

# Module 11 IPsec VPN

Module 11. IPSec VPN

Instructor: Kim Winfield

# Objectives

- Describe an IKE/IPSec key exchange for site to site VPN connectivity
- VPN Community Functionality
- Configuration Steps for Site to Site and Client to Site VPN

# IPsec

- Ipsec is not one protocol but a suite of protocols
  - IPsec crates a boundary between unprotected and protected interfaces
- Security Protocols
- Security Associations
- Key Management (IKE)
- Cryptographisd Algorithms

# Ipsec Security Protocols and Cryptographic Algorithms

- Authentication Header (AH)
- Encapsulating Security Payload (ESP)
- IPsec implementations **MUST** support ESP and **MAY** support AH
  
- IKE
- IKEv2

# Ipssec Security Associations

- IKE SA
- IP

# Check Point VPN

- Site to Site and Remote Access for Users
- Simplified and Traditional Mode VPN's
- VPN Communities

Check Point Gateway - R80.10-GW

**General Properties**

Machine

Name: R80.10-GW

IPv4 Address: 10.1.1.1  ☐ Dynamic

IPv6 Address:

Comment:

Secure Internal Communication: Trust established

Platform

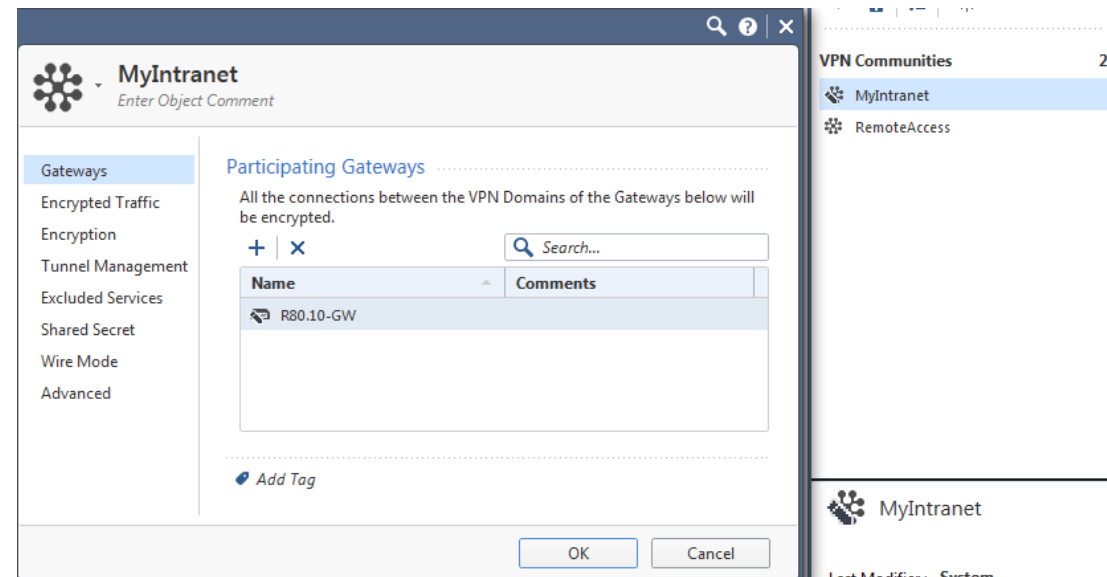
Hardware: Open server Version: R80.10 OS: Gaia

Network Security (7) Management (0)

<input checked="" type="checkbox"/> Firewall	<input checked="" type="checkbox"/> IPS	Advanced <input checked="" type="checkbox"/> D <input checked="" type="checkbox"/> S <input type="checkbox"/> Q <input type="checkbox"/> W
<input checked="" type="checkbox"/> IPSec VPN	<input type="checkbox"/> Anti-Bot	
<input type="checkbox"/> Policy Server	<input type="checkbox"/> Anti-Virus	
<input checked="" type="checkbox"/> Mobile Access	<input type="checkbox"/> Threat Emulation	
<input checked="" type="checkbox"/> Application Control	<input type="checkbox"/> Threat Extraction	
<input checked="" type="checkbox"/> IIRI Filtering	<input type="checkbox"/> Anti-Spam & Email Security	

