

Lab 4

Author: Benjamin Medicke

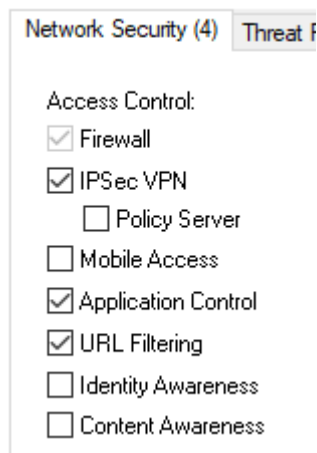
Topics: IPSec VPN

[lab1](#) | [lab2](#) | [lab3](#) | **lab4**

- Lab 4.1 IPSec VPN
 - 4.1.1 Aktivieren von IPSec VPN
 - 4.1.2 Erstellen eines neuen Interoperable Devices
 - 4.1.3 Erstellen einer neuen Meshed VPN Community
 - 4.1.4 Neue Firewall Regel
 - 4.1.5 Gateway Objekt Eigenschaften anpassen
 - 4.1.7 Testen der Erreichbarkeit via VPN Tunnel
 - 4.1.8 Erlauben von SSH Traffic
 - 4.1.9 Log des Blades: VPN
 - 4.1.10 Verbinden mit der Firewall via SSH
 - Aufgetretene Probleme

Lab 4.1 IPSec VPN

4.1.1 Aktivieren von IPSec VPN



"IPSec VPN" Blade aktiviert

General Properties
 Network Management
 NAT
 HTTPS Inspection
 HTTP/HTTPS Proxy
 ICAP Server
 Anti-Bot and Anti-Virus
 Platform Portal
 UserCheck
 Mail Transfer Agent
 ioc

IP Selection by Remote Peer

Locally managed VPN peers determine this gateway's IP address using the following method:

☒ Always use this IP address:

☐ Main address

☒ Selected address from topology table: 10.186.0.3

☐ Statically NATed IP:

☐ Calculate IP based on network topology

IPSec VPN Einstellungen

4.1.2 Erstellen eines neuen Interoperable Devices

Name	Network ...	IPv4 Address	IPv4 Netmask	IPv6 Address	Topology
external	External	10.186.0.3	255.255.255.0	N/A	External
internal	Internal	192.168.15.50	255.255.255.0	N/A	This Network

Anlegen eines neuen Interoperable Devices: 2 Interfaces

New Network

Niko-DMZ
 Enter Object Comment

General

NAT

IPv4

Network address: 192.168.15.0

Net mask: 255.255.255.0

Broadcast address:

☒ Included

☐ Not included

IPv6

Network address:

Prefix:

Groups

Add Tag

OK Cancel

Objekt zur Abbildung des internen Partnersubnetzwerkes

VPN Domain

☐ All IP Addresses behind Gateway based on Topology information
☒ User defined

...

Set Specific VPN Domain for Gateway Communities:

Auswahl der VPN Domain

4.1.3 Erstellen einer neuen Meshed VPN Community

New Meshed Community

niko_community
Enter Object Comment

“

Gateways

- Encrypted Traffic
- Encryption
- Tunnel Management
- Excluded Services
- Shared Secret
- Wire Mode
- Advanced

