LICITAÇÃO Nº 011/2022 – PARECER TÉCNICO

EMPRESA: Intersoft Soluções em Informática Eireli

Item I - Firewall tipo III (11 unidades) – Equipamento proposto: Forcepoint NGFW 335 Appliance – garantia e licenciamento de 36 meses

	Característica	Parecer	Validação	Local
1	A solução deve consistir de appliance de proteção de rede com funcionalidades de Next Generation .Firewall (NGFW) tais como reconhecimento e controle de aplicações, identificação de usuários, prevenção contra ameaças de vírus, spywares e malwares desconhecidos (Zero Day), IPS, filtro de URL e recursos de VPN;	OK	Página 1	https://www.forcepoint.com/sites/default/files/resources/datasheets/datasheet_forcepoint_ngfw_300_series_en_0_0_0_0_0_0_0.pdf
2	O hardware e software que executem as funcionalidades de proteção de rede devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;	OK	Página 1	https://www.forcepoint.com/sites/default/files/resources/datasheets/datasheet_forcepoint_ngfw_300_series_en_0_0_0_0_0_0_0.pdf
3	Deve possuir throughput de, no mínimo, 1 (um) Gbps com a funcionalidade de controle de aplicação para todas as assinaturas que o fabricante possuir;	OK	Página 2	https://www.forcepoint.com/sites/default/files/resources/datasheets/datasheet_forcepoint_ngfw_300_series_en_0_0_0_0_0_0_0.pdf
4	Deve possuir throughput de, no mínimo, 500 (quinhentos) Mbps com as funcionalidades de controle de aplicação, IPS, Antivírus e Anti-Spyware habilitadas simultaneamente na solução. A comprovação se dará através de documentação técnica do fabricante de acesso público informando os throughput aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real;	OK	Página 2	https://www.forcepoint.com/sites/default/files/resources/datasheets/datasheet_forcepoint_ngfw_300_series_en_0_0_0_0_0_0_0.pdf
5	Deve suportar, no mínimo, 60.000 (sessenta mil) conexões simultâneas	OK	Página 2	https://www.forcepoint.com/sites/default/files/resources/datasheets/datasheet_forcepoint_ngfw_300_series_en_0_0_0_0_0_0_0.pdf
6	Deve suportar, no mínimo, 11.000 (onze mil) novas conexões por segundo	OK	Página 2	https://www.forcepoint.com/sites/default/files/resources/datasheets/datasheet_forcepoint_ngfw_300_series_en_0_0_0_0_0_0_0.pdf
7	Deve possuir, no mínimo, 7 (sete) interfaces físicas de rede de 1 Gbps do tipo RJ-45;	OK	Página 2	https://www.forcepoint.com/sites/default/files/resources/datasheets/datasheet_forcepoint_ngfw_300_series_en_0_0_0_0_0_0_0.pdf
8	Deve possuir, no mínimo, 1 (uma) interface física de rede de 1 Gbps dedicada para gerenciamento, caso não possua a interface dedicada, será aceito utilizar interfaces físicas de rede de 1Gbps do tipo RJ-45, desde que o equipamento possua um número maior que o mínimo solicitado na alínea "7" desse item	OK (Gerência compartilhada)	Página 2	https://www.forcepoint.com/sites/default/files/resources/datasheets/datasheet_forcepoint_ngfw_300_series_en_0_0_0_0_0_0_0.pdf
9	Deve possuir, no mínimo, 1 (uma) interface física do tipo console ou similar;	OK	Página 2	https://www.forcepoint.com/sites/default/files/resources/datasheets/datasheet_forcepoint_ngfw_300_series_en_0_0_0_0_0_0_0.pdf
10	Deve possuir, no mínimo, 64 (sessenta e quatro) GB de armazenamento interno;	NÃO ENCONTRADO NA DOCUMENTAÇÃO	ausente	

11	Deve possuir fonte de alimentação elétrica capaz de operar entre 120 à 240 VAC;	OK	Página 2	https://www.forcepoint.com/sites/default/files/resources/datasheets/datasheet_forcepoint_ngfw_300_series_en_0_0_0_0_0_0_0.pdf
12	Deve suportar, no mínimo, 200 (duzentos) clientes de VPN SSL simultaneamente estando, caso necessário, devidamente licenciado para este fim;	OK	Página 2	https://www.forcepoint.com/sites/default/files/resources/datasheets/datasheet_forcepoint_ngfw_300_series_en_0_0_0_0_0_0_0.pdf
13	Deve suportar, no mínimo, 200 (duzentos) túneis de VPN IPSEC simultaneamente estando, caso necessário, devidamente licenciado para este fim;	OK	Página 2	https://www.forcepoint.com/sites/default/files/resources/datasheets/datasheet_forcepoint_ngfw_300_series_en_0_0_0_0_0_0_0.pdf

Item II - Firewall tipo II (02 unidades) – Equipamento proposto: Forcepoint NGFW 335 Appliance – garantia e licenciamento de 36 meses

	Característica	Parecer	Validação	Local
1	A solução deve consistir de appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW) tais como reconhecimento e controle de aplicações, identificação de usuários, prevenção contra ameaças de vírus, spywares e malwares desconhecidos (Zero Day), IPS, filtro de URL e recursos de VPN	OK	Página 1	https://www.forcepoint.com/sites/default/files/resources/datasheets/datasheet_forcepoint_ngfw_300_series_en_0_0_0_0_0_0_0.pdf
2	O hardware e software que executem as funcionalidades de proteção de rede devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;	OK	Página 1	https://www.forcepoint.com/sites/default/files/resources/datasheets/datasheet_forcepoint_ngfw_300_series_en_0_0_0_0_0_0_0.pdf
3	O equipamento deve ser fornecido com kit que permita a sua montagem em rack 19”;	OK	Página 2	https://www.forcepoint.com/sites/default/files/resources/datasheets/datasheet_forcepoint_ngfw_300_series_en_0_0_0_0_0_0_0.pdf
4	Deve possuir throughput de, no mínimo, 1.6 (um ponto seis) Gbps com a funcionalidade de controle de aplicação para todas as assinaturas que o fabricante possuir;	NÃO ATENDE “1.0Gbps”	Página 2	https://www.forcepoint.com/sites/default/files/resources/datasheets/datasheet_forcepoint_ngfw_300_series_en_0_0_0_0_0_0_0.pdf
5	Deve possuir throughput de, no mínimo, 850 (oitocentos e cinquenta) Mbps com as funcionalidades de controle de aplicação, IPS, Antivírus e Anti-Spyware habilitadas simultaneamente na solução. A comprovação se dará através de documentação técnica do fabricante de acesso público informando os throughput aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real;	OK	Página 2	https://www.forcepoint.com/sites/default/files/resources/datasheets/datasheet_forcepoint_ngfw_300_series_en_0_0_0_0_0_0_0.pdf
6	Deve suportar, no mínimo, 190.000 (cento e noventa mil) conexões simultâneas;	OK	Página 2	https://www.forcepoint.com/sites/default/files/resources/datasheets/datasheet_forcepoint_ngfw_300_series_en_0_0_0_0_0_0_0.pdf
7	Deve suportar, no mínimo, 35.000 (trinta e cinco mil) novas conexões por segundo;	OK	Página 2	https://www.forcepoint.com/sites/default/files/resources/datasheets/datasheet_forcepoint_ngfw_300_series_en_0_0_0_0_0_0_0.pdf
8	Deve possuir, no mínimo, 8 (oito) interfaces físicas de rede de 1 Gbps do tipo RJ-45;	OK	Página 2	https://www.forcepoint.com/sites/default/files/resources/datasheets/datasheet_forcepoint_ngfw_300_series_en_0_0_0_0_0_0_0.pdf
9	Deve possuir, no mínimo, 1 (uma) interface física de rede de 1 Gbps dedicada para gerenciamento;	NÃO ENCONTRADO NA DOCUMENTAÇÃO	ausente	

10	Deve possuir, no mínimo, 1 (uma) interface física do tipo console ou similar;	OK	Página 2	https://www.forcepoint.com/sites/default/files/resources/datasheets/datasheet_forcepoint_ngfw_300_series_en_0_0_0_0_0_0_0.pdf
11	Deve possuir, no mínimo, 128 (cento e vinte e oito) GB de armazenamento interno para o sistema operacional e registro de logs;	NÃO ENCONTRADO NA DOCUMENTAÇÃO	ausente	
12	Deve possuir fonte de alimentação elétrica redundante capaz de operar entre 120 à 240 VAC e devendo, em caso de problema com uma das fontes, permitir a substituição da fonte defeituosa com o equipamento em funcionamento;	OK	Página 2	https://www.forcepoint.com/sites/default/files/resources/datasheets/datasheet_forcepoint_ngfw_300_series_en_0_0_0_0_0_0_0.pdf
13	Deve suportar, no mínimo, 500 (quinhentos) clientes de VPN SSL simultaneamente estando, caso necessário, devidamente licenciado para este fim;	OK	Página 2	https://www.forcepoint.com/sites/default/files/resources/datasheets/datasheet_forcepoint_ngfw_300_series_en_0_0_0_0_0_0_0.pdf
14	Deve suportar, no mínimo, 200 (duzentos) túneis de VPN IPSEC simultaneamente estando, caso necessário, devidamente licenciado para este fim;	OK	Página 2	https://www.forcepoint.com/sites/default/files/resources/datasheets/datasheet_forcepoint_ngfw_300_series_en_0_0_0_0_0_0_0.pdf

Item III - Firewall tipo I (02 unidades) – Equipamento proposto: Forcepoint NGFW 2101 Appliance – garantia e licenciamento de 36 meses

	Característica	Parecer	Validação	Local
1	A solução deve consistir de appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW) tais como reconhecimento e controle de aplicações, identificação de usuários, prevenção contra ameaças de vírus, spywares e malwares desconhecidos (Zero Day), IPS, filtro de URL e recursos de VPN;	OK	Página 1	https://www.forcepoint.com/sites/default/files/resources/files/datasheet_forcepoint_ngfw_2100_series_en.pdf
2	O hardware e software que executem as funcionalidades de proteção de rede devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;	OK	Página 1	https://www.forcepoint.com/sites/default/files/resources/files/datasheet_forcepoint_ngfw_2100_series_en.pdf
3	O equipamento deve ser fornecido com kit que permita a sua montagem em rack 19”;	OK	Página 2	https://www.forcepoint.com/sites/default/files/resources/files/datasheet_forcepoint_ngfw_2100_series_en.pdf
4	Deve possuir throughput de, no mínimo, 4.4 (quatro ponto quatro) Gbps com a funcionalidade de controle de aplicação para todas as assinaturas que o fabricante possuir;	OK	Página 2	https://www.forcepoint.com/sites/default/files/resources/files/datasheet_forcepoint_ngfw_2100_series_en.pdf

5	Deve possuir throughput de, no mínimo, 2.1 (dois ponto um) Gbps com as funcionalidades de controle de aplicação, IPS, Antivírus e Anti-Spyware habilitadas simultaneamente na solução. A comprovação se dará através de documentação técnica do fabricante de acesso público informando os throughput aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real;	OK	Página 2	https://www.forcepoint.com/sites/default/files/resources/files/datasheet_forcepoint_ngfw_2100_series_en.pdf
6	Deve suportar, no mínimo, 400.000 (quatrocentos mil) conexões simultâneas;	OK	Página 2	https://www.forcepoint.com/sites/default/files/resources/files/datasheet_forcepoint_ngfw_2100_series_en.pdf
7	Deve suportar, no mínimo, 70.000 (setenta mil) novas conexões por segundo;	OK	Página 2	https://www.forcepoint.com/sites/default/files/resources/files/datasheet_forcepoint_ngfw_2100_series_en.pdf
8	Deve possuir, no mínimo, 8 (oito) interfaces físicas de rede de 1 Gbps do tipo RJ-45;	OK	Página 2	https://www.forcepoint.com/sites/default/files/resources/files/datasheet_forcepoint_ngfw_2100_series_en.pdf
9	Deve possuir, no mínimo, 1 (uma) interface física de rede de 1 Gbps dedicada para gerenciamento;	OK	Página 2	https://www.forcepoint.com/sites/default/files/resources/files/datasheet_forcepoint_ngfw_2100_series_en.pdf
10	Deve possuir, no mínimo, 1 (uma) interface física do tipo console ou similar;	OK	Página 2	https://www.forcepoint.com/sites/default/files/resources/files/datasheet_forcepoint_ngfw_2100_series_en.pdf
11	Deve possuir, no mínimo, 128 (cento e vinte e oito) GB de armazenamento interno para o sistema operacional e registro de logs;	NÃO ENCONTRADO NA DOCUMENTAÇÃO	ausente	
12	Deve possuir fonte de alimentação elétrica redundante capaz de operar entre 120 à 240 VAC e devendo, em caso de problema com uma das fontes, permitir a substituição da fonte defeituosa com o equipamento em funcionamento;	OK	Página 2	https://www.forcepoint.com/sites/default/files/resources/files/datasheet_forcepoint_ngfw_2100_series_en.pdf
1 3	Deve suportar, no mínimo, 1.500 (hum mil e quinhentos) clientes de VPN SSL simultaneamente estando, caso necessário, devidamente licenciado para este fim;	OK	Página 2	https://www.forcepoint.com/sites/default/files/resources/files/datasheet_forcepoint_ngfw_2100_series_en.pdf
14	Deve suportar, no mínimo, 2,000 (dois mil) túneis de VPN IPSEC simultaneamente estando, caso necessário, devidamente licenciado para este fim;	OK	Página 2	https://www.forcepoint.com/sites/default/files/resources/files/datasheet_forcepoint_ngfw_2100_series_en.pdf

Item IV – Solução de proteção avançada de Endpoint (300 unidades) – Proposto: SentinelOne NGAV & Behavioral All Prevention – garantia e licenciamento de 36 meses.

