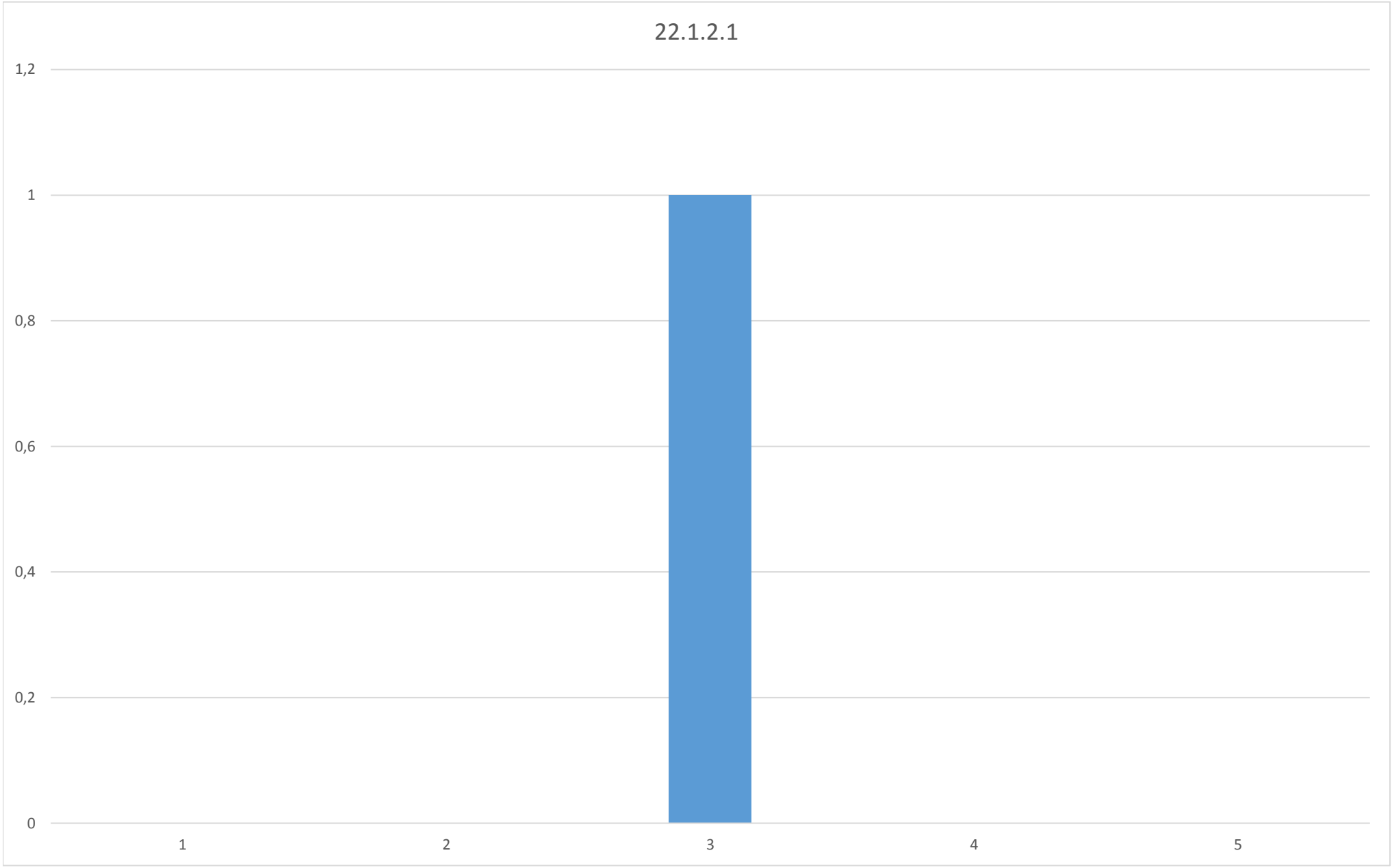
22.1.2.1
1,2
1
0,8
0,6
0,4
0,2
0
1
2
3
4
5

MÓDULO DE CONTROLE DE PERÍMETRO FÍSICO - FIREWALL					
	ITEM	Documento	Página	Localização	Analise
22.1	O módulo de segurança deve possuir a capacidade e as características abaixo, por equipamento.	N/A	N/A	N/A	
22.1.1	Performance mínima de:	N/A	N/A	N/A	
22.1.1.1	16 Gbps com a funcionalidade de controle de aplicação habilitada para todas as assinaturas que o fabricante possuir;	pa-5200-series.pdf	1	Performance and Capacities	ok
22.1.1.2	8 Gbps com as seguintes funcionalidade habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito;	pa-5200-series.pdf	1	Firewall throughput	ok
22.1.2	Condições de avaliação de performance:	N/A	N/A	N/A	
22.1.2.1	Os documentos públicos devem comprovar os throughputs aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real (real-word traffic blend/enterprise traffic mix);	pa-5200-series.pdf	1	Firewall throughput	ok
22.2	Não será aceito aceleração de pacotes na placa de rede limitando a análise somente até camada 4.	https://www.paloaltonetworks.com/technologies/single-pass-architecture			ok
22.3	Suporte a, no mínimo, 3,8 milhões de conexões simultâneas.	pa-5200-series.pdf	1	Max sessions	ok
22.4	Suporte a, no mínimo, 110 mil novas conexões HTTP por segundo.	pa-5200-series.pdf	1	New sessions per second3	ok
22.5	Fonte 120/240 AC ou DC, redundante e hot-swappble.	pa-5200-series.pdf	2	Max Current	ok
22.6	Disco Solid State Drive (SSD) redundante de, no mínimo, 220 GB.	pa-5200-series.pdf	2	Storage Capacity	ok
22.7	Discos de, no mínimo, 2 TB em RAID 1 para armazenamento de logs interno ou externo a solução de firewall.	pa-5200-series.pdf	2	Storage Capacity	ok
22.8	Possuir ao menos 24 interfaces de rede nas seguintes quantidades mínimas:	pa-5200-series.pdf	2	I/O	ok
22.8.1	04 (quatro) interfaces de rede 1 Gbps em portas cobre;	pa-5200-series.pdf	2	I/O	ok
22.8.2	08 (oito) interfaces de rede 1 Gbps SFP;	pa-5200-series.pdf	2	I/O	ok
22.8.3	08 (oito) interfaces de rede 10 Gbps SFP+;	pa-5200-series.pdf	2	I/O	ok
22.8.4	02 (duas) interfaces dedicadas para alta disponibilidade sendo pelo menos do tipo 10 Gbps;	section_3.pdf	5 (11)	AUX 1 and AUX 2 ports	ok
22.8.5	01 (uma) interface de rede 1 Gbps dedicada para gerenciamento;	section_3.pdf	6 (12)	MGT port	ok
22.8.6	01 (uma) interface do tipo console ou similar;	section_3.pdf	5 (11)	CONSOLE port (RJ-45)	ok
22.9	Todas os módulos para as interfaces referentes aos itens 19.8.2 e 19.8.3, deverá ser fornecida aos pares do mesmo modelo e fabric	De acordo com as especificações do edital			
22.10	Suporte a, no mínimo, 15 (quinze) roteadores virtuais;	https://www.paloalto-network.com/products/secure-the-network/next-generation-firewall/pa-5200-series		PA-5220	ok
22.11	Suporte a, no mínimo, 60 (sessenta) zonas de segurança;	WP-PA-5220-Performance	1	Max security zones	ok
22.12	Estar licenciada para ou suportar sem o uso de licença, 10.000 (dez mil) clientes de VPN SSL simultâneos e3.000 (três mil) túneis de VPN IPSEC simultâneos;	WP-PA-5220-Performance	5	IPSec VPN / GlobalProtect Client VPN	ok
22.13	Deve suportar, no mínimo, 10 sistemas virtuais lógicos (Contextos) no firewall Físico;	WP-PA-5220-Performance	3	Base virtual systems	ok
22.14	Deve permitir expansão futura a até 20 sistemas virtuais lógicos (Contextos) no firewall Físico;	WP-PA-5220-Performance	3	Max virtual systems	ok
22.15	Os contextos virtuais devem suportar as funcionalidades nativas do gateway de proteção incluindo: Firewall, IPS, Antivírus, Anti-Spyware, Filtro de URL, Filtro de Dados VPN, Controle de Aplicações, QOS, NAT e Identificação de usuários;	Virtual_Systems_Tech_Note.pdf		Traffic Flow and Virtual Systems (2º paragrafo)	ok
22.16	Por cada equipamento que compõe a plataforma de segurança, entende-se o hardware e as licenças de softwares necessárias para o seu funcionamento;	N/A	N/A	N/A	ok
22.17	Por console de gerência e monitoração, entende-se as licenças de software necessárias para as duas funcionalidades, bem como hardware dedicado para o funcionamento das mesmas;	N/A	N/A	N/A	ok
22.18	A console de gerência e monitoração podem residir na mesma solução de proteção de rede, desde que possuam recurso de CPU, memória, interface de rede e sistema operacional dedicados para esta função	https://www.paloaltonetworks.com/features/redundancy		Separate firewall data and control planes	ok
22.19	Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale	https://www.paloaltonetworks.com/services/support/end-of-life-announcements/end-of-sale	5	End-of-sale	ok
	CARACTERÍSTICAS GERAIS				ok
22.20	As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;	N/A	N/A	N/A	ok
22.21	A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;	techbrief-content-id	1	application identification	ok
22.22	O hardware e software que executem as funcionalidades de proteção de rede, bem como a console de gerência e monitoração, devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;	pa-5200-series.pdf	1	Palo Alto Networks® PA-5200	ok
22.23	Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se nec	pa-5200-series.pdf	2	Rack Mount (Dimensions)	ok
22.24	O software deverá ser fornecido em sua versão mais atualizada;	De acordo com as especificações do edital			ok
22.25	Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:	N/A	N/A	N/A	ok
22.25.1	Suporte a 4094 VLAN Tags 802.1q;	pa-5200-series.pdf	2	VLANs	ok
22.25.2	Agregação de links 802.3ad e LACP;	pa-5200-series.pdf	2	VLANs	ok
22.25.3	Policy based routing ou policy based forwarding;	PAN-OS 8.0 Administrator's Guide	988	Policy Based Forwarding	ok
22.25.4	Roteamento multicast (PIM-SM);	pa-5200-series.pdf	2	Routing	ok
22.25.5	DHCP Relay e Server;	PAN-OS 8.0 Administrator's Guide	802	DHCP	ok
22.25.6	Jumbo Frames;	PAN-OS 8.0 Administrator's Guide	255	Step 19	ok
22.25.7	Suporte à criação de objetos de rede que possam ser utilizados como endereço IP de interfaces L3;	PAN-OS 8.0 Administrator's Guide	924	Address/Address Group, Region	ok
22.26	Suportar sub-interfaces ethernet logicas;	PAN-OS 8.0 Administrator's Guide	755	VLAN-Tagged Traffic , segundo paragrafo	ok
22.27	O firewall deve ter a capacidade de testar o funcionamento de rotas estáticas e rota default com a definição de um endereço IP de destino que deve estar comunicável através de uma rota. Caso haja falha na comunicação o firewall deve ter a capacidade de usar rota alternativa para estabelecer a comunicação;	PAN-OS 8.0 Administrator's Guide	1037	Path Monitoring for PBF	ok
22.28	Deve suportar os seguintes tipos de NAT:	N/A	N/A	N/A	ok
22.28.1	Nat dinâmico (Many-to-1) e (Many-to-Many);	pa-5200-series.pdf	2	Network Address Translation	ok
22.28.2	Nat estático (1-to-1), (Many-to-Many) e bidirecional 1-to-1;	pa-5200-series.pdf	2	Network Address Translation	ok
22.28.3	Tradução de porta (PAT);	pa-5200-series.pdf	N/A	Network Address Translation	ok
22.28.4	Suportar NAT de Origem e Destino de forma independente e/ou simultaneamente;	PAN-OS 8.0 Administrator's Guide	831 e 832	Source NAT and Destination NAT	ok
22.28.5	Deve implementar Network Prefix Translation (NPTv6), prevenindo problemas de roteamento assimétrico;	PAN-OS 8.0 Administrator's Guide	848	NPTv6	ok
22.29	Deve implementar o protocolo ECMP;	PAN-OS 8.0 Administrator's Guide	866	ECMP	ok
866	Deve implementar balanceamento de link:	PAN-OS 8.0 Administrator's Guide	866	ECMP Load-Balancing Algorithms	ok
22.29.1.1	Por hash do IP de origem e destino;	PAN-OS 8.0 Administrator's Guide	866	Hash-based algorithms prioritize session stickiness	ok
22.29.1.2	através do método round-robin;	PAN-OS 8.0 Administrator's Guide	867	Balanced algorithm prioritizes load balancing	ok
22.29.1.3	por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, quarto links;	PAN-OS 8.0 Administrator's Guide	867	Weighted algorithm prioritizes link capacity and/or speed	ok
22.29.1.4	através de políticas por usuário e grupos de usuários do LDAP/AD;	PAN-OS 8.0 Administrator's Guide	990	3. (Optional) Add and select the Source User or groups of users to whom the policy applies.	ok
22.29.1.5	através de políticas por aplicação e porta de destino;	PAN-OS 8.0 Administrator's Guide	990	2. Select the Application(s) or Service(s) that you want to control using PBF.	ok

22.30	Deve implementar o protocolo Link Layer Dicovery (LLDP), permitindo que a plataforma e outros ativos da rede se comuniquem para identificação da topologia da rede em que estão conectados e a função dos mesmos facilitando o processo de throubleshooting. As informações aprendidas e armazenadas pela plataforma devem ser acessíveis via SNMP;	PAN-OS 8.0 Administrator's Guide	871	LLDP	ok
22.31	Enviar log para sistemas de monitoração externos, simultaneamente;	PAN-OS 8.0 Administrator's Guide	873	LLDP Syslog Messages and SNMP Traps	ok
22.32	Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;	PAN-OS 8.0 Administrator's Guide	356	Use Syslog for Monitoring	ok
22.33	Deve permitir configurar certificado caso necessário para autenticação no sistema de monitoração externo de logs;	PAN-OS 8.0 Administrator's Guide	357	STEP 5 | Create a certificate to secure syslog communication over TLSv1.2.	ok
22.34	Proteção contra anti-spoofing;	NEW-DoS	11	IP Spoof Protection	ok
22.35	Deve permitir bloquear sessões TCP que usarem variações do 3-way hand-shake, como 4 way e 5 way split hand-shake, prevenindo desta forma possíveis tráfegos maliciosos;	PAN-OS 8.0 Administrator's Guide	890 e 891	TCP Split Handshake Drop	ok
22.36	Dever permitir bloquear conexões que contenham dados no payload de pacotes TCP-SYN e SYN-ACK durante o three-way handshake;	PAN-OS 8.0 Administrator's Guide	516	Enable the drop TCP SYN with Data and drop TCP SYNACK with Data options	ok
22.37	Deve exibir nos logs de tráfego o motivo para o término da sessão no firewall, incluindo sessões finalizadas onde houver de-criptografia de SSL e SSH;	NEW-DoS	15 e 16	Logs with Random Early Drop	ok
22.38	Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);	pa-5200-series.pdf	2	Routing	ok
22.39	Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);	pa-5200-series.pdf	2	Routing	ok
22.40	Suportar a OSPF graceful restart;	pa-5200-series.pdf	2	Routing	ok
22.41	Deve suportar o protocolo MP-BGP (Multiprotocol BGP) permitindo que o firewall possa anunciar rotas multicast para IPv4 e rotas unicast para IPv6;	PAN-OS 8.0 Administrator's Guide	785	MP-BGP	ok
22.42	Suportar no mínimo as seguintes funcionalidades em IPv6: SLAAC (address auto configuration), NAT64, Identificação de usuários a partir do LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Regras de proteção contra DoS (Denial of Service), De-criptografia SSL e SSH, PBF (Policy Based Forwarding), QoS, DHCPv6 Relay, IPSEc, VPN SSL, Ativo/Ativo, Ativo/Passivo, SNMP, NTP, SYSLOG, DNS, Neighbor Discovery (ND), Recursive DNS Server (RDNSS), DNS Search List (DNSSL) e controle de aplicação;	pa-5200-series.pdf	1 e 2	IPv6 / Network Address Translation / Enforces security policies for any user / Prevents known and unknown threats / Classifies all applications, on all ports, all the time /	ok
22.43	O dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (l2) e camada 3 (l3);	pa-5200-series.pdf	2	Interface Modes	ok
741	Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;	PAN-OS 8.0 Administrator's Guide	741	Tap Interfaces	ok
22.43.2	Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;	PAN-OS 8.0 Administrator's Guide	748	Layer 2 Interfaces	ok
22.43.3	Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;	PAN-OS 8.0 Administrator's Guide	751	Layer 3 Interfaces	ok
22.43.4	Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;	PAN-OS 8.0 Administrator's Guide	741	Configure Interfaces	ok
22.44	Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;	PAN-OS 8.0 Administrator's Guide	226	HA Modes	ok
22.45	Em modo transparente;	PAN-OS 8.0 Administrator's Guide	226	HA Modes	ok
22.46	Em layer 3;	PAN-OS 8.0 Administrator's Guide	226	HA Modes	ok
22.47	A configuração em alta disponibilidade deve sincronizar:				ok
22.48	Sessões;	PAN-OS 8.0 Administrator's Guide	277	Session Table	ok
22.49	Configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QOS e objetos de rede;	PAN-OS 8.0 Administrator's Guide	271	Reference: HA Synchronization	ok
22.50	Certificados de-criptografados;	HA_Synchronization_RevD.pdf	9	Certificates	ok
22.51	Associações de Segurança das VPNs;	https://live.paloaltonetworks.com/t5/Learning-Articles/Information-Synchronized-on-an-HA-Pair/ta-p/57293		IPSec Sas	ok
22.52	Tabelas FIB;	PAN-OS 8.0 Administrator's Guide	277	Forward Information Base (FIB)	ok
22.53	O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link.	PAN-OS 8.0 Administrator's Guide	230	Link Monitoring / Path Monitoring	ok
22.54	As funcionalidades de controle de aplicações, VPN IPSec e SSL, QOS, SSL e SSH Decryption e protocolos de roteamento dinâmico devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.	https://live.paloaltonetworks.com/t5/Management-Articles/What-Happens-When-the-Threat-Prevention-License-Expires/ta-p/56	N/A	What Happens When the Threat Prevention License Expires?	ok
CONTROLE POR POLÍTICA DE PROTEÇÃO DE ACESSO					ok
22.55	Deverá suportar controles por zona de segurança.	PAN-OS 8.0 Administrator's Guide	31	Segment Your Network Using Interfaces and Zones	ok
22.56	Controles de políticas por porta e protocolo.	PAN-OS 8.0 Administrator's Guide	920	Service	ok
22.57	Controle de políticas por aplicações grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações.	PAN-OS 8.0 Administrator's Guide	919 / 486	Application / Use Application Objects in Policy	ok
22.58	Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança.	PAN-OS 8.0 Administrator's Guide	918	Components of a Security Policy Rule	ok
22.59	Deve suportar a consulta a fontes externas de endereços IP, domínios e URLs podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego;	PAN-OS 8.0 Administrator's Guide	967	Use an External Dynamic List in Policy	ok
22.59.1	Deve permitir autenticação segura através de certificado nas fontes externas de endereços IP, domínios e URLs;	PAN-OS 8.0 Administrator's Guide	971	TEP 9 | If the list source is secured with SSL (i.e. lists with an HTTPS URL), enable server authentication. Select a Certificate Profile or create a New Certificate Profile for authenticating the server that hosts the list.	ok
22.59.2	Deve permitir consultar e criar exceção para objetos das listas externas a partir da interface de gerência do próprio firewall;	PAN-OS 8.0 Administrator's Guide	973	Exclude Entries from an External Dynamic List	ok
22.60	Controle de políticas por código de País (Por exemplo: BR, USA, UK, RUS).	PAN-OS 8.0 Administrator's Guide	919 / 924	Address/Address Group, Region	ok
22.61	Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound).	PAN-OS 8.0 Administrator's Guide	557 / 559 / 560	Decryption Overview / SSL Forward Proxy / SSL Inbound Inspection	ok
22.62	Deve suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound);	PAN-OS 8.0 Administrator's Guide	560	SSL Inbound Inspection	ok
22.63	Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2;	PAN-OS 8.0 Administrator's Guide	210	STEP 6 | Define the range of protocols that the service can use:	ok
22.64	Deve de-criptografar sites e aplicações que utilizam certificados ECC, incluindo Elliptical Curve Digital Signature Algorithm (ECDSA);	PAN-OS 8.0 Administrator's Guide	562	SSL Decryption for Elliptical Curve Cryptography (ECC) Certificates	ok
22.65	Controle de inspeção e de-criptografia de SSH por política;	PAN-OS 8.0 Administrator's Guide	561 / 567	SSH Proxy / 2. Set the Type of decryption for the firewall to perform on matching traffic:	ok
22.66	A de-criptografia de SSH deve possibilitar a identificação e bloqueio de tráfego caso o protocolo esteja sendo usado para tunelar aplicações como técnica evasiva para burlar os controles de segurança;	PAN-OS 8.0 Administrator's Guide	561	SSH Proxy	ok
22.67	A plataforma de segurança deve implementar espelhamento de tráfego de-criptografado (SSL e TLS) para soluções externas de análise (Forense de rede, DLP, Análise de Ameaças, entre outras);	PAN-OS 8.0 Administrator's Guide	562	Decryption Mirroring	ok
22.67.1	É permitido uso de appliance externo, específico para a de-criptografia de (SSL e TLS), com espelhamento de cópia do tráfego de-criptografado tanto para a plataforma de segurança, quanto para as soluções de análise.	Não é necessário Appliance Externo			ok
22.68	Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, pif, e reg	PAN-OS 8.0 Administrator's Guide	508	basic file blocking	ok
22.69	Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo)	PAN-OS 8.0 Administrator's Guide	645 / 647	QoS Overview / QoS Profile	ok
22.70	QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações.	PAN-OS 8.0 Administrator's Guide	661	Enforce QoS Based on DSCP Classification	ok
22.71	Suporte a objetos e regras IPV6.	PAN-OS 8.0 Administrator's Guide	924	Address/Address Group, Region	ok
22.72	Suporte a objetos e regras multicast.	https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Configure-Basic-Multicast-with-Static-Rendezvous-P	N/A	How to Configure Basic Multicast	ok
22.73	Deve suportar no mínino três tipos de negação de tráfego nas políticas de firewall: Drop sem notificação do bloqueio ao usuário, Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego, TCP-Reset para o client, TCP-Reset para o server ou para os dois lados da conexão;	PAN-OS 8.0 Administrator's Guide	920 e 921	Security Policy Actions	ok

