

# Project G-Cloud Setup

Name	value
Project	SAWFT
Project ID	sawft-275017
Cloudguard Admin User	admin
Cloudguard Admin PW	MesvQPH5h95c
Cloudguard internal IP(default)	10.128.0.2
Cloudguard internal IP(my-vpc)	192.168.23.2
Cloudguard external IP	34.71.14.71
LinuxHost IP	192.168.23.50
Cloudguard external IP Remote	35.194.38.233
LinuxHost IP Remote	192.168.27.50

## Lab 4: IPSec VPN

Eine Schwierigkeit, welche immer wieder auftauchte, war dass der RemoteClient regelmaessig haengen bleibt, und auch ab und zu abstuerzt.

Found 39 results (1.2 sec.)

	B...	L...	Origin	A...	Source	Source User...	Destination	Service	User	Source Machine...	Description
PM			cloudguard...		LinuxHost (192...		RemoteLinuxHost (192.168.27.50)	ICMP (CMP/O)			
PM			cloudguard...		LinuxHost (192...		RemoteLinuxHost (192.168.27.50)	echo-reque...			Encrypted in community MeshedComObj
PM			cloudguard...		cloudguard-gw...						
PM			cloudguard...		LinuxHost (192...						
PM			cloudguard...		LinuxHost (192...						
PM			cloudguard...		LinuxHost (192...						
PM			cloudguard...		LinuxHost (192...						
PM			cloudguard...		LinuxHost (192...						
PM			cloudguard...		LinuxHost (192...						
PM			cloudguard...		LinuxHost (192...						
PM			cloudguard...		LinuxHost (192...						
PM			cloudguard...		LinuxHost (192...						
PM			cloudguard...		LinuxHost (192...						
PM			cloudguard...		LinuxHost (192...						
2 AM			cloudguard...		cloudguard-gw...						
0 AM			cloudguard...		LinuxHost (192...						
4 AM			cloudguard...		LinuxHost (192...						
4 AM			cloudguard...		cloudguard-gw...						
9 AM			cloudguard...		LinuxHost (192...						
9 AM			cloudguard...		cloudguard-gw...						
2 AM			cloudguard...		LinuxHost (192...						
9 AM			cloudguard...		cloudguard-gw...						
9 AM			cloudguard...		cloudguard-gw...						
4 AM			cloudguard...		LinuxHost (192...						
6 AM			cloudguard...		cloudguard-gw...						
5 AM			cloudguard...		LinuxHost (192...						
3 AM			cloudguard...		cloudguard-gw...						
3 AM			cloudguard...		cloudguard-gw...						

Log Details

Reject

cloudguard-gw-vm (10.128.0.2) was blocked access to RaphaelGW (35.194.38.233) Today at 1:50:14 PM

Log Info

Log Server Origin cloudguard-gw-vm (10.128.0.2)

Origin cloudguard-gw-vm

Time Today, 1:50:14 PM

Blade VPN

Type Log

Traffic

Source cloudguard-gw-vm (10.128.0.2)

Interface Direction inbound

Interface Name daemon

Interface daemon

Destination RaphaelGW (35.194.38.233)

Policy

Action Reject

Actions

Report Log Report Log to Check Point

More

Community MeshedComObj

Description VPN Peer Gateway

Reject Category IKE failure

Check Point SmartConsole

Check Point SmartConsole is not responding

If you close the program, you might lose information.

