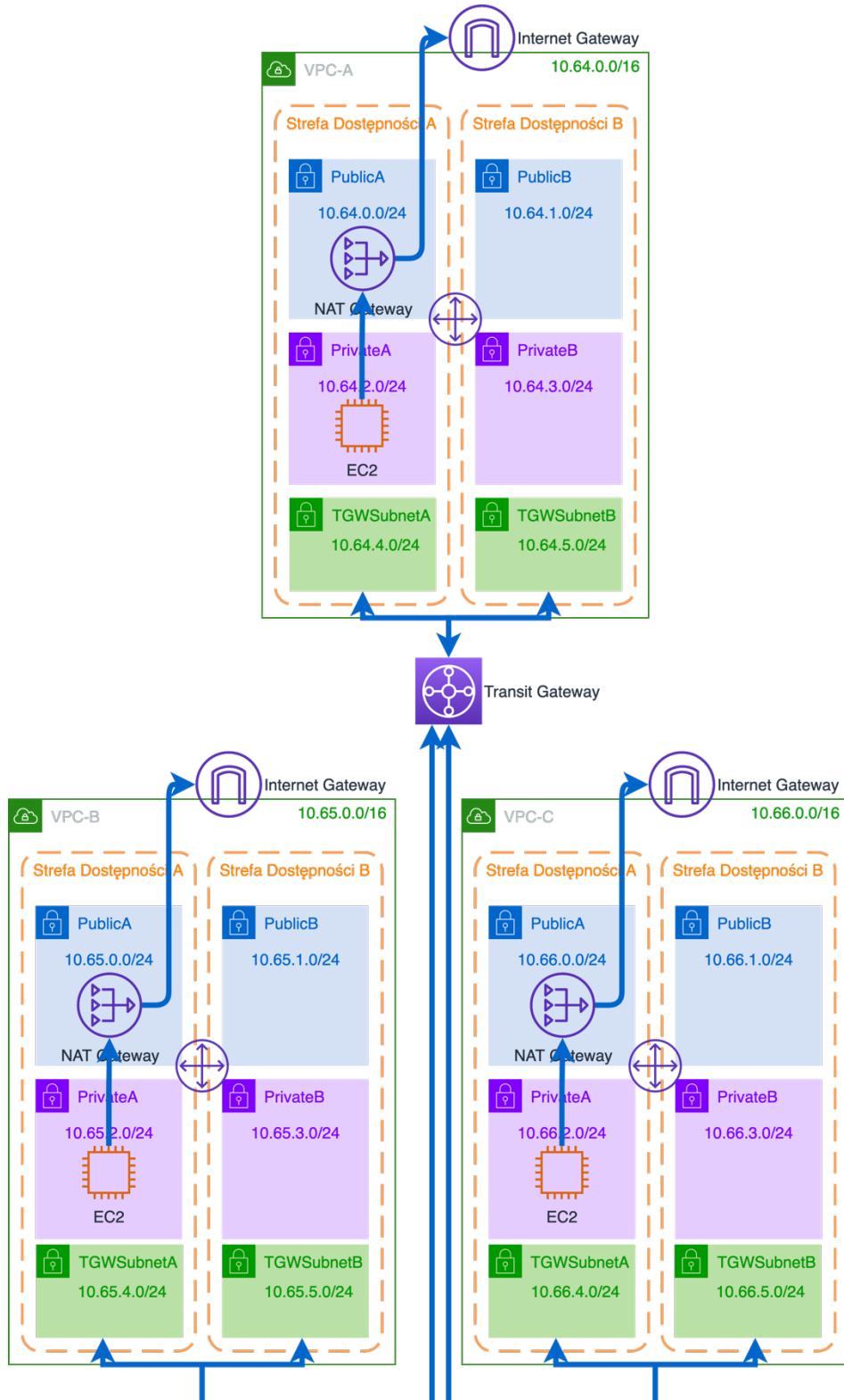


ĆWICZENIE NR 5

W tym ćwiczeniu połączymy się prywatnym interfejsem z usługą S3.