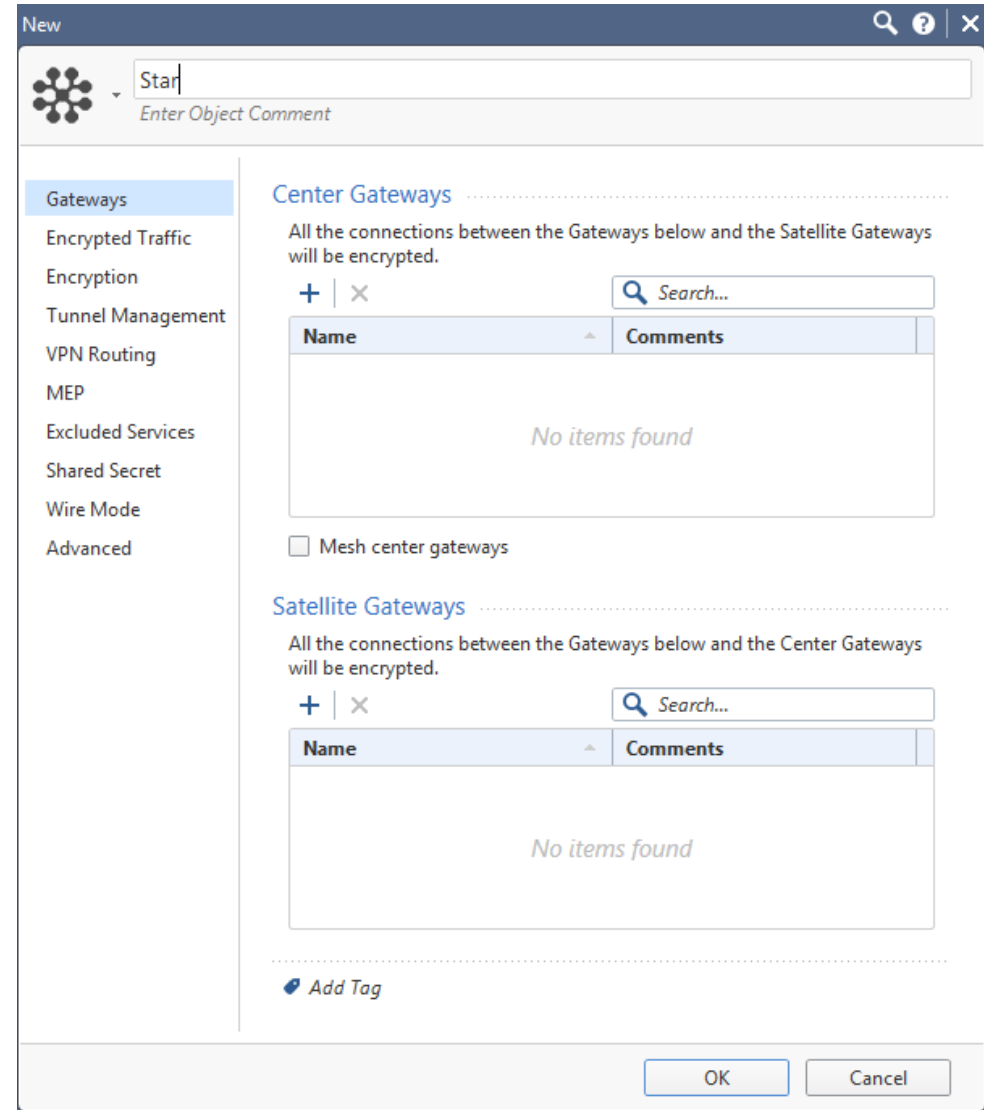
# Meshed Communities

- Multiple Gateways all connected to each other
- Number of Tunnels of Gateways is N-1
  - Ex. 4 Gateways in the Community each gateway would potentially have 3 tunnels
- Excluded Services



# Star Community

- Center Gateway
- Satellite Gateway
- VPN Routing



New

Star | Enter Object Comment

**Gateways**

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

**Center Gateways**

All the connections between the Gateways below and the Satellite Gateways will be encrypted.

+ | x Search...

