Architecture Diagrams

Inspection Deployment Models with AWS Network Firewall

Inspection Deployment Models with AWS Network Firewall: Architecture Diagrams

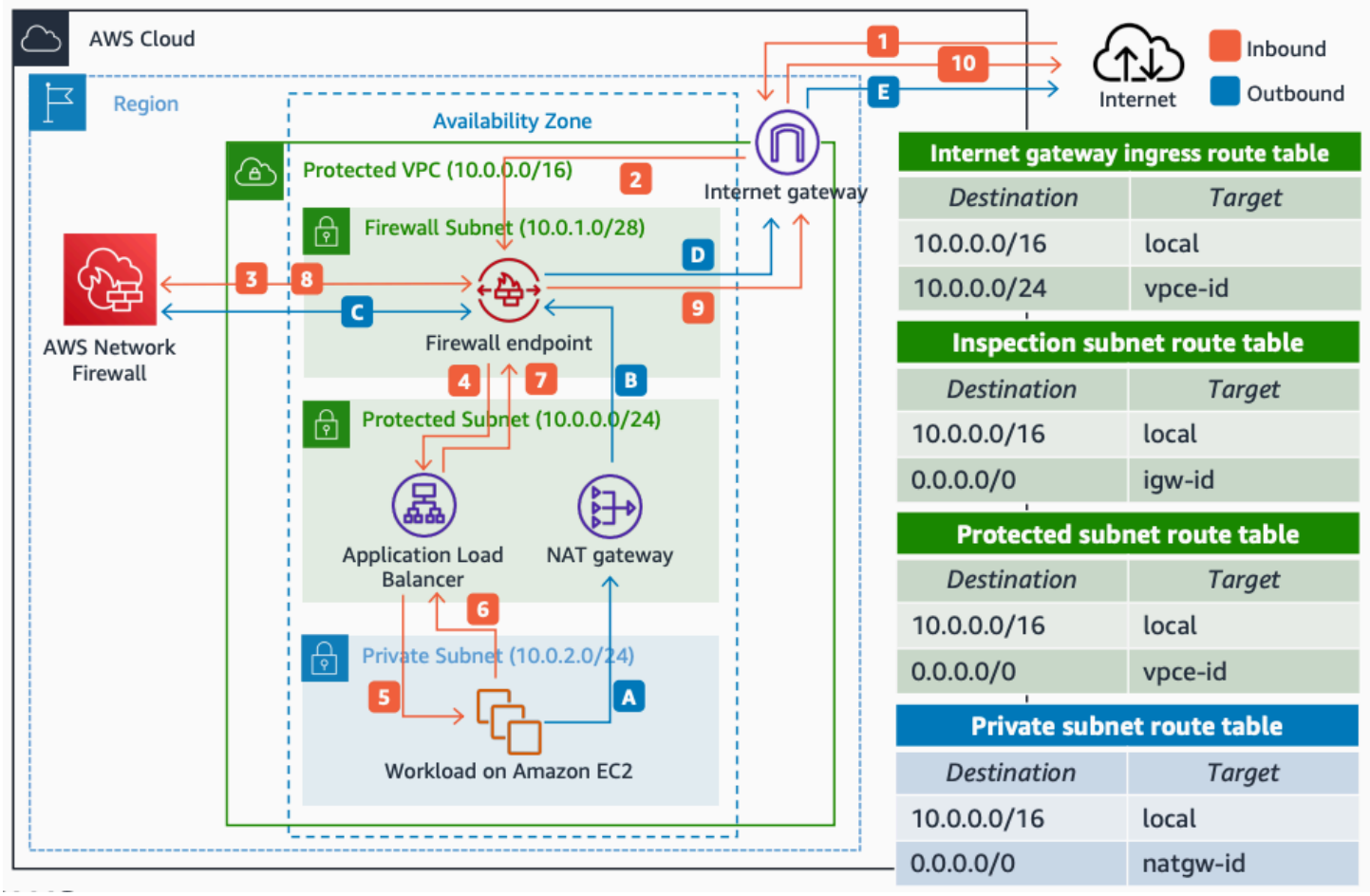
Table of Contents

Traffic Inspection with AWS Network Firewall

Publication date: **March 16, 2022 (Diagram history)**

This architecture shows how to inspect inbound and outbound traffic using AWS Network Firewall in a single Amazon VPC deployment. Traffic from the internet destined for an Application Load Balancer is transparently inspected by Network Firewall, while outbound traffic from instances is also inspected before reaching the internet through a NAT gateway.

Single Amazon VPC inspection with Network Firewall architecture



The following steps describe the inbound traffic flow in this architecture:

1. Traffic initiated from a client on the internet and destined to the public IP of the Application Load Balancer arrives at the internet gateway.