1.1 Przygotuj konfigurację startową

W ćwiczeniu 5 i 6 wykorzystamy konfigurację, jak w ćwiczeniu numer 2, trzech VPC połączonych przez TransitGateway. Konfiguracja pokazana jest na diagramie:



1.2 Wgraj skrypty konfiguracyjne na S3

Całość konfiguracji powołamy ze skryptu CloudFormation, żeby wykorzystać zagnieźdzoną konfigurację 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 search bar at the top contains 'S3'. The results are categorized under 'Services' and 'Features'. Under 'Services', there is a card for 'S3' (Scalable Storage in the Cloud) with a 'Top features' section containing 'Buckets', 'Access points', and 'Batch Operations'. Other services listed include 'S3 Glacier' (Archive Storage in the Cloud), 'Athena' (Query Data in S3 using SQL), and 'AWS Transfer Family' (Fully managed support for SFTP, FTPS and FTP). Under 'Features', there are cards for 'Datasets' (IoT Analytics feature), 'Batch Operations' (S3 feature), and 'Buckets' (S3 feature). A link to 'Access points' is also visible. At the bottom of the page, there are links for 'Privacy Policy', 'Terms of Use', and 'Cookie preferences'.

Wybierz polecenie **Create bucket**

The screenshot shows the Amazon S3 Management Console. The left sidebar has a 'Buckets' section with options like 'Access Points', 'Object Lambda Access Points', 'Batch Operations', and 'Access analyzer for S3'. Below that is a 'Block Public Access settings for this account' section. Under 'Storage Lens', there are 'Dashboards' and 'AWS Organizations settings'. A 'Feature spotlight' section is also present. The main content area is titled 'Amazon S3' and shows an 'Account snapshot' with a 'View Storage Lens dashboard' button. Below it is a 'Buckets (0)' section with a 'Create bucket' button highlighted with a red box. There is also a search bar and a 'Find buckets by name' button. At the bottom, there is a table header for 'Name', 'AWS Region', 'Access', and 'Creation date'. The message 'No buckets' and 'You don't have any buckets.' is displayed. At the very bottom, there are links for 'Feedback', 'English (US)', 'Privacy Policy', 'Terms of Use', and 'Cookie preferences'.

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.

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

General configuration

Bucket name
cf-template-012634247170

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

Otwieramy koszyk.

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

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](#)

Buckets (1)

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

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

Wgrywamy skrypty konfiguracyjne wybierając polecenie **Upload**.

The screenshot shows the AWS S3 Management Console. On the left, the sidebar has sections for Buckets, Storage Lens, and Feature spotlight. The main area is titled 'cf-template-012634247170' and shows the 'Objects' tab selected. A red box highlights the 'Upload' button in the top navigation bar. Below it, there's a search bar and a table header with columns: Name, Type, Last modified, Size, and Storage class. The table body displays a message: 'No objects' and 'You don't have any objects in this bucket.' At the bottom right of the main area is another 'Upload' button.

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-lab5-start.yml** – skrypt łączący wywołanie całości konfiguracji opisanej w powyższych skryptach.

The screenshot shows the AWS S3 Management Console after an upload. A green banner at the top says 'Upload succeeded'. Below it, a summary table shows 'Destination' as 's3://cf-template-012345678' and 'Succeeded' as '3 files, 18.9 KB (100.00%)'. The 'Files and folders' tab is selected, showing a table with three entries: 'networkingdemo-lab1.yml', 'networkingdemo-lab2-transitgateway.yml', and 'networkingdemo-lab5-start.yml'. All three entries show a status of 'Succeeded' with a green checkmark icon. The table has columns: Name, Folder, Type, Size, Status, and Error.

Po wgraniu plików kopujemy adres URL skryptu startującego **networkingdemo-lab5-start.yml**.

