Sieć: VNet, peering, trasy, NSG, Bastion, prywatne punkty końcowe, DNS i Load Balancer

Poziom: średnio

Dotyczy: AZ-104, domena „Implement and manage virtual networking” (15 do 20%), Azure Virtual Network, NSG i ASG, trasy definiowane przez użytkownika, Azure Bastion, punkty końcowe usług i prywatne, Azure DNS, Azure Load Balancer, Network Watcher, Azure CLI 2.91, moduł Az

Czas: 4 dni po 1,5 do 2 godzin

Dni 18 do 21 programu: sieci wirtualne i podsieci, peering, publiczne adresy i trasy UDR, grupy zabezpieczeń sieci z grupami zabezpieczeń aplikacji, Bastion, punkty końcowe usług i prywatne, strefy DNS, równoważenie obciążenia i diagnostyka Network Watcher. Wracamy tu przy każdym pytaniu „dlaczego ta maszyna nie widzi tamtej”.

ZAŁOŻENIA SCENARIUSZA

sieć laboratorium z pliku `lab-siec.bicep` (hub 10.32.0.0/20, app 10.32.16.0/20, dane 10.32.32.0/20) w grupie `rg-lab-siec`, maszyny z dni 13 i 15 w `rg-lab-obliczenia`. Laboratorium nie ma tunelu do Zielonej: połączenie Azure z serwerownią przez IPsec opisuje strona Łącza operatora: światłowód, radiolinia, LTE i 5G oraz przełączanie na FortiGate, gdzie produkcyjny `edge-az01` (10.30.0.4) zestawia tunele z `fw01`. Strefa publiczna `azlab.zielona.example` w Azure DNS jest fikcyjna i nie zostanie delegowana.

Skróty użyte na tej stronie (22)

Skrót	Co znaczy
API	Application Programming Interface: sposób, w jaki programy rozmawiają ze sobą

Skrót	Co znaczy
ASG	Application Security Group: grupa zabezpieczeń aplikacji w Azure, etykieta nadawana kartom sieciowym maszyn, używana w regułach NSG zamiast adresów IP
AZ-104	numer egzaminu Microsoft Azure Administrator: egzamin, którego zdanie daje certyfikat Microsoft Certified: Azure Administrator Associate, ważny rok i odnawiany bezpłatną oceną online
CLI	Command Line Interface: praca przez wpisywanie komend w terminalu
DNS	Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP
HTTP	Hypertext Transfer Protocol: protokół stron WWW
HTTPS	HTTP zabezpieczony szyfrowaniem TLS
IP	Internet Protocol: adres komputera w sieci; w elektryce: stopień ochrony obudowy (Ingress Protection)
IPsec	Internet Protocol Security: zestaw protokołów szyfrujących i uwierzytelniających ruch sieciowy, na nim stoi tunel VPN typu IKEv2
NAT	Network Address Translation: podmiana adresów IP na granicy sieci
NSG	Network Security Group: grupa zabezpieczeń sieci w Azure, lista reguł przepuszczających albo blokujących ruch do podsieci i kart sieciowych maszyn
NVA	Network Virtual Appliance: wirtualne urządzenie sieciowe, czyli maszyna pełniąca rolę routera albo zapory, przez którą trasy UDR kierują ruch
PaaS	Platform as a Service: chmura dająca gotową platformę, np. bazę danych, bez zarządzania serwerem
RDP	Remote Desktop Protocol: protokół pulpitu zdalnego Windows, uruchamiany poleceniem mstsc
SSH	Secure Shell: szyfrowane zdalne logowanie do serwera
TCP	Transmission Control Protocol: protokół sieciowy z potwierdzaniem dostarczenia
TLS	Transport Layer Security: szyfrowanie połączeń, np. w HTTPS
UDP	User Datagram Protocol: szybki protokół sieciowy bez potwierdzeń
UDR	User-Defined Route: trasa definiowana przez użytkownika w tabeli tras Azure, która zmienia domyślną drogę ruchu z podsieci, na przykład przez zaporę
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
WWW	World Wide Web: strony i aplikacje otwierane w przeglądarce po HTTP albo HTTPS

Fiszka

Komendy wykonujemy po `az account set --subscription zielona-lab`. Gdy sieć leży w innej grupie zasobów niż zasób, który do niej podłączamy, podajemy pełny identyfikator sieci albo podsieci. Parametry sprawdziliśmy w pomocy Azure CLI 2.91.0, w dokumentacji rozszerzenia `bastion` i w dokumentacji modułu Az (19 października 2026).

◫◫ ZMIENIA SYSTEM

Utworzenie sieci wirtualnej z podsiecią: az network vnet create

```
az network vnet create --resource-group rg-lab-siec --name vnet-lab-test --address-prefixes 10.32.48.0/20 \
  --subnet-name snet-test --subnet-prefixes 10.32.48.0/24
```

Sieć do ćwiczeń poza plikiem Bicep, w wolnym zakresie 10.32.48.0/20. W PowerShell: `New-AzVirtualNetwork -Name vnet-lab-test -ResourceGroupName rg-lab-siec -Location polandcentral -AddressPrefix 10.32.48.0/20 -Subnet $podsiec`, gdzie `$podsiec` tworzy `New-AzVirtualNetworkSubnetConfig -Name snet-test -AddressPrefix 10.32.48.0/24`.

◫◫ **az** = Azure CLI: narzędzie chmury Microsoftu

◫◫ ZMIENIA SYSTEM

Dodanie podsieci do istniejącej sieci: az network vnet subnet create

```
az network vnet subnet create --resource-group rg-lab-siec --vnet-name vnet-lab-test --name snet-test2 --address-prefixes 10.32.49.0/24
```

Azure rezerwuje w każdej podsieci pięć adresów: sieć, trzy pierwsze adresy (brama i DNS Azure) i rozgłoszeniowy. W podsieci /24 zostaje więc 251 adresów dla maszyn.