	Característica	Parecer	Validação	Referência
1	Solução de proteção avançada de endpoint através da instalação de um agente nos endpoints (entende por endpoint uma estação de trabalho ou servidor de rede) para proteção contra exploits, malware, ransomware e console central de gerenciamento dos agentes;	OK	Página 10	Datasheet SentinelOne Endpoint Protection (EPP+EDR)

2	O console central de gerenciamento dos agentes instalados nos endpoints deve ser baseado em nuvem e acessado através de web browser;	OK	Página 2	https://go.sentinelone.com/rs/327-MNM-087/images/SEN0202_DataSheet_EPP_WEB.pdf
3	Deve prevenir contra ameaças conhecidas baseado em assinatura;	OK	13/05/2022	https://assets.sentinelone.com/c/singularity-xdr?x=950GFD&lb-mode=overlay&&lb-width=100&lb-height=100
4	Deve prevenir contra ameaças baseada em comportamento através do monitoramento das atividades realizadas pelo endpoint;	OK	13/05/2022	https://assets.sentinelone.com/c/singularity-xdr?x=950GFD&lb-mode=overlay&&lb-width=100&lb-height=100
5	Deve prevenir contra ameaças através do uso de machine learning através da análise local de arquivos desconhecidos;	OK	13/05/2022	https://assets.sentinelone.com/c/singularity-xdr?x=950GFD&lb-mode=overlay&&lb-width=100&lb-height=100
6	Deve possuir integração com serviço de análise de malwares desconhecidos em nuvem para uma análise mais profunda dos arquivos. O serviço de análise em nuvem pode ser do mesmo fabricante da solução de proteção avançada de endpoint ou de fabricantes terceiros devendo ser fornecidas todas as licenças necessárias para o seu perfeito funcionamento;	OK	Página 11	Datasheet SentinelOne Endpoint Protection (EPP+EDR)
7	O serviço de análise de malwares desconhecidos em nuvem deve realizar a análise de, no mínimo, os seguintes tipos de arquivos: arquivos executáveis, DLLs, arquivos Word (.doc, .docm e docx) e Excel (.xls, .xlsm e .xlsx) que contenham macros, arquivos DMG;	NÃO ENCONTRADO NA DOCUMENTAÇÃO	ausente	
8	Deve possuir mecanismos para detectar, em tempo real, ataques LotL – Living off the Land, ataques baseados em scripts e ataques fileless;	OK	13/05/2022	https://assets.sentinelone.com/c/singularity-xdr?x=950GFD&lb-mode=overlay&&lb-width=100&lb-height=100
9	Deve prevenir contra exploits incluindo Heap Spray, DEP – Data Execution Protection, ROP – Return-oriented Programming e exploits baseados em JIT – Just-in-time;	NÃO ENCONTRADO NA DOCUMENTAÇÃO	ausente	
10	Deve permitir bloquear o uso dispositivos portáteis USB como pen drivers, discos, drivers de CDROM nos endpoints para prevenir contra a transferência de arquivos maliciosos que possam estar nestes dispositivos;	OK	Página 2	https://go.sentinelone.com/rs/327-MNM-087/images/SEN0202_DataSheet_EPP_WEB.pdf
11	Deve possuir host firewall permitindo o controle da comunicação do endpoint através de regras de permissão e bloqueio do tráfego;	NÃO ENCONTRADO NA DOCUMENTAÇÃO	Ausente	
12	Deve permitir executar a varredura no endpoint em busca de arquivos infectados por malware a partir do console central de gerenciamento e a partir do próprio agente instalado no endpoint. Deve ser possível também configurar varreduras agendadas;	Ok	Página 2	https://go.sentinelone.com/rs/327-MNM-087/images/SEN0202_DataSheet_EPP_WEB.pdf
13	A atualização do motor de detecção de ameaças deve ser realizada de forma transparente para o usuário;	OK	Página 11	Datasheet SentinelOne Endpoint Protection (EPP+EDR)
14	Deve exibir lista com todos os alertas de incidentes detectados pelos agentes instalados nos endpoints no console central de gerenciamento. Deve mostrar, para cada alerta da lista, no mínimo, a data e hora que o incidente ocorreu, o nome ou endereço IP do endpoint, a ação tomada pelo agente 17 com relação ao incidente e a categoria do incidente informando se o mesmo se trata de, por exemplo, um exploit ou um malware;	OK	13/05/2022	https://assets.sentinelone.com/c/sentinelone_demo_shi?x=950GFD&lb-mode=overlay&&lb-width=100&lb-height=100

15	Deve ser possível visualizar a cadeia de processos executados que levaram a geração do alerta exibindo o primeiro processo executado o qual foi responsável pela execução dos demais processos. Para cada processo executado deve ser possível visualizar, no mínimo, o caminho onde o processo estava localizado (por exemplo c:/temp/pe.exe), o nome do usuário que iniciou o processo e o tempo em que o processo ficou em execução informando a data e hora do início e do fim da execução do mesmo;	OK	13/05/2022	https://assets.sentinelone.com/c/sentinelone_demo_shi?x=950GFD&lb-mode=overlay&&lb-width=100&lb-height=100
16	Deve ser possível também visualizar, em uma linha do tempo, todos os processos e eventos, desde a execução do primeiro processo responsável pela execução dos demais, que geraram um alerta de incidente. Os tipos de eventos que devem ser exibidos, além de processos executados, são conexões de entrada e saída, conexões fracassadas e download e upload de dados;	OK	13/05/2022	https://assets.sentinelone.com/c/sentinelone_demo_shi?x=950GFD&lb-mode=overlay&&lb-width=100&lb-height=100
17	A solução deve possuir integração com o firewall de próxima geração em processo de compra desse edital e que será utilizado por este órgão para correlação dos eventos e alertas gerados pelo firewall permitindo visualizar na cadeia de processos executados de um determinado alerta as informações de acessos externos realizados pelos processos e atividades maliciosos detectados pela solução;	NÃO ENCONTRADO NA DOCUMENTAÇÃO	ausente	
18	Deve possuir ferramenta de busca para a investigação de incidentes permitindo a realização de buscas com base em, no mínimo, processos executados, em arquivos criados, alterados e deletados, em atributos de rede como endereço IP, nome do host, porta e protocolo, em registros criados, modificados e deletados, em eventos de log do Windows e Linux. Deve permitir também realizar a busca através da combinação dos diversos atributos descritos anteriormente;	OK	13/05/2022	https://assets.sentinelone.com/c/binaryvault?x=950GFD&lb-mode=overlay&&lb-width=100&lb-height=100
19	A solução deve permitir realizar a configuração de alertas com base em incidentes com base em indicadores de comprometimento (IOCs). Os tipos de indicadores de comprometimento que podem ser criados pelo administrador da solução devem ser, no mínimo, nome do arquivo, domínio e endereço IP de destino. Além de permitir a criação dos indicadores de comprometimento a solução deve permitir também importar listas de indicadores de comprometimentos de serviços externos de inteligência contra ameaça;	OK	13/05/2022	https://assets.sentinelone.com/c/ds-s1singularityepp-?x=950GFD&lb-mode=overlay&&lb-width=100&lb-height=100
20	A solução deve permitir realizar a configuração de alertas com base em incidentes com base em indicadores de comprometimento baseados no comportamento do endpoint. Os tipos de comportamentos que devem ser detectados são, no mínimo, execução de processos, manipulação de privilégios em arquivo, ofuscação do tipo do arquivo, atividade de reconhecimento na rede, escalonamento de privilégio e movimentos laterais na rede.	OK	13/05/2022	https://assets.sentinelone.com/c/ds-s1singularityepp-?x=950GFD&lb-mode=overlay&&lb-width=100&lb-height=100

21	A solução deve permitir, realizar o acesso diretamente aos endpoints através de um terminal remoto para execução de ações para investigação e repostas aos incidentes de segurança. As ações que podem ser executadas através do terminal remoto devem ser, no mínimo, visualizar e encerrar processos que estão sendo executados no endpoint, apagar, mover e renomear arquivos localizados no endpoint, prover interface de linha de comando para execução de comandos do sistema operacional, prover interface de linha de comando para execução de scripts e comandos Pyhton. Ao final da sessão de acesso ao endpoint dever se possível salvar um relatório contendo todas as atividades realizadas durante a sessão;	OK	13/05/2022	https://assets.sentinelone.com/c/sentinelone_demo_shi?x=950GFD&lb-mode=overlay&&lb-width=100&lb-height=100
22	Deve ser possível também realizar, a partir do console central de gerenciamento, a execução de scripts em diversos endpoints simultaneamente de forma centralizada;	OK	13/05/2022	https://assets.sentinelone.com/c/sentinelone_demo_shi?x=950GFD&lb-mode=overlay&&lb-width=100&lb-height=100
23	A solução deve permitir, a partir do console central de gerenciamento, isolar um endpoint impedindo a comunicação do mesmo com a rede para evitar que um possível ataque se propague pela rede;	OK	13/05/2022	https://assets.sentinelone.com/c/sentinelone_demo_shi?x=950GFD&lb-mode=overlay&&lb-width=100&lb-height=100
24	Deve ser possível a correlação com a lista de CVE – Common Vulnerabilities and Exposures conhecidos e permitir visualizar quais endpoints estão sendo afetados por uma determinada CVE;	OK	Página 2	https://go.sentinelone.com/rs/327-MNM-087/images/SEN0202_DataSheet_EPP_WEB.pdf
25	A solução deve permitir, a partir da console central de gerenciamento, a realização de busca de um determinado arquivo em todos os endpoints. A busca pode ser realizada com base no caminho completo onde o arquivo pode estar presente (c:\windows\system32\file.exe) e também com base 18 no hash do arquivo gerado pela solução. Deve ser possível ainda, a partir da console central de gerenciamento, apagar o arquivo de todos os endpoints onde ele está presente;	OK	13/05/2022	https://assets.sentinelone.com/c/sentinelone_demo_shi?x=950GFD&lb-mode=overlay&&lb-width=100&lb-height=100
26	A solução deve armazenar as informações de alertas, incidentes e suas respectivas atividades e ações e demais dados relacionados aos eventos de segurança detectados por um período de, no mínimo, 30 (trinta) dias;	OK	Página 1	https://www.sentinelone.com/wp-content/uploads/2021/02/SentinelOne-Data-Retention-Solution-Brief.pdf
27	A solução deve permitir a instalação do agente em endpoints com sistema operacional MS Windows 8.1, MS Windows 10, MS Windows Server 2016, MS Windows Server 2019, nas principais distribuições Linux como CentOS, Debian, Red Hat e SUSE nos sistemas operacionais MacOS e MacOS X;	OK	13/05/2022	https://success.alienvault.com/s/article/SentinelOne-System-Requirements https://www.sentinelone.com/press/sentinelone-now-supports-broadest-set-linux-distributions-market/
28	A solução deve permitir realizar o upgrade dos agentes instalados nos endpoints a partir do console central de gerenciamento;	OK	13/05/2022	https://assets.sentinelone.com/c/sentinelone_demo_shi?x=950GFD&lb-mode=overlay&&lb-width=100&lb-height=100
29	A solução deve possuir subscrição pelo período de, no mínimo, 36 (meses) permitindo, durante este período, acesso ilimitado ao console central de gerenciamento na nuvem, acesso a todas as atualização e serviços de segurança e assinaturas de proteção da solução e o pleno funcionamento do agente de proteção instalado no endpoint.	OK	Página 2	Proposta Técnica

Item V – Software de gerenciamento centralizado e armazenamento de logs (1 unidade) – Proposto: Forcepoint NGFW Management Center, Cloud Access Network Security – garantia e licenciamento de 36 meses.

