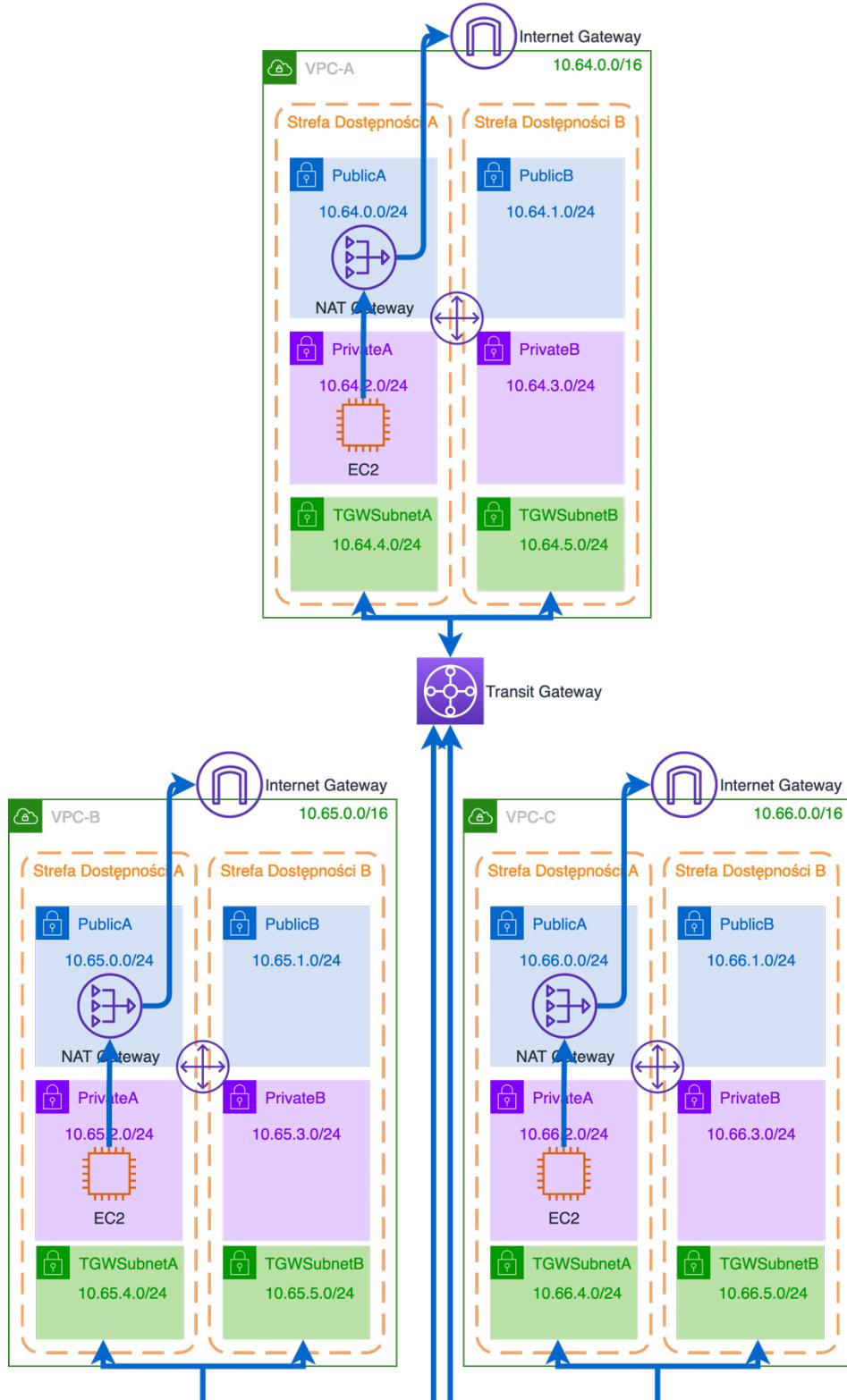


ĆWICZENIE NR 3

W tym ćwiczeniu połączymy multi-VPC z Transit Gateway do sieci prywatnej.

1.1 Przygotuj konfigurację startową

Od strony sieci w chmurze wykorzystamy konfigurację, jak w ćwiczeniu numer 2, trzech VPC połączonych przez TransitGateway. Konfiguracja pokazana jest na diagramie:



Stronę on-prem zasymulujemy również w AWS. Konfiguracja on-prem będzie się składać z serwera DNS, serwera webowego oraz serwera bastion.

1.2 Wgraj skrypty konfiguracyjne na S3

Całość konfiguracji powołamy ze skryptu CloudFormation, żeby wykorzystać zagnieździone konfiguracje udostępnimy serwisowi CloudFormation skrypty do pobierania w S3.

