolvido e mantido pelo próprio fabricante, no mesmo equipamento do firewall;	Sim	fortios-handbook-54.pdf fortigate-whats-new-56.pdf	2562 65	Application Control Using the Application Control Security Profile feature, your FortiGate unit can detect and take action against network traffic depending on the application generating the traffic. Based on FortiGate Intrusion Protection protocol decoders, application control is a user-friendly and powerful way to use Intrusion Protection features to log and manage the behavior of application traffic passing through the FortiGate unit. Application control uses IPS protocol decoders that can analyze network traffic to detect application traffic even if the traffic uses nonstandard ports or protocols. Application Control is a free service Application Control is now a free FortiGuard service and the database for Application Control signatures is separate from the IPS database. However, Botnet Application signatures are still part of the IPS signature database since these are more closely related with security issues and less about application detection. With the release of FortiOS 5.6.1, Application Control signature database information is displayed under on the System > FortiGuard page in the FortiCare section. And the Botnet category is no longer available when searching the Application Signatures list.	OK
2	5,12,19,26,33	2.6.2.	Deve ser capaz de identificar as aplicações mesmo que não estejam utilizando sua porta default.	Sim	fortios-handbook-54.pdf	2562	Application control concepts You can control network traffic generally by the source or destination address, or by the port, the quantity or similar attributes of the traffic itself in the security policy. If you want to control the flow of traffic from a specific application, these methods may not be sufficient to precisely define the traffic. To address this problem, the application control feature examines the traffic itself for signatures unique to the application generating it. Application control does not require knowledge of any server addresses or ports. The FortiGate unit includes signatures for over 1000 applications, services, and protocols.	OK
2	5,12,19,26,33	2.6.3.	Deve ser capaz de identificar aplicações encapsuladas dentro de protocolos, como HTTP e HTTPS.	Sim	fortios-handbook-54.pdf	2467	Inside FortiOS: Application Control Application control technologies detect and take action against network traffic based on the application that generated the traffic. Application control uses protocol decoders with signatures that analyze network traffic to detect application traffic, even if the traffic uses nonstandard ports or protocols. Enhance Control and Network Visibility Controlling and monitoring applications on a network can seem like a daunting task due to the wide range of available applications. It is no longer an option to simply block or allow TCP and/or UDP ports since most applications do not map to individual ports. For example, controlling traffic on an HTTP or HTTPS port is futile against complex social networking sites and cloud applications.	OK
2	5,12,19,26,33	2.6.4.	Deve ser capaz de identificar aplicações que utilizam comunicação criptografada através de SSL.	Sim	fortios-handbook-54.pdf	2469	SSL Inspection for Encrypted Traffic SSL (Secure Sockets Layer) is a popular encryption standard used to protect Internet traffic but may also be used to evade traditional inspection. FortiOS enables organizations to adopt effective application control even when traffic is encrypted.	OK
2	5,12,19,26,33	2.6.5.	Permitir o agrupamento de aplicações em grupos personalizados;	Sim	fortios-handbook-54.pdf	2564	These actions are briefly defined under Application Control actions on page 2566. 3. If you wish to add individual applications, select Add Signatures under Application Overrides. a. Use the Add Filter search field to narrow down the list of possible signatures by a series of attributes. b. When finished, select Use Selected Signatures. 4. If you wish to add advanced filters, select Add Filter under Filter Overrides.	OK
