

CLOUD NETWORK SEGMENTATION IN PURSUIT OF ZERO TRUST

Atif Siddiqui

WE HAD A MASSIVE DATA BREACH. HACKERS GOT INTO THE PRIVATE DATA OF ALL OF OUR CUSTOMERS.



DILBERT.COM @SCOTTADAMSSAYS

NO PROBLEM. WE'LL ISSUE A PRESS RELEASE THAT SAYS WE'RE SORRY AND IT WILL NEVER HAPPEN AGAIN.



5-7-18 ©2018 Scott Adams, Inc./Dist. by Andrews McMeel

THAT'S WHAT WE SAID THE LAST THREE TIMES IT HAPPENED.



OUR STRATEGY IS TO WEAR THEM DOWN.





AGENDA

- Emergence of Zero Trust
- Network Segmentation Concepts and Transit Gateway
- Cloud Network Segmentation Design

ZERO TRUST HISTORY

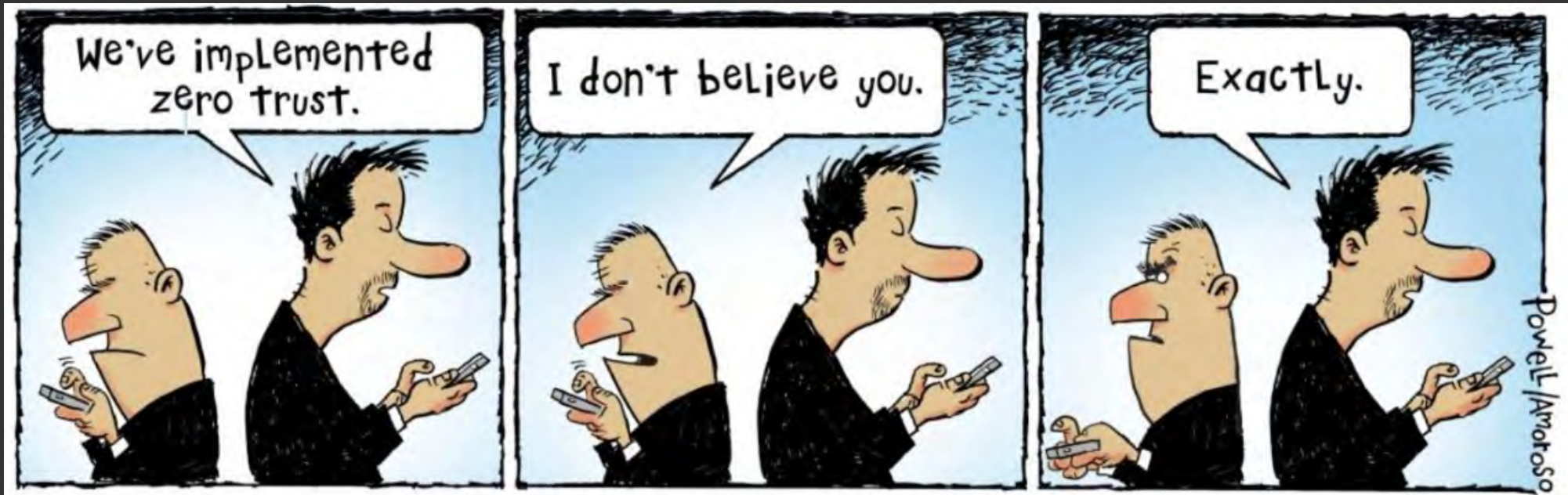
- Zero Trust term introduced in 1994
- Zero Trust Model coined in 2010 in Forrester Research paper
 - › Build Security Into Your Network's DNA: The Zero Trust Network Architecture
- NIST publication served as the endorsement

The screenshot shows the NIST website page for the publication "Zero Trust Architecture" (NIST SP 800-207). The page is titled "COMPUTER SECURITY RESOURCE CENTER" and includes a "PUBLICATIONS" section. The main heading is "Zero Trust Architecture" with a yellow icon. Below the heading are social media icons for Facebook and Twitter. The "Date Published" is August 2020, and the "Planning Note (12/11/2020)" is also present. A note mentions a Japanese translation developed by PwC Consulting LLC for the Information Technology Promotion Agency (IPA), Japan. A disclaimer states that the translation is not an official U.S. Government or NIST translation. The page also features a "DOCUMENTATION" section with links for "Publication" (https://doi.org/10.6028/NIST.SP.800-207), "Download URL", "Supplemental Material" (ZTA project at NCCoE), and "Japanese translation (unofficial--from)".