◫◫ **DNS** = Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP ·**az** = Azure CLI: narzędzie chmury Microsoftu

◫◫ ZMIENIA SYSTEM

Utworzenie peeringu w obie strony: az network vnet peering create

```
az network vnet peering create --resource-group rg-lab-siec --name test-do-hub --vnet-name vnet-lab-test \
  --remote-vnet vnet-lab-hub --allow-vnet-access --allow-forwarded-traffic
az network vnet peering create --resource-group rg-lab-siec --name hub-do-test --vnet-name vnet-lab-hub \
```

```
  --remote-vnet vnet-lab-test --allow-vnet-access --allow-forwarded-traffic
```

Peering tworzymy z obu stron, dopiero wtedy ma stan Connected. Sieć w innej grupie albo subskrypcji podajemy w `--remote-vnet` pełnym identyfikatorem. W PowerShell: `Add-AzVirtualNetworkPeering -Name test-do-hub -VirtualNetwork $vnetTest -RemoteVirtualNetworkId $vnetHub.Id -AllowForwardedTraffic`.

az = Azure CLI: narzędzie chmury Microsoftu

ZMIENIA SYSTEM

Utworzenie publicznego adresu strefowo nadmiarowego: az network public-ip create

```
az network public-ip create --resource-group rg-lab-siec --name pip-lab-lb --sku Standard --allocation-method Static --zone 1 2 3
```

Adres w wersji Standard jest zawsze statyczny, a wersję Basic Microsoft wycofał 30 września 2025 roku (strona o łączach operatora). Trzy strefy oznaczają adres strefowo nadmiarowy. W PowerShell: `New-AzPublicIpAddress -Name pip-lab-lb -ResourceGroupName rg-lab-siec -Location polandcentral -Sku Standard -AllocationMethod Static`.

az = Azure CLI: narzędzie chmury Microsoftu

ZMIENIA SYSTEM

Włączenie przekazywania pakietów na karcie maszyny: az network nic update --ip-forwarding

```
az network nic update --resource-group rg-lab-siec --name NazwaKarty --ip-forwarding true
```

Bez tego Azure odrzuca pakiety, których adres docelowy nie jest adresem maszyny. W systemie maszyny trzeba dodatkowo włączyć przekazywanie, na Linuksie `sysctl -w net.ipv4.ip_forward=1` i wpis w `/etc/sysctl.d/`.

az = Azure CLI: narzędzie chmury Microsoftu

ZMIENIA SYSTEM

Utworzenie tabeli tras: az network route-table create

```
az network route-table create --resource-group rg-lab-siec --name rt-lab-app
```

W PowerShell: `New-AzRouteTable -ResourceGroupName rg-lab-siec -Name rt-lab-app -Location polandcentral`.

az = Azure CLI: narzędzie chmury Microsoftu

ZMIENIA SYSTEM

Dodanie trasy przez urządzenie sieciowe: az network route-table route create

```
az network route-table route create --resource-group rg-lab-siec --route-table-name rt-lab-app --name do-dane \
  --address-prefix 10.32.32.0/20 --next-hop-type VirtualAppliance --next-hop-ip-address 10.32.1.4
```

Następnym przeskokiem dla sieci danych staje się `vm-lab-nva01`. Inne typy przeskoku to `VirtualNetworkGateway`, `VnetLocal`, `Internet` i `None` (odrzucenie). W PowerShell: `Add-AzRouteConfig -RouteTable $tabela -Name do-dane -AddressPrefix 10.32.32.0/20 -NextHopType VirtualAppliance -NextHopIpAddress 10.32.1.4 | Set-AzRouteTable`.

az = Azure CLI: narzędzie chmury Microsoftu

ZMIENIA SYSTEM

Przypisanie tabeli tras do podsieci: az network vnet subnet update --route-table

```
az network vnet subnet update --resource-group rg-lab-siec --vnet-name vnet-lab-app --name snet-web --route-table rt-lab-app
```

Tabela działa dla ruchu wychodzącego z podsieci. Żeby odpowiedzi wracały tą samą drogą, w `snet-dane` potrzebna jest lustrzana trasa do 10.32.16.0/20 przez 10.32.1.4.

az = Azure CLI: narzędzie chmury Microsoftu

ZMIENIA SYSTEM

Utworzenie grupy zabezpieczeń aplikacji: az network asg create

```
az network asg create --resource-group rg-lab-siec --name asg-lab-web
```

W PowerShell: `New-AzApplicationSecurityGroup -ResourceGroupName rg-lab-siec -Name asg-lab-web -Location polandcentral`.

az = Azure CLI: narzędzie chmury Microsoftu

ZMIENIA SYSTEM

Dodanie karty maszyny do grupy zabezpieczeń aplikacji: az network nic ip-config update

```
az network nic ip-config update --resource-group rg-lab-obliczenia --nic-name NazwaKarty
--name ipconfig1 \
  --application-security-groups /subscriptions/IdSubskrypcji/resourceGroups/rg-lab-
siec/providers/Microsoft.Network/applicationSecurityGroups/asg-lab-web
```

Nazwę konfiguracji IP karty (często `ipconfig1` albo `ipconfigNazwaMaszyny`) sprawdzamy `az network nic show --resource-group rg-lab-obliczenia --name NazwaKarty --query "ipConfigurations[].name"`.

IP = Internet Protocol: adres komputera w sieci; w elektryce: stopień ochrony obudowy (Ingress Protection) · **az** = Azure CLI: narzędzie chmury Microsoftu

ZMIENIA SYSTEM

Dodanie reguły NSG z grupą zabezpieczeń aplikacji: az network nsg rule create

```
az network nsg rule create --resource-group rg-lab-siec --nsg-name nsg-lab-web --name
Zezwol-HTTPS-do-web \
  --priority 210 --direction Inbound --access Allow --protocol Tcp \
  --source-address-prefixes Internet --destination-port-ranges 443 --destination-asgs
asg-lab-web
```

Priorytet od 100 do 4096, niższy liczy się pierwszy, a przetwarzanie kończy się na pierwszej pasującej regule. W PowerShell regułę tworzy `New-AzNetworkSecurityRuleConfig` z parametrami `-Priority`, `-Direction`, `-Access`, `-Protocol` i `-DestinationApplicationSecurityGroup`.

NSG = Network Security Group: grupa zabezpieczeń sieci w Azure, lista reguł przepuszczających albo blokujących ruch do podsieci i kart sieciowych maszyn · **az** = Azure CLI: narzędzie chmury Microsoftu

□□ TYLKO ODCZYT

Sprawdzenie reguł działających na karcie: az network nic list-effective-nsg

```
az network nic list-effective-nsg --resource-group rg-lab-obliczenia --name NazwaKarty
```

Pokazuje reguły ze wszystkich NSG działających na karcie (z podsieci i z karty), razem z regułami domyślnymi i rozwiniętymi tagami usług. Maszyna musi być uruchomiona. W PowerShell: `Get-AzEffectiveNetworkSecurityGroup -NetworkInterfaceName NazwaKarty -ResourceGroupName rg-lab-obliczenia`.

