# IPND VPC Design Overview



## Dev VPC: 10.10.0.0/16

Firewall Subnet (AZ1) subnet-062ef1f8022699b40 10.10.0.0/24

Firewall Subnet (AZ2) subnet-0ddd6117c5abdddfa 10.10.1.0/24

Presentation Subnet (AZ1) subnet-033eed40ff43102a5 10.10.10.0/24

Presentation Subnet (AZ2) subnet-04dfda0c04b3af13d 10.10.11.0/24

Application Subnet (AZ1) subnet-04e04dd3d9b4d8262 10.10.20.0/24

Application Subnet (AZ2) subnet-0cf210c6c75085de7 10.10.21.0/24

Database Subnet (AZ1) subnet-0ab5e8d4f43bc4f3a 10.10.30.0/24

Database Subnet (AZ2) subnet-09b2ab0b6596c51c7 10.10.31.0/24

## Test VPC: 10.11.0.0/16

Firewall Subnet (AZ1) subnet-062ef1f8022699b40 10.11.0.0/24

Firewall Subnet (AZ2) subnet-0ddd6117c5abdddfa 10.11.2.0/24

Presentation Subnet (AZ1) subnet-033eed40ff43102a5 10.11.10.0/24

Presentation Subnet (AZ2) subnet-04dfda0c04b3af13d 10.11.11.0/24

Application Subnet (AZ1) subnet-04e04dd3d9b4d8262 10.11.20.0/24

Application Subnet (AZ2) subnet-0cf210c6c75085de7 10.11.21.0/24

Database Subnet (AZ1) subnet-0ab5e8d4f43bc4f3a 10.11.30.0/24

Database Subnet (AZ2) subnet-09b2ab0b6596c51c7 10.11.31.0/24

## Prod VPC: 10.12.0.0/16

Firewall Subnet (AZ1) subnet-062ef1f8022699b40 10.12.0.0/24

Firewall Subnet (AZ2) subnet-0ddd6117c5abdddfa 10.12.1.0/24

Presentation Subnet (AZ1) subnet-033eed40ff43102a5 10.12.10.0/24

Presentation Subnet (AZ2) subnet-04dfda0c04b3af13d 10.12.11.0/24

Application Subnet (AZ1) subnet-04e04dd3d9b4d8262 10.12.20.0/24

Application Subnet (AZ2) subnet-0cf210c6c75085de7 10.12.21.0/24

Database Subnet (AZ1) subnet-0ab5e8d4f43bc4f3a 10.12.30.0/24

Database Subnet (AZ2) subnet-09b2ab0b6596c51c7 10.12.31.0/24

# Server Ips:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| DEV - 10.10.0.0/16 | | TEST - 10.11.0.0/16 | | PROD - 10.12.0.0/16 | | |
| Host | **IP** | Host | **IP** | Host | **IP** | AZ |
| ~~dfw01-1~~ | **~~10.10.0.5~~** | ~~tfw01-1~~ | **~~10.11.0.5~~** | ~~pfw01-1~~ | **~~10.12.0.5~~** | ~~1~~ |
| ~~dfw01-2~~ | **~~10.10.1.5~~** | ~~tfw01-2~~ | **~~10.11.2.5~~** | ~~pfw01-2~~ | **~~10.12.1.5~~** | ~~2~~ |
| dbast01-1 | **10.10.10.10** | tbast01-1 | **10.11.10.10** | pbast01-1 | **10.12.10.10** | 1 |
| dbast01-2 | **10.10.11.10** | tbast01-2 | **10.11.11.10** | pbast01-2 | **10.12.11.10** | 2 |
| dvpn01-1 | **10.10.10.20** | tvpn01-1 | **10.11.10.20** | pvpn01-1 | **10.12.10.20** | 1 |
| dvpn01-2 | **10.10.11.20** | tvpn01-2 | **10.11.11.20** | pvpn01-2 | **10.12.11.20** | 2 |
| dadm01-1 | **10.10.20.30** | tadm01-1 | **10.11.20.30** | padm01-1 | **10.12.20.30** | 1 |