ZERO TRUST PRINCIPLES

'Never Trust, Always Verify' instead of 'Trust but Verify'

- } Verify explicitly
- } Use least privilege access
- } Minimize blast radius and segment access



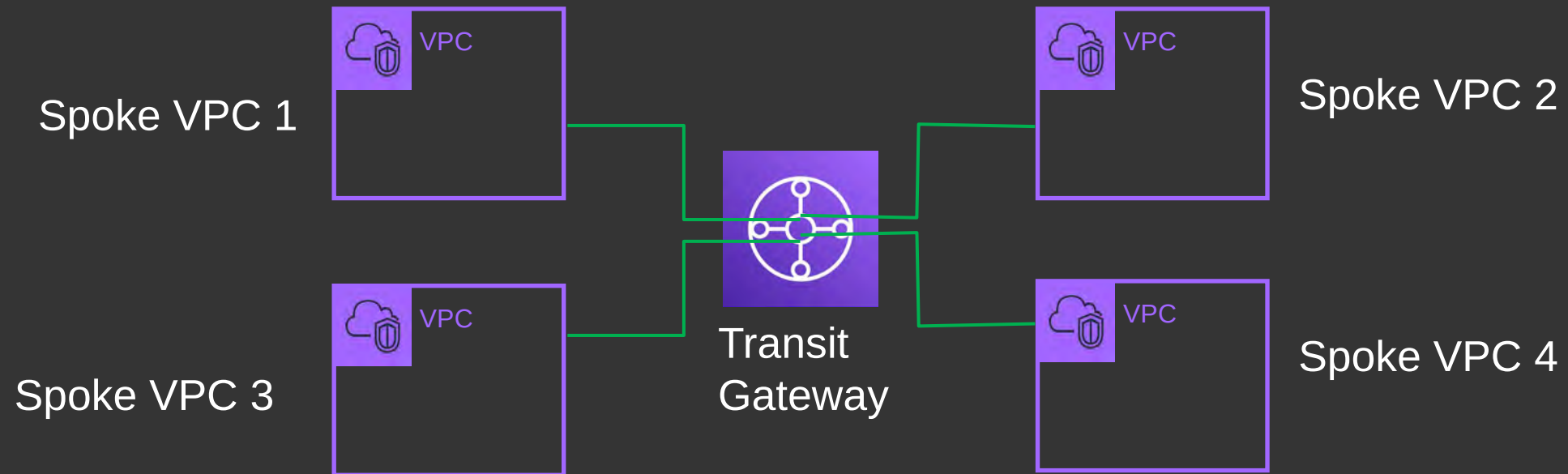
NETWORK SEGMENTATION

- Architectural approach to split network into multiple smaller segments
 - › Stronger network security by reducing attack plane
 - › Prevent lateral movement
 - › Reduce compliance scope

TRANSIT GATEWAY (TGW)

- Announced in November 2018
- Layer 3 Router provided as a managed service by AWS
- Tight integration with Hyperplane allows Transit Gateway to be highly scalable
- Hub and Spoke model

HUB AND SPOKE MODEL



KEY CONCEPTS OF TRANSIT GATEWAY

- Attachment
- Route Table
- Association
- Route propagation
- Route

TRANSIT GATEWAY ATTACHMENT

Create transit gateway attachment [Info](#)

A transit gateway (TGW) is a network transit hub that interconnects attachments (VPCs and VPNs) within the same AWS account or across AWS accounts.