□□ **NSG** = Network Security Group: grupa zabezpieczeń sieci w Azure, lista reguł przepuszczających albo blokujących ruch do podsieci i kart sieciowych maszyn · **az** = Azure CLI: narzędzie chmury Microsoftu

□□ TYLKO ODCZYT

Sprawdzenie tras działających na karcie: az network nic show-effective-route-table

```
az network nic show-effective-route-table --resource-group rg-lab-obliczenia --name NazwaKarty -o table
```

Pokazuje trasy systemowe, z peeringu i nasze UDR, z informacją, która wygrywa. W PowerShell: `Get-AzEffectiveRouteTable -NetworkInterfaceName NazwaKarty -ResourceGroupName rg-lab-obliczenia`.

□□ **UDR** = User-Defined Route: trasa definiowana przez użytkownika w tabeli tras Azure, która zmienia domyślną drogę ruchu z podsieci, na przykład przez zaporę · **az** = Azure CLI: narzędzie chmury Microsoftu

□□ ZMIENIA SYSTEM

Utworzenie hosta Bastion: az network bastion create

```
az network public-ip create --resource-group rg-lab-siec --name pip-lab-bastion --sku Standard --allocation-method Static
az network bastion create --resource-group rg-lab-siec --name bas-lab --vnet-name vnet-lab-hub \
  --public-ip-address pip-lab-bastion --sku Basic --location polandcentral
```

Polecenie pochodzi z rozszerzenia `bastion`, które CLI instaluje przy pierwszym użyciu. Sieć musi mieć podsieć `AzureBastionSubnet` o rozmiarze co najmniej /26. Bastion jest płatny od godziny, więc w laboratorium żyje tylko w dniu 19. W PowerShell: `New-AzBastion -ResourceGroupName rg-lab-siec -Name bas-lab -PublicIpAddress $pip -VirtualNetwork $vnet -Sku Basic`.

CLI = Command Line Interface: praca przez wpisywanie komend w terminalu · **az** = Azure CLI: narzędzie chmury Microsoftu

ZMIENIA SYSTEM

Włączenie punktu końcowego usługi w podsieci: az network vnet subnet update --service-endpoints

```
az network vnet subnet update --resource-group rg-lab-siec --vnet-name vnet-lab-app --name snet-web --service-endpoints Microsoft.Storage
```

Ruch z podsieci do Azure Storage idzie wtedy optymalną trasą sieci szkieletowej, a zapora konta może wpuścić podsieć regułą sieci wirtualnej. Konto nadal ma publiczny adres.

az = Azure CLI: narzędzie chmury Microsoftu

ZMIENIA SYSTEM

Utworzenie prywatnego punktu końcowego konta magazynu: az network private-endpoint create

```
az network private-endpoint create --resource-group rg-lab-siec --name pe-lab-blob --vnet-name vnet-lab-hub --subnet snet-pe \
  --private-connection-resource-id $(az storage account show --name NazwaKonta --resource-group rg-lab-magazyn --query id -o tsv) \
  --group-id blob --connection-name pe-lab-blob-polaczenie
```

Konto dostaje prywatny adres z `snet-pe` (na przykład 10.32.2.4) dla podzasobu `blob`. Dla plików podajemy `--group-id file`. W PowerShell: `New-AzPrivateEndpoint` z obiektem połączenia z `New-AzPrivateLinkServiceConnection -PrivateLinkServiceId IdKonta -GroupId blob`.

az = Azure CLI: narzędzie chmury Microsoftu

ZMIENIA SYSTEM

Utworzenie prywatnej strefy DNS i połączenie z siecią: az network private-dns zone create

```
az network private-dns zone create --resource-group rg-lab-siec --name
privatelink.blob.core.windows.net
az network private-dns link vnet create --resource-group rg-lab-siec --zone-name
privatelink.blob.core.windows.net \
  --name link-hub --virtual-network vnet-lab-hub --registration-enabled false
az network private-endpoint dns-zone-group create --resource-group rg-lab-siec --
endpoint-name pe-lab-blob \
  --name domyslna --private-dns-zone privatelink.blob.core.windows.net --zone-name blob
```

Trzecia komenda każe punktowi końcowemu samemu dopisywać rekord A w strefie. Bez strefy prywatnej nazwa `NazwaKonta.blob.core.windows.net` nadal rozwiązuje się na adres publiczny.

□□ **DNS** = Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP ·**az** = Azure CLI: narzędzie chmury Microsoftu

□□ **ZMIENIA SYSTEM**

Utworzenie strefy prywatnej z autorejestracją maszyn: az network private-dns link vnet create --registration-enabled true

```
az network private-dns zone create --resource-group rg-lab-siec --name
wew.azlab.zielona.example
az network private-dns link vnet create --resource-group rg-lab-siec --zone-name
wew.azlab.zielona.example \
  --name link-app --virtual-network vnet-lab-app --registration-enabled true
```

Maszyny w `vnet-lab-app` same zapisują swoje rekordy A, na przykład `vm-lab-web01.wew.azlab.zielona.example`. Sieć może mieć autorejestrację tylko w jednej strefie prywatnej.

□□ **az** = Azure CLI: narzędzie chmury Microsoftu

□□ **ZMIENIA SYSTEM**

Utworzenie publicznej strefy DNS z rekordem A: az network dns zone create

```
az network dns zone create --resource-group rg-lab-siec --name azlab.zielona.example
az network dns record-set a add-record --resource-group rg-lab-siec --zone-name
azlab.zielona.example --record-set-name www --ipv4-address 203.0.113.70
```

(gdzie 203.0.113.70 to przykładowy adres z puli dokumentacyjnej; w laboratorium wpisujemy adres `pip-lab-lb`)

Strefa działa w internecie dopiero po delegowaniu jej u rejestratora na serwery nazw podane przez Azure (`az network dns zone show --query nameServers`). W PowerShell: `New-AzDnsZone -Name azlab.zielona.example -ResourceGroupName rg-lab-siec` i `New-AzDnsRecordSet -Name www -RecordType A -ZoneName azlab.zielona.example -ResourceGroupName rg-lab-siec -Ttl 3600 -DnsRecords (New-AzDnsRecordConfig -Ipv4Address 203.0.113.70)`.

