Informação nº 24/2023 – STI

Brasília, 27 de novembro de 2023.

Processo nº. 6592/2023

Interessados: Tribunal de Contas do Distrito Federal; PPN TECNOLOGIA E INFORMÁTICA LTDA.

Assunto: Verificação quanto à aderência ou não aos requisitos solicitados no Edital do Pregão Eletrônico nº 18/2023, para contratação de empresa especializada no fornecimento de firewall e atendimento de demandas internas do Tribunal de Contas do Distrito Federal.

Senhor(a) Pregoeiro(a),

1. Trata-se de Informação em resposta ao Despacho-SELIC presente na peça n.º 47 do Processo n.º 6592/2023. O referido despacho solicita, por parte da equipe técnica responsável pela contratação, manifestação quanto ao atendimento ou não da proposta técnica apresentada pela empresa PPN TECNOLOGIA E INFORMÁTICA LTDA (peça n.º 46).

2. A equipe responsável pelo projeto entende que a documentação apresentada pela licitante é suficiente, conforme apresentado no documento anexo à esta informação.

3. Importante observar que todos os itens solicitados em edital também serão objeto de verificação durante a fase de recebimento da solução.

[assinado digitalmente]

Luiz Antônio Moreira Serrado Ribeiro

Integrante Técnico (substituto)

[assinado digitalmente]

Fernando de Abrantes Figueiredo

Integrante Técnico

[assinado digitalmente]

Miguel Kojiio Nobre

Integrante Técnico

ANEXO

	FIREWALL – ESPECIFICAÇÕES Processo nº 00600-00006592/2023-08-e CARACTERÍSTICAS TÉCNICAS COMUNS DA SOLUÇÃO GERAL	COMPROVAÇÕES	TRECHO	TÓPICO	SITUAÇÃO
1	Suporte técnico on-site, 24h x 7dias, por 60 (sessenta) meses, a contar do recebimento definitivo da solução (ITEM 1).	PROPOSTA INICIAL_PREGÃO 18-2023-TCDF	N/A	N/A	ATENDE
2	Interface de gerência centralizada;	FortiManager Data Sheet	pag.1	Automation-Driven Centralized Device Management from a Single Console	ATENDE
3	No mínimo, 4 interfaces SFP28 de 25 Gbits/s;	FortiGate 900G Series Data Sheet	pag.6	Hardware	ATENDE
4	No mínimo, 8 interfaces, além das interfaces de gerência e sincronismo, 100/1000Base-T;	FortiGate 900G Series Data Sheet	pag.6	Hardware	ATENDE
5	A solução deverá ser implementada em modo cluster de alta disponibilidade, com uso de 2 equipamentos, e ser capaz de suportar um throughput de, pelo menos, 7,2 Gbps, com a funcionalidade de threat prevention habilitada;	FortiGate 900G Series Data Sheet	pag.7	Specifications	ATENDE
6	Implementar a configuração de cluster de alta disponibilidade (cluster H.A.) Ativo/Passivo e permitir extensão de licença do equipamento para suportar o modo Ativo/Ativo;	FortiGate 900G Series Data Sheet	pag.7	Specifications	ATENDE
7	Implementar tecnologia de filtragem de pacotes baseada em estados (stateful inspection);	FortiOS 7.0 CLI Reference	pag.1497	Firewall Session-dirty / Check-all	ATENDE
8	Implementar tecnologia de filtragem capaz de atuar em múltiplas camadas;	FortiOS 7.0 Administration Guide FortiOS 7.0 Data Sheet	pag.809 pag. 3	Firewall policies Highlights	ATENDE
9	Suportar a criação de regras de filtragem por:	FortiOS 7.0 Administration Guide	pag.831 e pag.832	Policies / Firewall policy parameters	ATENDE
a	Endereço de origem e destino;	FortiOS 7.0 Administration Guide	pag.831 e pag.832	Policies / Firewall policy parameters	ATENDE
b	Sub-rede IP;	FortiOS 7.0 Administration Guide	pag.929 e pag.230	Address Types	ATENDE
c	Porta de destino;	FortiOS 7.0 Administration Guide	pag. 812, pag.831 e pag.832	Configure SD-WAN Policies / Firewall policy parameters	ATENDE
d	Tipo de protocolo;	FortiOS 7.0 Administration Guide	pag. 812, pag.831 e pag.832	Configure SD-WAN Policies / Firewall policy parameters	ATENDE
e	Tipo de serviço ou aplicação;	FortiOS 7.0 Administration Guide	pag.675, pag.831 a pag.832	Application matching Policies / Firewall policy parameters	ATENDE
f	Código/Nome de País (Por exemplo: BR, USA, UK, RUS).	FortiOS 7.0 Administration Guide https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-block-by-country-or-geolocation/ta-p/196741	pag.831 a pag.832 e pag.929 a pag.230 N/A	Policies / Firewall policy parameters Address Types	ATENDE
10	Implementar NAT (Network Address Translation) e PAT (Port Address Translation);	FortiOS 7.0 Data Sheet	pag.8, pag.12 e pag.13	Routing/NAT	ATENDE
11	Implementar tags de VLAN Tagging (802.1q);	FortiOS 7.0 Data Sheet	pag.8 e pag.13	L2/Switching	ATENDE
12	Implementar VPN;	FortiOS 7.0 Data Sheet	pag.6 e pag.12	VPN	ATENDE
13	Possuir sistema de prevenção e detecção de intrusão (IPS/IDS);	FortiOS 7.0 Data Sheet	pag.7 e pag.11	IPS and DoS	ATENDE
14	Controle de aplicações;	FortiOS 7.0 Data Sheet	pag.7 e pag.12	Application Control	ATENDE
15	Filtragem de conteúdo e URL;	FortiOS 7.0 Data Sheet	pag.7 e pag.12	Web and Video Filtering	ATENDE
16	Sistema antimalware;	FortiOS 7.0 Data Sheet	pag.7 e pag.11	Anti-Malware	ATENDE
17	Sistema de inspeção de pacotes SSL/TLS;	FortiOS 7.0 Data Sheet	pag.6 e pag.11	SSL Inspection	ATENDE
18	Qualidade de Serviço;	FortiOS 7.0 Data Sheet	pag.8 e pag.13	SD-WAN	ATENDE
19	SANDBOX.	FortiOS 7.0 Data Sheet	pag.4, pag.7, pag.10 e pag.11	Advance Threat Protection (ATP) Anti-Malware System Integration	ATENDE
	Item 1 - FIREWALL				ATENDE
	CONFIGURAÇÕES GERAIS DE HARDWARE E SOFTWARE				ATENDE
20	Os equipamentos devem ser do tipo Appliance, ou seja, hardware e software integrados. Não serão aceitas soluções compostas por hardwares genéricos;	FortiGate 900G Series Data Sheet	pag.2	FortiOS Everywhere	ATENDE

21	A solução será implementada em modo cluster de alta disponibilidade com uso de 2 equipamentos e capaz de suportar um throughput de 7,2 Gbps, com a funcionalidade de threat prevention habilitada;	FortiGate 900G Series Data Sheet	pag.7	Specifications	ATENDE
22	O Throughput e as interfaces solicitados deverão ser comprovados através de datasheet público na internet. Não serão aceitas declarações de fabricantes informando números de performance e interfaces;	FortiGate 900G Series Data Sheet	pag.7	Specifications	ATENDE
23	Os valores de capacidade são considerados para cada equipamento, não sendo permitido a soma dos valores dos membros do cluster;	FortiGate 900G Series Data Sheet	pag.7	Specifications	ATENDE
24	A solução deve ser do tipo Bundle (Hardware/Software) obrigatoriamente do mesmo fabricante, com capacidade suficiente para atender os requisitos exigidos;	FortiGate 900G Series Data Sheet	pag.2	FortiOS Everywhere	ATENDE
25	A solução deverá ser composta por sistema operacional proprietário, desenvolvido para ser seguro e robusto e otimizado para as suas funcionalidades;	FortiGate 900G Series Data Sheet	pag.2	FortiOS Everywhere	ATENDE
26	Todos os equipamentos, produtos, peças ou softwares necessários à implementação da solução deverão ser de primeiro uso e não poderão constar, no momento da apresentação da proposta, em listas de end-of-sale, end-of-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante. Da mesma maneira, todo o hardware a ser utilizado na prestação dos serviços deverá estar coberto por contratos de suporte e atualização de versão do fabricante. Os produtos utilizados devem possuir licenciamento, suporte e garantia do fabricante por todo o período contratual;	PROPOSTA INICIAL_PREGÃO 18-2023-TCDF	pag.5	Declaração	ATENDE
27	Os equipamentos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação, se necessário, e cabos de alimentação;	FortiGate 900G Series Data Sheet	pag.7	Specifications	ATENDE
28	Possuir no máximo 2RU (Rack Units);	FortiGate 900G Series Data Sheet	pag.7	Specifications	ATENDE
29	Possuir no mínimo:	FortiGate 900G Series Data Sheet	pag.7	Specifications	ATENDE
a	8 interfaces compatíveis com cabeamento de rede UTP com conector RJ-45 no padrão 100/1000Base-T Gigabit Ethernet;	FortiGate 900G Series Data Sheet	pag.7	Specifications	ATENDE
b	4 interfaces, compatíveis com cabeamento SFP28 10/25 GbE.	FortiGate 900G Series Data Sheet	pag.7	Specifications	ATENDE
c	Possuir pelo menos 1 (uma) interface de rede dedicada para sincronismo;	FortiGate 900G Series Data Sheet	pag.7	Specifications	ATENDE
d	Possuir pelo menos 1 (uma) interface de rede dedicada ao gerenciamento, não sendo permitido utilizar qualquer outra interface para exercer a função de gerenciamento do equipamento;	FortiGate 900G Series Data Sheet	pag.7	Specifications	ATENDE
e	Possuir 1 (uma) interface do tipo console RS232 ou similar;	FortiGate 900G Series Data Sheet	pag.7	Specifications	ATENDE
30	Cada equipamento deverá acompanhar os seguintes acessórios:	PROPOSTA INICIAL_PREGÃO 18-2023-TCDF	Pag. 5	Declaração	ATENDE
a	Cada equipamento deverá acompanhar os seguintes acessórios:Cada equipamento deverá acompanhar os seguintes acessórios:Cada equipamento deverá acompanhar os seguintes acessórios:Cada equipamento deverá acompanhar os seguintes acessórios:Cada equipamento deverá acompanhar os seguintes acessórios:Cada equipamento deverá acompanhar os seguintes acessórios:	PROPOSTA INICIAL_PREGÃO 18-2023-TCDF	Pag. 5	Declaração	ATENDE
b	4 (quatro) cabos SFP28 Direct Attach (DAC), de 25 Gbit/s, com 3 (três) metros de comprimento;	PROPOSTA INICIAL_PREGÃO 18-2023-TCDF	Pag. 5	Declaração	ATENDE
c	4 (quatro) cabos de rede UTP Cat6 1GBase-T com terminais RJ-45, com 3 (três) metros de comprimento.	PROPOSTA INICIAL_PREGÃO 18-2023-TCDF	Pag. 5	Declaração	ATENDE
31	Todas as interfaces fornecidas nos appliances devem estar licenciadas e habilitadas para uso imediato, mesmo se forem fornecidas interfaces além das exigidas.	FortiGate 900G Series Data Sheet	pag.6	Hardware	ATENDE
32	Possuir fonte de alimentação redundante e hot swap interna;	FortiGate 900G Series Data Sheet	pag.7	Specifications	ATENDE
33	Cada um dos appliances deve possuir 2 discos Solid State Drive (SSD), redundantes, com, no mínimo, 480 GB de capacidade de armazenamento;	FortiGate 900G Series Data Sheet	pag.7	Specifications	ATENDE

