Amazon Elastic Cloud Compute (EC2): EC2 Security Features

Andru Estes
Principal Author
andru-estes

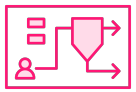
Connecting to EC2 Instances with Bastion Hosts

Bastion Host

Servers running at the edge of a network allowing secured and controlled access into your private network.
Sometimes referred to as a jump server.

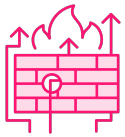
Bastion Hosts and Jump Servers

Setup to control and allow external connections into your private network



Serves as a middle point (jump server) to connect to private resources

Typically deployed into a public subnet



Primarily going to leverage SSH (Port 22) for initial connections

Be sure to set up other security group rules correctly if using these!

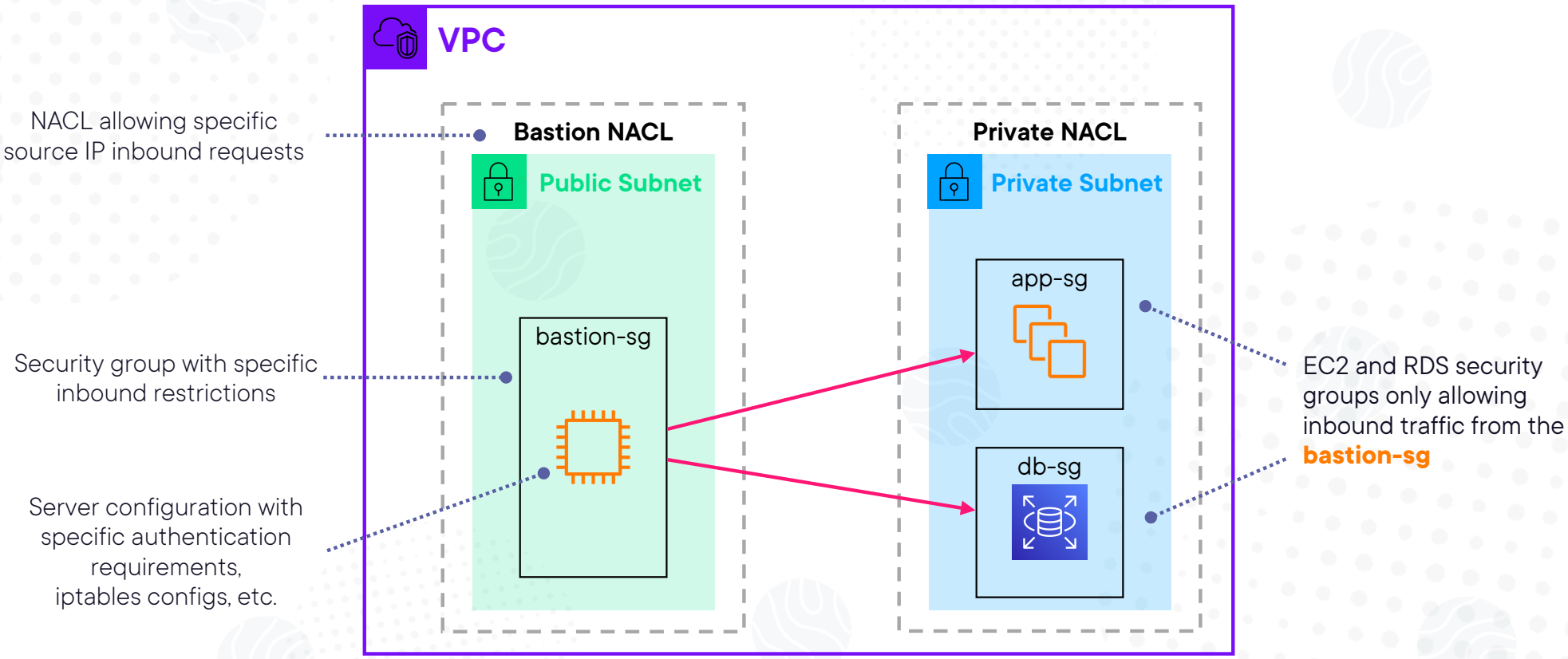
Bastion Hosts

Should be locked down to a small set of allowed users or IP ranges

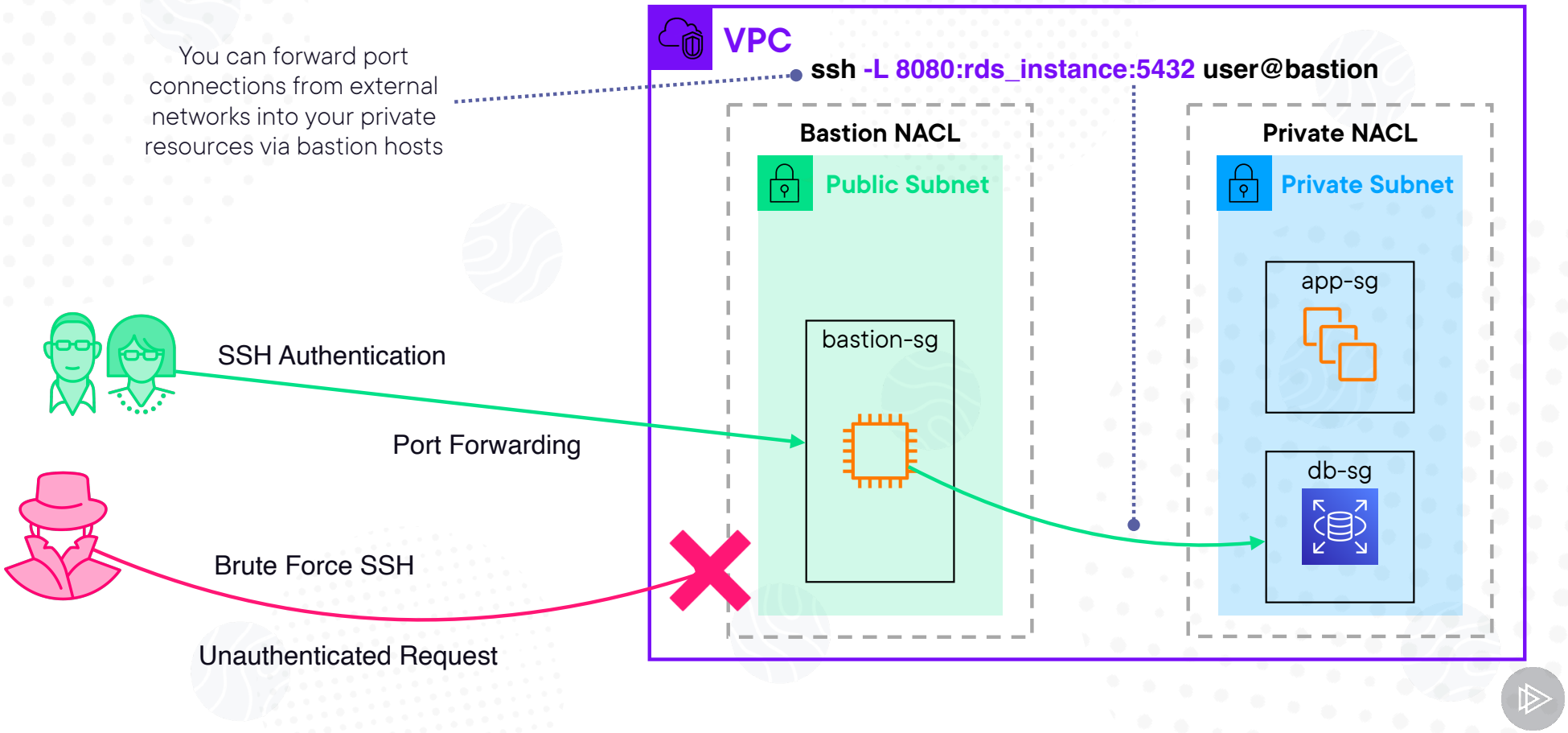
Their firewalls can be leveraged to perform port forwarding and implement other security controls

