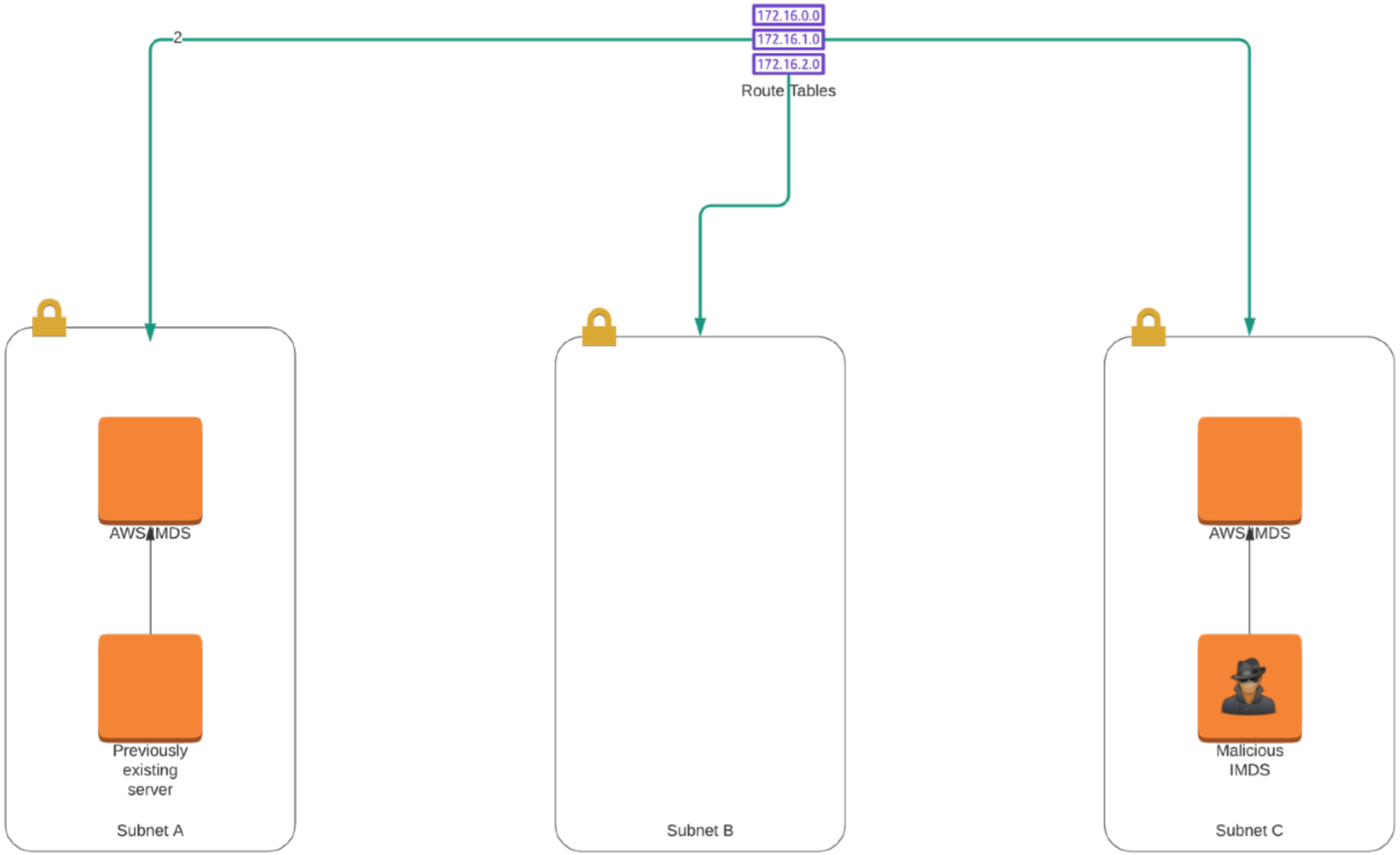
AWS IMDS Persistence/Priv escalation

Ryan Gerstenkorn | November 29, 2020

⟶ Default Routing

Use the tabs at the bottom to cycle between states.



Attacker Assumptions

- Controls an existing instance that has source IP checking disabled.
- Can modify routes
- Can trigger a lambda they control on RunInstance event's.

End Result

- New Instances in specific subnet's are automatically rooted on creation.