22.74	Suportar a atribuição de agendamento as políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.	https://live.paloaltonetworks.com/t5/Management-Articles/How-to-Schedule-Policy-Actions/ta-p/56328	N/A	How to Schedule Policy Actions	ok
CONTROLE DE APLICAÇÕES					ok
22.75	Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:	PAN-OS 8.0 Administrator's Guide	479	App-ID Overview	ok
22.76	Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos.	PAN-OS 8.0 Administrator's Guide	486	Use Application Objects in Policy	ok
22.77	Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;	https://applipedia.paloaltonetworks.com	N/A	2568 Applications	ok
22.78	Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs, etc;	https://applipedia.paloaltonetworks.com	N/a	Contem a lista de todas as aplicações existentes atualmente	ok
22.79	Deve inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo. A checagem de assinaturas também deve determinar se uma aplicação está utilizando a porta default ou não, incluindo, mas não limitado a RDP na porta 80 ao invés de 389;	PAN-OS 8.0 Administrator's Guide	479	App-ID Overview	ok
22.80	Deve aplicar heurística a fim de detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Encrypted Bittorrent e aplicações VOIP que utilizam criptografia proprietária;	techbrief-app-id.pdf	2	Heuristics:	ok
22.81	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.	techbrief-app-id.pdf	1	..even those that try to evade detection by masquerading as legitimate traffic, hopping ports or sneaking through the firewall using encryption (TLS/SSL or SSH)..	ok
22.82	Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;	techbrief-app-id.pdf	2	Figure 1: How App-ID classifies traffic.	ok
22.83	Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas;	techbrief-app-id.pdf	2	Application and Protocol Decoding	ok
22.84	Deve permitir a utilização de aplicativos para um determinado grupo de usuário e bloquear para o restante, incluindo, mas não limitado a Skype. Deve permitir também a criação de políticas de exceção concedendo o acesso a aplicativos como Skype apenas para alguns usuários;	PAN-OS 8.0 Administrator's Guide	34	Set Up a Basic Security Policy	ok
22.85	Identificar o uso de táticas evasivas via comunicações criptografadas;	techbrief-app-id.pdf	1	App-ID Traffic Classification Technology	ok
22.86	Atualizar a base de assinaturas de aplicações automaticamente;	techbrief-app-id.pdf	4	As new App-IDs are introduced and delivered to the firewall via weekly updates, dynamic filters are automatically updated for those applications that meet the filter criteria.	ok
22.87	Reconhecer aplicações em IPv6;	https://www.paloaltonetworks.com/documentation/global/compatibility-matrix/pan-support-by-feature/pan-support-by-feature-pan-os-version-8	N/A	App-id	ok
22.88	Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP/AD;	PAN-OS 8.0 Administrator's Guide	647	QoS Concepts	ok
22.89	Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;	PAN-OS 8.0 Administrator's Guide	440	Configure User Mapping Using the PAN-OS Integrated User-ID Agent	ok
22.90	Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;	PAN-OS 8.0 Administrator's Guide	976	A best practice policy allows you to safely enable applicationsWhat Is a Best Practice Internet Gateway Security Policy?	ok
22.91	Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos e análise heurística;	techbrief-app-id.pdf	2	Heuristics:	ok
22.92	Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;	PAN-OS 8.0 Administrator's Guide	480	Manage Custom or Unknown Applications	ok
22.93	Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;	PAN-OS 8.0 Administrator's Guide	480	Manage Custom or Unknown Applications	ok
22.94	A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de pelo menos os seguintes protocolos:	Tech_Note-Creating_Custom_Signatures.Rev0.pdf	4	Regex Syntax with Examples / Custom Signature Examples / Context Qualifier	ok
22.95	HTTP, FTP, SMB, SMTP, Telnet, SSH, MS-SQL, IMAP, IMAP, MS-RPC, RTSP e File body.	Tech_Note-Creating_Custom_Signatures.Rev0.pdf	2-4	Existem contextos para todas as aplicações listadas no indice	ok
22.96	O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;	https://live.paloaltonetworks.com/t5/Management-Articles/How-to-Request-a-new-App-ID/ta-p/58839			ok
22.97	Deve alertar o usuário quando uma aplicação for bloqueada;	PAN-OS 8.0 Web Interface Reference	490	Application Block Page	ok
22.98	Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;	Firewall-features-overview.pdf	2	Using Security to Empower Your Business	ok
22.99	Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, neonet, etc.) possuindo granularidade de controle/politicas para os mesmos;	https://applipedia.paloaltonetworks.com			ok
22.100	Deve possibilitar a diferenciação:	N/A	N/A	N/A	ok
22.100.1	de tráfegos de Instant Messaging (AIM, Gtalk, Facebook Chat, etc.) possuindo granularidade de controle/politicas para os mesmos;	techbrief-app-id.pdf	4	Application Groups:	ok
22.100.2	de partes das aplicações como por exemplo permitir o Gtalk chat e bloquear a transferência de arquivos;	techbrief-app-id.pdf	4	Application Function-Level Controls	ok
22.100.3	de aplicações Proxies (ghostsurf, freegate, etc.) possuindo granularidade de controle/politicas para os mesmos;	techbrief-app-id.pdf	4	Application Groups:	ok
22.101	Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:	PAN-OS 8.0 Administrator's Guide	486 / 487	Create an Application Group / Create an Application Filter	ok
22.101.1	Tecnologia utilizada na aplicações (Client-Server, Browse Based, Network Protocol, etc).	techbrief-app-id.pdf / applipedia.paloaltonetworks.com	4	Dynamic Filters / TECHNOLOGY	ok
22.101.2	Nível de risco da aplicação.	PAN-OS 8.0 Administrator's Guide	487	STEP 4 | Define the filter by selecting attribute values from the Category, Subcategory, Technology, Risk, and Characteristic sections.	ok
22.101.3	Categoria e sub-categoria de aplicações.	PAN-OS 8.0 Administrator's Guide	487	STEP 4 | Define the filter by selecting attribute values from the Category, Subcategory, Technology, Risk, and Characteristic sections.	ok
22.101.4	Aplicações que usem técnicas evasivas, utilizadas por malwares, como transferência de arquivos e/ou uso excessivo de banda, etc.	PAN-OS 8.0 Administrator's Guide / applipedia.paloaltonetworks.com	487	STEP 4 | Define the filter by selecting attribute values from the Category, Subcategory, Technology, Risk, and Characteristic sections. / CHARACTERISTIC	ok
PREVENÇÃO DE AMEAÇAS					ok
22.102	Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio plataforma de segurança ou entregue através de composição com outro equipamento ou fabricante.	Guide-Evaluation	1 a 5	Content id	ok

22.103	Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);	NGFW Content-ID	2 e 3	Threat Prevention (pag 2) e ntrusion Prevention (pag 3)	ok
22.104	As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.	https://live.paloaltonetworks.com/t5/Learning-Articles/What-Happens-When-the-Threat-Prevention-License-Expires/ta-p/53114			ok
22.105	Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;	PAN-OS 8.0 Administrator's Guide	502	5. (HA only) Decide whether to Sync To Peer, which enables peers to synchronize content updates after download and install (the update schedule does not sync across peers; you must manually configure the schedule on both peers	ok
22.106	Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS, Antipyware e Antivirus: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar tcp-reset;	PAN-OS 8.0 Web Interface Reference	183	Actions in Security Profiles	ok
22.107	As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;	PAN-OS 8.0 Web Interface Reference	183	Actions in Security Profiles / Alert	ok
22.108	Exceções por IP de origem ou de destino devem ser possíveis nas regras, de forma geral e assinatura a assinatura;	PAN-OS 8.0 Web Interface Reference	104	Creating and Managing Policies	ok
22.109	Deve suportar granularidade nas politicas de IPS Antivírus e Anti-Spyware , possibilitando a criação de diferentes politicas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.	PAN-OS 8.0 Web Interface Reference	104	Creating and Managing Policies	ok
22.110	Deve permitir o bloqueio de vulnerabilidades e exploits conhecidos.	NGFW Content-ID	1	Palo Alto Networks then goes beyond stopping known threats....	ok
22.111	Deve incluir proteção contra ataques de negação de serviços.	NGFW Content-ID	3	DoS attacks and port scans that lead to the compromise and....	ok
22.112	Deve suportar a inspeção e criação de regras de proteção de DOS e QOS para o conteúdo de tráfego tunelados pelos protocolos GRE e IPSEC não criptografado;	PAN-OS 8.0 Administrator's Guide	650	QoS for Clear Text and Tunneled Traffic	ok
22.113	Deverá possuir os seguintes mecanismos de inspeção de IPS:	N/A	N/A	N/A	ok
22.113.1	Análise de padrões de estado de conexões;	NGFW Content-ID	3	Protocol decoders and anomaly detection	ok
22.113.2	Análise de decodificação de protocolo;	NGFW Content-ID	2	SSL decryption	ok
22.113.3	Análise para detecção de anomalias de protocolo;	NGFW Content-ID	3	Statistical anomaly detection	ok
22.113.4	Análise heurística;	NGFW Content-ID	3	Heuristic-based analysis	ok
22.113.5	IP Defragmentation;	NGFW Content-ID	3	IP defragmentation	ok
22.113.6	Remontagem de pacotes de TCP;	NGFW Content-ID	3	TCP reassembly	ok
22.113.7	Bloqueio de pacotes malformados.	NGFW Content-ID	3	Invalid or malformed packet detection	ok
22.114	Ser imune e capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPfloof, etc;	PAN-OS 8.0 Administrator's Guide	1040	Configure DoS Protection Against Flooding of New Sessions	ok
925	Detectar e bloquear a origem de portscans com possibilidade de criar exceções para endereços IPs de ferramentas de monitoramento da organização;	PAN-OS 8.0 Administrator's Guide	1030	Configure Reconnaissance Protection	ok
22.116	Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;	PAN-OS 8.0 Administrator's Guide	925	Antivirus Profiles	ok
22.117	Suportar os seguintes mecanismos de inspeção contra ameaças de rede: análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, análise heurística, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;	NGFW Content-ID	2 e 3	Intrusion Prevention	ok
22.118	Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;	NGFW Content-ID	3	Content-ID protects networks from all types of vulnerability exploits	ok
22.119	Possuir assinaturas para bloqueio de ataques de buffer overflow;	NGFW Content-ID	3	Content-ID protects networks from all types of vulnerability exploits	ok
22.120	Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;	custom Signatures	5	These contexts are available for custom IPS signatures,	ok
22.121	Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS e anti-spyware, permitindo a criação de exceções com granularidade nas configurações;	PAN-OS 8.0 Web Interface Reference	178	Standard Signature	ok
22.122	Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;	PAN-OS 8.0 Administrator's Guide	925	The default profile inspects all of the listed protocol decoders for viruses....	ok
22.122.1	É permitido uso de appliance externo (antivírus de rede), para o bloqueio de vírus e spywares em protocolo SMB de forma a conter malwares se espalhando horizontalmente pela rede;	N/A	N/A	N/A	ok
22.123	Suportar bloqueio de arquivos por tipo;	PAN-OS 8.0 Administrator's Guide	928	File Blocking Profiles	ok
22.124	Identificar e bloquear comunicação com botnets;	PAN-OS 8.0 Administrator's Guide	327	Malicious	ok
22.125	Deve suportar varias técnicas de prevenção, incluindo Drop e tcp-rst (Cliente, Servidor e ambos);	PAN-OS 8.0 Administrator's Guide	925 -926	Antivirus Profiles / Anti-Spyware Profiles	ok
22.126	Deve suportar referencia cruzada com CVE;	PAN-OS 8.0 Administrator's Guide	550 / 936	and CVEs associated with the threat / Create Best Practice Security Profiles for the Internet Gateway	ok
22.127	Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:	N/A	N/A	N/A	ok
22.127.1	O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;	PAN-OS 8.0 Administrator's Guide	325-327	Log Types and Severity Levels	ok
22.128	Deve suportar a captura de pacotes (PCAP), por assinatura de IPS e Antyspyware;	PAN-OS 8.0 Administrator's Guide	313	Threat Packet Capture	ok
22.129	Deve permitir que na captura de pacotes por assinaturas de IPS e Antispyware seja definido o número de pacotes a serem capturados. Esta captura deve permitir selecionar, no mínimo, 50 pacotes;	PAN-OS 8.0 Administrator's Guide	318	Take a Threat Packet Capture	ok
22.130	Deve possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos sejam resolvidas pelo Firewall com endereços (IPv4 e IPv6), previamente definidos;	PAN-OS 8.0 Administrator's Guide	534	DNS Sinkholing	ok
22.131	Permitir o bloqueio de vírus, pelo menos, nos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;	PAN-OS 8.0 Administrator's Guide	925	The default profile inspects all of the listed protocol decoders for viruses....	ok
22.132	Os eventos devem identificar o país de onde partiu a ameaça;	PAN-OS 8.0 Administrator's Guide	367	Source Country	ok
22.133	Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms.	PAN-OS 8.0 Administrator's Guide	925	Antivirus Profiles	ok
22.134	Proteção contra downloads involuntários usando HTTP de arquivos executáveis. maliciosos.	PAN-OS 8.0 Administrator's Guide	925	Antivirus Profiles	ok
22.135	Rastreamento de vírus em pdf.	PAN-OS 8.0 Administrator's Guide	925	Antivirus Profiles	ok
22.136	Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.)	PAN-OS 8.0 Administrator's Guide	928	basic file blocking	ok
22.137	Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada regra de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.	PAN-OS 8.0 Administrator's Guide	921-922	Create a Security Policy Rule	ok
	ANÁLISE DE MALWARES MODERNOS				ok
22.138	Devido aos Malwares hoje em dia serem muito dinâmicos e um antivírus comum reativo não ser capaz de detectar os mesmos com a mesma velocidade que suas variações são criadas, a solução ofertada dever possuir funcionalidades para análise de Malwares não conhecidos incluídas na própria ferramenta ou entregue com composição com outro fabricante;	WildFire Datasheet	1	Automatically Prevent Highly Evasive Zero-Day Exploits and Malware	ok
22.139	O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "In Cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado;	WildFire Datasheet	1	Automatically Prevent Highly Evasive Zero-Day Exploits and Malware	ok
22.140	Selecionar através de políticas granulares quais tipos de arquivos sofrerão esta análise incluindo, mas não limitado a: endereço IP de origem/destino, usuário/grupo do AD/LDAP, aplicação, porta, URL/categoria de URL de destino, tipo de arquivo e todas estas opções simultaneamente;	https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Configure-WildFire/ta-p/58165	N/A	How to configure	ok

22.141	Deve possuir a capacidade de diferenciar arquivos analisados em pelo menos três categorias: malicioso, não malicioso e arquivos não maliciosos, mas com características indesejáveis como softwares que deixa o sistema operacional lento, que alteram parâmetros do sistema, etc.;	https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Configure-WildFire/ta-p/58165	N/A	How to configure...	ok
in clo	Suportar a análise com pelo menos 100 (cem) tipos de comportamentos maliciosos para a análise da ameaça não conhecida;	WildFire Datasheet	1	Dynamic analysis	ok
22.143	Suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows XP, Windows 7 (32 bits) e Windows 7 (64 bits);	WildFire Datasheet	4	The WildFire global cloud subscription provides	ok
22.144	Deve suportar a monitoração de arquivos trafegados na internet (HTTPs, FTP, HTTP, SMTP) como também arquivos trafegados internamente entre servidores de arquivos usando SMB em todos os modos de mplementação: sniffer, transparente e L3;	WildFire Admin Guide	12	WildFire can discover zero-day malware in web traffic...	ok
22.145	A solução deve possuir a capacidade de analisar em sand-box links (http e https) presentes no corpo de e-mails trafegados em SMTP e POP3. Deve ser gerado um relatório caso a abertura do link pela sand-box o identifique como site hospedeiro de exploits;	WildFire Admin Guide	14	Email Link Analysis	ok
22.146	A análise de links em sand-box deve ser capaz de classificar sites falsos na categoria de phishing e atualizar a base de filtro de URL da solução;	WildFire Admin Guide	13	The link directs users to a phishing site...	ok
22.147	Para ameaças trafegadas em protocolo SMTP e POP3, a solução deve ter a capacidade de mostrar nos relatórios o remetente, destinatário e assunto dos e-mails permitindo identificação ágil do usuário vítima do ataque;	WildFire Admin Guide	14	The firewall only extracts links and associated session...	ok
22.148	O sistema de análise "In Cloud" ou local deve prover informações sobre as ações do Malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo Malware, gerar assinaturas de Antivírus e Anti-spyware automaticamente, definir URLs não confiáveis utilizadas pelo novo Malware e prover informações sobre o usuário infectado (seu endereço ip e seu login de rede);	WildFire Admin Guide	70	The detailed log view displays Log Info and the WildFire Analysis...	ok
22.149	O sistema automático de analise "In Cloud" ou local deve emitir relatório com identificação de quais soluções de antivírus existentes no mercado possuem assinaturas para bloquear o malware;	WildFire Admin Guide	77	Coverage Status	ok
22.150	Deve permitir exportar o resultado das análises de malwares de dia Zero em PDF e CSV a partir da própria interface de gerência;	WildFire Admin Guide	75	click the Download as PDF button on the upper right of the report page	ok
22.151	Deve permitir o download dos malwares identificados a partir da própria interface de gerência;	WildFire Admin Guide	70	(imagem 3) "download file"	ok
22.152	Deve permitir visualizar os resultados das análises de malwares de dia zero nos diferentes sistemas operacionais suportados;	WildFire Admin Guide	70	For all samples, the WildFire analysis report displays...	ok
22.153	Deve permitir informar ao fabricante quanto a suspeita de ocorrências de falso-positivo e falso-negativo na análise de malwares de dia Zero a partir da própria interface de gerência.	WildFire Admin Guide	79	Report an Incorrect Verdict	ok
22.154	Caso a solução seja fornecida em appliance local, deve possuir, no mínimo, 28 ambientes controlados (sand-box) independentes para execução simultânea de arquivos suspeitos;	Não se aplica, não é appliance local			ok
22.155	Caso seja necessárias licenças de sistemas operacional e softwares para execução de arquivos no ambiente controlado (sand-box), as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a contratante;	Não se aplica, não é appliance local			ok
22.156	Suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;	WildFire Admin Guide	13	File Analysis	ok
22.157	Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e class), Android APKs MacOS (mach-O, DMG e PKG) no ambiente de sandbox;	WildFire Admin Guide	13	File Analysis	ok
22.158	Deve atualizar a base com assinaturas para bloqueio dos malwares identificados em sand-box com frequência de, pelo menos, 5 minutos;	WildFire Admin Guide	8	WildFire then generates signatures to recognize the newly-discovered malware, and...	ok
22.159	Permitir o envio de arquivos e links para análise no ambiente controlado de forma automática via API.	WildFire Admin Guide	10	Samples are all file types and email links submitted for WildFire analysis from the firewall and the public API	ok
22.160	Deve permitir o envio para análise em sand-box de malwares bloqueados pelo antivírus da solução;	WildFire Admin Guide	25	you can also manually submit files for analysis using the WildFire portal.	ok
	FILTRO DE URL				ok
22.161	Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);	https://live.paloaltonetworks.com/t5/Management-Articles/How-to-Schedule-Policy-Actions/ta-p/58168	N/A	How to Schedule Policy Actions	ok
22.162	Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, Ips, Redes e Zonas de segurança.	PAN-OS 8.0 Administrator's Guide	921-922	Create a Security Policy Rule	ok
22.163	Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via ldap, Active Directory, E-directory e base de dados local.	PAN-OS 8.0 Administrator's Guide	921-922 / 149	Create a Security Policy Rule / Authentication Types	ok
22.164	Permite popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório;	PAN-OS 8.0 Administrator's Guide	326	URL Filtering Logs	ok
22.165	Suporta a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;	PAN-OS 8.0 Administrator's Guide	922	STEP 6 | (Optional) Specify a URL category as match criteria for the rule.	ok
22.166	Deve bloquear o acesso a sites de busca (Google, Bing e Yahoo), caso a opção Safe Search esteja desabilitada. Deve ainda exibir página de bloqueio fornecendo instruções ao usuário de como habilitar a função;	PAN-OS 8.0 Administrator's Guide	613	Safe Search Enforcement	ok
22.167	Suportar base ou cache de URLs local na plataforma, evitando delay de comunicação/validação das URLs;	PAN-OS 8.0 Administrator's Guide	599	Management Plane (MP) URL Cache / Dataplane (DP) URL Cache	ok
22.168	Possui pelo menos 60 categorias de URLs;	https://live.paloaltonetworks.com/t5/Management-Articles/Complete-List-of-PAN-DB-URL-Filtering-Categories/ta-p/54237	N/A	Lista de catogorias existentes atualmente	ok
22.169	A categorização de URL deve analisar toda a URL e não somente até o nível de diretório;	PAN-OS 8.0 Web Interface Reference	9	Full-path Categorization of URLs in PAN-DB	ok
22.170	Suporta a criação categorias de URLs customizadas;	PAN-OS 8.0 Web Interface Reference	181	Objects > Custom Objects > URL Category	ok
22.171	Suporta a exclusão de URLs do bloqueio, por categoria;	PAN-OS 8.0 Administrator's Guide	591	Block and Allow Lists	ok
22.172	Permite a customização de página de bloqueio;	PAN-OS 8.0 Administrator's Guide	610	Customize the URL Filtering Response Pages	ok
22.173	Deve proteger contra o roubo de credenciais, usuários e senhas identificadas através da integração com Active Directory submetidos em sites não corporativos. Deve ainda permitir criação de regra onde usuários do Active Directory só possam enviar informações de login para sites autorizados na solução;	PAN-OS 8.0 Administrator's Guide	523	Prevent Credential Phishing	ok
22.174	Deve permitir bloquear o acesso do usuário caso o mesmo tente fazer o envio de suas credencias em sites classificados como phishing pelo filtro de URL da solução;	PAN-OS 8.0 Administrator's Guide	523	To enable Credential phishing prevention you must configure both User-ID to detect when users submit valid corporate credentials to a site (as opposed to personal credentials) and URL Filtering to specify the URL categories in which you want to prevent users from entering their corporate credentials. The following topics describe the different methods you can use to detect credential submissions and provide instructions for configuring credential phishing protection.	ok
22.175	Permite o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para permitir o usuário continuar acessando o site);	PAN-OS 8.0 Administrator's Guide	590	continue	ok
22.176	A funcionalidade de Filtro de URL deve operar em caráter permanente, para base ou cache instalado na solução até a data de vencimento da licença, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.	https://live.paloaltonetworks.com/t5/Management-Articles/What-Happens-When-Licenses-Expire-on-the-Palo-Alto-Networks/ta-p/52418	N/A	N/A	ok
22.177	Suporta a inclusão nos logs do produto de informações das atividades dos usuários;	PAN-OS 8.0 Administrator's Guide	359	Source User	ok
22.178	Deve salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: UserAgent, Referer, e X-Forwarded For;	PAN-OS 8.0 Web Interface Reference	57, 58 e 200	(57 e 58 =Tabela - Linha; Traffic e linha: URL Filtering) (200 HTTP Header Logging)	ok