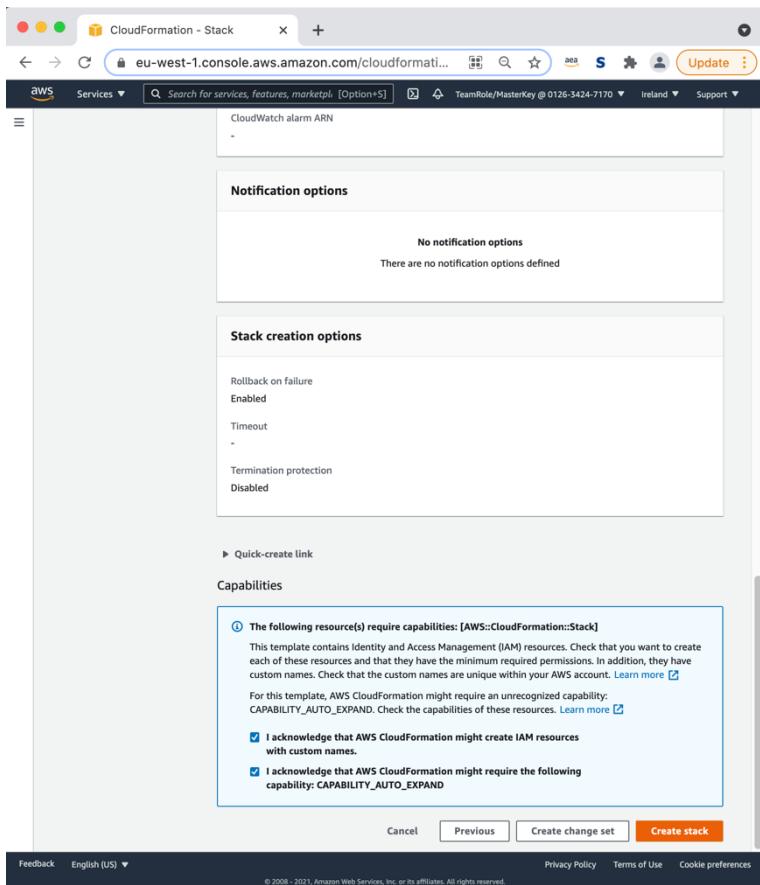
The screenshot shows the AWS S3 Management Console. In the left sidebar, under 'Buckets', there's a section for 'Access Points'. The main content area displays the properties of a file named 'networkingdemo-lab5-start.yml'. The 'Object overview' section includes details like Owner (ee-account+9d8555fbaab4cd08cbc3c4dd396636a), AWS Region (EU (Ireland) eu-west-1), Last modified (May 21, 2021, 13:00:56 (UTC+02:00)), Size (2.8 KB), Type (yml), and Key (networkingdemo-lab5-start.yml). A tooltip 'Object URL Copied' appears over the URL link.

1.3 Utwórz CloudFormation stack z `networkingdemo-lab5-start.yml`

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

The screenshot shows the AWS CloudFormation - Stack creation wizard. On the left, a sidebar lists steps: Step 1 (Specify template), Step 2 (Specify stack details), Step 3 (Configure stack options), and Step 4 (Review). The main panel is titled 'Create stack' and 'Prerequisite - Prepare template'. It shows the 'Prepare template' section with three options: 'Template is ready' (selected), 'Use a sample template', and 'Create template in Designer'. Below this is the 'Specify template' section, which contains a note about JSON or YAML files and a 'Template source' field. The 'Amazon S3 URL' radio button is selected, and the URL <https://cf-template-012345678.s3-eu-west-1.amazonaws.com/networkingdemo-lab5-start.yml> is entered. At the bottom right are 'Cancel' and 'Next' buttons.

Ciąg BUCKET w adresach URL skryptów zamień na właściwą nazwę koszyka, który utworzyłeś i załadowałeś do niego pliki. Zaakceptuj opcje domyślne.



Tworzenie konfiguracji może potrwać około 10 minut.

1.4 Sprawdź komunikację z usługą S3

Wybierz w konsoli AWS usługę EC2. Podłącz się do jednej z maszyn uruchomionych w VPC A lub B lub C korzystając z Session Managera. Teraz jeszcze konfiguracja każdej z maszyn jest analogiczna, wszystkie mają dostęp do internetu.

Użyj polecenia wylistowania wszystkich obiektów w koszyku zamieniając BUCKET_NAME nazwą własnego koszyka (może to być koszyk stworzony na potrzeby skryptów CloudFormation):

```
aws s3 ls s3://BUCKET_NAME
```

```
aws s3 ls s3://cf-template-012345678
2021-05-21 11:00:55      10715 networkingdemo-lab1.yml
2021-05-21 11:00:56      5777 networkingdemo-lab2-transitgateway.yml
2021-05-21 11:00:56      2867 networkingdemo-lab5-start.yml
sh-4.2$
```

```
echo 'Hello ☺' > hello.txt
aws s3 cp hello.txt s3://BUCKET_NAME/
aws s3 ls s3://BUCKET_NAME/
```

```
aws s3 cp hello.txt s3://cf-template-012345678/hello.txt
upload: ./hello.txt to s3://cf-template-012345678/hello.txt
sh-4.2$ aws s3 ls s3://cf-template-012345678
2021-05-21 11:00:55      10715 networkingdemo-lab1.yml
2021-05-21 11:00:56      5777 networkingdemo-lab2-transitgateway.yml
2021-05-21 11:00:56      2867 networkingdemo-lab5-start.yml
sh-4.2$
```

Możesz zweryfikować zawartość koszyka również w konsoli webowej AWS.