□□ **DNS** = Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP · **az** = Azure CLI: narzędzie chmury Microsoftu

□□ ZMIENIA SYSTEM

Utworzenie publicznego równoważenia obciążenia: az network lb create

```
az network lb create --resource-group rg-lab-siec --name lb-lab-web --sku Standard \
  --public-ip-address pip-lab-lb --frontend-ip-name fe-web --backend-pool-name pula-web
```

Dla wewnętrznego równoważenia zamiast publicznego adresu podajemy `--vnet-name`, `--subnet` i `--private-ip-address`, na przykład 10.32.16.10.

□□ **az** = Azure CLI: narzędzie chmury Microsoftu

□□ ZMIENIA SYSTEM

Dodanie sondy kondycji HTTP: az network lb probe create

```
az network lb probe create --resource-group rg-lab-siec --lb-name lb-lab-web --name
sonda-http --protocol Http --port 80 --path /
```

Maszyna, która nie odpowiada na sondę, wypada z rozdziału ruchu.

□□ **HTTP** = Hypertext Transfer Protocol: protokół stron WWW · **az** = Azure CLI: narzędzie chmury Microsoftu

□□ ZMIENIA SYSTEM

Dodanie reguły równoważenia: az network lb rule create

```
az network lb rule create --resource-group rg-lab-siec --lb-name lb-lab-web --name http
\
  --protocol Tcp --frontend-port 80 --backend-port 80 --frontend-ip fe-web --backend-
pool-name pula-web --probe sonda-http
```

□□ **az** = Azure CLI: narzędzie chmury Microsoftu

□□ TYLKO ODCZYT

Dodanie karty maszyny do puli: az network nic ip-config address-pool add

```
az network nic ip-config address-pool add --resource-group rg-lab-obliczenia --nic-name
NazwaKarty --ip-config-name ipconfig1 \
  --lb-name /subscriptions/IdSubskrypcji/resourceGroups/rg-lab-
siec/providers/Microsoft.Network/loadBalancers/lb-lab-web --address-pool pula-web
```

Powtarzamy dla obu maszyn WWW. Pulę można też budować z adresów IP (`az network lb address-pool address add`).

□□ **WWW** = World Wide Web: strony i aplikacje otwierane w przeglądarce po HTTP albo HTTPS · **IP** = Internet Protocol: adres komputera w sieci; w elektryce: stopień ochrony obudowy (Ingress Protection) · **az** = Azure CLI: narzędzie chmury Microsoftu

□□ TYLKO ODCZYT

Włączenie Network Watcher w regionie: az network watcher configure

```
az network watcher configure --resource-group NetworkWatcherRG --locations polandcentral
--enabled true
```

Network Watcher zwykle włącza się sam przy pierwszej sieci w regionie, w grupie `NetworkWatcherRG`.

□□ **az** = Azure CLI: narzędzie chmury Microsoftu

TYLKO ODCZYT

Sprawdzenie, czy NSG przepuści pakiet: az network watcher test-ip-flow

```
az network watcher test-ip-flow --resource-group rg-lab-obliczenia --vm vm-lab-web01 --direction Inbound \
  --protocol TCP --local 10.32.16.4:80 --remote 203.0.113.10:50000
```

Odpowiada „Allow” albo „Deny” i podaje nazwę reguły, która zdecydowała. W PowerShell: `Test-AzNetworkWatcherIPFlow -Location polandcentral -TargetVirtualMachineId IdMaszyny -Direction Inbound -Protocol TCP -LocalIPAddress 10.32.16.4 -LocalPort 80 -RemoteIPAddress 203.0.113.10 -RemotePort 50000`.

NSG = Network Security Group: grupa zabezpieczeń sieci w Azure, lista reguł przepuszczających albo blokujących ruch do podsieci i kart sieciowych maszyn · **TCP** = Transmission Control Protocol: protokół sieciowy z potwierdzaniem dostarczenia · **az** = Azure CLI: narzędzie chmury Microsoftu

TYLKO ODCZYT

Sprawdzenie następnego przeskoku: az network watcher show-next-hop

```
az network watcher show-next-hop --resource-group rg-lab-obliczenia --vm vm-lab-web01 --source-ip 10.32.16.4 --dest-ip 10.32.32.4
```

Przy działającej trasie UDR wynik pokazuje `VirtualAppliance` i adres 10.32.1.4. W PowerShell: `Get-AzNetworkWatcherNextHop -NetworkWatcher $nw -TargetVirtualMachineId IdMaszyny -SourceIPAddress 10.32.16.4 -DestinationIPAddress 10.32.32.4`.

UDR = User-Defined Route: trasa definiowana przez użytkownika w tabeli tras Azure, która zmienia domyślną drogę ruchu z podsieci, na przykład przez zaporę · **az** = Azure CLI: narzędzie chmury Microsoftu

TYLKO ODCZYT

Sprawdzenie połączenia między maszynami: az network watcher test-connectivity

```
az network watcher test-connectivity --resource-group rg-lab-obliczenia --source-resource vm-lab-web01 --dest-address 10.32.32.4 --dest-port 5432
```

Testuje połączenie TCP z maszyny źródłowej i pokazuje przeskoki. Wymaga rozszerzenia Network Watcher na maszynie, które polecenie może doinstalować.

TCP = Transmission Control Protocol: protokół sieciowy z potwierdzaniem dostarczenia ·**az** = Azure CLI: narzędzie chmury Microsoftu

Dzień 18: VNet, podsieci, peering, publiczne adresy i trasy

Z ŻYCIA WZIĘTE

Poniedziałek, 10:30. Tomek ma działającą `vm-lab-web01` w sieci app i `vm-lab-db01` w sieci dane, obie z peeringiem do huba, a `ping` z jednej do drugiej milczy. Pytamy, gdzie jest peering między app a dane: nigdzie, i tak miało być. Tomek dokłada tabelę tras z przeskokiem przez `vm-lab-nva01`, włącza przekazywanie na karcie, a połączenie nadal nie działa. Dopiero `sysctl` w systemie nva01 i lustrzana trasa w sieci dane zamykają sprawę, a w dzienniku ląduje trójka: trasa tam, trasa z powrotem, przekazywanie w Azure i w systemie.