Force authentication and security requirements, and log connections

Bastion Host Architecture Example

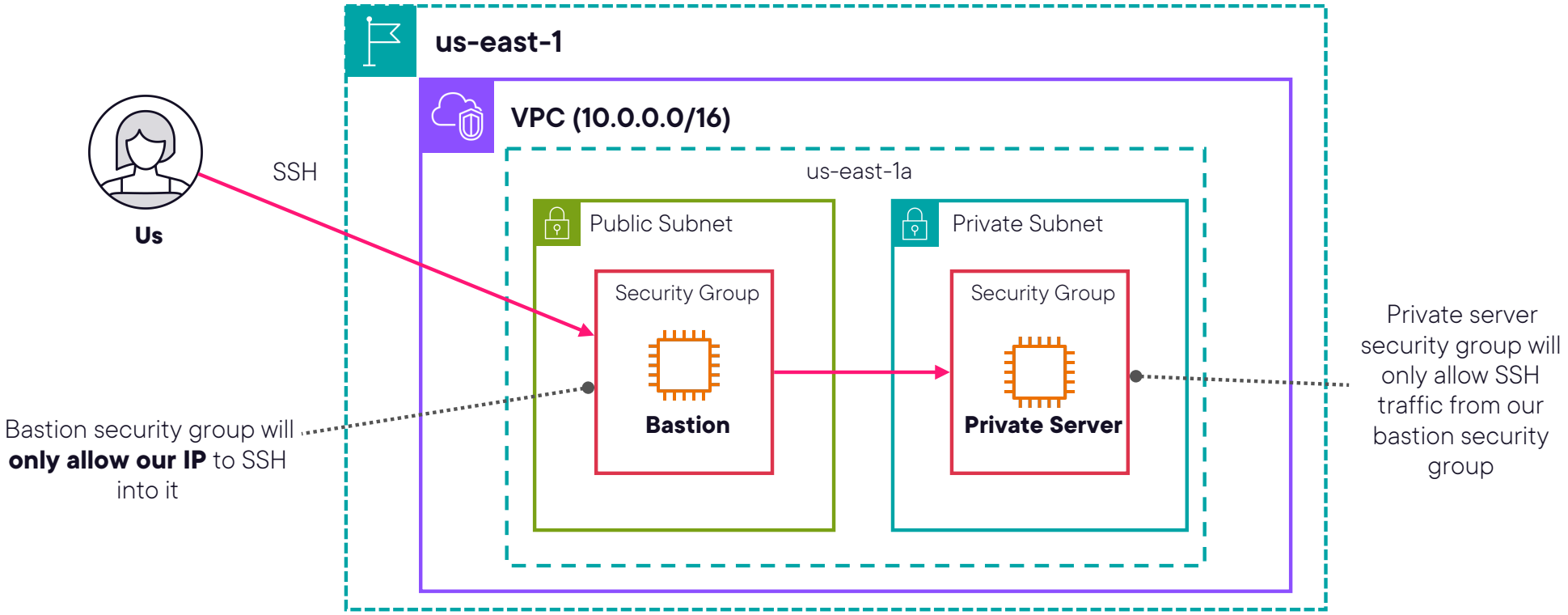


Bastion Host Architecture Port Forward Example

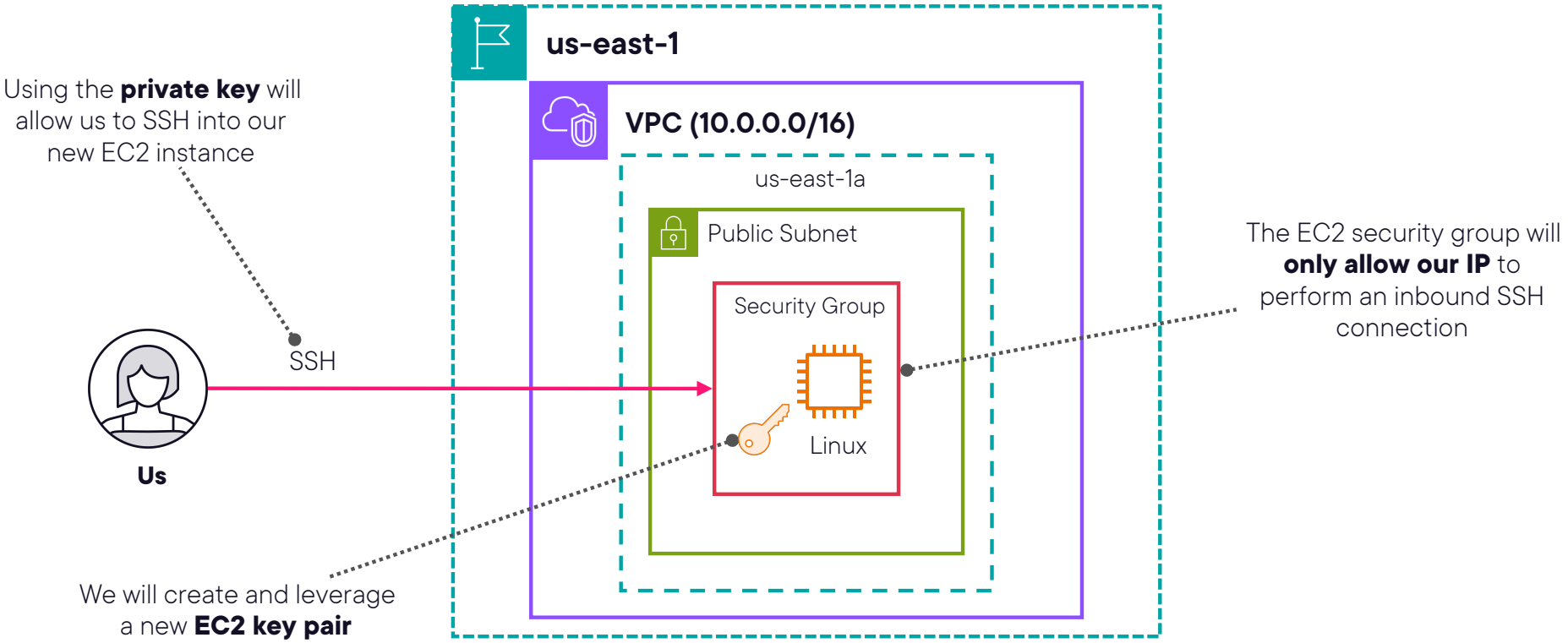


Typically, you will want to favor Systems Manager Session Manager over using bastion hosts in these scenarios.