The screenshot shows the AWS S3 Management Console interface. On the left, there's a sidebar with various AWS services like Buckets, Storage Lens, Dashboards, and AWS Organizations settings. The main area displays the contents of a bucket named 'cf-template-012345678'. The 'Objects' tab is selected. There are four objects listed:

Name	Type	Last modified	Size	Storage class
hello.txt	txt	May 24, 2021, 10:22:57 (UTC+02:00)	10.0 B	Standard
networkingdemo-lab1.yml	yml	May 21, 2021, 13:00:55 (UTC+02:00)	10.5 KB	Standard
networkingdemo-lab2-transitgateway.yml	yml	May 21, 2021, 13:00:56 (UTC+02:00)	5.6 KB	Standard
networkingdemo-lab5-start.yml	yml	May 21, 2021, 13:00:56 (UTC+02:00)	2.8 KB	Standard

1.5 Zablokuj wyjście z podsieci prywatnej w VPC A do internetu

Dla podsieci w której jest utworzona maszyna w VPC A zdefiniuj ACL, który pozwala wyłącznie na komunikację w lokalnych VPC A, B i C. Zweryfikuj połączenie poprzez Session Manager. Powinieneś utracić możliwość komunikacji z maszyną.

Na stronie usługi VPC z lewego menu wybierz Network ACLs i następnie Create network ACL.

The screenshot shows the AWS VPC Network ACLs page. On the left, there's a sidebar with various VPC-related services like New VPC Experience, Managed Prefix Lists, Endpoints, Peering Connections, Network ACLs, Security Groups, DNS Firewall, AWS Network Firewall, and Virtual Private Network (VPN). The main area displays a list of Network ACLs:

Name	Network ACL ID	Associated with	Default
-	acl-2aa18653	3 Subnets	Yes
-	acl-0675fe4e2ce3d5ad5	6 Subnets	Yes
-	acl-071c0ef1f27ae0e14	6 Subnets	Yes
-	acl-0fc5cc276b917706	6 Subnets	Yes

At the bottom, there's a section titled 'Select a network ACL' with three options: 'Create a new network ACL', 'Edit an existing network ACL', and 'View details for an existing network ACL'.

Podaj nazwę dla ACL-ki oraz wybierz VPC-A.

Create network ACL info

A network ACL is an optional layer of security that acts as a firewall for controlling traffic in and out of a subnet.

Network ACL settings

Name - optional
Creates a tag with a key of 'Name' and a value that you specify.

VPC
VPC to use for this network ACL.

Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional
<input type="text" value="Name"/>	<input type="text" value="privateSubnetACL"/>

Add new tag
You can add 49 more tags.

Cancel **Create network ACL**

Zauważ, że w odróżnieniu od domyślnego ACL dla VPC nowo utworzona ACL ma tylko regułę blokowania całości ruchu wchodzącego i wychodzącego.

You successfully created acl-06270dff9797ac05f / privateSubnetACL

Details **Info**

Network ACL ID: **acl-06270dff9797ac05f** Associated with: **-** Default: **Yes** VPC ID: **vpc-0facd6045062e247e / VPC-A**

Owner: **220743612060**

Inbound rules (1) **Edit inbound rules**

Rule number	Type	Protocol	Port range	Source	Allow/Deny
*	All traffic	All	All	0.0.0.0/0	Deny

Zdefiniuj ograniczenie ruchu do lokalnych sieci VPC-A, VPC-B oraz VPC-C tak samo dla wchodzącego jak i wychodzącego.

Edit inbound rules

Inbound rules control the incoming traffic that's allowed to reach the VPC.

Rule number	Type	Protocol	Port range	Source	Allow/Deny	Info
100	Custom TCP	TCP (6)	0	10.64.0.0/16	Allow	Remove
110	Custom TCP	TCP (6)	0	10.65.0.0/16	Allow	Remove
120	Custom TCP	TCP (6)	0	10.66.0.0/16	Allow	Remove
*	All traffic	All	All	0.0.0.0/0	Deny	Info

[Add new rule](#) [Sort by rule number](#)

[Cancel](#) [Preview changes](#) [Save changes](#)

Edit outbound rules

Outbound rules control the outgoing traffic that's allowed to leave the VPC.

Rule number	Type	Protocol	Port range	Destination	Allow/Deny	Info
100	Custom TCP	TCP (6)	0	10.64.0.0/16	Allow	Remove
110	Custom TCP	TCP (6)	0	10.65.0.0/16	Allow	Remove
120	Custom TCP	TCP (6)	0	10.66.0.0/16	Allow	Remove
*	All traffic	All	All	0.0.0.0/0	Deny	Info

[Add new rule](#) [Sort by rule number](#)

[Cancel](#) [Preview changes](#) [Save changes](#)

Przypisz nowy ACL do podsieci, której używa maszyna EC2. Przy zaznaczonej ACL wybierz zakładkę **Subnet associations** i polecenie **Edit subnet associations**.

