Bezpieczne architektury, część 2: VPC, szyfrowanie KMS, sekrety i ochrona aplikacji

Poziom: średnio

Dotyczy: SAA-C03 domena 1, zadania 1.2 (bezpieczne obciążenia i aplikacje) i 1.3 (kontrola bezpieczeństwa danych), Amazon VPC, AWS KMS, AWS Secrets Manager, Systems Manager Parameter Store, AWS Certificate Manager, AWS WAF, AWS Shield, Amazon GuardDuty, Amazon Macie, Amazon Cognito, dni 6, 8 i 9 planu

Czas: 3 dni po 1,5 do 2 godzin

Druga część bezpiecznych architektur odpowiada na dwa pytania: którędy ruch może dojść do naszych zasobów i co się stanie, gdy ktoś dostanie dane do ręki. Opisujemy sieć VPC z grupami zabezpieczeń, listami ACL, bramami NAT i punktami końcowymi, połączenia z serwerownią, usługi ochrony aplikacji oraz szyfrowanie z KMS, certyfikaty i sekrety.

ZAŁOŻENIA SCENARIUSZA

ćwiczenia robimy w VPC laboratorium 10.60.0.0/16 ze stosu `lab-vpc` ze strony Plan 28 dni i laboratorium AWS w Zielonej. Domena `sklep.zielona.example` i tunel VPN z `fw01` (203.0.113.10) do AWS występują tylko w projekcie sklepu B2B, na papierze: laboratorium nie łączy się z siecią Zielonej.

Skróty użyte na tej stronie (27)

Skrót	Co znaczy
ACL	Access Control List: lista, kto ma jakie prawa do pliku lub zasobu
ACM	AWS Certificate Manager: usługa wydająca i odnawiająca certyfikaty TLS dla równoważników, CloudFront i API Gateway

Skrót	Co znaczy
ALB	Application Load Balancer: równoważnik AWS warstwy 7, kieruje żądania HTTP i HTTPS według ścieżki i nazwy hosta
API	Application Programming Interface: sposób, w jaki programy rozmawiają ze sobą
ARN	Amazon Resource Name: jednoznaczna nazwa zasobu AWS, na przykład arn:aws:s3:::nazwa-kubelka
AWS	Amazon Web Services: chmura Amazonu
B2B	business to business: sprzedaż i systemy skierowane do innych firm, nie do klientów indywidualnych
CLI	Command Line Interface: praca przez wpisywanie komend w terminalu
DNS	Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP
DynamoDB	baza danych typu klucz-wartość w chmurze AWS; Lore trzyma w niej fragmenty, stan, magazyn zmienny i blokady, gdy działa na AWS
EBS	Elastic Block Store: dyski blokowe maszyn wirtualnych EC2 w chmurze AWS, rozliczane osobno od maszyny
IAM	Identity and Access Management: zarządzanie tożsamościami i uprawnieniami (w AWS: użytkownicy, role, polityki)
IP	Internet Protocol: adres komputera w sieci; w elektryce: stopień ochrony obudowy (Ingress Protection)
JSON	JavaScript Object Notation: tekstowy format danych z klamrami i cudzysłowami
KMS	Key Management Service: usługa chmurowa przechowująca i zarządzająca kluczami szyfrującymi
NAT	Network Address Translation: podmiana adresów IP na granicy sieci
RDS	Remote Desktop Services: zdalne pulpity i aplikacje Windows Server
S3	Simple Storage Service: magazyn plików w chmurze AWS
SAA-C03	kod wersji egzaminu AWS Solutions Architect Associate zdawanej od 30 sierpnia 2022, aktualnej w październiku 2026
SDK	Software Development Kit: zestaw narzędzi i bibliotek do budowania programów dla jakiejś platformy, tu zależny od hosta agenta budującego
SQL	Structured Query Language: język zapytań do relacyjnych baz danych
SSE-S3	szyfrowanie po stronie serwera kluczami zarządzanymi w całości przez S3, domyślne dla nowych obiektów od 2023
SSH	Secure Shell: szyfrowane zdalne logowanie do serwera
TLS	Transport Layer Security: szyfrowanie połączeń, np. w HTTPS
VPC	Virtual Private Cloud: prywatna sieć wirtualna klienta w chmurze AWS, w której stawiamy maszyny i zakładamy tablice tras

Skrót	Co znaczy
VPN	Virtual Private Network: szyfrowany tunel do sieci firmowej
WAF	Web Application Firewall: zapora aplikacji WWW, która filtruje żądania HTTP, na przykład wstrzykiwanie SQL i zalew żądań

Fiszka

Komendy wykonujemy w CloudShell albo w bash z profilem Identity Center, w regionie `eu-central-1`. `IdVpc`, `IdPodsieci`, `IdGrupy`, `IdTablicyTras`, `IdListyAcl`, `IdKlucza`, `NazwaKubelka` i podobne zastępujemy własnymi albo odczytujemy z wyników stosu `lab-vpc`.