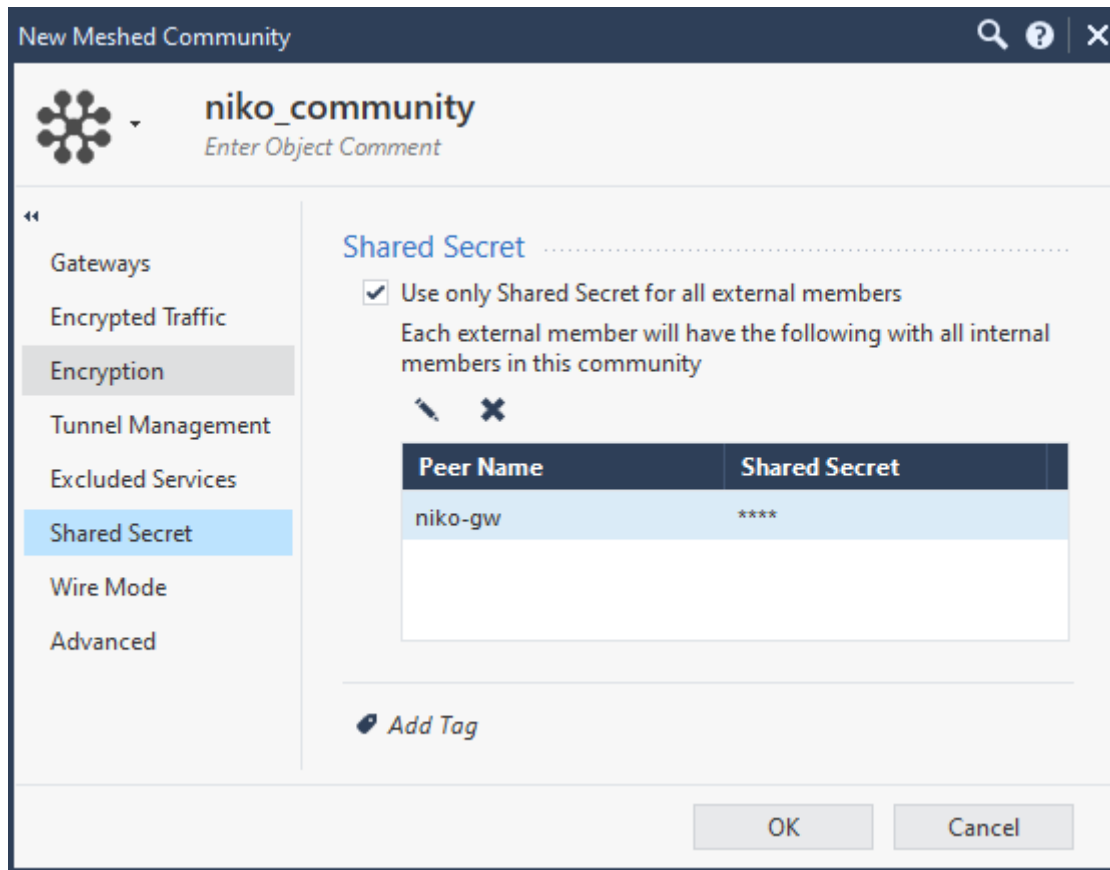
Participating Gateways

All the connections between the VPN Domains of the gateways below will be encrypted.

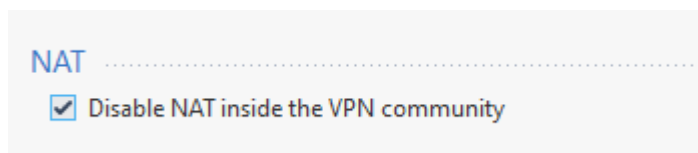
+ - x Search... 2 items

Gateway	Gateway Comments	VPN Domain
cloudguard-gw-vm		All IP addresses behind gateway based on topo...
niko-gw		Niko-DMZ

Neues Meshed VPN Community Objekt



Festlegen eines Shared Secrets (PSK)



Deaktivieren von NAT innerhalb der VPN Community



4.1.4 Neue Firewall Regel

Diese neue Regel erlaubt den Traffic von der eigenen Linux Instanz auf die des Kollegen.

1	VPN	Linux Instance Niko-linux-instance	Linux Instance Niko-linux-instance	niko_commu...	* Any	Accept	Log	* Policy Targets
---	-----	---------------------------------------	---------------------------------------	---------------	-------	--------	-----	------------------

Bidirektionale Kommunikation zwischen den VPN Teilnehmern erlauben

4.1.5 Gateway Objekt Eigenschaften anpassen

<div> <div>Get Interfaces..</div> <div>Edit</div> <div>Actions</div> <div></div> <div>Search...</div> </div>			
Name	Topology	IP	Comments
 eth0	External	10.186.0.3/20	
 eth1	This network	192.168.20.3/24	