Network ACLs (1/5) Info

Name	Network ACL ID	Associated with	Default
acl-2aa18655	3 Subnets	Yes	
acl-0675fe4e2ce3d5ad5	6 Subnets	Yes	
acl-0710ef1f127ae0e14	6 Subnets	Yes	
acl-0fcfc2c276b917706	6 Subnets	Yes	
privateSubnetACL	acl-06270dff9797ac05f	—	No

acl-06270dff9797ac05f / privateSubnetACL

[Details](#) [Inbound rules](#) [Outbound rules](#) [Subnet associations](#) [Tags](#)

Subnet associations

Name	Subnet ID	Associated with	Availability zone	IPv4 C
No subnets in this region are associated with this network ACL.				

Szukana podsieć to APC-A-PrivateA Subnet.

Edit subnet associations

Available subnets (1/6)

Name	Subnet ID	Associated with	Availability zone	IPv4 CIDR	IPv6 CIDR
VPC-A-PrivateA Subnet	subnet-004dccee31876c01	acl-06270dff9797ac05f / privateSubnetACL	eu-west-1a	10.64.2.0/24	-
VPC-A-PublicA Subnet	subnet-047e59822770d6571	acl-06270dff9797ac05f / privateSubnetACL	eu-west-1a	10.64.0.0/24	-
VPC-A TGW SubnetA	subnet-02775bb3d9aeb8324	acl-071c0ef1f27ae0e14	eu-west-1a	10.64.4.0/24	-
VPC-A TGW SubnetB	subnet-08fbec6f3360b562	acl-071c0ef1f27ae0e14	eu-west-1b	10.64.5.0/24	-
VPC-A-PrivateB Subnet	subnet-0d39cab8d2296bdfa	acl-06270dff9797ac05f / privateSubnetACL	eu-west-1b	10.64.3.0/24	-
VPC-A-PublicB Subnet	subnet-0dd4a300c0e22c31d	acl-071c0ef1f27ae0e14	eu-west-1b	10.64.1.0/24	-

Selected subnets

subnet-004dccee31876c01 / VPC-A-PrivateA Subnet

Cancel Save changes

Network ACLs (1/5) Info

Name	Network ACL ID	Associated with	Default
privateSubnetACL	acl-06270dff9797ac05f	subnet-004dccee31876c01 / VPC-A-PrivateA ...	No

act-06270dff9797ac05f / privateSubnetACL

Details Inbound rules Outbound rules Subnet associations Tags

Details

Network ACL ID: acl-06270dff9797ac05f	Associated with: subnet-004dccee31876c01 / VPC-A-PrivateA Subnet	Default: No	VPC ID: vpc-0facd6045062e247e / VPC-A
Owner: 220743612060			

Zweryfikuj połączenie do maszyny. Session Manager powinien teraz być odcięty od maszyny w podsieci z nową ACL. Usługi Session Manager nie są dostępne w lokalnej sieci.

1.6 Zablokuj wyjście z podsieci prywatnej w VPC B do internetu

Dla podsieci w której jest utworzona maszyna w VPC B zmień tabelę routingu, tak by obsłużyć wyłącznie komunikację w lokalnych VPC A, B i C. Utracisz możliwość podłączenia do maszyny z Session Manager'a.

Create route table Actions

Route Table: rtb-0cab57524c3aa7054

Summary Routes Subnet Associations Edge Associations Route Propagation Tags

Destination Target Status Propagated

10.65.0.0/16	local	active	No
0.0.0.0	nat-052ace045af737ef2	active	No
10.64.0.0/16	tgw-0ecf2cf6aa110e5db	active	No
10.66.0.0/16	tgw-0ecf2cf6aa110e5db	active	No

Zweryfikuj, czy dostęp do maszyny został zablokowany.

1.7 Zablokuj wyjście z maszyny w VPC C do internetu

Dla maszyny w VPC C zmień definicję security group, tak aby ograniczyć komunikację wyłącznie do sieci z VPC A, B i C. Security groups są dostępne do modyfikacji ze strony usługi EC2, najwygodniej jest przejść do odpowiedniej przez informacje o maszynie wirtualnej EC2.

Modyfikujemy uprawnienia, tak aby ograniczyć ruch wychodzący wyłącznie do lokalnych sieci VPC-A, VPC-B i VPC-C.

Zweryfikuj efekt działania tej konfiguracji.