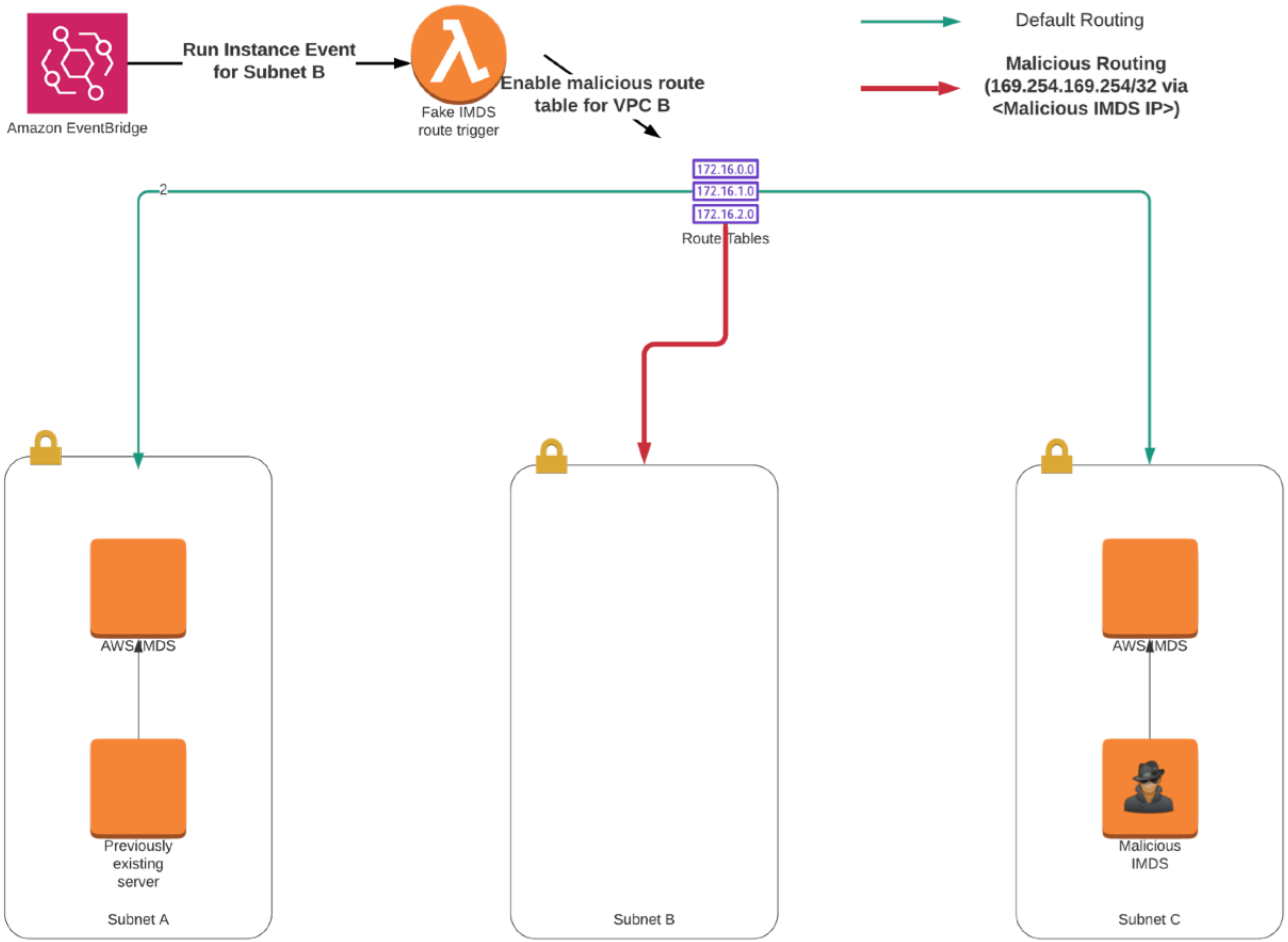
Notes

The key things that make this work.

- You can change what IMDS server a given instance connect's to by using a /32 route.
- Event Bridge is fast.
- Security groups are ignored for data to 169.254.169.254.
- No HTTPS w/ IMDS!

AWS IMDS Persistence/Priv escalation

Ryan Gerstenkorn | November 29, 2020



Run Instance Event for Subnet B

Enable malicious route table for VPC B

Default Routing

Malicious Routing (169.254.169.254/32 via <Malicious IMDS IP>)

Notes

1. RunInstance API is called.

2. Event Bridge trigger's a lambda tthe fake IMDS route trigger lambda.

3. 169.254.169.254/32 via <Malicious IMDS IP> is added to the route table in subnet B.

Event bridge/route updating is fast enough to complete before the new instance is started.