Details

Name tag - optional
Creates a tag with the key set to Name and the value set to the specified string.

Transit gateway ID [Info](#)

Attachment type [Info](#)

VPC attachment

Select and configure your VPC attachment.

DNS support [Info](#)

IPv6 support [Info](#)

Appliance Mode support [Info](#)

VPC ID

Select the VPC to attach to the transit gateway.

Subnet IDs [Info](#)

Select the subnets in which to create the transit gateway VPC attachment.

us-east-1a

Create transit gateway attachment [Info](#)

A transit gateway (TGW) is a network transit hub that interconnects attachments (VPCs and VPNs) within the same AWS account or across AWS accounts.

Details

Name tag - optional

Creates a tag with the key set to Name and the value set to the specified string.

Transit gateway ID [Info](#)

Attachment type [Info](#)

- VPC
- VPN
- Peering Connection
- Connect

TRANSIT GATEWAY ROUTE TABLE

Transit gateway route tables (1/1) [Info](#) Refresh Actions Create transit gateway route table

Filter transit gateway route tables

<input checked="" type="checkbox"/>	Name	Transit gateway route table ID	Transit gateway ID	State	Default association route table	Default propagation route table
<input checked="" type="checkbox"/>	-	tgw-rtb-0a9496e282c77b8cc	tgw-01b6cae76a6b8fcc7	Available	Yes	Yes

tgw-rtb-0a9496e282c77b8cc

[Details](#) | [Associations](#) | [Propagations](#) | [Prefix list references](#) | [Routes](#) | [Tags](#)

Details

Transit gateway route table ID	State	Default association route table	Default propagation route table
tgw-rtb-0a9496e282c77b8cc	Available	Yes	Yes
Transit gateway ID			
tgw-01b6cae76a6b8fcc7			

TRANSIT GATEWAY ASSOCIATION

The screenshot displays the AWS Management Console interface for Transit Gateway route tables. The top section, titled "Transit gateway route tables (1/1)", shows a table with one entry. Below this, the "Associations" tab for the selected route table is active, showing a table with one association entry.

Transit gateway route tables (1/1)

Name	Transit gateway route table ID	Transit gateway ID	State	Default association route table	Default propagation
-	tgw-rtb-0a9496e282c77b8cc	tgw-01b6cae76a6b8fc7	Available	Yes	Yes

tgw-rtb-0a9496e282c77b8cc

Details | **Associations** | Propagations | Prefix list references | Routes | Tags

Associations (1/1)

Attachment ID	Resource type	Resource ID	State
tgw-attach-0c5db8c1787db4b0e	VPC	vpc-05970a35ced9c607a	Associated

TRANSIT GATEWAY PROPAGATION

The screenshot displays the AWS Management Console interface for Transit Gateway route tables. The top section, titled "Transit gateway route tables (1/1)", shows a table with one entry. The entry has a checkmark in the selection column, a hyphen in the Name column, the ID "tgw-rtb-0a9496e282c77b8cc" in the Transit gateway route table ID column, the ID "tgw-01b6cae76a6b8fcc7" in the Transit gateway ID column, a green checkmark and "Available" in the State column, "Yes" in the Default association route table column, and "Yes" in the Default propagation column. A mouse cursor is pointing at the "Yes" in the Default propagation column.

Below this table, the console shows the details for the selected route table "tgw-rtb-0a9496e282c77b8cc". The "Propagations" tab is active, showing a table with one entry. The entry has a checkmark in the selection column, the ID "tgw-attach-0c5db8c1787db4b0e" in the Attachment ID column, "VPC" in the Resource type column, the ID "vpc-05970a35ced9c607a" in the Resource ID column, and a green checkmark and "Enabled" in the State column.