1.8 Skonfiguruj endpoint w VPC B dla Systems Manager

Z lewego menu na stronie usługi VPC wybierz **Endpoints** i polecenie **Create Endpoint**.

Systems Manager, aby umożliwić swoje usługi potrzebuje 4 interfejsów:

- com.amazonaws.eu-west-1.ec2
- com.amazonaws.eu-west-1.ec2messages
- com.amazonaws.eu-west-1.ssm
- com.amazonaws.eu-west-1.ssmmessages

Każdy z interfejsów utwórz w ten sam sposób wybierając:

- **VPC-B**
- Podsieć **VPC-B PrivateA Subnet**
- Security group **VPC-B-EC2-SG**

The screenshot shows the 'Create Endpoint' wizard in the AWS VPC console. The 'Service category' is set to 'AWS services'. The 'Service Name' is 'com.amazonaws.eu-west-1.ssm'. The 'VPC' dropdown shows 'vpc-0707949b47905edc'. Under 'Subnets', 'subnet-08481fc1b46ad1718' is selected, with 'eu-west-1a (euw1-az3)' checked. The 'Enable DNS name' checkbox is checked. At the bottom, there are links for 'Feedback', 'English (US)', 'Privacy Policy', 'Terms of Use', and 'Cookie preferences'.

The screenshot shows the 'Create Endpoint' page with the 'Actions' tab selected. It lists four existing endpoints:

Name	Endpoint ID	Service name	Type	Status	Creation time
vpc...	vpc-0707949b47...	com.amazonaws.eu-west-1.ec2	Interface	available	May 24, 2021 at 3:43:58 F
vpc...	vpc-0707949b47...	com.amazonaws.eu-west-1.ec2messages	Interface	available	May 24, 2021 at 3:44:21 F
vpc...	vpc-0707949b47...	com.amazonaws.eu-west-1.ssm	Interface	available	May 24, 2021 at 3:42:59 F
vpc...	vpc-0707949b47...	com.amazonaws.eu-west-1.ssmmessages	Interface	available	May 24, 2021 at 3:43:31 F

Dla security group **VPC-B-EC2-SG** ustawić możliwość odbierania komunikacji po HTTPS. Interfejsy Session Manager są wywoływanie przez agenta działającego na maszynie EC2 na porcie 443.

The screenshot shows the 'Security Groups (1/7) Info' page. It lists a single security group 'sg-0fe9bea95d84562fa - VPC-B-EC2-SG' with the following details:

- Name:** sg-0fe9bea95d84562fa
- Security group ID:** VPC-B-EC2-SG
- VPC ID:** vpc-0707949b47905edc
- Description:** Open-up ports for ICM... (partial)

Under 'Inbound rules', there is one rule:

Type	Protocol	Port range	Source	Description - optional
HTTPS	TCP	443	sg-0fe9bea95d84562fa / VPC-B-EC2-SG	-

Kiedy wszystkie 4 interfejsy będą dostępne możesz zweryfikować, czy mimo braku komunikacji z Internetem maszyna jest dostępna przez SessionManager.

1.9 Skonfiguruj endpoint w VPC B dla SNS i S3

Na takiej samej zasadzie są udostępniane dla sieci prywatnych inne usługi AWS. W tym kroku użyjemy usługi SNS i S3.

Dla usługi S3 stwórz com.amazonaws.eu-west-1.s3 gateway wskazując tablicę routowania podpiętą dla podsieci **VPC-B PrivateA Subnet**.

Zweryfikuj, czy komunikacja z usługą S3 działa:

```
aws s3 ls s3://BUCKET_NAME/
```

Session ID: MasterKey-0e8d34b99e2a089f8 Instance ID: i-05bf3663fde4908cf

sh-4.2\$ aws s3 ls s3://cf-template-01234567
2021-05-24 11:21:36 10715 networkingdemo-lab1.yml
2021-05-24 11:21:36 5777 networkingdemo-lab2-transitgateway.yml
2021-05-24 11:23:10 2579 networkingdemo-lab5-start.yml
sh-4.2\$

[Terminate](#)

Stwórz interfejs dla usługi com.amazonaws.eu-west-1.sns. Nie czekając na uaktynienie się interfejsu, przejdź do konfiguracji usługi SNS, wybierając ją w wyszukiwarce usług w konsoli AWS.

Podaj nazwę **Topic**, na który będziemy wysyłać powiadomienia i wybierz standardowy model komunikacji (nie gwarantuje kolejności dostarczenia wiadomości).