◫◫ ZMIENIA SYSTEM

Utworzenie grupy zabezpieczeń: aws ec2 create-security-group

```
aws ec2 create-security-group --group-name NazwaGrupy --description "Opis grupy" --vpc-id IdVpc
```

Grupa zabezpieczeń to zapora przy interfejsie sieciowym instancji. Nowa grupa nie wpuszcza nic i wypuszcza wszystko.

◫◫ **aws** = AWS CLI: narzędzie chmury Amazonu

◫◫ TYLKO ODCZYT

Otwarcie portu 443 dla internetu: aws ec2 authorize-security-group-ingress --cidr

```
aws ec2 authorize-security-group-ingress --group-id IdGrupyAlb --protocol tcp --port 443 --cidr 0.0.0.0/0
```

Tak otwieramy tylko równoważnik obciążenia, nigdy instancje aplikacji.

◫◫ **aws** = AWS CLI: narzędzie chmury Amazonu

◫◫ TYLKO ODCZYT

Wpuszczenie ruchu tylko z innej grupy: aws ec2 authorize-security-group-ingress --source-group

```
aws ec2 authorize-security-group-ingress --group-id IdGrupyAplikacji --protocol tcp --port 8080 --source-group IdGrupyAlb
```

Reguła wskazuje grupę, a nie adresy: wpuszcza wszystko, co ma przypiętą grupę równoważnika, niezależnie od adresu IP. To wzorzec warstw ALB, aplikacja, baza, o który egzamin pyta najczęściej.

IP = Internet Protocol: adres komputera w sieci; w elektryce: stopień ochrony obudowy (Ingress Protection) · **ALB** = Application Load Balancer: równoważnik AWS warstwy 7, kieruje żądania HTTP i HTTPS według ścieżki i nazwy hosta · **aws** = AWS CLI: narzędzie chmury Amazonu

ZMIENIA SYSTEM

Dodanie reguły do sieciowej listy ACL: aws ec2 create-network-acl-entry

```
aws ec2 create-network-acl-entry --network-acl-id IdListyAcl --ingress --rule-number 90 --protocol tcp --port-range From=22,To=22 --cidr-block 203.0.113.200/32 --rule-action deny
```

Lista ACL działa na całą podsieć, jest bezstanowa i czyta reguły od najniższego numeru do pierwszego trafienia. Ten przykład blokuje SSH z jednego adresu przed regułami, które ruch dopuszczają.

ACL = Access Control List: lista, kto ma jakie prawa do pliku lub zasobu · **SSH** = Secure Shell: szyfrowane zdalne logowanie do serwera · **aws** = AWS CLI: narzędzie chmury Amazonu

ZMIENIA SYSTEM

Utworzenie punktu końcowego bramy dla S3: aws ec2 create-vpc-endpoint --vpc-endpoint-type Gateway

```
aws ec2 create-vpc-endpoint --vpc-id IdVpc --vpc-endpoint-type Gateway --service-name com.amazonaws.eu-central-1.s3 --route-table-ids IdTablicyTras
```

Dopisuje do tablicy tras trasę do S3 przez sieć AWS, bez bramy NAT i internetu. Punkt końcowy bramy istnieje tylko dla S3 i DynamoDB i jest bezpłatny.

S3 = Simple Storage Service: magazyn plików w chmurze AWS · **AWS** = Amazon Web Services: chmura Amazonu · **NAT** = Network Address Translation: podmiana adresów IP na granicy sieci · **DynamoDB** = baza danych typu klucz-wartość w chmurze AWS; Lore trzyma w niej fragmenty, stan, magazyn zmienny i blokady, gdy działa na AWS · **aws** = AWS CLI: narzędzie chmury Amazonu

ZMIENIA SYSTEM

Utworzenie punktu końcowego interfejsu: aws ec2 create-vpc-endpoint --vpc-endpoint-type Interface

```
aws ec2 create-vpc-endpoint --vpc-id IdVpc --vpc-endpoint-type Interface --service-name com.amazonaws.eu-central-1.secretsmanager --subnet-ids IdPodsieciA IdPodsieciB --security-group-ids IdGrupy --private-dns-enabled
```

Tworzy interfejsy sieciowe w podsieciach (AWS PrivateLink), płatne za godzinę i za gigabajt. Z `--private-dns-enabled` zwykła nazwa usługi wskazuje prywatny adres w VPC, więc aplikacja nie wymaga zmian.

AWS = Amazon Web Services: chmura Amazonu · **VPC** = Virtual Private Cloud: prywatna sieć wirtualna klienta w chmurze AWS, w której stawiamy maszyny i zakładamy tablice tras · **aws** = AWS CLI: narzędzie chmury Amazonu

ZMIENIA SYSTEM

Włączenie dzienników ruchu odrzuconego w VPC: aws ec2 create-flow-logs

```
aws ec2 create-flow-logs --resource-type VPC --resource-ids IdVpc --traffic-type REJECT --log-destination-type cloud-watch-logs --log-group-name NazwaGrupyLogow --deliver-logs-permission-arn ArnRoli
```

VPC Flow Logs zapisują metadane połączeń (adresy, porty, decyzja), bez treści pakietów. Z `--log-destination-type s3` i `--log-destination` z ARN kubełka rola nie jest potrzebna.

