NGFW Deployment & Management	Description	Cloud NGFW for AWS		VM-Series
		Native Management	Panorama Management	
Cloud-Native	Cloud NGFW for AWS is a cloud-native regional service similar to other AWS services. This resource is delivered on the AWS platform to protect your AWS Virtual network (VPC) traffic in an AWS region.	√	√	N/A
Zero Mantenance	N/A Infrastructure to Manage. Palo Alto Networks does the heavy lifting of deploying firewall instances, and managing scaling and failover	√	√	N/A
Build-in Resiliency (HA)	Cloud NGFW resource offers built-in resiliency within an availability zone and across availability zones in an AWS region	√	√	N/A
Build-in Scalability	Cloud NGFW resource scales with your VPC traffic. The Autoscaling group provisioned for each AWS availability zone (within the Cloud NGFW resource) scales out independently and includes more instances to inspect higher traffic volume. As the traffic volume decreases within an AWS availability zone, the corresponding Auto scaling group scales in independently.	√	√	N/A
Built-in Lifecycle management (SW and Content Updates)	Cloud NGFW resources have built-in software and content updates	√	√	N/A
Firewall-as-a-code	You can automate the Cloud NGFW resource deployment using published and supported extensions in Cloud Formation and Terraform registry	√	√	√
Policy-as-a-code	You can automate the Cloud NGFW policy deployment using published and supported extensions in Cloud Formation and Terraform registry	√	√	√
Multi-Cloud Support	Centralized policy management across Cloud NGFW deployed in AWS & Azure	NA	√	√

Policy Objects	Description	Cloud NGFW for AWS		VM-Series
		Native Policy Management (Rulestacks)	Panorama Policy Management (Cloud Device Groups)	
Address	You can specify an address object to include either IPv4 or IPv6 addresses (a single IP address, a range of addresses, or a subnet), an FQDN, or a wildcard address (IPv4 address followed by a slash and wildcard mask).	√	√	√
Address Groups	You can group specific source or destination addresses that require the same policy enforcement.	N/A	√	√
Regions	You can allow or block traffic from (or to) an IP addresses based on their geographic location such as a country. The region is available as an option when specifying source and destination for your policies. You can choose from a standard list of countries or specify a custom region/geolocation along with its associated IP addresses	√	√	√
Service (Port & Protocol)	You can granularly control VPC traffic session usage to specific ports on your network (in other words, you can define the default port for the application). Cloud NGFW includes two pre-defined services—service-http and service-https— that use TCP ports 80 and 8080 for HTTP, and TCP port 443 for HTTPS. You can however, create any custom service on any TCP/UDP port of your choice.	√	√	√
Service Group	You can combine services that have the same security settings into service groups to reduce the number of rules in security policy	N/A	√	√
External Dynamic List	You can granularly control your VPC traffic using a dynamic list of IP addresses, Domains or URLs. stored in a file hosted on an external web server. Palo Alto Networks also offers built-in (Bulletproof, High-Risk, KN/Awn Malicious, and Tor Exit IP address) EDLs. Additonally, Palo Alto Networks offers a free EDL hosting service that maintains the ever-dynamic list of IP addresses for Microsoft 365, Azure, Amazon Web Services (AWS), and Google Cloud Platform (GCP). You can use these EDLs to control your VPC Ingress and Egress traffic.	√	√	√
Applications	You can granularly control your VPC traffic by using Palo Alto Network's App-ID™ traffic classification system that relies on application signatures to accurately identify applications in your network.	√	√	√
Application Group	You can group together a set of APP-IDs that require the same policy enforcement.	N/A	√	√
Application Filter	You can granulary control your VPC trafic by defining an Application Filter that groups current APP-IDs and any future APP-IDs that match a certain attributes. For example, You can create an Application Filter by one or more attributes—category, sub-category, techN/Alogy, risk, characteristics. From N/Aw on, whenever a new APP-ID is introduced to Cloud NGFW based on a content update, all new applications matching the filter criteria are automatically added to your set.	N/A	√	√