Name	Transit gateway route table ID	Transit gateway ID	State	Default association route table	Default propagation
-	tgw-rtb-0a9496e282c77b8cc	tgw-01b6cae76a6b8fcc7	Available	Yes	Yes

Attachment ID	Resource type	Resource ID	State
tgw-attach-0c5db8c1787db4b0e	VPC	vpc-05970a35ced9c607a	Enabled

TRANSIT GATEWAY ROUTE

The screenshot displays the AWS Transit Gateway console interface. At the top, the page title is "Transit gateway route tables (1/1) Info". A search bar is present with the placeholder text "Filter transit gateway route tables". A table lists the available transit gateway route tables. A mouse cursor is pointing at the "Transit gateway route table ID" column header.

<input checked="" type="checkbox"/>	Name	Transit gateway route table ID	Transit gateway ID	State	Default association route table	Default propagation
<input checked="" type="checkbox"/>	-	tgw-rtb-0a9496e282c77b8cc	tgw-01b6cae76a6b8fcc7	Available	Yes	Yes

Below the table, the selected route table "tgw-rtb-0a9496e282c77b8cc" is detailed. The "Routes" tab is active, showing a filter for "Filter routes by CIDR (2)".

Routes (1/1)

<input checked="" type="checkbox"/>	CIDR	Attachment ID	Resource ID	Resource type	Route type	Route state
<input checked="" type="checkbox"/>	172.31.0.0/16	tgw-attach-0c5db8c1787db4b0e	vpc-05970a35ced9c607a	VPC	Propagated	Active

NETWORK DESIGN

- Considerations
 - } AWS Accounts' landscape
 - } Environments: Dev, QA, UAT and Prod
 - } Traffic patterns
 - } Inspection model

DESIGN CONSIDERATION - ISOLATION OF ACCOUNTS

- With an application having four environments (dev, qa, uat and prod), each environment is in its own AWS account
- VPCs (virtual private cloud) are connected via AWS Transit Gateway