	IDENTIFICAÇÃO DE USUÁRIOS				ok
22.179	Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via ldap, Active Directory, E-directory e base de dados local;	PAN-OS 8.0 Administrator's Guide	921-922 / 149	Create a Security Policy Rule / Authentication Types	ok
22.180	Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;	PAN-OS 8.0 Administrator's Guide	921-922 / 149	Create a Security Policy Rule / Authentication Types	ok
22.181	Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;	PAN-OS 8.0 Administrator's Guide	921-922 / 149	Create a Security Policy Rule / Authentication Types	ok
22.182	Deve implementar a criação de políticas de segurança baseada em atributos específicos do Radius, incluindo mas não limitado a: baseado no sistema operacional do usuário remoto exigir autenticação padrão Windows e on-time password (OTP) para usuários Android;	PAN-OS 8.0 Administrator's Guide	173 / 150	Configure RADIUS Authentication / One-time password (OTP	ok
22.183	Deve possuir integração com Ldap para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;	PAN-OS 8.0 Administrator's Guide	921-922 / 149	Create a Security Policy Rule / Authentication Types	ok
22.183.1	Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via syslog, para a identificação de endereços IP e usuários;	PAN-OS 8.0 Administrator's Guide	422 / 442	These services include wireless controllers, 802.1x devices, Apple Open Directory servers... / Configure the PAN-OS Integrated User-ID Agent as a Syslog Listener	ok
22.184	Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);	PAN-OS 8.0 Administrator's Guide	450	Map IP Addresses to Usernames Using Captive Portal	ok
22.185	Suporte a autenticação Kerberos;	PAN-OS 8.0 Administrator's Guide	151	Kerberos	ok
22.186	Deve suportar autenticação via Kerberos para administradores da plataforma de segurança, captive Portal e usuário de VPN SSL;	PAN-OS 8.0 Administrator's Guide	149 / 450	External Authentication Services / Kerberos SSO	ok
22.187	Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;	PAN-OS 8.0 Administrator's Guide	431 / 455	Map IP Addresses to Users / Configure User Mapping for Terminal Server Users	ok
22.188	Deve identificar usuários através de leitura do campo x-fowarded-for, populando nos logs do firewall o endereço IP, bem como o usuário de rede responsável pelo acesso;	PAN-OS 8.0 Administrator's Guide	986	Use XFF Values for Policies and Logging Source Users	ok
22.189	Deve permitir a criação de políticas de segurança baseadas em usuários de rede com reconhecimento dos mesmos através de leitura do campo x-fowarded-for;	PAN-OS 8.0 Administrator's Guide	986	Use XFF Values for Policies and Logging Source Users	ok
22.190	O firewall deve operar/suportar Security Assertion Markup Language (SAML) 2.0, com single sign-on e single logout para as funcionalidades de Captive Portal e VPN SSL (client to server), permitindo login único e interativo para fornecer acesso automático a serviços autenticados, internos e externos a organização;	PAN-OS 8.0 Administrator's Guide	149 / 150	External Authentication Services / SAML	ok
22.191	Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;	https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/user-id/map-users-to-groups.html	N/A	Select Custom Group and Add the group	ok
22.192	Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em servidores acessados remotamente, mesmo que não sejam servidores Windows.	PAN-OS 8.0 Administrator's Guide	422	Port Mapping / For terminal servers that do not support the Terminal Services agent, such as Linux terminal servers, you can use the XML API to send user mapping information from login and logout events to User-ID	ok
	CONTROLE DE TRÁFEGO E QUALIDADE DE SERVIÇO				ok
22.193	Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming.	PAN-OS 8.0 Administrator's Guide	647	QoS for Applications and Users	ok
22.194	Suportar a criação de políticas de QoS por:	N/A	N/A	N/A	ok
22.194.1	Endereço de origem e destino;	PAN-OS 8.0 Administrator's Guide	647	QoS Policy	ok
22.194.2	Por usuário e grupo do LDAP/AD.	PAN-OS 8.0 Administrator's Guide	647	QoS Policy	ok
22.194.3	Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;	PAN-OS 8.0 Administrator's Guide	647	QoS Policy	ok
22.194.4	Por porta;	PAN-OS 8.0 Administrator's Guide	647	QoS Policy	ok
22.194.5	O QoS deve possibilitar a definição de classes por Banda Garantida, Banda Máxima e Fila de Prioridade.	PAN-OS 8.0 Administrator's Guide	648	QoS Classes	ok
22.195	Suportar priorização RealTime de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype.	PAN-OS 8.0 Administrator's Guide / appipedia.paloaltonetworks.com	647	The Palo Alto Networks firewall provides this capability by integrating the features A	ok
22.196	Suportar marcação de pacotes Diffserv, inclusive por aplicação;	PAN-OS 8.0 Administrator's Guide	661 / 647	Enforce QoS Based on DSCP Classification / QoS Policy	ok
22.197	Deve implemetar QOS (traffic-shapping), para pacotes marcados por outros ativos na rede (DSCP). A priorização e limitação do tráfego deve ser efetuada nos dois sentidos da conexão (inboud e outbound);	PAN-OS 8.0 Administrator's Guide	661 / 647	Enforce QoS Based on DSCP Classification / QoS Policy	ok
22.198	Disponibilizar estatísticas RealTime para classes de QoS.	PAN-OS 8.0 Web Interface Reference	664	Select Network > QoS and then Statistics to view QoS bandwidth	ok
22.199	Deve suportar QOS (traffic-shapping), em interface agregadas;	https://live.paloaltonetworks.com/t5/Management-Articles/Is-Quality-of-Service-QoS-Supported-on-Aggregate-Interfaces/ta-p/59658			ok
22.200	Deverá permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.	PAN-OS 8.0 Web Interface Reference	344	QoS Interface Statistics	ok
	FUNCIONALIDADES DE FILTRO DE DADOS				ok
22.201	Permite a criação de filtros para arquivos e dados pré-definidos;	PAN-OS 8.0 Administrator's Guide	506	Set Up Data Filtering - Predefined patterns and built-in settings make it easy for you to create custom patterns for filtering on social security and credit card numbers or on file properties, such as a document title or author.	ok
22.202	Os arquivos devem ser identificados por extensão e assinaturas;	PAN-OS 8.0 Administrator's Guide	508	Set Up File Blocking	ok
22.203	Permite identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (P2P, InstantMessaging, SMB, etc);	PAN-OS 8.0 Administrator's Guide	508	basic file blocking	ok
22.204	Suportar identificação de arquivos compactados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;	PAN-OS 8.0 Administrator's Guide	508	basic file blocking	ok
22.205	Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;	PAN-OS 8.0 Administrator's Guide	506	Set Up Data Filtering	ok
22.206	Permitir listar o número de aplicações suportadas para controle de dados;	PAN-OS 8.0 Web Interface Reference	206	Applications	ok
22.207	Permitir listar o número de tipos de arquivos suportados para controle de dados;	PAN-OS 8.0 Web Interface Reference	206	File Types	ok
	FUNCIONALIDADES DE GEO-LOCALIZAÇÃO				ok
22.208	Suportar a criação de políticas por Geo Localização, permitindo o tráfego de determinado Pais/Países sejam bloqueados.	PAN-OS 8.0 Administrator's Guide	924	Address/Address Group, Region	ok
22.209	Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.	PAN-OS 8.0 Administrator's Guide	361	Source Country Destination Country	ok
22.210	Deve permitir visualizar nos logs e criar políticas para liberar e bloquear tráfego de países por: tipo de arquivo, aplicação e categoria de URL;	PAN-OS 8.0 Administrator's Guide	921 / 358	Create a Security Policy Rule / Traffic Log Fields	ok
22.211	Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas.	PAN-OS 8.0 Web Interface Reference	149	Objects > Regions	ok
	FUNCIONALIDADE DE REDES PRIVADAS VIRTUAIS				ok
22.212	Suportar VPN Site-to-Site e Cliente-To-Site;	PAN-OS 8.0 Administrator's Guide	672	Site-to-Site VPN Overview	ok
22.213	Suportar IPSec VPN;	PAN-OS 8.0 Administrator's Guide	687	Set Up an IPSec Tunnel	ok
22.214	Suportar SSL VPN;	PAN-OS 8.0 Administrator's Guide	671	Remote User-to-Site VPN	ok
22.215	A VPN IPSEc deve suportar:	N/A	N/A	N/A	ok
22.215.1	DES e 3DES;	PAN-OS 8.0 Administrator's Guide	686	Encryption	ok

22.215.2	Autenticação MD5 e SHA-1;	PAN-OS 8.0 Administrator's Guide	686	Authentication	ok
22.215.3	Diffie-Hellman Group 1 , Group 2, Group 5 e Group 14;	PAN-OS 8.0 Administrator's Guide	686	DH Group	ok
22.215.4	Algoritmo Internet Key Exchange (IKEv1 e v2);	PAN-OS 8.0 Administrator's Guide	676	An IPSec VPN gateway uses IKEv1 or IKEv2 to negotiate the IKE security association (SA) and IPSec tunnel. IKEv2 is defined in RFC 5996.	ok
22.215.5	AES 128, 192 e 256 (Advanced Encryption Standard)	PAN-OS 8.0 Administrator's Guide	686	Encryption	ok
22.215.6	Autenticação via certificado IKE PKI.	PAN-OS 8.0 Administrator's Guide	674	IKE Phase 1	ok
22.215.7	Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Checkpoint, Juniper, Palo Alto Networks, Fortinet e Sonic Wall;	PAN-OS 8.0 Administrator's Guide	669	or a Palo Alto Networks firewall along with a VPN-capable device from another vendor.	ok
22.216	Deve permitir habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEc a partir da interface gráfica da solução, facilitando o processo de throubleshooting	PAN-OS 8.0 Web Interface Reference	367	IPSec VPN Tunnel Management	ok
22.217	A VPN SSL deve suportar:	N/A	N/A	N/A	ok
22.217.1	O usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;	GlobalProtect AdminGuide	9	GlobalProtect Client	ok
22.217.2	A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;	GlobalProtect AdminGuide	11	What Client OS Versions are Supported with GlobalProtect?	ok
22.217.3	Atribuição de endereço IP nos clientes remotos de VPN SSL;	GlobalProtect AdminGuide	76	n a gateway agent configuration, select Agent > IP Pools...	ok
22.217.4	Deve permitir a atribuição de IPs fixos nos usuários remotos de VPN SSL;	GlobalProtect AdminGuide	76	static IP addresses, select the Retrieve Framed-IP-Address attribute from authentication server...	ok
22.217.5	Deve permitir a criação de rotas de acesso e faixas de endereços IP atribuídas a clientes remotos de VPN de forma customizada por usuário AD/LDAP e grupo de usuário AD/LDAP;	GlobalProtect AdminGuide	75	Configure the user or user group and the endpoint OS...	ok
22.217.6	Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;	GlobalProtect AdminGuide	73	Enable tunneling and configure the tunnel parameters	ok
22.217.7	Atribuição de DNS nos clientes remotos de VPN;	GlobalProtect AdminGuide	77	anually assign the DNS server(s) and suffix, and WINS	ok
22.217.8	Deve permitir que seja definido métodos de autenticação distintos por sistema operacional do dispositivo remoto de VPN (Android, IOS, Mac e Windows);	GlobalProtect AdminGuide	75	To deliver this configuration to agents or apps running on specific operating system, Add the OS (Android, Chrome, iOS, Mac, Windows, or WindowsUWP) to which this configuration applies	ok
22.217.9	A solução de VPN deve verificar se o client que está conectando é o mesmo para o qual o certificado foi emitido inicialmente. O acesso deve ser bloqueado caso o dispositivo não seja o correto;	GlobalProtect AdminGuide	87	To enable users to authenticate with the portal using client certificates, select the Client Certificate source (SCEP, Local, or None) that distributes the certific	ok
22.217.10	Através do agente, deve possibilitar o bloqueio de dispositivos que forem reportados como roubado ou perdido pelo usuário;	GlobalProtect AdminGuide	190	Block Device Access	ok
22.217.11	Deve haver a opção de ocultar o agente de VPN instalado no cliente remoto, tornando o mesmo invisível para o usuário;	GlobalProtect AdminGuide	94	If you want hide the GlobalProtect agent on end-user systems, set Display GlobalProtect Icon	ok
22.217.12	Deve exibir mensagens de notificação customizada toda vez que um usuário remoto se conectar a VPN. Deve permitir que o usuário desabilite a exibição da mensagem nas conexões seguintes;	GlobalProtect AdminGuide	99	you can create your own custom pages with your corporate branding	ok
22.217.13	Deve avisar ao usuário remoto de VPN quanto a proximidade da expiração de senha LDAP. Deve permitir também a customização da mensagem com informações relevantes para o usuário;	https://www.paloaltonetworks.com/documentation/71/pan-os/new-features/globalprotect-features/customizable-password-expiry-notification-messages			ok
22.217.14	Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;	PAN-OS 8.0 Administrator's Guide	921 / 147	Create a Security Policy Rule / End users authenticate through Captive Portal or GlobalProtect to access various services and applications.	ok
22.217.15	A VPN SSL deve suportar proxy arp e uso de interfaces PPPOE;	PANOS-4.0.1-RN-revA.pdf	5	Proxy ARP Support / VPNs using PPPoE Interfaces	ok
22.217.16	Suportar autenticação via AD/LDAP, OTP (One Time Password), certificado e base de usuários local;	GlobalProtect AdminGuide	27	The user authentication functions are performed by an external LDAP...	ok
22.217.17	Deve permitir a distribuição de certificado para o usuário de remoto através do portal de VPN de forma automatizada;	GlobalProtect AdminGuide	9	any client certificates that may be required to connect to the GlobalProtect	ok
22.217.18	Deve possuir lista de bloqueio para dispositivos em casos quando, por exemplo, o usuário reportar que o dispositivo foi perdido ou roubado;	GlobalProtect AdminGuide	190	Block Device Access	ok
22.217.19	Permite estabelecer um túnel VPN client-to-site do cliente a plataforma de segurança, fornecendo uma solução de single-sign-on aos usuários, integrando-se com as ferramentas de Windows-logon;	GlobalProtect AdminGuide	212	Pre-logon is a connect method that establishes a VPN tunnel before a user logs in	ok
22.217.20	Suporta leitura e verificação de CRL (certificate revocation list);	GlobalProtect AdminGuide	143	If the OCSP or CRL service...	ok
22.217.21	Permite a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;	GlobalProtect AdminGuide	237	Configure all firewalls to use security policies and profiles based on...	ok
22.217.22	O agente de VPN a ser instalado nos equipamentos desktop e laptops, dever ser capaz de ser distribuído de maneira automática via Microsoft SMS, Active Directory e ser descarregado diretamente desde o seu próprio portal, o qual residirá no centralizador de VPN;	GlobalProtect AdminGuide	103	Deploy the GlobalProtect Agent Software	ok
22.217.23	O agente deverá comunicar-se com o portal para determinar as políticas de segurança do usuário,	GlobalProtect AdminGuide	9	The GlobalProtect portal provides the management functions for your GlobalProtect	ok
22.217.24	Deve permitir que a conexão com a VPN SSL seja estabelecida das seguintes formas:	N/A	N/A	N/A	ok
22.217.25	Antes do usuário autenticar na estação;	GlobalProtect AdminGuide	212	Pre-logon is a connect method that establishes a VPN tunnel before a user logs in	ok
22.217.26	Após autenticação do usuário na estação;	GlobalProtect AdminGuide	211	Always On VPN Configuration	ok
22.217.27	Sob demanda do usuário;	GlobalProtect AdminGuide	92	On-demand (Manual user initiated connection	ok
22.217.28	Deverá manter uma conexão segura com o portal durante a sessão.	GlobalProtect AdminGuide	9	GlobalProtect Portal	ok
22.217.29	O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows XP, Vista Windows 7, Windows 8 e Mac OSx;	GlobalProtect AdminGuide	11	What Client OS Versions are Supported with GlobalProtect?	ok
22.217.30	O cliente de VPN SSL cliente-to-site também deve suportar dispositivos móveis (IOS e ANDROID);	GlobalProtect AdminGuide	9	The GlobalProtect App	ok
22.217.31	Deve possuir mecanismos de checagem de conformidade do dispositivo remoto;	GlobalProtect AdminGuide	176	...HIP matches for hosts that are in compliance with a particular state...	ok
22.217.32	A checagem de conformidade deve permitir verificar, no mínimo, as seguintes informações no cliente remoto: sistema operacional e patches instalados, antivírus e versão instalada, firewall no host, criptografia do disco, agente de DLP instalado, backup de disco, chaves de registros e processos ativos;	GlobalProtect Datasheet	2	Host Information Profile	ok
22.217.33	Deve ser possível a criação de perfis customizados de conformidade com, no mínimo, as seguintes opções: sistema operacional e patches instalados, antivírus e versão instalada, firewall no host, criptografia do disco, agente de DLP instalado backup de disco, chaves de registros e processos ativos;	GlobalProtect AdminGuide	177 a 183	Configure HIP-Based Policy Enforcement	ok
22.217.34	O portal de VPN deve enviar ao cliente remoto, a lista de gateways de VPN ativos para estabelecimento da conexão, os quais devem poder ser administrados centralmente;	GlobalProtect AdminGuide	9	GlobalProtect network receives configuration information from the portal, including information about available gateways...	ok
22.217.35	Deve haver a opção do cliente remoto escolher manualmente o gateway de VPN e de forma automática através da melhor rota entre os gateways disponíveis com base no tempo de resposta mais rápido;	GlobalProtect AdminGuide	86	he configuration can include the following...	ok
22.217.36	Deve possuir a capacidade de identificar se a origem da conexão de VPN é externa ou interna;	GlobalProtect AdminGuide	68	Types of Gateways	ok
	CONSOLE DE GERÊNCIA E MONITORAÇÃO				ok
22.218	O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;	PAN-OS 8.0 Administrator's Guide	53	Management Interfaces	ok