Cele egzaminu

- tworzenie i konfiguracja sieci wirtualnych i podsieci
- tworzenie i konfiguracja peeringu sieci wirtualnych
- konfiguracja publicznych adresów IP
- konfiguracja tras definiowanych przez użytkownika
- rozwiązywanie problemów z łącznością sieciową

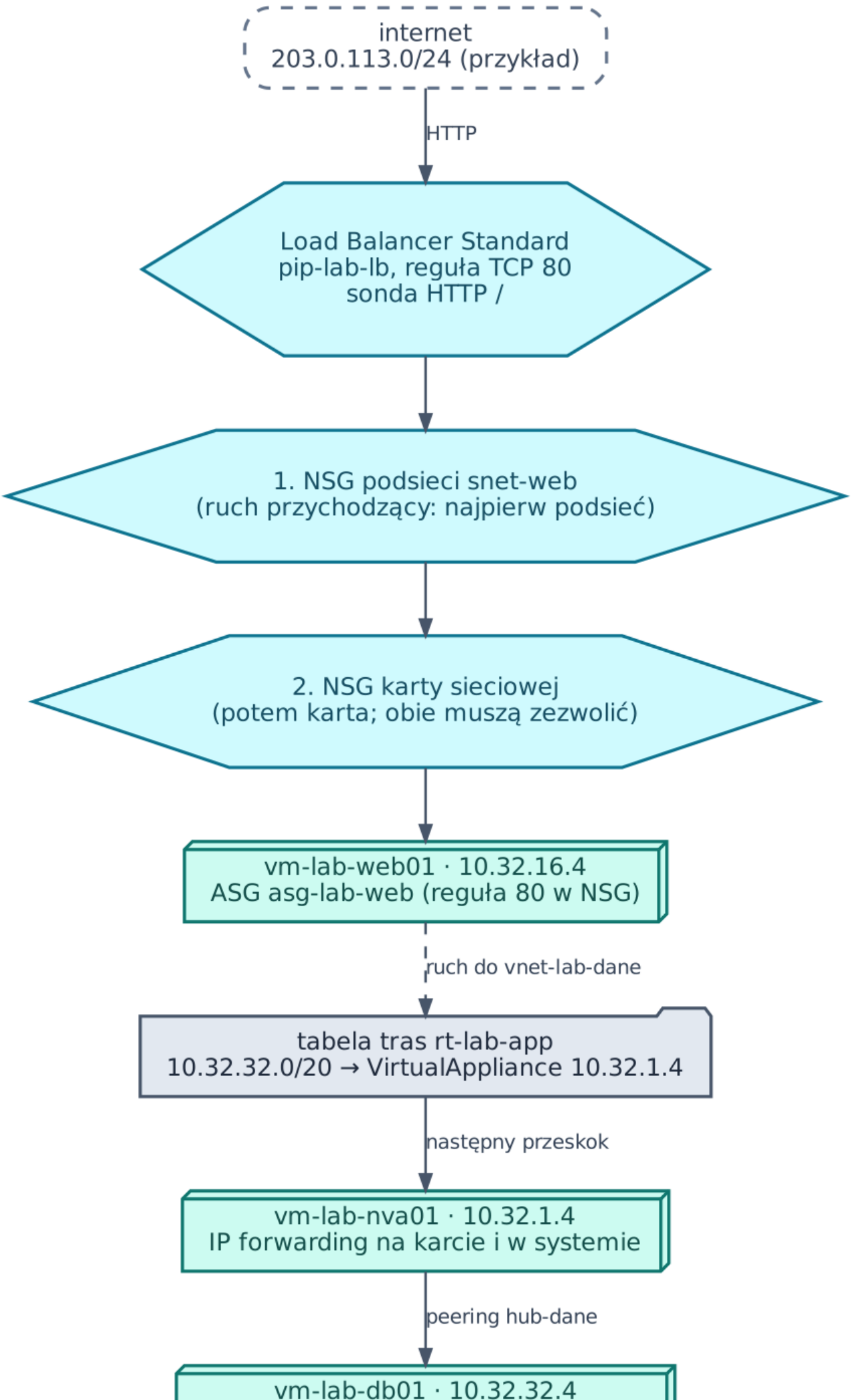
Jak to działa

Pojęcie: sieć wirtualna (VNet). Prywatna sieć w jednym regionie i jednej subskrypcji, z własną przestrzenią adresów i podsieciami. Maszyny w jednej sieci widzą się domyślnie, a ruch między sieciami wymaga peeringu, bramy VPN albo innego połączenia.

Pojęcie: peering. Połączenie dwóch sieci wirtualnych przez sieć szkieletową Microsoftu, w jednym regionie albo między regionami (peering globalny). Peering nie jest przechodni, przestrzenie adresów nie mogą się nakładać i zawsze tworzy się go z obu stron.

Ustawienie peeringu	Co znaczy
Allow virtual network access	ruch między sieciami w ogóle dozwolony
Allow forwarded traffic	sieć przyjmuje ruch, który nie zaczął się w sieci partnera (na przykład z NVA)
Allow gateway transit	sieć udostępnia swoją bramę VPN partnerowi
Use remote gateways	sieć korzysta z bramy VPN partnera

> **Pojęcie: trasa definiowana przez użytkownika (UDR).** Wpis w tabeli tras podsieci, który zmienia domyślną drogę ruchu, na przykład kieruje go przez urządzenie sieciowe (NVA) albo zaporę. Azure ma trasy systemowe dla sieci, peeringu i internetu, a UDR z dłuższym prefiksem albo o tym samym prefiksie wygrywa z trasą systemową.


internet
203.0.113.0/24 (przykład)
HTTP
Load Balancer Standard
pip-lab-lb, reguła TCP 80
sonda HTTP /
1. NSG podsieci snet-web
(ruch przychodzący: najpierw podsieć)
2. NSG karty sieciowej
(potem karta; obie muszą zezwolić)
vm-lab-web01 · 10.32.16.4
ASG asg-lab-web (reguła 80 w NSG)
ruch do vnet-lab-dane
tabela tras rt-lab-app
10.32.32.0/20 → VirtualAppliance 10.32.1.4
następny przeskok
vm-lab-nva01 · 10.32.1.4
IP forwarding na karcie i w systemie
peering hub-dane
vm-lab-db01 · 10.32.32.4



Rysunek 1. Droga pakietu w laboratorium: z internetu przez Load Balancer i dwie grupy NSG (najpierw podsieci, potem karty) do vm-lab-web01, a dalej do vnet-lab-dane przez tabelę tras rt-lab-app, urządzenie vm-lab-nva01 i peering hub-dane (kliknięcie otwiera pełny rozmiar)

Od 31 marca 2026 roku nowe podsieci tworzone API w nowszych wersjach są według dokumentacji Microsoftu prywatne: maszyna bez publicznego adresu nie wyjdzie do internetu. Portal ustawia podsieci prywatne już wcześniej. Jawną drogę wyjścia daje brama NAT (zalecana), reguły wychodzące Load Balancer Standard, publiczny adres Standard na karcie albo NVA z trasą UDR.