VPC = Virtual Private Cloud: prywatna sieć wirtualna klienta w chmurze AWS, w której stawiamy maszyny i zakładamy tablice tras · **ARN** = Amazon Resource Name: jednoznaczna nazwa zasobu AWS, na przykład arn:aws:s3:::nazwa-kubelka · **aws** = AWS CLI: narzędzie chmury Amazonu

ZMIENIA SYSTEM

Utworzenie strefowej bramy NAT: aws ec2 create-nat-gateway --subnet-id

```
aws ec2 create-nat-gateway --subnet-id IdPodsieciPublicznej --allocation-id
IdAdresuElastic
```

Brama strefowa stoi w podsieci publicznej jednej strefy. Odporny układ to brama w każdej strefie i osobna tablica tras dla podsieci prywatnych każdej strefy.

NAT = Network Address Translation: podmiana adresów IP na granicy sieci · **aws** = AWS CLI: narzędzie chmury Amazonu

ZMIENIA SYSTEM

Utworzenie regionalnej bramy NAT: aws ec2 create-nat-gateway --availability-mode regional

```
aws ec2 create-nat-gateway --vpc-id IdVpc --availability-mode regional
```

Tryb regionalny, dostępny od listopada 2025 roku, nie potrzebuje podsieci publicznej i sam rozszerza się na strefy, w których pojawiają się zasoby (według dokumentacji do 60 minut). Nie obsługuje prywatnego NAT. Przewodnik SAA-C03 jest starszy, więc na egzaminie wzorcem pozostaje brama strefowa w każdej strefie.

NAT = Network Address Translation: podmiana adresów IP na granicy sieci · **SAA-C03** = kod wersji egzaminu AWS Solutions Architect Associate zdawanej od 30 sierpnia 2022, aktualnej w październiku 2026 · **aws** = AWS CLI: narzędzie chmury Amazonu

ZMIENIA SYSTEM

Utworzenie klucza KMS zarządzanego przez klienta: aws kms create-key

```
aws kms create-key --description "Dane sklepu, laboratorium"
aws kms create-alias --alias-name alias/lab-dane --target-key-id IdKlucza
```

Alias to wygodna nazwa, której używamy w innych usługach zamiast identyfikatora. Klucz bez polityki podanej w poleceniu dostaje politykę domyślną, która oddaje kontrolę kontu przez IAM.

KMS = Key Management Service: usługa chmurowa przechowująca i zarządzająca kluczami szyfrującymi · **IAM** = Identity and Access Management: zarządzanie tożsamościami i uprawnieniami

(w AWS: użytkownicy, role, polityki) · **aws** = AWS CLI: narzędzie chmury Amazonu

ZMIENIA SYSTEM

Włączenie automatycznej rotacji klucza: aws kms enable-key-rotation

```
aws kms enable-key-rotation --key-id IdKlucza --rotation-period-in-days 365
aws kms get-key-rotation-status --key-id IdKlucza
```

Rotacja tworzy nowy materiał klucza, a stare zostają do odszyfrowania wcześniejszych danych, więc nic nie trzeba przeszyfrowywać. Okres podajemy w dniach, zakres sprawdzamy w dokumentacji KMS.

KMS = Key Management Service: usługa chmurowa przechowująca i zarządzająca kluczami szyfrującymi · **aws** = AWS CLI: narzędzie chmury Amazonu

TYLKO ODCZYT

Domyślne szyfrowanie kubełka kluczem KMS: aws s3api put-bucket-encryption

```
aws s3api put-bucket-encryption --bucket NazwaKubelka --server-side-encryption-configuration '{"Rules":[{"ApplyServerSideEncryptionByDefault":{"SSEAlgorithm":"aws:kms","KMSMasterKeyID":"alias/lab-dane"},"BucketKeyEnabled":true}]}'
```

Od stycznia 2023 roku każdy nowy obiekt w S3 jest szyfrowany co najmniej SSE-S3. Klucz KMS dokładamy, gdy chcemy decydować, kto może odszyfrować, i widzieć użycie klucza w CloudTrail. Klucz kubełka (`BucketKeyEnabled`) zmniejsza liczbę wywołań KMS i ich koszt.

KMS = Key Management Service: usługa chmurowa przechowująca i zarządzająca kluczami szyfrującymi · **S3** = Simple Storage Service: magazyn plików w chmurze AWS · **SSE-S3** = szyfrowanie po stronie serwera kluczami zarządzanymi w całości przez S3, domyślne dla nowych obiektów od 2023 · **aws** = AWS CLI: narzędzie chmury Amazonu

ZMIENIA SYSTEM

Domyślne szyfrowanie nowych dysków EBS w regionie: aws ec2 enable-ebs-encryption-by-default

```
aws ec2 enable-ebs-encryption-by-default
aws ec2 get-ebs-encryption-by-default
```

Ustawienie dotyczy konta i regionu. Istniejących dysków nie zmienia: niezaszyfrowany dysk szyfrujemy przez migawkę skopiowaną z szyfrowaniem.