22.219	Deve permitir substituir o certificado de fábrica no acesso HTTPS a gerência do firewall como possibilidade de uso de certificado criado localmente na própria solução ou importado de fonte externa;	PAN-OS 8.0 Administrator's Guide	72	Configure Certificate-Based Administrator Authentication to the Web Interface	ok
22.220	Caso haja a necessidade de instalação de cliente para administração da solução o mesmo deve ser compatível com sistemas operacionais Windows e Linux;	PAN-OS 8.0 Administrator's Guide	54	Launch the Web Interface	ok
22.221	O gerenciamento deve permitir/possuir;	N/A	N/A	N/A	ok
22.221.1	Criação e administração de políticas de firewall e controle de aplicação;	PAN-OS 8.0 Web Interface Reference	95 a 112	Policy Types	ok
22.221.2	Criação e administração de políticas de IPS, Antivírus e Anti-Spyware;	PAN-OS 8.0 Web Interface Reference	183 a 216	Objects > Security Profiles	ok
22.221.3	Criação e administração de políticas de Filtro de URL;	PAN-OS 8.0 Web Interface Reference	195 a 200	Objects > Security Profiles > URL Filtering	ok
22.221.4	Monitoração de logs;	PAN-OS 8.0 Web Interface Reference	57 a 92	Monitor > Logs	ok
22.221.5	Ferramentas de investigação de logs;	PAN-OS 8.0 Administrator's Guide	331	Filter Logs	ok
22.221.6	Debugging;	CLI Commands	33	CLI debug mode	ok
22.221.7	Captura de pacotes.	PAN-OS 8.0 Web Interface Reference	67 a 71	Monitor > Packet Capture	ok
22.222	Acesso concorrente de administradores;	PAN-OS 8.0 Web Interface Reference	33	To help you coordinate configuration tasks with other firewall administrators during concurrent login sessions	ok
22.223	Deve permitir que administradores concorrentes façam modificações, valide configurações e reverta configurações do firewall simultaneamente e que cada administrador consiga aplicar apenas as suas alterações de forma independente das realizadas por outro administrador;	PAN-OS 8.0 Administrator's Guide	58-60	Commit, Validate, and Preview Firewall Configuration Changes	ok
22.224	Deve mostrar ao administrador do firewall a hora e data do último login e tentativas de login com falha para acessos a partir da interface gráfica e CLI.	PAN-OS 8.0 Administrator's Guide	56	Use the Administrator Login Activity Indicators to Detect Account Misuse	ok
22.225	Deve possuir mecanismo busca global na solução onde possa se consultar por uma string tais como: nome de objetos, ID ou nome de ameaças, nome de aplicações, nome de políticas, endereços IPs, permitindo a localização e uso dos mesmo na configuração do dispositivo;	PAN-OS 8.0 Web Interface Reference	35	Global Find	ok
22.226	Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;	CLI Commands	12 a 16	Find a Command	ok
22.227	Deve permitir usar palavras chaves e cores para facilitar identificação de regras;	PAN-OS 8.0 Web Interface Reference	165 a 168	Objects > Tags	ok
22.228	Deve permitir monitorar via SNMP falhas de hardware, inserção ou remoção de fontes, discos e coolers, uso de recursos por número elevado de sessões, número de túneis estabelecidos na VPN cliente-to-site, porcentagem de utilização em referência ao número total suportado/licenciado e número de sessões estabelecidas, estatísticas/taxa de logs, uso de disco, período de retenção dos logs e status do envio de logs para soluções externas;	PAN-OS 8.0 Administrator's Guide	390	SNMP Monitoring and Traps	ok
22.229	Deve suportar também o monitoramento dos seguintes recursos via SNMP: IP fragmentation, TCP state e dropped packets;	PAN-OS-7.0-RN.pdf	6	Extended SNMP Support	ok
22.230	Bloqueio de alterações, no caso acesso simultâneo de dois ou mais administradores;	PAN-OS 8.0 Administrator's Guide	61-62	Manage Locks for Restricting Configuration Changes	ok
22.231	Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;	PAN-OS 8.0 Web Interface Reference	453 e 454	Device > Admin Roles	ok
22.232	Autenticação integrada ao Microsoft Active Directory e servidor Radius;	PAN-OS 8.0 Administrator's Guide	152 e 153 e 421	(152 e 153 Radius) (421 The firewall supports a variety of directory servers, including Microsoft Active Directory ...)	ok
22.233	Localização de em quais regras um endereço IP, IP Range, subnet ou objetos estão sendo utilizados;	PAN-OS 8.0 Web Interface Reference	35	Global Find enables you to search the candidate configuration on a firewall or on Panorama for a particular string...	ok
22.234	Deve atribuir sequencialmente um número a cada regra de firewall, NAT, QOS e regras de DOS;	PAN-OS 8.0 Administrator's Guide	917 e 959	917 - Policy Types 959 - Enumeration of Rules Within a Rulebase	ok
22.235	Criação de regras que fiquem ativas em horário definido;	PAN-OS 8.0 Web Interface Reference	227	Objects > Schedules	ok
22.236	Criação de regras com data de expiração;	PAN-OS 8.0 Web Interface Reference	227	Objects > Schedules Non-recurring	ok
22.237	Backup das configurações e rollback de configuração para a última configuração salva;	PAN-OS 8.0 Administrator's Guide	63 a 66	63 - Manage Configuration Backups Revert Firewall Configuration Changes 64 - Revert Firewall Configuration Changes	ok
22.238	Suportar Rollback de Sistema Operacional para a ultima versão local;	PAN-OS 8.0 Web Interface Reference	525	Select Device > Software to view the available software releases...	ok
22.239	Habilidade de upgrade via SCP, TFTP e interface de gerenciamento;	https://live.paloaltonetworks.com/t5/Management-Articles/How-to-Manually-Import-and-Install-PAN-OS-from-the-CLI/ta-p/58646			ok
22.240	Deve possuir mecanismo de análise de impacto na política de segurança antes de atualizar a base com novas aplicações disponibilizadas pelo fabricante;	PAN-OS 8.0 Administrator's Guide	481 a 485	Manage New App-IDs Introduced in Content Releases	ok
22.241	Validação de regras antes da aplicação;	PAN-OS 8.0 Administrator's Guide	58 a 60	Commit, Validate, and Preview Firewall Configuration Changes --- When you initiate a commit, the firewall checks the validity of the changes before activating them...	ok
22.242	Deve implementar mecanismo de validação de configurações antes da aplicação das mesmas permitindo identificar erros, tais como: rota de destino inválida, regras em shadowing etc.	PAN-OS 8.0 Administrator's Guide	59	When you initiate a commit, the firewall checks the validity of the changes before activating them	ok
22.242.1	É permitido o uso de appliance externo para permitir a validação de regras antes da aplicação.	Não é necessário Appliance Externo	N/A	N/A	ok
22.242.2	Validação da políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);	PAN-OS 8.0 Web Interface Reference	23	warnings that a commit would display, including rule shadowing and application dependency warnings	ok
22.242.3	É permitido o uso de appliance externo para permitir a validação de políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);	Não é necessário Appliance Externo	N/A	N/A	ok
22.243	Deve possibilitar a visualização e comparação de configurações Atuais, configuração anterior e configurações antigas.	PAN-OS 8.0 Web Interface Reference	448	Device > Config Audit	ok
22.244	Deve possibilitar a integração com outras soluções de SIEM de mercado (third-party SIEM vendors)	PAN-OS 8.0 Administrator's Guide	356	Use Syslog for Monitoring	ok
22.245	Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;	PAN-OS 8.0 Administrator's Guide	328	Config Logs	ok
22.246	Deverá ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado;	PAN-OS 8.0 Web Interface Reference	73	App Scope Change Monitor Report	ok
22.247	Geração de relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego gerado na instituição;	PAN-OS 8.0 Administrator's Guide	305	Threat Map Report	ok
22.248	Deve prover relatórios com visão correlacionada de aplicações, ameaças (IPS, Antivírus e Anti-Spware), URLs e filtro de arquivos, para melhor diagnóstico e resposta a incidentes;	PAN-OS 8.0 Administrator's Guide	283 a 286	Use the Application Command Center	ok
22.249	Deve permitir a criação de Dash-Boards customizados para visibilidades do tráfego de aplicativos, usuários, categorias de URL, ameaças identificadas pelo IPS, antivírus, anti-spyware, malwares "Zero Day"detectados em sand-box e tráfego bloqueado;	PAN-OS 8.0 Administrator's Guide	293 a 296	Interact with the ACC	ok
22.250	O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança;	panorama.pdf	3	Traffic Monitoring: Analysis, Reporting and Forensics	ok
22.251	Dever permitir a visualização dos logs de malwares modernos, tráfego (IP de origem, destino, usuário e porta), aplicação, IPS, antivírus, anti-spyware, Filtro de URL e filtro de arquivos em uma única tela.	PAN-OS 8.0 Administrator's Guide	330	Unified Logs	ok
22.252	Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti-Spware), etc;	PAN-OS 8.0 Administrator's Guide			ok
22.253	Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus e Anti-Spware), e URLs que passaram pela solução;	PAN-OS 8.0 Administrator's Guide	337 a 339	Custom Reports (Summary databases—These databases are available for Application Statistics, Traffic, Threat, URL Filtering, and Tunnel Inspection..)	ok
22.254	Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em RealTime;	PAN-OS 8.0 Administrator's Guide	299	To further drill-down into each vulnerability...	ok

22.255	Nas opções de "Drill-Down", ser possível identificar o usuário que fez determinado acesso;	PAN-OS 8.0 Administrator's Guide	299	Then, view the User Activity widget in the Network Activity tab...	ok
22.256	Deve possuir relatório de visibilidade e uso sobre aplicativos (SaaS). O relatório também deve mostrar os riscos para a segurança do ambiente, tais como a entrega de malwares através de aplicativos SaaS com a informação do usuário responsável pelo acesso;	PAN-OS 8.0 Administrator's Guide	342 a 345	Generate the SaaS Application Usage Report	ok
22.257	Os relatórios de visibilidade e uso sobre aplicativos (SaaS) devem poder ser extraídos por grupo de usuários apresentando o uso e consumo de aplicações por grupo de usuário;	PAN-OS 8.0 Administrator's Guide	344	If you want to include specific user groups in the report, select Include user group information in the report and click the manage groups link to select the groups you want to include...	ok
22.258	Deve ser possível exportar os logs em CSV;	PAN-OS 8.0 Administrator's Guide	331 e 332	Export Logs	ok
22.259	Deverá ser possível acessar o equipamento a aplicar configurações durante momentos onde o trafego é muito alto e a CPU e memória do equipamento estiver totalmente utilizada.	Single_Pass_Parallel_Processing_Architecture.pdf	7	Hardware Acceleration	ok
22.260	Rotação do log;				ok
22.261	Deve permitir que os logs e relatórios sejam rotacionados automaticamente baseado no tempo em que estão armazenados na solução, assim como no espaço em disco usado;	PAN-OS 8.0 Administrator's Guide	332	Configure Log Storage Quotas and Expiration Periods	ok
22.262	Deve permitir fazer o envio de logs para soluções externas de forma granular podendo selecionar quais campos dos logs serão enviados incluindo, mas não limitado a: tipo de ameaça, usuário, aplicação, etc;	PAN-OS 8.0 Administrator's Guide	332 e 333	Schedule Log Exports to an SCP or FTP Server	ok
22.263	Exibição das seguintes informações, de forma histórica e em tempo real (atualizado de forma automática e contínua a cada 1 minuto):	PAN-OS 8.0 Web Interface Reference	43 e 44	Dashboard refresh option	ok
22.263.1	Situação do dispositivo e do cluster;	PAN-OS 8.0 Web Interface Reference	43	High Availability	ok
22.263.2	Principais aplicações;	PAN-OS 8.0 Web Interface Reference	43	Top Applications	ok
22.263.3	Principais aplicações por risco;	PAN-OS 8.0 Web Interface Reference	43	Top High Risk Applications	ok
22.263.4	Administradores autenticados na gerência da plataforma de segurança;	PAN-OS 8.0 Web Interface Reference	44	Logged In Admins	ok
22.263.5	Número de sessões simultâneas;	PAN-OS 8.0 Web Interface Reference	44	System Resources	ok
22.263.6	Status das interfaces;	PAN-OS 8.0 Web Interface Reference	44	Interfaces	ok
22.263.7	Uso de CPU;	PAN-OS 8.0 Web Interface Reference	43	System Resources	ok
22.264	Geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:	N/A	N/A	N/A	ok
22.264.1	Resumo gráfico de aplicações utilizadas;	PAN-OS 8.0 Administrator's Guide	283	Use the Application Command Center	ok
22.264.2	Principais aplicações por utilização de largura de banda de entrada e saída;	PAN-OS 8.0 Administrator's Guide	285	ACC Tabs -> Network Activity	ok
22.264.3	Principais aplicações por taxa de transferência de bytes;	PAN-OS 8.0 Administrator's Guide	285	ACC Tabs -> Network Activity	ok
22.264.4	Principais hosts por número de ameaças identificadas;	PAN-OS 8.0 Administrator's Guide	285	ACC Tabs -> Threat Activity	ok
22.264.5	Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti-Spware), de rede vinculadas a este tráfego;	PAN-OS 8.0 Administrator's Guide	288	Widget Descriptions -> User Activity	ok
22.264.6	Deve permitir a criação de relatórios personalizados;	PAN-OS 8.0 Web Interface Reference	90 e 91	Monitor > Manage Custom Reports	ok
22.265	Em cada critério de pesquisa do log deve ser possível incluir múltiplas entradas (ex. 10 redes e IP's distintos; serviços HTTP, HTTPS e SMTP), exceto no campo horário, onde deve ser possível definir um faixa de tempo como critério de pesquisa;	PAN-OS 8.0 Administrator's Guide	331	Filter Logs	ok
22.266	Gerar alertas automáticos via Email, SNMP e Syslog;	PAN-OS 8.0 Administrator's Guide	355, 356 e 390	355 - Configure Email Alerts 356 - Use Syslog for Monitoring 390 - SNMP Monitoring and Traps	ok
22.267	A plataforma de segurança deve permitir através de API-XML (Application Program Interface) a integração com sistemas existentes no ambiente da contratante de forma a possibilitar que aplicações desenvolvidas na contratante possam interagir em RealTime com a solução possibilitando assim que regras e políticas de segurança de possam ser modificadas por estas aplicações com a utilização de scripts em linguagens de programação como Perl ou PHP.	PAN-OS 8.0 API Guide	5	About the PAN-OS XML API	ok
	MÓDULO DE PROTEÇÃO À USUÁRIOS E SERVIDORES CRÍTICOS				ok
23.1	Deverá oferecer proteção de estações de trabalho e/ou servidores de rede no combate a vírus, malware, vulnerabilidades conhecidas e d	Traps_Datasheet.pdf	Página 1	Traps secures endpoints with..	ok
23.2	A solução deve ser expansível podendo:				ok
23.2.1	Aumentar sua capacidade de tratamento de tráfego com adição de novas de licenças;	De acordo com especificações do edital/proposta comercial	N/A	N/A	ok
23.2.2	A quantidade mínima, para aquisição, deverá ser de 200 (duzentas) licenças para estações de trabalho ou 50 (cinquenta) licenças para servidores.	De acordo com especificações do edital/proposta comercial	N/A	N/A	ok
23.3.	As funcionalidades de proteção que compõe a solução de segurança, podem funcionar em múltiplos equipamentos e/ou softwares desde que obedeçam a todos os requisitos desta especificação;	De acordo com especificações do edital/proposta comercial	N/A	N/A	ok
23.4.	A solução deverá proporcionar capacidade de gestão centralizada de políticas, logs e relatórios;	Traps Administrator's Guide.pdf	Páginas 13, 231 e 233	ESM Console Reports and Logging	ok
	FUNCIONALIDADES DE GERENCIAMENTO				ok
23.5.	A solução proposta deve ser gerenciada a partir de console única do tipo Interface Gráfica de Usuário (GUI) baseada na Web ou cliente;	Traps Administrator's Guide.pdf	Página 13	ESM Console	ok
23.6.	Caso a administração da solução seja via cliente deverá ser compatível com, no mínimo, os sistemas operacionais Windows e Linux;	Administração não é via cliente, é via WEB	N/A	N/A	ok
23.7.	Caso a administração da solução seja via browser deverá ser compatível com, no mínimo, Firefox, Chrome e Internet Explorer;	Traps Administrator's Guide.pdf	Página 35	Browser, any of the following:	ok
23.8.	A solução proposta deverá ter uma arquitetura de gerenciamento multicamadas que consista de Console de Gerenciamento, binários ou serviços e Banco de Dados. A solução deve fornecer opção para instalar os três componentes em um único hardware ou implementações distribuídas de acordo com a necessidade de escalabilidade do parque de máquinas protegidas;	Traps Administrator's Guide.pdf	Página 13	ESM Console	ok
23.9.	Caso a solução necessite de Banco de Dados (Ex. SQL Server Enterprise), deverão estar inclusas em sua proposta as licenças necessárias para pleno funcionamento;	De acordo com especificações do edital/proposta comercial	N/A	N/A	ok
23.10.	A solução proposta deve ser capaz de instalar vários servidores de gerenciamento para implantações distribuídas e ainda ser gerenciada por uma única console web centralizada;	Traps Administrator's Guide.pdf	Página 24	Large Single-Site Deployment	ok
23.11.	A solução proposta deve permitir implementação em ambiente virtual sendo, no mínimo, compatível com VMware;	Traps Matrix.pdf	Página 88	Virtual Desktop Operating Systems Supported with Traps	ok
23.12.	O servidor de gerenciamento deverá possuir compatibilidade para instalação nos sistemas operacionais Microsoft Windows Server 2003 R2, SP1 ou superior e Microsoft Windows Server 2008, 2008 R2 ou superior;	Traps Matrix.pdf	Página 85	Tabela	ok
23.13.	Mecanismo de comunicação randômico (via pull) em tempo determinado pelo administrador entre o cliente e servidor, para consulta de novas configurações e assinaturas evitando sobrecarga de rede e servidor;	Traps Administrator's Guide.pdf	Página 14	Tabela: Traps status	ok
23.14.	Integração completa ao serviço de diretórios Active Directory (AD), da Microsoft;	Traps Administrator's Guide.pdf	Página 89	Manage Administrator Access to the ESM Console	ok
23.15.	Possibilidade de agrupamento, com base nos objetos do AD, das estações de trabalho e servidores, e definição de políticas por grupos;	Traps Administrator's Guide.pdf	Página 128	Target Objects	ok
23.16.	Permitir a divisão lógica dos computadores, dentro da estrutura de gerenciamento, em sites, domínios e grupos, com administração individualizada por domínio;	Traps Administrator's Guide.pdf	Página 128	Target Objects	ok
23.17.	O módulo de gestão da solução deve permitir autenticação integrada ao Active Directory;	Traps Administrator's Guide.pdf	Página 89	Manage Administrator Access to the ESM Console	ok
23.18.	Deve permitir a criação de, no mínimo, três perfis de acesso distintos para os usuários administradores da solução;	Traps Administrator's Guide.pdf	Página 89	Administrative Roles	ok
23.19.	Deve registrar nos logs as alterações realizadas pelos administradores na solução;	Traps Administrator's Guide.pdf	Páginas 234 e 235	Policies - Rules / Process Management / Restrction Settings	ok
23.20.	A solução proposta deve ser capaz de exportar seus logs no formato syslog para outras soluções de gerenciamento de logs;	Traps Administrator's Guide.pdf	Página 15	External Logging Platform	ok