2. In accordance with the **internet gateway ingress table**, traffic is sent to the firewall endpoint.
3. Traffic is transparently inspected by AWS Network Firewall. Allowed traffic is sent back to the firewall endpoint.
4. According to the **inspection subnet route table**, traffic is sent to the Application Load Balancer.
5. As per the **protected subnet route table**, the Application Load Balancer forwards the traffic to the target group (workload on Amazon Elastic Compute Cloud).
6. Response traffic is returned back to the Application Load Balancer according to the **private subnet route table**.
7. In accordance with the **protected subnet route table**, traffic is sent to the firewall endpoint.
8. Traffic is sent to AWS Network Firewall. Traffic that complies with firewall rules is sent back to the firewall endpoint.
9. As per the **inspection subnet route table**, traffic is sent to the internet gateway.
10. Traffic is sent back to the internet.

The following steps describe the outbound traffic flow:

NaT. Traffic initiated from an instance and directed to the internet is forwarded to the NAT gateway, in accordance with the **private subnet route table**.

NaS. Source IP of traffic is changed to the IP of the NAT gateway, and the traffic is forwarded to the firewall endpoint as per the **protected subnet route table**.

NaT. Traffic is sent to AWS Network Firewall for inspection. Traffic that complies with firewall rules is sent back to the firewall endpoint.

NaA. According to the **inspection subnet route table**, traffic is forwarded to the internet gateway.

NaT. Traffic is sent out to the internet.

Further reading

For additional information, see the following resources:

- AWS Architecture Icons
- AWS Architecture Center
- AWS Well-Architected

Diagram history

To be notified about updates to this reference architecture diagram, subscribe to the RSS feed.

Change	Description	Date
Initial publication	Reference architecture diagram first published.	March 16, 2022
Initial publication	Reference architecture diagram first published.	March 16, 2022
Initial publication	Reference architecture diagram first published.	March 16, 2022
Initial publication	Reference architecture diagram first published.	March 16, 2022
Initial publication	Reference architecture diagram first published.	March 16, 2022
Initial publication	Reference architecture diagram first published.	March 16, 2022

Note

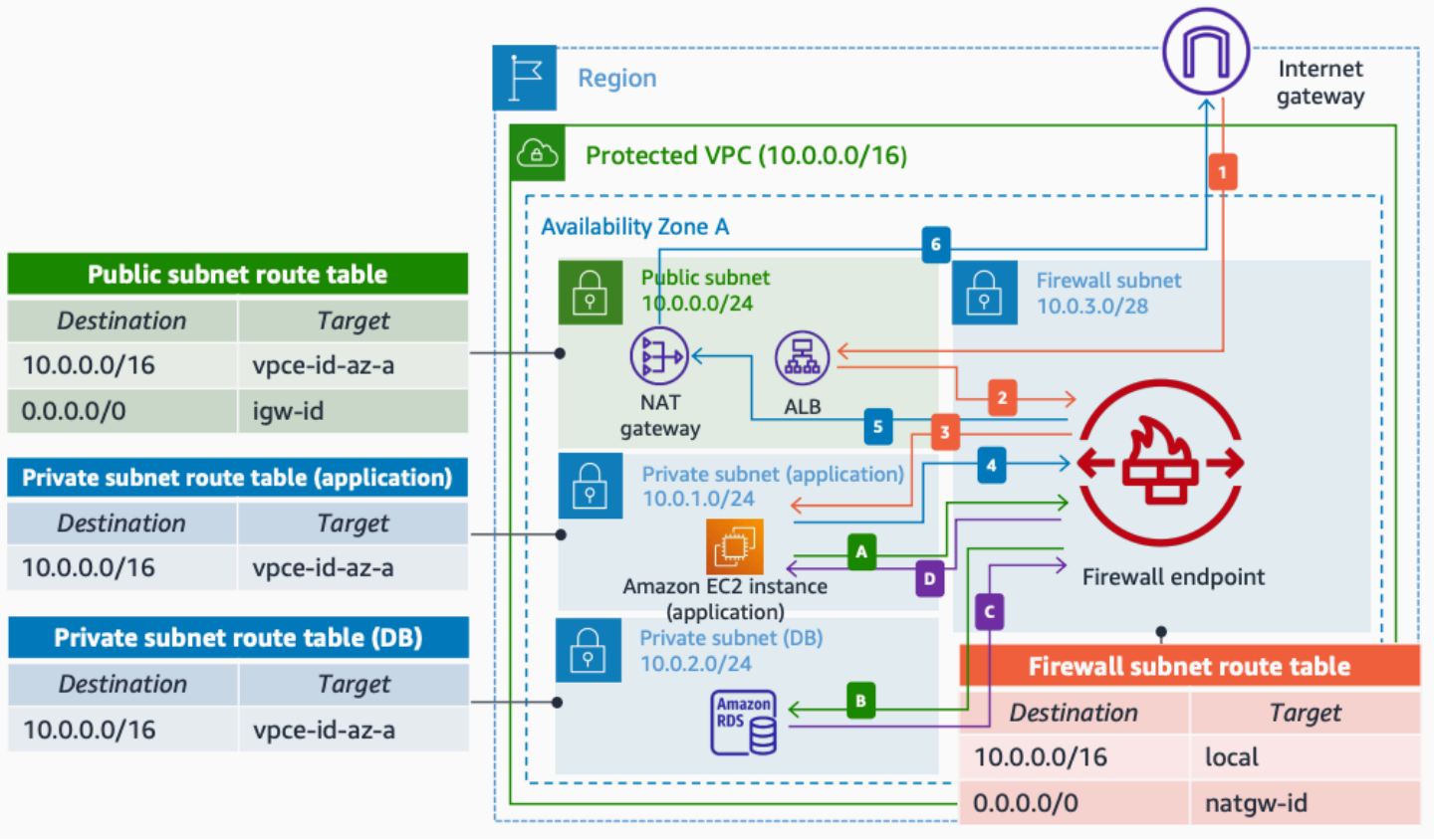
To subscribe to RSS updates, you must have an RSS plugin enabled for the browser you are using.