Tags	Tags allow you to group objects using keywords or phrases. You can apply tags to address objects, address groups (static and dynamic), applications, zones, services, service groups, and to policy rules.		NA	√	√
Dynamic user group	Allow you to create a list of users from the local database, an external database, or match criteria and group them		N/A	√	√
Certificates Management	Cloud NGFW uses certificates to access an intelligent feed and to enable inbound and outbound decryption. Each certificate contains a cryptographic key to encrypt plaintext or decrypt ciphertext. Each certificate also includes a digital signature to authenticate the identity of the issuer.	Self-signed Root CA certificates	NA	√	√
		Import a Certificate and Private Key	NA	√	√
		Cloud Certificates (AWS Secrets Manager)	√	√	√
Log Forwarding	Log Forwarding to Palo Alto Networks CDL & Cloud destinations	**Customer Managed Log Collectors**	NA	NA	√
		Cortex Data Lake	N/A	√	√
		Cloud Provider Destinations	√	√	N/A
		Syslog Profile	Planned	Planned	√
		HTTP Profile	Planned	Planned	√

Security Services	**Description**		**Cloud NGFW for AWS**		**VM-Series**
			Native Policy Management (Rulestacks)	**Panorama Policy Management (Cloud Device Groups)**	
Security Policy	Security policy protects your VPC traffic from threats and disruptions. Individual Security policy rules determine whether to block or allow a VPC/VNET traffic session based on traffic attributes, such as the source and destination security zone, the source and destination IP address, the application, the user, and the service.		√	√	√
IPS Vulnerability Protection	Vulnerability Protection protects against on inbound threats, where an attacker is attempting to exploit a system vulenrability to breach your network, The system vulnerabilies may be in the form buffer overflows, illegal code execution etc.	**Best-Practices Profile**	√	√	√
		Custom Profiles	N/A	√	√
Anti-Spyware	Anti-Spyware detects and blocks outbound threats, especially command-and-control (C2) activity, initiated by a (cyber-attack leveraged) malware infected workloads in your AWS VPC. You can also define custom regular expression patterns to identify spyware phone home communication.	**Best-Practices Profile**	√	√	√
		Custom Profiles	N/A	√	√
File Blocking	File Blocking allows you to granularly control file types in your VPC traffic in a specified direction (inbound/outbound/both). You can proactively block files that are kN/Awn to carry threats or that have N/A real use case for upload/download.	**Best-Practices Profile**	√	√	√
		Custom Profiles	N/A	√	√
Antivirus	Antivirus detects and protects against malware concealed in compressed files, executables, PDF files, and HTML and JavaScript viruses in your VPC traffic	**Best-Practices Profile**	√	√	√
		Custom Profiles	N/A	√	√

