

netwerkverkeer binnen een vnet instellen



context

Standaard wordt binnen een [Azure vnet](#) ALLE verkeer doorgelaten waardoor je eigenlijk op 1 groot (niet te beveiligen) network uitkomt. Vooraleer we kunnen beveiligen, moeten we die default regel ongedaan maken.

default regel

1. onderstaande default regel laat alle inkomende verkeer toe:

+ Add Default rules							
Priority	Name	Port	Protocol	Source	Destination	Action	
100	InTcp50275	50275	TCP	Internet	VirtualNetwork	Allow	...
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow	...
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow	...
65500	DenyAllInBound	Any	Any	Any	Any	Deny	...

2. voeg onderstaande Inbound regel toe:
 1. **Source:** Service Tag
 2. **Source service tag:** VirtualNetwork
 3. **Source port range:***
 4. **Destination:***
 5. **Destination port range:***
 6. **Protocol:**Any
 7. **Action:**Deny
 8. **Priority:**4096

Inbound security rules

+ Add

Default rules

Priority	Name	Port
100	InTcp22	22
110	InTcp80	80
4096	BlockVnetInbound	Any
65000	AllowVnetInBound	Any
65001	AllowAzureLoadBalancerInBound	Any
65500	DenyAllInBound	Any

registratie

Save Discard Basic Delete

Source * ⓘ

Service Tag

Source service tag * ⓘ

VirtualNetwork

Source port ranges * ⓘ

*

Destination * ⓘ

VirtualNetwork

Destination port ranges * ⓘ

*

Protocol *

Any TCP UDP ICMP

Action *

Allow Deny

Priority * ⓘ

4096

Deze regel **blokkeert** ALLE verkeer binnen je vnet. De regel staat als laatste ingesteld. Alles wat voor die regel niet expliciet toegelaten wordt, wordt geblokkeerd. Ook het verkeer binnen het eigen subnet!
Nu kan je [netwerkverkeer gericht toelaten](#).

meer info

voeg hier linken toe naar verdere uitleg

[azure](#)

From:
<https://www.louslab.be/> - Lou's lab

Permanent link:
https://www.louslab.be/doku.php?id=azure:netwerk_verkeer_binnen_vnet_beperken

Last update: 2024/11/16 18:14