Wybierz z konsoli AWS usługę S3.

The screenshot shows the AWS Management Console search results for 'S3'. The top result is 'S3 Scalable Storage in the Cloud'. Below it are other services like S3 Glacier, Athena, and AWS Transfer Family. Under 'Features', there are sections for Datasets, Batch Operations, Buckets, and Access points. The 'Create bucket' button is not visible in this view.

Wybierz polecenie **Create bucket**

The screenshot shows the S3 Management Console. On the left, there's a sidebar with 'Amazon S3' and sections for Buckets, Access Points, Storage Lens, and Feature spotlight. The main area shows an 'Account snapshot' and a table for 'Buckets (0)'. A red box highlights the 'Create bucket' button at the top right of the table. Below the table, it says 'No buckets' and 'You don't have any buckets.' with another 'Create bucket' button.

Podaj nazwę koszyka, zweryfikuj region w którym tworzysz koszyk (w ćwiczeniu wybieramy region w Irlandii) i zaakceptuj wszystkie domyślne ustawienia. Nazwa musi być unikalna, możemy wykorzystać numer konta lub inny losowy ciąg znaków do zapewnienia sobie unikalności.

Create bucket

Buckets are containers for data stored in S3. [Learn more](#)

General configuration

Bucket name
cf-template-012634247170

Bucket name must be unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)

AWS Region
EU (Ireland) eu-west-1

Copy settings from existing bucket - *optional*
Only the bucket settings in the following configuration are copied.

[Choose bucket](#)

Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Block all public access
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

Block public access to buckets and objects granted through new access control lists (ACLs)
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access

Feedback English (US) ▾ Privacy Policy Terms of Use Cookie preferences

© 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Otwieramy koszyk.

Amazon S3

Buckets

Access Points Object Lambda Access Points Batch Operations Access analyzer for S3

Block Public Access settings for this account

Storage Lens Dashboards AWS Organizations settings

Feature spotlight [1](#)

AWS Marketplace for S3

Successfully created bucket cf-template-012634247170
To upload files and folders, or to configure additional bucket settings choose [View details](#).

Account snapshot
Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

[View Storage Lens dashboard](#)

Buckets (1)

Buckets are containers for data stored in S3. [Learn more](#)

[Create bucket](#)

[Find buckets by name](#)

Name	AWS Region	Access	Creation date
cf-template-012634247170	EU (Ireland) eu-west-1	Bucket and objects not public	May 17, 2021, 10:06:47 (UTC+02:00)

Feedback English (US) ▾ Privacy Policy Terms of Use Cookie preferences

© 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Wgrywamy skrypty konfiguracyjne wybierając polecenie **Upload**.

The screenshot shows the AWS S3 Management Console interface. On the left, there's a sidebar with 'Amazon S3' selected. Under 'Buckets', it lists 'Access Points', 'Object Lambda Access Points', 'Batch Operations', and 'Access analyzer for S3'. Below that are 'Block Public Access settings for this account', 'Storage Lens', 'Dashboards', 'AWS Organizations settings', and a 'Feature spotlight' section. At the bottom of the sidebar are links for 'AWS Marketplace for S3', 'Feedback', 'English (US)', 'Privacy Policy', 'Terms of Use', and 'Cookie preferences'. The main area shows the bucket 'cf-template-012634247170'. The 'Objects' tab is active. It displays a message: 'Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory [?] to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more [?]' with a blue link. Below this are buttons for 'Create folder', 'Upload' (which is highlighted with a red box), 'Copy URL', 'Open', 'Download', and 'Delete'. A search bar says 'Find objects by prefix:'. A table header includes 'Name', 'Type', 'Last modified', 'Size', and 'Storage class'. The table body says 'No objects' and 'You don't have any objects in this bucket.' with a 'Upload' button. At the bottom right of the main area is a small note: '© 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.'

Potrzebujemy następujących skryptów:

- **networkingdemo-lab1.yml** – tworzenie VPC z 4 podsieciami, IGW,NAT Gateway oraz EC2 w prywatnej podsieci;
- **networkingdemo-lab2-transitgateway.yml** – tworzenie TGW z podsieciami w 3 VPC;
- **networkingdemo-lab3-on-prem.yml** – konfiguracja VPC symulującego lokalne środowisko;
- **networkingdemo-lab3-start.yml** – skrypt łączący wywołanie całości konfiguracji opisanej w powyższych skryptach.