EBS = Elastic Block Store: dyski blokowe maszyn wirtualnych EC2 w chmurze AWS, rozliczane osobno od maszyny · **aws** = AWS CLI: narzędzie chmury Amazonu

ZMIENIA SYSTEM

Zapisanie sekretu bazy: aws secretsmanager create-secret

```
aws secretsmanager create-secret --name lab/sklep/baza --secret-string file://sekret-bazy.json
```

Plik zawiera JSON z polami `username` i `password`, a po wgraniu usuwamy go z dysku. Secrets Manager szyfruje sekret kluczem KMS i umie go rotować funkcją Lambda.

JSON = JavaScript Object Notation: tekstowy format danych z klamrami i cudzysłowami · **KMS** = Key Management Service: usługa chmurowa przechowująca i zarządzająca kluczami szyfrującymi · **aws** = AWS CLI: narzędzie chmury Amazonu

TYLKO ODCZYT

Odczyt sekretu przez aplikację: aws secretsmanager get-secret-value

```
aws secretsmanager get-secret-value --secret-id lab/sklep/baza --query SecretString --output text
```

Aplikacja robi to samo przez SDK, z rolą instancji. W kodzie i w plikach konfiguracyjnych nie ma hasła.

SDK = Software Development Kit: zestaw narzędzi i bibliotek do budowania programów dla jakiejś platformy, tu zależny od hosta agenta budującego · **aws** = AWS CLI: narzędzie chmury Amazonu

TYLKO ODCZYT

Zapisanie parametru zaszyfrowanego: aws ssm put-parameter --type SecureString

```
aws ssm put-parameter --name /lab/sklep/adres-api --type SecureString --value
"WartoscParametru"
aws ssm get-parameter --name /lab/sklep/adres-api --with-decryption
```

Parameter Store w warstwie standardowej jest bezpłatny i dobry do konfiguracji, ale nie ma wbudowanej rotacji sekretów, którą ma Secrets Manager.

aws = AWS CLI: narzędzie chmury Amazonu

TYLKO ODCZYT

Zamówienie publicznego certyfikatu TLS: aws acm request-certificate

```
aws acm request-certificate --domain-name sklep.zielona.example --validation-method DNS
--subject-alternative-names www.sklep.zielona.example
```

Certyfikaty publiczne ACM są bezpłatne i odnawiają się same, dopóki rekord walidacji DNS istnieje. Działają tylko w usługach AWS (ALB, CloudFront, API Gateway). Dla CloudFront certyfikat musi być w regionie `us-east-1`.

TLS = Transport Layer Security: szyfrowanie połączeń, np. w HTTPS · **ACM** = AWS Certificate Manager: usługa wydająca i odnawiająca certyfikaty TLS dla równoważników, CloudFront i API Gateway · **DNS** = Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP · **AWS** = Amazon Web Services: chmura Amazonu · **ALB** = Application Load Balancer: równoważnik AWS warstwy 7, kieruje żądania HTTP i HTTPS według ścieżki i nazwy hosta · **API** = Application Programming Interface: sposób, w jaki programy rozmawiają ze sobą · **aws** = AWS CLI: narzędzie chmury Amazonu

ZMIENIA SYSTEM

Włączenie wykrywania zagrożeń: aws guardduty create-detector

```
aws guardduty create-detector --enable
```

GuardDuty analizuje dzienniki CloudTrail, VPC Flow Logs i zapytania DNS i zgłasza podejrzane zachowania, na przykład kopanie kryptowalut albo logowanie z nietypowych miejsc. Nie wymaga agentów.

VPC = Virtual Private Cloud: prywatna sieć wirtualna klienta w chmurze AWS, w której stawiamy maszyny i zakładamy tablice tras · **DNS** = Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP · **aws** = AWS CLI: narzędzie chmury Amazonu

ZMIENIA SYSTEM

Ścieżka w konsoli: AWS WAF przed równoważnikiem

```
Konsola AWS → WAF & Shield → Web ACLs → Create web ACL
Resource type: Regional resources, Region: Europe (Frankfurt)
Associated AWS resources → Add → Application Load Balancer: alb-sklep
Rules → Add managed rule groups → AWS managed rule groups → Core rule set, SQL database
Rules → Add my own rules → Rate-based rule: 2000 requests per 5 minutes per IP
```

ZRZUT EKRANU DO UZUPEŁNIENIA

Zrzut do uzupełnienia: ekran WAF & Shield → Web ACLs → web ACL laboratorium, zakładka Rules, widoczne grupy reguł Core rule set i SQL database oraz reguła limitu żądań, a w zakładce Associated AWS resources równoważnik `alb-sklep`.

