Next Gen Firewall with 1 Year and 3 Year Support.

NGFW - PA 450 with 1 Year Support.

Part Name	Description	INR Unit price	QTY	Extended Price
PAN-PA-450	Palo Alto Networks PA-450	197709	1	197709
PAN-PA-450-TP	PA-450, Threat prevention subscription, 1 year (12 months), term.	36400	1	36400
PAN-PA-450-ADVURL	Advanced URL Filtering subscription, 1-year, PA-450	54600	1	54600
PAN-PA-450-WF	PA-450, WildFire subscription, 1 year (12 months), term.	36400	1	36400
PAN-SVC-BKLN-450	PA-450, Partner enabled premium support, 1 years (12 months), term.	45102	1	45102
				3,70,211.00

NGFW - PA 450 with 3 Year Support.

Part Name	Description	INR Unit price	QTY	Extended Price
PAN-PA-450	Palo Alto Networks PA-450	197709	1	197709
PAN-PA-450-TP-3YR	PA-450, Threat prevention subscription, 3 years (36 months), term.	85800	1	85800
PAN-PA-450-ADVURL-3YR	Advanced URL Filtering subscription, 3-year, PA-450	128960	1	128960
PAN-PA-450-WF-3YR	PA-450, WildFire subscription, 3 years (36 months), term.	85800	1	85800
PAN-SVC-BKLN-450-3YR	PA-450, Partner enabled premium support, 3 years (36 months), term.	118124	1	118124
		6,16,393.00		**6,16,393.00**

NGFW Technology Highlights

* Palo Alto Networks are the only vendor to provide Inline Machine Learning on the NGFW
In PAN-OS 10.0 the ability to prevent attacks directly on the NGFW due to our inline Machine Learning engine. Able to block fileless and other attacks that no sandbox can even test for.
With Zero delay updates, any NGFW in the world will receive data on any newly discovered attack immediately, delivered with the power of our Cloud Security Subscriptions.
Leveraging the power of the Cloud Machine Learning models we already have and all the data we collect world wide. The Inline Machine Learning engine is constantly updated against all of this User

* Palo Alto Networks NGFW provides security at exceptional speeds
All signatures for Threat, Content, WildFire, and DNS are active at all times, maximum coverage while maintaining the highest performance
Our NGFW has physically separated management and data planes. This allows the firewall to remain responsive even under stress.
Our Threat Prevention and AV signatures can be updated without halting traffic flowing through the firewall.
Our NGFW is capable of natively inspecting SSL at scale.
Our NGFW utilizes a single pass architecture allowing us to inspect and protect traffic at high rates. Other vendors suffer from performance degradation

* Palo Alto Networks provides streamlined management
All our network centric management is done through one interface, having fewer interfaces to learn requires less operational overhead
Our NGFW can be managed from the command line, web UI, API, or Panorama.
We have a distributed logging architecture allowing us to expand and accommodate enterprise scale and retention requirements.

* Palo Alto Networks has a superior security platform
Our platform is capable of natively understanding and protecting over 3,000 applications independent of port, with category and characteristic classifications to help ease management.
Parallel Processing allows on-box and cloud delivered functionality to expand with little to no impact on performance
NGFW is capable of ingesting third party feeds via MineMeld and AutoFocus or any sort of properly formatted list.
Our NGFW starts with App-ID, User-ID, and Content-ID to make security policies that line up to real world needs
App-ID blocks all applications by default, this ensures a good security posture out of the box.

Key Advantages

1. Natively integrated capabilities: Each capability exchanges data and protections in a frictionless way, with full understanding of the application and user context.

2. Prevention-focused: We deliver prevention through automation and analytics, reducing the noise and freeing up security resources to focus on higher value activities.

3. Consistent security: For all users, data, and applications, whether they reside in the network, endpoint, or cloud, new protections are automatically delivered everywhere, at the same time, via the globally distributed cloud-based infrastructure.

4. Superior management: Manage security across your entire organization as one coordinated system. Manage policies, logging, and reporting centrally from Panorama.

5. Rapidly adopt security innovations that are natively integrated: Perform cloud-based, advanced analytics and generate insights. Easily consume new security innovations, such as behavioural analytics, to find hidden threats on the network

6. Zero Trust - Our Next-Generation Firewalls directly align with Zero Trust, including enabling secure access for all users irrespective of location, inspecting all traffic, enforcing policies for least-privileged access control, and detecting and preventing advanced threats. This significantly reduces the pathways for adversaries, whether they are inside or outside your organization, to access your critical assets.

End Point Security - 1 Year Support

Option 1

PART CODE	**DESCRIPTION**	**Partner**	**QTY**	**TOTAL TP**
PAN-XDR-ADV-EP	Cortex XDR Pro for 1 endpoint, includes 30 days of data retention	2050.00	1500	3075000.00

Option 2

PART CODE	**DESCRIPTION**	**Partner**	**QTY**	**TOTAL TP**
PAN-XDR-PRVT	Cortex XDR Prevent, includes 30 days of alerts retention and standard	1350.00	1500	2025000.00

End Point Security - 3 Year Support

Option 1

PART CODE	**DESCRIPTION**	**Partner**	**QTY**	**TOTAL TP**
PAN-XDR-ADV-EP -3YR	Cortex XDR Pro for 1 endpoint, includes 30 days of data retention	5850.00	1500	8775000.00

Option 2

PART CODE	**DESCRIPTION**	**Partner**	**QTY**	**TOTAL TP**
PAN-XDR-PRVT - 3YR	Cortex XDR Prevent, includes 30 days of alerts retention and standard	3850.00	1500	5775000.00

Optional

Host Insights & MTH

PART CODE	**DESCRIPTION**	**Partner**	**QTY**	**TOTAL TP**
PAN-XDR-HOST-INST	Host Insights add-on for Cortex XDR	600.00	1500	900000.00
PAN-XDR-MTH	Cortex XDR Managed Threat Hundting Service	1200000	1	1200000.00

LICENSE FEATURES	CORTEX XDR PRE	CORTEX XDR PRO
Endpoint Prevention Features		
Endpoint management	YES	YES
Device control	YES	YES
Host firewall	YES	YES
Disk encryption	YES	YES
Response Actions		
Live Terminal	YES	YES
Endpoint isolation	YES	YES
External dynamic list (EDL)		YES
Script execution		YES
Remediation analysis		YES
Incident Scoring Rules		YES
Featured Alert Fields		YES
Widget Library		YES
Assets		
Asset Management		YES
Analysis		
Analytics		YES
Alert and Log Collectors		
Cortex XDR agent alerts	YES	YES
Enhanced data collection for EDR and other Pro features		YES
Other alerts (from Palo Alto Networks and third-party sources)		YES
Integrations		
Threat intelligence (AutoFocus, VirusTotal)	YES	YES
Outbound integration and notification forwarding (Slack, Syslog)	YES	YES
Broker VM		
Agent Proxy	YES	YES
Network Mapper		YES
Pathfinder		YES
Windows Event Collector		
MSSP		
MSSP (requires additional MSSP license)	YES	YES
Managed Threat Hunting (requires an additional Managed Threat Hunting License)		YES (MIN License 500)

Host Insight Datasheet
https://www.paloaltonetworks.com/resources/datasheets/host-insights-for-cortex-xdr#

Managed Threat Hunting Solution Brief
https://www.paloaltonetworks.com/resources/techbriefs/cortex-xdr-managed-threat-hunting