Intra-VPC Inspection with AWS Network Firewall

Publication date: **March 16, 2022 (Diagram history)**

This architecture shows how to use the Amazon VPC routing enhancement to inspect intra-VPC traffic (between subnets of the same Amazon VPC) using AWS Network Firewall. With Amazon VPC routing enhancement, any traffic between private subnets in the Amazon VPC can be first sent to the firewall endpoint to inspect the traffic.

Intra-VPC inspection with Network Firewall architecture



The following numbered items describe the key components in this architecture:

1. Ingress traffic is routed directly to a public workload: web servers or a load balancer.
2. Traffic between the public subnet and the application servers is inspected. It is recommended that you place the firewall endpoint in its own subnet ("**Firewall subnet**").
3. When the inspection is done, allowed traffic is routed to the application servers.

4. With Amazon VPC routing enhancement, any traffic between private subnets in the Amazon VPC can be first sent to the firewall endpoint to inspect the traffic.
5. You can add a more specific classless inter-domain routing (CIDR) block than the default block in the routing tables to select which intra-VPC traffic is inspected.
6. Outbound traffic to the internet from the application servers: the packets are first sent to the firewall endpoint, and the allowed traffic goes to the load balancer, web servers, or NAT gateway before being sent to the internet.

For more information about Multi-AZ options or connectivity options using AWS Transit Gateway, see Deployment models for AWS Network Firewall with VPC routing enhancements on the AWS Blog.

Further reading

For additional information, see the following resources:

- AWS Architecture Icons
- AWS Architecture Center
- AWS Well-Architected

Diagram history

To be notified about updates to this reference architecture diagram, subscribe to the RSS feed.

Change	Description	Date
Initial publication	Reference architecture diagram first published.	March 16, 2022
Initial publication	Reference architecture diagram first published.	March 16, 2022
Initial publication	Reference architecture diagram first published.	March 16, 2022

Initial publication	Reference architecture diagram first published.	March 16, 2022
Initial publication	Reference architecture diagram first published.	March 16, 2022
Initial publication	Reference architecture diagram first published.	March 16, 2022