Bramy VPN (VPN Gateway, podsieć `GatewaySubnet`, połączenia site-to-site i point-to-site) nie ma na liście umiejętności z 17 kwietnia 2026 roku. Zastosowanie w Zielonej i porównanie z własną maszyną `edge-az01` opisuje strona Łącza operatora: światłowód, radiolinia, LTE i 5G oraz przełączanie na FortiGate, a ustawienia peeringu z bramą zdalną warto znać na poziomie tabeli wyżej.

Zadania laboratoryjne

1. Wdrażamy `lab-siec.bicep`, tworzymy `vm-lab-db01` (10.32.32.4) i `vm-lab-nva01` (10.32.1.4) bez publicznych adresów.
2. Sprawdzamy `az network nic show-effective-route-table` na `vm-lab-web01`: brak trasy do 10.32.32.0/20.
3. Tworzymy `rt-lab-app` z trasą do 10.32.32.0/20 przez 10.32.1.4 i `rt-lab-dane` z trasą do 10.32.16.0/20 przez 10.32.1.4, przypisujemy je do `snet-web` i `snet-dane`.
4. Włączamy przekazywanie na karcie nva01 i w systemie, potem `ping 10.32.32.4` z `vm-lab-web01` (przez konsolę szeregową albo Bastion w dniu 19).
5. Tworzymy `vnet-lab-test`, łączymy ją peeringiem z hubem i sprawdzamy, że nie widzi `vnet-lab-app`.

Pułapki egzaminacyjne

- Peering nie jest przechodni: dwie sieci połączone z hubem nie widzą się przez hub bez NVA i UDR albo bramy.
- Peering wymaga nienakładających się przestrzeni adresów.
- Trasa przez NVA wymaga przekazywania na karcie i w systemie oraz trasy powrotnej.
- Publiczny adres Basic nie istnieje już w nowych wdrożeniach, Standard jest statyczny i domyślnie zamknięty (wymaga NSG z regułą zezwalającą).

Ćwiczenia

1. Sieci A, B i C: A ma peering z B, B ma peering z C. Czy maszyna w A dosięgnie maszyny w C i co trzeba dołożyć?

Odpowiedź

Nie, peering nie jest przechodni. Trzeba dołożyć peering A z C albo urządzenie przekazujące w B (NVA albo Azure Firewall) z trasami UDR w A i C oraz „Allow forwarded traffic” w peeringach. Inną drogą jest brama VPN w B z tranzytem przez bramę.

Dzień 19: NSG i ASG, Bastion, punkty końcowe usług i prywatne

Z ŻYCIA WZIĘTE

Wtorek, 14:00. Ola prosi o dostęp SSH do `vm-lab-db01`, żeby sprawdzić wersję bazy, a Tomek już sięga po publiczny adres dla maszyny. Pytamy, kto będzie skanował port 22 do wieczora. Tomek stawia Bastion na godzinę, Ola loguje się z przeglądarki przez portal, a maszyna nadal nie ma publicznego adresu. Przy okazji Tomek zamyka konto magazynu dla internetu i daje mu prywatny adres 10.32.2.4.

Cele egzaminu

- tworzenie i konfiguracja grup zabezpieczeń sieci (NSG) i grup zabezpieczeń aplikacji
- ocena reguł działających w NSG
- wdrażanie Azure Bastion
- konfiguracja punktów końcowych usług dla PaaS
- konfiguracja prywatnych punktów końcowych dla PaaS

Jak to działa

Pojęcie: grupa zabezpieczeń sieci (NSG). Lista reguł filtrujących ruch po adresie, porcie i protokole, przypisana do podsieci, karty sieciowej albo obu. Ruch przychodzący przechodzi najpierw przez NSG podsieci, potem karty, a wychodzący odwrotnie: obie muszą zezwolić.

Reguła domyślna	Kierunek	Priorytet	Działanie
AllowVNetInBound	przychodzący	65000	zezwala na ruch z sieci wirtualnej (także z peeringu)

Reguła domyślna	Kierunek	Priorytet	Działanie
AllowAzureLoadBalancerInBound	przychodzący	65001	zezwala na sondy Load Balancera
DenyAllInbound	przychodzący	65500	odrzuca resztę
AllowVnetOutBound	wychodzący	65000	zezwala do sieci wirtualnej
AllowInternetOutBound	wychodzący	65001	zezwala do internetu
DenyAllOutBound	wychodzący	65500	odrzuca resztę

Reguł domyślnych nie da się usunąć, można je przesłonić regułą o niższym numerze. W jednej regule można podać wiele portów i adresów, ale nie wiele tagów usług ani wiele grup ASG.

> **Pojęcie: grupa zabezpieczeń aplikacji (ASG).** Etykieta nadawana kartom sieciowym maszyn, używana w regułach NSG zamiast adresów. Reguła „HTTPS do `asg-lab-web`" obejmie każdą nową maszynę WWW, której kartę dodamy do grupy, bez zmiany reguły.

> **Pojęcie: Azure Bastion.** Usługa w podsieci `AzureBastionSubnet` (minimum /26), która daje SSH i RDP do maszyn przez portal po HTTPS, bez publicznych adresów na maszynach. Poziom Developer nie wymaga podsieci ani publicznego adresu, Basic ma dwie instancje bez skalowania, Standard dokłada skalowanie, własne porty i link do udostępnienia, Premium nagrywanie sesji.

	Punkt końcowy usługi	Prywatny punkt końcowy
Adres usługi	nadal publiczny	prywatny adres w naszej podsieci
Ruch	sieć szkieletowa Microsoftu	prywatny adres przez sieć wirtualną, także z lokalnej sieci przez VPN
Zapora usługi	reguła sieci wirtualnej w zaporze konta	można całkiem wyłączyć dostęp publiczny
DNS	bez zmian	potrzebna strefa `privatelink.*`
Koszt	bez opłat za punkt końcowy	płatny od godziny i za ruch

Zadania laboratoryjne

1. Tworzymy `asg-lab-web`, dodajemy do niej karty obu maszyn WWW i regułę HTTPS w `nsg-lab-web`.
2. Sprawdzamy `az network nic list-effective-nsg` dla `vm-lab-web01` i odnajdujemy reguły domyślne.
3. Stawiamy Bastion w `vnet-lab-hub` i logujemy się do `vm-lab-db01` przez portal (peering huba z siecią dane wystarcza).