WildFire Analysis	Cloud NGFW detects and forwards files, and executables in your VPC traffic to WildFire™ cloud service for analysis, and also performs inline ML analysis for certain files. If a threat is detetced on the files, Wildfire creates protections to block malware and globally distributes protection for that threat in under five minutes.		N/A	√	√
URL Filtering	URL Filtering analyzes the VPC traffic and controls the URLs accessed by your VPC workloads (in both clear-text and encrypted traffic) by perfoming inline analysis and comparing against Palo Alto Networks managed URL categories or the custom categories you provide.	**Best-Practices Profile**	√	√	√
		Custom Profiles	√	√	√
DNS Security	DNS Security protects outbound DNS requests from your VPCs against threats such as DNS tunneling, Domain Generation Algorithm (DGA) detection, Malware domains etc.	**Best-Practices Profile**	N/A	√	√
		Custom Profiles	N/A	√	√
Data Filtering & Enterprise DLP	Data filtering detects sensitive information in your VPC traffic—such as credit card or social security numbers or internal corporate documents—and prevent this data from leaving your AWS environment. With Enterprise DLP you would gain a benefit of Advanced Data Filtering on your VPC traffic with pre-defined a huge list of data patterns with the cloud based analytics.		N/A	√	√
Security profile groups	A security profile group is a set of security profiles that can be treated as a unit and then easily added to security policies.		N/A	√	√
Decryption	Cloud NGFW can decrypt, inspect, and re-encrypt your VPC Ingress and Egress traffic as a policy-based decision. You can granularly control what VPC traffic can be decrypted and what traffic canN/At be decrypted and the type of SSL decryption, you want to perform on the indicated traffic. To enable decryption, you set up the certificates required to act as a trusted third-party to a session	**SSL Forward Proxy**	√	√	√
		SSL Inbound Inspection	√	√	√
		SSH Proxy	N/A	√	√
DoS & Zone Protection	Zone protection defends network security zones against flood attacks, reconnaissance attempts, packet-based attacks		N/A	Planned	√
APP-ID Cloud Engine (SaaS Inline)	Palo Alto Network firewalls can download specific AWS PaaS APP-IDs from App-ID Cloud Engine (ACE) service. You can use ACE App-IDs in Security policy rules to gain visibility into cloud services and applications and control them.		N/A	Planned	√
Networking Services	**Description**		**Cloud NGFW for AWS**		**VM-Series**
			Native Policy Management (Rulestacks)	**Panorama Policy Management (Cloud Device Groups)**	
Application Override	You can configure Cloud NGFW to override the N/Armal Application Identification (App-ID) of specific traffic passing through the firewall. As soon as the Application Override policy takes effect, all further App-ID inspection of the traffic is stopped and the session is identified with the custom application signatures your provide		N/A	√	√
NAT	Palo Alto Networks Fiirewalls can enforce Destination NAT on your Ingress VPC traffic and Source NAT your Egress VPC traffic	**Ingress NAT**	NA	NA	√
		Egress NAT	Planned	Planned	√
		Private NAT	N/A	N/A	√

Policy Based Forwarding	Palo Alto Networks firewalls Policy Based Forwading rules allow traffic to take an alternative path for security or performance reasons. Let's say your company has two links between the corporate office and the branch office: a cheaper internet link and a more expensive leased line. For enhanced security, you can use PBF to send applications that aren’t encrypted traffic, such as FTP traffic, over the private leased line and all other traffic over the internet link. Or, for performance, you can choose to route business-critical applications over the leased line while sending all other traffic, such as web browsing, over the cheaper link.		NA	NA	√

Device Settings	Description		Cloud NGFW for AWS		VM-Series
			Native Management	**Panorama Management**	
Security Zones	Security zones are a logical way to group interfaces on the firewall, and Cloud NGFW endpoints to control and log the VPC traffic	**Private & Public zones**	NA	Planned	√
		Zone Mapping	NA	Planned	√
		VPC endpoint zones	NA	Planned	√
XFF	Traffic to your VPC workloads might have passed more than one proxy server (such as CDN or ALB) before it reaches the Cloud NGFW. If there's an existing XFF header, these proxies appends its IP address to it or adds the XFF header with its IP address. Therefore XFF request header may contain multiple IP addresses that are separated by commas. Cloud NGFW uses the The X-Forwarded-For (XFF) HTTP header field to identify the the original clieng IP address . Cloud NGFW always uses the most recently added address in the XFF header to enforce policy.		√	√	√
DNS Proxy	When you configure Cloud NGFW as a DNS proxy, it acts as an intermediary between clients and servers and as a DNS server by resolving queries from its DNS cache or forwarding queries to other DNS servers. Use this page to configure the settings that determine how the firewall serves as a DNS proxy.		NA	Planned	√
Interface Management	Palo Alto Neworks Firewalls allow you to configure VLANs, Virtual Wires Link Layer Discovery Protocol (LLDP) , Bidirectional Forwarding Detection (BFD) on its interfaces		NA	NA	√
Routing Management	Palo Alto Networks Firewalls allow you to configure Static Routing and Routing Protocols (BGP, BFD, OSPF, OSPFv3, multicast, RIPv2, and filters)		NA	NA	√
IPSec Tunnel Management	Palo Alto Neworks firewalls terminate IPSec tunnels and inpect tunneled traffic		NA	NA	√
Global Protect Management	Palo Alto Networks firewalls secure mobile workforce by specifyinfg algorithms for authentication and encryption in VPN tunnels between a GlobalProtect gateway module and client.		NA	NA	√
QoS	Palo Alto Networks' firewalls allow you to specify traffic that requires preferential treatment or bandwidth limiting. QoS rules allow you to dependably run high-priority applications and traffic under limited network capacity.		NA	NA	√
GRE Tunnel Management	Palo Alto Networks firewalls terminate Generic Routing Encapsulation (GRE) tunnels and inspect tunneled traffic		NA	NA	√
SD-WAN link Management	Palo Alto Networks firewalls bind multiple WAN connections (ADSL/DSL, cable modem, Ethernet, fiber, LTE/3G/4G/5G, MPLS, microwave/radio, satellite, WiFI) to a virtual interface and support dynamic, intelligent path selection based on applications and services and the conditions of links that each application or service is allowed to use.		NA	NA	√