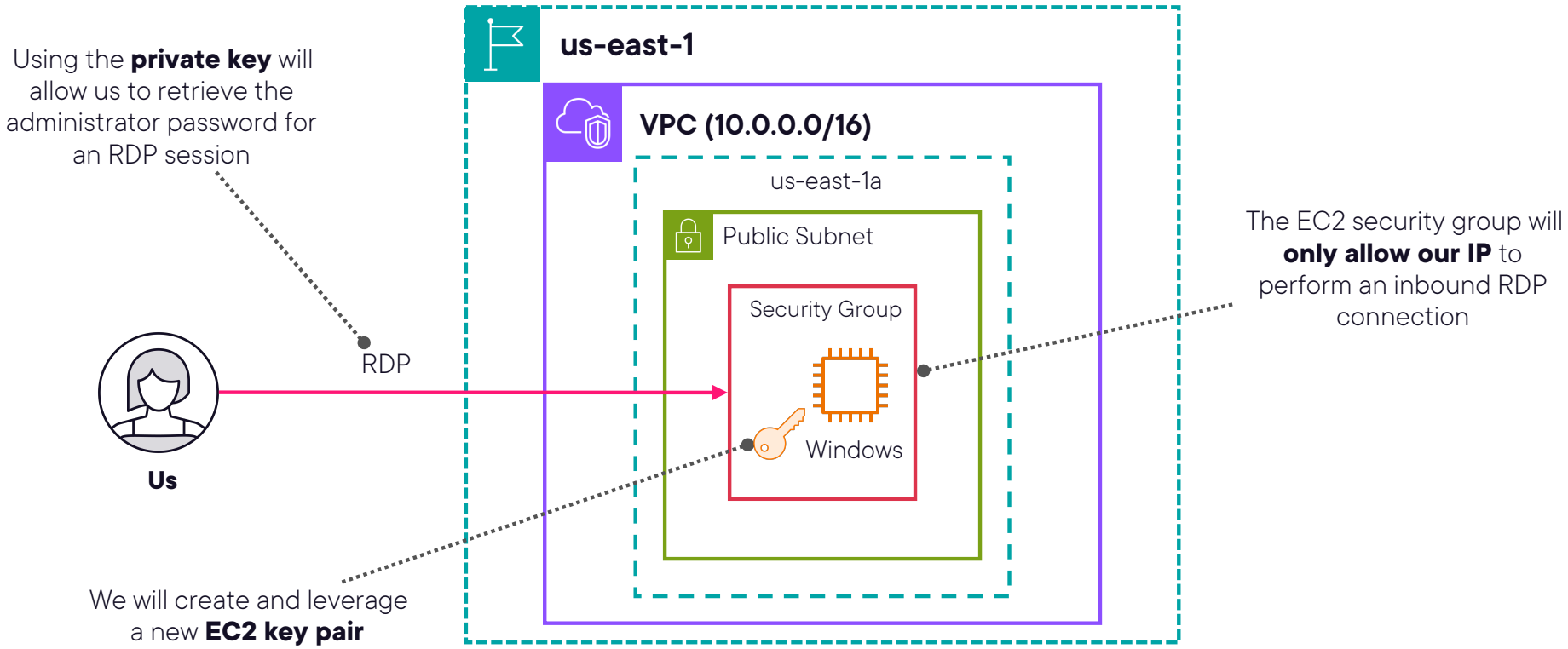
Demo: Deploying a Bastion Host



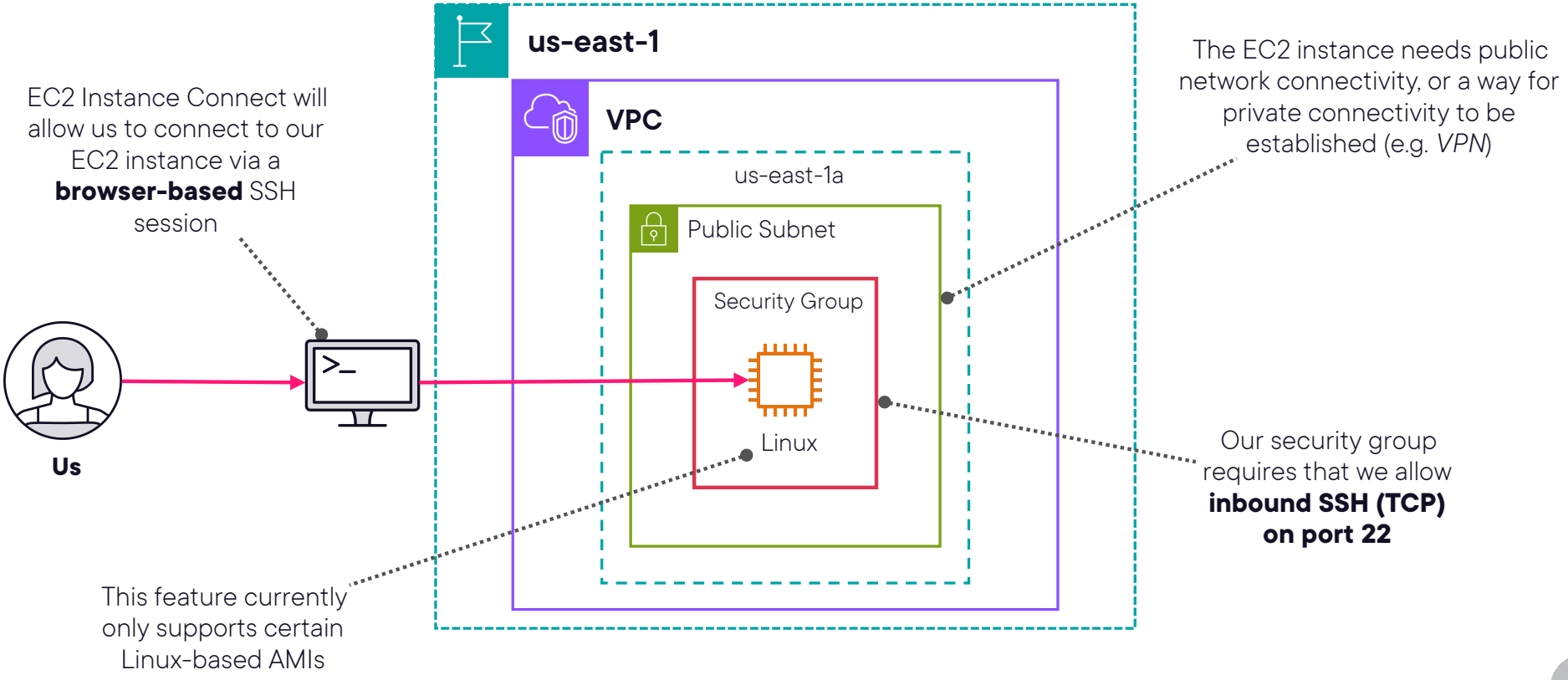
Demo: Connect to EC2 Using SSH



Demo: Connect to EC2 Using RDP



Demo: Using EC2 Instance Connect



Connecting to EC2 via Session Manager (SSM)

Session Manager

Capability offered within AWS Systems Manager that provides an agent-based connection to managed EC2 instances, edge devices, and managed on-premises VMs

Session Manager Concepts

Connections are done via the SSM Agent, so no more SSH or RDP requirements

Centralized access control via IAM policies to allow SSM to connect

Log and audit connections via CloudTrail, S3, and CloudWatch integrations

AWS Systems Manager Agent (SSM Agent)

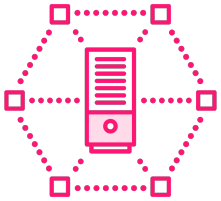
Amazon software that runs on Amazon Elastic Compute Cloud (Amazon EC2) instances, edge devices, on-premises servers, and virtual machines (VMs). SSM Agent makes it possible for Systems Manager to update, manage, and configure these resources

Citation: https://docs.aws.amazon.com/systems-manager/latest/userguide/ssm-agent.html

Three Major Requirements

Session Manager supports Windows, Linux, and MacOS systems.