The screenshot shows the Amazon SNS console with a success message: "Topic HelloTopic created successfully. You can create subscriptions and send messages to them from this topic." The "Topics" section is selected. A new topic named "HelloTopic" is listed with the following details:

- Name: HelloTopic
- Display name: Hello World topic
- ARN: arn:aws:sns:eu-west-1:488251668476>HelloTopic
- Topic owner: 488251668476
- Type: Standard

The "Subscriptions" tab is active, showing 0 subscriptions. Other tabs include Access policy, Delivery retry policy (HTTP/S), Delivery status logging, and Encryption.

Dodaj subskrypcję na SMS lub email, tak aby odebrać faktyczne powiadomienie.

Teraz zmodyfikuj uprawnienia roli na jakiej działa maszyna EC2, tak żeby możliwe było wysłanie wiadomości poleceнием z maszyny. Na stronie usługi IAM, wybierz **Roles** i wyszukaj roli o nazwie zaczynającej się od **VPC-B**.

The screenshot shows the AWS IAM console under the Identity Access Management (IAM) service. The left sidebar shows various options like Dashboard, Access management, Users, Policies, and Roles. The Roles section is selected. A modal window titled "What are IAM roles?" is open, providing information about IAM roles and their use cases. Below the modal, a search bar shows the text "VPC-B". A table lists a single role:

Role name	Trusted entities	Last activity
VPC-B-SSMRole-eu...	AWS service: ec2	Today

Dla tej roli dodaj inline policy.

Identity and Access Management (IAM)

Role ARN: arn:aws:iam::488251668476:role/VPC-B-SSMRole-eu-west-1

Role description: Edit

Instance Profile ARNs: arn:aws:iam::488251668476:instance-profile/Lab5-VPCB1TG9YDTBZJOCW-VPCInstanceProfile-WDPGCPZVTTY0

Path: /

Creation time: 2021-05-24 13:24 UTC+0200

Last activity: 2021-05-24 15:44 UTC+0200 (Today)

Maximum session duration: 1 hour Edit

Permissions Trust relationships Tags Access Advisor Revoke sessions

Add inline policy

Policy name: AmazonEC2RoleforSSM Policy type: AWS managed policy

Permissions boundary (not set)

Generate policy based on CloudTrail events

You can generate a new policy based on the access activity for this role, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. Learn more ↗

Generate policy

No requests to generate a policy in the past 7 days.

Otworzy się wizualny edytor uprawnień. Wybierz usługę SNS, następnie jako jedyną akcję Publish.

Create policy

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more

Visual editor JSON Import managed policy

Expand all Collapse all

Select a service Select a service below Clone Remove

Service close Enter service manually

SNS

Actions Choose a service before defining actions

Resources Choose actions before applying resources

Request conditions Choose actions before specifying conditions

Add additional permissions

acter count: 39 of 10,240. current character count includes character for all inline policies in the role: VPC-B-SSMRole-eu-west-1.

Actions Specify the actions allowed in SNS

Filter actions

Manual actions (add actions)

All SNS actions (sns:*)

Access level

List Read Tagging Write (1 selected)

ConfirmSubscription DeleteTopic SetSubscriptionAttribu...

CreatePlatformApplica... OptInPhoneNumber SetTopicAttributes

CreatePlatformEndpoint Publish Subscribe

CreateTopic SetEndpointAttributes Unsubscribe

DeleteEndpoint SetPlatformApplication...

DeletePlatformApplicat... SetSMSAttributes

Permissions management

Ogranicz uprawnienia publikowania wiadomości do konkretnego zasobu podając region oraz nazwę Topic'u.

A policy defines the AWS resources using JSON. Learn more

Visual editor JSON editor

Expand all | Collapse all

SNS (1 action)

Region * eu-west-1 Any

Account * 488251668476 Any

Topic name * HelloTopic Any

topic Specify topic resource ARN for the Publish action. Add ARN to restrict access

Request conditions Specify request conditions (optional)

Add additional permissions

Cancel Add

topic Specify topic resource ARN for the Publish action. Add ARN to restrict access

Request conditions Specify request conditions (optional)

Add additional permissions

Review policy

Nadaj nazwę tej regule i ją zapisz. To zmodyfikowało uprawnienia maszyny.

Name* lab5PublishToSNS

Maximum 128 characters. Use alphanumeric and '+,-,_,-' characters.

