Azure VPN mit lokalem Netz über FortiGate Firewall verbinden Expertslive Cafe Q2/2019

Roman Stadlmair

www.cloudnative.at

ww.powershell.co.at



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 Addressen 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	DeinAzureC	W	
Template Type	Site to Site	Remote Access	Custom

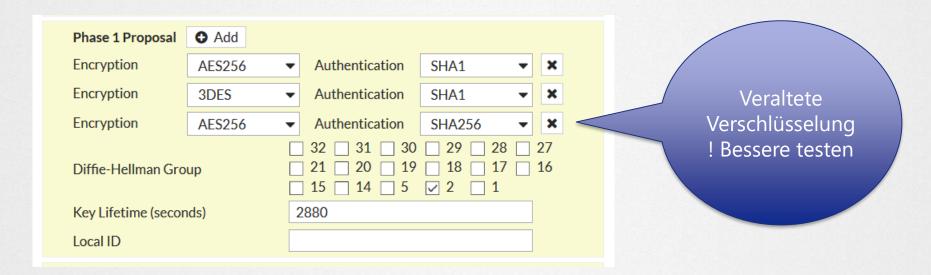


FG Config Step 2

Name	DeinAzureGW
Comments	Commentsii 0/255
Network	
IP Version	IPv4 IPv6
Remote Gateway	Static IP Address ▼
IP Address	123.123.123.123
Interface	
Local Gateway	•
Mode Config	
NAT Traversal	Enable Disable Forced
Dead Peer Detection	Disable On Idle On Demand
Forward Error Correction	Egress Ingress
Authentication	
Method	Pre-shared Key ▼
Pre-shared Key	
IKE	



FG Config Step 3 – Phase 1





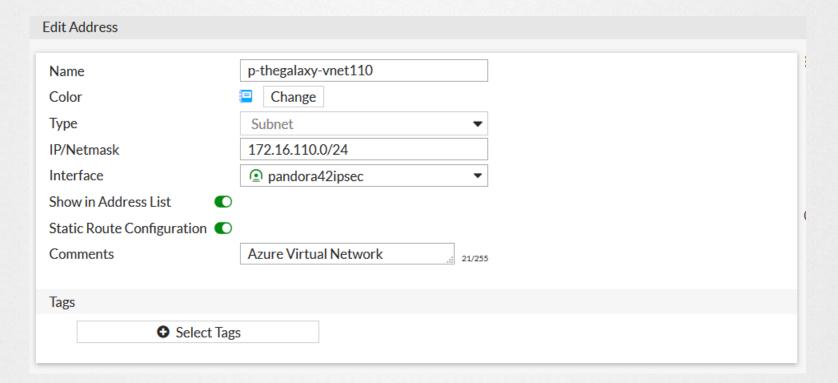
FG Step 3 – Phase 2

Phase 2 Selectors							
Name	Local	Local Address		Remote Address			
DeinAzureGW	0.0.0	.0/0.0.0.0	.0.0		0.0.0/0.0.0		
New Phase 2						•	0
Name		DeinAzureGW					
Comments		Comments					
Local Address		Subnet	Subnet ▼ 0		0.0.0.0/0.0.0.0		
Remote Address		Subnet	-	0.0.0.0/0.0.0.0			
Advanced							
Phase 2 Proposal	◆ Add						
Encryption	AES256	▼ Auth	enticatio	n [SHA1	•	×
Encryption	3DES	▼ Auth	Authentication		SHA1	•	×
Encryption	AES256	▼ Auth	Authentication		SHA256	•	×
Enable Replay Dete	ection						
Enable Perfect For	ward Secrecy (PF	S)					
Local Port		All 🗹					
Remote Port		All 🗸					
Protocol		All 🔽					
Auto-negotiate							
Autokey Keep Alive							
Key Lifetime		Seconds				•	
Seconds	27000						

Veraltete Verschlüsselung ! Bessere testen

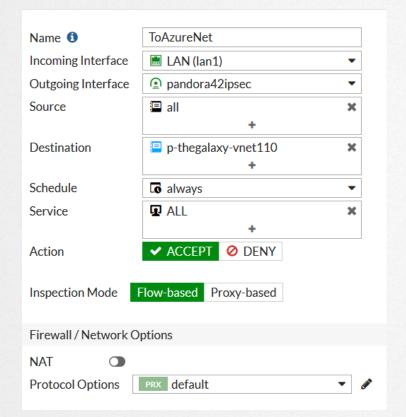


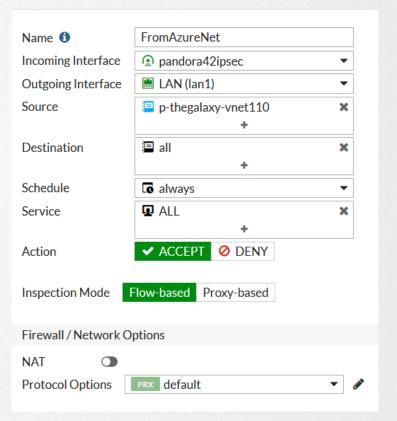
FG Step 4 - FW Objekt anlegen





FG Step 5 – Regeln anlegen





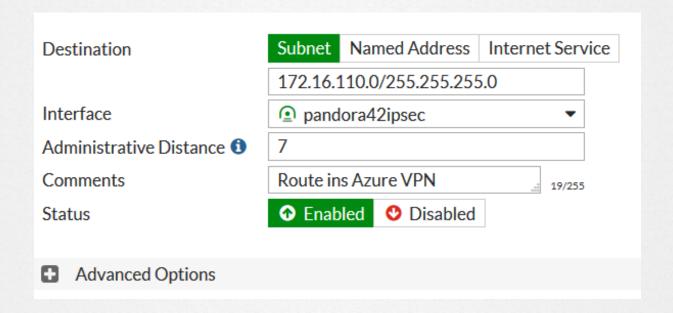


FG Step 6 – Packet Size limts

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



FG Step 7 – Route anlegen





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)



- Netzwerkplan
 Namen mit Resourcetypen "p-thegalaxy-vngateway"
 Routing!
 Diagrammfunktion (VNET) nutzen
 Monitoring:

- - 1. Azure: Connections
 - 2. FG: Monitor → IPSec Monitor



Links

 https://cookbook.fortinet.com/ipsec-vpnmicrosoft-azure-54/



Q&A