	Característica	Parecer	Validação	Referência
1	Deve ser fornecido solução de gerenciamento centralizado, possibilitando o gerenciamento de diversos equipamentos de firewall de mesmo fabricante da solução;	OK	Página 1	Datasheet – NGFW Security Management Center
2	A solução de gerenciamento centralizado deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos de firewall gerenciados pela solução, além de consolidar os registros de eventos (logs) e relatórios de todos os equipamentos que compõem a solução de proteção de rede;	OK	Página 3	Datasheet – NGFW Security Management Center
3	Deve ser homologado e totalmente compatível com a Solução de Proteção de Rede Firewall especificada neste Termo de Referência para permitir o gerenciamento centralizado e armazenamento de logs do mesmo, estando devidamente licenciado para este fim;	OK	Página 5	Datasheet – NGFW Security Management Center
4	Deve permitir o controle sobre todos os equipamentos de firewall em uma única console, com administração de privilégios e funções;	OK	Página 1	Datasheet – NGFW Security Management Center
5	O gerenciamento centralizado poderá ser entregue como appliance físico ou virtual. Caso seja entregue em appliance físico ele deve ser compatível com rack 19 polegadas e possuir todos os acessórios necessários para sua instalação. Caso seja entregue em appliance virtual deve ser compatível com VMware ESXi;	OK	Página 9	Datasheet – NGFW Security Management Center
6	Deve permitir o armazenamento de logs sem limite de tempo nem limite da quantidade de logs diários a ser recebido ou armazenado, considerando que a infra do SENAR-PR possa vir a absorver o mesmo crescimento. Caso seja necessário licenciamento adicional, deverá ser entregue licenciado com a maior capacidade suportada;	OK	Página 3	Datasheet – NGFW Security Management Center
7	Deve permitir controle global de políticas para todos os equipamentos gerenciados pela solução;	OK	Página 7	Datasheet – NGFW Security Management Center
8	Deve suportar organizar os equipamentos gerenciados em grupos: os sistemas virtuais devem ser administrados como dispositivos individuais, os grupos podem ser geográficos, por funcionalidade (por exemplo, IPS), e distribuição;	OK	Página 7	Datasheet – NGFW Security Management Center
9	Deve implementar sistema de hierarquia entre os equipamentos gerenciados, onde seja possível aplicar configurações de forma granular em grupos de firewalls;	OK	Página 7	Datasheet – NGFW Security Management Center

10	Deve implementar a criação de perfis de usuários com acesso a solução de gerenciamento com definição exata de quais informações e de quais equipamento de firewalls e grupos de equipamentos de firewalls o usuário terá acesso referente a logs e relatórios;	OK	Página 7	Datasheet – NGFW Security Management Center
11	Deve permitir a criação de objetos e políticas compartilhadas;	OK	Página 4	Datasheet – NGFW Security Management Center
12	Deve consolidar logs e relatórios de todos os equipamentos de firewall gerenciados;	OK	Página 6	Datasheet – NGFW Security Management Center
13	Deve permitir exportar o backup de configuração automaticamente via agendamento;	OK	Página 4	Datasheet – NGFW Security Management Center
14	Deve permitir que a configuração dos firewalls seja importada de forma automática na solução de gerenciamento centralizado e que possa ser usada em outros firewalls e grupos de firewalls;	OK	Página 4	Datasheet – NGFW Security Management Center
15	Deve mostrar os status dos equipamentos de firewalls em alta disponibilidade a partir da solução de gerenciamento centralizado;	OK	Página 4	Datasheet – NGFW Security Management Center
16	Dever permitir salvar no mínimo 15 Tb de dados de Logs dos equipamentos por ele administrados, permitindo a pesquisa e filtragem de dados dos últimos 180 dias;	OK	Página 4	Datasheet – NGFW Security Management Center
17	Deve estar licenciado para no mínimo 15 devices;	OK	Página 4	Datasheet – NGFW Security Management Center
18	A solução de gerenciamento centralizado e armazenamento de logs deve possuir garantia pelo período de, no mínimo, 36 (trinta e seis) meses, compreendendo a atualização do software para obter novas funcionalidades e correções de bugs.	OK	Proposta comercial	Proposta comercial

Anexo II – Características obrigatórias mínimas comuns para os objetos: Item I, item II e item III

	Característica	Parecer	Validação	Referência
1	Deve operacionalizar no mínimo os seguintes critérios de SD-WAN	OK	Página 1	Datasheet – NGFW Security Management Center
1.1	A plataforma de segurança deverá recuperar pacotes perdidos antes que seja necessário alterar o caminho principal.	NÃO ENCONTRADO NA DOCUMENTAÇÃO	ausente	
1.2	As configurações de profiles de SD-WAN devem partir de um ponto central permitindo alteração e criação dos elementos primordiais para o funcionamento da solução. Deve também entregar a criação automática dos tuneis IPSEC entre as localidades	OK	Página 5	Datasheet – NGFW Security Management Center
1.3	A solução deve permitir operar em caráter de diagrama hub-spoke.	NÃO ENCONTRADO NA DOCUMENTAÇÃO	ausente	

1.4	É considerado diferencial dispositivos que tenha a capacidade de exibir impactos por aplicação.	OK	Página 4	Datasheet – NGFW Security Management Center
1.5	A solução deve permitir ao administrador métricas de utilização de banda por circuito disponível e desta forma exibir no mínimo os seguintes itens em porcentagem ou contadores, jitter, latência e perda de pacote	NÃO ENCONTRADO NA DOCUMENTAÇÃO	ausente	
1.6	O dispositivo deve compreender o que está causando desempenho de degradação para as aplicações e serviços ativos e assim garantir que experiência do usuário sofra o menor impacto possível.	OK	Página 2	Datasheet – NGFW Security Management Center
1.7	O SD-WAN deve suportar os seguintes tipos de conexões WAN: ADSL/DSL, Cable Modem com Ethernet ou fibra, LT /3G/4G/5G, MPLS,Link de rádio e Link satélite desde que a sua terminação permita conectividade com interfaces ethernet.	OK	Página 1	Datasheet - 300 Series
1.8.1	Distribuição de tráfego por prioridade de circuito, circuitos exclusivos de contingenciamento em 3G/4G/5G devem ser utilizados apenas em caso de falha geral dos circuitos ADSL/MPLS.	NÃO ENCONTRADO NA DOCUMENTAÇÃO	ausente	
1.8.2	Distribuição de tráfego de acordo com métricas definidas por origem e destino, o dispositivo deve permitir ao administrador criar perfis com base em latência, jitter ou perda de pacotes para que uma vez que estes limites sejam atingidos o dispositivo possa manter a conexão por circuitos que apresente resultados abaixo dos limites definidos	OK	Página 1	Datasheet - 300 Series
1.8.3	Distribuição de tráfego com balanceamento de sessão entre os circuitos existentes	OK	Página 1	Datasheet - 300 Series
1.9	Quando ambos os pontos de extremidade dos túneis SD-WAN estiverem ativos, deve haver a duplicação de pacotes (PD) para manter a experiência dos usuários mesmo em condição de perda de pacotes. A duplicação de pacotes deve criar uma cópia do fluxo de tráfego do aplicativo e a enviar em ambos os túneis disponiveis que está orientado ao mesmo destino.	NÃO ENCONTRADO NA DOCUMENTAÇÃO	ausente	
1.10	O dispositivo de SD-WAN deve utilizar Forward Error Correction (FEC) habilitado, para permitir que aplicativos sensíveis à perda de pacotes não sejam impactos em caso de perda de pacote e recupere os pacotes perdidos ou corrompidos usando pacotes de paridade incorporados no fluxo da comunicação. O objetivo é reparar o fluxo antes que ele precise fazer failover para outro caminho.	NÃO ENCONTRADO NA DOCUMENTAÇÃO	Ausente	

1.10.1	Distribuição orientada a qualidade, o dispositivo deve validar o melhor caminho disponível e utilizar deste path para manter sessões ativas, caso o melhor caminho entre em de-gradação por fatores anômalos o dispositivo deverá entender estes fatores e distribuir para os demais circuitos existentes.	NÃO ENCONTRADO NA DOCUMENTAÇÃO	ausente	
2	Deve possuir suporte à criação de rede virtuais (VLAN), conforme o padrão IEEE 802.1Q, de, no mínimo, 4.000 (quatro mil) VLANs;	OK	Página 2	Datasheet - 300 Series
3	Deve implementar o protocolo LLDP – Link Layer Discovery Protocol;	OK	11/05/2022	https://help.stonesoft.com/onlinehelp/StoneGate/SMC/6.8.0/GUID-AECC77FF-8441-45DC-8AB5-5D6FBF10F87F.html
4	Deve possuir o recurso de agregação de links conforme padrão IEEE 802.3ad (LACP) permitindo o agrupamento de interfaces físicas de rede em um link agrupado virtualmente (LAG – Link Aggregation Group);	OK	Página 2	DATASHEET – Firewall N335 e N2101
5	Deve possuir o recurso de NAT – Network Address Translation nas modalidades de NAT estático 1 para 1, NAT dinâmico 1 para vários e NAT dinâmico vários para vários. Este recurso deve ser aplicado tanto para o endereço de origem quanto para endereço de destino. Deve possuir também NAT64 para tradução entre endereços IPv6 e IPv4 e NPTv6 (Network Prefix Translation) para tradução de um prefixo IPv6 para outro prefixo IPv6 prevenindo problemas de roteamento assimétrico;	OK	Página 2	DATASHEET – Firewall N335 e N2101
6	Deve suportar a criação de rotas estáticas e os protocolos de roteamento estático e dinâmico RIPv2, OSPFv2 e OSPFv3 incluindo OSPF graceful restart e BGP;	OK	Página 2	DATASHEET – Firewall N335 e N2101
7	Deve implementar o protocolo ECMP – Equal Cost Multiple Path para balanceamento de carga entre links baseados no hash do endereço IP de origem, no hash do endereço IP de origem e de destino, pela técnica conhecida como round-robin e com base no peso ou prioridade atribuído a cada link. Deve suportar o balanceamento entre, no mínimo 4 (quatro) links;	OK	Página 2	DATASHEET – Firewall N335 e N2101
8	Deve permitir o envio de logs para sistemas de monitoração externos utilizando o padrão syslog, bem como o envio de forma segura através do protocolo SSL/TLS;	OK	Página 2	DATASHEET – Firewall N335 e N2101
9	Deve possuir o recurso de alta disponibilidade e permitir a configuração nos modos ativo/passivo e ativo/ativo;	OK	Página 2	DATASHEET – Firewall N335 e N2101
10	Deve implementar controle por políticas/regras de firewall capaz de permitir ou bloquear o tráfego de rede por porta e protocolo, por aplicações, por grupos estáticos de aplicações, por grupos dinâmicos de aplicações baseados em características e comportamento das aplicações, por usuários e grupos de usuários, por endereços IP e faixas de endereços IP e por país de origem e destino do tráfego	OK	Página 2	DATASHEET – Firewall N335 e N2101

11	A identificação do país deve ser através do código do país, por exemplo, BR, USA, UK, RUS, etc e também através de geolocalização possibilitando a criação de regiões geográficas;	OK	Página 2	DATASHEET – Firewall N335 e N2101
12	Deve permitir configurar o agendamento das políticas/regras de firewall para habilitar ou desabilitar tais políticas/regras em horários pré-definidos;	OK	Página 2	DATASHEET – Firewall N335 e N2101
13	Deve possuir a capacidade para realizar a decriptografia do tráfego SSL e SSH permitindo o controle e inspeção tanto do tráfego de entrada quanto de saída. A decriptografia deve ser realizada com base em políticas/regras de acordo com a origem e destino do tráfego;	OK	Página 2	DATASHEET – Firewall N335 e N2101
14	Deve possuir recurso de QoS – Quality of Service com suporte a DSCP – Differentiated Services Code Point. Deve permitir também definir, baseado em políticas/regras, a prioridade e o limite máximo de largura de banda de um determinado tipo de tráfego. As definições de prioridade e limite de largura de banda devem ser baseadas no endereço IP de origem e destino, no usuário e na aplicação;	OK	Página 2	DATASHEET – Firewall N335 e N2101
15	Deve possuir a capacidade de reconhecer, no mínimo, 3.000 (três mil) aplicações diferentes tais como redes sociais, compartilhamento de arquivos, e-mail, atualização de softwares, acesso remoto, VoIP, áudio e vídeo, peer-to-peer, sistemas de mensagem instantânea, etc, sendo esta uma lista não exaustiva;	NÃO ENCONTRADO NA DOCUMENTAÇÃO	ausente	
16	O reconhecimento da aplicação se dará, independentemente de porta e protocolo, através de, no mínimo, os seguintes métodos: baseado na assinatura da aplicação conhecida pelo fabricante da solução de firewall, através da decodificação de protocolos para detectar aplicações encapsuladas dentro do protocolo e identificação através de análise heurística a fim de detectar aplicações através de análise comportamental do tráfego analisado;	OK	Página 2	DATASHEET – Firewall N335 e N2101
17	Deve permitir a criação de assinaturas personalizadas para o reconhecimento de aplicações proprietárias na própria interface gráfica do equipamento sem a necessidade de intervenção do fabricante;	OK	Página 2	DATASHEET – Firewall N335 e N2101
18	Deve permitir a diferenciação e controle de partes da aplicação como, por exemplo, em uma aplicação de mensagem instantânea permitir a troca de mensagens de texto e bloquear a transferência de arquivos por dentro da aplicação;	OK	Página 2	DATASHEET – Firewall N335 e N2101
19	Deve permitir bloquear sessões TCP que utilizarem variações do three-way handshake como fourway e o five-way split handshake, prevenindo assim possíveis tráfegos maliciosos;	OK	Página 2	DATASHEET – Firewall N335 e N2101
20	Deve permitir bloquear conexões que contenham dados no payload dos pacotes TCP SYN e TCP SYN-ACK durante o three-way handshake;	OK	Página 2	DATASHEET – Firewall N335 e N2101

