RFP Document Page	RFP PDF Version Page	Technical Specification	Points		Clause	Queries	Response
71	74	Requirements			The proposed NGFW firewall throughput (Firewall throughput is measured with App-ID and logging enabled, utilizing 64 KB HTTP/appmix transactions)	The performance methods / terminologies mentioned are vendor specific.	PTA wants Next Generation firewall which are mainly working on application based/ levels, in this regard to secue PTA network and reduce the attack risk / policey optimizer, and wants the firewall troughtput to measure with Application Identification classification technology that determines the exact identity of applications, irrespective of port, protocol, Transport Layer Security/ Secure Sockets Layer/ Secure Shell encryption, or any other evasive tactic the application may use. This features in also available in Juniper. https://www.juniper.net/documentation/us/en/software/junos/application-identification/topics/topic-map/security-application-identification-overview.html Other vendors are also having similar performance methodology for IPSEC VPN https://www.juniper.net/content/dam/www/assets/datasheets/us/en/secur
71	74	Requirements			The proposed NGFW minimum threat prevention throughput (Threat Prevention throughput measured with App-ID, IPS, antivirus, anti-spyware, Wildfire , DNS Security, file blocking, and logging enabled, utilizing 64 KB HTTP/appmix transactions)		
71	74	Requirements			The proposed NGFW of IPsec VPN throughput (IPsec VPN throughput is measured with 64 KB HTTP transactions and logging enabled)		
71	74	Requirements			Max sessions		
71	74	Requirements			New connections per second (measured with application-override utilizing 1byte HTTP transactions)		
71	74	Requirements			Interfaces	Port density is specific to a particular model of a speciifc vendor. Please rationalize the port / interfaces as per your actual requirement	Port density mentioned in the RFP is the minimun requirment of PTA however vendors may quote equal or high density.
72	75	Requirements			Wildfire subscription years term	Wildfire is PaloAlto specific terminology.	Wildfire terms may be repalced with Sandboxing
73	76	General Requirements	1		The proposed NGFW should be the leader in the latest Gartner Magic Quadrant for Enterprise Network Firewalls for more than 05 years .	Last MQ for NW firewalls was published by Gartner in 2022. Will you refer the MQs from 2018-2022?	Last avaible five years from Gartner published report
73	76	General Requirements	2		The proposed NGFW should be ISO 27001, ISO 27017, ISO 27018, ISO 27701, SOC2, FedRAMP, Germany C5, Common Criteria, FIPS 140-2, CMVP, NCSC Foundation, ANSSI, DoDIN, CSfC, USGV6, ICSA and NEBS certified	Some of these certifications are not related to your project and are specific to PaloAlto. Most of these certifications are not required for the procurement of the firewalls	All the mentioned certifcted are 3rd party certification releated to IT/Cyber Security and netwrok compliecne, these are not vendor specifci certifactes, however these certificates are mentioned in the Annexure A in details. Howecewr, bidder quoted product must qualify atleast 60 percent of the mentioned certifications.
73	76	General Requirements	4		The proposed NGFW should have integrated reporting capabilities requiring no additional hardware to generate reports	Every vendor offers different solution for reporting. Therefore, PTA should specify reporting requirements and let the vendors offer solution	PTA does not want additonal harware for the reporting , however vendor may quote software for the reporting.
73	76	General Requirements	15		The proposed NGFW should support an unfettered open API without a paywall (subscription) to access Dev toolkit, Tools and Scripts and samples	What is the use-case / requirement to access Dev toolkit, tools. Please share for better understanding of the requirement.	Progmetic access to create and manage the open APIs access .
73	76	General Requirements	16		The proposed NGFW should support the ability to dynamically and automatically regroup user/s based on security events relating to that user, no manual response needed	This point require more elaboration of the use-case. This is more of an administrative level task for which each OEM offers its own GUI, features and functions. Not all OEMs can offer this feature.	The purpose is to have a strong GUI feature to dynamically assign user-based security event and group them
74	77	General Requirements	18		The proposed NGFW must be able to tag objects to enable dynamic enforcement of policy no matter any changes to IP, area, or direction traffic originates from with no need to recommit policy	This feature require integration with a ZTNA solution provider. The RFP does not ask to provide a ZTNA solution along with NGFW. If PTA is using any ZTNA solution kindly let us know so that we can check its compatibility.	Solution must have support for future integration.
