Check Point
SOFTWARE TECHNOLOGIES LTD

TRANSIT GATEWAY

Southbound HUB

Autoscaling versus Geo-Cluster

Eugene Tcheby | Cloud Security Architect

WELCOME TO THE FUTURE OF
CYBER SECURITY

POWERED BY CHECK POINT INFINITY

CLOUD • MOBILE • THREAT PREVENTION

Agenda

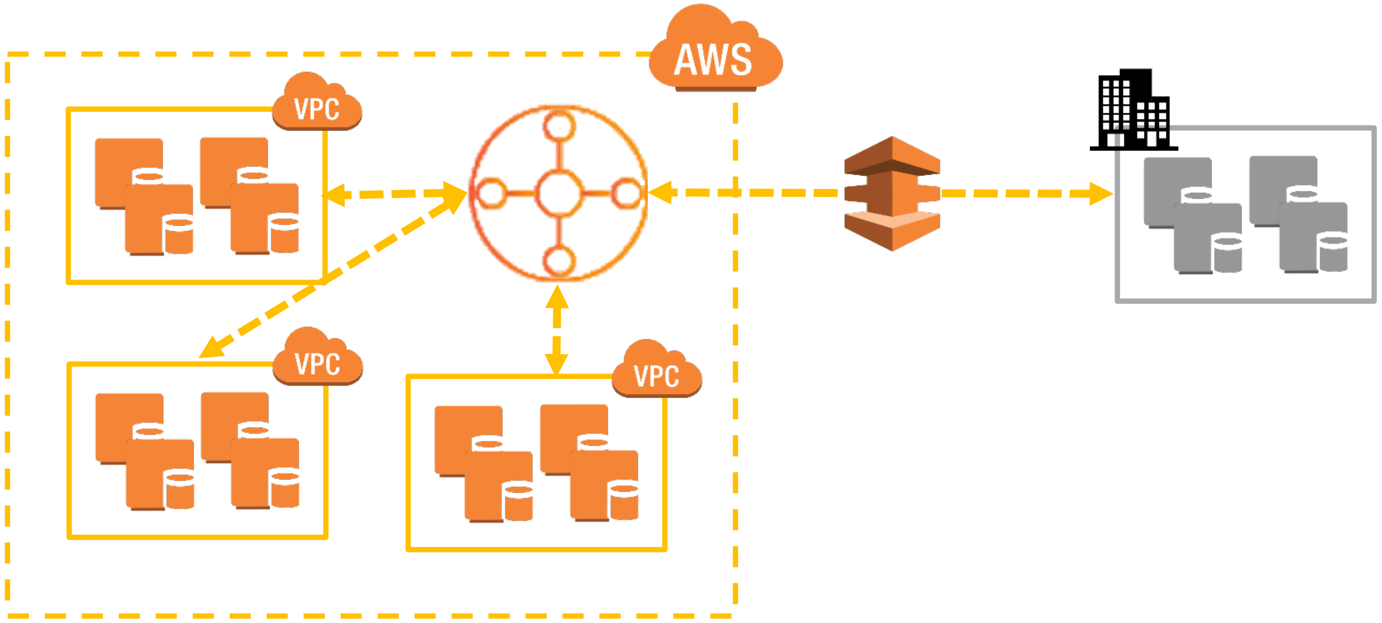
- Transit Gateway Basics
- TGW Southbound ASG Solution
- TGW Southbound HA Solution
- Comparison Chart

Transit Gateway Basics

- Interconnecting VPCs and on-premises
- Attachment:
  - Connect a resource to Transit Gateway (TGW)
  - VPN connections
  - A single subnet per Availability Zone (AZ) per VPC
- Association:
  - Associate an attachment with a single TGW Route Table (RT)
- Propagation:
  - Propagate attachment routes to one or more TGW RTs