21	A solução de firewall deve possuir funcionalidades de IPS, antivírus e anti-spyware que permita o bloqueio de vulnerabilidades e exploits conhecidos e proteção contra vírus e spywares baseado em assinaturas de ameaças conhecidas;	OK	Página 2	DATASHEET – Firewall N335 e N2101
22	Deve ser possível a criação de assinaturas customizadas de ameaças;	OK	Página 2	DATASHEET – Firewall N335 e N2101
23	Deve permitir realizar o bloqueio de vírus realizando a inspeção em, no mínimo, os protocolos HTTP, FTP, SMB, SMTP e POP3. Será permitido o uso de appliance externo para o bloqueio de vírus caso a solução de firewall ofertada não realize nativamente a inspeção em algum dos protocolos solicitados;	OK	Página 2	DATASHEET – Firewall N335 e N2101
24	Deve possuir a capacidade de detectar e prevenir ameaças em tráfego HTTP/2;	OK	Página 2	DATASHEET – Firewall N335 e N2101
25	Deve possuir proteção contra ataques de negação de serviço (DoS) capaz de impedir ataques de SYN Flood, ICMP Flood, UDP Flood, etc e deve também bloquear port scans, bloquear ataques de buffer overflow e identificar e bloquear comunicação com botnets;	OK	Página 5	Datasheet – NGFW Security Management Center
26	Para cada ameaça detectada pela solução deve ser realizado o registro nos logs do sistema das informações de data e hora, tipo da ameaça, origem e destino da comunicação e a ação tomada (se permitiu ou bloqueou o tráfego);	OK	Página 6	Datasheet – NGFW Security Management Center
27	A solução de firewall deve possuir funcionalidade para análise de malwares não conhecidos (Malware Zero Day) onde o dispositivo envia o arquivo de forma automática para análise na “cloud” ou em um appliance instalado na rede local onde o arquivo será executado e simulado em um ambiente controlado (sandbox);	OK	Página 4	Datasheet – NGFW Security Management Center
28	Caso seja fornecido um appliance local para análise de malwares não conhecidos ele deve possuir, no mínimo, 28 (vinte e oito) ambientes controlados (sandbox) independentes para execução simultânea de arquivos suspeitos;	OK	Página 6	Datasheet – NGFW Security Management Center
29	Caso seja necessário licença de sistema operacional e software para execução de arquivos no ambiente controlado (sandbox) as mesmas devem ser fornecidas em sua totalidade para o seu perfeito funcionamento;	OK	Página 5	Datasheet – NGFW Security Management Center
30	O resultado da análise de malwares não conhecidos deve ter a capacidade de categorizar o arquivo analisado como, no mínimo, um arquivo malicioso, um arquivo não malicioso, mas com características indesejáveis que deixam o sistema operacional lento ou que alteram parâmetros do sistema;	OK	Página 4	Datasheet – NGFW Security Management Center
31	A análise de malwares não conhecidos deve ser realizada em arquivos trafegados na internet através dos protocolos HTTP, HTTPS e FTP bem como em arquivos trafegados entre servidores de arquivos utilizando o protocolo SMB. A análise também deve ser realizada em arquivos anexos em e-mails e links HTTP e HTTPS presentes no corpo de e-mails trafegados utilizando os protocolos SMTP e POP3. A análise do link HTTP e HTTPS presente no corpo do e-mail deve identificar se o website é um hospedeiro de exploits ou atividade de phishing;	OK	Página 4	Datasheet – NGFW Security Management Center

32	Deve suportar a análise dos arquivos em ambientes controlados (sandbox) com, no mínimo, os sistemas operacionais MS Windows 10, MacOS e Linux;	OK	Página 5	Datasheet – NGFW Security Management Center
33	A análise de malwares não conhecidos em ambiente controlado (sandbox) deve ser realizada em arquivos tipo executáveis, DLLs, arquivos compactados RAR e 7-ZIP, arquivos do pacote MS Office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos PDF, arquivos JAVA (.jar e class), arquivos DMG, arquivos ELF e arquivos APK;	OK	Página 7	Datasheet – NGFW Security Management Center
34	Deve atualizar a base de assinaturas para bloqueio dos malwares identificados no ambiente controlado (sandbox) dentro de, no máximo, 5 (cinco) minutos;	OK	Página 6	Datasheet – NGFW Security Management Center
35	A solução de firewall deve possuir funcionalidade de filtro URL que permita a criação de políticas/regras para controle do acesso a websites baseado em categorias de URL devendo o fabricante da solução disponibilizar a base de dados de URL categorizadas para consulta por parte da solução. As políticas/regras que permitem ou bloqueiam o acesso a determinada categoria de URL devem ser com base no usuário e grupos de usuários e por endereços IP e faixas de endereços IP;	OK	Página 4	DATASHEET – Firewall N335 e N2101
36	A funcionalidade de filtro URL deve possuir categoria específica para classificar domínios recém registrados com menos de 30 dias;	OK	Página 3	DATASHEET – Firewall N335 e N2101
37	Deve permitir a criação de categoria de URL customizada permitindo inserir uma lista de URLs específicas;	OK	Página 3	DATASHEET – Firewall N335 e N2101
38	Deve permitir a customização da página de bloqueio exibida ao usuário quando o mesmo tentar realizar um acesso a um website pertencente a uma categoria de URLs bloqueada;	OK	Página 4	DATASHEET – Firewall N335 e N2101
39	Deve possuir recurso para proteger contra o roubo de credenciais de usuário e senha, identificadas através da integração com o Active Directory, submetidas em sites não corporativos. Deve ser possível definir em quais websites é permitido ou bloqueado o envio das credenciais baseado na categoria de URL a qual o website pertencer. Caso o usuário tente submeter suas credenciais de usuário e senhas pertencentes ao Active Directory em um website não autorizado deve ser exibido no web browser do mesmo uma página de bloqueio informando que o uso de tais credenciais no website específico não está autorizado;	NÃO ENCONTRADO NA DOCUMENTAÇÃO	ausente	
40	A solução de firewall deve possuir recurso que permita bloquear a transferência de arquivos baseado na extensão dos mesmos e também definir por qual aplicação a transferência do arquivo está bloqueada, por exemplo, bloquear a transferência de arquivos .exe através de web browser. Deve permitir bloquear, no mínimo, arquivo com as extensões .exe, .bat, .dll, .pif e .torrent;	OK	Página 2	DATASHEET – Firewall N335 e N2101

41	A solução de firewall deve possuir integração com LDAP, MS Active Directoy e RADIUS para identificação dos usuários e grupos da rede para uso nas políticas/regras baseadas por usuários e grupo de usuários;	OK	Página 2	DATASHEET – Firewall N335 e N2101
42	A integração com MS Active Directory para identificação dos usuários da rede deve ser realizada sem a necessidade de instalação de um agente no Controlador de Domínio e nem nas estações dos usuários;	OK	Página 2	DATASHEET – Firewall N335 e N2101
43	A solução de firewall deve possuir recurso de portal de autenticação prévia (Captive Portal) para identificação dos usuários que realizam o acesso à internet, sem a necessidade de instalação de software cliente ou agente no computador. O portal de autenticação deve ser exibido antes de o usuário iniciar a navegação pela internet;	OK	Página 2	DATASHEET – Firewall N335 e N2101
44	A solução de firewall deve possuir o recurso de VPN – Virtual Private Network dos tipos site-tosite e client-to-site e suportar IPSEc – Internet Protocol Security e SSL – Secure Sockets Layer;	OK	Página 2	DATASHEET – Firewall N335 e N2101
45	O recurso de VPN IPSec deve suportar os algoritmos de criptografia 3DES, AES 128, AES 192 e AES 256, os algoritmos de autenticação MD5 e SHA 1, o algoritmo IKEv1 e IKEv2 e os algoritmos de troca de chaves Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 e Grupo 14 e suportar também a autenticação através de certificados IKE PKI;	OK	Página 2	DATASHEET – Firewall N335 e N2101
46	O recurso de VPN SSL deve permitir que o usuário remoto se conecte através de um software cliente de VPN instalado no sistema operacional do equipamento do usuário sendo possível a atribuição de endereços IP fixos e atribuição de DNS ao mesmo;	OK	Página 5	Datasheet – NGFW Security Management Center
47	Deve suportar a autenticação dos usuários remotos que se conectam à VPN via LDAP, MS Active Directory, TACACS+, RADIUS, SAML e através de base de usuários local no equipamento da solução de firewall. Deve suportar também a autenticação via certificado e OTP – One Time Password;	NÃO ENCONTRADO NA DOCUMENTAÇÃO	ausente	
48	Deve ser disponibilizado o software cliente de VPN do mesmo fabricante da solução de firewall ofertada compatível para instalação em computadores com sistema operacional MS Windows 10, MacOS e Linux e para instalação em dispositivos móveis Android e IOS;	OK	Página 5	Datasheet – NGFW Security Management Center
49	O recurso de VPN SSL deve possuir mecanismo de checagem da conformidade do computador do usuário remoto para o firewall tipo 1 e a checagem deve permitir verificar, no mínimo, as informações de qual sistema operacional e patches estão instalados, se o antivírus está instalado e ativo no computador, se o firewall está instalado e ativo no computador, se o disco está criptografado, se o agente de DLP – Data Loss Prevention está instalado e ativo, informações de chaves de registro e processos ativos no computador;	NÃO ENCONTRADO NA DOCUMENTAÇÃO	ausente	
50	Deve ser possível criar perfis customizados de conformidade com, no mínimo, as mesmas informações obtidas pelo mecanismo de checagem da conformidade do computador do usuário remoto. Tais perfis devem ser utilizados para assegurar que apenas computadores de usuários remotos que atendem aos requisitos solicitados nos perfis customizados possam ter acesso através da VPN aos dados e sistemas hospedados na rede interna do órgão;	OK	Página 6	Datasheet – NGFW Security Management Center

51	A solução de firewall deve possuir console de gerenciamento do equipamento acessada através de interface gráfica web permitindo realizar as configurações da solução como criar e administrar as políticas/regras de firewall e controle de aplicações, criar e administrar as políticas de IPS, antivírus e anti-spyware, criar e administrar as políticas de filtro URL, monitorar e investigar os registros de logs de eventos e demais configurações;	OK	Página 2	Datasheet – NGFW Security Management Center
52	Deve suportar a autenticação dos usuários administradores que se conectam à interface de gerenciamento do equipamento via LDAP, MS Active Directory, RADIUS e através de base de usuários local no equipamento da solução de firewall;	OK	Página 2	Datasheet NGFW Security Management Center
53	Deve ser possível criar perfis de acesso à interface de gerenciamento com permissões granulares como acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações entre outros;	OK	Página 3	Datasheet NGFW Security Management Center
54	Deve permitir realizar o backup das configurações do equipamento e a restauração da configuração salva através de interface de gerenciamento;	OK	Página 3	Datasheet NGFW Security Management Center
55	A interface de gerenciamento do equipamento deve possuir recurso para análise das políticas indicando, quando houver, regras que ofusquem, conflitem ou sobreponham outras regas (shadowing) e quais objetos não estão sendo utilizados, para avaliação de elementos dispensáveis, permitindo assim, a higienização gradual das regras e seus respectivos elementos. Deve possuir também recurso para análise das políticas indicando, quando houver, regras baseadas em porta e protocolo, permitindo a conversão da mesma para uma regra baseada em aplicação, melhorando assim o controle do tráfego e a segurança do ambiente;	OK	Página 4	Datasheet NGFW Security Management Center
55.1	É permitido o uso de appliance externo para realização da análise das políticas;	OK	Página 1	Datasheet Next Generation Firewall 300 Series
56	Deve ser possível através de interface de gerenciamento do equipamento a geração de relatórios tais como um resumo gráfico das aplicações utilizadas e ameaças vistas, principais aplicações por utilização de largura de banda, atividades de um usuário ou grupo de usuário específicos incluindo aplicações e URLs acessadas e permitir a criação de relatórios personalizados;	OK	Página 5	Datasheet NGFW Security Management Center
57	Deve ser possível gerar relatório de visibilidade e uso das aplicações do tipo SaaS – Software as a Service mostrando 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 a aplicação SaaS e o consumo da aplicação SaaS pelo usuário;	OK	Página 5	Datasheet NGFW Security Management Center

