**Secure EC2 Instances**

1. One would need a **VPC**. A VPC is short for **Virtual Private Cloud.** A VPC is a dedicated virtual network for your AWS account. It's logically separated from the rest of the AWS Cloud's virtual networks.
2. Another way to secure ECT is to implement **MFA**, which stands for **multi-factor authentication.** This is to prevent any users that does not have the rights to login into accounts without a security token.
3. **For each subnet, create a separate route table.** A route table is made up of a set of rules called routes that control where network traffic from your subnet or gateway goes. Which ties into number one (VPC) because each subnet must be associated with a route table to see where the traffic going.
4. We have **VM-Series firewall**. The Amazon Web Services (AWS) public cloud and AWS GovCloud both support the VM-Series firewall. It can then be set up to secure access to applications hosted on EC2 instances and stored in an AWS Virtual Private Cloud (VPC).

**Common vulnerabilities**

1. **Use of Public Subnets in Excess:** This strategy, however, can be highly harmful. Public subnets are routed to Internet gateways, which make them available to the public. As a result, any sensitive data stored on the subnet is exposed to attack. Which result to what I said above about “**Private Subnets**”
2. **Database Origin Servers That Have Been Revealed:** Unless particularly requested, the IP addresses of database origin servers should never be made visible to any person or application.
3. **Request Forgery on the Server (SSRF):** Is an attempt to obtain access to instance metadata by abusing lawful AWS features. An attacker may be able to obtain credentials for an IAM role associated with the instance and achieve privileged access to the target application if they are successful.

**Link**

[Use Case: Secure the EC2 Instances in the AWS Cloud (paloaltonetworks.com)](https://docs.paloaltonetworks.com/vm-series/9-1/vm-series-deployment/set-up-the-vm-series-firewall-on-aws/use-case-secure-the-ec2-instances-in-the-aws-cloud)

[Message from Cobalt](https://cobalt.io/blog/aws-cloud-security)