Name	Comments
No items found	

☐ Mesh center gateways

**Satellite Gateways**

All the connections between the Gateways below and the Center Gateways will be encrypted.

+ | x Search...

Name	Comments
No items found	

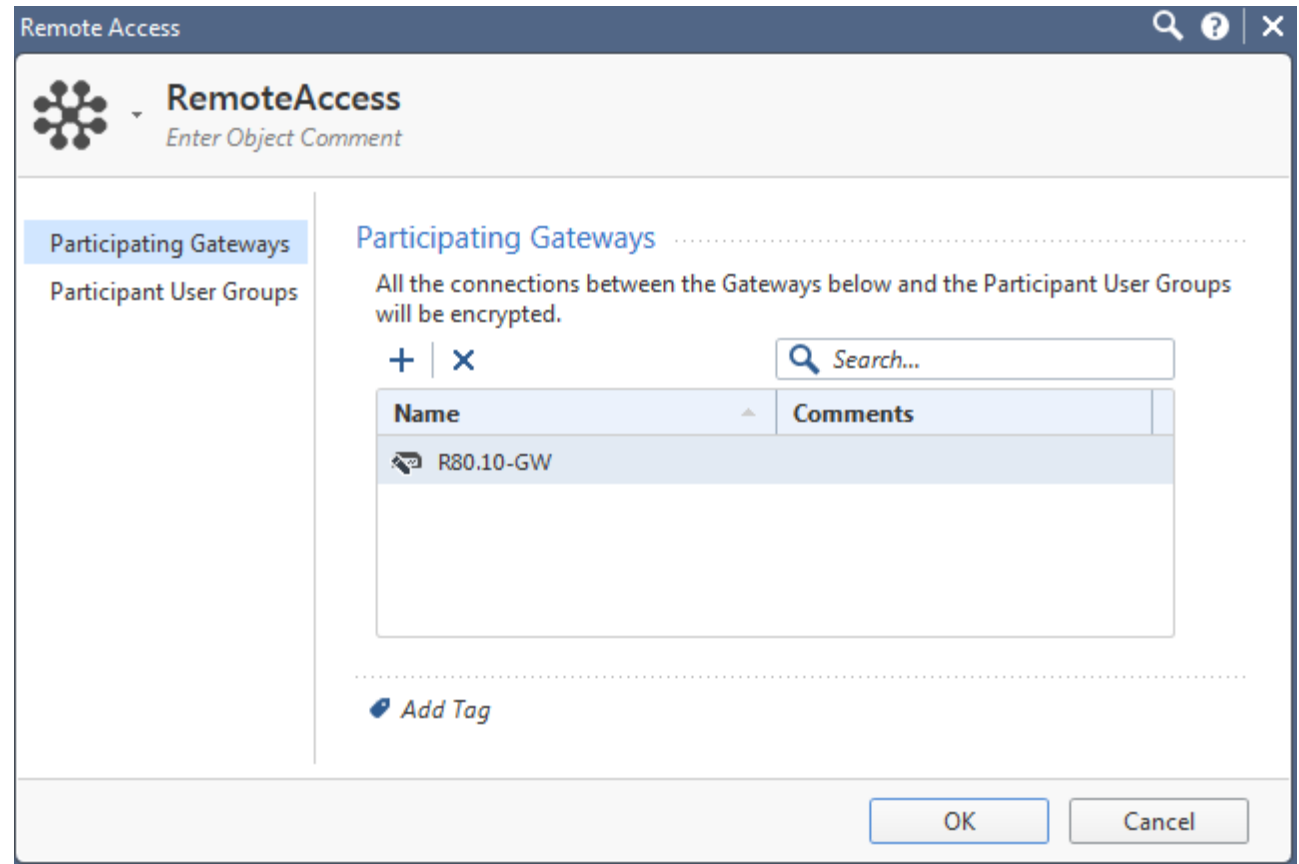
Add Tag

OK Cancel




# Remote Access Community

- Participating Gateways
- Participating User Groups



The screenshot shows a software window titled "Remote Access" with a search, help, and close icon bar. The main area has a header with a network icon, the title "RemoteAccess", and a subtitle "Enter Object Comment". Below this is a sidebar with two tabs: "Participating Gateways" (selected) and "Participant User Groups". The main content area under the "Participating Gateways" tab contains the text "All the connections between the Gateways below and the Participant User Groups will be encrypted." followed by a "+ | x" button and a search bar labeled "Search...". Below these is a table with two columns: "Name" and "Comments". The table contains one entry: "R80.10-GW" with a small icon to its left. At the bottom of the main area is an "Add Tag" button. The dialog box concludes with "OK" and "Cancel" buttons at the bottom right.