The screenshot shows the AWS S3 Management Console interface, similar to the previous one but with a different URL in the address bar: 's3.console.aws.amazon.com/s3/upload/cf-template-012634247170'. The main area is titled 'Upload'. It says 'Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. Learn more [?]' with a blue link. Below this is a large dashed box with the placeholder text 'Drag and drop files and folders you want to upload here, or choose Add files, or Add folders.' In the 'Files and folders' section, it shows '4 Total, 32.8 KB'. There are 'Remove', 'Add files', and 'Add folder' buttons. A search bar says 'Find by name'. A table lists the files:

Name	Folder	Type	Size
networkingdemo-lab1.yml	-	application/x-yaml	10.5 KB
networkingdemo-lab2-transitgateway.yml	-	application/x-yaml	5.6 KB
networkingdemo-lab3-on-prem.yml	-	application/x-yaml	13.2 KB
networkingdemo-lab3-start.yml	-	application/x-yaml	3.5 KB

Below this is a 'Destination' section with a dropdown menu set to 's3://cf-template-012634247170'. At the bottom are 'Feedback', 'English (US)', 'Privacy Policy', 'Terms of Use', and 'Cookie preferences'.

Po wgraniu plików kopujemy adres URL skryptu startującego **networkingdemo-lab3-start.yml**.

The screenshot shows the AWS S3 Management Console with the URL <https://s3.console.aws.amazon.com/s3/object/cf-template-012634247170/networkingdemo-lab3-start.yml>. The object details page for 'networkingdemo-lab3-start.yml' is displayed. The 'Object overview' section shows the following information:

- Owner: ee-account+71d9e5cbeb0f48f49bb099f2d97c162f
- AWS Region: EU (Ireland) eu-west-1
- Last modified: May 17, 2021, 10:23:02 (UTC+0:00)
- Size: 3.5 KB
- Type: yml
- Key: networkingdemo-lab3-start.yml

The 'S3 URI' field contains <https://cf-template-012634247170.s3-eu-west-1.amazonaws.com/networkingdemo-lab3-start.yml>. A tooltip 'Object URL Copied' is shown next to the URI. The 'Entity tag (Etag)' field shows `2d6a72a816675b2c5298fd7455e5df0a`.

The 'Object management overview' section notes that the following bucket properties and object management configurations impact the behavior of this object.

Feedback English (US) ▾ Privacy Policy Terms of Use Cookie preferences © 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

1.3 Utwórz CloudFormation stack z `networkingdemo-lab3-start.yml`

W konsoli AWS wybierz usługę CloudFormation, utwórz stack podając skopiowany adres URL skryptu.

The screenshot shows the AWS CloudFormation - Stack creation wizard with the URL <https://eu-west-1.console.aws.amazon.com/cloudformation/stacks/create?arn=arn%3aws%3cf%3template%3012634247170%2fnetworkingdemo-lab3-start%2eyml>. The 'Create stack' step is selected. The 'Specify template' section shows:

- Step 1: Specify template (selected)
- Step 2: Specify stack details
- Step 3: Configure stack options
- Step 4: Review

The 'Prerequisite - Prepare template' section has the 'Template is ready' radio button selected. The 'Specify template' section shows the 'Template source' as 'Amazon S3 URL' with the URL <https://cf-template-012634247170.s3-eu-west-1.amazonaws.com/networkingdemo-lab3-start.yml> entered. The 'Next' button is visible at the bottom right.

Feedback English (US) ▾ Privacy Policy Terms of Use Cookie preferences © 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Ciąg BUCKET w adresach URL skryptów zamień na właściwą nazwę koszyka, który utworzyłeś i załadowałeś do niego pliki. Podaj zakres lub konkretne IP z którego będziesz się łączył do serwera bastion (tutaj nie stosujemy AWS SSM do łączenia się z konsoli AWS, ponieważ symulujemy środowisko lokalne).

Screenshot of the AWS CloudFormation 'Specify stack details' step. The 'Stack name' field contains 'Lab3'. The 'Parameters' section shows three modules: 'Networking', 'VPC', and 'TransitGateway'. The 'Other parameters' section includes 'AvailabilityZoneA' set to 'eu-west-1a' and 'AvailabilityZoneB' set to 'eu-west-1b'. The 'SSHAccessIP' field contains '89.242.1.242/32'. Navigation buttons at the bottom are 'Cancel', 'Previous', and 'Next'.