23.21.	Instalação e atualização do software sem a intervenção do usuário;	Traps Administrator's Guide.pdf	Páginas 54 e 200	Traps Installation Options: Install using na action rule / Uninstall or Upgrade Traps on the Endpoint	ok
23.22.	Deve permitir integração com soluções de SIEM enviando logs no formato Syslog ou compatível;	Traps Administrator's Guide.pdf	Página 15	External Logging Platform	ok
23.23.	Deve permitir notificar eventos ao administrador por e-mail;	Traps Administrator's Guide.pdf	Página 301	Forward Logs to Email	ok
23.24.	Deve permitir a criação de políticas para controle de Vulnerabilidades, Malwares e Restrições de execução por diretório;	Traps Administrator's Guide.pdf	Página 121	Policy Rule Types	ok
23.25.	Log centralizado dos eventos de segurança detectados nos endpoints;	Traps Administrator's Guide.pdf	Páginas 15, 242 e 243	External Logging Platform / Settings - Agent	ok
23.26.	Deve identificar e gerar log de qualquer interferência no serviço de endpoint na máquina afetada, como por exemplo:				ok
23.26.1.	Tentativa de shutdown do processo de endpoint;	Traps Administrator's Guide.pdf	Páginas 14 e 15	Traps Agent: Message type Table	ok
23.26.2.	Tentativa de shutdown do serviço de endpoint;	Traps Administrator's Guide.pdf	Páginas 14 e 15	Traps Agent: Message type Table	ok
23.26.3.	Logs de sistema relacionados.	Traps Administrator's Guide.pdf	Páginas 14 e 15	Traps Agent: Message type Table	ok
23.27.	A solução proposta deve permitir o ajuste das políticas forenses dentro do servidor de gerenciamento centralizado com granularidade para definição do tipo de informações forenses a serem coletadas quando ocorrer uma ameaça;	Traps Administrator's Guide.pdf	Páginas 16, 17 e 117	Forensics Folder / Monitor Forensics Retrieval	ok
23.28.	Deve suportar e possuir agente para pelo menos os seguintes sistemas operacionais:				ok
23.28.1.	Windows XP (32-bit e/ou 64-bit, SP3 ou posterior);	Traps Matrix.pdf	Páginas 86, 87 e 88	Endpoint Operating Systems Supported with Traps	ok
23.28.2.	Windows 7 (32-bit, 64-bit, RTM e SP1);	Traps Matrix.pdf	Páginas 86, 87 e 88	Endpoint Operating Systems Supported with Traps	ok
23.28.3.	Windows 8 (32-bit e 64-bit);	Traps Matrix.pdf	Páginas 86, 87 e 88	Endpoint Operating Systems Supported with Traps	ok
23.28.4.	Windows 8.1 (32-bit e 64-bit);	Traps Matrix.pdf	Páginas 86, 87 e 88	Endpoint Operating Systems Supported with Traps	ok
23.28.5.	Windows Server 2003 (32-bit e SP2 ou posterior);	Traps Matrix.pdf	Páginas 86, 87 e 88	Endpoint Operating Systems Supported with Traps	ok
23.28.6.	Windows Server 2003 R2 (32-bit, SP2 ou posterior);	Traps Matrix.pdf	Páginas 86, 87 e 88	Endpoint Operating Systems Supported with Traps	ok
23.28.7.	Windows Server 2008 (32-bit e 64-bit);	Traps Matrix.pdf	Páginas 86, 87 e 88	Endpoint Operating Systems Supported with Traps	ok
23.28.8.	Windows Server 2012 (todas as versões);	Traps Matrix.pdf	Páginas 86, 87 e 88	Endpoint Operating Systems Supported with Traps	ok
23.28.9.	Windows Server 2012 R2 (todas as versões);	Traps Matrix.pdf	Páginas 86, 87 e 88	Endpoint Operating Systems Supported with Traps	ok
23.28.10.	Windows Vista (32-bit, 64-bit e SP2);	Traps Matrix.pdf	Páginas 86, 87 e 88	Endpoint Operating Systems Supported with Traps	ok
23.28.11.	Windows 10 RTM (32-bit e 64-bit)	Traps Matrix.pdf	Páginas 86, 87 e 88	Endpoint Operating Systems Supported with Traps	ok
23.29.	Deve suportar e possuir agente para maquinas virtuais instaladas em pelo menos:				ok
23.29.1.1.	Citrix Xenserver;	Traps Matrix.pdf	Página 88	Virtual Desktop Operating Systems Supported with Traps	ok
23.29.2.2.	Vmware ESX;	Traps Matrix.pdf	Página 88	Virtual Desktop Operating Systems Supported with Traps	ok
23.30.	Proteção contra desinstalação não autorizada dos agentes de endpoint que compõem a solução;	Traps Administrator's Guide.pdf	Página 59	Uninstall Traps Components: You must specify the UNISNTALL_PASSWORD	ok
23.31.	Proteção contra a desativação não autorizada dos serviços que compõem a solução;	Traps Administrator's Guide.pdf	Página 209	Manage Agent Tampering Protection	ok
23.32.	Ser eficaz na prevenção de Vulnerabilidades e Malwares mesmo quando estiver sem conectividade com servidores de gerenciamento e/ou recursos baseados em nuvem;	Traps tech nology overview.pdf	Página 2	Multi-Method Prevention: Figure 1	ok
23.33.	O agente de endpoint deve continuar funcionando a aplicando políticas de controle mesmo se houver interrupção da comunicação com o gerenciamento centralizado;	Traps technology overview.pdf	Página 2	Multi-Method Prevention: Figure 1	ok
23.34.	Impedir executável malicioso, sem requerer nenhum conhecimento prévio do artefato;	Traps_Datasheet.pdf	Páginas 1 e 2		ok
23.35.	Possibilidade de colocar arquivos, diretórios e processos em listas de exclusões para não serem verificados pela proteção em tempo real;	Traps Administrator's Guide.pdf	Páginas 156, 158 e 159	Manage Global Whitelist / Whitelist a Network Folder	ok
23.36.	Possuir funcionalidades que permitam o isolamento (área de quarentena) de arquivos contaminados por códigos maliciosos que não sejam conhecidos ou que não possam ser reparados em um servidor central da rede;	Traps Administrator's Guide.pdf	Página 16 e 182	Forensic Folder e Manage Quarantine Settings	ok
23.37.	A solução proposta deve permitir implementação em modo de monitoramento ou aprendizado do ambiente em fase inicial de instalação;	Traps Administrator's Guide.pdf	Página 53	Recommended Traps Deployment Process	ok
23.38.	A solução proposta não deve utilizar intensivamente os recursos de hardware do endpoint, ou seja, não mais que 1% de CPU e não mais que 70 Mega Bytes de memória RAM;	protect yourself from antivirus.pdf	Página 59	Traps Replces Antivirus	ok
23.39.	A solução proposta deve fornecer a capacidade de configurar listas brancas globais para permitir que determinados arquivos executáveis sejam executados dentro de determinadas condições da instituição;	Traps Administrator's Guide.pdf	Página 156	Manage Global Whitelist	ok
23.40.	A solução proposta deve ter a capacidade de criar a partir de incidentes, uma regra de exceção para permitir que um processo seja executado em um determinado endpoint;	Traps Administrator's Guide.pdf	Página 106	Manage Security Events	ok
	CARACTERÍSTICA DE PROTEÇÃO CONTRA VULNERABILIDADES				ok
23.41.	A solução proposta deve suportar a proteção de processo e aplicativos em execução no sistema operacional;	Traps Administrator's Guide.pdf	Página 187	Exploit Protection Rules: To protect processes and additional applications that are important to your organization	ok
23.42.	A solução proposta deve suportar a adição de aplicações proprietárias e personalizadas a lista de aplicações protegidas;	Traps Administrator's Guide.pdf	Página 187	Exploit Protection Rules: To protect processes and additional applications that are important to your organization	ok
23.43.	A solução proposta deve ser capaz de fornecer prevenção em tempo real contra exploração de vulnerabilidades de aplicações, bloqueando em tempo real a exploração, não limitadas a falhas de lógica de software, corrupção de memória, sequestro de DLL, etc.;	Traps Administrator's Guide.pdf	Páginas 187, 188 e 189	Exploit Protection Rules / Windows Exploit Protection Modules (EPMs)	ok
23.44.	A solução proposta deve ser capaz de proteger contra explorações de quaisquer vulnerabilidades não descobertas (desconhecidas) dos aplicativos através do bloqueio de métodos (técnicas e subtécnicas) utilizados para exploração;	Traps Administrator's Guide.pdf	Páginas 187, 188 e 189	Exploit Protection Rules / Windows Exploit Protection Modules (EPMs)	ok
23.45.	Ao impedir ou bloquear uma técnica de exploração, a solução proposta deve congelar o processo, coletar informações forenses, de no mínimo, nome do processo, origem e caminho do arquivo, data/hora, dump de memória, versão do SO, usuário, versão vulnerável do aplicativo;	Traps Administrator's Guide.pdf	Página 187	Exploit Protection Rules: To protect processes and additional applications that are important to your organization	ok
23.46.	Ao impedir ou bloquear uma técnica de exploração, a solução proposta deve finalizar apenas o processo específico alvo do ataque;	Traps Administrator's Guide.pdf	Página 187	When a security event triggers a prevention, the Traps agent also takes a snapshot of the memory for subsequent forensic investigation.	ok
23.47.	A solução proposta deve utilizar módulos de métodos de exploração para prevenir ou bloquear tentativas de exploração. Os módulos de métodos de exploração devem proteger aplicações conhecidas, bem como aplicações desconhecidas e desenvolvidas internamente pela instituição;	Traps Administrator's Guide.pdf	Páginas 187, 188 e 189	Exploit Protection Rules / Windows Exploit Protection Modules (EPMs)	ok
23.48.	A solução proposta deve ser capaz de criar regras de exclusão para excluir endpoints específicos e processos específicos do log de eventos de ameaças de segurança do console de gerenciamento de solução proposta;	Traps Administrator's Guide.pdf	Página 194	Exclude an Endpoint from an Exploit Protection Rule	ok
23.49.	Suportar detecção e bloqueio de, no mínimo, os seguintes métodos:				ok
23.49.1.	Deve ser capaz de impedir execução de dados na memória;	Traps Administrator's Guide.pdf	Página 188	Windows Exploit Protection Modules (EPMs)	ok
23.49.2.	Deve ser capaz de impedir acessos não autorizados a DLLs do sistema;	Traps Administrator's Guide.pdf	Página 188	Windows Exploit Protection Modules (EPMs)	ok

23.49.3.	Deve prevenir utilização de DLLs protegidas com fim de ganhar controle de processos e carregar arquivos CPL (painel de controle) maliciosos;	Traps Administrator's Guide.pdf	Página 188	Windows Exploit Protection Modules (EPMs)	ok
23.49.4.	Deve ser capaz de interromper a ocorrência de heap sprays após detecção de exceções suspeitas ou indicativos de tentativas de exploração no host monitorado;	Traps Administrator's Guide.pdf	Página 188	Windows Exploit Protection Modules (EPMs)	ok
23.49.5.	Deve ser capaz de prevenir processamento incorreto de fontes de texto em documentos e arquivos, técnica comum de exploração de processadores de texto;	Traps Administrator's Guide.pdf	Página 188	Windows Exploit Protection Modules (EPMs)	ok
23.49.6.	Deve ser capaz de prevenir processamento incorreto de fontes de texto em documentos e arquivos, técnica comum de exploração de processadores de texto;	Traps Administrator's Guide.pdf	Página 188	Windows Exploit Protection Modules (EPMs)	ok
23.49.7.	Deve ser capaz de prevenir o acionamento de vulnerabilidades que resultem na corrupção da área heap na memoria. Exemplo: "free() double";	Traps Administrator's Guide.pdf	Página 188	Windows Exploit Protection Modules (EPMs)	ok
23.49.8.	Deve prevenir o uso de novas técnicas que possam evadir o DEP (prevenção de execução de dados em memória) e ASLR (randomização do layout de endereçamento em memória);	Traps Administrator's Guide.pdf	Página 188	Windows Exploit Protection Modules (EPMs)	ok
23.49.9.	Deve obrigar a realocação de módulos do sistema operacional, protegendo-os de tentativas de exploração;	Traps Administrator's Guide.pdf	Página 188	Windows Exploit Protection Modules (EPMs)	ok
23.49.10.	Deve ser capaz de detectar e prevenir instâncias de heap spray usando algoritmo de detecção de aumento de consumo de memória, indicando execução de exploração de vulnerabilidade;	Traps Administrator's Guide.pdf	Página 188	Windows Exploit Protection Modules (EPMs)	ok
23.49.11.	Deve ser capaz de prevenir mapeamento de código no endereço zero (início da memória) do espaço de memória do sistema operacional, dessa forma impedindo uso de explorações de referência nula para execução de código arbitrário, exposição de informações de debug, etc;	Traps Administrator's Guide.pdf	Página 188	Windows Exploit Protection Modules (EPMs)	ok
23.49.12.	Deve ser capaz de proteger o acesso a meta dados de bibliotecas críticas do sistema operacional quando estas são descompactadas em memória;	Traps Administrator's Guide.pdf	Página 188	Windows Exploit Protection Modules (EPMs)	ok
23.49.13.	Deve ser capaz de agir preventivamente contra heap spray ao checar periodicamente a zona .heap da memória virtual;	Traps Administrator's Guide.pdf	Página 188	Windows Exploit Protection Modules (EPMs)	ok
23.49.14.	Deve ser capaz de prevenir a exploração de vulnerabilidade bem- sucedida através da pré-alocação aleatória do layout de memória de processos no sistema operacional;	Traps Administrator's Guide.pdf	Página 188	Windows Exploit Protection Modules (EPMs)	ok
23.49.15.	Deve ser capaz de prevenir uso de programação orientada a retorno (return oriented programming) protegendo APIs (interface de programação de aplicação) usadas em cadeias de ROP e técnicas de exploração usando compilações "Just-in-time" (JIT);	Traps Administrator's Guide.pdf	Página 188	Windows Exploit Protection Modules (EPMs)	ok
23.49.16.	Deve ser capaz de mitigar o abuso e captura das estruturas de gerenciamento de exceções (SEH) em memória, e dessa forma impedindo execução de código malicioso arbitrário no sistema operacional;	Traps Administrator's Guide.pdf	Página 188	Windows Exploit Protection Modules (EPMs)	ok
23.49.17.	Deve ser capaz de reservar e proteger determinadas áreas da memória comumente utilizadas para armazenamento de cargas (payload) e instruções maliciosas usando técnicas como heap spray, por exemplo;	Traps Administrator's Guide.pdf	Página 188	Windows Exploit Protection Modules (EPMs)	ok
23.49.18.	Deve ser capaz de prevenir vulnerabilidades lógicas na estrutura de atalhos (links) de sistemas operacionais Windows, onde o carregamento impróprio de atalhos permite execução arbitrária de código em memória (exemplo: CVE-2015-0096);	Traps Administrator's Guide.pdf	Página 188	Windows Exploit Protection Modules (EPMs)	ok
23.49.19.	Deve ser capaz de prevenir contra vulnerabilidades utilizadas em ataques de escalação de privilégios no sistema operacional explorando a instrução sys.exit para retornar ao nível de execução de usuário, após execução de código em nível de sistema (privilege level 0);	Traps Administrator's Guide.pdf	Página 188	Windows Exploit Protection Modules (EPMs)	ok
23.49.20.	Deve ser capaz de aprimorar ou implementar a randomização do layout de endereços em memória (ASLR), garantindo maior aleatoriedade e robustez. Deve também ser capaz de tornar obrigatório o uso da função ASLR;	Traps Administrator's Guide.pdf	Página 188	Windows Exploit Protection Modules (EPMs)	ok
	CARACTERÍSTICA DE PROTEÇÃO CONTRA MALWARE				ok
23.50.	A solução proposta deve suportar a proteção contra a execução de arquivos maliciosos;	Traps Administrator's Guide.pdf	Página 149	Manage Malware Protection Rules	ok
23.51.	A solução proposta deve fornecer a capacidade de fazer controle e restringir os parâmetros sobre como executáveis podem rodar incluindo proteção contra criação de processos filhos;	Traps Administrator's Guide.pdf	Página 149	Malware Protection Rules	ok
23.52.	A solução proposta deve ser capaz de fornecer prevenção contra malware desconhecido usando análise dinâmica em ambiente de sandbox. Além disso, deve fornecer veredito com relatório de análise completa com o resultado da análise em sandbox;	Traps Administrator's Guide.pdf	Página 163	WildFire Integration	ok
23.53.	A solução proposta deve fornecer a capacidade de criar exceções para hash específicos de arquivos analisados em nuvem na solução de sandbox;	Traps Administrator's Guide.pdf	Página 147	Administrative Hash Control Policy	ok
23.54.	A solução proposta deve fornecer a capacidade de impedir a execução de um arquivo quando seu valor de hash for desconhecido pela solução de sandbox do fabricante;	Traps Administrator's Guide.pdf	Página 147	Administrative Hash Control Policy	ok
23.55.	A solução proposta deve fornecer a capacidade de impedir a execução de um arquivo quando o hash do arquivo for desconhecido por cache local e o mesmo não tiver comunicação com o servidor de gerência;	Traps Administrator's Guide.pdf	Página 148	Local Static Analysis	ok
23.56.	Caso um malware seja detectado, deve ser possível o envio do mesmo para quarentena automaticamente através de política pré-definida na gerência centralizada;	Traps Administrator's Guide.pdf	Página 182	Manage Quarantine Settings	ok
23.57.	Capacidade de procurar códigos maliciosos pelo tipo real de arquivo e não apenas por sua extensão;	Traps Administrator's Guide.pdf	Página 164	File Type Analysis	ok
23.58.	Deve extrair o hash de arquivos executáveis e verificar se o mesmo já foi analisado na solução de sand-box do fabricante de forma automática sem necessidade de scprits externos ou adaptações não nativas da solução. Caso o malware já tenha apresentado comportamento malicioso em sandbox, o mesmo deve ser impedido de ser executado no endpoint;	Traps Administrator's Guide.pdf	página 146	Malware Protection Flow	ok
23.59.	Deve permitir o administrador reportar falsos positivos na análise de malwares em sandbox. A solução deve informar o administrador o resultado desta análise e exibir a correção na gerência da solução;	Traps Administrator's Guide.pdf	Página 181	Report an Incorrect Verdict	ok
23.60.	Deve avisar o usuário quando a execução de um arquivo for bloqueada incluindo casos quando não houver veredito da sandbox sobre o arquivo e o seu status estiver definido como desconhecido;	Traps Administrator's Guide.pdf	Página 167 e 168	Configure a WildFire Rule: Step 5	ok
23.61.	Possibilitar o bloqueio automático de malwares já descobertos através da sandbox do fabricante em outros endpoints/localidades do órgão;	Traps Administrator's Guide.pdf	Página 163	Verdicts: Malware	ok
23.62.	Restringir execução de arquivos específicos somente em diretórios conhecidos e protegidos, tanto na maquina local quanto em drives remotos.	Traps Administrator's Guide.pdf	página 154	Restriction Rules	ok
23.62.1.	Prevenir execução de arquivos não assinados.	Traps Administrator's Guide.pdf	Página 147	Trusted Signers	ok
23.62.2.	Prevenir execução de arquivos em mídia externa.	Traps Administrator's Guide.pdf	Páginas 159 e 160	Define External Media Restrictions	ok
23.62.3.	Controlar executáveis não assinados por WhiteLists.	Traps Administrator's Guide.pdf	Página 156	Manage Global Whitelists	ok
23.62.4.	Restringir a execução de processos.	Traps Administrator's Guide.pdf	Página 154	Manage Restrictions on Executable Files	ok
23.62.5.	Controlar e limitar a criação de processos filhos.	Traps Administrator's Guide.pdf	Páginas 160 e 161	Define Child Process Restrictions	ok
23.62.6.	Deve possibilitar o controle de arquivos:				ok
23.62.7.	Conhecidos	Traps Administrator's Guide.pdf	Página 13	Local Analysis of Unknown Executable Files	ok
23.62.8.	Desconhecidos	Traps Administrator's Guide.pdf	Página 14	Trusted Signers	ok
23.63.	Suporte a submissão de arquivos executáveis desconhecidos para análise em sandbox do fabricante automaticamente caso o arquivo não seja conhecido.	Traps Administrator's Guide.pdf	Páginas 181 e 182	Upload a File to WildFire for Analysis	ok
23.64.	Definir e classificar Hash conhecidos.	Traps Administrator's Guide.pdf	Página 171	Manage Hashes for Files	ok
	CARACTERÍSTICA DE COLETA DE INFORMAÇÕES FORENSE				ok
23.65.	A solução proposta deve apresentar na gerência centralizada dados forenses capturados pelo agente de endpoint;	Traps Administrator's Guide.pdf	Páginas 117	Monitor Forensics Retrieval	ok
23.66.	A solução proposta deve coletar, pelo menos, os seguintes dados no endpoint para análise via gerência centralizada:				ok
23.66.1.	Dump de memória;	Traps Administrator's Guide.pdf	Página 218	Forensic Data Types: Table	ok