AWS = Amazon Web Services: chmura Amazonu · **WAF** = Web Application Firewall: zapora aplikacji WWW, która filtruje żądania HTTP, na przykład wstrzykiwanie SQL i zalew żądań · **ACL** = Access Control List: lista, kto ma jakie prawa do pliku lub zasobu · **SQL** = Structured Query Language: język zapytań do relacyjnych baz danych

Z życia wzięte

Z ŻYCIA WZIĘTE

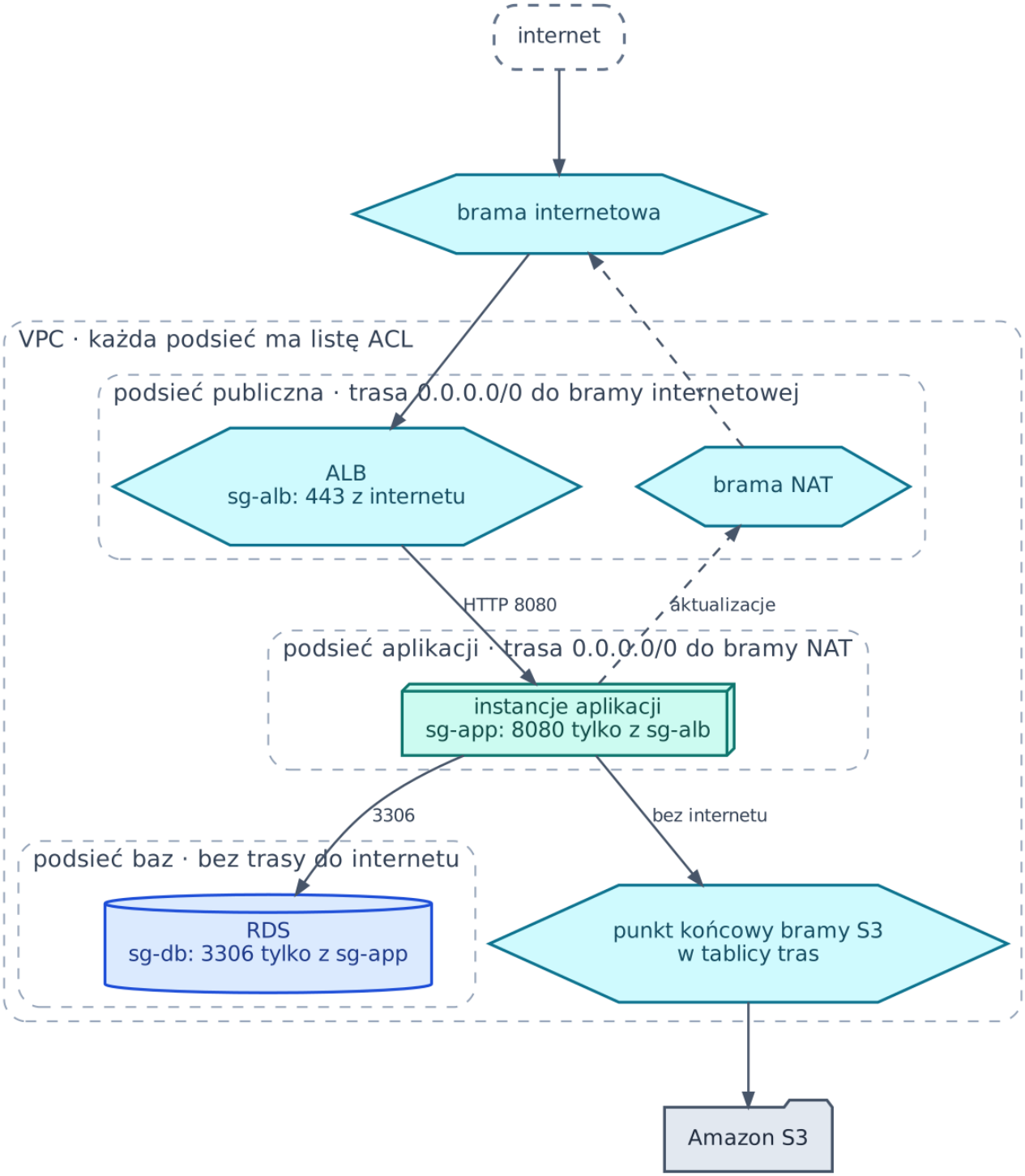
Wtorek, 15:10. Tomek stawia w laboratorium bazę w podsieci `db-a` i nie może się z nią połączyć z instancji w `app-a`. W grupie zabezpieczeń bazy wpisał adres instancji, potem całą podsieć, a połączenia dalej nie ma. Ola patrzy na listę ACL podsieci baz, którą Tomek dzień wcześniej „uszczelnił”, i widzi, że wpuszcza port 3306, ale nie wypuszcza odpowiedzi na porty efemeryczne. Tomek dopisuje regułę wyjściową 1024 do 65535 i zapisuje w dzienniku: grupa pamięta połączenia, lista ACL nie.