Close the program

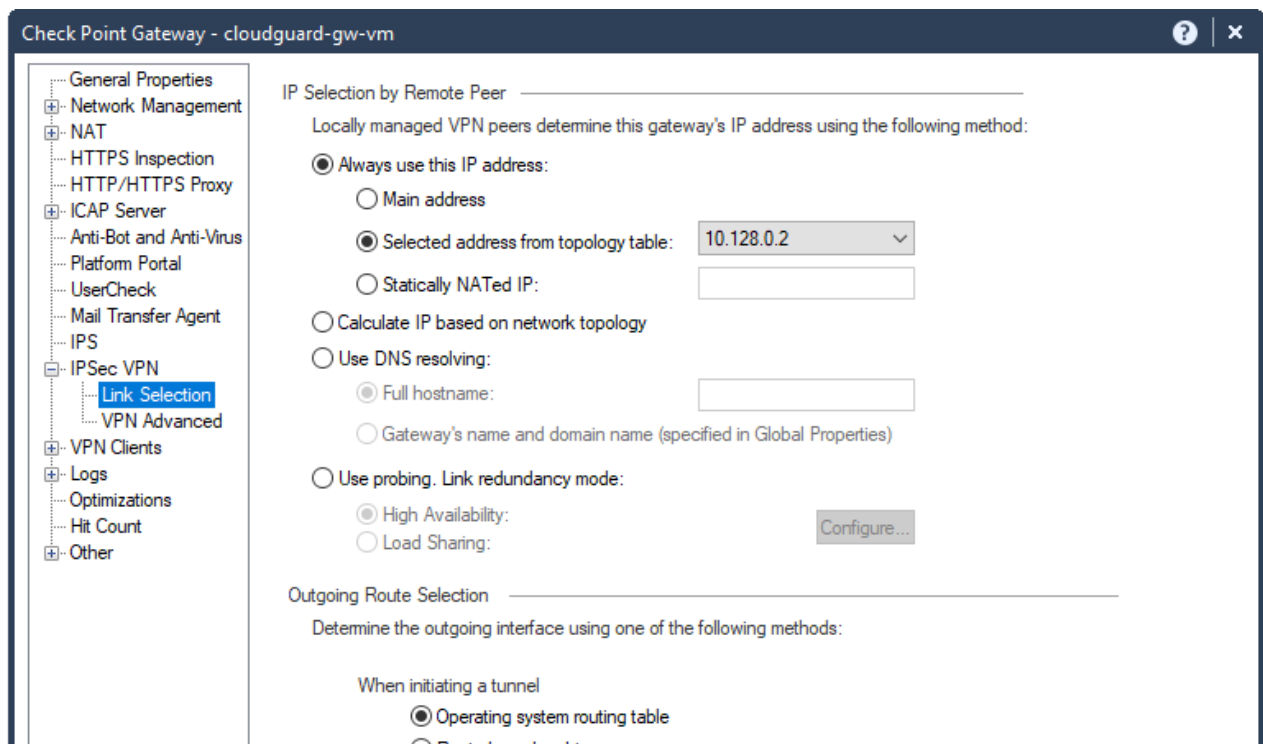
Wait for the program to respond

## Aufbau/Vorgangsweise

Im Prinzip ist die Vorgangsweise in der Angabe erklärt, alleine die "externe" IP des Partners als Gateway muss die "echte" externe IP sein und nicht wie in der Angabe (2.b) angegeben die "interne-externe" IP.

### 4.1

Nach aktivieren des IP-Sec VPN Blades wurde unter "Always use this IP address" die fuer die Firewall extern IP Adresse gewaehlt. G-Cloud routet diese automatisch auf die vom WAN aus erreichbare IP Adresse. Daher glaubt die Firewall ihre externe Adresse sei 10.128.0.2 . Dies soll durch das automatische NAT'ing dieser auf die externe IP 34.71.14.71 fuer uns kein weiteres Hindernis darstellen.



### 4.2

Interoperable Device - RaphaelPUBIP

General Properties

Topology

IPSec VPN

Type to Search

Get...

New...

Edit...

Delete

Actions

Name	Network ...	IPv4 Address	IPv4 Netmask	IPv6 Address	Topology
RemExt...	External	34.194.38.233	255.255.255.255	N/A	External
remINT	Internal	192.168.38.0	255.255.255.0	N/A	This Network

VPN Domain

All IP Addresses behind Gateway based on Topology information

User defined

Remote DMZ

...

View...