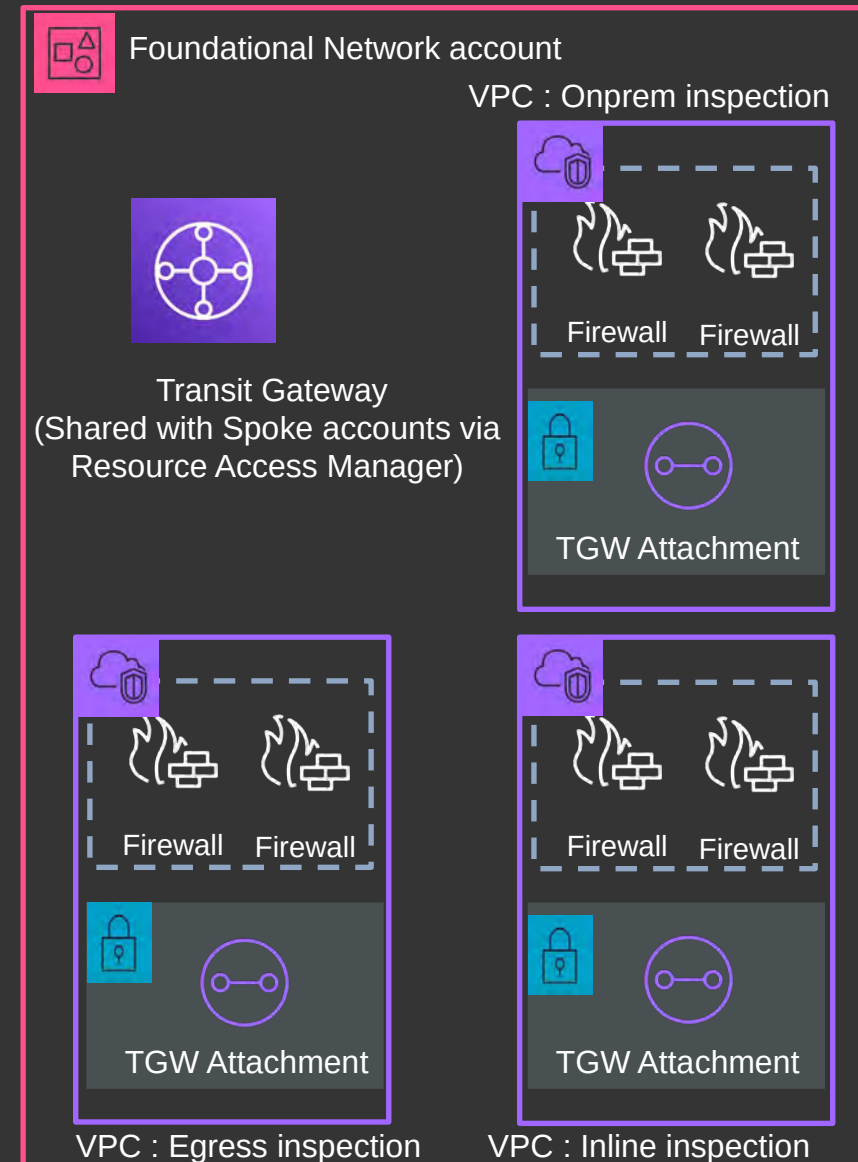
DESIGN CONSIDERATION – TGW ROUTE TABLES

- Routing is driven by Transit Gateway
- Two key Transit Gateway Route tables
 - } Route table 1 named *Spoke*
 - } Route table 2 named *Inspection*

DESIGN CONSIDERATION - TRAFFIC INSPECTION PATTERNS

- Onprem
- Inline
- Egress

NOTE: Any traffic crossing VPC boundary must be inspected regardless of the destination



VPC DETAILS

Your VPCs (5) [info](#)

Find resources by attribute or tag

<input type="checkbox"/>	Name	VPC ID	State	IPv4 CIDR
<input type="checkbox"/>	app1-vpc	vpc-0d03a5ba727361bd1	Available	10.120.8.0/23
<input checked="" type="checkbox"/>	app2-vpc	vpc-09704f7cd3232a672	Available	10.120.8.0/23

Spoke VPCs

Your VPCs (5) [info](#)

Find resources by attribute or tag

<input type="checkbox"/>	Name	VPC ID	State	IPv4 CIDR
<input checked="" type="checkbox"/>	Nezafat			
<input type="checkbox"/>	egress-vpc	vpc-00e7db45a5268f5d3	Available	10.120.1.0/24
<input type="checkbox"/>	onprem-vpc	vpc-0b65e26d68c198a21	Available	10.120.2.0/24
<input type="checkbox"/>	inline-vpc	vpc-0a01f7bb5cae15142	Available	10.120.3.0/24

Inspection VPCs

TRANSIT GATEWAY ROUTE TABLES

Transit gateway route tables (2) [Info](#)

Filter transit gateway route tables

<input type="checkbox"/>	Name	Transit gateway route table ID	Transit gateway ID	State
<input type="checkbox"/>	spoke	tgw-rtb-0265ab9bf532a1730	tgw-07cb214dc885ea4ee	Available
<input type="checkbox"/>	inspection	tgw-rtb-0a508e9041aa7f04d	tgw-07cb214dc885ea4ee	Available

TGW ASSOCIATIONS (SPOKE)

Transit gateway route tables (1/2) [Info](#)

Filter transit gateway route tables

<input type="checkbox"/>	Name	Transit gateway route table ID	Transit gateway ID	State
<input checked="" type="checkbox"/>	spoke	tgw-rtb-0265ab9bf532a1730	tgw-07cb214dc885ea4ee	Available
<input type="checkbox"/>	inspection	tgw-rtb-0a508e9041aa7f04d	tgw-07cb214dc885ea4ee	Available

tgw-rtb-0265ab9bf532a1730 / spoke

Details | **Associations** | Propagations | Prefix list references | Routes | Tags

Associations (2) [Info](#)

Filter associations

<input type="checkbox"/>	Attachment ID	Resource type	Resource ID	State
<input type="checkbox"/>	tgw-attach-0da42e0ca9fba6b3f	VPC	vpc-09704f7cd3232a672	Associated
<input type="checkbox"/>	tgw-attach-01e9cdc28f12a2d18	VPC	vpc-0d03a5ba727361bd1	Associated