Die Einstellungen waren bereits OK

4.1.7 Testen der Erreichbarkeit via VPN Tunnel

```
cs20m027@linux-vm: ~
PING 192.168.15.50 (192.168.15.50) 56(84) bytes of data.
64 bytes from 192.168.15.50: icmp_seq=1 ttl=62 time=3912 ms
64 bytes from 192.168.15.50: icmp_seq=5 ttl=62 time=6.94 ms
64 bytes from 192.168.15.50: icmp_seq=6 ttl=62 time=2.81 ms
64 bytes from 192.168.15.50: icmp_seq=7 ttl=62 time=2.48 ms
64 bytes from 192.168.15.50: icmp_seq=8 ttl=62 time=2.72 ms
64 bytes from 192.168.15.50: icmp_seq=9 ttl=62 time=2.96 ms
64 bytes from 192.168.15.50: icmp_seq=10 ttl=62 time=2.42 ms
64 bytes from 192.168.15.50: icmp_seq=11 ttl=62 time=2.06 ms
64 bytes from 192.168.15.50: icmp_seq=12 ttl=62 time=2.76 ms
64 bytes from 192.168.15.50: icmp_seq=13 ttl=62 time=3.02 ms
```

VPN Tunnel wird automatisch aufgebaut und funktioniert

4.1.8 Erlauben von SSH Traffic

```
cs20m027@linux-vm:~$ ssh cs20m001@192.168.15.50
The authenticity of host '192.168.15.50 (192.168.15.50)' can't be established.
ECDSA key fingerprint is SHA256:BENtFo09oxln6lm9ZZJz6KK+89BQ3WyBwZTdzbwCyGQ.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.15.50' (ECDSA) to the list of known hosts.
cs20m001@192.168.15.50: Permission denied (publickey).
cs20m027@linux-vm:~$
```

Der Tunnel ist funktionsfähig (SSH Verbindung scheitert nur an nicht vorhandenem Public Key)

```

cs20m027@linux-vm: ~
cs20m027@linux-vm:~$ curl 192.168.15.50:1234
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>Directory listing for /</title>
</head>
<body>
<h1>Directory listing for /</h1>
<hr>
<ul>
</ul>
<hr>
</body>
</html>
cs20m027@linux-vm:~$

```

`curl` auf Python Webserver, der bei meinem Kollegen läuft (`python3 -m http.server 1234`) funktioniert

4.1.9 Log des Blades: VPN

Log Details

Decrypt
Decrypted in community niko_community

Details | Matched Rules

VPN Details		Access Rule Name	
VPN Peer Gateway	niko-gw (34.118.70.205)	Access Rule Name	VPN
VPN Feature	VPN	Access Rule Number	1
Scheme	IKE	Actions	
Methods	ESP: AES-128 + SHA1	Report Log	Report Log to Check Point
Community	niko_community	More	
Traffic		Id	5c0a3a55-85d1-f4cf-60a1-0d3e00000...
Source	Niko-linux-instance (192.168.15.50)	Marker	@A@@B@1621154503@C@6818
Source Port	44488	Log Server Origin	cloudguard-gw-vm (10.186.0.3)
Source Zone	External	Id Generated By Indexer	false
Destination Zone	Internal	First	true
Service	tcp-high-ports (TCP/8000)	Sequencenum	1
Interface	eth0	Db Tag	{095892E3-1E51-D445-82DE-D35164B...
Destination	Linux Instance (192.168.20.50)	Logid	0
		Description	Decrypted in community niko_com...