Feedback English (US) ▾

© 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

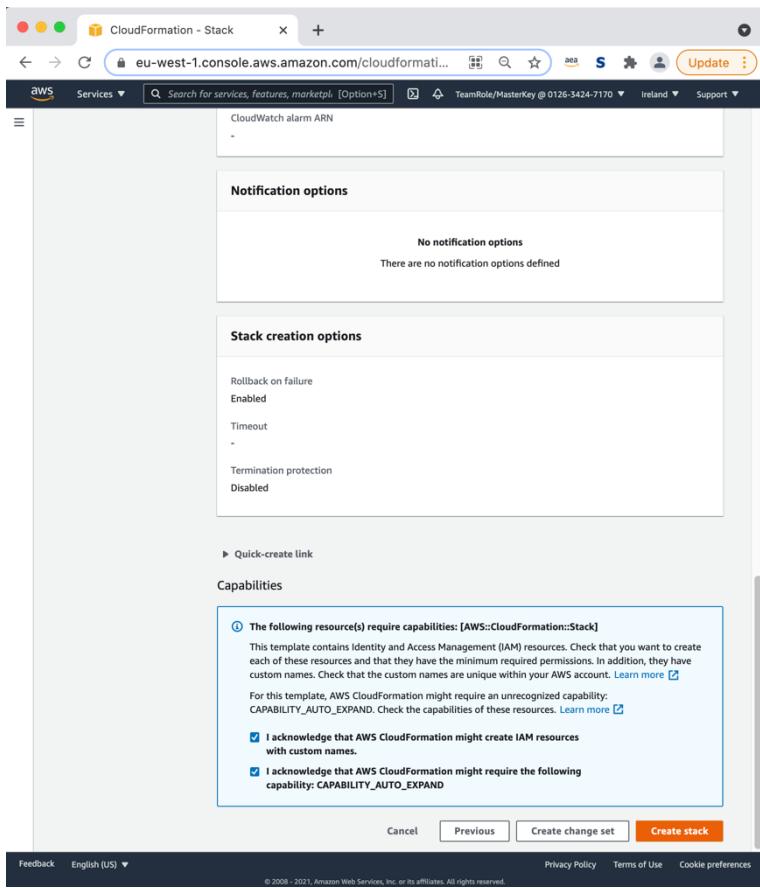
Zaakceptuj opcje domyślne.

Screenshot of the AWS CloudFormation 'Configure stack options' step. It shows sections for 'Tags' (with a 'Key' and 'Value' input), 'Permissions' (with an 'IAM role - optional' dropdown containing 'Sample-role-name'), and 'Advanced options' (with sections for 'Stack policy', 'Rollback configuration', 'Notification options', and 'Stack creation options'). Navigation buttons at the bottom are 'Cancel', 'Previous', and 'Next'.

Feedback English (US) ▾

© 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Potwierdź, że skrypty mogą tworzyć role z uprawnieniami oraz, że



Tworzenie konfiguracji może potrwać około 10 minut.

1.4 Zweryfikuj konfigurację on-prem

W konsoli AWS wybierz usługę EC2, z listy uruchomionych instancji wybierz maszynę OnPremBastion.

Podłącz się do maszyny korzystając z lokalnego klienta SSH. Klucz ee-default-keypair.pem możesz pobrać z panelu w EventEngine (<https://dashboard.eventengine.run/dashboard>). Użytkownik ec2-user jest utworzony domyślnie na serwerze.

Po zapisaniu lokalnie klucza dostępowego do serwera, zmień uprawnienia dla pliku na tylko do odczytu (w przypadku systemu Windows, proszę użyj odpowiedniego ustawienia).

```
chmod 400 ee-default-keypair.pem
```

Połącz się do serwera na jego publiczny adres IP:

```
ssh -i ee-default-keypair.pem ec2-user@<PUBLIC IP>
```

Sprawdź ustawienie DNS:

```
cat /etc/resolv.conf
```

```
bash-3.2$ chmod 400 ee-default-keypair.pem
bash-3.2$ ssh -i "ee-default-keypair.pem" ec2-user@18.202.231.102
The authenticity of host '18.202.231.102' (18.202.231.102) can't be established.
ECDSA key fingerprint is SHA256:MiAYwTd8mAIJd8g6dB8gOFZ1P+0zwIgBzNNeAGzhxgk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '18.202.231.102' (ECDSA) to the list of known hosts.

      _|_ _|_
      _\|_|_|
https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-10-0-160 ~]$ cat /etc/resolv.conf
; generated by /usr/sbin/dhclient-script
search example.corp
options timeout:2 attempts:5
nameserver 10.10.1.164
[ec2-user@ip-10-10-0-160 ~]$
```

