**IPND Firewall Build Document**

**About the VM-Series Firewall**

The Palo Alto Networks VM-Series firewall is the virtualized form of the Palo Alto Networks next-generation firewall. It is positioned for use in a virtualized or cloud environment where it can protect and secure east-west and north-south traffic.

The VM-Series firewall secures inbound and outbound traffic to and from [EC2](https://docs.paloaltonetworks.com/content/techdocs/en_US/vm-series/9-0/vm-series-deployment/set-up-the-vm-series-firewall-on-aws/about-the-vm-series-firewall-on-aws/aws-terminology.html#id746e6e03-a9b8-4425-9b51-03b1c8da54d1_id80095e9e-192f-40dd-8f6e-3313a2d9d8a5) instances within the AWS Virtual Private Cloud ([VPC](https://docs.paloaltonetworks.com/content/techdocs/en_US/vm-series/9-0/vm-series-deployment/set-up-the-vm-series-firewall-on-aws/about-the-vm-series-firewall-on-aws/aws-terminology.html#id746e6e03-a9b8-4425-9b51-03b1c8da54d1_id9751e221-e1cd-4646-a67f-feaf95bc1851)). Because the AWS VPC only supports an IP network (Layer 3 networking capabilities), the VM-Series firewall can only be deployed with Layer 3 interfaces.

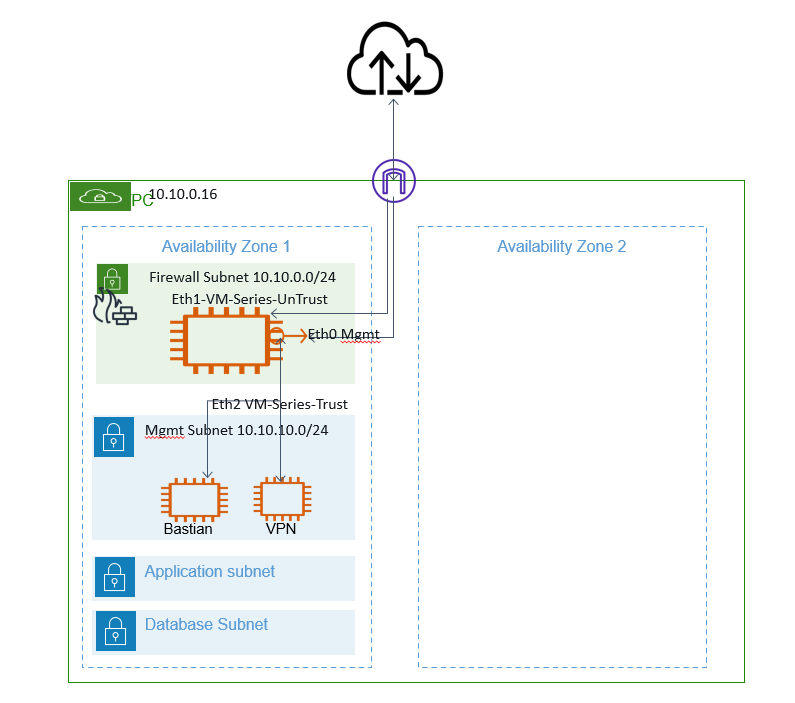
When users need to access the applications in the private subnet, the firewall receives the request and directs it to the appropriate application, after verifying security policy and performing Destination NAT. On the return path, the firewall receives the traffic, applies security policy and uses Source NAT to deliver the content to the user.

**Manage Subscriptions in AWS**

Manage Palo Alto Subscription through

<https://console.aws.amazon.com/marketplace/home?region=ap-southeast-2#/subscriptions>

Non Production IPND Firewall Design



[**Deploy the VM-Series Firewall on AWS**](https://docs.paloaltonetworks.com/content/techdocs/en_US/vm-series/9-0/vm-series-deployment/set-up-the-vm-series-firewall-on-aws/deploy-the-vm-series-firewall-on-aws.html#id7b5212c9-770f-411f-a449-e7a075a6a330)

**Obtain the AMI**

The AMI for the VM-Series firewall is available in the AWS Marketplace for both the [Bring Your Own License](https://docs.paloaltonetworks.com/vm-series/9-0/vm-series-deployment/license-the-vm-series-firewall/license-typesvm-series-firewalls.html) (BYOL) and the [Usage-based](https://docs.paloaltonetworks.com/vm-series/9-0/vm-series-deployment/license-the-vm-series-firewall/license-typesvm-series-firewalls.html) pricing options.

<https://aws.amazon.com/marketplace/pp/prodview-ccntnbzdod74k?ref_=aws-mp-console-subscription-detail>

<https://docs.paloaltonetworks.com/vm-series/9-0/vm-series-deployment/set-up-the-vm-series-firewall-on-aws/deploy-the-vm-series-firewall-on-aws/obtain-the-ami/ami-in-the-public-aws-cloud.html#ide03acaec-b3b4-4928-bf7e-48224d042094>

**Get the VM-Series Firewall Amazon Machine Image (AMI) ID**

<https://docs.paloaltonetworks.com/vm-series/9-0/vm-series-deployment/set-up-the-vm-series-firewall-on-aws/deploy-the-vm-series-firewall-on-aws/obtain-the-ami/get-amazon-machine-image-ids.html#idbbf4f307-3aaf-44e3-8ce9-04c0a8140330>