Jak to działa

Rozwiń: jak to działa pod spodem

Warstwy sieci w VPC

Ruch z internetu do aplikacji przechodzi przez bramę internetową, tablicę tras podsieci publicznej, listę ACL podsieci i grupę zabezpieczeń równoważnika, a dalej przez te same elementy w podsieci aplikacji. Każda warstwa może go zatrzymać, a diagnozę zaczynamy od tablicy tras.



Rysunek 1. Warstwy ochrony w VPC: brama internetowa, podsieć publiczna z ALB, podsieć aplikacji za grupą zabezpieczeń, podsieć baz bez trasy do internetu, brama NAT do aktualizacji i punkt końcowy bramy do S3 (kliknięcie otwiera pełny rozmiar)

Pojęcie: podsieć publiczna. Podsieć, której tablica tras ma trasę `0.0.0.0/0` do bramy internetowej. Instancja w niej jest osiągalna z internetu tylko wtedy, gdy ma też publiczny adres i grupa zabezpieczeń ją wpuszcza.

Pojęcie: brama NAT. Usługa, która pozwala instancjom w podsieciach prywatnych wychodzić do internetu (aktualizacje, wywołania API), ale nie pozwala nikomu z internetu nawiązać połączenia do nich.

Cecha	Grupa zabezpieczeń	Sieciowa lista ACL
Działa na	interfejs sieciowy (instancja, ALB, baza)	podsieć
Stan	stanowa: odpowiedź wraca sama	bezstanowa: odpowiedź potrzebuje reguły wyjściowej na porty efemeryczne
Reguły	tylko pozwolenia	pozwolenia i odmowy, numerowane
Ocena	wszystkie reguły naraz	od najniższego numeru do pierwszego trafienia
Odwołanie do innej grupy	tak	nie, tylko zakresy adresów
Kiedy na egzaminie	domyślna ochrona każdej warstwy	zablokowanie konkretnego adresu albo zakresu dla całej podsieci

Połączenia z serwerownią i między sieciami

Potrzeba	Usługa	Cecha do zapamiętania
Szybkie, szyfrowane połączenie przez internet	AWS Site-to-Site VPN	dwa tunele IPsec do bramy VPN albo Transit Gateway, gotowe w godzinę
Stała przepustowość, przewidywalne opóźnienie	AWS Direct Connect	łącze dzierżawione do punktu AWS, tygodnie na uruchomienie, bez szyfrowania z definicji (szyfrujemy VPN przez Direct Connect albo MACsec)
Zapasowe łącze dla Direct Connect	Site-to-Site VPN	najtańszy zapas
Połączenie dwóch VPC	VPC peering	bez przechodniości: A z B i B z C nie daje A z C
Wiele VPC i serwerownia w gwiazdę	AWS Transit Gateway	węzeł centralny z tablicami tras

Potrzeba	Usługa	Cecha do zapamiętania
Udostępnienie jednej usługi innemu VPC bez otwierania sieci	AWS PrivateLink	punkt końcowy interfejsu po stronie klienta
Dostęp administratorów do instancji bez SSH z internetu	Systems Manager Session Manager	bez otwartego portu 22 i bez bastionu

Ochrona aplikacji

Zagrożenie albo potrzeba	Usługa
Wstrzykiwanie SQL, skrypty w formularzach, boty, limit żądań z adresu	AWS WAF na ALB, CloudFront, API Gateway albo AppSync
Atak DDoS na warstwy sieciową i transportową	AWS Shield Standard, bezpłatny i zawsze włączony
DDoS z zespołem reagowania AWS i ochroną kosztów	AWS Shield Advanced
Wykrywanie zagrożeń na podstawie dzienników	Amazon GuardDuty
Dane osobowe w kubełkach S3	Amazon Macie
Podatności w instancjach, obrazach kontenerów i funkcjach Lambda	Amazon Inspector
Logowanie klientów aplikacji WWW i mobilnej	Amazon Cognito (pule użytkowników i pule tożsamości)
Zbiorczy widok ustaleń bezpieczeństwa	AWS Security Hub

Szyfrowanie i klucze

Pojęcie: AWS KMS (Key Management Service). Usługa, która przechowuje klucze szyfrujące w sprzętowych modułach bezpieczeństwa i wykonuje nimi operacje na nasze żądanie. Klucz nigdy nie opuszcza KMS w postaci jawnej, a każde użycie jest zapisane w CloudTrail.

Pojęcie: szyfrowanie kopertowe. Dane szyfruje klucz danych wygenerowany przez KMS, a klucz danych szyfruje klucz KMS. Duże pliki nie wędrują do KMS, idzie tam tylko mały klucz danych.