34	O equipamento deverá estar licenciado para implementar a configuração de cluster de alta disponibilidade (cluster H.A.) pelo menos em modo ativo/passivo, sendo a troca de um equipamento para o outro feita de forma automática e sem intervenção humana.	FortiOS 7.0 Administration Guide FortiOS 7.0 Data Sheet	pag.2095, pag.2109 e pag.2111 pag.13	High Availability HA active-passive cluster setup HA active-active cluster setup High Availability	ATENDE
35	O cluster H.A. deve sincronizar:	FortiOS 7.0 Administration Guide	pag.2097	Synchronizing the configuration	ATENDE
a	Todas as sessões TCP;	FortiOS 7.0 Administration Guide	pag.1549	IPsec VPN in an HA environment	ATENDE
b	Todas as Associações de Segurança das VPNs;	FortiOS 7.0 Administration Guide	pag.1549	IPsec VPN in an HA environment	ATENDE
c	Todas as assinaturas de Antivírus, Antispyware e Aplicações;	FortiOS 7.0 Administration Guide	pag.2097	Synchronizing the configuration	ATENDE
d	Todas as configurações necessárias para que não haja perda de funcionalidade em caso de falha;	FortiOS 7.0 Administration Guide	pag.2097	Synchronizing the configuration	ATENDE
36	Todos os LOGs devem ser disponibilizados de modo a permitir acesso independente de qual unidade do cluster que estiver ativo.	FortiOS 7.0 Administration Guide FortiAnalyzer Data Sheet	pag.2678 pag.1	Remote Logging and Archiving Highlights	ATENDE
37	Permitir a monitoração de falha de conexão entre os dispositivos do cluster com possibilidade de gerar alertas via SNMP e e-mail;	https://community.fortinet.com/t5/FortiGate/Technical-Tip-Setup-FortiGate-HA-failover-alert-on-SNMP-managers/ta-p/216711	N/A	N/A	ATENDE
38	Implementar compatibilidade com sistemas de monitoramento como Zabbix, Nagios e Cacti via SNMP v2;	FortiOS 7.0 Data Sheet	pag.11	Monitoring	ATENDE
39	A solução deve possuir minimamente as seguintes especificações técnicas:	FortiGate 900G Series Data Sheet	pag.7	Specifications	ATENDE
a	Throughput com threat protection/prevention habilitado de, pelo menos, 7,2 Gbits/s	FortiGate 900G Series Data Sheet	pag.7	Specifications	ATENDE
b	Throughput com VPN habilitada de, pelo menos, 9 Gbits/s	FortiGate 900G Series Data Sheet	pag.7	Specifications	ATENDE
c	Admitir, no mínimo, 200.000 novas conexões por segundo;	FortiGate 900G Series Data Sheet	pag.7	Specifications	ATENDE
d	Tratar, no mínimo, 2.000.000 de sessões simultâneas;	FortiGate 900G Series Data Sheet	pag.7	Specifications	ATENDE
40	Como “threat protection/prevention”, entende-se que estarão habilitadas, pelo menos, as funções de firewall, controle de aplicações, IPS e antimalware.	FortiGate 900G Series Data Sheet	pag.7	Specifications	ATENDE
41	Os equipamentos da solução devem ser otimizados para análise de conteúdo de aplicações em camada 7 do modelo OSI;	FortiOS 7.0 Data Sheet	pag.12	Application Control	ATENDE
42	O equipamento ou a fabricante deve possuir certificação da ICSA Labs na modalidade "ICSA Labs Certified Firewall Product" ou Common Criteria EAL4+	https://www.fortinet.com/corporate/about-us/product-certifications https://www.fortinet.com/corporate/about-us/product-certifications/common-criteria https://www.fortinet.com/content/dam/fortinet/assets/certifications/certification-report-icsa-labs-firewall.pdf https://www.tuv-nederland.nl/assets/files/cerfiticaten/2023/08/nscib-cc-0590233-cert.pdf	N/A	N/A	ATENDE https://www.fortinet.com/content/dam/fortinet/assets/certifications/certification-report-icsa-labs-firewall.pdf
43	O fabricante do equipamento deve ser membro do programa "Microsoft Active Protections Program" (MAPP). Membros do MAPP recebem acesso antecipado a informações de vulnerabilidades para que estas sejam corrigidas de modo rápido reduzindo a exposição do cliente a ameaças	https://www.microsoft.com/en-us/msrc/mapp	N/A	Fortinet Technologies	ATENDE
44	Implementar transmissão de logs em rede IP por meio do padrão syslog.	FortiOS 7.0 Data Sheet	pag.11	Log and Report	ATENDE
45	Implementar funcionamento em “tap mode”	FortiOS 7.0 Administration Guide	pag.211	One-arm sniffer	ATENDE
46	Implementar tecnologia de filtragem de pacotes baseada em estados (stateful inspection);	FortiOS 7.0 CLI Reference	pag.1497	Firewall Session-dirty / Check-all	ATENDE
47	Implementar tecnologia de filtragem capaz de atuar em múltiplas camadas (stateful multilayer inspection);	FortiOS 7.0 CLI Reference https://community.fortinet.com/t5/FortiGate/Troubleshooting-Tip-FortiGate-session-table-information/ta-p/196988	pag.1497 N/A	Firewall Session-dirty / Check-all	ATENDE

48	Capacidade de atuar como proxy, de modo a inspecionar conteúdo do tráfego de aplicações e filtrar URLs acessadas; a solução deverá apresentar relatório dos sites acessados e os respectivos IPs ou usuários que iniciaram a conexão.	FortiOS 7.0 Administration Guide FortiAnalyzer Administration Guide	pag.242 pag.263	Explicit and transparent proxies List of report templates	ATENDE
49	Registrar os fluxos de dados relativos a cada sessão iniciada, informar para cada uma destas:	FortiOS 7.0 Administration Guide FortiOS 7.0 Data Sheet	pag.2682 a pag.2683 pag.11	Sample log Log and Report	ATENDE
a	Protocolo	FortiOS 7.0 Administration Guide FortiOS 7.0 Data Sheet	pag.2682 a pag.2683 pag.11	Sample log Log and Report	ATENDE
b	Aplicação	FortiOS 7.0 Administration Guide FortiOS 7.0 Data Sheet	pag.2682 a pag.2683 pag.11	Sample log Log and Report	ATENDE
c	Endereços de origem e destino dos pacotes	FortiOS 7.0 Administration Guide FortiOS 7.0 Data Sheet	pag.2682 a pag.2683 pag.11	Sample log Log and Report	ATENDE
d	Portas TCP e UDP de origem e destino	FortiOS 7.0 Administration Guide FortiOS 7.0 Data Sheet	pag.2682 a pag.2683 pag.11	Sample log Log and Report	ATENDE
e	Quantidade de pacotes trafegados	FortiOS 7.0 Administration Guide FortiOS 7.0 Data Sheet	pag.2682 a pag.2683 pag.11	Sample log Log and Report	ATENDE
f	Quantidade de dados trafegado	FortiOS 7.0 Administration Guide FortiOS 7.0 Data Sheet	pag.2682 a pag.2683 pag.11	Sample log Log and Report	ATENDE
50	Implementar toda a pilha de protocolos do modelo TCP/IP, com as seguintes funcionalidades:	FortiOS 7.0 Data Sheet	pag.12	Routing/NAT	ATENDE
a	IPv4 e IPv6;	FortiOS 7.0 Data Sheet	pag.12	Routing/NAT Firewall	ATENDE
b	Roteamento estático e dinâmico de tráfego;	FortiOS 7.0 Data Sheet	pag.12	Routing/NAT	ATENDE
c	RIP v2	FortiOS 7.0 Data Sheet	pag.12	Routing/NAT	ATENDE
d	OSPF	FortiOS 7.0 Data Sheet	pag.12	Routing/NAT	ATENDE
e	BGP v4	FortiOS 7.0 Data Sheet	pag.12	Routing/NAT	ATENDE
f	Suporte a roteamento IPv6	FortiOS 7.0 Data Sheet	pag.8, pag.12 e pag.13	IPV6 / Routing/NAT	ATENDE
g	Suporte a RFC 4291 de Arquitetura de endereçamento IPv6	FortiOS 7.0 Data Sheet FortiOS 7.0 Supported RFCs	pag.13 pag.10	IPV6 IPV6	ATENDE
h	Randomizar o número de sequência TCP, atuando como um proxy de número de sequência TCP ou possuir outra técnica para prevenção de ataques de roubo de sessão TCP (TCP Session Hijacking);	https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-FortiGate-perform-TCP-randomized-Initial/ta-p/220731	N/A	N/A	ATENDE
51	Suportar a criação de regras de filtragem por:	FortiOS 7.0 Administration Guide FortiOS 7.0 Data Sheet	pag.832 pag.11	Firewall policy parameters Policy Modes	ATENDE
a	Endereço de origem e destino;	FortiOS 7.0 Administration Guide FortiOS 7.0 Data Sheet	pag.832 pag.11	Firewall policy parameters Policy Modes	ATENDE
b	Sub-rede IP;	FortiOS 7.0 Administration Guide FortiOS 7.0 Data Sheet	pag.832 e pag.929 a pag.930 pag.11	Firewall policy parameters Address Types Policy Modes	ATENDE
c	Porta de destino;	FortiOS 7.0 Administration Guide FortiOS 7.0 Data Sheet	pag.832 pag.11	Firewall policy parameters Policy Modes	ATENDE
d	Tipo de protocolo;	FortiOS 7.0 Administration Guide FortiOS 7.0 Data Sheet	pag.832 pag.11	Firewall policy parameters Policy Modes	ATENDE
e	Tipo de serviço ou aplicação;	FortiOS 7.0 Administration Guide FortiOS 7.0 Data Sheet	pag.832 pag.11	Firewall policy parameters Policy Modes	ATENDE