TGW ROUTES (SPOKE)

Transit gateway route tables (1/2) [Info](#) ↻ Actions ▾ Create transit gateway route table

<input type="checkbox"/>	Name ▾	Transit gateway route table ID ▾	Transit gateway ID ▾	State ▾	Default association route table ▾	Default propag
<input checked="" type="checkbox"/>	spoke	tgw-rtb-0265ab9bf532a1730	tgw-07cb214dc885ea4ee	🟢 Available	No	No
<input type="checkbox"/>	inspection	tgw-rtb-0a508e9041aa7f04d	tgw-07cb214dc885ea4ee	🟢 Available	No	No

tgw-rtb-0265ab9bf532a1730 / spoke

[Details](#) | [Associations](#) | [Propagations](#) | [Prefix list references](#) | [Routes](#) | [Tags](#)

▶ Filter routes by CIDR (2)

Routes (3) ↻ Actions ▾ Create static route

<input type="checkbox"/>	CIDR ▲	Attachment ID ▾	Resource ID ▾	Resource type ▾	Route type ▾	Route state
<input type="checkbox"/>	0.0.0.0/0	tgw-attach-09f1a17b4f06ea4a4	vpc-00e7db45a5268f5d3	VPC	Static	🟢 Active
<input type="checkbox"/>	10.0.0.0/8	tgw-attach-0115d7cb5d167736a	vpc-0b65e26d68c198a21	VPC	Static	🟢 Active
<input type="checkbox"/>	10.120.0.0/16	tgw-attach-0662317fd994a0757	vpc-0a01f7bb5cae15142	VPC	Static	🟢 Active

TGW ASSOCIATIONS (INSPECTION)

Transit gateway route tables (1/2) [Info](#)

Filter transit gateway route tables

<input type="checkbox"/>	Name	Transit gateway route table ID	Transit gateway ID	State
<input type="checkbox"/>	spoke	tgw-rtb-0265ab9bf532a1730	tgw-07cb214dc885ea4ee	Available
<input checked="" type="checkbox"/>	inspection	tgw-rtb-0a508e9041aa7f04d	tgw-07cb214dc885ea4ee	Available

tgw-rtb-0a508e9041aa7f04d / inspection

Details | **Associations** | Propagations | Prefix list references | Routes | Tags

Associations (3) [Info](#)

Filter associations

<input type="checkbox"/>	Attachment ID	Resource type	Resource ID	State
<input type="checkbox"/>	tgw-attach-09f1a17b4f06ea4a4	VPC	vpc-00e7db45a5268f5d3	Associated
<input type="checkbox"/>	tgw-attach-0115d7cb5d167736a	VPC	vpc-0b65e26d68c198a21	Associated
<input type="checkbox"/>	tgw-attach-0662317fd994a0757	VPC	vpc-0a01f7bb5cae15142	Associated

TGW ROUTES (INSPECTION)

Transit gateway route tables (1/2) [info](#) Refresh Actions Create transit gateway route table

Filter transit gateway route tables

<input type="checkbox"/>	Name	Transit gateway route table ID	Transit gateway ID	State	Default association route table	Default propagation
<input type="checkbox"/>	spoke	tgw-rtb-0265ab9bf532a1730	tgw-07cb214dc885ea4ee	Available	No	No
<input checked="" type="checkbox"/>	inspection	tgw-rtb-0a508e9041aa7f04d	tgw-07cb214dc885ea4ee	Available	No	No

tgw-rtb-0a508e9041aa7f04d / inspection Refresh Actions Settings

Details | Associations | Propagations | Prefix list references | **Routes** | Tags

Filter routes by CIDR (2)