| dadm01-2 | **10.10.21.30** | tadm01-2 | **10.11.21.30** | padm01-2 | **10.12.21.30** | 2 |
| dfts01-1 | **10.10.20.40** | tfts01-1 | **10.11.20.40** | pfts01-1 | **10.12.20.40** | 1 |
| dfts01-2 | **10.10.21.40** | tfts01-2 | **10.11.21.40** | pfts01-2 | **10.12.21.40** | 2 |
| dwbs01-1 | **10.10.20.50** | twbs01-1 | **10.11.20.50** | pwbs01-1 | **10.12.20.50** | 1 |
| dwbs01-2 | **10.10.21.50** | twbs01-2 | **10.11.21.50** | pwbs01-2 | **10.12.21.50** | 2 |
| dcore01-1 | **10.10.20.60** | tcore01-1 | **10.11.20.60** | pcore01-1 | **10.12.20.60** | 1 |
| dcore01-2 | **10.10.21.60** | tcore01-2 | **10.11.21.60** | pcore01-2 | **10.12.21.60** | 2 |
| daps01-1 | **10.10.20.70** | taps01-1 | **10.11.20.70** | paps01-1 | **10.12.20.70** | 1 |
| daps01-2 | **10.10.21.70** | taps01-2 | **10.11.21.70** | paps01-2 | **10.12.21.70** | 2 |
|  |  |  |  | ufts01-1 | **10.12.40.40** | 1 |
|  |  |  |  | ufts01-2 | **10.12.41.40** | 2 |
|  |  |  |  | uwbs01-1 | **10.12.40.50** | 1 |
|  |  |  |  | uwbs01-2 | **10.12.41.50** | 2 |
|  |  |  |  | ucore01-1 | **10.12.40.60** | 1 |
|  |  |  |  | ucore01-2 | **10.12.41.60** | 2 |
|  |  |  |  | uaps01-1 | **10.12.40.70** | 1 |
|  |  |  |  | uaps01-2 | **10.12.41.70** | 2 |

Note: AWS n/w Firewall used and auto assigns IP from the subnet range.

# Route Tables:



## Dev Firewall Subnet:

|  |  |  |
| --- | --- | --- |
| **Destination** | **Target** | **Comments** |
| 0.0.0.0/0 | [igw-046dc36f22e712278](https://ap-southeast-2.console.aws.amazon.com/vpc/home?region=ap-southeast-2#igws:internetGatewayId=igw-046dc36f22e712278) | Internet Gateway for external traffic |
| 10.10.0.0/16 | local | Local Router within the VPC |

## Dev Public Subnet:

|  |  |  |
| --- | --- | --- |
| **Destination** | **Target** | **Comments** |
| 10.11.110.8/32 | [eni-0926488b6440d5e73](https://ap-southeast-2.console.aws.amazon.com/ec2/home?region=ap-southeast-2#NIC:networkInterfaceId=eni-0926488b6440d5e73) | VPN server to FTS floating IP. Target automatically gets updated via start-up script to the applicable ENI based on the server zone |
| 10.10.0.0/16 | local | Local Router within the VPC |
| 0.0.0.0/0 | [vpce-0006390e9890f3abc](https://ap-southeast-2.console.aws.amazon.com/vpc/home?region=ap-southeast-2#Endpoints:vpcEndpointId=vpce-0006390e9890f3abc),  [vpce-0059471415b232bb3](https://ap-southeast-2.console.aws.amazon.com/vpc/home?region=ap-southeast-2#Endpoints:vpcEndpointId=vpce-0059471415b232bb3) | Firewall Endpoint for external traffic |