f	Código/Nome de País (Por exemplo: BR, USA, UK, RUS);	FortiOS 7.0 Administration Guide FortiOS 7.0 Data Sheet https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-block-by-country-or-geolocation/ta-p/196741	pag.832 pag.11 N/A	Firewall policy parameters Policy Modes	ATENDE
52	Permitir a definição de período de validade de regras, ou seja, determinar a validade por um horário e data;	FortiOS 7.0 Administration Guide https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-configure-schedule-policy-with-deny-action/ta-p/193508	pag.832 N/A	Firewall policy parameters	ATENDE
53	Implementar NAT (Network Address Translation) e PAT (Port Address Translation);	FortiOS 7.0 Data Sheet	pag.12 e pag.13	Routing/NAT	ATENDE https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/7f7eba66-4037-11ee-8e6d-fa163e15d75b/FortiManager-7.4.1-Administration_Guide.pdf pag 541
54	Suporte a, no mínimo, 1000 VLAN Tags 802.1q, agregação de links 802.3ad, policy based routing ou policy based forwarding, roteamento multicast, DHCP Relay, DHCP Server e Jumbo Frames;	FortiOS 7.0 Data Sheet FortiOS 7.0 Administration Guide https://community.fortinet.com/t5/FortiGate/Technical-Note-MTU-size-and-Jumbo-frames-support-on-FortiGate/ta-p/195797 https://docs.fortinet.com/max-value-table	pag.8 e pag.13 pag.209 e pag.314 N/A N/A	L2/Switching / SD-WAN Interface MTU packet size DHCP servers and relays OS: 7.0.13 e Models: 900G Search: system.interface	ATENDE
55	Implementar pelo menos 10.000 (dez mil) regras de firewall	FortiGate 900G Series Data Sheet	pag.7	Specifications	ATENDE
56	Permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;	FortiOS 7.0 Administration Guide	pag.843	Dynamic SNAT	ATENDE sb-secure-open-platform-commmunications-ot-environments.pdf (fortinet.com)
57	Ser compatível com o estabelecimento ou passagem de túneis VPN Site-to-Site e Client-To-Site. Por “estabelecimento”, entende-se que a solução é capaz de fechar túneis VPN entre ela e os clientes e vice-versa. Por “passagem”, entende-se que a solução permite, por exemplo, que clientes em um segmento de rede interno fechem túneis VPN com clientes na internet e vice-versa	FortiOS 7.0 Data Sheet	pag.12	VPN	ATENDE
58	Implementar Framework H.323	FortiOS 7.0 Data Sheet	pag.12	Firewall	ATENDE
59	Implementar multicast e unicast;	FortiOS 7.0 Data Sheet	pag.13	L2/Switching	ATENDE

60	Para autenticação VPN e aplicação de regras baseadas em usuários/grupos do serviço de diretórios, implementar as seguintes formas de autenticação:	FortiOS 7.0 Data Sheet FortiOS 7.0 Administration Guide	pag.10 pag.1890	Network Access Control (NAC) Users	ATENDE
a	RADIUS;	FortiOS 7.0 Data Sheet FortiOS 7.0 Administration Guide	pag.10 pag.1890	Network Access Control (NAC) Users	ATENDE
b	LDAP;	FortiOS 7.0 Data Sheet FortiOS 7.0 Administration Guide	pag.10 pag.1890	Network Access Control (NAC) Users	ATENDE
c	Windows AD;	FortiOS 7.0 Data Sheet FortiOS 7.0 Administration Guide	pag.10 pag.1890	Network Access Control (NAC) Users	ATENDE
61	Para administração da ferramenta implementar as seguintes formas de autenticação:	FortiOS 7.0 Administration Guide	pag.2031	Remote authentication for administrators	ATENDE
a	RADIUS;	FortiOS 7.0 Administration Guide	pag.2031	Remote authentication for administrators	ATENDE
b	LDAP;	FortiOS 7.0 Administration Guide	pag.2031	Remote authentication for administrators	ATENDE
c	Windows AD;	FortiOS 7.0 Administration Guide	pag.2031	Remote authentication for administrators	ATENDE
d	Autenticação Local.	FortiOS 7.0 Administration Guide	pag.2031	Remote authentication for administrators	ATENDE
62	Implementar compatibilidade com Microsoft Active Directory 2016	FortiOS 7.0 Data Sheet https://community.fortinet.com/t5/FortiAuthenticator/Technical-Tip-Windows-event-IDs-used-by-FSSO-in-WinSec-polling/ta-p/189910	pag.10 N/A	Network Access Control (NAC)	ATENDE https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/5f17e02f-7286-11ee-a142-fa163e15d75b/FortiOS-7.0.13-Administration_Guide.pdf pag 1950
63	Ser administrado por ferramenta com interface gráfica remota segura, preferencialmente web, a partir de plataforma Windows 10 e superiores;	FortiOS 7.0 Data Sheet FortiOS 7.0 Administration Guide	pag.11 pag.22	Configuration Using the GUI	ATENDE
64	Implementar, junto com as características acima detalhadas, as seguintes funcionalidades simultaneamente habilitadas e integradas:	FortiOS 7.0 Data Sheet	pag.6 a pag.13	N/A	ATENDE
a	VPN;	FortiOS 7.0 Data Sheet	pag.6 e pag.12	VPN	ATENDE
b	Sistema de prevenção e detecção de intrusão (IPS/IDS);	FortiOS 7.0 Data Sheet	pag.7 e pag.11	IPS and DOS	ATENDE
c	Filtragem de conteúdo e URL	FortiOS 7.0 Data Sheet	pag.7 e pag.12	Web and Video Filtering	ATENDE
d	antivírus e antispyware	FortiOS 7.0 Data Sheet	pag 12	Anti-Malware	ATENDE
e	inspeção de pacotes SSL/TLS	FortiOS 7.0 Data Sheet	pag.7 e pag.11	SSL Inspection	ATENDE
f	controle de aplicações (reconhecimento e filtragem de aplicações)	FortiOS 7.0 Data Sheet	pag.6 e pag.11	Application Control	ATENDE
g	QoS.	FortiOS 7.0 Data Sheet	pag.8 e pag.13	SD-WAN	ATENDE
	GERÊNCIA E ADMINISTRAÇÃO CENTRALIZADA				ATENDE
65	O módulo de gerência deve ser capaz de gerenciar e administrar todas as soluções descritas neste termo;	FortiManager Data Sheet	pag.1	Automation-Driven Centralized Device Management from a Single Console	ATENDE
66	Não será permitida central de gerenciamento na nuvem;	FortiManager Data Sheet	N/A	(Applience FMG-200G)*	ATENDE
67	A central de gerenciamento deverá ser fornecida em appliance físico ou virtual;	FortiManager Data Sheet	N/A	(Applience FMG-200G)*	ATENDE