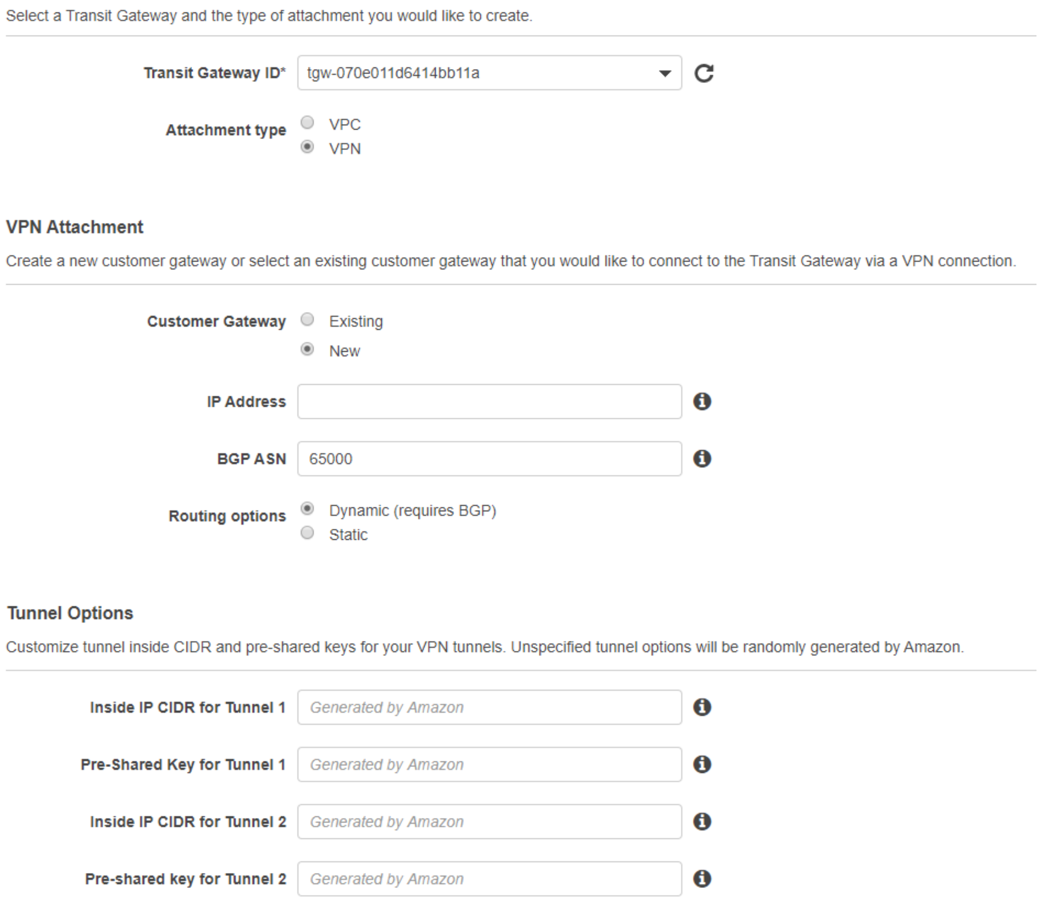
Transit Gateway Basics

- Network transit hub for interconnecting VPCs and on-premises
- Easier to manage than VPC peering
- Works across accounts and availability zones in a **single** region



TGW Basics - Attachments

- Attachment is a connection between a resource and TGW
- There are 2 types of attachments:
  - VPC attachment:
    - To one or more subnets per VPC
    - Single subnet per zone
    - Single attachment per subnet
  - VPN attachment:
    - Single attachment per VPN connection
    - Routing can be static or dynamic (BGP)
    - Performs ECMP between multiple tunnels



Select a Transit Gateway and the type of attachment you would like to create.

Transit Gateway ID* tgw-070e011d6414bb11a

Attachment type ○ VPC ● VPN

VPN Attachment

Create a new customer gateway or select an existing customer gateway that you would like to connect to the Transit Gateway via a VPN connection.

Customer Gateway ○ Existing ● New

IP Address

BGP ASN 65000

Routing options ● Dynamic (requires BGP) ○ Static

Tunnel Options

Customize tunnel inside CIDR and pre-shared keys for your VPN tunnels. Unspecified tunnel options will be randomly generated by Amazon.