## Dev Private Subnets:

|  |  |  |
| --- | --- | --- |
| **Destination** | **Target** | **Comments** |
| 10.11.119.0/24 | [eni-0a580f45595e5dbd8](https://ap-southeast-2.console.aws.amazon.com/ec2/home?region=ap-southeast-2#NIC:networkInterfaceId=eni-0a580f45595e5dbd8) | FTS to VPN Traffic (Dynamic Range). Target automatically gets updated via start-up script to the applicable ENI based on the server zone |
| 10.11.120.0/22 | [eni-0a580f45595e5dbd8](https://ap-southeast-2.console.aws.amazon.com/ec2/home?region=ap-southeast-2#NIC:networkInterfaceId=eni-0a580f45595e5dbd8) | FTS to VPN Traffic (Static Range). Target automatically gets updated via start-up script to the applicable ENI based on the server zone |
| 10.10.0.0/16 | local | Local Router within the VPC |
| 0.0.0.0/0 | [nat-0db46ac32d6d83358](https://ap-southeast-2.console.aws.amazon.com/vpc/home?region=ap-southeast-2#NatGateways:natGatewayId=nat-0db46ac32d6d83358),  [nat-0032c45bdc264fe6b](https://ap-southeast-2.console.aws.amazon.com/vpc/home?region=ap-southeast-2#NatGateways:natGatewayId=nat-0032c45bdc264fe6b) | NAT Gateway for external traffic |

## Test Firewall Subnet;

|  |  |  |
| --- | --- | --- |
| **Destination** | **Target** | **Comments** |
| 0.0.0.0/0 | [igw-0c729a37162d7ecf8](https://ap-southeast-2.console.aws.amazon.com/vpc/home?region=ap-southeast-2#igws:internetGatewayId=igw-0c729a37162d7ecf8) | Internet Gateway for external traffic |
| 10.11.0.0/16 | local | Local Router within the VPC |

## Test Public Subnet:

|  |  |  |
| --- | --- | --- |
| **Destination** | **Target** | **Comments** |
| 10.10.110.8/32 | [eni-0b93e97c715c62abf](https://ap-southeast-2.console.aws.amazon.com/ec2/home?region=ap-southeast-2#NIC:networkInterfaceId=eni-0b93e97c715c62abf) | VPN server to FTS floating IP. Target automatically gets updated via start-up script to the applicable ENI based on the server zone |
| 10.11.0.0/16 | local | Local Router within the VPC |
| 0.0.0.0/0 | [vpce-058de1ff3675cb01e](https://ap-southeast-2.console.aws.amazon.com/vpc/home?region=ap-southeast-2#Endpoints:vpcEndpointId=vpce-058de1ff3675cb01e),  [vpce-0b6e34ba837921ca2](https://ap-southeast-2.console.aws.amazon.com/vpc/home?region=ap-southeast-2#Endpoints:vpcEndpointId=vpce-0b6e34ba837921ca2) | Firewall Endpoint for external traffic |

## Test Private Subnets:

|  |  |  |
| --- | --- | --- |
| **Destination** | **Target** | **Propagated** |
| 10.10.119.0/24 | [eni-0e508b717b11ed90a](https://ap-southeast-2.console.aws.amazon.com/ec2/home?region=ap-southeast-2#NIC:networkInterfaceId=eni-0e508b717b11ed90a) | FTS to VPN Traffic (Dynamic Range). Target automatically gets updated via start-up script to the applicable ENI based on the server zone |
| 10.10.120.0/22 | [eni-0e508b717b11ed90a](https://ap-southeast-2.console.aws.amazon.com/ec2/home?region=ap-southeast-2#NIC:networkInterfaceId=eni-0e508b717b11ed90a) | FTS to VPN Traffic (Static Range). Target automatically gets updated via start-up script to the applicable ENI based on the server zone |
| 10.11.0.0/16 | local | Local Router within the VPC |
| 0.0.0.0/0 | [nat-0652e2c2de206b93d](https://ap-southeast-2.console.aws.amazon.com/vpc/home?region=ap-southeast-2#NatGateways:natGatewayId=nat-0652e2c2de206b93d),  [nat-051906077d108bb31](https://ap-southeast-2.console.aws.amazon.com/vpc/home?region=ap-southeast-2#NatGateways:natGatewayId=nat-051906077d108bb31) | NAT Gateway for external traffic |
| [pl-6ca54005](https://ap-southeast-2.console.aws.amazon.com/vpc/home?region=ap-southeast-2#ManagedPrefixLists:PrefixListId=pl-6ca54005) | [vpce-09a9f3e607bda2efc](https://ap-southeast-2.console.aws.amazon.com/vpc/home?region=ap-southeast-2#Endpoints:vpcEndpointId=vpce-09a9f3e607bda2efc) | Route to S3 Endpoint to avoid S3 traffic via internet |
| 10.0.12.35/32 | [vgw-0e04ba160688575ef](https://ap-southeast-2.console.aws.amazon.com/vpc/home?region=ap-southeast-2#VpnGateways:VpnGatewayId=vgw-0e04ba160688575ef) | Route to Virtual Private Gateway for Site-to-site |