74	77	General Requirements	30		The proposed NGFW should support selective commit of configuration changes	This is PaloAlto specific feature. See the below reference https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/firewall-administration/use-the-web-interface/commit-selective-configuration-changes	PTA require the practice of implementing or updating specific rules or configurations without applying changes to the entire firewall policy. Multiple vendor support this feature
74	77	Security Policy Control features	3		The proposed NGFW should have a built-in security policies optimization tool which facilitates converting legacy Layer 4 port-based security policies to Layer 7 application-based ones	This is PaloAlto specific tool called as Policy Optmizer. Kindly confirm if PTA looking for PA firewall to quote. https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/app-id/security-policy-rule-optimization/migrate-port-based-to-app-id-based-security-policy-rules	All Majore NGFW OEM are having Secuirty Policy L-4/L-7 tools/techniques. PTA wants to secure their netwrok , however other vendors may offer their equivlant solution, PTA preferring builtin in solution and avoding additional boxing, it hard to manage.
75	78	Advanced Threat Prevention Features	6		The proposed NGFW should continuously collect telemetry to enable data-intensive ML processes to automatically compute and recommend policy changes	This is PaloAlto specific feature. See the below reference https://www.exclusive-networks.com/ch-fr/pan-first-machine-learning-ngwf/	PTA wants to secure their netwrok, these are avaible in multiple vendors,howeever bidder may quote thier option.
77	80	Advanced Threat Prevention Features	35		The proposed NGFW should disrupt ultra-low/slow DNS tunnels that spread tunneled data and exploits across multiple domains and use very slow rates to evade detection, stealing data or sending additional malicious payloads into your	PaloAlto specific statement copied from the below reference https://www.westconcomstor.com/content/dam/wcgcom/pan-vip/dns-security.pdf	This is PTA requirmenet however bidder may quote their own builitin solution in equivlant

77	80	Advanced Threat Prevention Features	47		The proposed NGFW analysis environment should replicate macOS, Android, Windows XP/7/10, and Linux	This is not a NGFW feature. NFGW cannot replicate OS enviroments themselves, rather this is particularly a Sandbox feature which can then integrates with an NGFW. Kindly confirm if PTA has Sandbox integrated requirements with NGFW.	Need cloud beased Sandboxing feature in NGFW, or Bidder may Propose builitn sandboxing solution
77	80	Advanced Threat Prevention Features	51		The proposed NGFW should provide protection updates for unknown malware within seconds	Unknown malware protection requires Sandbox integration. An NGFW has to wait for Sandbox verdict depends upon Sandbox location (on-prem or on-cloud) which can never be within seconds. The RFP does not ask for on-prem Sandbox. Kindly confirm if PTA has any on-prem Sandbox available to integrate with NGFW	The NGFW should support Cloud based Sandbox feature
77	80	Advanced Threat Prevention Features	52		The proposed NGFW should support Domain Front Detection protects networks from malicious attackers using a crafted packet to indicate a fake website in the SNI while surreptitiously connecting to a different website via the HTTP Host Header	This is PaloAlto specific feature as per given below reference https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-new-features/content-inspection-features/domain-fronting-detection	This is PTA requirement, however bidder may propose /quote their own solution in equivlant.
78	81	Advanced URL Filtering	15		The proposed NGFW should support crawling and analysis in 41 languages	Kindly elaborate, what is the use-case for PTA to have such analysis in exact 41 languages?	Should support maximum languages
79	82	Advanced URL Filtering	17		The proposed NGFW should have an enhanced HTTP header insertion supporting header values up to 16K bytes	This is Palto Alto specific as per below reference. https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-new-features/url-filtering-features/http-header-expansion	All Firewalls OEM supports HTTP header Insertion. However bidders are allowed to quote equivilant or higher values.
79	82	User Identification & Authentication Features	2		The proposed NGFW should support identifying user-id by integrating with Exchange through WinRM and WMI	This is supported by PaloAlto, hence PaloAlto specific feature. https://live.paloaltonetworks.com/t5/general-topics/best-way-of-doing-user-id-mapping-wmi-winrm-http-there-is-also/td-p/292854	Required feature is to support integration with an external authentication system.OEM should support as deemed fit.