Routes (5) Refresh Actions Create static route

Filter routes

<input type="checkbox"/>	CIDR	Attachment ID	Resource ID	Resource type	Route type	Route state
<input type="checkbox"/>	0.0.0.0/0	tgw-attach-09f1a17b4f06ea4a4	vpc-00e7db45a5268f5d3	VPC	Static	Active
<input type="checkbox"/>	10.0.0.0/8	tgw-attach-0115d7cb5d167736a	vpc-0b65e26d68c198a21	VPC	Static	Active
<input type="checkbox"/>	10.120.0.0/16	tgw-attach-0662317fd994a0757	vpc-0a01f7bb5cae15142	VPC	Static	Active
<input type="checkbox"/>	10.120.4.0/23	tgw-attach-01e9cdc28f12a2d18	vpc-0d03a5ba727361bd1	VPC	Static	Active
<input type="checkbox"/>	10.120.8.0/23	tgw-attach-0da42e0ca9fba6b3f	vpc-09704f7cd3232a672	VPC	Static	Active

APPLICATION VPC ROUTES

VPC > Route tables > rtb-01f47e379639fe1c2

rtb-01f47e379639fe1c2 / app1-rtb-private1-us-east-1a Actions ▾

Details Info

Route table ID 📄 rtb-01f47e379639fe1c2	Main 📄 No	Explicit subnet associations subnet-09578cfd7ba64032f / app1-subnet-private1-us-east-1a	Edge associations -
VPC vpc-0d03a5ba727361bd1 app1-vpc	Owner ID 📄 255405915932		

Routes | Subnet associations | Edge associations | Route propagation | Tags

Routes (2) Edit routes

🔍 *Filter routes* Both ▾ < 1 > ⚙️

Destination ▾	Target ▾	Status ▾	Propagated ▾
0.0.0.0/0	tgw-07cb214dc885ea4ee	🟢 Active	No
10.120.4.0/23	local	🟢 Active	No

TAKING DESIGN FURTHER

- Isolating traffic at the routing level
 - › Dev traffic can only get routed to other Dev environments
 - › QA traffic can only get routed to other QA environments
 - › UAT traffic can only get routed to other UAT environments
 - › Prod traffic can only get routed to other Prod environments

ISOLATION AT ENVIRONMENT TYPE

Transit gateway route tables (1/1) [Info](#)

Filter transit gateway route tables

search: spoke X Clear filters

Dev-spoke, QA-spoke, UAT-spoke, Prod-spoke

Name	Transit gateway route table ID	Transit gateway ID	State	Default association route table	Default propagation
spoke	tgw-rtb-0265ab9bf532a1730	tgw-07cb214dc885ea4ee	Available	No	No

tgw-rtb-0265ab9bf532a1730 / spoke

Details Associations Propagations Prefix list references **Routes** Tags

Filter routes by CIDR (2)

Routes (3)

Filter routes

Introduce blackhole route

CIDR	Attachment ID	Resource ID	Resource type	Route type	Route state
0.0.0.0/0	tgw-attach-09f1a17b4f06ea4a4	vpc-00e7db45a5268f5d3	VPC	Static	Active
10.0.0.0/8	tgw-attach-0115d7cb5d167736a	vpc-0b65e26d68c198a21	VPC	Static	Active
10.120.0.0/16	tgw-attach-0662317fd994a0757	vpc-0a01f7bb5cae15142	VPC	Static	Active

VPC > Transit gateway route tables > tgw-rtb-0265ab9bf532a1730 > Create static route

Create static route [Info](#)

Add a static route to your transit gateway route table.

Details

Transit gateway ID
tgw-07cb214dc885ea4ee

Transit gateway route table ID
tgw-rtb-0265ab9bf532a1730

CIDR [Info](#)
10.x.y.z/w

Type [Info](#)
 Active
 Blackhole

Cancel Create static route

THANK YOU

References

- <https://www.ibm.com/reports/data-breach>
- https://www.ndm.net/firewall/pdf/palo_alto/Forrester-Build-Security-Into-Your-Network.pdf
- <https://aws.amazon.com/transit-gateway/>
- <https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/>