2	5,12,19,26,33	2.6.6.	Garantir que as atualizações regulares do produto sejam realizadas de forma transparente, sem paradas perceptíveis dos serviços;	Sim	fortios-handbook-54.pdf	311	Automatic updates The FortiGate can be configured to request updates from the FortiGuard Distribution Network. You can configure this to be on a scheduled basis, or with push notifications.	OK
2	5,12,19,26,33	2.6.7.	Identificar aplicações e permitir ou bloquear sua utilização, independentemente das portas e protocolos utilizados para conexão (inclusive tráfego criptografado), assim como possuir categorias para classificação das aplicações, bem como das técnicas de evasões utilizadas;	Sim	fortios-handbook-54.pdf	2562, 2469	Application control concepts You can control network traffic generally by the source or destination address, or by the port, the quantity or similar attributes of the traffic itself in the security policy. If you want to control the flow of traffic from a specific application, these methods may not be sufficient to precisely define the traffic. To address this problem, the application control feature examines the traffic itself for signatures unique to the application generating it. Application control does not require knowledge of any server addresses or ports. The FortiGate unit includes signatures for over 1000 applications, services, and protocols. SSL Inspection for Encrypted Traffic SSL (Secure Sockets Layer) is a popular encryption standard used to protect Internet traffic but may also be used to evade traditional inspection. FortiOS enables organizations to adopt effective application control even when traffic is encrypted.	OK
2	5,12,19,26,33	2.6.8.	Possuir, no mínimo, proteção para aplicações do tipo P2P, Instant Messaging, Web e VOIP;	Sim	fortios-handbook-54.pdf	2468/2568	Imagem " Categories" Blocking instant messaging	OK
2	5,12,19,26,33	2.6.9.	Possuir perfis/políticas de segurança de aplicações pré-definidas/pré-configuradas na solução;	Sim	fortios-handbook-54.pdf	2571	4. Go to Security Profiles > Application Control and edit the default policy. 5. Under Application Overrides, select Add Signatures. The new signature should appear at the top of the list. If it does not, search for the signature's name. 6. Select the signature, then select Use Selected Signatures. 7. Go to Policy & Objects > IPv4 Policy and edit the policy that allows connections from the internal network to the Internet. 8. Under Security Profiles, turn on Application Control and use the default profile.	OK
2	5,12,19,26,33	2.6.10.	Possuir atualização manual e automática de novas assinaturas;	Sim	fortios-handbook-54.pdf	311	Manual updates / Automatic updates	OK

Lote	Item do Lote	Item	Descrição do Item	Atende	Referência/Documento	Página	Observações	Análise do grupo técnico
2	5,12,19,26,33	2.6.11.	Permitir a criação de regras de acesso/bloqueio baseadas em usuários ou grupo de usuários do LDAP e do Microsoft Active Directory;	Sim	fortios-handbook-54.pdf	9,1020,1021	<p>IPv4 Policy</p> <p>5. Set the Source parameter by selecting the field with the "+" next to the field label. The source in this case is either the source address, source user or source device of the initiating traffic. When the field is selected a window will slide out from the right. Tabs indicating Address, User or Device options ...</p> <p>Disable or enable the various Security Profiles.</p> <p>Once a Profile has been toggled into the enabled mode a drop down menu will appear for the purpose of choosing a specific profile. Only one profile can be chosen for each profile type. The "+" icon next to the Search field in the drop down menu is a shortcut for creating a new profile.</p> <p>The list of Security Profiles available to set includes:</p> <ul style="list-style-type: none">I AntiVirusI Web FilterI DNS FilterI Application ControlI CASII IPSI Anti-SpamI DLP SensorI VoIPI ICAPI Web Application FirewallI Proxy OptionsI SSL/SSH Inspection	OK
