

Policy based IPsec VPN (IKEv1)

What will be done

- Setup a IKEv1 Remote Access VPN with PSK + XAuth Authentication
- Policy-based Split Tunneling

Prerequisites

- Static IP
- Port 500 (UDP) for IKE open
- Port 4500 (UDP) for NAT-T open
- ESP open
- User Group for XAuth

I'll be referring to this Tunnel as VPN-RA-Test. Give it whatever name you need!

1. Creating a VPN Tunnel

1. Go to VPN - IPsec Tunnels
2. Click Create New and select IPsec Tunnel
 - Template Type: Custom
 - Name: VPN-RA

1.1. Network Settings

1. Set *IP Version* to **IPv4**
2. Set *Remote Gateway* to **Dialup User**
 - Interface: Your WAN Interface
3. Disable *Local Gateway*
4. Enable *Mode Config*
5. Set *Client Address Range* manually or Assign Range Address Object
6. Set *Subnet Mask* to prevent Inter-Device Communication inside the Tunnel or specify explicitly
7. Set your preferred DNS Server.

8. Enable *Enable IPv4 Split Tunnel*
 - Select your Address Object representing the Networks that should be accessible
9. Disable *IPv6 Mode Config - Client Address Range*
10. Set *NAT Traversal* to **Enable**
11. Set *Dead Peer Detection* to **On Idle**

Network

IP Version **IPv4** IPv6

Remote Gateway Dialup User ▼

Interface FB WAN (wan1) ▼

Local Gateway

Mode Config

Use system DNS in mode config

Assign IP From Address/Address Group ▼

IPv4 mode config

Client Address Range RNG-RA-VPN ▼

Subnet Mask 255.255.255.255

DNS Server 0.0.0.0

Enable IPv4 Split Tunnel

Accessible Networks GRP-ALLOWED-VPN ▼

IPv6 mode config

Client Address Range

Prefix Length 128

DNS Server ::

Enable IPv6 Split Tunnel

NAT Traversal **Enable** Disable Forced

Dead Peer Detection Disable **On Idle** On Demand

DPD retry count 3

DPD retry interval 60 s

Forward Error Correction Egress Ingress

Advanced...

1.2. Authentication

1. Set *Method* to **Pre-shared Key**
2. Write your PSK to the *Pre-shared Key* Input Field

3. Set *IKE - Version* to **1**
4. Set *IKE - Mode* to **Agressive**
5. Set *Peer Options - Accept Types* to **Any Peer ID**

Authentication

Method:

Pre-shared Key:

Password must conform to the following rules:

- 8 Minimum length
- 4 Minimum number of new characters

IKE

Version:

Mode: Aggressive Main (ID protection)

Peer Options

Accept Types:

You can set a Peer ID here to differentiate different Tunnels that might share Settings and/or PSKs

1.3. Phase 1 Proposal

Remove all existing Phase 1 Proposals beforehand by clicking the **X** Button the right side

1. Add the following Proposals
 - Encryption: **AES256**, Authentication: **SHA256**
 - Encryption: **AES256**, Authentication: **SHA1**
2. Check *Diffie-Hellmann Groups* **14, 19, 20**
3. Set *Key Lifetime (seconds)* to **28800**

Phase 1 Proposal

Encryption	<input type="text" value="AES256"/>	Authentication	<input type="text" value="SHA256"/>	<input type="button" value="X"/>
Encryption	<input type="text" value="AES256"/>	Authentication	<input type="text" value="SHA1"/>	<input type="button" value="X"/>

Diffie-Hellman Groups

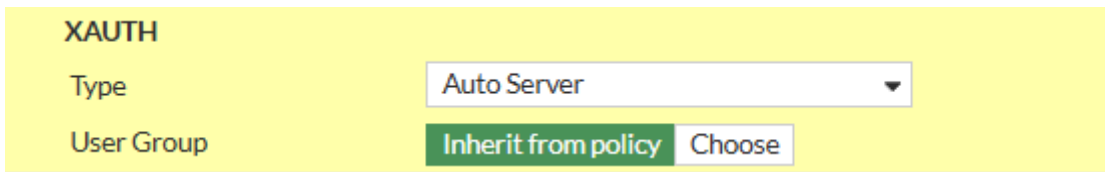
<input type="checkbox"/>	32	<input type="checkbox"/>	31	<input type="checkbox"/>	30	<input type="checkbox"/>	29	<input type="checkbox"/>	28	<input type="checkbox"/>	27
<input type="checkbox"/>	21	<input checked="" type="checkbox"/>	20	<input checked="" type="checkbox"/>	19	<input type="checkbox"/>	18	<input type="checkbox"/>	17	<input type="checkbox"/>	16
<input type="checkbox"/>	15	<input checked="" type="checkbox"/>	14	<input type="checkbox"/>	5	<input type="checkbox"/>	2	<input type="checkbox"/>	1		