a	No caso do appliance virtual, será permitida solução virtual no ambiente VMware ou outro virtualizador homologado pela solução da contratada, desde que todas as licenças sejam fornecidas pela contratada. Além das licenças, também será necessário o fornecimento de equipamento servidor, de, no máximo, 2U, para a instalação do software de virtualização, além de cabos e demais componentes de interconexão. Os equipamentos fornecidos serão de propriedade do TCDF;	FortiManager Data Sheet	N/A	(Applience FMG-200G)*	ATENDE
68	Permitir a replicação de configurações e a aplicação de atualização de softwares entre os elementos do cluster;	FortiManager Data Sheet	pag.3	Device Configuration and Provisioning	ATENDE
69	O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança;	FortiAnalyzer Data Sheet FortiAnalyzer Administration Guide	pag.2 pag.34 e pag.215	Centralized NOC/SOC Visibility for the Attack Surface Logs Creating a custom event handler	ATENDE
70	O gerenciamento deve permitir/possuir monitoração de logs, ferramentas de investigação de logs e acesso concorrente de administradores;	FortiAnalyzer Data Sheet FortiAnalyzer Administration Guide	pag.2 pag.34 e pag.215	Centralized NOC/SOC Visibility for the Attack Surface Logs Creating a custom event handler	ATENDE
71	Caso a solução de gerenciamento, monitoração e relatoria, possua licenciamento relacionado a armazenamento, este deve ser entregue com a maior capacidade suportada ou ilimitada sem a necessidade de licenciamento adicional;	FortiAnalyzer Data Sheet	N/A	(Appliance FAZ-300G fornecido em sua capacidade máxima Appliance não possui licença de armazenamento)*	ATENDE
72	Suportar backup das configurações e rollback de configuração para a última configuração salva;	FortiManager Administration Guide FortiOS 7.0 Administration Guide	pag.45 pag.60 a pag.63	Revert Configuration backups	ATENDE
73	Suportar validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);	FortiManager Administration Guide	pag.369 e pag.370	Conflict Perform a policy consistency check	ATENDE
74	Suportar geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;	FortiManager Administration Guide	pag.834	Event Log	ATENDE
75	A solução deve permitir o login de múltiplos usuários administradores simultâneos com perfil de escrita, possibilitando agilidade e rapidez no gerenciamento pelo grupo de administradores da solução.	FortiManager Administration Guide FortiManager Best Practices	pag.814 pag.14	Assigning administrators to an ADOM Concurrent administrators	ATENDE
76	Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus, Anti-Malware), e URLs que passaram pela solução;	FortiAnalyzer Administration Guide	pag.83 e pag.122	Viewing Compromised Hosts Security: Summary dashboard	ATENDE
77	Permitir a definição de diferentes níveis de administração, sendo, no mínimo, um nível completo e outro somente de visualização de configurações e logs;	FortiManager Administration Guide	pag.880	Permissions	ATENDE
78	Permitir a geração das seguintes informações, por período e elemento:	FortiAnalyzer Administration Guide	a partir da pag.76	FortiView	ATENDE
a	Auditoria detalhada das alterações de configuração efetuadas, indicando usuário, ação e horário;	FortiAnalyzer Administration Guide	pag.834	Event Log	ATENDE
b	Informações estatísticas de quantidade de conexões completadas e bloqueadas;	FortiAnalyzer Administration Guide	pag.78	Trafic / Top Source Addresses	ATENDE
c	Informações estatísticas de fluxo de tráfego;	FortiAnalyzer Administration Guide	pag.78	Trafic / Top Source Addresses	ATENDE
d	Informações estatísticas de quantidade de sessões ou conexões e	FortiAnalyzer Administration Guide	pag.78	Trafic / Top Source Addresses	ATENDE
e	Informações estatísticas de quantitativo de ataques identificados por tipo.	FortiAnalyzer Administration Guide	pag.77	Threads / Top Threats	ATENDE
79	Possuir mecanismo que permite emitir, no mínimo, os seguintes relatórios:	FortiAnalyzer Administration Guide	pag.266	User report templates / Template - User Detailed Browsing Log	ATENDE
a	Sites com maior volume de dados acessados por usuário;	FortiAnalyzer Administration Guide	pag.78 e pag.266	Traffic / Applications & Websites User report templates / Template - User Detailed Browsing Log	ATENDE
b	Sites acessados por determinados usuários (ou IPs), classificado por username ou IP e data/hora;	FortiAnalyzer Administration Guide	pag.266	User report templates / Template - User Detailed Browsing Log	ATENDE
c	Sites bloqueados por determinados usuários (ou IPs), classificado por username ou IP e data/hora;	FortiAnalyzer Administration Guide	pag.266	User report templates / Template - User Detailed Browsing Log	ATENDE

d	Usuários que acessaram determinado site por determinado período;	FortiAnalyzer Administration Guide	pag.76 e pag.266	FortiView dashboards User report templates / Template - User Detailed Browsing Log	ATENDE
e	Sites bloqueados;	FortiAnalyzer Administration Guide	pag.266	User report templates / Template - User Detailed Browsing Log	ATENDE
f	Malware encontrados;	FortiAnalyzer Administration Guide	pag.265	Security report templates / Template - Threat Report	ATENDE
80	Exportar os relatórios em pelo menos 2 dos seguintes formatos: HTML; PDF; CSV ou outro compatível com programa de planilha; XML.	FortiAnalyzer Administration Guide	pag.246	Viewing completed reports	ATENDE
81	Permitir a seleção de período para emissão dos relatórios, sendo que devem estar disponíveis, no mínimo, os dados dos últimos 90 (noventa) dias;	FortiAnalyzer Administration Guide	pag.132 a pag.133 e pag.251	Log storage information Time Period	ATENDE
82	A solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credencias;	FortiAnalyzer Administration Guide	pag. 384	Password lockout and retry attempts	ATENDE
83	Deve suportar a geração de relatório gerencial para apresentar aos executivos os eventos de ataque de forma completamente visual, utilizando para tanto gráficos, consumo de banda utilizado pelos ataques e quantidade de eventos gerados e protegidos;	FortiAnalyzer Administration Guide	pag.265	Security report templates / Template - Cyber Threat Assessment	ATENDE
84	Deve permitir a integração com servidores de autenticação LDAP Microsoft Active Directory via Radius;	FortiManager Administration Guide	pag.907	Managing remote authentication servers	ATENDE
85	Criar certificados digitais para acesso dos usuários VPN;	FortiAuthenticator Data Sheet FortiAuthenticator Administration Guide	pag.7 pag.238	Specifications Certificate management	ATENDE https://docs.fortinet.com/document/fortigate/7.4.1/administration-guide/322226/generate-a-new-certificate
86	Criar certificados digitais para VPNs Site-to-Site;	FortiAuthenticator Data Sheet FortiAuthenticator Administration Guide	pag.7 pag.238	Specifications Certificate management	ATENDE https://docs.fortinet.com/document/fortigate/6.2.15/cookbook/45836/ssl-vpn-to-ipsec-vpn
87	Caso a solução possua licenciamento relacionado a capacidade de criação de certificados, deve ser contemplado a sua maior capacidade ou ilimitada;	FortiAuthenticator Data Sheet	N/A	(Appliance FAC-300F fornecido em sua capacidade máxima, Appliance não possui licença de controle de certificado)*	ATENDE
88	Deve possuir a capacidade de visualizar na interface gráfica da solução, informações do sistema como licenças, memória, disco e uso de CPU;	FortiManager Administration Guide https://docs.fortinet.com/document/fortimanager/6.0.2/cli-reference/95783/system-status	pag.31 e pag.54 N/A	Using the Process Monitor System Information widget system status	ATENDE
89	A solução deve ser capaz de correlacionar eventos de todas as fontes de log em tempo real;	FortiAnalyzer Administration Guide	pag.123 e pag.215 a pag.216	Viewing historical and real-time logs Creating a custom event handler	ATENDE
90	A solução deve ser capaz de personalizar e criar regras de correlação;	FortiAnalyzer Administration Guide	pag.215 a pag.216	Creating a custom event handler	ATENDE
91	A solução deve possuir painéis de eventos em tempo real com possibilidade de configuração das atualizações e frequências.	FortiAnalyzer Administration Guide	pag.123	Viewing historical and real-time logs	ATENDE
	SISTEMA DE VPN				ATENDE
92	IPSec VPN Site-to-Site e Client-To-Site;	FortiOS 7.0 Data Sheet FortiGate 900G Series Data Sheet	pag.12 pag.7	VPN Specifications	ATENDE
93	SSL VPN;	FortiOS 7.0 Data Sheet FortiGate 900G Series Data Sheet	pag.12 pag.7	VPN Specifications	ATENDE
94	Atribuição de IPs nos clientes remotos de VPN;	FortiOS 7.0 Administration Guide	pag.1413 e pag.1438	Network To configure IPsec VPN with an IP address reuse delay interval	ATENDE