Note

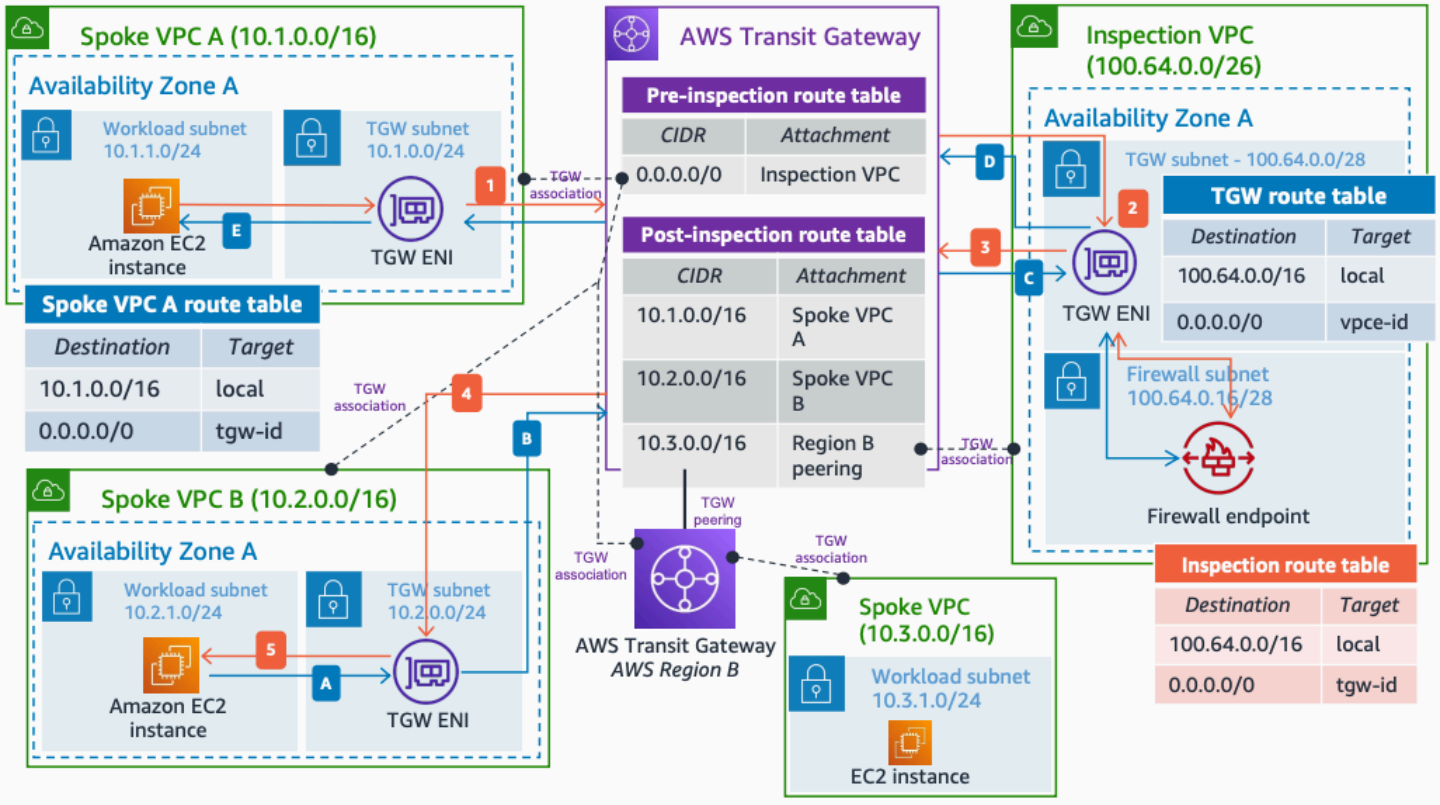
To subscribe to RSS updates, you must have an RSS plugin enabled for the browser you are using.

East-West Inspection with AWS Network Firewall and AWS Transit Gateway

Publication date: **March 16, 2022 (Diagram history)**

This architecture shows how to use AWS Transit Gateway to centralize the traffic inspection between several VPCs, both in the same Region or between Regions, using AWS Network Firewall.

East-west centralized inspection with Network Firewall architecture



The following steps describe the east-west traffic flow in this architecture:

1. Any traffic leaving a spoke VPC is routed to AWS Transit Gateway (TGW). The Transit Gateway route table associated with the VPCs and Transit Gateway peering forwards the traffic to the **Inspection VPC**.
2. The **Inspection VPC** route table forwards all the traffic to the firewall endpoint. The allowed traffic is forwarded back to the Transit Gateway.

3. The Transit Gateway route table associated with the **Inspection VPC** attachment has all the routes within the network.
4. In this particular example, the traffic is destined to **Spoke VPC B**.
5. In **Spoke VPC B**, the **TGW subnet** route table routes the traffic to the destination instance.

The following steps describe the return traffic flow:

Na. Traffic from an instance in **Spoke VPC B** to **Spoke VPC A** first reaches the Transit Gateway endpoint in the **TGW subnet**. The traffic is routed to the Transit Gateway.

Na. The Transit Gateway route table sends the traffic to the **Inspection VPC**, where it is routed to the firewall endpoint for inspection.

Na. Allowed traffic comes back to the Transit Gateway. The route table associated with the **Inspection VPC** forwards the traffic to **Spoke VPC A**.

> **Note**
>
> It is recommended to use Transit Gateway appliance mode in the **Inspection VPC** Transit Gateway attachment to maintain flow symmetry.

For more information about deployment models with AWS Network Firewall and AWS Transit Gateway, see Deployment Models for AWS Network Firewall on the AWS Blog.

Further reading

For additional information, see the following resources:

- AWS Architecture Icons
- AWS Architecture Center
- AWS Well-Architected

Diagram history

To be notified about updates to this reference architecture diagram, subscribe to the RSS feed.

Change	Description	Date
Initial publication	Reference architecture diagram first published.	March 16, 2022
Initial publication	Reference architecture diagram first published.	March 16, 2022
Initial publication	Reference architecture diagram first published.	March 16, 2022
Initial publication	Reference architecture diagram first published.	March 16, 2022
Initial publication	Reference architecture diagram first published.	March 16, 2022
Initial publication	Reference architecture diagram first published.	March 16, 2022

