**Perimeter Firewall assessment for IPND**

[**What is Perimeter Firewall?**](https://www.vmware.com/topics/glossary/content/perimeter-firewall)

## [What is Perimeter Firewall? | VMware Glossary](https://www.vmware.com/topics/glossary/content/perimeter-firewall)

**What are AWS Firewalls?**

## [AWS Firewalls | Barracuda Networks](https://www.barracuda.com/glossary/aws-firewall)

**AWS Web Application Firewall**

## [AWS WAF - Web Application Firewall - Amazon Web Services (AWS)](https://aws.amazon.com/waf/)

**How does AWS WAF protect your web applications?**

Protect your web applications from common web exploits. AWS WAF is a web application firewall that helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources.

### (Need to discuss on this with Shamim)

**AWS Network Firewall**

The AWS Network Firewall was announced last week. It’s a new service for AWS VPCs that provides a high availability, managed network firewall. It’s features include stateful inspection, intrusion prevention and detection, and web filtering to protect your virtual networks on AWS. It is delivered as a fully managed service.

## [The AWS Network Firewall - RedBear - Cloud Services (redbearit.com.au)](https://www.redbearit.com.au/aws/the-aws-network-firewall/)

Using next-generation firewalls (NGFWs) gives you deeper packet inspection capabilities because malware inside the packet’s contents—not just signs of malware in the header—can be detected. It is important to not only secure the perimeter of your network but the interior as well, particularly because a threat introduced by a connected user can work its way through your network without being detected by a perimeter firewall.

Sadly, the service doesn’t come for free! You can find the full pricing on the service product [page](https://aws.amazon.com/network-firewall/pricing/).

For 3 AZ endpoints, the cost is $850 per month plus traffic charges (at $0.065/GB). If you are running the Network Firewall though, you don’t have to pay for NAT Gateways so that brings the differential down to about $750 on top of running just NAT Gateways. This is US pricing as the service isn’t available in the Sydney region yet.

When is expected in Sydney Market?

**Differences between AWS Security Groups and Palo Alto Networks Virtual Firewall**

Need of Network Firewall explained through the below link which mandates the need for firewall

## [Differences between AWS Security Groups and Palo Alto Networks ... - Knowledge Base - Palo Alto Networks](https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClDGCA0)

**Managed Palo Alto egress firewall**

Currently used in legacy IPND. To use the same services in AWS, explained through below link.

Traffic control /  Architecture / Network Flow / Allow list Modification / Failover model / Scaling options / Backup and restore Options /Update Options / access model / event management / Metrics / Cloud Watch Integration / Panorama integration / Licensing Options explained through

## [Managed Palo Alto egress firewall - AWS Managed Services Introduction (amazon.com)](https://docs.aws.amazon.com/managedservices/latest/ams-intro/networking-palo-alto.html)

**Palo Alto egress firewall Licensing options summary**

The price of the AMS Managed Firewall depends on the type of license used, hourly or bring your own license (BYOL), and the instance size in which the appliance runs. You are required to order the instances size and the licenses of the Palo Alto firewall you prefer through AWS Marketplace.

* Marketplace Licenses: Accept the terms and conditions of the VM-Series Next-Generation Firewall Bundle 1 from the networking account in MALZ.
* BYOL Licenses: Accept the terms and conditions of the VM-Series Next-Generation Firewall (BYOL) from the networking account in MALZ and share the "BYOL auth code" obtained after purchasing the license to AMS.

Communication initiated with Telstra Licensing team to see if BYOL possible through Telstra.

**Limitations of Palo Alto egress firewall**

The AMS solution runs in Active-Active mode as each PA instance in its AZ handles egress traffic for their respected AZ. So, with two AZs, each PA instance handles egress traffic up to 5 Gbps and effectively provides overall 10 Gbps throughput across two AZs. The same is true for all limits in each AZ. Should the AMS health check fail, we shift traffic from the AZ with the bad PA to another AZ, and during the instance replacement, capacity is reduced to the remaining AZs limits.

AMS does not currently support other Palo Alto bundles available on AWS Marketplace; for example, you cannot ask for the "VM-Series Next-Generation Firewall Bundle 2". Note that the AMS Managed Firewall solution using Palo Alto currently provides only an egress traffic filtering offering, so using advanced VM-Series bundles would not provide any additional features or benefits.

**Onboarding requirements**

* You must review and accept the Terms and Conditions of the VM-Series Next-Generation Firewall from Palo Alto in AWS Marketplace.
* You must confirm the instance size you want to use based on your expected workload.
* You must provide a /24 CIDR Block that does not conflict with networks in your Multi-Account Landing Zone environment or On-Prem. It must be of same class as the Egress VPC (the Solution provisions a /24 VPC extension to the Egress VPC).

**Pricing**

AMS Managed Firewall base infrastructure costs are divided in three main drivers: the EC2 instance that hosts the Palo Alto firewall, the software license Palo Alto VM-Series licenses, and CloudWatch Integrations.

* EC2 Instances: The Palo Alto firewall runs in a high-availability model of 2-3 EC2 instances, where instance is based on expected workloads. Cost for the instance depends on the region and number of AZs
* Ex. us-east-1, m5.xlarge, 3AZs
* $0.192 \* 24 \* 30 \* 3 = $414.72
* <https://aws.amazon.com/ec2/pricing/on-demand/>
* Palo Alto Licenses: The software license cost of a Palo Alto VM-300 next-generation firewall depends on the number of AZ as well as instance type.
* Ex. us-east-1, m5.xlarge, 3AZs
* $0.87 \* 24 \* 30 \* 3 = $1879.20
* <https://aws.amazon.com/marketplace/pp/B083M7JPKB?ref_=srh_res_product_title#pdp-pricing>
* CloudWatch Logs Integration: CloudWatch logs integration utilizes SysLog servers (EC2 - t3.medium), NLB, and CloudWatch Logs. The cost of the servers is based on region and number of AZs, and the cost of the NLB/CloudWatch logs varies based on traffic utilization.
* Ex. us-east-1, t3.medium, 3AZ
* $0.0416 \* 24 \* 30 \* 3 = $89.86
* <https://aws.amazon.com/ec2/pricing/on-demand/>
* <https://aws.amazon.com/cloudwatch/pricing/>