Rodzaj klucza	Kto zarządza	Polityka i rotacja	Kiedy na egzaminie
klucz należący do AWS	AWS, niewidoczny w koncie	brak wpływu	domyślne szyfrowanie bez wymagań

Rodzaj klucza	Kto zarządza	Polityka i rotacja	Kiedy na egzaminie
klucz zarządzany przez AWS (`aws/s3`, `aws/rds`)	AWS w naszym koncie	rotacja automatyczna, polityki nie zmienimy	szyfrowanie z audytem, bez własnej kontroli dostępu
klucz zarządzany przez klienta	my	własna polityka klucza, rotacja do włączenia	kontrola, kto może odszyfrować, współdzielenie z innym kontem, wyłączenie klucza na żądanie
AWS CloudHSM	my, moduł sprzętowy na wyłączność	pełna kontrola	wymóg dedykowanego modułu (FIPS 140 na najwyższym poziomie, własne klucze poza AWS)

Szyfrowanie bazy RDS i dysku EBS włączamy przy tworzeniu. Nie da się zaszyfrować istniejącej instancji bazy w miejscu: robimy migawkę, kopiujemy ją z szyfrowaniem i odtwarzamy nową instancję. Szyfrowanie w ruchu zapewnia TLS z certyfikatem z ACM na ALB albo CloudFront, a dla baz wymuszamy połączenia TLS parametrem silnika.

Pułapki egzaminacyjne

- Baza ma być niedostępna z internetu: podsieć bez trasy do bramy internetowej i grupa wpuszczająca tylko grupę aplikacji. Sama prywatna podsieć bez reguł grupy nie wystarcza do pełnej odpowiedzi.
- Instancje prywatne pobierają dużo danych z S3: punkt końcowy bramy, a nie brama NAT (taniej i bez internetu).
- Zablokować jeden złośliwy adres IP: lista ACL albo reguła WAF. Grupa zabezpieczeń nie ma reguł odmowy.
- Hasło do bazy z rotacją co 30 dni: Secrets Manager. Parameter Store nie rotuje sam.
- Certyfikat dla CloudFront: ACM w `us-east-1`, niezależnie od regionu aplikacji.
- Obiekty w S3 mają być niemożliwe do usunięcia przez określony czas: S3 Object Lock, opisany na stronie Zimne archiwum w chmurze: Azure Blob Storage i Amazon S3 Glacier.
- Dostęp administratorów bez otwierania portu 22: Session Manager, a nie bastion z publicznym adresem.
- Szyfrowanie z możliwością natychmiastowego odcięcia dostępu do danych: klucz zarządzany przez klienta, który można wyłączyć.

Częste błędy

Objaw	Przyczyna	Co robimy
Połączenie z bazą wisi mimo reguły w grupie	lista ACL nie wypuszcza odpowiedzi na porty efemeryczne	reguła wyjściowa 1024 do 65535 w liście ACL albo domyślna lista ACL
Instancja w podsieci prywatnej nie pobiera aktualizacji	brak bramy NAT albo trasy w tablicy podsieci	trasa `0.0.0.0/0` do bramy NAT w tablicy tej podsieci
Instancja ma publiczny adres, a nie odpowiada z internetu	podsieć nie ma trasy do bramy internetowej albo grupa nie wpuszcza portu	tablica tras, potem grupa
Punkt końcowy interfejsu działa, ale aplikacja nadal idzie przez NAT	brak prywatnego DNS albo VPC bez `enableDnsHostnames`	`--private-dns-enabled` i ustawienia DNS VPC
`AccessDenied` przy odczycie zaszyfrowanego obiektu S3	rola ma `s3:GetObject`, ale nie `kms:Decrypt` na kluczu	uprawnienie w polityce klucza albo w IAM, gdy polityka klucza oddaje kontrolę kontu
Certyfikat ACM nie pojawia się w CloudFront	certyfikat w innym regionie niż `us-east-1`	nowy certyfikat w `us-east-1`

□□ Ćwiczenia

1. Dzień 6. W VPC laboratorium tworzymy trzy grupy: `sg-alb` (443 z internetu), `sg-app` (8080 tylko z `sg-alb`) i `sg-db` (3306 tylko z `sg-app`). Jakie polecenia?

Odpowiedź

```
alb=$(aws ec2 create-security-group --group-name sg-alb --description "ALB sklepu" --vpc-id IdVpc --query GroupId --output text)
app=$(aws ec2 create-security-group --group-name sg-app --description "Aplikacja sklepu" --vpc-id IdVpc --query GroupId --output text)
db=$(aws ec2 create-security-group --group-name sg-db --description "Baza sklepu" --vpc-id IdVpc --query GroupId --output text)
aws ec2 authorize-security-group-ingress --group-id "$alb" --protocol tcp --port 443 --cidr 0.0.0.0/0
aws ec2 authorize-security-group-ingress --group-id "$app" --protocol tcp --port 8080 --source-group "$alb"
aws ec2 authorize-security-group-ingress --group-id "$db" --protocol tcp --port 3306 --source-group "$app"
```

Grupy usuwamy przed usunięciem stosu, bo stos nie wie o zasobach dodanych ręcznie, a VPC z grupami spoza stosu nie da się usunąć.