4. Włączamy punkt końcowy usługi `Microsoft.Storage` w `snet-web`, dodajemy regułę podsieci w zaporze konta i ustawiamy domyślną odmowę.
5. Tworzymy prywatny punkt końcowy konta w `snet-pe` ze strefą `privatelink.blob.core.windows.net`, a z maszyny w hubie sprawdzamy `nslookup NazwaKonta.blob.core.windows.net`: ma wrócić adres 10.32.2.x.
6. Usuwamy Bastion i publiczny adres `pip-lab-bastion` tego samego dnia.

Pułapki egzaminacyjne

- Ruch przychodzący musi przejść oba NSG (podsieci i karty), wystarczy odmowa w jednym.
- Reguła domyślna AllowVNetInBound wpuszcza ruch z sieci partnerskich, więc izolację między sieciami w peeringu robimy własną regułą odmowy.
- Bastion wymaga podsieci o nazwie dokładnie `AzureBastionSubnet` (poza poziomem Developer).
- Prywatny punkt końcowy bez strefy DNS działa tylko po adresie IP, nazwa nadal wskazuje adres publiczny.

Ćwiczenia

1. NSG podsieci zezwala na TCP 80 z internetu, a NSG karty nie ma żadnej reguły własnej. Czy ruch HTTP z internetu dotrze do maszyny?

Odpowiedź

Nie. NSG karty ma tylko reguły domyślne, a z internetu nic nie przepuszcza (DenyAllInbound, 65500). Ruch musi przejść obie grupy, więc dodajemy regułę w NSG karty albo usuwamy NSG z karty i zostawiamy tylko podsieć.

1. Konto magazynu ma prywatny punkt końcowy, a maszyna w sieci łączy się nadal z adresem publicznym. Co sprawdzamy?

Odpowiedź

Strefę prywatną `privatelink.blob.core.windows.net`: czy istnieje, czy ma rekord A dla konta (grupa stref DNS punktu końcowego) i czy jest połączona z siecią, z której pyta maszyna. Gdy maszyna używa własnego serwera DNS, ten serwer musi przekazywać zapytania do DNS Azure (168.63.129.16).

Dzień 20: Azure DNS, Load Balancer i Network Watcher

Z ŻYCIA WZIĘTE

Środa, 9:20. Tomek stawia `lb-lab-web` przed dwiema maszynami WWW, a strona przez publiczny adres zwraca błąd połączenia. Sonda pokazuje obie maszyny jako niezdrowe. Test przepływu IP z Network Watchera wskazuje regułę DenyAllInbound na karcie `vm-lab-web02`, której NSG nie miał reguły dla portu 80. Po dodaniu reguły sonda przechodzi, a odświeżanie strony pokazuje na zmianę stronę z web01 i web02.

Cele egzaminu

- konfiguracja Azure DNS
- konfiguracja wewnętrznego albo publicznego Load Balancera
- rozwiązywanie problemów z równoważeniem obciążenia

Jak to działa

Strefa	Kto ją widzi	Do czego
Publiczna strefa Azure DNS	internet, po delegowaniu u rejestratora	rekordy firmowej domeny, na przykład `www`
Prywatna strefa Azure DNS	sieci połączone ze strefą	nazwy wewnętrzne, autorejestracja maszyn, `privatelink.*`
DNS Azure 168.63.129.16	każda maszyna w sieci wirtualnej	rozwiązywanie nazw Azure i stref prywatnych

Pojęcie: Load Balancer. Usługa warstwy 4 (TCP i UDP), która rozdziela ruch z adresu frontowego na pulę maszyn według reguł, sprawdzając je sondami kondycji. Publiczny ma adres publiczny, wewnętrzny adres prywatny w podsieci. Wersję Basic Microsoft wycofał 30 września 2025 roku, w nowych wdrożeniach zostaje Standard, który jest domyślnie zamknięty: ruch do maszyn musi przepuścić NSG.

Usługa	Warstwa	Kiedy w pytaniu
Load Balancer	4, TCP i UDP	rozdział połączeń, porty inne niż HTTP, ruch wewnętrzny

Usługa	Warstwa	Kiedy w pytaniu
Application Gateway	7, HTTP i HTTPS	ścieżki URL, kończenie TLS, zapora aplikacji WAF
Front Door, Traffic Manager	globalnie	kilka regionów

Application Gateway występuje w przewodniku tylko w tabeli materiałów do nauki, więc wystarczy go rozpoznać jako równoważenie warstwy 7.

Rozwiązywanie problemów zaczynamy od sondy: jeśli obie maszyny są niezdrowe, winna jest zwykle NSG (brak reguły dla portu aplikacji albo sondy), usługa na maszynie albo zła ścieżka sondy HTTP. Network Watcher daje narzędzia do każdego kroku: test przepływu IP (czy NSG przepuści), następny przeskok (dokąd poleci pakiet), test łączności (czy połączenie się zestawi) i Connection monitor (ciągłe pomiary, opisane na stronie o monitorowaniu).

Zadania laboratoryjne

1. Tworzymy publiczną strefę `azlab.zielona.example` z rekordem `www` na adres `pip-lab-lb` i odczytujemy serwery nazw strefy.
2. Tworzymy prywatną strefę `wew.azlab.zielona.example` z autorejestracją dla `vnet-lab-app` i sprawdzamy rekordy maszyn.
3. Stawiamy `lb-lab-web` z sondą HTTP i regułą 80, dodajemy obie karty do puli.
4. Usuwamy regułę 80 z NSG jednej maszyny, oglądamy stan sondy i diagnozujemy `az network watcher test-ip-flow`, potem przywracamy regułę.
5. Sprawdzamy `az network watcher show-next-hop` z web01 do db01 (wynik VirtualAppliance) i `test-connectivity` na port 22 bazy.
6. Wieczorem usuwamy Load Balancer, publiczne adresy i maszyny, które nie są potrzebne w tygodniu 4.