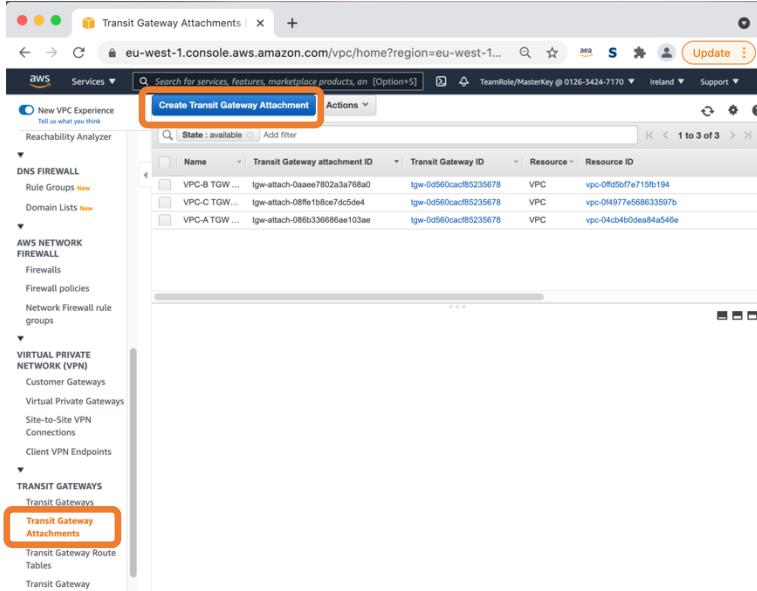
Używamy prywatnego DNS (nie dostarczanego z AWS). Sprawdzamy połączenie do naszego wewnętrznego serwera webowego:

```
curl http://myapp.example.corp
```

```
[ec2-user@ip-10-10-0-160 ~]$ curl http://myapp.example.corp
Hello, world.
[ec2-user@ip-10-10-0-160 ~]$
```

1.5 Utwórz VPN Attachment do TransitGateway

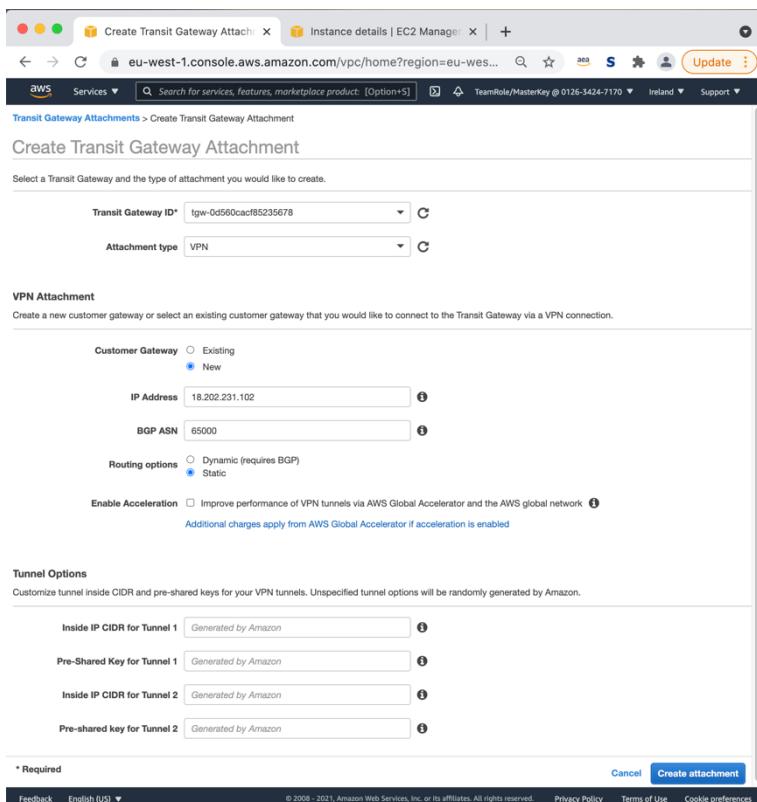
Z konsoli AWS wybierz usługę **VPC**, następnie z lewego menu **Transit Gateway Attachments**. Wybierz polecenie **Create Transit Gateway Attachment**.



The screenshot shows the AWS VPC console with the 'Transit Gateway Attachments' page open. On the left, there's a navigation sidebar with sections like 'DNS FIREWALL', 'AWS NETWORK FIREWALL', and 'VIRTUAL PRIVATE NETWORK (VPN)'. Under 'TRANSPORT GATEWAYS', 'Transit Gateways' is selected, and 'Transit Gateway Attachments' is highlighted with a red box. At the top, there's a search bar and a 'Create Transit Gateway Attachment' button, also highlighted with a red box.

Podaj dane niezbędne do konfiguracji:

- wybierz TransitGateway
- wybierz typ attachment'u – VPN
- zaznacz, że chcemy stworzyć nowy Customer Gateway
- podaj publiczny adres IP serwera bastion, do którego się łączysz
- routing użij statyczny
- pozostałe opcje zostaw domyślne



The screenshot shows the 'Create Transit Gateway Attachment' wizard. Step 1: Select a Transit Gateway and the type of attachment you would like to create. It shows a 'Transit Gateway ID' dropdown set to 'tgw-0d560cacfb5235678' and an 'Attachment type' dropdown set to '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 18.202.231.102
BGP ASN 65000
Routing options Dynamic (requires BGP) Static

Enable Acceleration Improve performance of VPN tunnels via AWS Global Accelerator and the AWS global network (Additional charges apply from AWS Global Accelerator if acceleration is enabled)

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

* Required

Wybierz **Site-to-Site VPN Connections** z lewego menu i zaczekaj na utworzenie się połączenia VPN.