Inside IP CIDR for Tunnel 1 *Generated by Amazon*

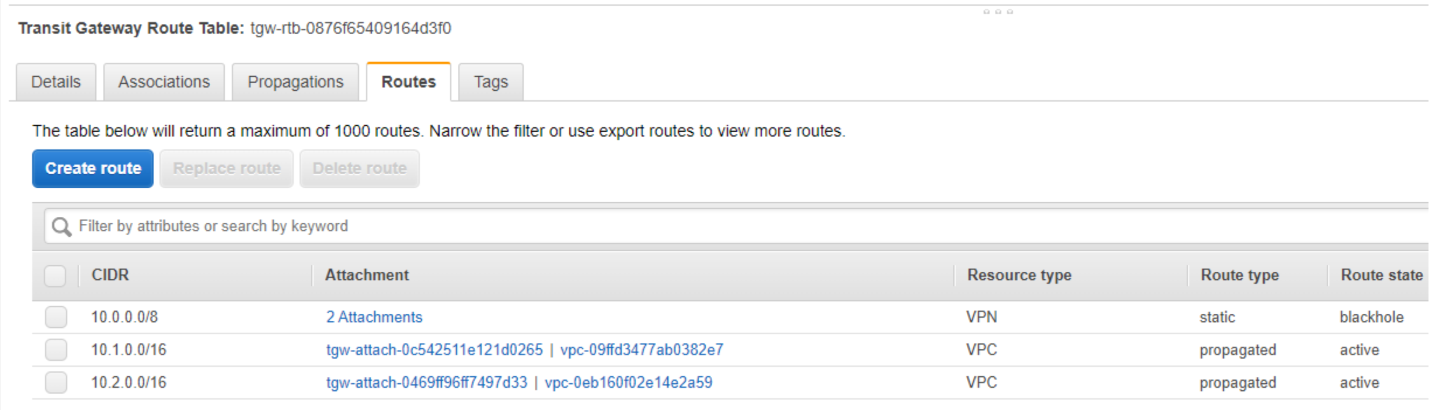
Pre-Shared Key for Tunnel 1 *Generated by Amazon*

Inside IP CIDR for Tunnel 2 *Generated by Amazon*

Pre-shared key for Tunnel 2 *Generated by Amazon*

TGW Basic – TGW Route Tables

- A TGW has one or more route tables
- Each attachment can be **associated** with a single route table
- An attachment follows route rules of the route table it is associated with
- An attachment can **propagate** its route to any TGW route table
- Routes can be static or propagated, and must point an attachment