1. Dzień 8. Mierzymy różnicę: z instancji w `app-a` bez bramy NAT próbujemy `aws s3 ls`, potem dodajemy punkt końcowy bramy S3 do tablicy tras prywatnych i powtarzamy. Co się zmienia i dlaczego?

Odpowiedź

Bez bramy NAT i bez punktu końcowego polecenie wisi i kończy się przekroczeniem czasu, bo instancja nie ma drogi do publicznego punktu końcowego S3. Po dodaniu punktu końcowego bramy tablica tras dostaje trasę do listy prefiksów S3 i polecenie działa, mimo braku internetu. Instancja potrzebuje jeszcze roli z uprawnieniem `s3:ListAllMyBuckets`.

1. Dzień 9. Tworzymy klucz `alias/lab-dane`, włączamy rotację, ustawiamy go jako domyślne szyfrowanie kubełka laboratorium i wgrywamy plik. Jak sprawdzić, którym kluczem obiekt jest zaszyfrowany?

Odpowiedź

```
aws s3 cp test.txt s3://NazwaKubelka/test.txt
aws s3api head-object --bucket NazwaKubelka --key test.txt --query
"[ServerSideEncryption,SSEKMSKeyId]"
```

Wynik zawiera `aws:kms` i ARN klucza. Klucza KMS nie da się usunąć od razu: `aws kms schedule-key-deletion --key-id IdKlucza --pending-window-in-days 7` planuje usunięcie z okresem oczekiwania od 7 do 30 dni, a dane zaszyfrowane tym kluczem po jego usunięciu są nie do odzyskania.

1. Pytanie w stylu egzaminu: aplikacja w podsieciach prywatnych trzech stref ma wychodzić do internetu, a awaria jednej strefy nie może odciąć pozostałych. Co jest odpowiedzią?

Odpowiedź

Brama NAT w podsieci publicznej każdej strefy i osobna tablica tras dla podsieci prywatnych każdej strefy, wskazująca bramę z tej samej strefy. Jedna brama NAT to pojedynczy punkt awarii i ruch między strefami. W dzisiejszym AWS ten sam cel daje regionalna brama NAT, ale na egzaminie zgodnym z przewodnikiem z 2022 roku spodziewamy się wariantu strefowego.

1. Pytanie w stylu egzaminu: firma chce połączyć serwerownię z AWS w ciągu tygodnia, a za pół roku przejść na łącze o stałej przepustowości. Co wybiera teraz, a co później, i jaki będzie zapas?

Odpowiedź

Teraz Site-to-Site VPN, bo działa w godzinę przez istniejący internet. Później Direct Connect, którego uruchomienie trwa tygodnie, a VPN zostaje jako zapasowe łącze. Gdy wymagane jest szyfrowanie na Direct Connect, dokładamy VPN przez Direct Connect albo MACsec.

Krok projektu: sklep B2B

Sklep dostaje w koncie `sklep-prod` VPC 10.61.0.0/16 (osobne od laboratorium) z trzema warstwami podsieci w trzech strefach, grupy `sg-alb`, `sg-app`, `sg-db`, punkt końcowy bramy S3 i punkty końcowe interfejsu do Secrets Manager. Przed ALB stoi AWS WAF z regułami zarządzanymi i limitem żądań, certyfikat `sklep.zielona.example` pochodzi z ACM. Baza i kubełek ze zdjęciami są szyfrowane kluczem zarządzanym przez klienta, a hasło bazy leży w Secrets Manager z rotacją. Połączenie z `fw01` do synchronizacji z systemem magazynowym na `ora01` to Site-to-Site VPN, a jego konfigurację po stronie FortiGate opisuje strona IPsec site-to-site: Pamiątkowo i Swarzędz między FortiGate a routerem innej firmy.

Powiązane: Bezpieczne architektury, część 1: IAM, role, organizacje i SCP · Odporne architektury, część 1: strefy, ELB, Auto Scaling, Route 53 i luźne powiązania · S3: kubełki, obiekty, uprawnienia

Źródła: przewodnik SAA-C03, domena 1, zadania 1.2 i 1.3; dokumentacja Amazon VPC (grupy zabezpieczeń, listy ACL, punkty końcowe, Flow Logs, bramy NAT, regionalne bramy NAT z listopada 2025); dokumentacja AWS KMS (rodzaje kluczy, rotacja, usuwanie); dokumentacja Amazon S3 (domyślne szyfrowanie od stycznia 2023, klucze kubełka); dokumentacja AWS Secrets Manager, Systems Manager Parameter Store, AWS Certificate Manager, AWS WAF, AWS Shield, Amazon GuardDuty. Parametry poleceń sprawdzone z modelem usług AWS CLI (botocore 1.43) 19 października 2026.

Revision #3
Created 2026-10-18 23:00:35 UTC by Tomasz Konieczny
Updated 2026-10-26 14:27:32 UTC by Tomasz Konieczny