Note

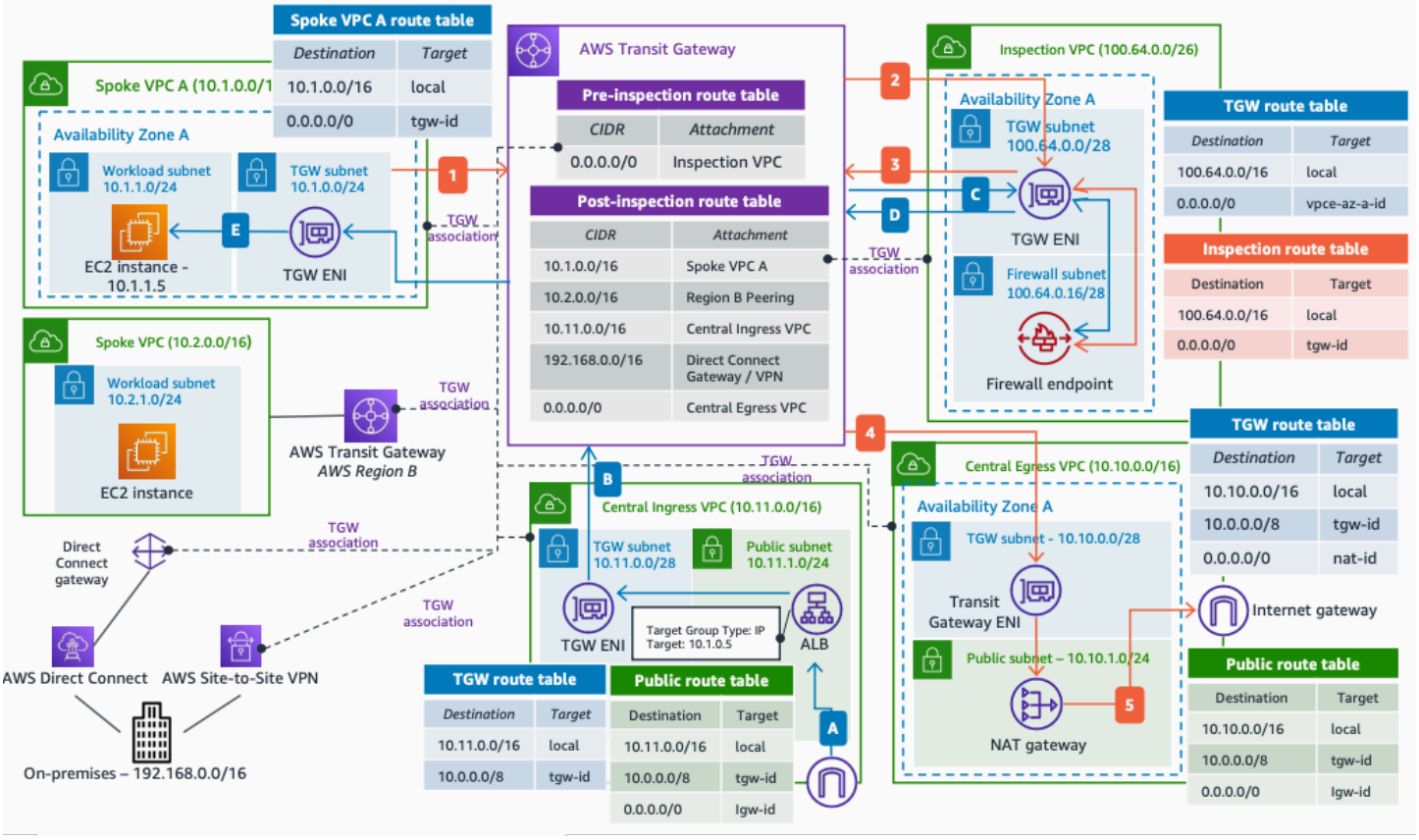
To subscribe to RSS updates, you must have an RSS plugin enabled for the browser you are using.

North-South Inspection with AWS Network Firewall and AWS Transit Gateway

Publication date: **March 16, 2022 (Diagram history)**

This architecture shows how to use AWS Transit Gateway to centralize the traffic inspection from and to the internet, or from and to on-premises facilities connected through AWS Direct Connect or AWS Site-to-Site VPN, using AWS Network Firewall.

North-south centralized inspection with Network Firewall architecture



The following steps describe the egress traffic flow in this architecture:

1. Traffic from the instance in **Spoke VPC A** destined to the internet is routed to the Transit Gateway. The Transit Gateway route table associated with the attachment sends all the traffic (**0.0.0.0/0**) to the **Inspection VPC**.

2. The **Inspection VPC TGW subnet** route table sends all the traffic to the firewall endpoint. The allowed traffic is forwarded back to the Transit Gateway.
3. The Transit Gateway route table associated with the **Inspection VPC** attachment has all the routes within the network.
4. In this particular use case, as the traffic needs to be routed to the internet, the Transit Gateway will forward the traffic to the **Central Egress VPC**.
5. The **TGW subnet** route table of the **Central Egress VPC** sends the traffic to the NAT gateway, so the private IP of the client can be translated to the private IP of the NAT gateway, and in turn, translated to the public IP by the internet gateway.

The following steps describe the ingress traffic flow:

Na. Traffic coming from the internet reaches the **Central Ingress VPC**. In this example, an Application Load Balancer sends the request to the target group of configured IP addresses through the Transit Gateway.