23.66.2.	Arquivos Acessados;	Trapx Administrator's Guide.pdf	Página 218	Forensic Data Types: Table	ok
23.66.3.	Módulos carregados;	Trapx Administrator's Guide.pdf	Página 218	Forensic Data Types: Table	ok
23.66.4.	URls acessadas;	Trapx Administrator's Guide.pdf	Página 218	Forensic Data Types: Table	ok
23.66.5.	Local de execução do arquivo;	Trapx Administrator's Guide.pdf	Página 106	Manage Security Events: Image	ok
23.66.6.	Tempo de execução;		Página 108	Each security event on the Events tab displays the date and time of the event	ok
23.66.7.	Nome do arquivo;	Trapx Administrator's Guide.pdf	Página 106	Manage Security Events: Image	ok
23.66.8.	HASH do arquivo;	Trapx Administrator's Guide.pdf	Página 106	Manage Security Events: Image	ok
23.66.9.	Nome do usuário relacionado;	Trapx Administrator's Guide.pdf	Página 106	Manage Security Events: Image	ok
23.66.10.	Nome do computador;	Trapx Administrator's Guide.pdf	Página 106	Manage Security Events: Image	ok
23.66.11.	Endereço IP;	Trapx Administrator's Guide.pdf	Página 250	IP address of the endpoint	ok
23.66.12.	Versão de sistema operacional;	Trapx Administrator's Guide.pdf	Página 106	Manage Security Events: Image	ok
23.66.13.	Histórico de arquivo maliciosos;	Trapx Administrator's Guide.pdf	Página 106	Select Security Events > Threats to display a list of threats that have occurred in your network. The default view of the threats page includes all prevention and notification events. The menu on the side of the Threats page also provides links to filtered lists of threats by event (Preventions and Notifications) and also by rule type	ok
	CARACTERÍSTICA DE RELATÓRIOS:				ok
23.67.	A solução proposta deve fornecer uma visualização Web das ameaças;	Trapx Administrator's Guide.pdf	Página 106	Manage Security Events	ok
23.68.	A solução proposta deve suportar exportação no formato CSV dos eventos relacionados a ameaças e ao status do agente de endpoints;	Trapx Administrator's Guide.pdf	Página 106	Export events to a comma separated values (CSV) file.	ok
23.69.	Capacidade de Geração de relatórios, estatísticos e gráficos contendo no mínimo os seguintes tipos pré-definidos:				ok
23.69.1.	As 10 máquinas com maior ocorrência de códigos maliciosos;	Trapx Administrator's Guide.pdf	Página 104	MOST TARGETED COMPUTERS	ok
23.69.2.	Os 10 usuários com maior ocorrência de códigos maliciosos;	Trapx Administrator's Guide.pdf	Página 104	MOST TARGETED USERS	ok
23.69.3.	Localização dos códigos maliciosos;	Trapx Administrator's Guide.pdf	Página 104	MOST TARGETED COMPUTERS	ok
23.69.4.	Sumários das ações realizadas;	Trapx Administrator's Guide.pdf	Página 105	The Security Events Dashboard displays both events where exploit attempts were blocked and events that triggered only notifications.	ok
23.69.5.	Número de infecções detectadas diário, semanal e mensal;	Trapx Administrator's Guide.pdf	Página 105	Use the Security Events Dashboard	ok
23.70.	Códigos maliciosos detectados;	Trapx Administrator's Guide.pdf	Página 106	Select Security Events > Threats to display a list of threats that have occurred in your network. The default view of the threats page includes all prevention and notification events. The menu on the side of the Threats page also provides links to filtered lists of threats by event (Preventions and Notifications) and also by rule type.	ok
23.71.	A solução proposta deverá ter os seguintes dashboards nativos para monitorar a postura de segurança e o status da instituição:				ok
23.71.1.	Relatório de restrição de acesso a arquivos e processos;	Trapx Administrator's Guide.pdf	Páginas 105, 106 e 107	Monitor Security Events	ok
23.71.2.	Técnicas de Malwares utilizadas;	Trapx Administrator's Guide.pdf	Páginas 105, 106 e 107	Monitor Security Events	ok
23.71.3.	Técnicas de exploração utilizadas;	Trapx Administrator's Guide.pdf	Páginas 105, 106 e 107	Monitor Security Events	ok
23.71.4.	Informações Forenses coletadas.	Trapx Administrator's Guide.pdf	Páginas 105, 106 e 107	Monitor Security Events	ok
23.72.	A solução proposta deverá ter os seguintes dashboards de controle para monitorar a situação dos endpoints da intuição:				ok
23.72.1.	Detalhes da saúde dos agentes de endpoints;	Trapx Administrator's Guide.pdf	Página 109	View Endpoint Health Details	ok
23.72.2.	Dashboard de controle do histórico de regras dos endpoints;	Trapx Administrator's Guide.pdf	Página 111	Historic	ok
23.72.3.	Dashboard de Controle da Política de Segurança instalada nos endpoints;	Trapx Administrator's Guide.pdf	Página 111	Active	ok
23.72.4.	Dashboard de controle do histórico de status do serviço do endpoints;	Trapx Administrator's Guide.pdf	Página 104	SERVICE STATUS	ok
	MÓDULO DE INTELIGENCIA NO COMBATE À AMEAÇAS				ok
24.1.	Deverá ser fornecido, no mínimo, 01 (uma) licença de acesso a portal de inteligência no combate a malwares	De acordo com a proposta comercial			ok
24.2.	Deve permitir o time de resposta a incidentes identificar se um artefato malicioso de dia zero encontrado na rede faz parte de alguma campanha específica de malware, se foi visto até o momento somente na rede da instituição e se já foi encontrado em outras indústrias/países globalmente;	ActiveFocus-ds.pdf	1	Outcome-Driven Threat Intelligence, Analytics and Prevention	ok
24.3.	Deve ser possível pesquisar por informações sobre malwares encontrados na rede da instituição através de:	N/A	N/A	N/A	ok
24.3.1.	Hash dos arquivo	ActiveFocus Admin Guide	57 e 58	General Artifacts -> Hash	ok
24.3.2.	Nome do arquivo	ActiveFocus Admin Guide	57 e 58	General Artifacts -> Filename	ok
24.3.3.	Endereço IP de origem	ActiveFocus Admin Guide	57 e 58	General Artifacts -> IP Address	ok
24.3.4.	Endereço IP de destino	ActiveFocus Admin Guide	57 e 58	General Artifacts -> IP Address	ok
24.3.5.	URL	ActiveFocus Admin Guide	57 e 58	General Artifacts -> URL	ok
24.3.6.	Domínio	ActiveFocus Admin Guide	57 e 58	General Artifacts -> Domain	ok
24.3.7.	Aplicação por onde o malware passou	ActiveFocus Admin Guide	60	Session Artifacts -> Application	ok
24.3.8.	Endereço de email remetente ou destinatário do malware	ActiveFocus Admin Guide	60 e 61	Session Artifacts -> Email Recipient Address Session Artifacts -> Email Subject	ok
24.3.9.	User Agent	ActiveFocus Admin Guide	57 e 58	General Artifacts -> User Agent	ok
24.3.10.	Nome da ameaça	ActiveFocus Admin Guide	58	General Artifacts -> Threat Name	ok
24.3.11.	Campanhas específicas de malware	ActiveFocus Admin Guide	94	Tag Class	ok
24.3.12.	O portal de inteligência deve prover as seguintes informações sobre malwares encontrados globalmente:	N/A	N/A	N/A	ok
24.3.13.	Tamanho do arquivo	ActiveFocus Admin Guide	58 a 60	Sample Artifacts -> File Size	ok
24.3.14.	Hash	ActiveFocus Admin Guide	58 a 60	Sample Artifacts -> MD5	ok
24.3.15.	País de origem	ActiveFocus Admin Guide	60 a 62	Session Artifacts -> Source Country	ok
24.3.16.	País de destino	ActiveFocus Admin Guide	60 a 62	Session Artifacts -> Destination Country	ok
24.3.17.	Se o malware descoberto faz parte de alguma campanha específica de ataque	ActiveFocus Admin Guide	57 e 58	General Artifacts -> Tag Class	ok
24.3.18.	Caso o malware faça parte de alguma campanha, deve ser detalhado qual o objetivo da mesma	ActiveFocus Admin Guide	96 a 98	Tag Details	ok
24.3.19.	Tipos de indústria que já foram alvo do malware. Ex: governo, mercado financeiro, tecnologia, etc		61	Industry	ok
24.3.20.	Comportamento malicioso conhecido sobre o malware	ActiveFocus Admin Guide	62 a 64	Analysis Artifacts --> Observed Behavior	ok
24.3.21.	Acesso/Alterações nos registros do sistema operacional ocasionadas pelo artefato malicioso	ActiveFocus Admin Guide	64	Windows Artifacts --> Registry Activity	ok
24.3.22.	Acesso/Alterações nos processo do sistema operacional ocasionadas pelo artefato malicioso	ActiveFocus Admin Guide	62 a 64	Analysis Artifacts --> Process Activity	ok
24.3.23.	Acesso/Alterações em arquivos binário ocasionadas pelo artefato malicioso	ActiveFocus Admin Guide	62 a 64	Analysis Artifacts --> File Activity	ok
24.3.24.	Tentativas de resolução de domínio realizadas pelo artefato malicioso	ActiveFocus Admin Guide	62 a 64	Analysis Artifacts --> DNS Activity	ok
24.3.25.	Tentativas de gets e post realizadas pelo artefato malicioso	ActiveFocus Admin Guide	62 a 64	Analysis Artifacts --> HTTP Activity	ok
24.3.26.	Endereço IP de origem	ActiveFocus Admin Guide	60 a 62	Session Artifacts -> Source IP	ok
24.3.27.	Endereço IP de destino	ActiveFocus Admin Guide	60 a 62	Session Artifacts -> Destination IP	ok
24.3.28.	URL	ActiveFocus Admin Guide	60 a 62	Session Artifacts -> File URL	ok
24.3.29.	Domínio				ok

24.3.30.	Aplicação por onde o malware passou	AutoFocus Admin Guide	60 a 62	Session Artifacts -> Application	ok
24.3.31.	Endereço de email remetente ou destinatário do malware	AutoFocus Admin Guide	60 e 61	Session Artifacts -> Email Recipient Address Session Artifacts -> Email Subject	ok
24.3.32.	User Agent	AutoFocus Admin Guide	57 e 58	General Artifacts -> User Agent	ok
24.3.33.	Nome da ameaça	AutoFocus Admin Guide	58	General Artifacts -> Threat Name	ok
24.3.34.	Deve ser possível pesquisar malwares encontrados somente na rede da instituição, somente na mesma indústria do órgão (governo), e globalmente em todos os clientes do fabricante	AutoFocus Admin Guide	23	Dashboard Overview (My Organization / My Industry / All)	ok
24.3.35.	Relatórios e Dashboard:	AutoFocus Admin Guide	21 a 30	Pag 21 a 30 - AutoFocus Dashboard	ok
24.3.36.	Deve exibir a de tendência diária de malware com a quantidade encontrada por dia;	AutoFocus Admin Guide	136	Malware Session Percentage By Day	ok
24.3.37.	Deve exibir as aplicação que mais trazem malwares para dento da rede da instituição. Ex: Flash, FTP, Navegação WEB pelo Browser, SMTP, HTTP-Proxy, Gmail, etc	AutoFocus Admin Guide	137	Top Applications	ok
24.3.38.	Principais malwares encontrados por quantidade no período selecionado	AutoFocus Admin Guide	136-137	Threat Summary Report Overview	ok
24.3.39.	Feeds de informações do fabricante sobre ataques e campanhas descobertas	autofocus-ds.pdf	2	Unit 42 Threat Intelligence Team	ok
	LOTE 2 – SOLUÇÃO DE PROTEÇÃO DE PERÍMETRO VIRTUAL				ok
26.1.	A solução deverá ser composta por softwares, desde que atendidos todos os requisitos de integração e performance apresentados.	De acordo com especificações do edital/proposta comercial			ok
26.2.	Toda solução deverá ser fornecida e instalada e possuir garantia do fabricante pelo período de 48 (quarenta e oito) meses contra falhas em todos os seus componentes	De acordo com especificações do edital/proposta comercial			ok
26.3.	Deverá ser fornecido transferência de conhecimento de no mínimo 20 horas, para até quatro pessoas, designadas pela Contratante, em até 15 dias após o término da instalação, afim de repassar as informações necessárias dos produtos adquiridos, incluindo detalhamento do produto e seus aspectos gerais de configuração e operação.	De acordo com especificações do edital/proposta comercial			ok
	MÓDULO DE CONTROLE DE PERÍMETRO VIRTUAL				ok
27.1.	Cada módulo deve possuir a capacidade e as características abaixo individualmente:	N/A	N/A	N/A	ok
27.1.1.	Throughput de 1.3 Gbps com a funcionalidade de controle de aplicação habilitada para todas as assinaturas que o fabricante possuir;	vm-series-vmware.pdf	4	Performance and Capacities	ok
27.1.2.	Throughput de 900 Mbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito;	vm-series-vmware.pdf	4	Performance and Capacities	ok
27.1.3.	Os documentos públicos devem comprovar os throughputs aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real (real-word traffic blend/Enterprise Mix);	vm-series-vmware.pdf	4	Performance and Capacities	ok
27.1.4.	Suporte a, no mínimo, 800.000 conexões simultâneas;	vm-series-vmware.pdf	4	Performance and Capacities	ok
27.1.5.	Deve suportar os drivers vmxnet3 e e1000;	vm-series-vmware.pdf	5	Performance and Capacities	ok
27.2.	Por cada módulo que compõe o controle de perímetro virtual, entende-se o software e as licenças necessárias para o seu funcionamento;	vm-series-vmware.pdf	5	Virtualization Specifications	ok
27.3.	Deve ser possível definir interfaces de rede dedicada para gerência do módulo virtual;	VM-Series 8.0 Deployment Guide	60	Minimum of two network interfaces (vmNICs). One will be a dedicated vmNIC for the management interface and one for the data interface.	ok
27.4.	Deve suportar adição de, no mínimo, 4 vCPUs para cada módulo virtual;	vm-series-vmware.pdf	5	System Requirements	ok
27.5.	Deve suportar adição de, no mínimo, 9 GB de memória RAM para cada módulo virtual;	vm-series-vmware.pdf	5	System Requirements	ok
	CARACTERÍSTICAS GERAIS				ok
27.6.	As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos módulos desde que obedeçam a todos os requisitos desta especificação;	De acordo com especificações do edital/proposta comercial			ok
27.7.	O módulo deve ser otimizada para análise de conteúdo de aplicações em camada 7;	datasheet_pa-5000_0.pdf	1	application identification	ok
27.8.	Os módulos virtuais que executem as funcionalidades de proteção de rede, bem como a console de gerência e monitoração, devem ser de um mesmo fabricante;	De acordo com especificações do edital/proposta comercial			ok
27.9.	O software deverá ser fornecido em sua versão mais atualizada;	De acordo com especificações do edital	N/A	N/A	ok
27.10.	Enviar log para sistemas de monitoração externos, simultaneamente;	PAN-OS 8.0 Administrator's Guide	873	LLDP Syslog Messages and SNMP Traps	ok
27.11.	Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;	PAN-OS 8.0 Administrator's Guide	356	Use Syslog for Monitoring	ok
27.12.	Deve permitir configurar certificado caso necessário para autenticação no sistema de monitoração externo de logs;	PAN-OS 8.0 Administrator's Guide	357	STEP 5 | Create a certificate to secure syslog communication over TLSv1.2.	ok
27.13.	Deve possuir proteção anti-spoofing;	NEW Book	11	IP Spoof Protection	ok
27.14.	As funcionalidades de controle de aplicações, QOS, SSL e SSH Decryption devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.	https://live.paloaltonetworks.com/t5/Management-Articles/What-Happens-When-Licenses-Expire-on-the-Palo-Alto-Net	N/A	What Happens When the Threat Prevention License Expires?	ok
	CARACTERÍSTICAS DE INTEGRAÇÃO COM PLATAFORMA DE VIRTUALIZAÇÃO				ok
27.15.	A módulo virtual deve ser do tipo "host-based", ou seja, módulo virtual virtual compatível com (VMware ESXi) e integrável de forma nativa com o (VMware NSX);	vm-series-specsheet.pdf	1	Supports a wide range of cloud and virtualization environments, including VMware NSX, ESXi	ok
27.16.	Deve inspecionar e controlar o tráfego entre máquinas virtuais em uma mesma sub-net através de integração com o VMware NSX sem a necessidade de atribuição de endereços IP nas interfaces do módulo virtual de proteção;	VM-Series 8.0 Deployment Guide	111	VM-Series Firewall for NSX	ok
27.17.	Deve inspecionar e controlar o tráfego entre máquinas virtuais via software através de integração com o VMware NSX sem a necessidade modificações na topologia de rede do ambiente virtualizado;	VM-Series 8.0 Deployment Guide	111	VM-Series Firewall for NSX	ok
27.18.	O módulo virtual de proteção deve permitir implementação (multi-tenancy) com criação de pelo menos 30 (trinta) instâncias que separem logicamente tráfegos desejados;	VM-Series 8.0 Deployment Guide	116	What is Multi-Tenant Support on the VM-Series Firewall for NSX?	ok
27.19.	Deve possuir tabelas de políticas de segurança individualizadas para cada instância criada internamente aos módulos virtuais de proteção;	vm-series-specsheet.pdf	2	Automated Security Deployment and Policy Updates	ok
27.20.	O deployment de novos módulos virtuais deve acompanhar o dinamismo do ambiente virtualizado, ou seja, um novo módulo virtual deve ser criado e configurado automaticamente em novos servidores físicos adicionados ao pool automaticamente;	VM-Series 8.0 Deployment Guide	115	Automated Deployment	ok
27.21.	O módulo virtual de proteção deve estabelecer comunicação com a gerência centralizada da solução para obtenção de licenças e políticas de controle de tráfego de forma automatizada sem a necessidade de intervenção humana no processo;	VMWARE NSX Add-ons.pptx	7	Panorama Centralized Management	ok
27.22.	Deve suportar implementação com (distributed switch);	VM-Series 8.0 Deployment Guide	63	STEP 2 | Before deploying the OVA file, set up virtual standard switch(es) and virtual distributed switch(es) that you will need for the VM-Series firewall.	ok
27.23.	Deve permitir a criação de objetos dinâmicos para servidores virtuais do pool, ou seja, quando uma máquina virtual hospedada em um servidor físico (A) e protegida por um modulo virtual de firewall (A), movimentar-se para um servidor físico (B) o objeto dinâmico deverá ser movido automaticamente para o módulo virtual (B), sem a necessidade de intervenção humana no processo;	VM-Series 8.0 Deployment Guide	114	Policy Enforcement using Dynamic Address Groups	ok
27.24.	Deve permitir a criação de regras de segurança de firewall camada 7, IPS, antivírus e anti-spyware usando objetos dinâmicos baseados em agrupamento de máquinas por "tag" existentes no Vmware NSX;	VM-Series 8.0 Deployment Guide	143 a 145	Apply Security Policies to the VM-Series Firewall	ok
27.25.	Deve permitir a criação de regras de redirect de tráfego no NSX usando security groups a partir da gerência centralizada da solução de firewall camada 7;	VM-Series 8.0 Deployment Guide	139	Create Steering Rules on Panorama	ok