58	Deve ser exibida na interface gráfica de gerenciamento do equipamento informações em tempo real, atualizadas de forma automática a cada 1 (um) minuto, as principais aplicações acessadas, o risco das principais aplicações, número de sessões simultâneas, status das interfaces de rede e uso de CPU;	OK	Página 5	Datasheet NGFW Security Management Center
59	Deve ser possível configurar o envio de alertas do sistema via e-mail;	OK	Página 3	Datasheet NGFW Security Management Center
60	Deve suportar o monitoramento via SNMPv3;	OK	Página 6	Datasheet NGFW Security Management Center
61	O sistema operacional a ser instalado no equipamento que compõe a solução deverá ser fornecido em sua versão mais atualizada, não sendo aceito sistema operacional de uso genérico;	OK	Página 1	Datasheet Next Generation Firewall 300 Series
62	Por cada equipamento que compõe a solução de segurança, entende-se o hardware e as licenças de softwares necessárias para o seu funcionamento;	OK		Proposta comercial
63	Na data do certame, nenhum dos equipamentos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;	NÃO ENCONTRADO NA DOCUMENTAÇÃO	ausente	Não encontrada referência de end-of-life e end-of-sale para os produtos propostos
64	Durante o período de vigência do contrato de garantia todos os componentes da solução de firewall, incluindo o equipamento, o sistema operacional do mesmo, as licenças necessárias para atender as funcionalidades e recursos solicitados, os softwares clientes de VPN e demais itens necessários para o perfeito funcionamento devem estar cobertos por garantia e suporte técnico do fabricante da solução em caso de problema;	OK		Proposta comercial
65	A solução de firewall deve possuir garantia pelo período de, no mínimo, 36 (trinta e seis) meses, compreendendo a reposição de peças/equipamentos, atualizações do sistema operacional do equipamento e demais software e das assinaturas de proteção da solução.	OK		Proposta comercial

EMPRESA: ASGS Seg. em Tecnologia da Inf. Ltda

Item I - Firewall tipo III (11 unidades) – Equipamento proposto: Palo Alto Network PA410 – garantia e licenciamento de 36 meses

	Característica	Parecer	Validação	Local
1	A solução deve consistir de appliance de proteção de rede com funcionalidades de Next Generation .Firewall (NGFW) tais como reconhecimento e controle de aplicações, identificação de usuários, prevenção contra ameaças de vírus, spywares e malwares desconhecidos (Zero Day), IPS, filtro de URL e recursos de VPN;	OK	Páginas: 18,19,19,20	Datasheet PA-400 Series
2	O hardware e software que executem as funcionalidades de proteção de rede devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;	OK	Página 18	Datasheet PA-400 Series
3	Deve possuir throughput de, no mínimo, 1 (um) Gbps com a funcionalidade de controle de aplicação para todas as assinaturas que o fabricante possuir;	OK	Página 18	Datasheet PA-400 Series
4	Deve possuir throughput de, no mínimo, 500 (quinhentos) Mbps com as funcionalidades de controle de aplicação, IPS, Antivírus e Anti-Spyware habilitadas simultaneamente na solução. A comprovação se dará através de documentação técnica do fabricante de acesso público informando os throughput aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real;	OK	Página 18	Datasheet PA-400 Series
5	Deve suportar, no mínimo, 60.000 (sessenta mil) conexões simultâneas	OK	Página 18	Datasheet PA-400 Series
6	Deve suportar, no mínimo, 11.000 (onze mil) novas conexões por segundo	OK	Página 18	Datasheet PA-400 Series
7	Deve possuir, no mínimo, 7 (sete) interfaces físicas de rede de 1 Gbps do tipo RJ-45;	OK	Página 19	Datasheet PA-400 Series
8	Deve possuir, no mínimo, 1 (uma) interface física de rede de 1 Gbps dedicada para gerenciamento, caso não possua a interface dedicada, será aceito utilizar interfaces físicas de rede de 1Gbps do tipo RJ-45, desde que o equipamento possua um número maior que o mínimo solicitado na alínea "7" desse item	OK	Página 19	Datasheet PA-400 Series
9	Deve possuir, no mínimo, 1 (uma) interface física do tipo console ou similar;	OK	Página 19	Datasheet PA-400 Series
10	Deve possuir, no mínimo, 64 (sessenta e quatro) GB de armazenamento interno;	OK	11/05/2022	https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-400-series
11	Deve possuir fonte de alimentação elétrica capaz de operar entre 120 à 240 VAC;	OK	11/05/2022	https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-400-series

12	Deve suportar, no mínimo, 200 (duzentos) clientes de VPN SSL simultaneamente estando, caso necessário, devidamente licenciado para este fim;	OK	Página 20	Datasheet PA-400 Series
13	Deve suportar, no mínimo, 200 (duzentos) túneis de VPN IPSEC simultaneamente estando, caso necessário, devidamente licenciado para este fim;	OK	Página 21	Datasheet PA-400 Series

Item II - Firewall tipo II (02 unidades) – Equipamento proposto: Palo Alto Network PA440 – garantia e licenciamento de 36 meses

	Característica	Parecer	Validação	Local
1	A solução deve consistir de appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW) tais como reconhecimento e controle de aplicações, identificação de usuários, prevenção contra ameaças de vírus, spywares e malwares desconhecidos (Zero Day), IPS, filtro de URL e recursos de VPN	OK	Páginas: 21,22,23,24	Datasheet PA-400 Series
2	O hardware e software que executem as funcionalidades de proteção de rede devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;	OK	Página 21	Datasheet PA-400 Series
3	O equipamento deve ser fornecido com kit que permita a sua montagem em rack 19”;	OK	11/05/2022	https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-400-series
4	Deve possuir throughput de, no mínimo, 1.6 (um ponto seis) Gbps com a funcionalidade de controle de aplicação para todas as assinaturas que o fabricante possuir;	OK	Página 21	Datasheet PA-400 Series
5	Deve possuir throughput de, no mínimo, 850 (oitocentos e cinquenta) Mbps com as funcionalidades de controle de aplicação, IPS, Antivírus e Anti-Spyware habilitadas simultaneamente na solução. A comprovação se dará através de documentação técnica do fabricante de acesso público informando os throughput aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real;	OK	Página 21	Datasheet PA-400 Series
6	Deve suportar, no mínimo, 190.000 (cento e noventa mil) conexões simultâneas;	OK	Página 21	Datasheet PA-400 Series
7	Deve suportar, no mínimo, 35.000 (trinta e cinco mil) novas conexões por segundo;	OK	Página 21	Datasheet PA-400 Series
8	Deve possuir, no mínimo, 8 (oito) interfaces físicas de rede de 1 Gbps do tipo RJ-45;	OK	Página 23	Datasheet PA-400 Series
9	Deve possuir, no mínimo, 1 (uma) interface física de rede de 1 Gbps dedicada para gerenciamento;	OK	Página 23	Datasheet PA-400 Series
10	Deve possuir, no mínimo, 1 (uma) interface física do tipo console ou similar;	OK	Página 23	Datasheet PA-400 Series
11	Deve possuir, no mínimo, 128 (cento e vinte e oito) GB de armazenamento interno para o sistema operacional e registro de logs;	OK	11/05/2022	https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-400-series

12	Deve possuir fonte de alimentação elétrica redundante capaz de operar entre 120 à 240 VAC e devendo, em caso de problema com uma das fontes, permitir a substituição da fonte defeituosa com o equipamento em funcionamento;	OK	11/05/2022	https://paloaltofirewalls.co.uk/product/palo-alto-networks-enterprise-firewall-pa-440/
13	Deve suportar, no mínimo, 500 (quinhentos) clientes de VPN SSL simultaneamente estando, caso necessário, devidamente licenciado para este fim;	OK	11/05/2022	https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PPBCCA4
14	Deve suportar, no mínimo, 200 (duzentos) túneis de VPN IPSEC simultaneamente estando, caso necessário, devidamente licenciado para este fim;	OK	Página 24	Datasheet PA-400 Series

Item III - Firewall tipo I (02 unidades) – Equipamento proposto: Palo Alto Network PA460 – garantia e licenciamento de 36 meses

	Característica	Parecer	Validação	Local
1	A solução deve consistir de appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW) tais como reconhecimento e controle de aplicações, identificação de usuários, prevenção contra ameaças de vírus, spywares e malwares desconhecidos (Zero Day), IPS, filtro de URL e recursos de VPN;	OK	Páginas: 25,26,27,28	Datasheet PA-400 Series
2	O hardware e software que executem as funcionalidades de proteção de rede devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;	OK	Página 25	Datasheet PA-400 Series
3	O equipamento deve ser fornecido com kit que permita a sua montagem em rack 19”;	OK	11/05/2022	https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-400-series
4	Deve possuir throughput de, no mínimo, 4.4 (quatro ponto quatro) Gbps com a funcionalidade de controle de aplicação para todas as assinaturas que o fabricante possuir;	OK	Página 25	Datasheet PA-400 Series
5	Deve possuir throughput de, no mínimo, 2.1 (dois ponto um) Gbps com as funcionalidades de controle de aplicação, IPS, Antivírus e Anti-Spyware habilitadas simultaneamente na solução. A comprovação se dará através de documentação técnica do fabricante de acesso público informando os throughput aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real;	OK	Página 25	Datasheet PA-400 Series
6	Deve suportar, no mínimo, 400.000 (quatrocentos mil) conexões simultâneas;	OK	Página 25	Datasheet PA-400 Series
7	Deve suportar, no mínimo, 70.000 (setenta mil) novas conexões por segundo;	OK	Página 25	Datasheet PA-400 Series

8	Deve possuir, no mínimo, 8 (oito) interfaces físicas de rede de 1 Gbps do tipo RJ-45;	OK	Página 26	Datasheet PA-400 Series
9	Deve possuir, no mínimo, 1 (uma) interface física de rede de 1 Gbps dedicada para gerenciamento;	OK	Página 26	Datasheet PA-400 Series
10	Deve possuir, no mínimo, 1 (uma) interface física do tipo console ou similar;	OK	Página 26	Datasheet PA-400 Series
11	Deve possuir, no mínimo, 128 (cento e vinte e oito) GB de armazenamento interno para o sistema operacional e registro de logs;	OK	11/05/2022	https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-400-series
12	Deve possuir fonte de alimentação elétrica redundante capaz de operar entre 120 à 240 VAC e devendo, em caso de problema com uma das fontes, permitir a substituição da fonte defeituosa com o equipamento em funcionamento;	OK	11/05/2022	https://paloaltofirewalls.co.uk/product/palo-alto-networks-enterprise-firewall-pa-460/
13	Deve suportar, no mínimo, 1.500 (hum mil e quinhentos) clientes de VPN SSL simultaneamente estando, caso necessário, devidamente licenciado para este fim;	OK	Página 28	Datasheet PA-400 Series
14	Deve suportar, no mínimo, 2,000 (dois mil) túneis de VPN IPSEC simultaneamente estando, caso necessário, devidamente licenciado para este fim;	OK	Página 28	Datasheet PA-400 Series

Item IV – Solução de proteção avançada de Endpoint (300 unidades) – Proposto: Palo Alto Networks – Cortex xDR + Host Insight – garantia e licenciamento de 36 meses.

	Característica	Parecer	Validação	Referência
1	Solução de proteção avançada de endpoint através da instalação de um agente nos endpoints (entende por endpoint uma estação de trabalho ou servidor de rede) para proteção contra exploits, malware, ransomware e console central de gerenciamento dos agentes;	OK	Página 55/64	Datasheet Cortex XDR
2	O console central de gerenciamento dos agentes instalados nos endpoints deve ser baseado em nuvem e acessado através de web browser;	OK	Página 59/60	Datasheet Cortex XDR
3	Deve prevenir contra ameaças conhecidas baseado em assinatura;	OK	Página 56	Datasheet Cortex XDR
4	Deve prevenir contra ameaças baseada em comportamento através do monitoramento das atividades realizadas pelo endpoint;	OK	Página 56	Datasheet Cortex XDR
5	Deve prevenir contra ameaças através do uso de machine learning através da análise local de arquivos desconhecidos;	OK	Página 49	Datasheet Cortex XDR
6	Deve possuir integração com serviço de análise de malwares desconhecidos em nuvem para uma análise mais profunda dos arquivos. O serviço de análise em nuvem pode ser do mesmo fabricante da solução de proteção avançada de endpoint ou de fabricantes terceiros devendo ser fornecidas todas as licenças necessárias para o seu perfeito funcionamento;	OK	Página 54	Datasheet Cortex XDR Overview