4.1.10 Verbinden mit der Firewall via SSH

```
Peer 34.118.70.205 , niko-gw SAs:  
  
IKE SA <03dce0d77dd5f884,67fbfcl7d9ab28fe>
```

IKE Security Associations via `vpn tu`

```
SAs of all instances:  
  
Peer 34.118.70.205 , niko-gw SAs:  
  
IKE SA <03dce0d77dd5f884,67fbfcl7d9ab28fe>  
INBOUND:  
1. 0x463c34b (i: 2)  
OUTBOUND:  
1. 0x95e0bcb2 (i: 2)
```

IPSec Security Associations via `vpn tu`

```
0  
Deleting all IPsec+IKE SAs for ALL peers on ALL instances  
Hit <Enter> key to continue ...
```

Neustart des Tunnels durch Löschen der Associations

a. Verbindungsaufbau

Log Details

Key Install

cloudguard-gw-vm (10.186.0.3) accessed niko-gw (34.118.70.205) Today at 15:00:08

Log Info		More	
Log Server Origin	cloudguard-gw-vm (10.186.0.3)	Community	niko_community
Origin	cloudguard-gw-vm	Description	
Time	Today, 15:00:08	VPN Peer Gateway	niko-gw (34.118.70.205)
Blade	VPN	VPN Feature	IKE
Type	Log	IKE Responder Cookie	2e3bb533e482c8a2
		IKE Initiator Cookie	c6de662219818232
		Id	0aba0003-2228-7c14-60a1-1758000f0...
		Marker	@A@@B@1621154503@C@8549
		Id Generated By Indexer	false
		First	true
		Sequencenum	1
		Scheme	IKE [UDP (IPv4)]
		Ike	Main Mode completion [UDP (IPv4)].
		Methods	AES-256 + SHA1 + Group 2, Pre shared secrets
			less
Traffic			
Source	cloudguard-gw-vm (10.186.0.3)		
Interface Direction	inbound		
Interface Name	daemon		
Interface	daemon		
Destination	niko-gw (34.118.70.205)		
Policy			
Action	Key Install		
Actions			
Report Log	Report Log to Check Point		

Sequence Number 1: IKE Phase 1 (AES-256 + Group 2, PSK)

Log Details

Key Install

cloudguard-gw-vm (10.186.0.3) accessed niko-gw (34.118.70.205) Today at 15:00:08

Log Server Origin	cloudguard-gw-vm (10.186.0.3)	Community	niko_community
Origin	cloudguard-gw-vm	Description	
Time	Today, 15:00:08	Destination Key ID	0xea5cee57
Blade	VPN	IKE Phase2 Message ID	f40ff826
Type	Log	VPN Peer Gateway	niko-gw (34.118.70.205)
		Source Key ID	0xf4e73807
		VPN Feature	IKE
		IKE Responder Cookie	2e3bb533e482c8a2
		IKE Initiator Cookie	c6de662219818232
		Id	0aba0003-2228-7c14-60a1-1758000f0...
		Marker	@A@@B@1621154503@C@8550
		Id Generated By Indexer	false
		First	true
		Sequencenum	2
		Scheme	IKE [UDP (IPv4)]
		Ike	Quick Mode completion [UDP (IPv4)].
		Methods	ESP: AES-128 + SHA1
		Ike Ids	subnet: 192.168.20.0 (mask= 255.255.255.0) and subnet: 192.168.15.0 (mask= 255.255.255.0)
			less
Traffic			
Source	cloudguard-gw-vm (10.186.0.3)		
Interface Direction	inbound		
Interface Name	daemon		
Interface	daemon		
Destination	niko-gw (34.118.70.205)		
Policy			
Action	Key Install		
Actions			
Report Log	Report Log to Check Point		

Sequence Number 2: IKE Phase 2 (AES-128 + SHA1)

b. IPSec Parameterwahl

Welche IPSec Parameter haben Sie verwendet bzw. sind empfehlenswert?

Wir haben uns für die Standardeinstellungen entschieden, um eine hohe Kompatibilität zu gewährleisten. Zumindest `SHA-1` ist allerdings nicht mehr zeitgerecht: Google konnte bei diesem Algorithmus eine Kollision hervorrufen, womit dieser als gebrochen anzusehen ist. Siehe: <http://shattered.io/> (Es war Google möglich zwei PDF Dokumente mit unterschiedlichem Inhalt, aber gleichem SHA-1 Hash zu erzeugen, also eine Chosen-Plaintext Attack)

Aufgetretene Probleme

- Die SmartConsole ist nicht die ausgereifteste Software. Oft erscheinen Logs erst nach einem Neustart oder stark verzögert.