Identity Services	Description		Cloud NGFW for AWS		VM-Series
			Native Policy Management (Rulestacks)	**Panorama Policy Management (Cloud Device Groups)**	
User-ID based policies	User-ID™, a standard feature on the Palo Alto Networks firewall, enables you to author user- and group-based policies. User-ID provides many mechanisms to collect this User Mapping information. For example, the User-ID agent monitors server logs for login events and listens for syslog messages from authenticating services. leverage user information stored in a wide range of repositories.		N/A	Planned	√
Panorama/Firewall based Identity Distribition	You can congfigure some firewalls to collect user-ID mapping information from various sources and then redistribute them to other firewalls such as Cloud NGFWs.		N/A	Planned	√
Cloud Identity Engine (CIE) Directory Sync	Cloud Identity Engine (Directory Sync) allows Palo Alto Networks Firewalls to access your Active Directory information, so that you can easily set up and manage security and decryption policies for users and groups.		N/A	√	√

Cloud Identity Engine (CIE) based Identity Distrubition	Cloud Identity Engine (User Context) collects and distributes IP address-to-user name mappings, IP port to username mappings, user tags IP address tags, Host IDs, and quarantine list information to Palo Alto Networks firewalls		N/A	Planned	√

Security Posture, Health Posture & Operations	**Description**		**Cloud NGFW for AWS**		**VM-Series**
			Native Management	**Panorama Management**	
Log Visualization	You can review the logs to verify a wealth of information on a given session or transaction. Some examples of this information are the user who initiated the session, the action (allow or deny) that the firewall performed on the session, and the source and destination ports, zones, and addresses.		√	√	√
Log Analytics	Allows you to monitor the traffic by applications, users, and content activity—URL categories, threats, security policies that effectively block data or files		N/A	√	√
Rule Usage Metrics	Rule usage monitoring helps you evaluate whether your policy implementation continues to match your enforcement needs		N/A	√	√
Policy Analysis & Optimization	Policy Analyzer analyzes your Cloud NGFW rules and recommends possible consolidation or removal of specific rules to meet your intended Security posture. it also checks for aN/Amalies, such as shadows, redundancies, generalizations, correlations, and consolidations in your rulebase. Policy Optimizer identifies port-based rules so you can convert them to application-based allow rules or add applications from a port-based rule to an existing application-based rule without compromising application availability.		NA	√	√
Operational Metrics	Palo Alto Networks firewallls natively publishes custom metrics to monitoring systems in palo Alto Networks (AIOPs) and the public cloud such as AWS® CloudWatch. These metrics allow you to assess firewall performance and usage patterns	**AIOPS**	Planned	Planned	√
		AWS Cloud Watch	√	√	√
Packet Capture	Palo Alto Networks firewall to perform a custom packet capture or a threat packet capture		Planned	Planned	√