Summary

Service Access level Resource

Allow (1 of 284 services) Show remaining 283

SNS Limited: Write TopicName | string like | HelloTopic

Required

Create policy

Identity and Access Management (IAM)

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analyzers

Settings

Credential report

Organization activity

Service control policies (SCPs)

Search IAM

AWS account ID: 488251668476

Role ARN arn:aws:iam::488251668476:role/VPC-B-SSMRole-eu-west-1

Role description Edit

Instance Profile ARNs arn:aws:iam::488251668476:instance-profile/Lab5-VPCB-1TG9YDTBZJOCW-VPCHInstanceProfile-WDPGPGCZVTYY0

Path /

Creation time 2021-05-24 13:24 UTC+0200

Last activity 2021-05-24 15:44 UTC+0200 (Today)

Maximum session duration 1 hour Edit

Permissions Trust relationships Tags Access Advisor Revoke sessions

Permissions policies (2 policies applied)

Attach policies Add inline policy

Policy name	Policy type
AmazonEC2RoleforSSM	AWS managed policy
lab5PublishToSNS	Inline policy

Permissions boundary (not set)

Generate policy based on CloudTrail events

You can generate a new policy based on the access activity for this role, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. Learn more

Generate policy

No requests to generate a policy in the past 7 days.

Sprawdź komunikację z usługą SNS wywołując polecenie po podstawieniu pod sns-topic-arn właściwego identyfikatora tematu:

```
aws sns publish --region eu-west-1 --topic-arn sns-topic-arn --message "Hello ☺"
```

```
Session ID: MasterKey-0e8d34b99e2a089f8 Instance ID: i-05bf3663fde4908cf
sh-4.2$ aws sns publish --region eu-west-1 --topic-arn arn:aws:sns:eu-west-1:488251668476>HelloTopic --message "Hello"
{
    "MessageId": "e6a76a55-f372-5144-ae46-337045c27c1c"
}
sh-4.2$
```

Usługa działa, ale naraziliśmy się na dostawanie wiadomości typu „Hello”. Teraz zmodyfikuj zakres uprawnień jaki ma interfejs SNS wystawiony w VPC-B. W zakładce Policy dla zaznaczonego interfejsu SNS wybierz **Edit Policy**. Możesz wykorzystać generator uprawnień, lub poniżej załączony szablon, który wyklucza możliwość wysłania wiadomości ze słowem „Hello” w treści.

The screenshot shows the AWS VPC Endpoints service interface. On the left, there's a sidebar with various VPC-related options like VPC Dashboard, Virtual Private Cloud, Endpoints, and Security. The main area shows a list of endpoints, with one specifically selected (vpc-0709749b47...) which has its policy being edited. The policy editor window displays a JSON template for defining IAM permissions.

Name	Endpoint	VPC ID	Service name	Endpoint type	Status	Creation time
vpc...	vpc-0709749b47...	com.amazonaws.eu-west-1.s3	Gateway	available	May 24, 2021 at 3:50:04 PM UTC	
vpc...	vpc-0709749b47...	com.amazonaws.eu-west-1.sns	Interface	available	May 24, 2021 at 4:03:40 PM UTC	
vpc...	vpc-0709749b47...	com.amazonaws.eu-west-1.ec2	Interface	available	May 24, 2021 at 3:43:58 PM UTC	
vpc...	vpc-0709749b47...	com.amazonaws.eu-west-1.ec2messages	Interface	available	May 24, 2021 at 3:44:21 PM UTC	
vpc...	vpc-0709749b47...	com.amazonaws.eu-west-1.ssm	Interface	available	May 24, 2021 at 3:42:59 PM UTC	

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sns:Publish"
            ],
            "Effect": "Deny",
            "Resource": "arn:aws:sns:eu-west-1:488251668476>HelloTopic",
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/Message": "*Hello*"
                }
            },
            "Principal": "*"
        }
    ]
}
```

Sprawdź, czy teraz wiadomość z tekstem hello nie może być wysłana.

```
sh-4.2$ aws sns publish --region eu-west-1 --topic-arn arn:aws:sns:eu-west-1:488251668476>HelloTopic --message "Hello world"
An error occurred (AuthorizationError) when calling the Publish operation: User: arn:aws:sts::488251668476:assumed-role/VPC-B-SSMRole-eu-wes
t-1/i-05bf3663fde4908cf is not authorized to perform: SNS:Publish on resource: arn:aws:sns:eu-west-1:488251668476>HelloTopic
sh-4.2$ aws sns publish --region eu-west-1 --topic-arn arn:aws:sns:eu-west-1:488251668476>HelloTopic --message "Czesc :)"
{
    "MessageId": "8d93ced3-0f61-5567-a20b-97f6c14adce8"
}
sh-4.2$
```

Ukończyłeś ćwiczenie!