27.26.	Deve controlar o tráfego leste/oeste entre máquinas virtuais pertencentes ao pool de servidores estando ou não hospedados no mesmo servido físico;	VM-Series 8.0 Deployment Guide	59	One VM-Series firewall per ESXi host	ok
27.27.	Deve possuir API aberta que permita integração com tecnologias de orquestração;	VM-Series 8.0 Deployment Guide	111	Panorama -> REST-based XML API	ok
	CONTROLE POR POLÍTICA DE FIREWALL				ok
27.28.	Deverá suportar controles por zona de segurança.	PAN-OS 8.0 Administrator's Guide	31	Segment Your Network Using Interfaces and Zones	ok
27.29.	Controles de políticas por porta e protocolo.	PAN-OS 8.0 Administrator's Guide	920	Service	ok
27.30.	Controle de políticas por aplicações grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações.	PAN-OS 8.0 Administrator's Guide	919 / 486	Application / Use Application Objects in Policy	ok
27.31.	Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança.	PAN-OS 8.0 Administrator's Guide	918	Components of a Security Policy Rule	ok
27.32.	Deve permitir autenticação segura através de certificado nas fontes externas de endereços IP, domínios e URLs;	PAN-OS 8.0 Administrator's Guide	971	TEP 9 | If the list source is secured with SSL (i.e. lists with an HTTPS URL), enable server authentication. Select a Certificate Profile or create a New Certificate Profile for authenticating the server that hosts the list.	ok
27.33.	Deve permitir consultar e criar exceção para objetos das listas externas a partir da interface de gerência do próprio firewall;	PAN-OS 8.0 Administrator's Guide	973	Exclude Entries from an External Dynamic List	ok
27.34.	Controle de políticas por código de País (Por exemplo: BR, USA, UK, RUS).	PAN-OS 8.0 Administrator's Guide	919 / 924	Address/Address Group, Region	ok
27.35.	Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound).	PAN-OS 8.0 Administrator's Guide	557 / 559 / 560	Decryption Overview / SSL Forward Proxy / SSL Inbound Inspection	ok
27.36.	Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2;	PAN-OS 8.0 Administrator's Guide	210	STEP 6 | Define the range of protocols that the service can use:	ok
27.37.	Controle de inspeção e de-criptografia de SSH por política;	PAN-OS 8.0 Administrator's Guide	561 / 567	SSH Proxy / 2. Set the Type of decryption for the firewall to perform on matching traffic:	ok
27.38.	Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, pif, e reg	PAN-OS 8.0 Administrator's Guide	508	basic file blocking	ok
27.39.	Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo)	PAN-OS 8.0 Administrator's Guide	645 / 647	QoS Overview / QoS Profile	ok
27.40.	QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações.	PAN-OS 8.0 Administrator's Guide	661	Enforce QoS Based on DSCP Classification	ok
27.41.	Suportar a atribuição de agendamento as políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.	https://live.paloaltonetworks.com/t5/Management-Articles/How-to-Schedule-Policy-Actions/ta-p/56148	N/A	How to Schedule Policy Actions	ok
	CONTROLE DE APLICAÇÕES				ok
27.42.	Os módulos virtuais de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:	PAN-OS 8.0 Administrator's Guide	479	App-ID Overview	ok
27.42.1.	Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos.	PAN-OS 8.0 Administrator's Guide	486	Use Application Objects in Policy	ok
27.42.2.	Reconhecer pelo menos 1500 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;	https://applipedia.paloaltonetworks.com/	N/A	2568 Applications	ok
27.42.3.	Deve permitir criação de políticas por aplicação aderentes ao negócio da instituição, incluindo, mas não limitado a:	PAN-OS 8.0 Administrator's Guide	918-923	Security Policy	ok
27.42.3.1.	Permitir que somente a aplicação SSH seja utilizada pela equipe de suporte baseado em um grupo de usuários do LDAP/AD;	PAN-OS 8.0 Administrator's Guide / applipedia.paloaltonetworks.com	918-923	Security Policy	ok
27.42.3.2.	Permitir comunicação entre uma máquina virtual (A) e (B) para apenas uma sub-aplicação do Oracle;	PAN-OS 8.0 Administrator's Guide / VM-Series 8.0 Deployment Guide	918-924 / 59	Security Policy	ok
27.42.3.3.	Permitir que um determinado grupo de usuários do LDAP/AD tenha acesso restrito a uma sub-aplicação customizada do cliente incluída na base de aplicações da solução	PAN-OS 8.0 Administrator's Guide	918-923	Security Policy / One VM-Series firewall per ESXi host	ok
27.42.3.4.	Permitir que um determinado grupo de usuários do LDAP/AD acesso total a aplicação;	PAN-OS 8.0 Administrator's Guide	918-923	Security Policy	ok
27.42.4.	Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs, etc;	PAN-OS 8.0 Administrator's Guide	479	App-ID Overview	ok
27.42.5.	Deve inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo. A checagem de assinaturas também deve determinar se uma aplicação está utilizando a porta default ou não, incluindo, mas não limitado a RDP na porta 80 ao invés de 389;	techbrief-app-id.pdf	2	Heuristics:	ok
27.42.6.	Deve aplicar heurística a fim de detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Encrypted Bittorrent e aplicações VOIP que utilizam criptografia proprietária;	techbrief-app-id.pdf	1	..even those that try to evade detection by masquerading as legitimate traffic, hopping ports or sneaking through the firewall using encryption (TLS/SSL or SSH)..	ok
27.42.7.	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.	techbrief-app-id.pdf	2	Figure 1: How App-ID classifies traffic.	ok
27.43.	Para tráfego criptografado (SSL e SSH), deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;	techbrief-app-id.pdf	2	Application and Protocol Decoding	ok
27.44.	Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas;	techbrief-app-id.pdf	2	Application and Protocol Decoding	ok
27.45.	Identificar o uso de táticas evasivas via comunicações criptografadas;	techbrief-app-id.pdf	1	App-ID Traffic Classification Technology	ok
27.46.	Atualizar a base de assinaturas de aplicações automaticamente;	techbrief-app-id.pdf	4	As new App-IDs are introduced and delivered to the firewall via weekly updates, dynamic filters are automatically updated for those applications that meet the filter criteria.	ok
27.47.	Reconhecer aplicações em IPv6;	https://www.paloaltonetworks.com/documentation/compatibility-matrix/ipv6-support-by-feature/ipv6-support-b	N/A	App-id	ok
27.48.	Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP/AD;	PAN-OS 8.0 Administrator's Guide	647	QoS Concepts	ok
27.49.	Os módulos virtuais de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;	PAN-OS 8.0 Administrator's Guide	440	Configure User Mapping Using the PAN-OS Integrated User-ID Agent	ok
27.50.	Deve ser possível adicionar controle de aplicações em todas as regras de segurança do módulo virtual, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;	PAN-OS 8.0 Administrator's Guide	976	A best practice policy allows you to safely enable applicationsWhat is a Best Practice Internet Gateway Security Policy?	ok
27.51.	Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos e análise heurística;	techbrief-app-id.pdf	2	Heuristics:	ok
27.52.	Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;	PAN-OS 8.0 Administrator's Guide	480	Manage Custom or Unknown Applications	ok
27.53.	Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;	PAN-OS 8.0 Administrator's Guide	480	Manage Custom or Unknown Applications	ok

27.54.	A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de pelo menos os seguintes protocolos:	N/A	N/A	N/A	ok
27.54.1.	HTTP, FTP, SMB, SMTP, Telnet, SSH, MS-SQL, IMAP, IMAP, MS-RPC, RTSP e File body.	Tech Note-Creating Custom Signatures-Rev0.pdf	2-4	Existem contextos para todas as aplicações listadas no indice	ok
27.55.	O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;	https://live.paloaltonetworks.com/t5/Management-Articles/How-to-Request-a-new-App-ID/ta-p/59818		How to Request a new App-ID	ok
27.56.	Deve alertar o usuário quando uma aplicação for bloqueada;	PAN-OS 8.0 Web Interface Reference	490	Application Block Page	ok
27.57.	Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;	Content-Overview-overview.pdf	2	Using Security to Empower Your Business	ok
27.58.	Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, neonet, etc.) possuindo granularidade de controle/politicas para os mesmos;	https://apidocs.paloaltonetworks.com/			ok
27.59.	Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Gtalk, Facebook Chat, etc.) possuindo granularidade de controle/politicas para os mesmos;	techbrief-app-id.pdf	4	Application Groups:	ok
27.60.	Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Gtalk chat e bloquear a transferência de arquivos;	techbrief-app-id.pdf	4	Application Function-Level Controls	ok
27.61.	Deve possibilitar a diferenciação de aplicações Proxies (ghostsurf, freegate, etc.) possuindo granularidade de controle/politicas para os mesmos;	techbrief-app-id.pdf	4	Application Groups:	ok
27.62.	Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:	PAN-OS 8.0 Administrator's Guide	486 / 487	Create an Application Group / Create an Application Filter	ok
27.63.	Tecnologia utilizada na aplicações (Client-Server, Browse Based, Network Protocol, etc).	techbrief-app-id.pdf / apidocs.paloaltonetworks.com	4	Dynamic Filters / TECHNOLOGY	ok
27.64.	Nível de risco da aplicação.	PAN-OS 8.0 Administrator's Guide	487	STEP 4 | Define the filter by selecting attribute values from the Category, Subcategory, Technology, Risk, and Characteristic sections.	ok
27.65.	Categoria e sub-categoria de aplicações.	PAN-OS 8.0 Administrator's Guide	487	STEP 4 | Define the filter by selecting attribute values from the Category, Subcategory, Technology, Risk, and Characteristic sections.	ok
27.66.	Aplicações que usem técnicas evasivas, utilizadas por malwares, como transferência de arquivos e/ou uso excessivo de banda, etc.	PAN-OS 8.0 Administrator's Guide / apidocs.paloaltonetworks.com	487	STEP 4 | Define the filter by selecting attribute values from the Category, Subcategory, Technology, Risk, and Characteristic sections. / CHARACTERISTIC	ok
	PREVENÇÃO DE AMEAÇAS				ok
27.67.	Para proteção do ambiente contra ataques, os módulos virtuais devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados ou entregue através de composição com outro fabricante.	NGFW-Content-ID	1 a 5	Content id	ok
27.68.	Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);	NGFW-Content-ID	2 e 3	Threat Prevention (pag 2) e ntrusion Prevention (pag 3)	ok
27.69.	As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.	https://live.paloaltonetworks.com/t5/Learning-Articles/What-Happens-When-the-Threat-Prevention-License-Expires/ta-p/53414			ok
27.70.	Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;	PAN-OS 8.0 Administrator's Guide	502	5. (HA only) Decide whether to Sync To Peer, which enables peers to synchronize content updates after download and install (the update schedule does not sync across peers; you must manually configure the schedule on both peers	ok
27.71.	Quando utilizada as funções de IPS, Antivírus e Anti-spyware, o módulo virtual deve entregar a mesma performance (não degradar) entre ter 1 única assinatura de IPS habilitada ou ter todas as assinaturas de IPS, Anti-Vírus e Antispyware habilitadas simultaneamente.	Content_ID_tech.pdf	1 a 3	Integrated by Design / Intrusion Prevention	ok
27.72.	As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;	PAN-OS 8.0 Web Interface Reference	183	Actions in Security Profiles / Alert	ok
27.73.	Exceções por IP de origem ou de destino devem ser possíveis nas regras, de forma geral e assinatura a assinatura;	PAN-OS 8.0 Web Interface Reference	104	Creating and Managing Policies	ok
27.74.	Deve suportar granularidade nas politicas de IPS Antivírus e Anti-Spyware, possibilitando a criação de diferentes politicas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.	PAN-OS 8.0 Web Interface Reference	104	Creating and Managing Policies	ok
27.75.	Deve permitir o bloqueio de vulnerabilidades.	NGFW-Content-ID	1	Palo Alto Networks then goes beyond stopping known threats....	ok
27.76.	Deve permitir o bloqueio de exploits conhecidos.	NGFW-Content-ID	1	Palo Alto Networks then goes beyond stopping known threats....	ok
27.77.	Deve incluir proteção contra ataques de negação de serviços.	NGFW-Content-ID	3	DoS attacks and port scans that lead to the compromise and....	ok
27.78.	Deve suportar a inspeção e criação de regras de proteção de DOS e QOS para o conteúdo de tráfego tunelados pelos protocolos GRE e IPSEC não criptografado;	PAN-OS 8.0 Administrator's Guide	650	QoS for Clear Text and Tunneled Traffic	ok
27.79.	Deverá possuir os seguintes mecanismos de inspeção de IPS:	N/A	N/A	N/A	ok
27.79.1.	Análise de padrões de estado de conexões;	NGFW-Content-ID	3	Protocol decoders and anomaly detection	ok
27.79.2.	Análise de decodificação de protocolo;	NGFW-Content-ID	2	SSL decryption	ok
27.79.3.	Análise para detecção de anomalias de protocolo;	NGFW-Content-ID	3	Statistical anomaly detection	ok
27.79.4.	Análise heurística;	NGFW-Content-ID	3	Heuristic-based analysis	ok
27.79.5.	IP Defragmentation;	NGFW-Content-ID	3	IP defragmentation	ok
27.79.6.	Remontagem de pacotes de TCP;	NGFW-Content-ID	3	TCP reassembly	ok
27.79.7.	Bloqueio de pacotes malformados.	NGFW-Content-ID	3	Invalid or malformed packet detection	ok
27.80.	Ser imune e capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPfloof, etc;	PAN-OS 8.0 Administrator's Guide	1040	Configure DoS Protection Against Flooding of New Sessions	ok
27.81.	Detectar e bloquear a origem de portscans;	PAN-OS 8.0 Administrator's Guide	1030	Configure Reconnaissance Protection	ok
27.82.	Detectar e bloquear a origem de portscans com possibilidade de criar exceções para endereços IPs de ferramentas de monitoramento da organização;	PAN-OS 8.0 Administrator's Guide	1030	Configure Reconnaissance Protection	ok
27.83.	Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;	PAN-OS 8.0 Administrator's Guide	925	Antivirus Profiles	ok
27.84.	Suportar os seguintes mecanismos de inspeção contra ameaças de rede: análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, análise heurística, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;	NGFW-Content-ID	2 e 3	Intrusion Prevention	ok
27.85.	Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;	NGFW-Content-ID	3	Content-ID protects networks from all types of vulnerability exploits	ok
27.86.	Possuir assinaturas para bloqueio de ataques de buffer overflow;	NGFW-Content-ID	3	Content-ID protects networks from all types of vulnerability exploits	ok
27.87.	Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto.	Custom Signatures	5	These contexts are available for custom IPS signatures,	ok
27.88.	Permitir o bloqueio de malwares e spywares, pelo menos nos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;	PAN-OS 8.0 Administrator's Guide	925	The default profile inspects all of the listed protocol decoders for viruses....	ok
27.89.	Suportar bloqueio de arquivos por tipo;	PAN-OS 8.0 Administrator's Guide	928	File Blocking Profiles	ok
27.90.	Identificar e bloquear comunicação com botnets;	PAN-OS 8.0 Administrator's Guide	327	Malicious	ok
27.91.	Deve suportar varias técnicas de prevenção, incluindo Drop e tcp-rst (Cliente, Servidor e ambos);	PAN-OS 8.0 Administrator's Guide	925 -926	Antivirus Profiles / Anti-Spyware Profiles	ok
27.92.	Deve suportar referencia cruzada com CVE;	PAN-OS 8.0 Administrator's Guide	550 / 936	and CVEs associated with the threat / Create Best Practice Security Profiles for the Internet Gateway	ok
27.93.	Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:	N/A	N/A	N/A	ok

27.93.1.	O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo módulo virtual;	PAN-OS 8.0 Administrator's Guide	325-327	Log Types and Severity Levels	ok
27.94.	Deve suportar a captura de pacotes (PCAP), por assinatura de IPS e Antyspyware;	PAN-OS 8.0 Administrator's Guide	313	Threat Packet Capture	ok
27.95.	Deve permitir que na captura de pacotes por assinaturas de IPS e Antispyware seja definido o número de pacotes a serem capturados. Esta captura deve permitir selecionar, no mínimo, 50 pacotes;	PAN-OS 8.0 Administrator's Guide	318	Take a Threat Packet Capture	ok
27.96.	Deve possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos sejam resolvidas pelo Firewall com endereços (IPv4 e IPv6), previamente definidos;	PAN-OS 8.0 Administrator's Guide	534	DNS Sinkholing	ok
27.97.	Permitir o bloqueio de vírus, pelo menos, nos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;	PAN-OS 8.0 Administrator's Guide	925	The default profile inspects all of the listed protocol decoders for viruses....	ok
27.98.	Os eventos devem identificar o país de onde partiu a ameaça;	PAN-OS 8.0 Administrator's Guide	367	Source Country	ok
27.99.	Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms.	PAN-OS 8.0 Administrator's Guide	925	Antivirus Profiles	ok
27.100.	Proteção contra downloads involuntários usando HTTP de arquivos executáveis. maliciosos.	PAN-OS 8.0 Administrator's Guide	925	Antivirus Profiles	ok
27.101.	Rastreamento de vírus em pdf.	PAN-OS 8.0 Administrator's Guide	925	Antivirus Profiles	ok
27.102.	Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.)	PAN-OS 8.0 Administrator's Guide	928	basic file blocking	ok
27.103.	Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.	PAN-OS 8.0 Administrator's Guide	921-922	Create a Security Policy Rule	ok
	ANÁLISE DE MALWARES MODERNOS				ok
27.104.	Devido aos Malwares hoje em dia serem muito dinâmicos e um antivírus comum reativo não ser capaz de detectar os mesmos com a mesma velocidade que suas variações são criadas, a solução ofertada dever possuir funcionalidades para análise de Malwares não conhecidos incluídas na própria ferramenta ou entregue com composição com outro fabricante;	WildFire Datasheet	1	Automatically Prevent Highly Evasive Zero-Day Exploits and Malware	ok
27.105.	O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "In Cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado;	WildFire Datasheet	1	Automatically Prevent Highly Evasive Zero-Day Exploits and Malware	ok
27.106.	Selecionar através de políticas granulares quais tipos de arquivos sofrerão esta análise incluindo, mas não limitado a: endereço IP de origem/destino, usuário/grupo do AD/LDAP, aplicação, porta, tipo de arquivo e todas estas opções simultaneamente;	https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Configure-WildFire/ta-p/58165	N/A	How to configure	ok
27.107.	Deve possuir a capacidade de diferenciar arquivos analisados em pelo menos três categorias: malicioso, não malicioso e arquivos não maliciosos, mas com características indesejáveis como softwares que deixa o sistema operacional lento, que alteram parâmetros do sistema, etc.;	https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Configure-WildFire/ta-p/58165	N/A	How to configure...	ok
27.108.	Suportar a análise com pelo menos 100 (cem) tipos de comportamentos maliciosos para a análise da ameaça não conhecida;	WildFire Datasheet	1	Dynamic analysis	ok
27.109.	Suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows XP, Windows 7 (32 bits) e Windows 7 (64 bits);	WildFire Datasheet	4	The WildFire global cloud subscription provides	ok
27.110.	Deve suportar a monitoração de arquivos trafegados na internet (HTTPs, FTP, HTTP, SMTP) como também arquivos trafegados internamente entre servidores de arquivos usando SMB;	WildFire Admin Guide	12	WildFire can discover zero-day malware in web traffic...	ok
27.111.	A solução deve possuir a capacidade de analisar em sand-box links (http e https) presentes no corpo de e-mails trafegados em SMTP e POP3. Deve ser gerado um relatório caso a abertura do link pela sand-box o identifique como site hospedeiro de exploits;	WildFire Admin Guide	14	Email Link Analysis	ok
27.112.	A análise de links em sand-box deve deve ser capaz de classificar sites falsos na categoria de phishing e atualizar a base de filtro de URL da solução;	WildFire Admin Guide	13	The link directs users to a phishing site...	ok
27.113.	Para ameaças trafegadas em protocolo SMTP e POP3, a solução deve ter a capacidade de mostrar nos relatórios o remetente, destinatário e assunto dos e-mails permitindo identificação ágil do usuário vítima do ataque;	WildFire Admin Guide	14	The firewall only extracts links and associated session...	ok
27.114.	O sistema de análise "In Cloud" ou local deve prover informações sobre as ações do Malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo Malware, gerar assinaturas de Antivírus e Anti- spyware automaticamente, definir URLs não confiáveis utilizadas pelo novo Malware e prover informações sobre o usuário infectado (seu endereço ip e seu login de rede);	WildFire Admin Guide	70	The detailed log view displays Log Info and the WildFire Analysis...	ok
27.115.	O sistema automático de analise "In Cloud" ou local deve emitir relatório com identificação de quais soluções de antivírus existentes no mercado possuem assinaturas para bloquear o malware;	WildFire Admin Guide	77	Coverage Status	ok
27.116.	Deve permitir exportar o resultado das análises de malwares de dia Zero em PDF e CSV a partir da própria interface de gerência;	WildFire Admin Guide	75	click the Download as PDF button on the upper right of the report page	ok
27.117.	Deve permitir o download dos malwares identificados a partir da própria interface de gerência;	WildFire Admin Guide	70	(imagem 3) "download file"	ok
27.118.	Deve permitir visualizar o resultados das análises de malwares de dia zero nos diferentes sistemas operacionais suportados;	WildFire Admin Guide	70	For all samples, the WildFire analysis report displays...	ok
27.119.	Deve permitir informar ao fabricante quanto a suspeita de ocorrências de falso-positivo e falso-negativo na análise de malwares de dia Zero a partir da própria interface de gerência.	WildFire Admin Guide	79	Report an Incorrect Verdict	ok
27.120.	Caso seja necessário licenças de sistemas operacional e softwares para execução de arquivos no ambiente controlado (sand-box), as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a contratante;	Não se Aplica			ok
27.121.	Suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;	WildFire Admin Guide	13	File Analysis	ok
27.122.	Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e class) e Android APKs no ambiente controlado;	WildFire Admin Guide	13	File Analysis	ok
27.123.	Deve atualizar a base com assinaturas para bloqueio dos malwares identificados em sand-box com frequência de, pelo menos, 5 minutos	WildFire Admin Guide	8	WildFire then generates signatures to recognize the newly-discovered malware, and...	ok
27.124.	Permitir o envio de arquivos e links para análise no ambiente controlado via de forma automática via API.	WildFire Admin Guide	10	Samples are all file types and email links submitted for WildFire analysis from the firewall and the public API	ok
27.125.	Deve permitir o envio para análise em sand-box de malwares bloqueados pelo antivírus da solução;	WildFire Admin Guide	25	you can also manually submit files for analysis using the WildFire portal.	ok
	IDENTIFICAÇÃO DE USUÁRIOS				ok
27.126.	Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via ldap, Active Directory, E-directory e base de dados local.	PAN-OS 8.0 Administrator's Guide	921-922 / 149	Create a Security Policy Rule / Authentication Types	ok
27.127.	Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários.	PAN-OS 8.0 Administrator's Guide	921-922 / 149	Create a Security Policy Rule / Authentication Types	ok
27.128.	Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários.	PAN-OS 8.0 Administrator's Guide	921-922 / 149	Create a Security Policy Rule / Authentication Types	ok
27.129.	Deve possuir integração com Ldap para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários.	PAN-OS 8.0 Administrator's Guide	921-922 / 149	Create a Security Policy Rule / Authentication Types	ok
27.130.	Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via syslog, para a identificação de endereços IP e usuários;	PAN-OS 8.0 Administrator's Guide	422 / 442	These services include wireless controllers, 802.1x devices, Apple Open Directory servers... / Configure the PAN-OS Integrated User-ID Agent as a Syslog Listener	ok