7	O serviço de análise de malwares desconhecidos em nuvem deve realizar a análise de, no mínimo, os seguintes tipos de arquivos: arquivos executáveis, DLLs, arquivos Word (.doc, .docm e docx) e Excel (.xls, .xlsm e .xlsx) que contenham macros, arquivos DMG;	OK	11/05/2022	https://www.paloaltonetworks.com/blog/security-operations/detecting-vba-process-hollowing-with-cortex-xdr/
8	Deve possuir mecanismos para detectar, em tempo real, ataques LotL – Living off the Land, ataques baseados em scripts e ataques fileless;	OK	Página 7	Datasheet Cortex XDR
9	Deve prevenir contra exploits incluindo Heap Spray, DEP – Data Execution Protection, ROP – Return-oriented Programming e exploits baseados em JIT – Just-in-time;	OK	11/05/2022	https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-prevent-admin/endpoint-security/endpoint-protection-modules
10	Deve permitir bloquear o uso dispositivos portáteis USB como pen drivers, discos, drivers de CDROM nos endpoints para prevenir contra a transferência de arquivos maliciosos que possam estar nestes dispositivos;	OK	Página 47	Datasheet Cortex XDR
11	Deve possuir host firewall permitindo o controle da comunicação do endpoint através de regras de permissão e bloqueio do tráfego;	OK	Página 48	Datasheet Cortex XDR
12	Deve permitir executar a varredura no endpoint em busca de arquivos infectados por malware a partir do console central de gerenciamento e a partir do próprio agente instalado no endpoint. Deve ser possível também configurar varreduras agendadas;	OK	11/05/2022 Página 48	https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/investigation-and-response/investigate-endpoints/scan-endpoint-for-malware
13	A atualização do motor de detecção de ameaças deve ser realizada de forma transparente para o usuário;	OK	11/05/2022 Página 48	https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-prevent-admin/endpoint-security/about-content-updates
14	Deve exibir lista com todos os alertas de incidentes detectados pelos agentes instalados nos endpoints no console central de gerenciamento. Deve mostrar, para cada alerta da lista, no mínimo, a data e hora que o incidente ocorreu, o nome ou endereço IP do endpoint, a ação tomada pelo agente 17 com relação ao incidente e a categoria do incidente informando se o mesmo se trata de, por exemplo, um exploit ou um malware;	OK	11/05/2022	https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/endpoint-security/customizable-agent-settings/endpoint-data-collected-by-cortex-xdr
15	Deve ser possível visualizar a cadeia de processos executados que levaram a geração do alerta exibindo o primeiro processo executado o qual foi responsável pela execução dos demais processos. Para cada processo executado deve ser possível visualizar, no mínimo, o caminho onde o processo estava localizado (por exemplo c:/temp/pe.exe), o nome do usuário que iniciou o processo e o tempo em que o processo ficou em execução informando a data e hora do início e do fim da execução do mesmo;	OK	11/05/2022	https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/investigation-and-response/investigate-endpoint-alerts/timeline-view
16	Deve ser possível também visualizar, em uma linha do tempo, todos os processos e eventos, desde a execução do primeiro processo responsável pela execução dos demais, que geraram um alerta de incidente. Os tipos de eventos que devem ser exibidos, além de processos executados, são conexões de entrada e saída, conexões fracassadas e download e upload de dados;	OK	11/05/2022	https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/investigation-and-response/investigate-endpoint-alerts/timeline-view

17	A solução deve possuir integração com o firewall de próxima geração em processo de compra desse edital e que será utilizado por este órgão para correlação dos eventos e alertas gerados pelo firewall permitindo visualizar na cadeia de processos executados de um determinado alerta as informações de acessos externos realizados pelos processos e atividades maliciosos detectados pela solução;	OK	11/05/2022	https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/investigation-and-response/investigate-endpoint-alerts/timeline-view
18	Deve possuir ferramenta de busca para a investigação de incidentes permitindo a realização de buscas com base em, no mínimo, processos executados, em arquivos criados, alterados e deletados, em atributos de rede como endereço IP, nome do host, porta e protocolo, em registros criados, modificados e deletados, em eventos de log do Windows e Linux. Deve permitir também realizar a busca através da combinação dos diversos atributos descritos anteriormente;	OK	11/05/2022	https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/investigation-and-response/investigate-endpoint-alerts/timeline-view
19	A solução deve permitir realizar a configuração de alertas com base em incidentes com base em indicadores de comprometimento (IOCs). Os tipos de indicadores de comprometimento que podem ser criados pelo administrador da solução devem ser, no mínimo, nome do arquivo, domínio e endereço IP de destino. Além de permitir a criação dos indicadores de comprometimento a solução deve permitir também importar listas de indicadores de comprometimentos de serviços externos de inteligência contra ameaça;	OK	Página 7	Datasheet Cortex XDR
20	A solução deve permitir realizar a configuração de alertas com base em incidentes com base em indicadores de comprometimento baseados no comportamento do endpoint. Os tipos de comportamentos que devem ser detectados são, no mínimo, execução de processos, manipulação de privilégios em arquivo, ofuscação do tipo do arquivo, atividade de reconhecimento na rede, escalonamento de privilégio e movimentos laterais na rede.	OK	Página 7/8	Datasheet Cortex XDR
21	A solução deve permitir, realizar o acesso diretamente aos endpoints através de um terminal remoto para execução de ações para investigação e repostas aos incidentes de segurança. As ações que podem ser executadas através do terminal remoto devem ser, no mínimo, visualizar e encerrar processos que estão sendo executados no endpoint, apagar, mover e renomear arquivos localizados no endpoint, prover interface de linha de comando para execução de comandos do sistema operacional, prover interface de linha de comando para execução de scripts e comandos Pyhton. Ao final da sessão de acesso ao endpoint dever se possível salvar um relatório contendo todas as atividades realizadas durante a sessão;	OK	Página 10	Datasheet Cortex XDR
22	Deve ser possível também realizar, a partir do console central de gerenciamento, a execução de scripts em diversos endpoints simultaneamente de forma centralizada;	OK	Página 10	Datasheet Cortex XDR

23	A solução deve permitir, a partir do console central de gerenciamento, isolar um endpoint impedindo a comunicação do mesmo com a rede para evitar que um possível ataque se propague pela rede;	OK	Página 10	Datasheet Cortex XDR
24	Deve ser possível a correlação com a lista de CVE – Common Vulnerabilities and Exposures conhecidos e permitir visualizar quais endpoints estão sendo afetados por uma determinada CVE;	OK	Página 6	Datasheet Cortex XDR
25	A solução deve permitir, a partir da console central de gerenciamento, a realização de busca de um determinado arquivo em todos os endpoints. A busca pode ser realizada com base no caminho completo onde o arquivo pode estar presente (c:\windows\system32\file.exe) e também com base 18 no hash do arquivo gerado pela solução. Deve ser possível ainda, a partir da console central de gerenciamento, apagar o arquivo de todos os endpoints onde ele está presente;	OK	Página 8	Datasheet Cortex XDR
26	A solução deve armazenar as informações de alertas, incidentes e suas respectivas atividades e ações e demais dados relacionados aos eventos de segurança detectados por um período de, no mínimo, 30 (trinta) dias;	OK	11/05/2022	https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-prevent-admin/get-started-with-cortex-xdr-prevent/allocate-log-storage-for-cortex-xdr
27	A solução deve permitir a instalação do agente em endpoints com sistema operacional MS Windows 8.1, MS Windows 10, MS Windows Server 2016, MS Windows Server 2019, nas principais distribuições Linux como CentOS, Debian, Red Hat e SUSE nos sistemas operacionais MacOS e MacOS X;	OK	11/05/2022 Página 59	https://docs.paloaltonetworks.com/compatibility-matrix/cortex-xdr/where-can-i-install-the-cortex-xdr-agent
28	A solução deve permitir realizar o upgrade dos agentes instalados nos endpoints a partir do console central de gerenciamento;	OK	11/05/2022 Página 59	https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/endpoint-security/manage-cortex-xdr-agents/upgrade-the-cortex-agent
29	A solução deve possuir subscrição pelo período de, no mínimo, 36 (meses) permitindo, durante este período, acesso ilimitado ao console central de gerenciamento na nuvem, acesso a todas as atualização e serviços de segurança e assinaturas de proteção da solução e o pleno funcionamento do agente de proteção instalado no endpoint.	OK	11/05/2022	https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/cortex-xdr-overview/cortex-xdr-licenses/cortex-xdr-license-allocation#cortex-xdr-license-allocation

Item V – Software de gerenciamento centralizado e armazenamento de logs (1 unidade) – Proposto: Palo Alto Networks Panorama – garantia e licenciamento de 36 meses.

	Característica	Parecer	Validação	Referência
1	Deve ser fornecido solução de gerenciamento centralizado, possibilitando o gerenciamento de diversos equipamentos de firewall de mesmo fabricante da solução;	OK	Página 4	Datasheet Panorama

2	A solução de gerenciamento centralizado deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos de firewall gerenciados pela solução, além de consolidar os registros de eventos (logs) e relatórios de todos os equipamentos que compõem a solução de proteção de rede;	OK	11/05/2022	https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-web-interface-help/panorama-web-interface/panorama-log-settings
3	Deve ser homologado e totalmente compatível com a Solução de Proteção de Rede Firewall especificada neste Termo de Referência para permitir o gerenciamento centralizado e armazenamento de logs do mesmo, estando devidamente licenciado para este fim;	OK	Página 3	Datasheet Panorama
4	Deve permitir o controle sobre todos os equipamentos de firewall em uma única console, com administração de privilégios e funções;	OK	Página 4	Datasheet Panorama
5	O gerenciamento centralizado poderá ser entregue como appliance físico ou virtual. Caso seja entregue em appliance físico ele deve ser compatível com rack 19 polegadas e possuir todos os acessórios necessários para sua instalação. Caso seja entregue em appliance virtual deve ser compatível com VMware ESXi;	OK	Página 4	Datasheet Panorama
6	Deve permitir o armazenamento de logs sem limite de tempo nem limite da quantidade de logs diários a ser recebido ou armazenado, considerando que a infra do SENAR-PR possa vir a absorver o mesmo crescimento. Caso seja necessário licenciamento adicional, deverá ser entregue licenciado com a maior capacidade suportada;	OK	Página 5	Datasheet Panorama
7	Deve permitir controle global de políticas para todos os equipamentos gerenciados pela solução;	OK	Página 3	Datasheet Panorama
8	Deve suportar organizar os equipamentos gerenciados em grupos: os sistemas virtuais devem ser administrados como dispositivos individuais, os grupos podem ser geográficos, por funcionalidade (por exemplo, IPS), e distribuição;	OK	Página 4	Datasheet Panorama
9	Deve implementar sistema de hierarquia entre os equipamentos gerenciados, onde seja possível aplicar configurações de forma granular em grupos de firewalls;	OK	Página 4	Datasheet Panorama
10	Deve implementar a criação de perfis de usuários com acesso a solução de gerenciamento com definição exata de quais informações e de quais equipamento de firewalls e grupos de equipamentos de firewalls o usuário terá acesso referente a logs e relatórios;	OK	11/05/2022	https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/panorama-web-interface/panorama-administrators
11	Deve permitir a criação de objetos e políticas compartilhadas;	OK	Página 4	Datasheet Panorama
12	Deve consolidar logs e relatórios de todos os equipamentos de firewall gerenciados;	OK	Página 4	Datasheet Panorama
13	Deve permitir exportar o backup de configuração automaticamente via agendamento;	OK	11/05/2022	https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/administer-panorama/manage-panorama-and-firewall-configuration-backups/schedule-export-of-configuration-files

14	Deve permitir que a configuração dos firewalls seja importada de forma automática na solução de gerenciamento centralizado e que possa ser usada em outros firewalls e grupos de firewalls;	OK	11/05/2022	https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/administer-panorama/manage-panorama-and-firewall-configuration-backups/load-a-configuration-backup-on-a-managed-firewall
15	Deve mostrar os status dos equipamentos de firewalls em alta disponibilidade a partir da solução de gerenciamento centralizado;	OK	11/05/2022	https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/manage-firewalls/device-monitoring-on-panorama/monitor-device-health#id181JD0DD0C1
16	Dever permitir salvar no mínimo 15 Tb de dados de Logs dos equipamentos por ele administrados, permitindo a pesquisa e filtragem de dados dos últimos 180 dias;	OK	Página 6	Datasheet Panorama
17	Deve estar licenciado para no mínimo 15 devices;	OK	11/05/2022	https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/set-up-panorama/register-panorama-and-install-licenses
18	A solução de gerenciamento centralizado e armazenamento de logs deve possuir garantia pelo período de, no mínimo, 36 (trinta e seis) meses, compreendendo a atualização do software para obter novas funcionalidades e correções de bugs.	OK	11/05/2022	https://live.paloaltonetworks.com/t5/blogs/log-retention/ba-p/306150

Anexo II – Características obrigatórias mínimas comuns para os objetos: Item I, item II e item III