**Planning Worksheet for the VM-Series in the AWS VPC**

Planning Worksheet for the VM-Series in the AWS VPC For ease of deployment, plan the subnets within the VPC and the EC2 instances that you want to deploy within each subnet. Before you begin, use the following table to collate the network information required to deploy and insert the VM-Series firewall into the traffic flow in the VPC:

|  |  |
| --- | --- |
| Configuration Item | Value |
| VPC CIDR | 10.10.0.0/16 |
| Security Groups |  |
| Subnet (public) CIDR | 10.10.0.0/24 |
| Subnet (private) CIDR | 10.10.10.0/24 |
| Subnet (public) Route Table |  |
| Subnet (private) Route Table |  |
| Security Groups  • Rules for Management Access to the firewall (eth0/0)  • Rules for access to the dataplane interfaces of the firewall  • Rules for access to the interfaces assigned to the application servers. | sg-0a2cc8ded9ddd5d25 – devFwSG  (This security group is for restricting access to the management interface of the firewall. At a minimum consider enabling https and ssh access for the management interface.)  **Inbound rules**  Ssh tcp 22  HTTPS tcp 443  **Outbound rules (1/1)**  All traffic all 0.0.0.0/0  sg-0d7abb6dccaebf98d - devPublicSG    sg-0f43f1bc3c7aa5c6d – devBastSG    sg-0bf63cf29d6346829 - dev-vpn-sg |
| VM-Series firewall behind ELB |  |
| Requirements for HA | If you are deploying the VM-Series firewalls in a high availability (active/passive) configuration, you must ensure the following:   * Create an IAM role and assign the role to the VM-Series firewall when you are deploying the instance. See [IAM Roles for HA](https://docs.paloaltonetworks.com/content/techdocs/en_US/vm-series/9-0/vm-series-deployment/set-up-the-vm-series-firewall-on-aws/high-availability-for-vm-series-firewall-on-aws/iam-roles-for-ha.html#idf93e45a7-362d-49f5-88e2-f5fdf37a93dc). * Deploy the HA peers in the same AWS availability zone. * The active firewall in the HA pair must have at a minimum three ENIs: two dataplane interfaces and one management interface.   The passive firewall in the HA pair, must have one ENI for management, and one ENI that functions as dataplane interface; you will configure the dataplane interface as an HA2 interface.  Do not attach additional dataplane interfaces to the passive firewall in the HA pair. On failover, the dataplane interfaces from the previously active firewall are moved —detached and then attached—to the now active (previously passive) firewall. |

|  |  |
| --- | --- |
| EC2 Instance 1 (VM-Series firewall) | i-0e511013802107bb1 (dfw01-1) |
| Subnet | subnet-062ef1f8022699b40 / newdev Firewall Subnet (AZ1) |
| Instance type: | m3.xlarge |
| Mgmt interface IP: | 10.10.0.5 |
| Mgmt interface EIP: | 52.65.69.213 |
| Dataplane interface eth1/1   * Private IP: * EIP (if required): * Security Group: | eni-0cc355d7be75780ff (VM-Series-UnTrust)  10.10.10.176  sg-0d7abb6dccaebf98d - devPublicSG |
| Dataplane interface eth1/2   * Private IP: * EIP (if required): * Security Group: | eni-0b2dbd95de83275bd (VM-Series-Trust)  10.10.10.83  [sg-08f751d5c173c2653 (devVPNSG)](https://ap-southeast-2.console.aws.amazon.com/ec2/v2/home?region=ap-southeast-2#SecurityGroup:groupId=sg-08f751d5c173c2653)  [sg-0f43f1bc3c7aa5c6d (devBastSG)](https://ap-southeast-2.console.aws.amazon.com/ec2/v2/home?region=ap-southeast-2#SecurityGroup:groupId=sg-0f43f1bc3c7aa5c6d) |

|  |  |
| --- | --- |
| EC2 Instance 2 (Bastian Instance) | i-0fe52523d4e6cf414 (dbast01-1) |
| Subnet | [subnet-033eed40ff43102a5 (newdev Public Subnet (AZ1))](https://ap-southeast-2.console.aws.amazon.com/vpc/home?region=ap-southeast-2#subnets:subnetId=subnet-033eed40ff43102a5) |
| Instance type: | t3.large |
| Mgmt interface IP: |  |
| Default gateway |  |
| Dataplane interface 1   * Private IP: | 10.10.10.10 |

|  |  |
| --- | --- |
| EC2 Instance 2 (VPN Instance) | i-07a8bdde8fc76f477 (dvpn01-1) |
| Subnet | [subnet-033eed40ff43102a5 (newdev Public Subnet (AZ1))](https://ap-southeast-2.console.aws.amazon.com/vpc/home?region=ap-southeast-2#subnets:subnetId=subnet-033eed40ff43102a5) |
| Instance type: | t3.large |
| Mgmt interface IP: |  |
| Default gateway |  |
| Dataplane interface 1   * Private IP: | 10.10.10.20 |

**Launch the VM-Series Firewall on AWS**

<https://docs.paloaltonetworks.com/vm-series/9-0/vm-series-deployment/set-up-the-vm-series-firewall-on-aws/deploy-the-vm-series-firewall-on-aws/launch-the-vm-series-firewall-on-aws.html#ide07b93a2-ccb3-4c69-95fe-96e3328b8514>