Name	Comments
 R80.10-GW	

# Configuring a Site to Site VPN

- Use Meshed or Star Community
- Add Gateways with their encryption domain defined
- Specify encryption properties in the community
- Create rules in the rulebase

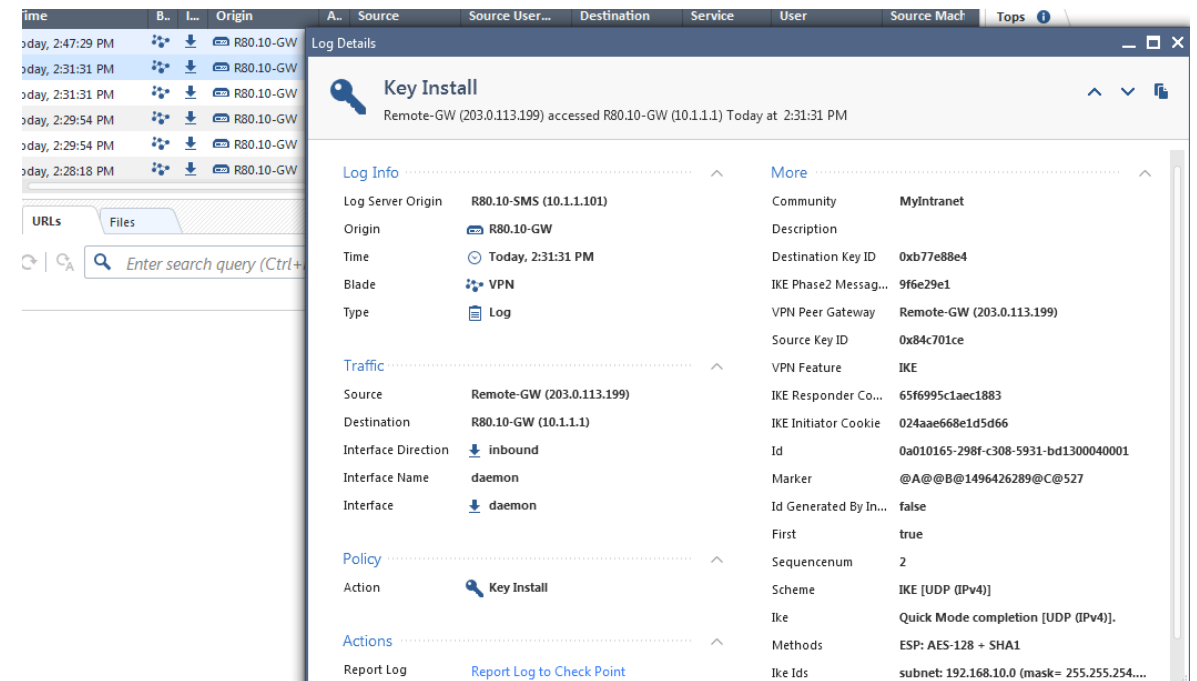
# Configuring a Remote Access VPN (Client to Site VPN)

- Add the security gateway to the Remote Access VPN Community
- Add user groups to the community
- Create rules on the gateway allowing the user group in the community access to resources inside the encryption domain

# The Encrypted Tunnel (SmartLog)

- Phase 1 key exchange in the logs
- Phase 2 key exchange in the logs

• <https://youtu.be/fNJCMjlYg7g>



# Summary

- Described an IKE/IPSec key exchange for site to site VPN connectivity
- Explained VPN Community Functionality
- Configured a Site to Site, and Client to Site, VPN

# Bibliography

*Check Point R80.10 Site to Site VPN Admin Guide California: USA*

*Check Point R80.10 Remote Access VPN Admin Guide California: USA*