95	Atribuição de DNS nos clientes remotos de VPN;	FortiOS 7.0 Administration Guide https://community.fortinet.com/t5/FortiGate/Technical-Tip-Setting-multiple-DNS-server-for-IPSec-dial-up-VPN/ta-p/198129	pag.1413 N/A	Network	ATENDE
96	Deve suportar, no mínimo, 400 túneis de VPN client-to-site simultaneamente, estando devidamente licenciado para este fim, bem como ser totalmente suportado pelo fabricante da solução durante toda vigência do contrato;	FortiGate 900G Series Data Sheet	pag.7	Specifications	ATENDE
97	A solução deve possuir checagem de conformidade e verificar, no mínimo, as seguintes informações no cliente remoto: sistema operacional e patches instalados, antivírus, firewall no host, chaves de registros e processos ativos;	FortiOS 7.0 Administration Guide FortiOS 7.0 Endpoint Posture Check	pag.1843 pag.4	Creating a custom host check list Recommended posture checks	ATENDE FortiOS 7.0 Administration Guide FortiOS 7.0 Endpoint Posture Check pag 1841 a 1845
98	O cliente da solução de VPN client-to-site deve suportar a instalação nos seguintes sistemas operacionais:	FortiClient Data Sheet	pag.9	Features Per Platform and Requirements	ATENDE
a	Microsoft Windows;	FortiClient Data Sheet	pag.9	Features Per Platform and Requirements	ATENDE
b	Apple macOS e iOS;	FortiClient Data Sheet	pag.9	Features Per Platform and Requirements	ATENDE
c	Android;	FortiClient Data Sheet	pag.9	Features Per Platform and Requirements	ATENDE
d	Linux.	FortiClient Data Sheet	pag.9	Features Per Platform and Requirements	ATENDE
99	A solução deve permitir bloquear o acesso do usuários aos recursos via VPN caso o usuário não esteja em conformidade com a verificação dos parâmetros configurados.	FortiOS 7.0 Administration Guide FortiClient & FortiClient EMS New Features Guide FortiOS 7.0 Endpoint Posture Check	pag.1841 pag.26 pag.4	Configuring OS and host check FortiGate-powered host check for free VPN client Endpoint posture check	ATENDE
100	A VPN SSL deve suportar:	FortiOS 7.0 Administration Guide	pag.1692 a pag.1694	SSL VPN	ATENDE
a	Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;	FortiOS 7.0 Data Sheet https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-establish-VPN-connection-between-Windows-10/ta-p/200001	pag.12 N/A	VPN	ATENDE
b	A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;	FortiOS 7.0 Administration Guide	pag.1692 a pag.1694	SSL VPN SSL VPN Tunnel Mode SSL VPN Web Mode	ATENDE
c	Suportar configuração de conformidade para acesso do usuário via portal SSL ou cliente no PC do usuário;	FortiOS 7.0 Administration Guide	pag.1841	Verifying remote user OS	ATENDE
d	Atribuição de endereço IP nos clientes remotos de VPN;	FortiOS 7.0 Administration Guide	pag.1413 e pag.1850 a pag.1851	Network To configure the SSL VPN server (FGT-B) in the CLI	ATENDE
e	Atribuição de DNS nos clientes remotos de VPN;	FortiOS 7.0 Administration Guide	pag.1413 e pag.1715	Network To configure DNS servers for all SSL VPN portals	ATENDE
f	Dever permitir criar políticas para tráfego dos clientes remotos conectados na VPN SSL;	FortiOS 7.0 Administration Guide	pag.1754	To configure SSL VPN using the GUI	ATENDE
g	Suportar autenticação via AD/LDAP, certificado e base de usuários local;	FortiOS 7.0 Administration Guide FortiOS 7.0 Data Sheet	pag.1748 pag 10	SSL VPN authentication Network Access Control (NAC)	ATENDE
h	Suportar leitura e verificação de CRL (certificate revocation list);	FortiOS 7.0 Administration Guide	pag 2266	CRL	ATENDE
i	O agente de VPN SSL client-to-site deve ser compatível com Windows 8 e superiores;	FortiClient Data Sheet	pag 9	Features Per Platform and Requirements	ATENDE
	SISTEMA DE PREVENÇÃO E DETECÇÃO DE INTRUSÃO (IPS/IDS)				ATENDE

101	Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS e suportar os módulos de: antivírus e anti-malware integrados no próprio equipamento de firewall;	FortiOS 7.0 Data Sheet	pag.7 e pag.11	IPS and DOS / Anti-Malware	ATENDE
102	Possuir capacidade de detecção de assinaturas de ataques pré-definidos;	FortiOS 7.0 Data Sheet	pag.7 e pag.11	IPS and DOS	ATENDE
103	Deve sincronizar as assinaturas de IPS, antivírus, anti-malware quando implementado em alta disponibilidade ativo/passivo;	FortiOS 7.0 Administration Guide FortiOS 7.0 Data Sheet	pag.2095 e pag.2097 pag.13	High Availability Synchronizing the configuration High Availability	ATENDE
104	Deve suportar granularidade nas políticas de antivírus e anti-malware, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;	FortiOS 7.0 Administration Guide FortiOS 7.0 Data Sheet	pag.832, pag.1158 e pag.1290 pag.11	Firewall policy parameters Configuring an antivirus profile Configuring an IPS sensor IPS and DOS	ATENDE
105	Deverá possuir os seguintes mecanismos de inspeção de IPS:	FortiOS 7.0 Data Sheet	pag.11	IPS and DOS	ATENDE
a	Análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;	FortiOS 7.0 Data Sheet	pag.11	IPS and DOS	ATENDE
106	Detectar e bloquear a origem de portscans;	FortiOS 7.0 Data Sheet https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-block-NMAP-port-scanner/ta-p/196222	pag.11 N/A	IPS and DOS	ATENDE
107	Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;	FortiOS 7.0 Data Sheet https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-configure-custom-IPS-signature-for-a/ta-p/207522	pag.11 N/A	IPS and DOS	ATENDE
108	Possuir assinaturas para bloqueio de ataques de buffer overflow;	https://www.fortiguard.com/search?q=buffer.overflow&engine=1&type=ips	N/A	N/A	ATENDE
109	Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;	FortiOS 7.0 Data Sheet	pag.7 e pag.11	IPS and DOS / Anti-Malware	ATENDE
110	Suportar bloqueio de arquivos por tipo;	FortiOS 7.0 Data Sheet	pag.11 e pag.14	IPS and DOS / Anti-Malware Others	ATENDE
111	Identificar e bloquear comunicação com botnets;	FortiOS 7.0 Data Sheet	pag.7 e pag.11	IPS and DOS / Anti-Malware	ATENDE
112	Deve suportar referência cruzada com CVE;	FortiOS 7.0 Data Sheet	pag.7	IPS and DOS	ATENDE FortiOS 7.0 Administration Guide FortiOS 7.0 Data Sheet https://www.fortinet.com/resources/cyberglossary/cve
113	Fazer inspeção profunda de pacotes (DPI), incluindo o payload, identificando perfis de tráfego anômalos, inclusive na modalidade stateful Inspection;	FortiOS 7.0 Administration Guide	pag.1371	Reasons for using deep inspection	ATENDE
114	Reconhecer e responder a ataques à rede e aos hosts, em tempo real;	FortiOS 7.0 Administration Guide FortiOS 7.0 Data Sheet	pag.1285 pag.11 e pag.12	Intrusion prevention IPS and DOS / Anti-Malware Web and Video Filtering	ATENDE
115	Implementar configuração de perfis que permitam selecionar quais assinaturas que devem ser aplicadas a um grupo de dispositivos;	FortiOS 7.0 Administration Guide	pag.1289 a pag.1290	Custom and predefined signature entries	ATENDE

116	Implementar o bloqueio de vulnerabilidades por assinatura;	FortiOS 7.0 Data Sheet https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-mitigating-vulnerabilities-fortigate-ips-overview.pdf	pag.7 e pag.11 N/A	IPS and DOS	ATENDE
117	Implementar o bloqueio de exploits conhecidos;	FortiOS 7.0 Administration Guide https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-mitigating-vulnerabilities-fortigate-ips-overview.pdf	pag.1286 N/A	IPS signatures	ATENDE
118	Implementar os seguintes mecanismos de inspeção de IPS e efetuar suas respectivas proteções:	FortiOS 7.0 Administration Guide	pag.1285 a pag.1310	Intrusion prevention	ATENDE
a	Análise de padrões de estado de conexões;	FortiOS 7.0 Data Sheet	pag.11	SSL Inspection	ATENDE
b	Análise de decodificação de protocolo;	https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-does-the-IPS-engine-determine-if-a-packet/ta-p/199692	N/A	N/A	ATENDE
c	Análise para detecção de anomalias de protocolo;	https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-does-the-IPS-engine-determine-if-a-packet/ta-p/199692	N/A	N/A	ATENDE
d	Remontagem de pacotes de TCP;	FortiOS 7.0 Hardware Acceleration Guide	pag.45	Reassembling and offloading fragmented packets	ATENDE
e	Bloqueio de pacotes malformados;	https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-does-the-IPS-engine-determine-if-a-packet/ta-p/199692	N/A	N/A	ATENDE
119	Bloquear os comportamentos e técnicas maliciosas abaixo:	FortiOS 7.0 Administration Guide	pag.1285 a pag.1310	Intrusion prevention	ATENDE
a	Cabeçalhos inválidos de protocolo	https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-does-the-IPS-engine-determine-if-a-packet/ta-p/199692	N/A	N/A	ATENDE
b	Técnicas de reconhecimento ativas, como varredura de IPs e portas e mapeamento de aplicações e sites web (Web Crawler);	FortiOS 7.0 Data Sheet https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-block-NMAP-port-scanner/ta-p/196222	pag.11 N/A	IPS and DOS	ATENDE
c	Técnicas de invasão de aplicações web como Cross-site scripting e Injection (SQL, LDAP, OS commands, argumentos de programas).	https://www.fortiguard.com/search?q=csrf&engine=1&type=ips	N/A	N/A	ATENDE
d	Técnicas de negação de serviço como DOS (Denial of Service), SYN Flood, UDP Flood e ICMP Flood;	FortiOS 7.0 Data Sheet https://community.fortinet.com/t5/FortiGate/Technical-Tip-Block-IP-address-with-DDoS-attacks-detection/ta-p/252839	pag.11 N/A	IPS and DOS	ATENDE
e	Consultas DNS de domínios maliciosos;	FortiOS 7.0 Data Sheet	pag.7 e pag.11	Protective DNS / IPS and DOS	ATENDE
f	Acessos a serviços e IPs conhecidamente maliciosos;	FortiOS 7.0 Data Sheet FortiOS 7.0 Administration Guide	pag.7 pag.1142	Anti-Malware IP reputation filtering	ATENDE
g	Canal de comando de controle de malwares e botnets;	FortiOS 7.0 Data Sheet	pag.7 e pag.11	Anti-Malware	ATENDE
h	Estouro de pilha (buffer overflow);	https://www.fortiguard.com/search?q=buffer+overflow&engine=1&type=ips	N/A	N/A	ATENDE
i	Tráfego com perfil malicioso gerado por ameaças como: Spywares, Adware, Backdoor, Keylogger, Password stealer, Trojan, Rootkit e Network worm;	FortiOS 7.0 Data Sheet	pag.7 e pag.11	Anti-Malware	ATENDE