79	82	User Identification & Authentication Features	3		The proposed NGFW should support identifying user-id by running as syslog sender.	This is supported by PaloAlto, hence PaloAlto specific feature. Reference below https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/map-ip-addresses-to-users/configure-user-id-to-monitor-syslog-senders-for-user-mapping	PTA require NGFW to be integrated with the external Syslog system
79	82	User Identification & Authentication Features	4		The proposed NGFW should support identifying user-id by Integrating through XML APIs with Third Party solutions	PaltoAlto specified feature https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/user-id-concepts/user-mapping/xml-api	Other OEM also support this feature.https://community.sophos.com/sophos-xg-firewall/f/recommended-reads/124698/sophos-firewall-importing-user-definitions-into-sophos-firewall-after-v18-0-mr3-and-v17-5-mr14/463127#mcetoc_1ep9t76cp1 https://www.juniper.net/documentation/us/en/software/junos/identity-
79	82	User Identification & Authentication Features	6		The proposed NGFW should support Identifying user-id in terminal servers	PaltoAlto specific feature https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/map-ip-addresses-to-users/configure-user-mapping-for-terminal-server-users	Other OEM also support this feature.https://community.sophos.com/sophos-xg-firewall/f/recommended-reads/128784/sophos-firewall-authentication-methods#mcetoc_1f9tvdapk0 https://www.juniper.net/documentation/us/en/software/junos/cli-reference/topics/ref/command/show-security-user-identification-user-provision.html
79	82	Advanced Mobility & Host Information Profiling Features	5		The proposed NGFW should offer a host information check feature by collecting & reporting device information & attributes. Host Information Profiling attributes based on Managed/Unmanaged certificates status, OS type, Client version, Host name, Host ID, Serial number, Mobile model, Phone number, Root/Jailbroken status, Passcode presence, Installed Applications, Patch presence & status, Firewall agent presence & status, Antimalware agent presence & status, Disk backup agent presence & status, Disk encryption agent presence & status, DLP agent presence & status, process list presence & status, registry key presence & status and Plist presence & status	This feature is part of ZTNA framework and requires per host/end point subscription licensing. If PTA requires such feature then kindly share the use-case and for how many remote users such functionality is required.	PTA require minimum profiling of 1500 remote users, however quoted firewall must support full capacity of SSL VPN termination (client & clienless)
80	83	Advanced Mobility & Host Information Profiling Features	6		The proposed NGFW should support enforcing security policies based on device/host information profiles	This feature is part of ZTNA framework and requires per host/end point subscription licensing. If PTA requires such feature then kindly share the use-case and for how many remote users such functionality is required.	PTA require this Feature in proposed Firewall to enforce Security as mentioned above.
80	83	Advanced Mobility & Host Information Profiling Features	7		The proposed NGFW should support the integration with Third Party MDM solutions like AirWatch or MobileIron	This feature is part of ZTNA framework and requires per host/end point subscription licensing. If PTA requires such feature then kindly share the use-case and for how many remote users such functionality is required.	PTA require this Feature to be supported in proposed Firewall for the futurisic approach
80	83	Advanced Mobility & Host Information Profiling Features	9		The proposed NGFW should support VPN authentication override using cookies	PaltoAlto Specific feature https://docs.paloaltonetworks.com/globalprotect/9-1/globalprotect-admin/authentication/about-globalprotect-user-authentication/how-does-the-app-know-what-credentials-to-supply/cookie-authentication-on-the-portal-or-gateway	All Major OEM supports VPN authentication https://community.fortinet.com/t5/Fortinet-Forum/Override-and-user-authentication/m-p/32580

80	83	Advanced Mobility & Host Information Profiling Features	10		The proposed NGFW should support the exclusion of video traffic from main remote user VPN tunnel	PaltoAlto Specific feature https://docs.paloaltonetworks.com/globalprotect/9-1/globalprotect-admin/globalprotect-gateways/split-tunnel-traffic-on-globalprotect-gateways/exclude-video-traffic-from-the-globalprotect-vpn-tunnel	Major OEM Suport this feature in NGFW Fortinet: https://www.reddit.com/r/fortinet/comments/ndnr55/set_up_vpn_to_direct_all_traffic_via_tunnel_with/ Cisco: https://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client/215343-optimize-anyconnect-split-tunnel-for-off.html Or bidder may quote equivalent.