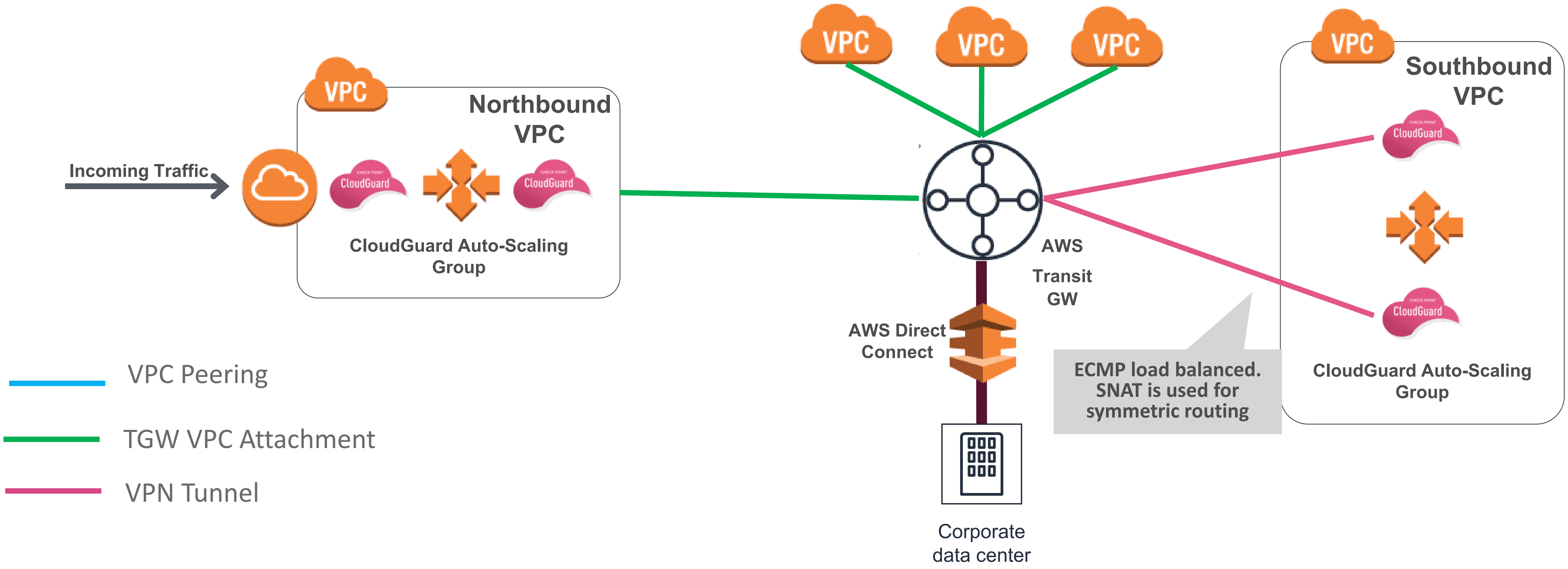


Transit Gateway Route Table: tgw-rtb-0876f65409164d3f0

The table below will return a maximum of 1000 routes. Narrow the filter or use export routes to view more routes.

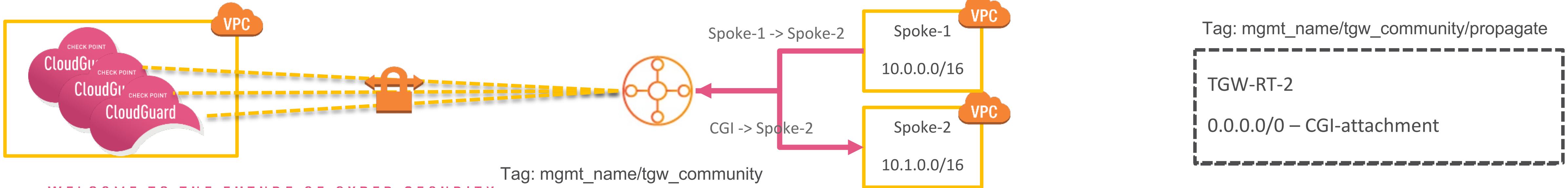
□	CIDR	Attachment	Resource type	Route type	Route state
□	10.0.0.0/8	2 Attachments	VPN	static	blackhole
□	10.1.0.0/16	tgw-attach-0c542511e121d0265 | vpc-09ffd3477ab0382e7	VPC	propagated	active
□	10.2.0.0/16	tgw-attach-0469ff96ff7497d33 | vpc-0eb160f02e14e2a59	VPC	propagated	active

Checkpoint TGW Blueprint



TGW Southbound – ASG Solution Architecture

- CGI AutoScaling Group (ASG) is deployed in a dedicated security VPC
- Each CGI instance is attached to the tagged TGW using VPN connection
- The CGI VPNs are associated with tagged TGW RTs
- The CGI VPNs are propagated as default route target to tagged TGW RTs
- The CGI instances learn the spoke routes from the TGW over BGP
- The TGW perform ECMP load balancing between the CGI ASG instances
- The CGI instances perform Source NAT on all connections from the TGW



Spoke-1

10.0.0.0/16

Spoke-2

10.1.0.0/16

Tag: mgmt_name/tgw_community

Tag: mgmt_name/tgw_community/propagate

TGW-RT-2

0.0.0.0/0 – CGI-attachment

TGW Southbound ASG – Automation Configuration

- Automation with CME using tgw_menu or autoprov_cfg tool
  - E.g. autoprov_cfg set template -tn "<TEMPLATE-NAME>" -vpn -vd "" -con "<VPN-COMMUNITY-NAME>" -dt TGW
- TGW Tagging (automatic):
  - TGW tags e.g. mgmt_name/tgw_comm_name
  - RT tags to associate CGI VPN attachments with it e.g. mgmt_name/tgw_comm_name/associate
  - RT tags to propagate CGI VPN attachments with it e.g. mgmt_name/tgw_comm_name/propagate
- Adding spokes (manual) – PS: can also be scripted
  - Create VPC attachment to spoke
  - In the VPC RT, create desired route with TGW as target
  - Associate the VPC attachment with TGW RT tagged with propagation
  - Propagate the attachment to the TGW RT tagged with association