1.6 Ściagnij konfigurację VPN

Kiedy już będzie dostępna konfiguracja VPN wybierz **Download configuration**.

VPN Connections | VPC Manager

Create VPN Connection Download Configuration Actions

Name	VPN ID	State	Virtual Private Gateway	Transit Gateway
vpn-009d70164501cc00c	available	-	tgw-0d580cadf85235678	cgw-08c

VPN Connection: vpn-009d70164501cc00c

Details Tunnel Details Static Routes Tags

VPN ID	vpn-009d70164501cc00c	State	available
Virtual Private Gateway	-	Customer Gateway	cgw-08ca751c3be07b31f
Transit Gateway	tgw-0d580cadf85235678	Customer Gateway Address	18.202.231.102
Type	ipsec.1	Category	VPN
VPC	-	Routing	Static
Acceleration Enabled	false	Authentication Type	Pre Shared Key
Local IPv4 Network Cidr	0.0.0.0/0	Remote IPv4 Network Cidr	0.0.0.0/0
Local IPv6 Network Cidr	-	Remote IPv6 Network Cidr	-

Wybierz **Openswan** z opcji dostawców.

VPN Connections | VPC Manager

Create VPN Connection Download Configuration Actions

Name	VPN ID	State	Virtual Private Gateway	Transit Gateway
vpn-009d70164501cc00c	available	-	tgw-0d580cadf85235678	cgw-08c

Download Configuration

Choose the sample configuration you wish to download based on your customer gateway. Please note these are samples, and will need modification to use Advanced Algorithms, Certificates, and/or IPv6.

Vendor: Openswan Platform: Openswan Software: Openswan 2.6.38+

Type	ipsec.1	Category	VPN
VPC	-	Routing	Static
Acceleration Enabled	false	Authentication Type	Pre Shared Key
Local IPv4 Network Cidr	0.0.0.0/0	Remote IPv4 Network Cidr	0.0.0.0/0
Local IPv6 Network Cidr	-	Remote IPv6 Network Cidr	-

Na tej samej stronie z połączeniem VPN wybierz zakładkę Tunel Details i zanotuj przydzielone IP publiczne dla tego tunelu.

1.7 Zdefiniuj trasowanie dla TransitGateway do OnPremisVPC

Dla statycznego routingu konieczne jest ustawienie w tablicy routingu TransitGateway routingu do środowiska on-premises. Wybierz **Transit Gateway Route Tables** z lewego menu i dla istniejącej tablicy w zakładce **Routes** wybierz **Create static route**.

Wpisz CIDR OnPremVPC, czyli 10.10.0.0/16 i skojarz to z attachment'em VPN, który wcześniej zrobileś.

Transit Gateway route table dropdown:

Attachment ID	Name tag	Resource ID	Resource Type	Resource owner ID	Associated table
tgw-attach-086b336686aae103ae	VPC-A TGW	vpc-04cb4b0dea84a546e	vpc	012634247170	tgw-rtb-06af375b0271cf738
tgw-attach-08fe1b8ce7dc5de4	VPC-C TGW	vpc-04977e568633597b	vpc	012634247170	tgw-rtb-06af375b0271cf738
tgw-attach-0aaee7802a3a768a0	VPC-B TGW	vpc-0ff5b7e715fb194	vpc	012634247170	tgw-rtb-06af375b0271cf738
tgw-attach-0e9ccfb951fe682	VPN	009d70164501cc00c	vpn	012634247170	tgw-rtb-06af375b0271cf738

Na ten moment routing nie będzie wskazywał na sieć, ponieważ jeszcze jej nie połączymy.

Transit Gateway Route Table details:

CIDR	Attachment	Resource	Route type	Route state	Prefix List ID
10.10.0.0/16	2 Attachments	VPN	static	blackhole	-
10.64.0.0/16	tgw-attach-086b336686aae103ae vpc-04cb4b0dea84a546e	VPC	propagated	active	-
10.65.0.0/16	tgw-attach-0aaee7802a3a768a0 vpc-0ff5b7e715fb194	VPC	propagated	active	-
10.66.0.0/16	tgw-attach-08fe1b8ce7dc5de4 vpc-04977e568633597b	VPC	propagated	active	-

1.8 Skonfiguruj reguły sieciowe dla serwera Bastion po stronie on-premises

W konsoli AWS dla usługi EC2 wybierz z listy instancji serwer Bastion. Wybierz dla niego **Actions->Networking->Change source/destination check**.