Na. The traffic is forwarded to the **Inspection VPC** in accordance with the **Pre-inspection route table** in Transit Gateway.

Na. As with the egress traffic, the **Inspection VPC TGW subnet** route table sends all the traffic to the firewall endpoint. Allowed traffic is forwarded back to the Transit Gateway and subsequently to the destination VPC (**Spoke VPC A**).

Na. The Transit Gateway route table associated with the **Inspection VPC** forwards the traffic to the **Spoke VPC A**.

Na. The **Spoke VPC A** route table sends the traffic to the desired instance.

> **Note**
>
> It is recommended to use Transit Gateway appliance mode in the **Inspection VPC** Transit Gateway attachment to maintain flow symmetry.

Further reading

For additional information, see the following resources:

- AWS Architecture Icons

- AWS Architecture Center
- AWS Well-Architected

Diagram history

To be notified about updates to this reference architecture diagram, subscribe to the RSS feed.

Change	Description	Date
Initial publication	Reference architecture diagram first published.	March 16, 2022
Initial publication	Reference architecture diagram first published.	March 16, 2022
Initial publication	Reference architecture diagram first published.	March 16, 2022
Initial publication	Reference architecture diagram first published.	March 16, 2022
Initial publication	Reference architecture diagram first published.	March 16, 2022
Initial publication	Reference architecture diagram first published.	March 16, 2022

Note

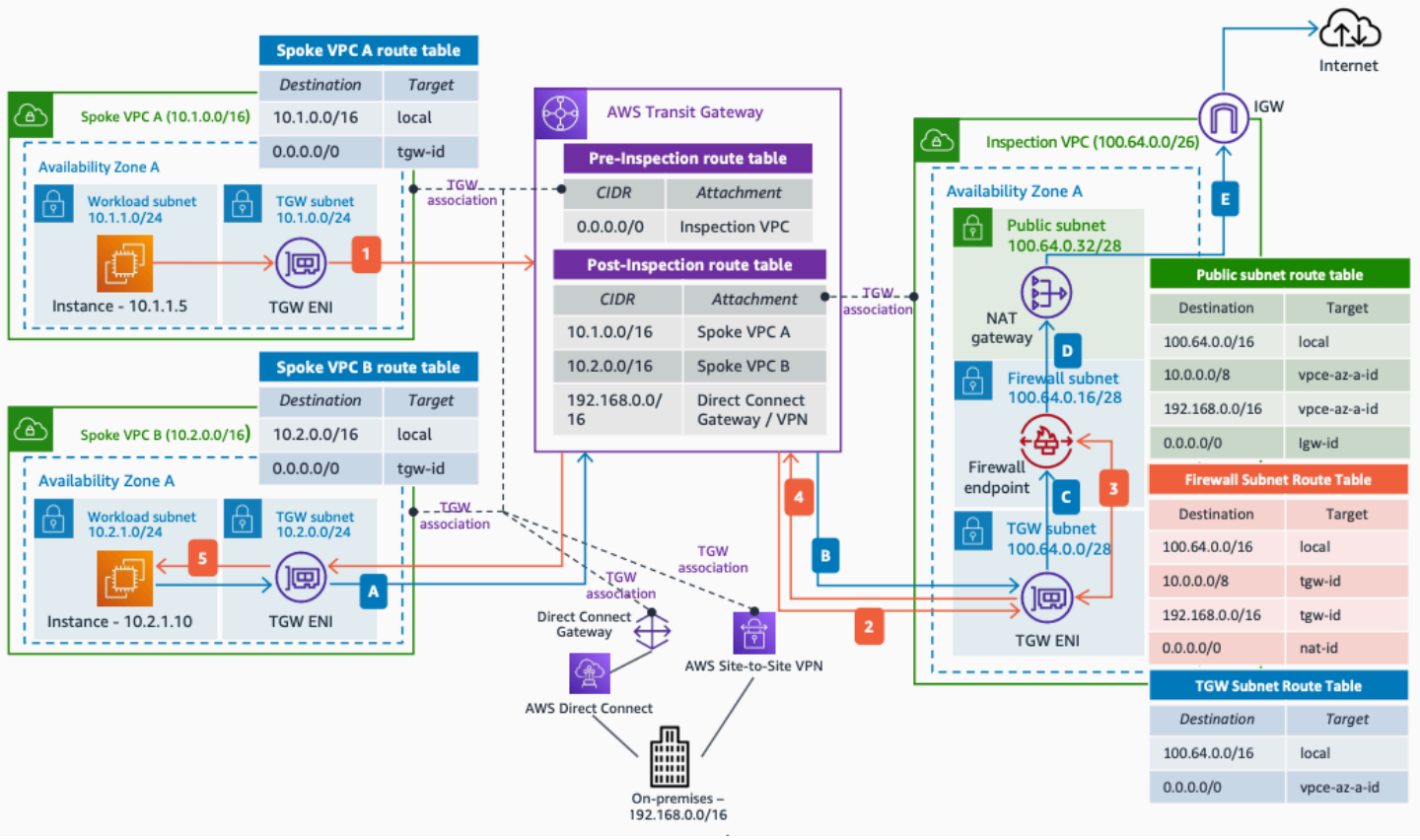
To subscribe to RSS updates, you must have an RSS plugin enabled for the browser you are using.

