

Azure VPN mit lokalem Netz über FortiGate Firewall verbinden

Expertslive Cafe Q2/2019

Roman Stadlmair

www.cloudnative.at

[!\[\]\(d66ff64371a51729ac8c1cdaa685ba6f_img.jpg\) www.powershell.co.at](https://twitter.com/powershellco)



Azure Virtual Networks

- RFC 1918 konforme Angabe (172.16.110.0/24)
- Internet Outbound default möglich





Vnet Subnets

- Eindeutiger Name und Adressraum
- Kleinster Raum /29
 - z.B. 192.168.0.0/29
 - Subnet ID: 0
 - Hosts: 1-6
 - Broadcast: 7
- Azure spezifisch:
 - Erste und letzte Adresse für Protokoll Konformität (-2)
 - Drei zusätzliche Adressen für Azure Servicenutzung (-3)
 - Es bleiben DREI IP Adressen für Hosts über
- Security Groups
 - Keine oder eine (gleiche Subscription und Location)
- Routing Tables
 - Keine oder eine (gleiche Subscription und Location)





Vnet Gateway

- Braucht ein Gateway Subnetz
 - Muss „GatewaySubnet“ heißen !
- Und eine Public IP
- Parameter
 - Route-based





Eine Public-IP Adresse erstellen

- Azure Netz muss von außen erreichbar sein





Azure Local Network Gateway

- Repräsentiert die lokale Firewall und die Netze dahinter in Azure
- IP Adresse wie die lokale FW erreichbar ist





Der Fortinet Teil

1.) VPN erzeugen mit VPN Wizard

1 VPN Setup

Name

Template Type ☐ ☐ ☒



FG Config Step 2

Name

Comments 0/255

Network

IP Version ☒ IPv4 ☐ IPv6

Remote Gateway

IP Address

Interface

Local Gateway ☐

Mode Config ☐

NAT Traversal

Dead Peer Detection

Forward Error Correction Egress ☐ Ingress ☐

Authentication

Method

Pre-shared Key

IKE



FG Config Step 3 – Phase 1

Phase 1 Proposal ⊕ Add

Encryption	AES256 ▼	Authentication	SHA1 ▼	✕
Encryption	3DES ▼	Authentication	SHA1 ▼	✕
Encryption	AES256 ▼	Authentication	SHA256 ▼	✕
Diffie-Hellman Group	<input type="checkbox"/> 32 <input type="checkbox"/> 31 <input type="checkbox"/> 30 <input type="checkbox"/> 29 <input type="checkbox"/> 28 <input type="checkbox"/> 27 <input type="checkbox"/> 21 <input type="checkbox"/> 20 <input type="checkbox"/> 19 <input type="checkbox"/> 18 <input type="checkbox"/> 17 <input type="checkbox"/> 16 <input type="checkbox"/> 15 <input type="checkbox"/> 14 <input type="checkbox"/> 5 <input checked="" type="checkbox"/> 2 <input type="checkbox"/> 1			
Key Lifetime (seconds)	<input type="text" value="2880"/>			
Local ID	<input type="text"/>			

Veraltete
Verschlüsselung
! Bessere testen



FG Step 3 – Phase 2

Phase 2 Selectors

Name	Local Address	Remote Address
DeinAzureGW	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0

New Phase 2 ☒

Name:

Comments:

Local Address: Subnet

Remote Address: Subnet

☒ Advanced...

Phase 2 Proposal ☒ Add

Encryption	AES256	Authentication	SHA1	<input checked="" type="checkbox"/>
Encryption	3DES	Authentication	SHA1	<input checked="" type="checkbox"/>
Encryption	AES256	Authentication	SHA256	<input checked="" type="checkbox"/>

Enable Replay Detection ☐

Enable Perfect Forward Secrecy (PFS) ☐

Local Port: All ☒

Remote Port: All ☒

Protocol: All ☒

Auto-negotiate ☐

Autokey Keep Alive ☐

Key Lifetime: Seconds



Seconds:

Veraltete
Verschlüsselung
! Bessere testen



FG Step 4 - FW Objekt anlegen

Edit Address

Name	<input type="text" value="p-thegalaxy-vnet110"/>
Color	 <input type="button" value="Change"/>
Type	<input data-bbox="699 478 1201 521" type="text" value="Subnet"/>
IP/Netmask	<input type="text" value="172.16.110.0/24"/>
Interface	 <input data-bbox="749 587 1201 631" type="text" value="pandora42ipsec"/>
Show in Address List	<input checked="" type="checkbox"/>
Static Route Configuration	<input checked="" type="checkbox"/>
Comments	<input data-bbox="699 744 1136 788" type="text" value="Azure Virtual Network"/> 21/255

Tags



FG Step 5 – Regeln anlegen

Name ⓘ	ToAzureNet
Incoming Interface	LAN (lan1) ▼
Outgoing Interface	pandora42ipsec ▼
Source	all ✕ +
Destination	p-thegalaxy-vnet110 ✕ +
Schedule	always ▼
Service	ALL ✕ +
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY
Inspection Mode	<input checked="" type="checkbox"/> Flow-based <input type="checkbox"/> Proxy-based
Firewall / Network Options	
NAT	<input type="checkbox"/>
Protocol Options	<input checked="" type="checkbox"/> PRX default ▼ ✎

Name ⓘ	FromAzureNet
Incoming Interface	pandora42ipsec ▼
Outgoing Interface	LAN (lan1) ▼
Source	p-thegalaxy-vnet110 ✕ +
Destination	all ✕ +
Schedule	always ▼
Service	ALL ✕ +
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY
Inspection Mode	<input checked="" type="checkbox"/> Flow-based <input type="checkbox"/> Proxy-based
Firewall / Network Options	
NAT	<input type="checkbox"/>
Protocol Options	<input checked="" type="checkbox"/> PRX default ▼ ✎










FG Step 6 – Packet Size limits

```
config firewall policy
  edit <policy-id>
    set tcp-mss-sender 1350
    set tcp-mss-receiver 1350
  next
end
```



FG Step 7 – Route anlegen

Destination	<div>Subnet</div> <div>172.16.110.0/255.255.255.0</div>
Interface	<div> pandora42ipsec</div>
Administrative Distance 	<div>7</div>
Comments	<div>Route ins Azure VPN</div>
Status	<div><div> Enabled</div><div> Disabled</div></div>
<div> Advanced Options</div>	





Zurück zu Azure – Site2Site Connection anlegen

- Verbindet die beiden Gateways
- Hält den Shared Key (unverschlüsselt!)





Routen und DNS in Azure

- Im VNET stehen die DNS Server (lokale eintragen)
- Routen erzeugen (eigenes Objekt, verlinkt mit den Subnetzen)





Tipps

1. Netzwerkplan
2. Namen mit Ressourcetypen „p-thegalaxy-vngateway“
3. Routing !
4. Diagrammfunktion (VNET) nutzen
5. Monitoring:
 1. Azure: Connections
 2. FG: Monitor → IPsec Monitor





Links

- <https://cookbook.fortinet.com/ipsec-vpn-microsoft-azure-54/>





Q&A