Key Lifetime (seconds):

Local ID:

1.4. XAuth

1. Set *Type* to **Auto Server**
2. Set *User Group* to **Inherit from policy**



XAUTH

Type: Auto Server

User Group: Inherit from policy Choose

1.5. Phase 2 Selectors

There should only be one Phase 2 Selector pre-existing with the Name of the Tunnel you specified

1.5.1 Edit Default Phase 2 Selector

1. Click on the Pen Icon at the Right Side of the Row to Edit
2. Expand the Advanced Menu by clicking on *Advanced*

1. Set *Name* to **VPN-RA-P2**
2. Set *Local Address* to Type **Subnet** and Value
3. Set *Remote Address* to Type **Subnet** and Value
4. Delete all existing Phase 2 Proposals
5. Add the following Phase 2 Proposals (same as with Phase 1)
 - Encryption: **AES256**, Authentication: **SHA256**
 - Encryption: **AES256**, Authentication: **SHA1**
6. Enable *Enable Replay Detection*
7. Enable *Enable Perfect Forward Secrecy (PFS)*
8. Check *Diffie-Hellmann Groups* **14, 19, 20**
9. Enable *Local Port*
10. Enable *Remote Port*
11. Enable *Protocol*
12. Set *Key Lifetime* to **Seconds** and set

New Phase 2 🔍 ↻

Name

Comments

Local Address

Remote Address

Advanced...

Phase 2 Proposal

Encryption	<input type="text" value="AES128"/>	Authentication	<input type="text" value="SHA1"/>	<input type="button" value="X"/>
Encryption	<input type="text" value="AES256"/>	Authentication	<input type="text" value="SHA1"/>	<input type="button" value="X"/>
Encryption	<input type="text" value="AES128"/>	Authentication	<input type="text" value="SHA256"/>	<input type="button" value="X"/>
Encryption	<input type="text" value="AES256"/>	Authentication	<input type="text" value="SHA256"/>	<input type="button" value="X"/>
Encryption	<input type="text" value="AES128GCM"/>			<input type="button" value="X"/>
Encryption	<input type="text" value="AES256GCM"/>			<input type="button" value="X"/>
Encryption	<input type="text" value="CHACHA20POLY1305"/>			<input type="button" value="X"/>

Enable Replay Detection

Enable Perfect Forward Secrecy (PFS)

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 checked="" type="checkbox"/> 14	<input checked="" type="checkbox"/> 5	<input type="checkbox"/> 2	<input type="checkbox"/> 1	

Local Port All

Remote Port All

Protocol All

Autokey Keep Alive

Key Lifetime

Seconds

2. Create Policies

For a Policy-based IPsec VPN you need Policies that allow both the Address Range of the Clients and the Users to access the Networks you need.

Depending on the Networks you specified, you need Policies from WAN->LAN and maybe WAN->OtherLAN.

2.1 Example Policy

This is an Example Policy from WAN to LAN

I use Address Objects here that i also specified in the Tunnel Configuration.

Note: You cannot specify Subnet Address Objects in the Tunnel Configuration, only IP Ranges. But if the Subnet contains the IP Range, this works fine. Example: Range is 192.168.10.100 - 192.168.10.200 so a Subnet of 192.168.10.0/24 would work just fine

ID	17
Name	Allow-VPN-RA-to-LAN
Incoming Interface	<div> VPN-RA-IOS ✕</div> <div> VPN-RA-WIN ✕</div> <div style="text-align: center;">+</div>
Outgoing Interface	<div> LAN (internal) ✕</div> <div style="text-align: center;">+</div>
Source	<div> NET-RA-VPN ✕</div> <div> VPN Users ✕</div> <div style="text-align: center;">+</div>
Negate Source	<input type="checkbox"/>
Destination	<div> GRP-ALLOWED-VPN ✕</div> <div style="text-align: center;">+</div>
Negate Destination	<input type="checkbox"/>
Schedule	<div> always ▼</div>
Service	<div> GRP-RA-VPN ✕</div> <div style="text-align: center;">+</div>
Action	<div><input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input type="checkbox"/> IPsec</div>
Inspection Mode	<div><input checked="" type="checkbox"/> Flow-based <input type="checkbox"/> Proxy-based</div>

Here my Policies allows Traffic from the VPN Tunnel Interfaces (created when creating the Tunnel) to the LAN Interface. As here, Authentication is Policy-based, for the Source we also need the User/User Groups.

Destination is a Group i created that is the same i used for the *Split Tunneling - Accessible Networks*

You can also specify a Schedule or Service if you want to.

You need Policies in both Directions for them to work correctly!

Revision #3

Created 11 September 2025 11:44:00 by Oliver Karger

Updated 11 September 2025 12:10:16 by Oliver Karger