TGW Southbound ASG – Automation Workflow

- Upon scaling event the CME automatically creates / deletes:
  - Gateway object in the management Smart Console
  - Cloud Formation Template for AWS VPN connection
  - TGW VPN attachment to the CGI VPN connection
  - TGW RT association and propagation to the CGI VPN connection attachment
  - VPN configurations on the management for the new VPN connection
- When a new spoke is added :
  - The TGW propagates the new route to the CGI over BGP
  - The Management Security Policy does **not** change

Check Point
SOFTWARE TECHNOLOGIES LTD

TGW HA (GEO-CLUSTER) SOLUTION

Architecture & Components

WELCOME TO THE FUTURE OF
CYBER SECURITY

POWERED BY CHECK POINT INFINITY

CLOUD • MOBILE • THREAT PREVENTION

TGW Southbound – HA Solution Architecture

External Subnet Route Table 3

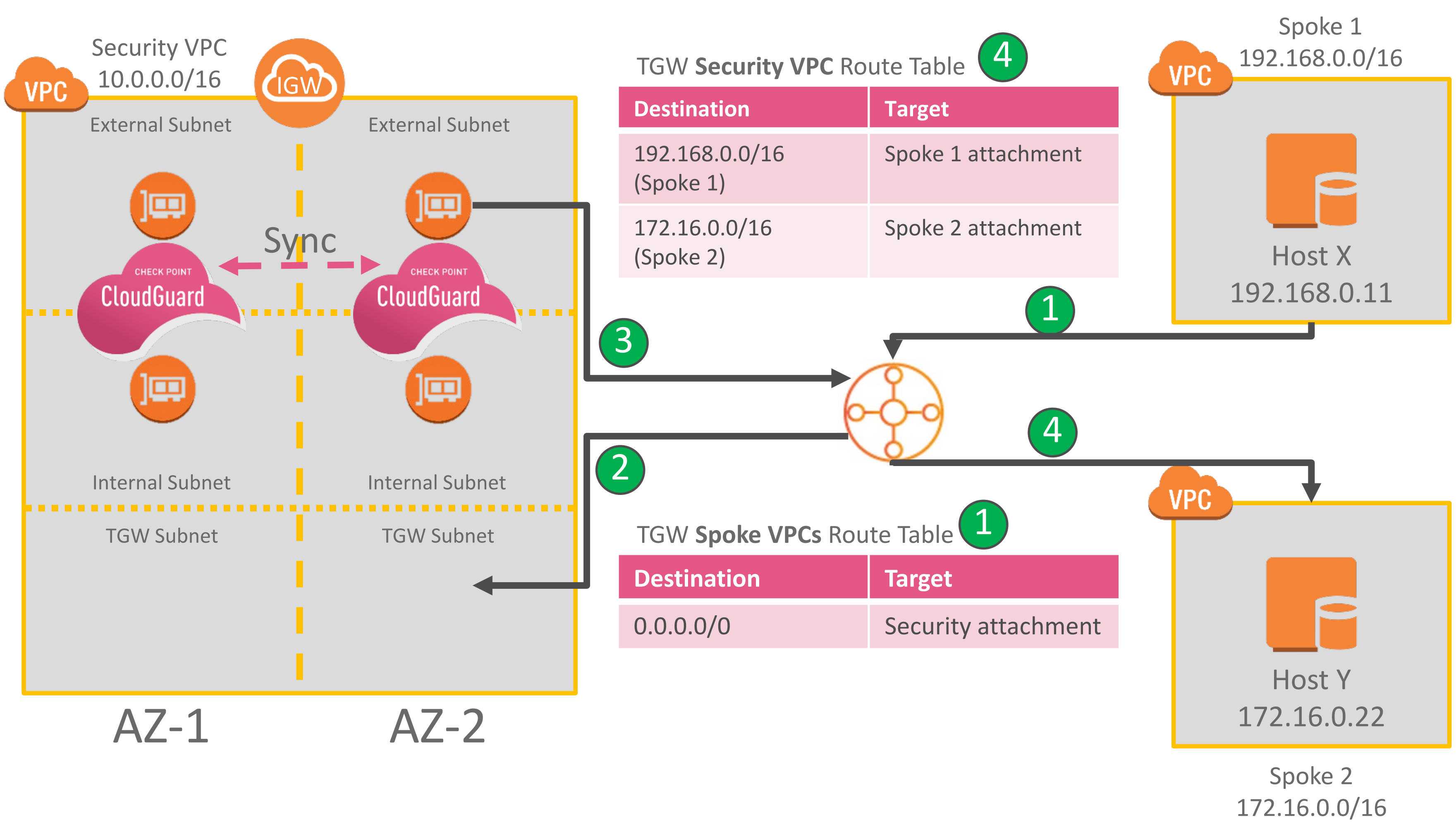
Destination	Target
10.0.0.0/16	Local
192.168.0.0/16 (Spoke 1)	Transit GW
172.16.0.0/16 (Spoke 2)	Transit GW
0.0.0.0/0	Internet GW