120	Detectar e prevenir ataques não orientados a conexão (stateless);	FortiOS 7.0 CLI Reference https://www.fortiguard.com/encyclopedia/ips/48409	pag.555 N/A	Config IPS Sensor	ATENDE
121	Permitir a aplicação de novas políticas sem interrupção de tráfego;	FortiOS 7.0 Administration Guide	pag.832 e pag.1291	Firewall policy parameters Configuring signatures and filters	ATENDE
122	Executar as suas funções sem a instalação de agentes nos hosts a serem protegidos;	FortiOS 7.0 Administration Guide	pag.832 pag.1285 e pag.1290	Firewall policy parameters Intrusion prevention Configuring an IPS sensor	ATENDE
123	Identificar hosts conectados à rede que apresentem comportamento anormal potencialmente danoso, como propagação de malwares e botnets	FortiOS 7.0 Administration Guide	pag. 1285	Intrusion prevention	ATENDE
124	Capturar e armazenar o perfil do tráfego associado a cada dispositivo de rede, disponibilizando relatórios com as seguintes informações:	FortiOS 7.0 Administration Guide https://community.fortinet.com/t5/FortiGate/Technical-Tip-Testing-of-IPS-sensor-packet-logging/ta-p/189652 https://community.fortinet.com/t5/Support-Forum/View-fortigate-AV-and-IPS-logs/td-p/214382	pag.104 N/A N/A	Monitors	ATENDE
a	Endereço IP;	FortiOS 7.0 Administration Guide https://community.fortinet.com/t5/FortiGate/Technical-Tip-Testing-of-IPS-sensor-packet-logging/ta-p/189652 https://community.fortinet.com/t5/Support-Forum/View-fortigate-AV-and-IPS-logs/td-p/214382	pag.104 N/A N/A	Monitors	ATENDE
b	Serviços e portas utilizadas;	FortiOS 7.0 Administration Guide https://community.fortinet.com/t5/FortiGate/Technical-Tip-Testing-of-IPS-sensor-packet-logging/ta-p/189652 https://community.fortinet.com/t5/Support-Forum/View-fortigate-AV-and-IPS-logs/td-p/214382	pag.104 N/A N/A	Monitors	ATENDE
c	Tipo e volume de tráfego;	FortiOS 7.0 Administration Guide https://community.fortinet.com/t5/FortiGate/Technical-Tip-Testing-of-IPS-sensor-packet-logging/ta-p/189652 https://community.fortinet.com/t5/Support-Forum/View-fortigate-AV-and-IPS-logs/td-p/214382	pag.104 N/A N/A	Monitors	ATENDE

d	Aplicativos;	FortiOS 7.0 Administration Guide https://community.fortinet.com/t5/FortiGate/Technical-Tip-Testing-of-IPS-sensor-packet-logging/ta-p/189652 https://community.fortinet.com/t5/Support-Forum/View-fortigate-AV-and-IPS-logs/td-p/214382	pag.104 N/A N/A	Monitors	ATENDE
e	Vulnerabilidades ou ameaças associadas a cada dispositivo;	FortiOS 7.0 Administration Guide https://community.fortinet.com/t5/FortiGate/Technical-Tip-Testing-of-IPS-sensor-packet-logging/ta-p/189652 https://community.fortinet.com/t5/Support-Forum/View-fortigate-AV-and-IPS-logs/td-p/214382	pag.104 N/A N/A	Monitors	ATENDE
125	Identificar serviços sendo executados em portas não autorizadas;	FortiOS 7.0 Administration Guide https://community.fortinet.com/t5/FortiGate/Technical-Tip-Port-enforcement-check/ta-p/196078	pag.1279 N/A	Port enforcement check	ATENDE
126	Bloquear automaticamente o tráfego oriundo e destinado a hosts cujo comportamento esteja fora de conformidade com as políticas estabelecidas, ou seja, identificado como efetivamente ou potencialmente danoso.	FortiOS 7.0 Data Sheet FortiOS 7.0 Administration Guide	pag.4 e pag.10 pag.1285	Automation Intrusion prevention	ATENDE
127	Suportar assinaturas, seja nativamente ou por meio de configurações, para protocolos de aplicação, entre os quais devem constar, no mínimo, os seguintes:	FortiOS 7.0 Data Sheet	pag.11 e pag.12	IPS and DOS / Anti-Malware Firewall	ATENDE
a	HTTP, SMTP, FTP, RPC (MS-RPC), POP3, TELNET, DNS, IMAP, DHCP, TFTP, NNTP, RTSP, SNMP, SYSLOG, SSH, SMB (NetBIOS), VNC, NTP, LDAP, NBNAME, SSL, NBDS e RADIUS;	FortiOS 7.0 Data Sheet	pag.11 e pag.12	IPS and DOS / Anti-Malware Firewall	ATENDE
b	AOL-IM, Yahoo-IM, Microsoft Live Messenger e IRC;	https://www.fortiguard.com/services/appcontrol https://www.fortiguard.com/encyclopedia/fct-app/13558 https://www.fortiguard.com/encyclopedia/ips/29736 https://www.fortiguard.com/encyclopedia/ips/18262	N/A N/A N/A N/A	N/A	ATENDE
c	SIP.	FortiOS 7.0 Data Sheet	pag.12	Firewall	ATENDE
128	Manter dados sobre ataques, com o número de vezes que um ataque ocorreu, quando e de que forma ele ocorreu e informações sobre quais aplicações foram usadas;	FortiAnalyzer Administration Guide	pag.78	Traffic	ATENDE
129	Deve suportar referência cruzada com CVE;	FortiOS 7.0 Data Sheet	pag.7	IPS and DOS	ATENDE https://www.fortinet.com/resources/cyberglossary/cve
130	Em cada proteção de segurança, deve estar incluso informações como:	FortiOS 7.0 Data Sheet FortiOS 7.0 Administration Guide	pag.7 e pag.11 pag.1300 a pag.1301	IPS and DOS CVE pattern	ATENDE

a	Código CVE (Common Vulnerabilities and Exposures), não sendo aceito outro código de referência;	FortiOS 7.0 Data Sheet FortiOS 7.0 Administration Guide	pag.7 e pag.11 pag.1300 a pag.1301	IPS and DOS CVE pattern	ATENDE
b	Severidade;	FortiOS 7.0 Data Sheet FortiOS 7.0 Administration Guide	pag.7 e pag.11 pag.1300 a pag.1301	IPS and DOS CVE pattern	ATENDE
c	Tipo de ação a ser executada.	FortiOS 7.0 Data Sheet FortiOS 7.0 Administration Guide	pag.7 e pag.11 pag.1300 a pag.1301	IPS and DOS CVE pattern	ATENDE
131	O IPS deve fornecer um mecanismo automatizado para ativar ou gerenciar novas assinaturas vindas de atualizações.	FortiOS 7.0 Administration Guide https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-manually-upgrade-the-IPS-Engine/ta-p/194513	pag.2246 N/A	Configuring FortiGuard updates	ATENDE
132	O IPS deve suportar exceções de rede com base na origem, destino, serviço ou uma combinação dos três.	FortiOS 7.0 Data Sheet FortiOS 7.0 Administration Guide	pag.11 pag.1290	IPS and DOS Configuring an IPS sensor	ATENDE
133	O IPS deve incluir um modo de solução de problemas que defina o perfil em uso para detectar apenas, sem modificar as proteções individuais.	FortiOS 7.0 Administration Guide	pag.1286, pag 1291 e pag.2852	IPS sensors Configuring signatures and filters CLI troubleshooting cheat sheet	ATENDE
	SISTEMA DE CATEGORIZAÇÃO / FILTRAGEM DE CONTEÚDO E URL				ATENDE
134	Filtrar o tráfego criptografado via SSL/TLS independente de porta, tanto na entrada quanto na saída (inbound e outbound), atuando como man-in-the-middle;	FortiOS 7.0 Data Sheet FortiOS 7.0 Administration Guide	pag.12 pag.1839 e pag.1371	Web and Video Filtering TLS 1.3 support Deep inspection	ATENDE
135	Verificar certificados de URL solicitadas, permitindo bloqueio, caso o certificado seja classificado como inválido;	FortiOS 7.0 Data Sheet FortiOS 7.0 Administration Guide	pag 12 pag.1370	Web and Video Filtering Certificate inspection	ATENDE
136	Aplicar para o conteúdo criptografado os mesmos filtros utilizados para o protocolo HTTP.	FortiOS 7.0 Data Sheet	pag 11 e pag.12	SSL Inspection Web and Video Filtering	ATENDE
137	Implementar filtros de URL bidirecionais (inbound e outbound) incluindo o exame de conteúdo de todas as requisições e respostas (requests e responses);	FortiOS 7.0 Administration Guide	pag.1198 a pag.1203	Web filter	ATENDE
138	Implementar filtros de URL customizados por políticas;	FortiOS 7.0 Data Sheet FortiOS 7.0 Administration Guide	pag.12 pag.1199 a pag.1203 e pag 1394	Web and Video Filtering URL filter Overrides	ATENDE
139	Implementar filtros de URL baseados em base de dados armazenada localmente nos equipamentos ou armazenada remotamente em nuvem de alta disponibilidade, com opção de cache local das informações já consultadas;	FortiOS 7.0 Administration Guide	pag.1205 pag.2252 a pag.2255	FortiGuard filter Filtering	ATENDE
140	Bloquear requisições por meio de filtros de extensão de arquivos;	FortiOS 7.0 Administration Guide	pag.1311	File filter	ATENDE
141	Implementar controle de acesso a sites HTTP, HTTPS baseado em lista negra e lista branca;	FortiOS 7.0 Data Sheet https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-configure-web-rating-override-for-specific/ta-p/193384	pag.12 N/A	Web and Video Filtering	ATENDE
142	Controlar o acesso a sites HTTP e HTTPS, permitindo a definição de perfis de acesso diferenciados para determinados serviços, endereços de origem, endereços de destinos, domínios, URLs, faixa de tempo, e usuários e grupos da rede Windows (utilizando a base de usuários e grupos do Active Directory);	FortiOS 7.0 Administration Guide FortiOS 7.0 Data Sheet	pag.832 pag.12	Firewall policy parameters Web and Video Filtering	ATENDE
143	Permitir ou bloquear sites ou categorias de sites, por:	FortiOS 7.0 Administration Guide	pag.832 e pag.904	Firewall policy parameters Use Active Directory objects directly in policies	ATENDE