Wybierz opcję Stop, to pozwoli maszynie działać jako router i przyjmować komunikację kierowaną dla innych adresów niż własny maszyny.

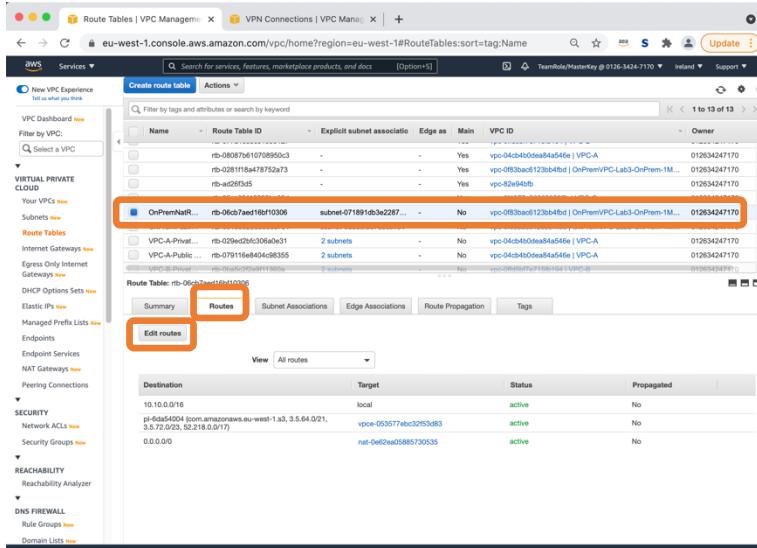
Również dla tej samej maszyny wybierz zakładkę **security** i przejdź do podlinkowanej **Security Group**.

W zakładce Inbound rules, w której już znajduje się reguła określona przy tworzeniu (otwarcie komunikacji po ssh dla twojego ip) dodaj reguły pozwalające na UDP na portach 500 i 4500 dla IP przydzielonych do tunelu VPN.

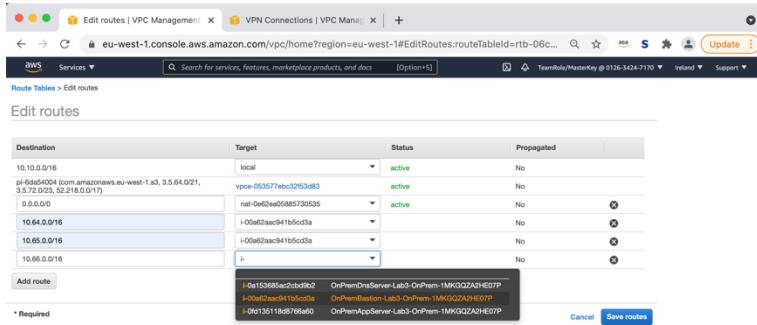
Edytor pozwala na zdefiniowanie zakresu IP, możemy ograniczyć regułę do pojedynczych adresów podając zakres /32.

1.9 Dodaj trasowanie komunikacji z VPC A,B i C przez Bastion w tablicy routingu dla podsieci OnPremNat

Wybierz **Route Tables** z menu z lewej strony oraz tablicę **OnPremNatRouteTable**. Następnie w zakładce **Routes Edit routes**.



Dodaj routing dla adresacji zgodnej z CIDR VPC-A, VPC-B i VPC-C. Całość komunikacji będzie przebiegać przez serwer Bastion, wybierz go w Target w pierwszym kroku wybierając **Instance** i następnie nazwę konkretnego serwera wirtualnego.



1.10 Skonfiguruj OpenSWAN

Polacz sie powtórnie do serwera wirtualnego Bastion, jeśli twoje połaczenie już straciło aktywność.

Zapisz w /etc/sysctl.conf odblokowanie przekazywania IP:

```
sudo nano /etc/sysctl.conf
```

Dodaj nastepujace linie do tego

```
net.ipv4.ip_forward = 1
```

```
net.ipv4.conf.default.rp_filter =
```

```
net.ipv4.conf.default.accept_source_route = 0
```

Zapisz i zamknij plik używając skrótów klawiszowych Ctrl+O,
poprzez:

sudo suaptl -n

Otwórz plik z konfiguracją VPN, któryściągnąłeś z konsoli AWS, jest tam instrukcja krok po kroku jak włączyć VPN i niezbędna konfiguracja.