Internal Subnet Route Table

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	Active GW ENI

TGW Subnet Route Table 2

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	Active GW ENI



TGW **Security VPC** Route Table 4

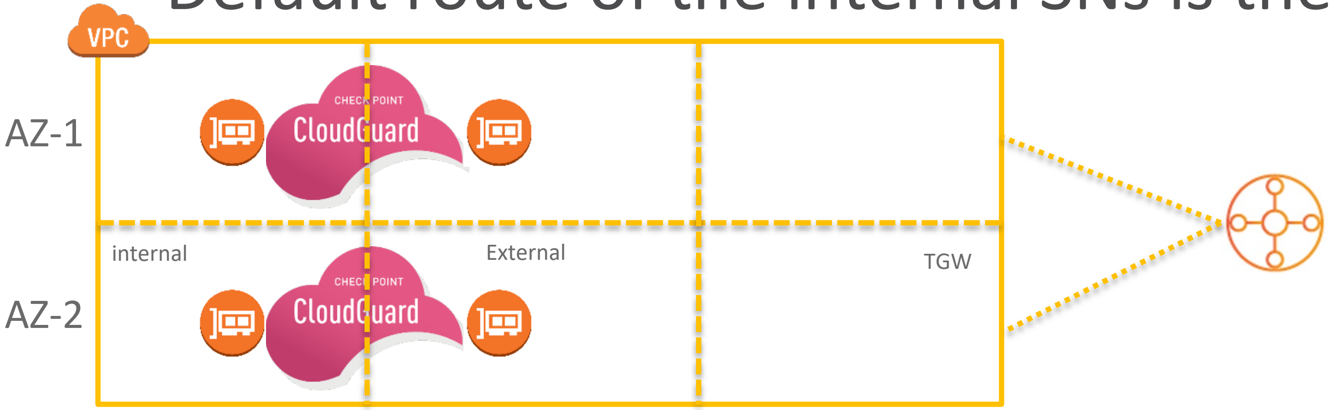
Destination	Target
192.168.0.0/16 (Spoke 1)	Spoke 1 attachment
172.16.0.0/16 (Spoke 2)	Spoke 2 attachment

TGW **Spoke VPCs** Route Table 1

Destination	Target
0.0.0.0/0	Security attachment

Transit Gateway HA Solution – Components

- CGI Cluster is deployed in a dedicated security VPC
- Each CGI instance is deployed in a separate AZ
- In each AZ 3 subnets (SNs) are created: external, internal and TGW
- Only the TGW SNs are attached to the TGW
- Default route of the TGW SNs is the Active CGI external ENI
- Default route of the internal SNs is the Active CGI internal ENI



Transit Gateway HA Solution – Configuration

- No CME configuration is required
- One time manual configuration of Smart Console object
- Configuration of TGW RT attachments, associations and propagations is manual
- Cloud Formation Template (CFT) will configure TGW RTs targeted to the Active member ENIs (external or internal)
- Any desired changes to the CFT RT configuration will be done manually