## Prod Firewall Subnet:

|  |  |  |
| --- | --- | --- |
| **Destination** | **Target** | **Comments** |
| 10.12.0.0/16 | local | Local Router within the VPC |
| 0.0.0.0/0 | [igw-0801527e5df73894c](https://ap-southeast-2.console.aws.amazon.com/vpc/home?region=ap-southeast-2#igws:internetGatewayId=igw-0801527e5df73894c) | Internet Gateway for external traffic |

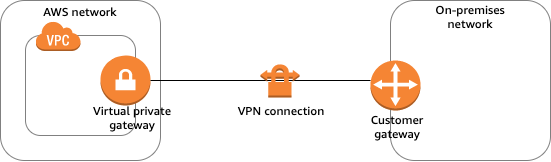
## Prod Public Subnets:

|  |  |  |
| --- | --- | --- |
| **Destination** | **Target** | **Comments** |
| 10.10.110.8/32 | [eni-0829e680566ae9d09](https://ap-southeast-2.console.aws.amazon.com/ec2/home?region=ap-southeast-2#NIC:networkInterfaceId=eni-0829e680566ae9d09) | VPN server to PFTS floating IP. Target automatically gets updated via start-up script to the applicable ENI based on the server zone |
| 10.11.110.8/32 | [eni-0c7921d84174d7ff2](https://ap-southeast-2.console.aws.amazon.com/ec2/home?region=ap-southeast-2#NIC:networkInterfaceId=eni-0c7921d84174d7ff2) | VPN server to UFTS floating IP. Target automatically gets updated via start-up script to the applicable ENI based on the server zone |
| 10.0.12.0/24 | [vgw-091d3001f461dde24](https://ap-southeast-2.console.aws.amazon.com/vpc/home?region=ap-southeast-2#VpnGateways:VpnGatewayId=vgw-091d3001f461dde24) | Route to Virtual Private Gateway for Site-to-site |
| 10.0.13.0/24 | [vgw-091d3001f461dde24](https://ap-southeast-2.console.aws.amazon.com/vpc/home?region=ap-southeast-2#VpnGateways:VpnGatewayId=vgw-091d3001f461dde24) | Route to Virtual Private Gateway for Site-to-site |
| 10.0.14.0/24 | [vgw-091d3001f461dde24](https://ap-southeast-2.console.aws.amazon.com/vpc/home?region=ap-southeast-2#VpnGateways:VpnGatewayId=vgw-091d3001f461dde24) | Route to Virtual Private Gateway for Site-to-site |
| 10.0.15.0/24 | [vgw-091d3001f461dde24](https://ap-southeast-2.console.aws.amazon.com/vpc/home?region=ap-southeast-2#VpnGateways:VpnGatewayId=vgw-091d3001f461dde24) | Route to Virtual Private Gateway for Site-to-site |
| 10.12.0.0/16 | local | Local Router within the VPC |
| 0.0.0.0/0 | [vpce-09a6bdca859341990](https://ap-southeast-2.console.aws.amazon.com/vpc/home?region=ap-southeast-2#Endpoints:vpcEndpointId=vpce-09a6bdca859341990),  [vpce-00f9863797a1df131](https://ap-southeast-2.console.aws.amazon.com/vpc/home?region=ap-southeast-2#Endpoints:vpcEndpointId=vpce-00f9863797a1df131) | Firewall Endpoint for external traffic |