Utwórz plik aws.conf w katalogu /etc/ipsec.d:

```
sudo nano /etc/ipsec.d/aws.conf
```

Zapisz w pliku fragment konfiguracji ze skopowanego pliku nakładając kilka modyfikacji:

- usuń linię auth=esp
- zamień <LOCAL-NETWORK> CIDR swojej sieci, czyli 10.10.0.0/16
- zamień <REMOTE-NETWORK> CIDR zdalnej sieci, czyli u nas 10.64.0.0/14

Finalnie plik powinien wyglądać jak poniżej:

```
GNU nano 2.9.8          /etc/ipsec.d/aws.conf          Modified

conn Tunnel1
    authby=secret
    auto=start
    left=defaultroute
    leftid=18.202.231.102
    right=52.51.216.254
    type=tunnel
    ikeLifetime=8h
    keyLife=1h
    phash=aes128-sha1;modpi024
    ikeSaes128-sha1;modpi024
    keyingtries=%forever
    keyexchange=ike
    leftsubnet=10.10.0.0/16
    rightsubnet=10.64.0.0/14
    dpddelay=0
    dpdtimeout=30
    dpdaction=restart_by_peer
```

Get Help Write Out Where Is Cut Text Justify Cur Pos M-U Undo
Exit Read File Replace Uncut Text To Spell Go To Line M-E Redo

Utwórz plik aws.secrets w katalogu /etc/ipsec.d, jest to krok piąty z pliku konfiguracyjnego.

```
sudo nano /etc/ipsec.d/aws.secrets
```

W pliku zapisz podaną linię autoryzacyjną i zapisz używając skrótów klawiszowych Ctrl+O, Enter, Ctrl+X. Teraz zostaje już tylko odblokować OpenSwan i go uruchomić:

```
sudo systemctl enable ipsec.service
```

```
sudo ipsec start
```

```
[ec2-user@ip-10-10-0-160 ~]$ sudo nano /etc/sysctl.conf
[ec2-user@ip-10-10-0-160 ~]$ sudo sysctl -p
net.ipv4.ip_forward = 1
net.ipv4.conf.default.rp_filter = 0
net.ipv4.conf.all.rp_filter = 0
[ec2-user@ip-10-10-0-160 ~]$ sudo nano /etc/ipsec.d/aws.conf
[ec2-user@ip-10-10-0-160 ~]$ sudo nano /etc/ipsec.d/aws.conf
[ec2-user@ip-10-10-0-160 ~]$ sudo nano /etc/ipsec.d/aws.secrets
[ec2-user@ip-10-10-0-160 ~]$ sudo systemctl enable ipsec.service
rt
Created symlink from /etc/systemd/system/multi-user.target.wants/ipsec.service to /usr/lib/systemd/system/ipsec.service.
[ec2-user@ip-10-10-0-160 ~]$ sudo ipsec start
Redirecting to: systemctl start ipsec.service
[ec2-user@ip-10-10-0-160 ~]$
```

1.11 Dodaj CIDR 10.10.0.0/16 do route tables w VPC-A, VPC-B i VPC-C

Mamy działający VPN i podłączony do TransitGateway. Teraz podłączmy w tablicy routingu podsieci z VPC-A, VPC-B i VPC-C dostęp do adresacji 10.10.0.0/16.

Destination	Target	Status	Propagated
10.64.0.0/16	local	active	No
0.0.0.0/0	nat-0fb83c7767494bf00	active	No
10.65.0.0/16	tgw-0d560cacf85235678	active	No
10.66.0.0/16	tgw-0d560cacf85235678	active	No
10.10.0.0/16	tgw-		No

1.12 Przetestuj połączenie

Możesz użyć polecenia curl http://myapp.example.corp . Na OnPremAppServer jest działający webserwer, co sprawdziliśmy na początku ćwiczenia.

Użyj polecenia dig @<PRYWATNE-IP-DNS> myapp.example.corp, żeby zapytać DNS on-premises o adres.

Session ID: MasterKey-0414cbc001f51e7a1 Instance ID: i-0e9d0b64df9ed64a9
sh-4.2\$ dig @10.10.1.164 myapp.example.corp

```
; <>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.amzn2.4 <>> @10.10.1.164 myapp.example.corp
; (1 server found)
;; global options: +cmd
;; Got answer:
;; -->HEADER<- opcode: QUERY, status: NOERROR, id: 20248
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2
;
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;myapp.example.corp.      IN      A
;
;; ANSWER SECTION:
myapp.example.corp.    60      IN      A      10.10.1.217
;
;; AUTHORITY SECTION:
example.corp.          86400   IN      NS      ns1.example.corp.
;
;; ADDITIONAL SECTION:
ns1.example.corp.      60      IN      A      10.10.1.164
;
;; Query time: 1 msec
;; SERVER: 10.10.1.164#53(10.10.1.164)
;; WHEN: Mon May 17 14:54:34 UTC 2021
;; MSG SIZE rcvd: 97
```

sh-4.2\$

Ukończyłeś ćwiczenie!