IKEv2 VPN

General Use IKEv2 VPN for FortiClient

FortiGate Configuration

Phase 1

```
edit "VPN-RA-FC"
    set type dynamic
    set interface "wan1"
    set ike-version 2
    set peertype any
    set net-device disable
    set mode-cfg enable
    set ipv4-dns-server1 10.0.0.254
    set internal-domain-list "<removed>"
    set proposal aes256gcm-prfsha384 aes256gcm-prfsha256 aes256-sha256
    set localid "<removed>"
    set dpd on-idle
    set dhgrp 21 19 14
    set eap enable
    set eap-identity send-request
    set authusrgrp "VPN Users"
    set assign-ip-from name
    set ipv4-split-include "GRP-VPN-ACCESS"
    set ipv4-name "RNG-RA-VPN-Clients"
    set psksecret <removed>
    set dpd-retryinterval 60
next
```

- `internal-domain-list` is a List of DNS Domains that should be resolveable by the connected Device (internal Domains only)
- `localid` is the public DNS Domain of the Firewall (required)
- `psksecret` is the Pre-Shared-Key

Phase 2

```
edit "VPN-RA-FC-P2-DEFAULT"
    set phase1name "VPN-RA-FC"
    set proposal aes256gcm aes256-sha256
    set dhgrp 21 19 14
    set keepalive enable
    set keylifeseconds 3600
next
```

Policies

```
config firewall policy
    edit 18
        set name "Allow-VPN-RA-to-LAN"
        set uuid b88f102a-dff6-51f0-6157-49a1d9450327
        set srcintf "VPN-RA-APPLE" "VPN-RA-WINDOWS" "VPN-RA-FC"
        set dstintf "VLAN-LAN-100" "SSID-WLAN-TUN" "SSID-IOT-TUN" "VLAN-DMZ-200"
        set action accept
        set srcaddr "RNG-RA-VPN-Clients"
        set dstaddr "GRP-VPN-ACCESS"
        set schedule "always"
        set service "ALL"
    next
    edit 20
        set name "Allow-VPN-RA-to-WAN"
        set uuid ee369aec-dff9-51f0-c276-83956b56cd9c
        set srcintf "VPN-RA-APPLE" "VPN-RA-FC" "VPN-RA-WINDOWS"
        set dstintf "wan1"
        set action accept
        set srcaddr "RNG-RA-VPN-Clients"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
```

```
        set nat enable
    next
end
```

Client Configuration

iOS FortiClient App

Secure Protocol	IKEv2 VPN
Name	<Name>
Server Address	Public DNS Domain (same as localid in Tunnel Config)
Authentication Method	Pre-shared Key
Pre-shared Key Secret	PSK
EAP-AUTH	Enabled
Local ID	empty
Remote-ID	Public DNS Domain (same as localid in Tunnel Config)
Phase 1 Encryption	AES256
Phase 1 Authentication	SHA256
Phase 1 DH GRoup	14
Phase 1 Key Lifetime	86400
Phase 1 Encryption	AES256
Phase 1 Authentication	SHA256
Phase 1 DH GRoup	14
Phase 1 Key Lifetime	43200
DPD	enabled
PFS	enabled
Username	Client Username (User in FortiGate)

Revision #2
Created 15 March 2026 13:35:12 by Oliver Karger
Updated 15 March 2026 13:41:18 by Oliver Karger