a	Usuário do Active Directory;	FortiOS 7.0 Administration Guide	pag.832 e pag.904	Firewall policy parameters Use Active Directory objects directly in policies	ATENDE
b	Grupo do Active Directory e	FortiOS 7.0 Administration Guide	pag.832 e pag.904	Firewall policy parameters Use Active Directory objects directly in policies	ATENDE
c	Faixa de tempo	FortiOS 7.0 Administration Guide https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-configure-schedule-policy-with-deny-action/ta-p/193508	pag.832 e pag.1198 N/A	Firewall policy parameters URL filter	ATENDE
144	Permitir o uso de wildcards, máscaras ou expressões regulares, permitindo que seja filtrado conteúdo presente no header HTTP;	FortiOS 7.0 Administration Guide	pag.1201, pag.935, pag.936 e pag.253	Configuring a URL filter in the GUI FQDN addresses Using wildcard FQDN addresses in firewall policies HTTP header	ATENDE
145	A base de URLs deve ser atualizada automaticamente, por meio de conexão internet, no site do fabricante e deve possuir:	FortiOS 7.0 Administration Guide https://www.fortiguard.com/webfilter	pag.2248 N/A	Automatic updates	ATENDE
a	Sites em português e inglês;	https://community.fortinet.com/t5/FortiGate/Web-filter-banned-word-blocking/ta-p/195937 https://www.fortiguard.com/webfilter	N/A N/A	N/A	ATENDE
b	Permitir a criação de categorias customizadas (user defined);	FortiOS 7.0 Administration Guide FortiOS 7.0 Data Sheet	pag.1394 pag.12	Overrides Web and Video Filtering	ATENDE
c	Permitir que qualquer site seja colocado manualmente em categoria customizada, diferente da original categorização de reputação do site	FortiOS 7.0 Administration Guide FortiOS 7.0 Data Sheet	pag.1394 pag.12	Overrides Web and Video Filtering	ATENDE
146	Definir tempo de expiração de conexões para os protocolos HTTP, HTTPS, FTP;	FortiOS 7.0 Administration Guide https://community.fortinet.com/t5/FortiGate/Technical-Tip-Session-timeout-settings/ta-p/191228	pag.909 N/A	No session timeout	ATENDE
147	Bloquear "scripts" como ActiveX e Javascript;	FortiOS 7.0 Administration Guide FortiOS 7.0 Data Sheet	pag.1230 pag.12	Remove Java applets, ActiveX, and cookies Web and Video Filtering	ATENDE
148	Bloquear download de arquivos baseado no tipo. Detectar o tipo de arquivo por meio das seguintes formas:	FortiOS 7.0 Administration Guide FortiOS 7.0 Data Sheet	pag. 1311 e pag.1317 pag.12	File filter Supported file types Web and Video Filtering	ATENDE
a	Parâmetro tipo de conteúdo (Content-Type) no cabeçalho da resposta HTTP e	FortiOS 7.0 Administration Guide FortiOS 7.0 Data Sheet	pag. 1311 e pag.1317 pag.12	File filter Supported file types Web and Video Filtering	ATENDE
b	Extensão do arquivo a ser recebido.	FortiOS 7.0 Administration Guide FortiOS 7.0 Data Sheet	pag. 1311 e pag.1317 pag.12	File filter Supported file types Web and Video Filtering	ATENDE
149	Controlar aplicações WEB, sendo possível definir ações de monitoramento e bloqueio de aplicações, incluindo: Instant Messaging e Streaming Media	FortiOS 7.0 Data Sheet FortiOS 7.0 Administration Guide	pag.12 pag 1272	ApplicationControl Configuring an application sensor	ATENDE
150	Registrar regras de exceção a sites HTTPS ou categoria de sites que não devem ter seu tráfego inspecionado;	FortiOS 7.0 Administration Guide	pag.1394, pag.1373, pag.1199 e pag.832	Overrides Exempt web sites from deep inspection URL filter Firewall policy parameters	ATENDE

151	Definir políticas que possam ser aplicadas por:	FortiOS 7.0 Administration Guide	pag.1394, pag.1199 e pag.832	Overrides URL filter Firewall policy parameters	ATENDE
a	Categorias;	FortiOS 7.0 Data Sheet	pag 12	Web and Video Filtering	ATENDE
b	Horários do dia;	FortiOS 7.0 Administration Guide https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-configure-schedule-policy-with-deny-action/ta-p/193508	pag.1394, pag.1199 e pag.832 N/A	Overrides URL filter Firewall policy parameters	ATENDE
c	Dias da semana;	FortiOS 7.0 Administration Guide https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-configure-schedule-policy-with-deny-action/ta-p/193508	pag.1394, pag.1199 e pag.832 N/A	Overrides URL filter Firewall policy parameters	ATENDE
d	Endereço IP;	FortiOS 7.0 Administration Guide	pag 832	Firewall policy parameters	ATENDE
e	Usuário do Active Directory;	FortiOS 7.0 Administration Guide	pag.832 e pag.904	Firewall policy parameters Use Active Directory objects directly in policies	ATENDE
f	Grupo do Active Directory;	FortiOS 7.0 Administration Guide	pag.832 e pag.904	Firewall policy parameters Use Active Directory objects directly in policies	ATENDE
g	Expressões de request de URL e	https://community.fortinet.com/t5/FortiGate/Technical-Tip-URL-Filter-expressions-for-the-FortiGate/ta-p/192746 https://community.fortinet.com/t5/FortiGate/Technical-Note-How-to-block-a-domain-and-sub-domains-using-Web/ta-p/190290	N/A N/A	N/A	ATENDE
h	Terminação de URLs (ex. "gov.br").	https://community.fortinet.com/t5/FortiGate/Technical-Tip-URL-Filter-expressions-for-the-FortiGate/ta-p/192746 https://community.fortinet.com/t5/FortiGate/Technical-Note-How-to-block-a-domain-and-sub-domains-using-Web/ta-p/190290	N/A N/A	N/A	ATENDE
152	Possuir mecanismo que permite ao administrador do sistema definir determinada página como resposta quando a URL for bloqueada;	FortiOS 7.0 Data Sheet FortiOS 7.0 Administration Guide	pag.11 pag.1204 e pag.2238	Web and Video Filtering Verifying the URL filter results Replacement message images	ATENDE
	SISTEMA DE ANTIMALWARE				ATENDE

153	Inspecionar conteúdo para verificação e eliminação de vírus e malwares;	FortiOS 7.0 Data Sheet FortiOS 7.0 Administration Guide	pag 11 pag.1156	Anti-Malware Antivirus	ATENDE FortiOS 7.0 CLI Reference https://www.fortiguard.com/encyclopedia/ips/48409 https://community.fortinet.com/t5/FortiGate/Technical-Tip-What-compression-file-formats-does-the-FortiGate/ta-p/192580 pag 1018
154	Inspecionar simultaneamente mais de um arquivo;	FortiOS 7.0 Data Sheet FortiSandbox Data Sheet	pag.7 e pag.11 pag.6 e pag.8	Anti-Malware Parallel scan to run multiple distinct VM types simultaneously System Performance	ATENDE https://docs.fortinet.com/document/fortisandbox/4.4.2/administration-guide/395793/scan-profile-advanced-tab
155	Efetuar análise de objetos encapsulados tais como ZIP, RAR, TAR ou 7z permitindo configuração de bloqueio;	FortiOS 7.0 Administration Guide	pag.1317 e pag.1318	Supported file types	ATENDE FortiOS 7.0 CLI Reference https://www.fortiguard.com/encyclopedia/ips/48409 https://community.fortinet.com/t5/FortiGate/Technical-Tip-What-compression-file-formats-does-the-FortiGate/ta-p/192580 pag 1018
156	As verificações de malware devem ocorrer de forma concorrente para cada objeto analisado, em tempo real, sem enfileiramento;	FortiOS 7.0 Data Sheet FortiSandbox Data Sheet	pag.7 e pag.11 pag.6 e pag.8	Anti-Malware Parallel scan to run multiple distinct VM types simultaneously System Performance	ATENDE https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf

157	Verificar tráfego analisando os dados de aplicação, identificando estações de trabalho da rede interna possivelmente infectadas por malwares.	FortiOS 7.0 Data Sheet FortiOS 7.0 Administration Guide FortiAnalyzer Administration Guide	pag 11 pag.1156 pag.176	Anti-Malware Antivirus Default event views	ATENDE
158	Identificar e bloquear aplicações maliciosas, inclusive dos tipos:	FortiOS 7.0 Data Sheet FortiOS 7.0 Administration Guide	pag.12 pag.1230 e pag.1190	Web and Video Filtering Remove Java applets, ActiveX, and cookies Accepted file types	ATENDE
a	Javascripts;	FortiOS 7.0 Administration Guide	pag.1311 e pag.1317 a pag.1318	File filter Supported file types	ATENDE
b	Java applets;	FortiOS 7.0 Data Sheet FortiOS 7.0 Administration Guide	pag.12 pag.1230 e pag.1190	Web and Video Filtering Remove Java applets, ActiveX, and cookies Accepted file types	ATENDE
c	Java applications;	FortiOS 7.0 Data Sheet FortiOS 7.0 Administration Guide	pag.12 pag.1230 e pag.1190	Web and Video Filtering Remove Java applets, ActiveX, and cookies Accepted file types	ATENDE
d	ActiveX;	FortiOS 7.0 Data Sheet FortiOS 7.0 Administration Guide	pag.12 pag.1230 e pag.1190	Web and Video Filtering Remove Java applets, ActiveX, and cookies Accepted file types	ATENDE
e	Flash;	https://www.fortiguard.com/appcontrol/16683	N/A	N/A	ATENDE
f	Executáveis Windows;	FortiOS 7.0 Administration Guide	pag.1311 e pag.1317	File filter Supported file types	ATENDE
g	Potencialmente não desejados (spywares);	FortiOS 7.0 Administration Guide https://www.fortiguard.com/search?q=spyware&engine=1&type=av	pag.1158 N/A	Configuring an antivirus profile	ATENDE
	SISTEMA DE INSPEÇÃO DE PACOTES SSL/TLS				ATENDE
159	Controlar, inspecionar e de-criptografar SSL/TLS por política para tráfego de entrada (Inbound) e Saída (Outbound):	FortiOS 7.0 Data Sheet FortiOS 7.0 Administration Guide FortiOS 7.0 Supported RFCs	pag.11 e pag.12 pag.832 pag.1368 e pag.1839 pag.14	SLL Inspection Application Control Firewall policy parameters To configure an SSL/SSH inspection profile in the GUI TLS 1.3 support TLS	ATENDE
a	Deve identificar, de-criptografar e analisar o tráfego SSL/TLS em conexões de saída (Outbound);	FortiOS 7.0 Data Sheet FortiOS 7.0 Administration Guide FortiOS 7.0 Supported RFCs	pag.11 e pag.12 pag.832 pag.1368 e pag.1839 pag.14	SLL Inspection Application Control Firewall policy parameters To configure an SSL/SSH inspection profile in the GUI TLS 1.3 support TLS	ATENDE

b	Deve identificar, de-criptografar e analisar o tráfego SSL/TLS em conexões de entrada (Inbound);	FortiOS 7.0 Data Sheet FortiOS 7.0 Administration Guide FortiOS 7.0 Supported RFCs	pag.11 e pag.12 pag.832 pag.1368 e pag.1839 pag.14	SLL Inspection Application Control Firewall policy parameters To configure an SSL/SSH inspection profile in the GUI TLS 1.3 support TLS	ATENDE
160	A inspeção de SSL/TLS deve permitir a criação de diferentes politicas para a diferenciação de trafegos pessoais dos demais tipos de trafego;	FortiOS 7.0 Data Sheet FortiOS 7.0 Administration Guide FortiOS 7.0 Supported RFCs	pag.11 e pag.12 pag.1367 pag.1368 e pag.1839 pag.14	SLL Inspection Application Control SSL & SSH Inspection To configure an SSL/SSH inspection profile in the GUI TLS 1.3 support TLS	ATENDE
161	Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2 e TLS 1.3.	FortiOS 7.0 Data Sheet FortiOS 7.0 Administration Guide FortiOS 7.0 Supported RFCs	pag.11 e pag.12 pag.290, pag.1368 e pag.1839 pag.14	SLL Inspection Application Control Example To configure an SSL/SSH inspection profile in the GUI TLS 1.3 support TLS	ATENDE
	SISTEMA DE CONTROLE DE APLICAÇÕES				ATENDE
162	Implementar a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:	FortiOS 7.0 Data Sheet FortiOS 7.0 Administration Guide	pag.12 pag.1271	Application control Application control	ATENDE
a	Deve ser possível a liberação e bloqueio somente das aplicações, sem a necessidade de liberação de portas e protocolos, e controlar o uso da largura de banda que cada aplicação utiliza ou que cada usuário utiliza.	FortiOS 7.0 Data Sheet FortiOS 7.0 Administration Guide	pag.12 pag.1272 a 1275	Application control Configuring an application sensor	ATENDE
b	Reconhecer, pelo menos, as seguintes aplicações: a tráfego relacionado a torrents e outras aplicações peer-to-peer, redes sociais, ferramentas de acesso remoto, mensageiros instantâneos, compartilhamento de arquivos, e-mail;	FortiOS 7.0 Data Sheet FortiOS 7.0 Administration Guide	pag.12 pag.1272 e pag.1273	Application control Configuring an application sensor Basic category filters and overrides	ATENDE
c	Deve inspecionar o payload do pacote de dados com o objetivo de determinar, através de assinaturas de aplicações conhecidas pelo fabricante, a que tipo de aplicação pertence, mesmo quando usada com portas não padrão;	FortiOS 7.0 Data Sheet FortiOS 7.0 Administration Guide	pag.12 pag.1271 e pag.1371	Application control Application control Reasons for using deep inspection	ATENDE
d	Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e ataques mediante a porta 443	FortiOS 7.0 Data Sheet FortiOS 7.0 Administration Guide	pag.11 pag.1273, pag.1367 e pag.1371	SSL Inspection Basic category filters and overrides SSL & SSH Inspection Deep inspection	ATENDE
e	Para tráfego criptografado HTTPS, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;	FortiOS 7.0 Data Sheet FortiOS 7.0 Administration Guide	pag.11 pag.1271 e pag.1372	SSL Inspection Application control Protocol port mapping	ATENDE
f	Atualizar a base de assinaturas de aplicações automaticamente;	FortiOS 7.0 Administration Guide	pag.2248	Automatic updates	ATENDE
g	Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;	FortiOS 7.0 Administration Guide	pag.1271	Application control	ATENDE
h	Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;	FortiOS 7.0 Administration Guide	pag.1386, pag.1289 e pag.2680	Blocking applications with custom signatures Application category filter Resolve Unknown Applications	ATENDE

i	Implementar controle de largura de banda para priorização por aplicações (como por exemplo Skype, Bittorrent, YouTube, Spotify, Azureus) ou grupos de aplicações (como por exemplo Instant Messaging ou P2P);	FortiOS 7.0 Data Sheet https://community.fortinet.com/t5/FortiGate/Technical-Tip-Checking-user-host-details-which-is-consuming-high/ta-p/198670	pag.12 e pag.13 N/A	Application control SD-WAN	ATENDE
j	Deve permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário;	FortiOS 7.0 Administration Guide	pag.115	FortiView Sessions	ATENDE
	QUALIDADE DE SERVIÇO (QoS)				ATENDE
163	Implementar a criação de políticas de QoS por:	FortiOS 7.0 Administration Guide	pag.965 a pag.994	Traffic shaping	ATENDE
a	Endereço de origem;	FortiOS 7.0 Administration Guide	pag.965 a pag.994	Traffic shaping	ATENDE
b	Endereço de destino;	FortiOS 7.0 Administration Guide	pag.965 a pag.994	Traffic shaping	ATENDE
c	Por usuário ou Grupo do AD;	FortiOS 7.0 Administration Guide	pag.965 a pag.994	Traffic shaping	ATENDE
d	Por porta	FortiOS 7.0 Administration Guide	pag.965 a pag.994	Traffic shaping	ATENDE
164	O QoS deve possibilitar a definição de classes por:	FortiOS 7.0 Administration Guide	pag.965 a pag.994	Traffic shaping	ATENDE
a	Banda Garantida	FortiOS 7.0 Administration Guide	pag.965 a pag.994	Traffic shaping	ATENDE
b	Banda Máxima;	FortiOS 7.0 Administration Guide	pag.965 a pag.994	Traffic shaping	ATENDE
c	Fila de Prioridade.	FortiOS 7.0 Administration Guide	pag.965 a pag.994	Traffic shaping	ATENDE
165	Suportar priorização RealTime de protocolos de voz (VOIP), como, por exemplo, H.323, SIP, SCCP, MGCP e aplicações como Skype.	FortiOS 7.0 Data Sheet	pag.12 e pag.13	Firewall SD-WAN	ATENDE
166	Implementar marcação de pacotes Diffserv;	FortiOS 7.0 Data Sheet	pag.13	SD-WAN	ATENDE
	SANDBOX				ATENDE
167	A Sandbox deverá ser integrada à solução, podendo ser on premisses ou na nuvem, sendo obrigatória a integração com o NGFW;	FortiOS 7.0 Data Sheet	pag.10	System Integration	ATENDE
168	Deverá ser possível analisar arquivos suspeitos incluindo, como, por exemplo, arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), .pdf, RAR, 7z, zip;	FortiSandbox Data Sheet	pag.6	Sandboxing (Dynamic AI Scan) Support	ATENDE
169	Deverá fazer análise dinâmica do comportamento do malware em ambientes que simulam ambientes reais;	FortiSandbox Data Sheet	pag.6	Sandboxing (Dynamic AI Scan) Support	ATENDE
170	A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows, Mac OS e Linux;	FortiSandbox Data Sheet	pag.6	Sandboxing (Dynamic AI Scan) Support	ATENDE
171	Para melhor administração da solução, a solução deve possibilitar as seguintes visualizações a nível de monitoração:	FortiSandbox Data Sheet	pag.7	Monitoring And Reporting	ATENDE
a	Número de arquivos emulados;	FortiSandbox Data Sheet	pag.7	Monitoring And Reporting	ATENDE
b	Número de arquivos com malware.	FortiSandbox Data Sheet	pag.7	Monitoring And Reporting	ATENDE