27.131.	Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal).	PAN-OS 8.0 Administrator's Guide	450	Map IP Addresses to Usernames Using Captive Portal	ok
27.132.	Suporte a autenticação Kerberos.	PAN-OS 8.0 Administrator's Guide	151	Kerberos	ok
27.133.	Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços.	PAN-OS 8.0 Administrator's Guide	431 / 455	Map IP Addresses to Users / Configure User Mapping for Terminal Server Users	ok
27.134.	Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em servidores acessados remotamente, mesmo que não sejam servidores Windows.	PAN-OS 8.0 Administrator's Guide	422	Port Mapping / For terminal servers that do not support the Terminal Services agent, such as Linux terminal servers, you can use the XML API to send user mapping information from login and logout events to User-ID	ok
	CONTROLE DE TRÁFEGO E QUALIDADE DE SERVIÇO				ok
27.135.	Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming.	PAN-OS 8.0 Administrator's Guide	647	QoS for Applications and Users	ok
27.136.	Suportar a criação de políticas de QoS por:	N/A	N/A	N/A	ok
27.136.1.	Endereço de origem	PAN-OS 8.0 Administrator's Guide	647	QoS Policy	ok
27.136.2.	Endereço de destino	PAN-OS 8.0 Administrator's Guide	647	QoS Policy	ok
27.136.3.	Por usuário e grupo do LDAP/AD.	PAN-OS 8.0 Administrator's Guide	647	QoS Policy	ok
27.136.4.	Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;	PAN-OS 8.0 Administrator's Guide	647	QoS Policy	ok
27.136.5.	Por porta;	PAN-OS 8.0 Administrator's Guide	647	QoS Policy	ok
27.137.	O QoS deve possibilitar a definição de classes por:	PAN-OS 8.0 Administrator's Guide	648	QoS Classes	ok
27.137.1.	Banda Garantida	PAN-OS 8.0 Administrator's Guide	648	QoS Classes	ok
27.137.2.	Banda Máxima	PAN-OS 8.0 Administrator's Guide	648	QoS Classes	ok
27.137.3.	Fila de Prioridade.	PAN-OS 8.0 Administrator's Guide	648	QoS Classes	ok
27.138.	Suportar priorização RealTime de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype.	PAN-OS 8.0 Administrator's Guide / appipedia.paloaltonetworks.com	647	The Palo Alto Networks firewall provides this capability by integrating the features A	ok
27.139.	Suportar marcação de pacotes Diffserv, inclusive por aplicação;	PAN-OS 8.0 Administrator's Guide	661 / 647	Enforce QoS Based on DSCP Classification / QoS Policy	ok
27.140.	Disponibilizar estatísticas RealTime para classes de QoS.	PAN-OS 8.0 Web Interface Reference	664	Select Network > QoS and then Statistics to view QoS bandwidth	ok
27.141.	Deverá permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.	PAN-OS 8.0 Web Interface Reference	344	QoS Interface Statistics	ok
	FUNCIONALIDADES DE FILTRO DE DADOS				ok
27.142.	Permite a criação de filtros para arquivos e dados pré-definidos;	PAN-OS 8.0 Administrator's Guide	506	Set Up Data Filtering - Predefined patterns and built-in settings make it easy for you to create custom patterns for filtering on social security and credit card numbers or on file properties, such as a document title or author.	ok
27.143.	Os arquivos devem ser identificados por extensão e assinaturas;	PAN-OS 8.0 Administrator's Guide	508	Set Up File Blocking	ok
27.144.	Permite identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (P2P, InstantMessaging, SMB, etc);	PAN-OS 8.0 Administrator's Guide	508	basic file blocking	ok
27.145.	Suportar identificação de arquivos compactados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;	PAN-OS 8.0 Administrator's Guide	508	basic file blocking	ok
27.146.	Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;	PAN-OS 8.0 Administrator's Guide	506	Set Up Data Filtering	ok
27.147.	Permitir listar o número de aplicações suportadas para controle de dados;	PAN-OS 8.0 Web Interface Reference	206	Applications	ok
27.148.	Permitir listar o número de tipos de arquivos suportados para controle de dados;	PAN-OS 8.0 Web Interface Reference	206	File Types	ok
	FUNCIONALIDADES DE GEO-LOCALIZAÇÃO				ok
27.149.	Suportar a criação de políticas por Geo Localização, permitindo o trafego de determinado Pais/Países sejam bloqueados.	PAN-OS 8.0 Administrator's Guide	924	Address/Address Group, Region	ok
27.150.	Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.	PAN-OS 8.0 Administrator's Guide	361	Source Country Destination Country	ok
27.151.	Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas.	PAN-OS 8.0 Web Interface Reference	149	Objects > Regions	ok
	MÓDULO DE GERÊNCIA CENTRALIZADO				ok
28.1.	Deve permitir o gerenciamento centralizado de diversos módulos virtuais;	PAN-Server-8.0-Deployment-Guide	Página 122	Create Template(s) and Device Group(s) on Panorama	ok
28.2.	O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o trafego que passar pelos módulos virtuais;	panorama_admin-guide_8-0.pdf	Página 11	About Panorama: Aggregated logging with central oversight for analysis and reporting	ok
28.3.	Controle sobre todos os módulos virtuais da plataforma de segurança em uma única console, com administração de privilégios e funções;	panorama_admin-guide_8-0.pdf	Página 11	About Panorama: Distributed administration	ok
28.4.	O gerenciamento centralizado poderá ser entregue como appliance físico ou virtual. Caso seja entregue em appliance físico deve ser compatível com rack 19 polegadas e possuir todos acessórios necessários para sua instalação. Caso seja entregue em appliance virtual dever ser compatível com VMware ESXi, nesse caso a estrutura de virtualização será fornecida pelo contratante.	panorama_datasheet.pdf	Páginas 4, 5 e 6	Deployment Flexibility	ok
28.5.	Deve permitir controle global de políticas para todos os módulos virtuais que compõe a plataforma de segurança;	panorama_admin-guide_8-0.pdf	página 14	Centralized Firewall Configuration and Update Management	ok
28.6.	Deve suportar organizar os módulos virtuais administrados em grupos;	panorama_admin-guide_8-0.pdf	Página 126	Add a Device Group	ok
28.7.	Deve permitir a criação de objetos e políticas compartilhadas;	panorama_admin-guide_8-0.pdf	Páginas 128 / 16	Create Objects for Use in Shared or Device Group Policy / Device Group Policies	ok
28.8.	Deve consolidar logs e relatórios de todos os módulos virtuais administrados;	panorama_admin-guide_8-0.pdf	Página 117	Monitor Network Activity	ok
28.9.	Deve permitir que exportar backup de configuração automaticamente via agendamento;	panorama_admin-guide_8-0.pdf	Páginas 251 e 252	Schedule Export of Configuration Files	ok
28.10.	Centralizar a administração de regras e políticas do cluster, usando uma única interface de gerenciamento;	panorama_admin-guide_8-0.pdf	Página 9	Panorama Overview	ok
28.11.	O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;	panorama_admin-guide_8-0.pdf	Páginas 100	Access and Navigate Panorama Management Interfaces	ok
28.12.	Deve permitir substituir o certificado de fábrica no acesso HTTPS a gerência do firewall como possibilidade de uso de certificado criado localmente na própria solução ou importado de fonte externa;	panorama_admin-guide_8-0.pdf	Página 46	Configure the general settings: Step 8 nº2	ok
28.13.	Caso haja a necessidade de instalação de cliente para administração da solução o mesmo deve ser compatível com sistemas operacionais Windows e Linux;	Não requer instalação de cliente	N/A	N/A	ok
28.14.	O gerenciamento deve permitir/possuir:	N/A	N/A	N/A	ok
28.14.1.	Criação e administração de políticas de firewall e controle de aplicação;	panorama_datasheet.pdf	Página 2	Simple Policy Control: Safely Enable Applications	ok
28.14.2.	Criação e administração de políticas de IPS, Antivírus e Anti- Spyware;	PAN-OS 8.0 Web Interface Reference	183 a 216	Objects > Security Profiles	ok
28.14.3.	Monitoração de logs;	panorama_admin-guide_8-0.pdf	página 24	Log Forwarding Options	ok
28.14.4.	Ferramentas de investigação de logs;	panorama_admin-guide_8-0.pdf	Páginas 20 e 230	Centralized Logging and Reporting / Review Threat Logs	ok
28.14.5.	Debugging;	CLI Commands	33	CLI debug mode	ok
28.14.6.	Captura de pacotes.	panorama_admin-guide_8-0.pdf	Página 230	Review Threat Logs	ok

28.15.	Deve permitir que administradores concorrentes façam modificações, valide configurações e reverta configurações do firewall simultaneamente e que cada administrador consiga aplicar apenas as suas alterações de forma independente das realizadas por outro administrador;	panorama_adminguide_8-0.pdf	Página 249	Preview, Validate, or Commit Configuration Changes	ok
28.16.	Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;	CLI Commands	12 a 16	Find a Command	ok
28.17.	Deve permitir usar palavras chaves e cores para facilitar identificação de regras;	PANOS_8-0_web-interface-help.pdf	Página 165	Objects > Tags	ok
28.18.	Deve permitir monitorar via SNMP uso de recursos por número elevado de sessões, porcentagem de utilização em referência ao número total suportado/licenciado e número de sessões estabelecidas;	panorama_adminguide_8-0.pdf	Pagina 264-266	Monitor Panorama and Log Collector Statistics Using SNMP	ok
28.19.	Bloqueio de alterações, no caso acesso simultâneo de dois ou mais administradores;	PANOS_8-0_web-interface-help.pdf	Página 33	Lock Configurations	ok
28.20.	Permitir definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;	panorama_adminguide_8-0.pdf	Página 27	Administrative Roles	ok
28.21.	Possuir Autenticação integrada ao Microsoft Active Directory e servidor Radius;	panorama_adminguide_8-0.pdf	Página 28	Authentication Profiles and Sequences	ok
28.22.	identificar por pesquisa de endereço IP, IP Range, subnet ou objetos, quais as regras que o estão sendo utilizados;	PANOS_8-0_web-interface-help.pdf	Página 35	Global Find	ok
28.23.	Deve atribuir sequencialmente um número a cada regra de firewall, NAT, QOS e regras de DOS;	PANOS_8-0_web-interface-help.pdf	Página 98	Building Blocks in a Security Policy Rule Table: Rule Number	ok
28.24.	Permitir a criação de regras que fiquem ativas em horário definido;	PANOS_8-0_web-interface-help.pdf	Página 227	Objects > Schedules	ok
28.25.	Permitir a criação de regras com data de expiração;	PANOS_8-0_web-interface-help.pdf	Página 227	Objects > Schedules	ok
28.26.	Suportar backup das configurações e rollback de configuração para a última configuração salva;	panorama_adminguide_8-0.pdf	Página 251	Manage Panorama and Firewall Configuration Backups	ok
28.27.	Suportar Rollback de Sistema Operacional para a ultima versão local;	panorama_adminguide_8-0.pdf	Página 230	Downgrade from Panorama 8.0	ok
28.28.	Possuir habilidade de upgrade via SCP, TFTP e interface de gerenciamento;	https://live.paloaltonetworks.com/t5/Management-Articles/How-to-Manually-Import-and-Install-PAN-OS-from-the-CLI/ta-p/58426			ok
28.29.	Executar a validação de regras antes da sua aplicação;	panorama_adminguide_8-0.pdf	Página 249 e 250	Preview, Validate, or Commit Configuration Changes: Step 4	ok
28.29.1.	É permitido o uso de appliance externo para permitir a validação de regras antes da aplicação.	Não é necessário appliance Externo	N/A	N/A	ok
28.30.	Efetuar a validação da políticas, avisando quando houver regras que ofusquem ou conflitem com outras (shadowing);	panorama_adminguide_8-0.pdf	Página 31	Panorama Commit, Validation, and Preview Operations: When you initiate a commit ...	ok
28.30.1.	É permitido o uso de appliance externo para permitir a validação de políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);	Não é necessário appliance Externo	N/A	N/A	ok
28.31.	Deve possibilitar a visualização e comparação de configurações Atuais, configuração anterior e configurações antigas.	panorama_adminguide_8-0.pdf	Página 20	Centralized Logging and Reporting: It also provides an audit trail...	ok
28.32.	Deve possibilitar a integração com outras soluções de SIEM de mercado (third-party SIEM vendors)	panorama_adminguide_8-0.pdf	Página 229	Use Case: Respond to an Incident Using Panorama	ok
28.33.	Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;	PANOS_8-0_web-interface-help.pdf	Página 59	Log Type Table: Configuration	ok
28.34.	Deverá ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado;	PANOS_8-0_web-interface-help.pdf	Página 72	App Scope Overview	ok
28.35.	Geração de relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego gerado na instituição;	PANOS_8-0_web-interface-help.pdf	Página 78	App Scope Traffic Map Report	ok
28.36.	Deve prover relatórios com visão correlacionada de aplicações, ameaças (IPS, Antivírus e Anti-Spware) e filtro de arquivos, para melhor diagnóstico e resposta a incidentes;	PAN-OS 8.0 Administrator's Guide	308 / 329	Use the Automated Correlation Engine / Unified Logs	ok
28.37.	O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos módulos virtuais de segurança;	panorama.pdf	3	Traffic Monitoring: Analysis, Reporting and Forensics	ok
28.38.	Deve possuir relatórios de utilização dos recursos por aplicações, ameaças (IPS, Antivírus e Anti-Spware), etc;	pan-os.pdf	275-277	Mostra consumo de bytes e sessões por apps e threats	ok
28.39.	Prover uma visualização sumarizada de todas as aplicações e ameaças (IPS, Antivírus e Anti-Spware), que passaram pela solução;	panorama_adminguide_8-0.pdf	Página 217	Monitor Network Activity	ok
28.40.	Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em RealTime;	PAN-OS 8.0 Administrator's Guide	299	To further drill-down into each vulnerability...	ok
28.41.	Nas opções de "Drill-Down", ser possível identificar o usuário que fez determinado acesso;	PAN-OS 8.0 Administrator's Guide	299	Then, view the User Activity widget in the Network Activity tab...	ok
28.42.	Deve ser possível exportar os logs em CSV;	PANOS_8-0_web-interface-help.pdf	Páginas 60 e 61	Log Actions Table: Export Logs	ok
28.43.	Deverá ser possível acessar o módulo virtual a aplicar configurações durante momentos onde o trafego é muito alto e a CPU e memória do estiver totalmente utilizada.	Single_Pass_Parallel_Processing_Architecture.pdf	7	Hardware Acceleration	ok
28.44.	Possuir rotação do log;	https://live.paloaltonetworks.com/t5/Management-Articles/When-are-Logs-Purged-on-the-Palo-Alto-Networks-Devices/	Página 1	Live Community Article	ok
28.45.	Deve permitir que os logs e relatórios sejam rotacionados automaticamente baseado no tempo em que estão armazenados na solução, assim como no espaço em disco usado;	https://live.paloaltonetworks.com/t5/Management-Articles/When-are-Logs-Purged-on-the-Palo-Alto-Networks-Devices/	Página 1	Live Community Article	ok
28.46.	Deve permitir fazer o envio de logs para soluções externas de forma granular podendo selecionar quais campos dos logs serão enviados incluindo, mas não limitado a: tipo de ameaça, usuário, aplicação, etc;	panorama_adminguide_8-0.pdf	Página 176	Configure Log Forwarding from Panorama to External Destinations	ok
28.47.	Exibição das seguintes informações, de forma histórica e em tempo real (atualizado de forma automática e contínua a cada 1 minuto):				ok
28.47.1.	Situação do módulo virtual e do cluster;	PANOS_8-0_web-interface-help.pdf	Páginas 43 e 44	Dashboard Widgets: High Availability	ok
28.47.2.	Principais aplicações;	PANOS_8-0_web-interface-help.pdf	Páginas 43 e 44	Dashboard Widgets: Top Applications	ok
28.47.3.	Principais aplicações por risco;	PANOS_8-0_web-interface-help.pdf	Páginas 43 e 44	Dashboard Widgets: Top High Risk Applications	ok
28.47.4.	Administradores autenticados na gerência da plataforma de segurança;	PANOS_8-0_web-interface-help.pdf	Páginas 43 e 44	Dashboard Widgets: Logged In Admins	ok
28.47.5.	Número de sessões simultâneas;	PANOS_8-0_web-interface-help.pdf	Páginas 43 e 44	Dashboard Widgets: Logged In Admins	ok
28.47.6.	Status das interfaces;	PANOS_8-0_web-interface-help.pdf	Páginas 43 e 44	Dashboard Widgets: Interfaces	ok
28.47.7.	Uso de CPU;	PANOS_8-0_web-interface-help.pdf	Páginas 43 e 44	Dashboard Widgets: System Resources	ok
28.48.	Geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:				ok
28.48.1.	Resumo gráfico de aplicações utilizadas;	PAN-OS 8.0 Administrator's Guide	283	Use the Application Command Center	ok
28.48.2.	Principais aplicações por utilização de largura de banda de entrada e saída;	PANOS_8-0_web-interface-help.pdf	Página 73	App Scope Summary Report	ok
28.48.3.	Principais aplicações por taxa de transferência de bytes;	PANOS_8-0_web-interface-help.pdf	Página 73	App Scope Summary Report	ok
28.48.4.	Principais hosts por número de ameaças identificadas;	PAN-OS 8.0 Administrator's Guide	285	ACC Tabs -> Threat Activity	ok
28.48.5.	Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas e ameaças (IPS, Antivírus e Anti-Spware), de rede vinculadas a este tráfego;	PANOS_8-0_web-interface-help.pdf	Páginas 85 e 86	Monitor > PDF Reports > User Activity Report	ok
28.48.6.	Deve permitir a criação de relatórios personalizados;	panorama_adminguide_8-0.pdf	Páginas 221 e 222	Generate, Schedule, and Email Reports: Step 2	ok
28.49.	Em cada critério de pesquisa do log deve ser possível incluir múltiplas entradas (ex. 10 redes e IP's distintos; serviços HTTP, HTTPS e SMTP), exceto no campo horário, onde deve ser possível definir um faixa de tempo como critério de pesquisa;	PAN-OS 8.0 Administrator's Guide	331	Filter Logs	ok
28.50.	Gerar alertas automáticos via:				ok
28.50.1.	Email;	panorama_adminguide_8-0.pdf	Página 20	Centralized Logging and Reporting	ok
28.50.2.	SNMP;	panorama_adminguide_8-0.pdf	Página 20	Centralized Logging and Reporting	ok
28.50.3.	Syslog;	panorama_adminguide_8-0.pdf	Página 20	Centralized Logging and Reporting	ok

28.47.7. Uso de CPU;
28.48. Geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:
28.48.1. Resumo gráfico de aplicações utilizadas;
28.48.2. Principais aplicações por utilização de largura de banda de entrada e saída;
28.48.3. Principais aplicações por taxa de transferência de bytes;
28.48.4. Principais hosts por número de ameaças identificadas;
28.48.5. Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas e ameaças (IPS, Antivírus e Anti-Spware), de rede vinculadas a este tráfego;
28.48.6. Deve permitir a criação de relatórios personalizados;
28.49. Em cada critério de pesquisa do log deve ser possível incluir múltiplas entradas (ex. 10 redes e IP's distintos; serviços HTTP, HTTPS e SMTP), exceto no campo horário, onde deve ser possível definir um faixa de tempo
28.50. Gerar alertas automáticos via:
28.50.1. Email;
28.50.2. SNMP;
28.50.3. Syslog;