2	5,12,19,26,33	2.6.12.	Deve ser capaz de identificar e filtrar um mínimo de 1.500 (mil e quinhentas) aplicações, contemplando no mínimo: peer-to-peer, streaming e download de áudio, streaming e download de vídeo, update de software, instant messaging, redes sociais, proxies, anonymizers, acesso e controle remoto, VOIP e email.	Sim	fortios-handbook-54.pdf	2564, 2469	<ul style="list-style-type: none">I BotnetI BusinessI Cloud.ITI CollaborationI EmailI GameI General.InterestI MobileI Network.ServiceI P2PI ProxyI Remote.AccessI Social.MediaI Storage.BackupI UpdateI Video/AudioI VoIPI Web.Clients <p>Advanced Application Detection and Control</p> <p>An application and its specific activity are identified using FortiGuard's Application Control database of over 2,500 distinct signatures. These signatures are crafted by researchers across the globe to include applications that may</p>	OK
2	5,12,19,26,33	2.6.13.	Identificação, bloqueio e restrição em profundidade e granularidade de aplicações, contemplando no mínimo: Bittorrent, Youtube, Livestream, Skype, Viber, WhatsApp, Snapchat, Facebook, Facebook Messenger, Google+, Google Talk, Google Docs, Instagram, Twitter, LinkedIn, Dropbox, Google Drive, One Drive, Logmein, Teamviewer, MS-RDP, VNC, Ultrasurf, TOR e Webex.	Sim	https://fortiguards.com/search?q=bittorrent&type=app&engine=1 https://fortiguards.com/search?q=youtube&type=app&engine=1 https://fortiguards.com/search?q=livestream&type=app&engine=1 https://fortiguards.com/search?q=skype&type=app&engine=1 https://fortiguards.com/search?q=viber&type=app&engine=1 https://fortiguards.com/search?q=whatsapp&type=app&engine=1 https://fortiguards.com/search?q=snapchat&type=app&engine=1 https://fortiguards.com/search?q=facebook&type=app&engine=1 https://fortiguards.com/search?q=googleplus&engine=1 https://fortiguards.com/search?q=googletalk&type=ips&engine=1 https://fortiguards.com/search?q=google+docs&engine=1 https://fortiguards.com/search?q=instagram&engine=1 https://fortiguards.com/search?q=twitter&type=app&engine=1 https://fortiguards.com/search?q=linkedin&type=app&engine=1		OK	
2	6,13,20,27,34	2.7	Treinamento oficial para até 5 pessoas					
2	6,13,20,27,34	2.7.1.	Deverá ser fornecido Voucher para treinamento oficial do fabricante.	Sim	De acordo			OK
2	6,13,20,27,34	2.7.2.	A carga horária do treinamento não poderá ser inferior a 24 horas, sendo cada voucher apto para até 5 pessoas. O treinamento é composto por turmas que podem ser formadas de um ou mais Vouchers de uma entidade CONTRATANTE, ou ainda, ser uma turma compartilhada por mais de uma entidade CONTRATANTE. Nos dois casos cada turma se limita a no máximo 10 pessoas.	Sim	De acordo			OK

Lote	Item do Lote	Item	Descrição do Item	Atende	Referência/Documento	Página	Observações	Análise do grupo técnico
2	6,13,20,27,34	2.7.3.	Os treinamentos deverão ser realizados no Brasil, em português, na modalidade presencial, em local fornecido pela CONTRATADA.	Sim	De acordo			OK
2	6,13,20,27,34	2.7.3.1.	O local de treinamento deverá possuir todas as facilidades para um perfeito desempenho das atividades, incluindo os recursos áudio visuais e laboratórios necessários, sem ônus algum para a CONTRATANTE.	Sim	De acordo			OK
2	6,13,20,27,34	2.7.4.	Caberá à CONTRATADA prover todos os recursos didáticos necessários à realização do treinamento, incluindo (mas não se restringindo a) sala de aula, data show, apostilas, bloco de anotações e caneta para cada treinando.	Sim	De acordo			OK
2	6,13,20,27,34	2.7.5.	Os treinamentos deverão ocorrer usando-se turnos diários de até 4 horas cada, podendo ser dois turnos no mesmo dia ou um turno por dia a ser acordado com a CONTRATANTE, com intervalos de, no mínimo, 15 minutos em cada turno e de pelo menos 1 hora entre os turnos que ocorrerem no mesmo dia.	Sim	De acordo			OK
2	6,13,20,27,34	2.7.6.	Toda a documentação didática necessária aos cursos de treinamento deverá ser disponibilizada em papel impresso e mídia digital.	Sim	De acordo			OK
2	6,13,20,27,34	2.7.7.	Os cursos referentes a equipamentos e softwares que façam parte do objeto deverão usar o material oficial de treinamento do respectivo fabricante por meio de qualquer um dos seus respectivos centros autorizados de treinamento.	Sim	De acordo			OK
2	6,13,20,27,34	2.7.8.	São produtos esperados de todos os treinamentos:	Sim	De acordo			OK
2	6,13,20,27,34	2.7.8.1.	Aulas teóricas e práticas.	Sim	De acordo			OK