	Característica	Parecer	Validação	Referência
1	Deve operacionalizar no mínimo os seguintes critérios de SD-WAN	OK	Página 1	Datasheet PAN-OS SD-WAN
1.1	A plataforma de segurança deverá recuperar pacotes perdidos antes que seja necessário alterar o caminho principal.	OK	Página 3	Datasheet PAN-OS SD-WAN
1.2	As configurações de profiles de SD-WAN devem partir de um ponto central permitindo alteração e criação dos elementos primordiais para o funcionamento da solução. Deve também entregar a criação automática dos tuneis IPSEC entre as localidades	OK	Página 4	Datasheet PAN-OS SD-WAN
1.3	A solução deve permitir operar em caráter de diagrama hub-spoke.	OK	Página 4	Datasheet PAN-OS SD-WAN
1.4	É considerado diferencial dispositivos que tenha a capacidade de exibir impactos por aplicação.	OK	Página 4	Datasheet PAN-OS SD-WAN
1.5	A solução deve permitir ao administrador métricas de utilização de banda por circuito disponível e desta forma exibir no mínimo os seguintes itens em porcentagem ou contadores, jitter, latência e perda de pacote	OK	Página 4	Datasheet PAN-OS SD-WAN
1.6	O dispositivo deve compreender o que está causando desempenho de degradação para as aplicações e serviços ativos e assim garantir que experiência do usuário sofra o menor impacto possível.	OK	Página 4	Datasheet PAN-OS SD-WAN

1.7	O SD-WAN deve suportar os seguintes tipos de conexões WAN: ADSL/DSL, Cable Modem com Ethernet ou fibra, LT /3G/4G/5G, MPLS,Link de rádio e Link satélite desde que a sua terminação permita conectividade com interfaces ethernet.	OK	11/05/2022	https://docs.paloaltonetworks.com/sd-wan/2-1/sd-wan-admin/sd-wan-overview/about-sd-wan
1.8.1	Distribuição de tráfego por prioridade de circuito, circuitos exclusivos de contingenciamento em 3G/4G/5G devem ser utilizados apenas em caso de falha geral dos circuitos ADSL/MPLS.	OK	11/05/2022	https://docs.paloaltonetworks.com/sd-wan/2-1/sd-wan-admin/sd-wan-overview/about-sd-wan
1.8.2	Distribuição de tráfego de acordo com métricas definidas por origem e destino, o dispositivo deve permitir ao administrador criar perfis com base em latência, jitter ou perda de pacotes para que uma vez que estes limites sejam atingidos o dispositivo possa manter a conexão por circuitos que apresente resultados abaixo dos limites definidos	OK	11/05/2022	https://docs.paloaltonetworks.com/sd-wan/2-1/sd-wan-admin/sd-wan-overview/about-sd-wan
1.8.3	Distribuição de tráfego com balanceamento de sessão entre os circuitos existentes	OK	11/05/2022	https://docs.paloaltonetworks.com/sd-wan/2-1/sd-wan-admin/sd-wan-overview/about-sd-wan
1.9	Quando ambos os pontos de extremidade dos túneis SD-WAN estiverem ativos, deve haver a duplicação de pacotes (PD) para manter a experiência dos usuários mesmo em condição de perda de pacotes. A duplicação de pacotes deve criar uma cópia do fluxo de tráfego do aplicativo e a enviar em ambos os túneis disponiveis que está orientado ao mesmo destino.	OK	11/05/2022	https://docs.paloaltonetworks.com/sd-wan/2-1/sd-wan-admin/sd-wan-overview/about-sd-wan
1.10	O dispositivo de SD-WAN deve utilizar Forward Error Correction (FEC) habilitado, para permitir que aplicativos sensíveis à perda de pacotes não sejam impactos em caso de perda de pacote e recupere os pacotes perdidos ou corrompidos usando pacotes de paridade incorporados no fluxo da comunicação. O objetivo é reparar o fluxo antes que ele precise fazer failover para outro caminho.	OK	11/05/2022	https://docs.paloaltonetworks.com/sd-wan/2-1/sd-wan-admin/sd-wan-overview/about-sd-wan
1.10.1	Distribuição orientada a qualidade, o dispositivo deve validar o melhor caminho disponível e utilizar deste path para manter sessões ativas, caso o melhor caminho entre em de-gradação por fatores anômalos o dispositivo deverá entender estes fatores e distribuir para os demais circuitos existentes.	OK	11/05/2022	https://docs.paloaltonetworks.com/sd-wan/2-1/sd-wan-admin/sd-wan-overview/about-sd-wan
2	Deve possuir suporte à criação de rede virtuais (VLAN), conforme o padrão IEEE 802.1Q, de, no mínimo, 4.000 (quatro mil) VLANs;	OK	Página 5	Datasheet PA-400
3	Deve implementar o protocolo LLDP – Link Layer Discovery Protocol;	OK	11/05/2022	https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/networking/lldp/lldp-overview#iddcfc6476-04f0-4a7f-9181-2353d6c5cede

4	Deve possuir o recurso de agregação de links conforme padrão IEEE 802.3ad (LACP) permitindo o agrupamento de interfaces físicas de rede em um link agrupado virtualmente (LAG – Link Aggregation Group);	OK	11/05/2022	https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/networking/configure-interfaces/configure-an-aggregate-interface-group
5	Deve possuir o recurso de NAT – Network Address Translation nas modalidades de NAT estático 1 para 1, NAT dinâmico 1 para vários e NAT dinâmico vários para vários. Este recurso deve ser aplicado tanto para o endereço de origem quanto para endereço de destino. Deve possuir também NAT64 para tradução entre endereços IPv6 e IPv4 e NPTv6 (Network Prefix Translation) para tradução de um prefixo IPv6 para outro prefixo IPv6 prevenindo problemas de roteamento assimétrico;	OK	11/05/2022	https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/networking/nat
6	Deve suportar a criação de rotas estáticas e os protocolos de roteamento estático e dinâmico RIPv2, OSPFv2 e OSPFv3 incluindo OSPF graceful restart e BGP;	OK	Página 4	Datasheet PA-400
7	Deve implementar o protocolo ECMP – Equal Cost Multiple Path para balanceamento de carga entre links baseados no hash do endereço IP de origem, no hash do endereço IP de origem e de destino, pela técnica conhecida como round-robin e com base no peso ou prioridade atribuído a cada link. Deve suportar o balanceamento entre, no mínimo 4 (quatro) links;	OK	11/05/2022	https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/networking/ecmp
8	Deve permitir o envio de logs para sistemas de monitoração externos utilizando o padrão syslog, bem como o envio de forma segura através do protocolo SSL/TLS;	OK	Página 4	Datasheet PAN-OS SD-WAN
9	Deve possuir o recurso de alta disponibilidade e permitir a configuração nos modos ativo/passivo e ativo/ativo;	OK	Página 1	Datasheet PA-400
10	Deve implementar controle por políticas/regras de firewall capaz de permitir ou bloquear o tráfego de rede por porta e protocolo, por aplicações, por grupos estáticos de aplicações, por grupos dinâmicos de aplicações baseados em características e comportamento das aplicações, por usuários e grupos de usuários, por endereços IP e faixas de endereços IP e por país de origem e destino do tráfego	OK	11/05/2022	https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/policy/security-policy
11	A identificação do país deve ser através do código do país, por exemplo, BR, USA, UK, RUS, etc e também através de geolocalização possibilitando a criação de regiões geográficas;	OK	11/05/2022	https://docs.paloaltonetworks.com/autofocus/autofocus-api/perform-direct-searches/get-geolocation
12	Deve permitir configurar o agendamento das políticas/regras de firewall para habilitar ou desabilitar tais políticas/regras em horários pré-definidos;	OK	11/05/2022	https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/objects/objects-schedules
13	Deve possuir a capacidade para realizar a decriptografia do tráfego SSL e SSH permitindo o controle e inspeção tanto do tráfego de entrada quanto de saída. A decriptografia deve ser realizada com base em políticas/regras de acordo com a origem e destino do tráfego;	OK	11/05/2022	https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/decryption/decryption-concepts/ssl-inbound-inspection

14	Deve possuir recurso de QoS – Quality of Service com suporte a DSCP – Differentiated Services Code Point. Deve permitir também definir, baseado em políticas/regras, a prioridade e o limite máximo de largura de banda de um determinado tipo de tráfego. As definições de prioridade e limite de largura de banda devem ser baseadas no endereço IP de origem e destino, no usuário e na aplicação;	OK	Página 3	Datasheet PAN-OS SD-WAN
15	Deve possuir a capacidade de reconhecer, no mínimo, 3.000 (três mil) aplicações diferentes tais como redes sociais, compartilhamento de arquivos, e-mail, atualização de softwares, acesso remoto, VoIP, áudio e vídeo, peer-to-peer, sistemas de mensagem instantânea, etc, sendo esta uma lista não exaustiva;	OK	11/05/2022	https://applipedia.paloaltonetworks.com/
16	O reconhecimento da aplicação se dará, independentemente de porta e protocolo, através de, no mínimo, os seguintes métodos: baseado na assinatura da aplicação conhecida pelo fabricante da solução de firewall, através da decodificação de protocolos para detectar aplicações encapsuladas dentro do protocolo e identificação através de análise heurística a fim de detectar aplicações através de análise comportamental do tráfego analisado;	OK	Página 2	Datasheet App-ID
17	Deve permitir a criação de assinaturas personalizadas para o reconhecimento de aplicações proprietárias na própria interface gráfica do equipamento sem a necessidade de intervenção do fabricante;	OK	Página 3	Datasheet App-ID
18	Deve permitir a diferenciação e controle de partes da aplicação como, por exemplo, em uma aplicação de mensagem instantânea permitir a troca de mensagens de texto e bloquear a transferência de arquivos por dentro da aplicação;	OK	Página 5	Datasheet App-ID
19	Deve permitir bloquear sessões TCP que utilizarem variações do three-way handshake como fourway e o five-way split handshake, prevenindo assim possíveis tráfegos maliciosos;	OK	11/05/2022	https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/networking/session-settings-and-timeouts/tcp/tcp-split-handshake-drop
20	Deve permitir bloquear conexões que contenham dados no payload dos pacotes TCP SYN e TCP SYN-ACK durante o three-way handshake;	OK	11/05/2022	https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/network/network-network-profiles/network-network-profiles-zone-protection/packet-based-attack-protection/tcp-drop
21	A solução de firewall deve possuir funcionalidades de IPS, antivírus e anti-spyware que permita o bloqueio de vulnerabilidades e exploits conhecidos e proteção contra vírus e spywares baseado em assinaturas de ameaças conhecidas;	OK	Página 915	https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/10-2/pan-os-admin/pan-os-admin.pdf
22	Deve ser possível a criação de assinaturas customizadas de ameaças;	OK	11/05/2022	https://docs.paloaltonetworks.com/pan-os/u-v/custom-app-id-and-threat-signatures/custom-application-and-threat-signatures/create-a-custom-threat-signature
23	Deve permitir realizar o bloqueio de vírus realizando a inspeção em, no mínimo, os protocolos HTTP, FTP, SMB, SMTP e POP3. Será permitido o uso de appliance externo para o bloqueio de vírus caso a solução de firewall ofertada não realize nativamente a inspeção em algum dos protocolos solicitados;	OK	Página 71	https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/10-2/pan-os-admin/pan-os-admin.pdf
24	Deve possuir a capacidade de detectar e prevenir ameaças em tráfego HTTP/2;	OK	11/05/2022	https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/app-id/http2

25	Deve possuir proteção contra ataques de negação de serviço (DoS) capaz de impedir ataques de SYN Flood, ICMP Flood, UDP Flood, etc e deve também bloquear port scans, bloquear ataques de buffer overflow e identificar e bloquear comunicação com botnets;	OK	11/05/2022	https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dos-protection/zone-defense/zone-protection-profiles/flood-protection
26	Para cada ameaça detectada pela solução deve ser realizado o registro nos logs do sistema das informações de data e hora, tipo da ameaça, origem e destino da comunicação e a ação tomada (se permitiu ou bloqueou o tráfego);	OK	11/05/2022	https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/monitoring/view-and-manage-logs/log-types-and-severity-levels/threat-logs
27	A solução de firewall deve possuir funcionalidade para análise de malwares não conhecidos (Malware Zero Day) onde o dispositivo envia o arquivo de forma automática para análise na "cloud" ou em um appliance instalado na rede local onde o arquivo será executado e simulado em um ambiente controlado (sandbox);	OK	11/05/2022	https://docs.paloaltonetworks.com/wildfire/10-2/wildfire-admin/wildfire-overview/about-wildfire
28	Caso seja fornecido um appliance local para análise de malwares não conhecidos ele deve possuir, no mínimo, 28 (vinte e oito) ambientes controlados (sandbox) independentes para execução simultânea de arquivos suspeitos;	OK	OK	100% em nuvem.
29	Caso seja necessário licença de sistema operacional e software para execução de arquivos no ambiente controlado (sandbox) as mesmas devem ser fornecidas em sua totalidade para o seu perfeito funcionamento;	OK	11/05/2022	https://docs.paloaltonetworks.com/wildfire/10-2/wildfire-admin/wildfire-overview/about-wildfire
30	O resultado da análise de malwares não conhecidos deve ter a capacidade de categorizar o arquivo analisado como, no mínimo, um arquivo malicioso, um arquivo não malicioso, mas com características indesejáveis que deixam o sistema operacional lento ou que alteram parâmetros do sistema;	OK	11/05/2022	https://docs.paloaltonetworks.com/wildfire/10-2/wildfire-admin/wildfire-overview/about-wildfire
31	A análise de malwares não conhecidos deve ser realizada em arquivos trafegados na internet através dos protocolos HTTP, HTTPS e FTP bem como em arquivos trafegados entre servidores de arquivos utilizando o protocolo SMB. A análise também deve ser realizada em arquivos anexos em e-mails e links HTTP e HTTPS presentes no corpo de e-mails trafegados utilizando os protocolos SMTP e POP3. A análise do link HTTP e HTTPS presente no corpo do e-mail deve identificar se o website é um hospedeiro de exploits ou atividade de phishing;	OK	Página 4	Datasheet Palo Alto Networks Approach to Intrusion Prevention
32	Deve suportar a análise dos arquivos em ambientes controlados (sandbox) com, no mínimo, os sistemas operacionais MS Windows 10, MacOS e Linux;	OK	11/05/2022	https://docs.paloaltonetworks.com/wildfire/10-2/wildfire-admin/wildfire-overview/wildfire-concepts/file-analysis
33	A análise de malwares não conhecidos em ambiente controlado (sandbox) deve ser realizada em arquivos tipo executáveis, DLLs, arquivos compactados RAR e 7-ZIP, arquivos do pacote MS Office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos PDF, arquivos JAVA (.jar e class), arquivos DMG, arquivos ELF e arquivos APK;	OK	11/05/2022	https://docs.paloaltonetworks.com/wildfire/10-2/wildfire-admin/wildfire-overview/wildfire-concepts/file-analysis
34	Deve atualizar a base de assinaturas para bloqueio dos malwares identificados no ambiente controlado (sandbox) dentro de, no máximo, 5 (cinco) minutos;	OK	11/05/2022	https://docs.paloaltonetworks.com/wildfire/10-2/wildfire-admin/wildfire-overview/about-wildfire