Combined Inspection with AWS Network Firewall and AWS Transit Gateway

Publication date: **March 16, 2022 (Diagram history)**

This architecture shows how to use AWS Transit Gateway to centralize the east-west inspection between VPCs, while having a NAT gateway in the Inspection Amazon VPC for centralized egress and north-south inspection using AWS Network Firewall.

Combined inspection with Network Firewall architecture



The following steps describe the east-west traffic flow in this architecture:

1. Traffic from an instance in **Spoke VPC A** destined to another instance in **Spoke VPC B** (east-west traffic) is routed to the Transit Gateway.
2. The Transit Gateway route table associated with the attachment sends all the traffic (**0.0.0.0/0**) to the **Inspection VPC**.

3. The **Inspection VPC TGW subnet** route table sends all the traffic to the firewall endpoint. The allowed traffic is forwarded back to the TGW ENI.
4. As per the Transit Gateway route table associated with the **Inspection VPC**, the traffic is sent to **Spoke VPC B**.
5. Finally, in the **TGW subnet** route table of **Spoke VPC B**, the traffic is sent to the destination.

The following steps describe the north-south traffic flow:

Na. Traffic from an instance in **Spoke VPC B** destined to the internet (north-south traffic) is routed to the Transit Gateway.

Na. The Transit Gateway route table associated with the attachment sends all the traffic (**0.0.0.0/0**) to the **Inspection VPC**, same as in the previous example.

Na. The **Inspection VPC TGW subnet** route table sends all the traffic to the firewall endpoint, where it is transparently analyzed.

Na. Allowed traffic is sent to the NAT gateway as per the **Firewall subnet** route table.

Na. The private IP of the client is translated to the private IP of the NAT gateway, and in turn, translated to the public IP by the internet gateway.

> **Note**
>
> It is recommended to use Transit Gateway appliance mode in the **Inspection VPC** Transit Gateway attachment to maintain flow symmetry.

For an example of this architecture in Terraform, see AWS Hub and Spoke Architecture with an Inspection VPC on GitHub.

Further reading

For additional information, see the following resources:

- AWS Architecture Icons
- AWS Architecture Center
- AWS Well-Architected

Diagram history

To be notified about updates to this reference architecture diagram, subscribe to the RSS feed.

Change	Description	Date
Initial publication	Reference architecture diagram first published.	March 16, 2022
Initial publication	Reference architecture diagram first published.	March 16, 2022
Initial publication	Reference architecture diagram first published.	March 16, 2022
Initial publication	Reference architecture diagram first published.	March 16, 2022
Initial publication	Reference architecture diagram first published.	March 16, 2022
Initial publication	Reference architecture diagram first published.	March 16, 2022