80	83	Advanced Mobility & Host Information Profiling Features	12		The proposed NGFW should support VPN gateway selection criteria based on source user-id, region, OS and IP address	PaltoAlto Specific feature https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/globalprotect-gateways/configure-a-globalprotect-gateway	Manu OEM support this feature. https://community.cisco.com/t5/security-knowledge-base/anyconnect-optimal-gateway-selection-operation/ta-p/3124296#toc-hId--86828332
80	83	Management, Logging & Reporting Features	4		The proposed NGFW should have a commit-based configuration management	PaltoAlto Specific feature https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-cli-quick-start/use-the-cli/commit-configuration-changes	https://www.juniper.net/documentation/us/en/software/junos/cli/topics/topic-map/junos-configuration-commit.html#:~:text=The%20device%20configuration%20is%20saved,gz%20and%20activated.
80	83	Management, Logging & Reporting Features	5		The proposed NGFW should support config-audit by comparing running config against candidate config	PaloAlto Specific featrue https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClEaCAK	Many OEM support this feature. https://www.juniper.net/documentation/us/en/software/connectivity-services-director5.3/csd-user-guide/connectivity-services-director-user-guide/topics/task/config-audit-perform.html However, it is good to have feature.
80	83	Management, Logging & Reporting Features	10		The proposed NGFW should support custom reporting with the ability to generate a report per user, user group and application	PaloAlto Specific feature https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/monitoring/view-and-manage-reports/generate-custom-reports	All Major OEM suport Custom reporting. https://www.juniper.net/documentation/us/en/software/junos-space21.3/junos-space-workspaces/topics/concept/reports-overview.html https://www.juniper.net/documentation/us/en/software/jweb-srx21.2/jweb-srx/topics/topic-map/j-web-security-reporting.html
81	84	Management, Logging & Reporting Features	11		The proposed NGFW should support exporting reports to PDF and sending reports by email	PaloAlto Specific feature https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/monitor-network-activity/use-panorama-for-visibility/generate-schedule-and-email-reports	All Major OEM support this basic feature.https://www.scribd.com/document/638754154/FW8005-19-0v1-Running-and-Customizing-Reports-on-Sophos-Firewall
81	84	Management, Logging & Reporting Features	12		The proposed NGFW should have a dedicated SaaS applications usage report	PaloAlto Specific feature https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/view-and-manage-reports/generate-the-saas-application-usage-report	Feature is availibile in other OEM i-e FORTISASE https://docs.fortinet.com/document/fortisase/latest/administration-guide/811575/report-types https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-protecting-enterprises-from-the-risks-of-saas.pdf. https://www.juniper.net/documentation/us/en/software/junos/application-identification/application-identification.pdf
					InLine Transparent	InLine Transparent	Bidder may qoute the WAF having the feature with activie /Passive mode . Or equilant
					True Transparent Proxy	True Transparent Proxy	Bidder may qoute equal features. WAF should be deployed in Active/Passive Mode or equilant feature
					OffLine Sniffing	OffLine Sniffing	Bidder may qoute equal features. WAF should be deployed in Active/Passive Mode
					Malware Detection	Malware Detection	Malware detection/sandboxing for zero day attack .Or Equilant
					Web Defacement Protection (2 clausals mentioning the same requirements)	Web Defacement Protection (2 clausals mentioning the same requirements)	Its a generic feature which is required, bidder may quote equivalent features
					Attachment Scanning for ActiveSync/MAPI applications, OWA, and FTP	Attachment Scanning for ActiveSync/MAPI applications, OWA, and FTP	Its a generic feature which is required, bidder may quote equivalent features.Desirebale
					OpenAPI 3.0 verification	OpenAPI 3.0 verification	It is PTA requirement, bidders are required to include this feature in quoted WAF . Desireable
					What does verification here means?	What does verification here means?	PTA require Authentication & Authorization in verification
					Ports and Throughput	Ports and Throughput	Bidder may qoute equla or greater than the mentioned throughput.
						What will be the tachnicnal evoluation criteria	Technical evaluation criteria is updated in bid document.