Pułapki egzaminacyjne

- Load Balancer Standard nie przepuści ruchu bez reguły NSG zezwalającej.
- Sonda HTTP oczekuje odpowiedzi 200 na podanej ścieżce, inna odpowiedź oznacza maszynę niezdrową.
- Strefa publiczna w Azure DNS nie działa w internecie bez delegowania u rejestratora.
- Autorejestracja: jedna sieć w jednej strefie prywatnej.

Ćwiczenia

1. Obie maszyny w puli Load Balancera są niezdrowe, a strona otwiera się bezpośrednio z maszyny w tej samej sieci. Co sprawdzamy po kolei?

Odpowiedź

Najpierw NSG podsieci i kart: czy zezwalają na port aplikacji z internetu i czy nie blokują sond (tag AzureLoadBalancer, reguła domyślna 65001 albo własna odmowa o niższym numerze). Potem konfigurację sondy: protokół, port i ścieżkę, która musi zwracać 200. Na końcu `test-ip-flow` z adresem źródłowym z internetu.

Dzień 21: powtórka tygodnia 3

Mini sprawdzian, dziesięć pytań na 15 minut:

1. Ile adresów Azure rezerwuje w podsieci?
2. Czy peering jest przechodni?
3. Co musi być włączone, żeby maszyna przekazywała ruch innych maszyn?
4. W jakiej kolejności NSG sprawdzają ruch przychodzący?
5. Jaki priorytet ma DenyAllInbound?
6. Jak nazywa się podsieć Bastionu i jaki ma minimalny rozmiar?
7. Czym różni się punkt końcowy usługi od prywatnego?
8. Dlaczego Load Balancer Standard nie przepuszcza ruchu po utworzeniu?
9. Które narzędzie Network Watchera pokaże regułę NSG, która zablokowała pakiet?
10. Czym różni się Load Balancer od Application Gateway?

Odpowiedzi

1. Pięć. 2. Nie. 3. Przekazywanie IP na karcie w Azure i w systemie maszyny. 4. Najpierw podsieć, potem karta. 5. 65500. 6. `AzureBastionSubnet`, co najmniej /26. 7. Punkt końcowy usługi zostawia publiczny adres usługi i otwiera drogę z podsieci, prywatny daje usłudze prywatny adres w naszej sieci. 8. Bo jest domyślnie zamknięty i potrzebuje NSG z regułą zezwalającą. 9. Test przepływu IP (IP flow verify). 10. Load Balancer działa w warstwie 4 (TCP, UDP), Application Gateway w warstwie 7 (HTTP, ścieżki, TLS, WAF).

Częste błędy

Objaw	Przyczyna	Co robimy
Peering w stanie Initiated	utworzony tylko z jednej strony	tworzymy drugą stronę

Objaw	Przyczyna	Co robimy
Maszyny w dwóch sieciach spoke się nie widzą	peering nie jest przechodni	peering bezpośredni albo NVA z UDR
Ruch przez NVA ginie	brak przekazywania na karcie lub w systemie, brak trasy powrotnej	`--ip-forwarding true`, `sysctl`, lustrzana trasa
Maszyna bez publicznego adresu nie pobiera pakietów	podsieć prywatna (nowe API albo portal)	brama NAT albo inna jawna droga wyjścia
`az network bastion create` odrzuca sieć	brak podsieci `AzureBastionSubnet` albo mniejsza niż /26	tworzymy podsieć o właściwej nazwie i rozmiarze
Nazwa konta nadal wskazuje adres publiczny	brak strefy `privatelink` albo połączenia ze strefą	strefa, link do sieci, grupa stref DNS punktu końcowego
Sonda Load Balancera pokazuje maszyny niezdrowe	NSG blokuje port, zła ścieżka sondy, usługa nie działa	`test-ip-flow`, sprawdzenie ścieżki i usługi

Powiązane: Obliczenia: ARM i Bicep, maszyny wirtualne, dostępność, App Service i kontenery · Monitorowanie i kopie: Azure Monitor, KQL, alerty, Backup i Site Recovery · Łącza operatora: światłowód, radiolinia, LTE i 5G oraz przełączanie na FortiGate · Plan 4 tygodni i laboratorium Azure w Zielonej

Źródła: Microsoft Learn: przewodnik do egzaminu AZ-104 (lista od 17 kwietnia 2026), „Network security groups” (priorytety 100 do 4096, reguły domyślne, reguły rozszerzone, ograniczenia ASG), „Azure Bastion configuration settings” (`AzureBastionSubnet`, /26, poziomy), „Default outbound access in Azure” (podsieci prywatne po 31 marca 2026, drogi wyjścia), „Upgrade from Basic Load Balancer” i odpowiedź Microsoft Q&A o wycofaniu Basic Load Balancer 30 września 2025, dokumentacja `az network bastion` (rozszerzenie `bastion`, parametry, poziomy); pomoc Azure CLI 2.91.0 (`az network vnet create`, `vnet subnet create` i `update`, `vnet peering create`, `public-ip create`, `nic update`, `route-table create`, `route-table route create`, `asg create`, `nic ip-config update`, `nsg rule create`, `nic list-effective-nsg`, `nic show-effective-route-table`, `private-endpoint create`, `private-dns zone create`, `private-dns link vnet create`, `private-endpoint dns-zone-group create`, `dns zone create`, `dns record-set a add-record`, `lb create`, `lb probe create`, `lb rule create`, `nic ip-config address-pool add`, `watcher configure`, `test-ip-flow`, `show-next-hop`, `test-connectivity`); dokumentacja modułu Az (`New-AzVirtualNetwork`, `New-AzVirtualNetworkSubnetConfig`, `Add-AzVirtualNetworkPeering`, `New-AzPublicIpAddress`, `New-AzRouteTable`, `Add-AzRouteConfig`, `New-AzApplicationSecurityGroup`, `New-AzNetworkSecurityRuleConfig`, `Get-AzEffectiveNetworkSecurityGroup`, `Get-AzEffectiveRouteTable`, `New-AzBastion`, `New-AzPrivateEndpoint`, `New-AzPrivateLinkServiceConnection`, `New-AzDnsZone`, `New-AzDnsRecordSet`, `New-AzDnsRecordConfig`, `Test-AzNetworkWatcherIPFlow`, `Get-AzNetworkWatcherNextHop`), stan na 19 października 2026.

Revision #3
Created 2026-10-18 23:00:24 UTC by Tomasz Konieczny
Updated 2026-10-26 14:27:21 UTC by Tomasz Konieczny