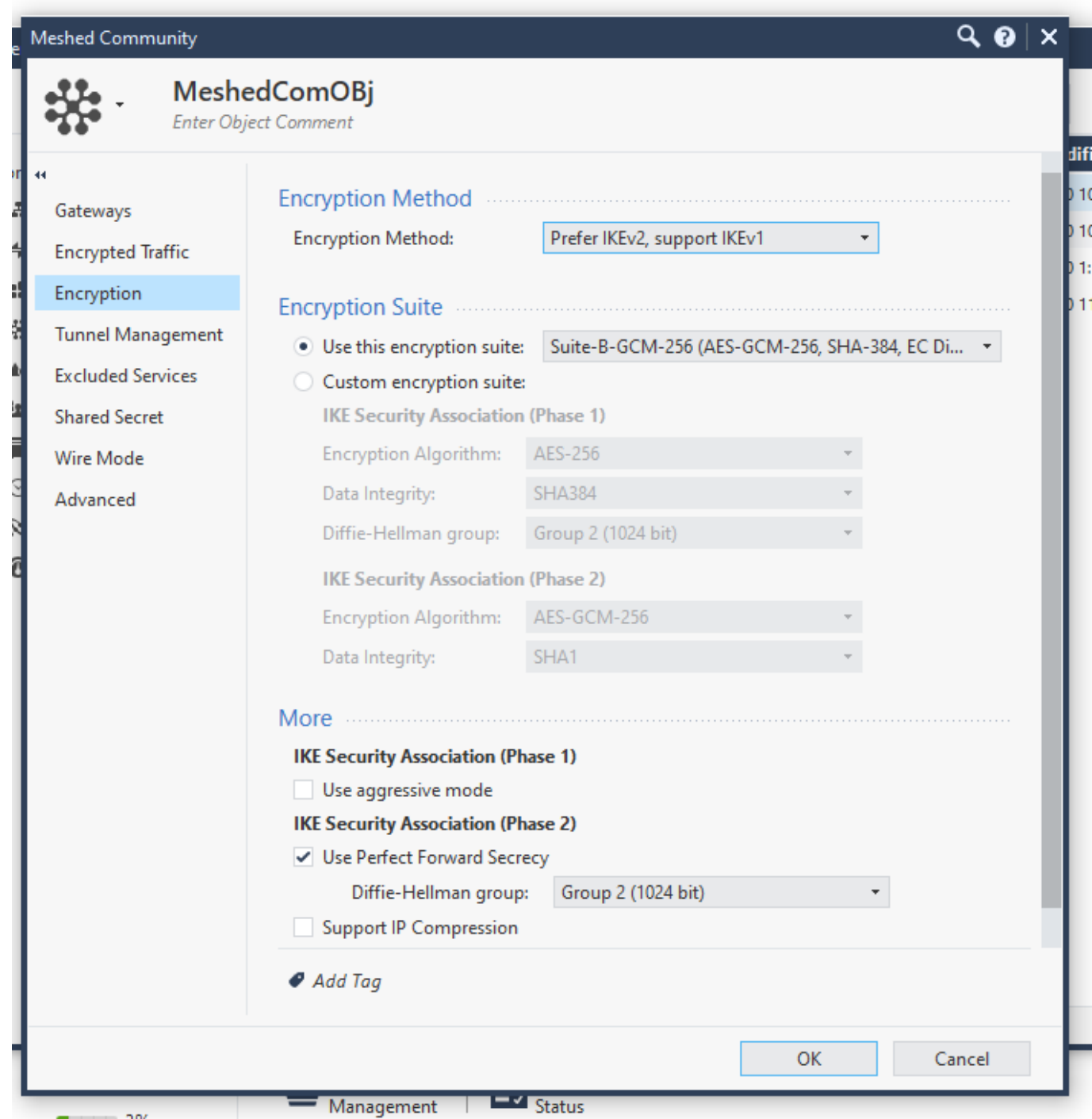
Set Specific VPN Domain for Gateway Communities:

OK

Cancel

4.3

3 / 8



4.4

No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1	allow VPN	cloudguard-gw-vm LinuxHost RaphaelPUBIP Remote DMZ	RaphaelPUBIP LinuxHost Remote DMZ	MeshedComObj	* Any	Accept	Log	* Policy Targets

4.8

Der Verbindungsaufbau konnte in folgenden Logs beobachtet werden.

**Log Details**

## Key Install

RaphaelGW (35.194.38.233) accessed cloudguard-gw-vm (10.128.0.2) Today at 3:06:25 AM

Log Info		More	
Log Server Origin	cloudguard-gw-vm (10.128.0.2)	Community	MeshedComObj
Origin	cloudguard-gw-vm	Description	
Time	Today, 3:06:25 AM	VPN Peer Gateway	RaphaelGW (35.194.38.233)
Blade	VPN	VPN Feature	IKE
Type	Log	IKE Responder Cookie	9416ad340d05cbfc
		IKE Initiator Cookie	43a2b1d7ed6498f4
		Id	0a800002-bc24-6c12-5ec1-0ca100c90...
		Id Generated By Indexer	true
		First	true
		Sequencenum	2
		Scheme	IKEv2 [NAT-T (IPv4)]
		Ike	Auth exchange: Received notification..
			<a href="#">more</a>
Traffic			
Source	RaphaelGW (35.194.38.233)		
Interface Direction	inbound		
Interface Name	daemon		
Interface	daemon		
Destination	cloudguard-gw-vm (10.128.0.2)		
Policy			
Action	Key Install		
Actions			
Report Log	<a href="#">Report Log to Check Point</a>		