IAM permissions are required for connections to be established. Remember this for EC2-related questions!



The SSM Agent must have network access to the Systems Manager service, either via Internet or VPC interface endpoints.

Session Manager VPC Interface Endpoints

ssm.region.amazonaws.com

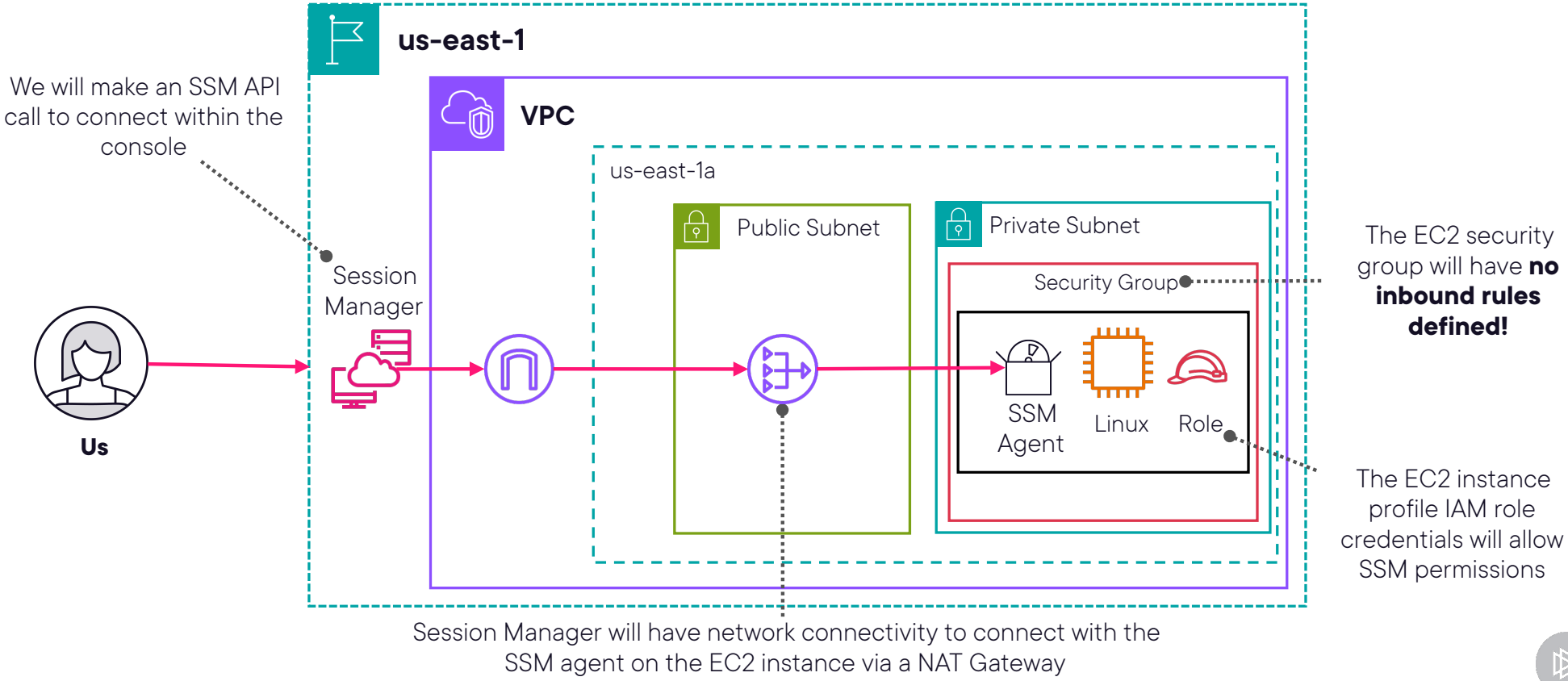
ssmmessages.region.amazonaws.com

ec2messages.region.amazonaws.com

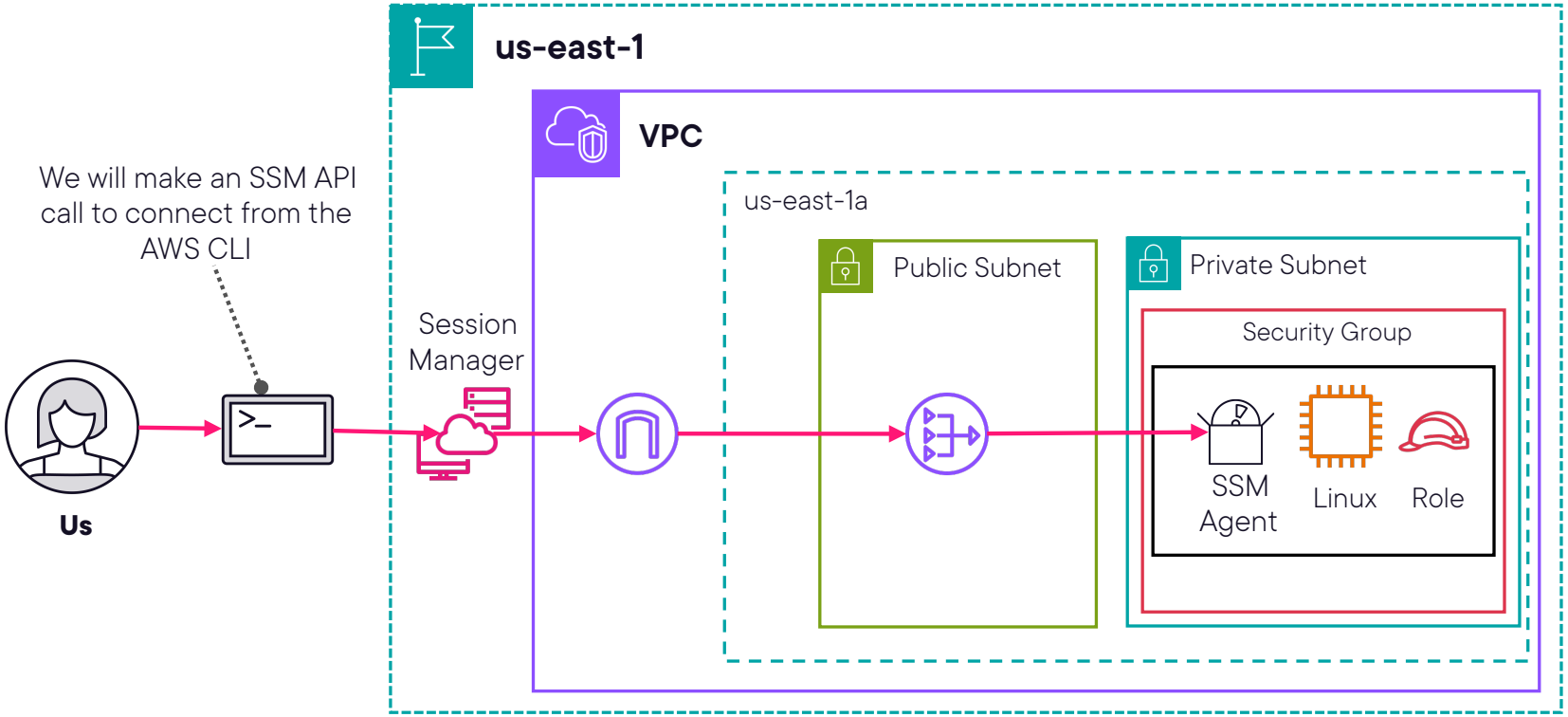
Image Source: https://unsplash.com/

Typically, Session Manager is the best choice for securely connecting to your EC2 instances!