35	A solução de firewall deve possuir funcionalidade de filtro URL que permita a criação de políticas/regras para controle do acesso a websites baseado em categorias de URL devendo o fabricante da solução disponibilizar a base de dados de URL categorizadas para consulta por parte da solução. As políticas/regras que permitem ou bloqueiam o acesso a determinada categoria de URL devem ser com base no usuário e grupos de usuários e por endereços IP e faixas de endereços IP;	OK	Página 4	Datasheet Advanced URL Filtering
36	A funcionalidade de filtro URL deve possuir categoria específica para classificar domínios recém registrados com menos de 30 dias;	OK	Página 3	Datasheet Advanced URL Filtering
37	Deve permitir a criação de categoria de URL customizada permitindo inserir uma lista de URLs específicas;	OK	Página 6	Datasheet Advanced URL Filtering
38	Deve permitir a customização da página de bloqueio exibida ao usuário quando o mesmo tentar realizar um acesso a um website pertencente a uma categoria de URLs bloqueada;	OK	Página 6	Datasheet Advanced URL Filtering
39	Deve possuir recurso para proteger contra o roubo de credenciais de usuário e senha, identificadas através da integração com o Active Directory, submetidas em sites não corporativos. Deve ser possível definir em quais websites é permitido ou bloqueado o envio das credenciais baseado na categoria de URL a qual o website pertencer. Caso o usuário tente submeter suas credenciais de usuário e senhas pertencentes ao Active Directory em um website não autorizado deve ser exibido no web browser do mesmo uma página de bloqueio informando que o uso de tais credenciais no website específico não está autorizado;	OK	11/05/2022	https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/objects/objects-security-profiles-url-filtering/user-credential-detection
40	A solução de firewall deve possuir recurso que permita bloquear a transferência de arquivos baseado na extensão dos mesmos e também definir por qual aplicação a transferência do arquivo está bloqueada, por exemplo, bloquear a transferência de arquivos .exe através de web browser. Deve permitir bloquear, no mínimo, arquivo com as extensões .exe, .bat, .dll, .pif e .torrent;	OK	11/05/2022	https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/threat-prevention/set-up-file-blocking
41	A solução de firewall deve possuir integração com LDAP, MS Active Directoy e RADIUS para identificação dos usuários e grupos da rede para uso nas políticas/regras baseadas por usuários e grupo de usuários;	OK	11/05/2022	https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/user-id/user-id-overview#id2cbce7b3-daa8-45bf-ad85-df3415a67dc6
42	A integração com MS Active Directory para identificação dos usuários da rede deve ser realizada sem a necessidade de instalação de um agente no Controlador de Domínio e nem nas estações dos usuários;	OK	11/05/2022	https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/user-id/user-id-overview#id2cbce7b3-daa8-45bf-ad85-df3415a67dc6
43	A solução de firewall deve possuir recurso de portal de autenticação prévia (Captive Portal) para identificação dos usuários que realizam o acesso à internet, sem a necessidade de instalação de software cliente ou agente no computador. O portal de autenticação deve ser exibido antes de o usuário iniciar a navegação pela internet;	OK	11/05/2022	https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/user-id/map-ip-addresses-to-users/map-ip-addresses-to-usernames-using-captive-portal/configure-captive-portal

44	A solução de firewall deve possuir o recurso de VPN – Virtual Private Network dos tipos site-tosite e client-to-site e suportar IPSEc – Internet Protocol Security e SSL – Secure Sockets Layer;	OK	11/05/2022	https://www.paloaltonetworks.com.br/apps/pan/public/downloadResource?pagePath=/content/pan/pt_BR/resources/datasheets/pa-400-series
45	O recurso de VPN IPSec deve suportar os algoritmos de criptografia 3DES, AES 128, AES 192 e AES 256, os algoritmos de autenticação MD5 e SHA 1, o algoritmo IKEv1 e IKEv2 e os algoritmos de troca de chaves Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 e Grupo 14 e suportar também a autenticação através de certificados IKE PKI;	OK	11/05/2022	https://www.paloaltonetworks.com.br/apps/pan/public/downloadResource?pagePath=/content/pan/pt_BR/resources/datasheets/pa-400-series
46	O recurso de VPN SSL deve permitir que o usuário remoto se conecte através de um software cliente de VPN instalado no sistema operacional do equipamento do usuário sendo possível a atribuição de endereços IP fixos e atribuição de DNS ao mesmo;	OK	11/05/2022	https://docs.paloaltonetworks.com/globalprotect/8-1/globalprotect-admin/globalprotect-gateways/configure-a-globalprotect-gateway
47	Deve suportar a autenticação dos usuários remotos que se conectam à VPN via LDAP, MS Active Directory, TACACS+, RADIUS, SAML e através de base de usuários local no equipamento da solução de firewall. Deve suportar também a autenticação via certificado e OTP – One Time Password;	OK	11/05/2022	https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/authentication/set-up-external-authentication/set-up-radius-or-tacacs-authentication
48	Deve ser disponibilizado o software cliente de VPN do mesmo fabricante da solução de firewall ofertada compatível para instalação em computadores com sistema operacional MS Windows 10, MacOS e Linux e para instalação em dispositivos móveis Android e IOS;	OK	11/05/2022	https://docs.paloaltonetworks.com/compatibility-matrix/globalprotect/where-can-i-install-the-globalprotect-app
49	O recurso de VPN SSL deve possuir mecanismo de checagem da conformidade do computador do usuário remoto para o firewall tipo 1 e a checagem deve permitir verificar, no mínimo, as informações de qual sistema operacional e patches estão instalados, se o antivírus está instalado e ativo no computador, se o firewall está instalado e ativo no computador, se o disco está criptografado, se o agente de DLP – Data Loss Prevention está instalado e ativo, informações de chaves de registro e processos ativos no computador;	OK	11/05/2022	https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/get-started/enable-ssl-between-globalprotect-components/globalprotect-certificate-best-practices
50	Deve ser possível criar perfis customizados de conformidade com, no mínimo, as mesmas informações obtidas pelo mecanismo de checagem da conformidade do computador do usuário remoto. Tais perfis devem ser utilizados para assegurar que apenas computadores de usuários remotos que atendem aos requisitos solicitados nos perfis customizados possam ter acesso através da VPN aos dados e sistemas hospedados na rede interna do órgão;	OK	11/05/2022	https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/get-started/enable-ssl-between-globalprotect-components/globalprotect-certificate-best-practices
51	A solução de firewall deve possuir console de gerenciamento do equipamento acessada através de interface gráfica web permitindo realizar as configurações da solução como criar e administrar as políticas/regras de firewall e controle de aplicações, criar e administrar as políticas de IPS, antivírus e anti-spyware, criar e administrar as políticas de filtro URL, monitorar e investigar os registros de logs de eventos e demais configurações;	OK	11/05/2022	https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/firewall-administration/use-the-web-interface

52	Deve suportar a autenticação dos usuários administradores que se conectam à interface de gerenciamento do equipamento via LDAP, MS Active Directory, RADIUS e através de base de usuários local no equipamento da solução de firewall;	OK	11/05/2022	https://live.paloaltonetworks.com/t5/general-topics/windows-kerberos-ldap-radius/td-p/300804
53	Deve ser possível criar perfis de acesso à interface de gerenciamento com permissões granulares como acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações entre outros;	OK	11/05/2022	https://docs.paloaltonetworks.com/prisma/prisma-sd-wan/prisma-sd-wan-admin/prisma-sd-wan-administrator-authorization-and-authentication/role-based-access-control
54	Deve permitir realizar o backup das configurações do equipamento e a restauração da configuração salva através de interface de gerenciamento;	OK	11/05/2022	https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/firewall-administration/manage-configuration-backups/save-and-export-firewall-configurations
55	A interface de gerenciamento do equipamento deve possuir recurso para análise das políticas indicando, quando houver, regras que ofusquem, conflitem ou sobreponham outras regas (shadowing) e quais objetos não estão sendo utilizados, para avaliação de elementos dispensáveis, permitindo assim, a higienização gradual das regras e seus respectivos elementos. Deve possuir também recurso para análise das políticas indicando, quando houver, regras baseadas em porta e protocolo, permitindo a conversão da mesma para uma regra baseada em aplicação, melhorando assim o controle do tráfego e a segurança do ambiente;	OK	11/05/2022	https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVXCA0
55.1	É permitido o uso de appliance externo para realização da análise das políticas;	OK	11/05/2022	https://www.paloaltonetworks.com.br/network-security/panorama
56	Deve ser possível através de interface de gerenciamento do equipamento a geração de relatórios tais como um resumo gráfico das aplicações utilizadas e ameaças vistas, principais aplicações por utilização de largura de banda, atividades de um usuário ou grupo de usuário específicos incluindo aplicações e URLs acessadas e permitir a criação de relatórios personalizados;	OK	11/05/2022	https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/dashboard/dashboard-widgets
57	Deve ser possível gerar relatório de visibilidade e uso das aplicações do tipo SaaS – Software as a Service mostrando 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 a aplicação SaaS e o consumo da aplicação SaaS pelo usuário;	OK	11/05/2022	https://www.paloaltonetworks.com.br/resources/techbriefs/aperture
58	Deve ser exibida na interface gráfica de gerenciamento do equipamento informações em tempo real, atualizadas de forma automática a cada 1 (um) minuto, as principais aplicações acessadas, o risco das principais aplicações, número de sessões simultâneas, status das interfaces de rede e uso de CPU;	OK	11/05/2022	https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-new-features/wildfire-features/wildfire-real-time-signature-updates
59	Deve ser possível configurar o envio de alertas do sistema via e-mail;	OK	11/05/2022	https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/monitoring/configure-email-alerts
60	Deve suportar o monitoramento via SNMPv3;	OK	11/05/2022	https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClHOCA0

61	O sistema operacional a ser instalado no equipamento que compõe a solução deverá ser fornecido em sua versão mais atualizada, não sendo aceito sistema operacional de uso genérico;	OK	11/05/2022	https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-release-notes/features-introduced-in-pan-os
62	Por cada equipamento que compõe a solução de segurança, entende-se o hardware e as licenças de softwares necessárias para o seu funcionamento;	OK	11/05/2022	https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/subscriptions/all-subscriptions
63	Na data do certame, nenhum dos equipamentos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;	OK	11/05/2022	https://www.paloaltonetworks.com/services/support/end-of-life-announcements/hardware-end-of-life-dates
64	Durante o período de vigência do contrato de garantia todos os componentes da solução de firewall, incluindo o equipamento, o sistema operacional do mesmo, as licenças necessárias para atender as funcionalidades e recursos solicitados, os softwares clientes de VPN e demais itens necessários para o perfeito funcionamento devem estar cobertos por garantia e suporte técnico do fabricante da solução em caso de problema;	OK	11/05/2022	https://support.paloaltonetworks.com/Support/Index
65	A solução de firewall deve possuir garantia pelo período de, no mínimo, 36 (trinta e seis) meses, compreendendo a reposição de peças/equipamentos, atualizações do sistema operacional do equipamento e demais software e das assinaturas de proteção da solução.	OK	11/05/2022	https://www.paloaltonetworks.com/services/support/product-warranty

Marcos Ribeiro
EQUIPE TÉCNICA - DETI – SENAR-PR