**Log Details**


## Key Install

RaphaelGW (35.194.38.233) accessed cloudguard-gw-vm (10.128.0.2) Today at 3:06:25 AM

Log Info		More	
Log Server Origin	cloudguard-gw-vm (10.128.0.2)	Community	MeshedComObj
Origin	cloudguard-gw-vm	Description	
Time	Today, 3:06:25 AM	VPN Peer Gateway	RaphaelGW (35.194.38.233)
Blade	VPN	VPN Feature	IKE
Type	Log	IKE Responder Cookie	9416ad340d05cbfc
		IKE Initiator Cookie	43a2b1d7ed6498f4
		Id	0a800002-bc24-6c12-5ec1-0ca100c90001
		Id Generated By Indexer	true
		First	true
		Sequencenum	3
		Scheme	IKEv2 [NAT-T (IPv4)]
		Ike	Auth exchange: Peer Authenticated
		Methods	AES-256 + HMAC-SHA2-384, Pre-shared secret, Group 20 (384-bit random ECP group)
			<a href="#">less</a>
Traffic			
Source	RaphaelGW (35.194.38.233)		
Interface Direction	inbound		
Interface Name	daemon		
Interface	daemon		
Destination	cloudguard-gw-vm (10.128.0.2)		
Policy			
Action	Key Install		
Actions			
Report Log	<a href="#">Report Log to Check Point</a>		



Log Details

 **Key Install**

RaphaelGW (35.194.38.233) accessed cloudguard-gw-vm (10.128.0.2) Today at 3:06:25 AM

Log Info

Log Server Origincloudguard-gw-vm (10.128.0.2)

Origincloudguard-gw-vm

TimeToday, 3:06:25 AM

BladeVPN

TypeLog

Traffic

SourceRaphaelGW (35.194.38.233)

Interface Directioninbound

Interface Namedaemon

Interfacedaemon

Destinationcloudguard-gw-vm (10.128.0.2)

Policy

ActionKey Install

Actions

Report LogReport Log to Check Point

More

CommunityMeshedComObj

Description

Destination Key ID0x98f80907

VPN Peer GatewayRaphaelGW (35.194.38.233)

Source Key ID0xa6bd728f

VPN FeatureIKE

IKE Responder Cookie9416ad340d05cbfc

IKE Initiator Cookie43a2b1d7ed6498f4

Id0a800002-bc24-6c12-5ec1-0ca100c90000  
[less](#)

Id Generated By Indexertrue

Firsttrue

Sequencenum4

SchemeIKEv2 [NAT-T (IPv4)]

IkeAuth exchange: Completed successful...

MethodsAES-GCM-256, No IPComp, No ESN,

Ike Ids<192.168.27.0 - 192.168.27.255> <192.168.23.0 - 192.168.23.255>  
[less](#)

**Log Details**

**Decrypt**  
Decrypted in community MeshedComObj

**Details** | Matched Rules

**Log Info**

Origin	cloudguard-gw-vm
Time	Today, 3:06:25 AM
Blade	VPN
Product Family	Access
Type	Connection

**VPN Details**

VPN Peer Gateway	RaphaelGW (35.194.38.233)
VPN Feature	VPN
Scheme	IKE
Methods	ESP: AES-GCM-256 + PFS (group 2)
Community	MeshedComObj

**Traffic**

Source	RemoteLinuxHost (192.168.27.50)
Source Zone	External
Destination Zone	Internal
Service	echo-request (ICMP)
Interface	eth0
Destination	LinuxHost (192.168.23.50)

**Policy**

Action	Decrypt
Policy Management	cloudguard-gw-vm
Policy Name	Standard
Policy Date	Today, 2:38:03 AM
Layer Name	Network
Access Rule Name	allow VPN
Access Rule Number	1

**Actions**

Report Log [Report Log to Check Point](#)

**More**

Id	760ec72d-2200-74fb-5ec1-0ca1000000... <a href="#">more</a>
Id Generated By Indexer	false
First	true
Sequencenum	5
ICMP	Echo Request
ICMP Type	8
ICMP Code	0
Db Tag	{58D00C7E-4190-E148-9B71-901610E6... <a href="#">more</a>
Logid	0
Log Server Origin	cloudguard-gw-vm (10.128.0.2)
Description	Decrypted in community MeshedCo... <a href="#">more</a>

## IPSec Parameter

Es wurde dir vorgegebene Encryption Suit verwendet, da diese eine gute Verschlüsselung bietet und beim Konfigurieren hier Fehlerquellen ausgeschlossen werden.