Demo: Connect to EC2 via Session Manager in Console



Demo: Connect to EC2 via Session Manager via CLI



Everything else will remain the same as if we connected via the console

Using the Instance Metadata Service Version 2 (IMDSv2)

EC2 Metadata

EC2 metadata is simply data about your EC2 instance.

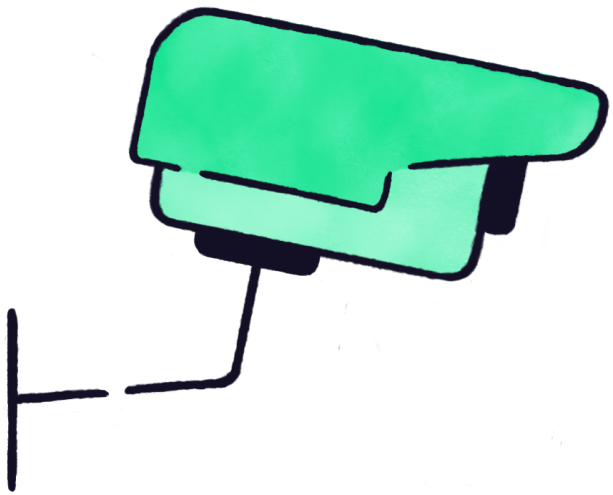
Instance Metadata Service Versions

IMDSv1
Original HTTP request/response method

IMDSv2
Newer, more secure session-oriented method requiring headers

IMDSv2 should be your preferred method!