## Prod Private Subnets:

|  |  |  |
| --- | --- | --- |
| **Destination** | **Target** | **Comments** |
| 10.10.119.0/24 | [eni-067c1834b42e27240](https://ap-southeast-2.console.aws.amazon.com/ec2/home?region=ap-southeast-2#NIC:networkInterfaceId=eni-067c1834b42e27240) | PFTS to VPN Traffic (Dynamic Range). Target automatically gets updated via start-up script to the applicable ENI based on the server zone |
| 10.10.120.0/22 | [eni-067c1834b42e27240](https://ap-southeast-2.console.aws.amazon.com/ec2/home?region=ap-southeast-2#NIC:networkInterfaceId=eni-067c1834b42e27240) | PFTS to VPN Traffic (Static Range). Target automatically gets updated via start-up script to the applicable ENI based on the server zone |
| 10.12.0.0/16 | local | Local Router within the VPC |
| 0.0.0.0/0 | [nat-006216427f3069cd5](https://ap-southeast-2.console.aws.amazon.com/vpc/home?region=ap-southeast-2#NatGateways:natGatewayId=nat-006216427f3069cd5) | NAT Gateway for external traffic |
| [pl-6ca54005](https://ap-southeast-2.console.aws.amazon.com/vpc/home?region=ap-southeast-2#ManagedPrefixLists:PrefixListId=pl-6ca54005) | [vpce-0cd9a5c25260dea8b](https://ap-southeast-2.console.aws.amazon.com/vpc/home?region=ap-southeast-2#Endpoints:vpcEndpointId=vpce-0cd9a5c25260dea8b) | Route to S3 Endpoint to avoid S3 traffic via internet |
| 10.0.10.40/32 | [vgw-091d3001f461dde24](https://ap-southeast-2.console.aws.amazon.com/vpc/home?region=ap-southeast-2#VpnGateways:VpnGatewayId=vgw-091d3001f461dde24) | Route to Virtual Private Gateway for Site-to-site |
| 10.0.10.45/32 | [vgw-091d3001f461dde24](https://ap-southeast-2.console.aws.amazon.com/vpc/home?region=ap-southeast-2#VpnGateways:VpnGatewayId=vgw-091d3001f461dde24) | Route to Virtual Private Gateway for Site-to-site |
| 10.0.11.40/32 | [vgw-091d3001f461dde24](https://ap-southeast-2.console.aws.amazon.com/vpc/home?region=ap-southeast-2#VpnGateways:VpnGatewayId=vgw-091d3001f461dde24) | Route to Virtual Private Gateway for Site-to-site |
| 10.0.12.0/24 | [vgw-091d3001f461dde24](https://ap-southeast-2.console.aws.amazon.com/vpc/home?region=ap-southeast-2#VpnGateways:VpnGatewayId=vgw-091d3001f461dde24) | Route to Virtual Private Gateway for Site-to-site |
| 10.0.13.0/24 | [vgw-091d3001f461dde24](https://ap-southeast-2.console.aws.amazon.com/vpc/home?region=ap-southeast-2#VpnGateways:VpnGatewayId=vgw-091d3001f461dde24) | Route to Virtual Private Gateway for Site-to-site |
| 10.0.14.0/24 | [vgw-091d3001f461dde24](https://ap-southeast-2.console.aws.amazon.com/vpc/home?region=ap-southeast-2#VpnGateways:VpnGatewayId=vgw-091d3001f461dde24) | Route to Virtual Private Gateway for Site-to-site |
| 10.0.15.0/24 | [vgw-091d3001f461dde24](https://ap-southeast-2.console.aws.amazon.com/vpc/home?region=ap-southeast-2#VpnGateways:VpnGatewayId=vgw-091d3001f461dde24) | Route to Virtual Private Gateway for Site-to-site |

# Site-to-site VPN:



Ref: [AWS Site-to-Site VPN (amazon.com)](https://docs.aws.amazon.com/vpn/latest/s2svpn/VPC_VPN.html)

## Test Env

Customer Gateway: ipndtest-legacy-cgw

Virtual Private Gateway: ipndtest-legacy-vgw

Site-to-site connection: ipndtest-legacy-arp-bridge

## Prod Env

### Primary

Customer Gateway: ipndprod-legacy-cgw

Virtual Private Gateway: ipndprod-legacy-vgw

Site-to-site connection: ipndarp-legacy-bridge

### ARP

Customer Gateway: ipndarp-legacy-cgw

Virtual Private Gateway: ipndprod-legacy-vgw

Site-to-site connection: ipndprod-legacy-bridge