Note

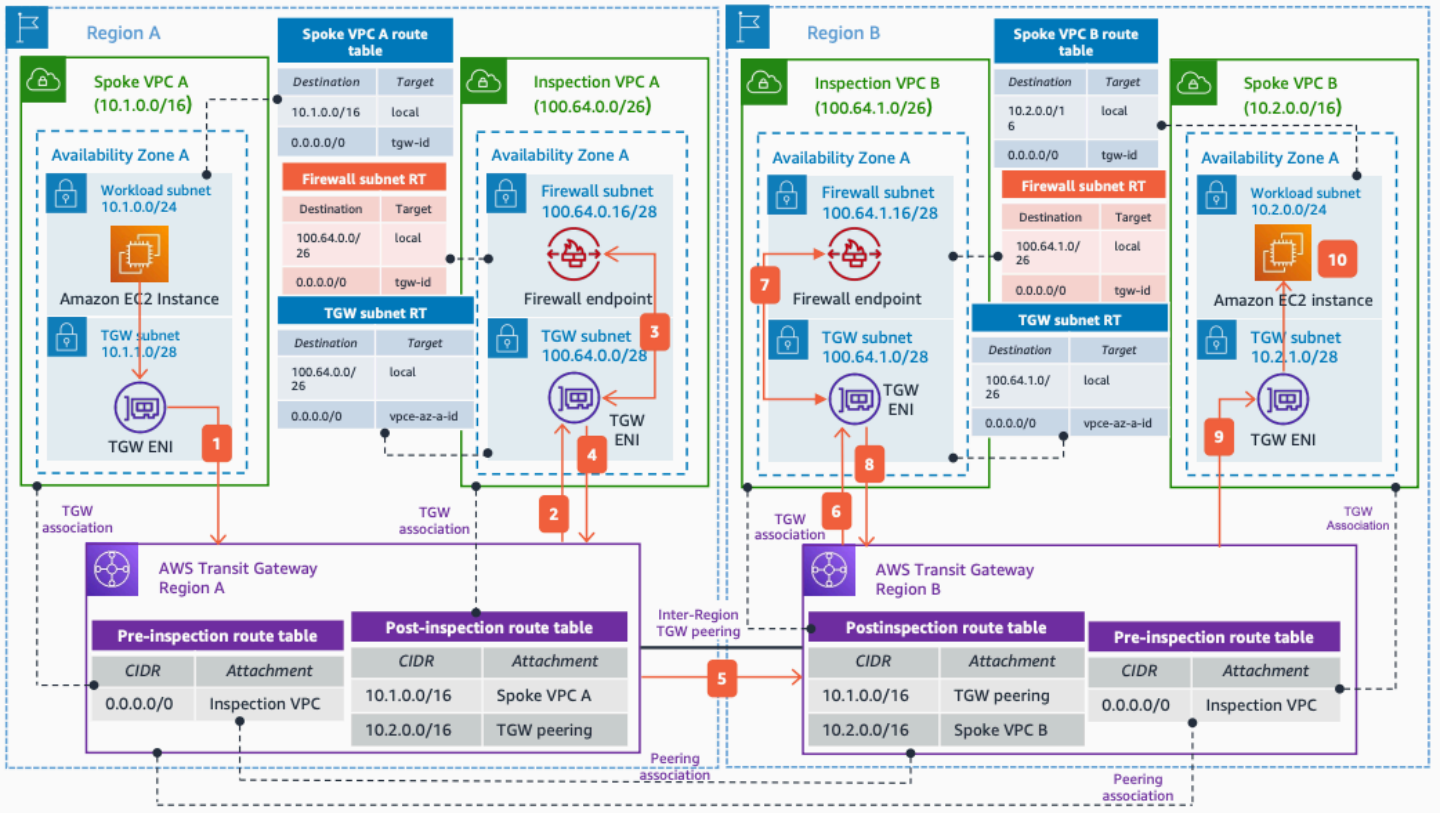
To subscribe to RSS updates, you must have an RSS plugin enabled for the browser you are using.

Multi-Region Inspection with AWS Network Firewall and AWS Transit Gateway

Publication date: **March 16, 2022 (Diagram history)**

This architecture shows how to inspect traffic in each AWS Region when using AWS Transit Gateway to centralize your inspection and inter-Region peering between two AWS Regions. Inspecting traffic in each Region is a best practice to avoid asymmetric traffic.

Multi-Region centralized inspection with Network Firewall architecture



The following numbered items describe the traffic flow in this architecture:

1. Traffic from an instance in **Spoke VPC A** destined to another instance in **Spoke VPC B** is routed to the Transit Gateway in Region A as per the **Spoke VPC A** route table.
2. The Transit Gateway (Region A) route table associated with the attachment (**Pre-inspection route table**) sends all the traffic (**0.0.0.0/0**) to the **Inspection VPC A**.

3. The **Inspection VPC A TGW subnet** route table sends all the traffic to the firewall endpoint for transparent inspection.
4. The allowed traffic is forwarded back to the TGW ENI.
5. As per the Transit Gateway (Region A) route table associated with the **Inspection VPC A** (**Post-inspection route table**), the traffic is sent to Region B through the Transit Gateway peering.
6. As per the Transit Gateway (Region B) route table associated with the Transit Gateway peering (**Pre-inspection route table**), the traffic is sent to the **Inspection VPC B** for inspection.
7. The **Inspection VPC B TGW subnet** route table sends all the traffic to the firewall endpoint for transparent inspection.
8. The allowed traffic is forwarded back to the TGW ENI.
9. As per the Transit Gateway (Region B) route table associated with the **Inspection VPC B** (**Post-inspection route table**), the traffic is sent to **Spoke VPC B**.
10. Traffic is forwarded to the destination, the Amazon Elastic Compute Cloud instance in **Spoke VPC B**.

> **Note**
>
> It is recommended to use Transit Gateway appliance mode in the **Inspection VPC** Transit Gateway attachments to maintain flow symmetry.

Further reading

For additional information, see the following resources:

- AWS Architecture Icons
- AWS Architecture Center
- AWS Well-Architected

Diagram history

To be notified about updates to this reference architecture diagram, subscribe to the RSS feed.

Change	Description	Date

Initial publication	Reference architecture diagram first published.	March 16, 2022
Initial publication	Reference architecture diagram first published.	March 16, 2022
Initial publication	Reference architecture diagram first published.	March 16, 2022
Initial publication	Reference architecture diagram first published.	March 16, 2022
Initial publication	Reference architecture diagram first published.	March 16, 2022
Initial publication	Reference architecture diagram first published.	March 16, 2022

Note

To subscribe to RSS updates, you must have an RSS plugin enabled for the browser you are using.