It offers a much more secure means of obtaining instance information.



Instance metadata allows you to view the following types of information:

- User data
- Host name
- Security group information
- Instance IAM credentials

You can require that only IMDSv2 be used, which disables IMDSv1

IMDSv2 requires a session token to successfully retrieve the available data

Retrieving Metadata via IPv4

You will always use the same local URL/IP addresses to obtain IMDS information!

169.254.169.254

Remember this address!

Retrieving Metadata via IPv6

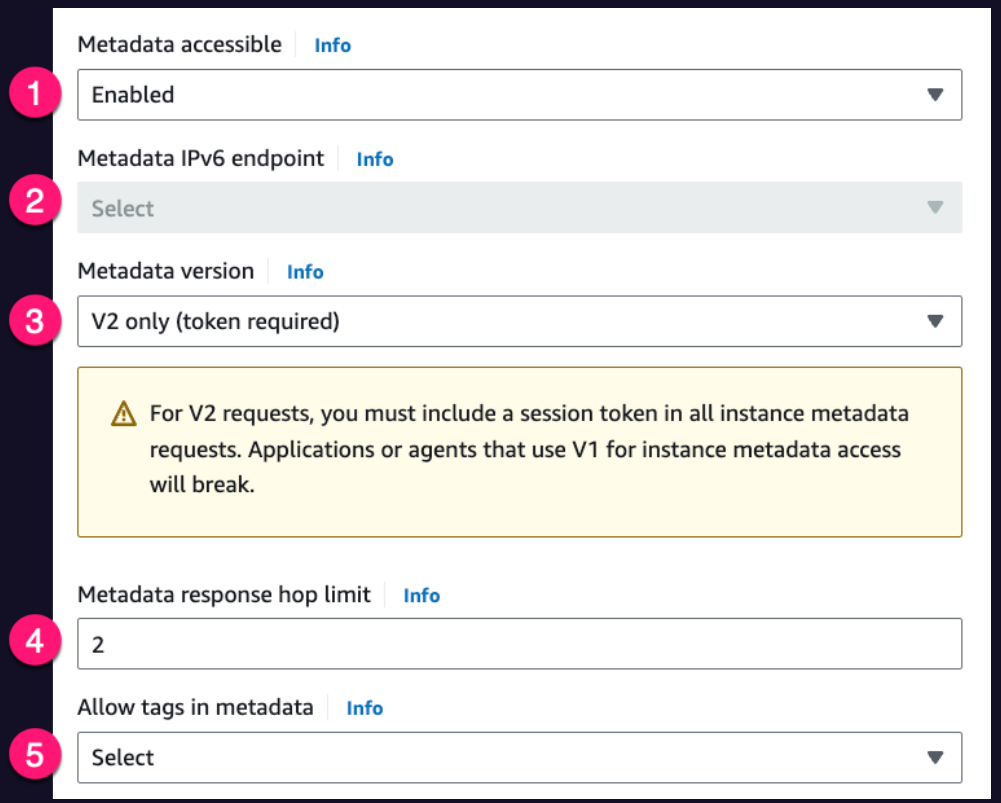
You will always use the same local URL/IP addresses to obtain IMDS information!

IPv6 requires a subnet with IPv6 enabled, and the EC2 instance must be an AWS Nitro System instance

[fd00:ec2::254]

IMDS Instance Settings

1. Specify if you even want the metadata service to be reachable
2. Enable the IPv6 endpoint (*if supported*)
3. Choose your IMDS version
4. How many hops the metadata response can travel
5. Do you want to allow the instance to get tag information through the IMDS?



Module Summary and Exam Tips

Connecting to EC2

Bastion hosts can be used to set up controlled access to private compute

Remember the options: SSH, RDP, EC2 Instance Connect, Session Manager

Session Manager will likely be the best choice for any scenario

Using Session Manager requires IAM permissions and network connectivity

Remember that the SSM agent is what you connect to for sessions

Session Manager Interface Endpoints

The following endpoints are critical for SSM to function:

- ssm.region.amazonaws.com
- ssmmessages.region.amazonaws.com
- ec2messages.region.amazonaws.com

Image Source: https://unsplash.com/

SSH and RDP both require key pairs in order to set up initial remote connections.

Information Available via IMDSv2

- User data script information
- Host name
- Security group information
- Instance IAM credentials

Remember this URL for IMDS scenarios:

http://169.254.169.254