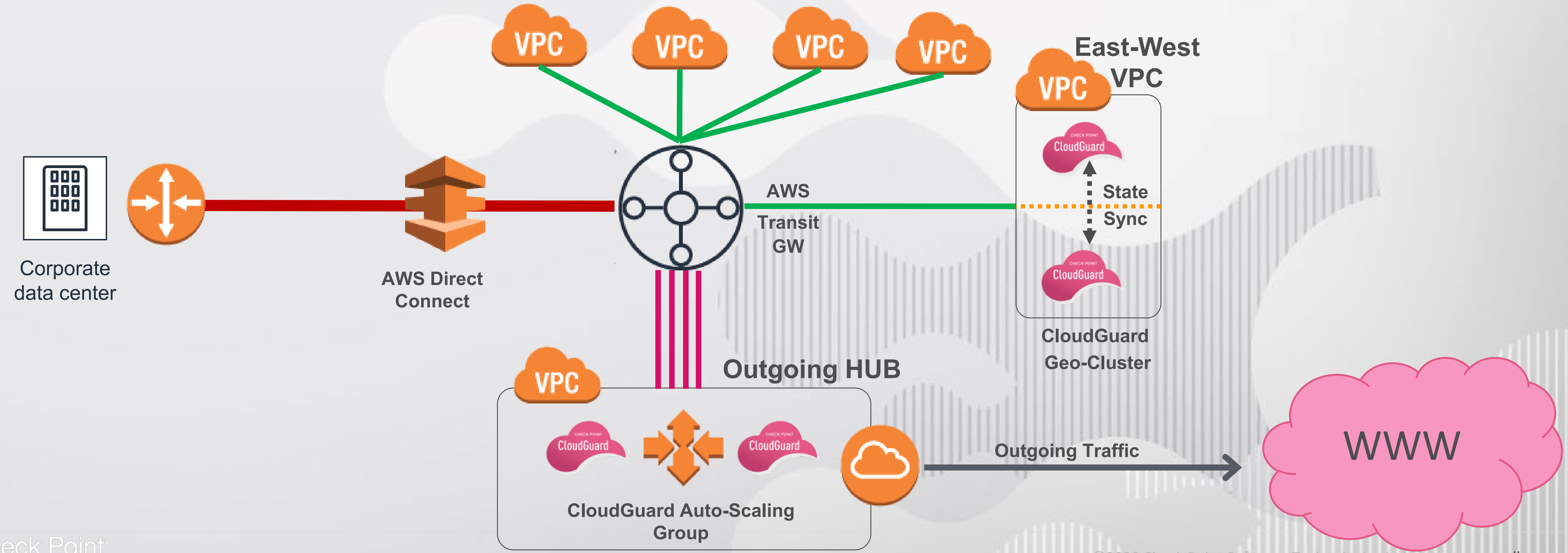
Transit Gateway HA Solution – Failover

- When failover occurs:
  - Standby CGI Cluster member will become active
  - RTs targeted to the failed CGI will automatically switch to the new active CGI
  - Connections are continued through the new active CGI with no interruptions
  - All Failover operations takes a few seconds

Transit Gateway - Southbound – Comparison

	TGW with Auto Scaling	TGW with Geo-Cluster
Scalability	Yes.	No. Static
Automation	Yes, with CME scripts – tags based	No. Manual Configuration
Deployment	CFT, Terraform	CFT.
Original Source IP	NATed by the gateways – SNAT required for symmetric routing.	Visible to the backend server – No SNAT required.
State Sync	No state sync	State is synced
Throughput	1.25Gbps per VPN attachment – Load Balanced with ECMP (Top aggregate: 50 Gbps) * using c5.large or c5n.large instance.	VPC attachment – Up to 11.3 Gbps NGFW & 4.7 Gbps NGTP per active gateway. (c5n.2xlarge instance)
Use Case	East/West - Egress	East/West - Egress
CG Controller	Supported	Not Supported (yet)
Versions	R80.20 and above	R80.40

TGW - Separate Outbound & E/W



Summary

- TGW ASG vs. TGW HA
- VPN vs. VPC attachment
- Scalable vs. static
- Automated vs. manual configuration
- Source NAT vs. original source

Check Point
SOFTWARE TECHNOLOGIES LTD

THANK YOU

WELCOME TO THE FUTURE OF
CYBER SECURITY

POWERED BY CHECK POINT INFINITY

CLOUD • MOBILE • THREAT PREVENTION