2	6,13,20,27,34	2.7.8.2.	Material didático contratado e aprovado pela CONTRATANTE.	Sim	De acordo			OK
2	6,13,20,27,34	2.7.8.3.	Referências para estudos e pesquisas complementares.	Sim	De acordo			OK
2	6,13,20,27,34	2.7.9.	A CONTRATANTE poderá, a seu critério, reproduzir o material didático usado e treinar multiplicadores para repetir o treinamento sem custos adicionais. E tal ação não representa a quebra do direito de propriedade do fabricante ou da empresa CONTRATADA. Isso porque o material fornecido não será usado para fins comerciais, mas apenas para uso interno do órgão ou entidade CONTRATANTE com o intuito de disseminar o conhecimento da solução entre os seus servidores profissionais técnicos.	Sim	De acordo			OK
2	6,13,20,27,34	2.7.10.	Os custos referentes ao deslocamento, hospedagem e alimentação dos treinados serão de responsabilidade da CONTRATANTE.	Sim	De acordo			OK
2	6,13,20,27,34	2.7.11.	A ementa do curso deve abranger conteúdos que vão desde configurações básicas até as avançadas dos equipamentos de hardware e de softwares que compõem a solução, bem como sua operação.	Sim	De acordo			OK
2	6,13,20,27,34	3	DEFINIÇÃO DOS LOTES E ITENS					
2	8	3.8.	LOTE 2 - item 01: Firewall multifuncional tipo 2					
2	8	3.8.1.	Requisitos específicos:					
2	8	3.8.1.1.	Atender a todos os requisitos do item 2.1;	Sim	De acordo			OK
2	8	3.8.1.2.	Possuir, no mínimo, o throughput de 250 Mbps para todas as funcionalidades dos itens 2.1, 2.2, 2.3, 2.4, 2.5 e 2.6, ativadas simultaneamente e com inspeção integral de todos os pacotes de dados, independentemente de seu tamanho ou direção de fluxo, levando-se em consideração o perfil de tráfego descrito no ANEXO E.	Sim	FortiGate_80E_Series.pdf	5	Threat Protection Throughput 250Mbps	A ser validado em testes
2	8	3.8.1.3.	O equipamento deve possuir no mínimo 01 (uma) fonte de alimentação, que pode ser interna ou externa, com alimentação nominal de 100~120VAC e 210~230VAC e frequência de 50 ou 60 Hz, ou auto-ranging. Deverá vir acompanhado de cabo de alimentação com, no mínimo, 1,80m (6 pés), com plug tripolar 2P+T no padrão ABNT NBR 14136.	Sim	FortiGate_80E_Series.pdf	6	Power 100–240V AC, 50–60 Hz	OK
2	8	3.8.1.4.	Possuir no mínimo 4 (quatro) portas de 10/100/1000 BASE-T.	Sim	FortiGate_80E_Series.pdf		1. Console Port 2. USB Port 3. 12x GE RJ45 Ports 4. 2x GE RJ45 DMZ/HA Ports 5. 2x GE RJ45/SFP Shared Media Pairs	OK
2	8	3.8.1.5.	Quantidade de sessões simultâneas 90.000.	Sim	FortiGate_80E_Series.pdf	5	Concurrent Sessions (TCP) 1,3 Million	A ser validado em testes
2	8	3.8.1.6.	Quantidade de novas sessões por segundo 12.000.	Sim	FortiGate_80E_Series.pdf	5	New Sessions/Second (TCP) 30,000	A ser validado em testes
2	8	3.8.1.7.	Throughput mínimo de 50 Mbps para IPSec VPN.	Sim	FortiGate_80E_Series.pdf	5	IPsec VPN Throughput 2.5Gbps	A ser validado em testes
2	9	3.9.	LOTE 2 – item 2: Conjunto de funcionalidades IPS/IDS					
2	9	3.9.1.	Atender a todos os requisitos do item 2.3;	Sim	De acordo			OK
2	10	3.10.	LOTE 3 - item 3: Conjunto de funcionalidades antivírus e anti-malware					
2	10	3.10.1.	Atender a todos os requisitos do 2.4;	Sim	De acordo			OK
2	11	3.11.	LOTE 2 – item 4: Conjunto de funcionalidades para tratamento de conteúdo web					
2	11	3.11.1.	Atender a todos os requisitos do item 2.5;	Sim	De acordo			A ser validado em testes
2	12	3.12.	LOTE 2 – item 5: Conjunto de funcionalidades para controle de aplicações e análise profunda					
2	12	3.12.1.	Atender a todos os requisitos do item 2.1.39 e do item 2.6;	Sim	De acordo			OK
2	13	3.13.	LOTE 2 - item 6: Treinamento oficial para até 5 pessoas					

Lote	Item do Lote	Item	Descrição do Item	Atende	Referência/Documento	Página	Observações	Análise do grupo técnico
2	13	3.13.1.	Atender a tudo o que foi exposto no item 2.7.;	Sim	De acordo			OK
2	14	3.14.	LOTE 2 - item7: Solução de gerência centralizada					
2	14	3.14.1.	Requisitos específicos					
2	14	3.14.1.1.	Atender a todos os requisitos do item 2.2;	Sim	De acordo			A ser validado em testes
2	14	3.14.1.2.	Possuir capacidade mínima de 250 GB para armazenamento de logs e eventos	Sim	FortiManager.pdf	4	FortiManager 200F Storage Capacity 1 TB	A ser validado em testes