

How to configure multiple FortiClients (remote VPN users) to a dial-in FortiGate gateway Step-by-step guide

The following describes how to configure two different VPN remote users to have access to two different networks on separate Fortigate interfaces (Internal and DMZ). A similar configuration could be applied so that the two users access two different subnets on the same Fortigate interface.

The configuration and GUI snapshots are based on FortOS v2.50 and FortiClient v1.0, but could be also applied to v2.80 and v1.2, since the basis of the configuration remains the same. v2.80 introduces some slight GUI changes.

A collection of debug log outputs are also supplied. They were taken simultaneously from both the FortiClient and Fortigate, under situations where connections are unsuccessful. These may assist in troubleshooting connection failures. The following Fortigate CLI commands were used to activate the debugging:

```
v2.50
set deb en
diag deb appl ike 2
```

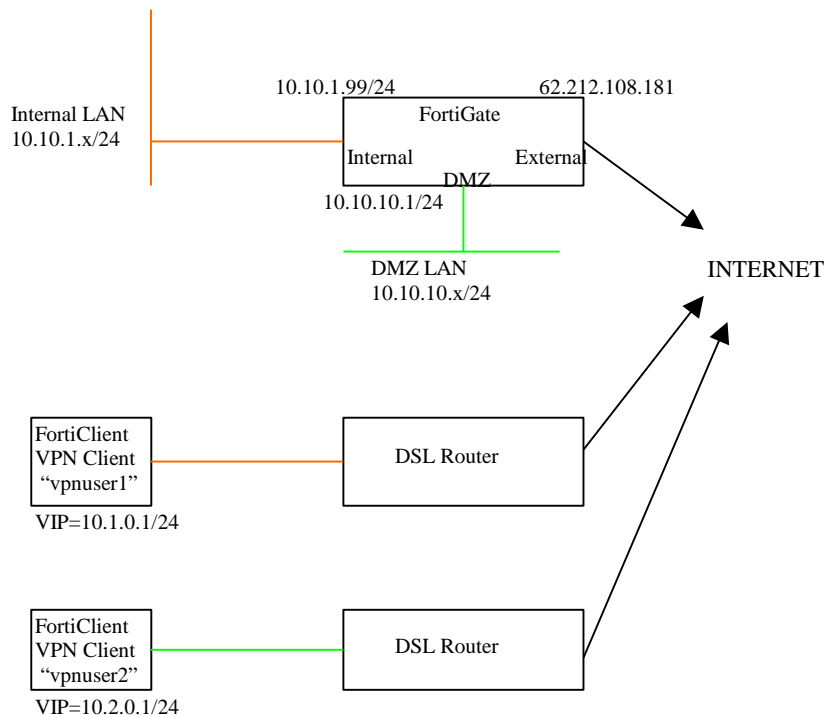
```
v2.80
diag deb en
diag deb appl ike 2
```

Each element in the VPN configuration builds upon another. For example, you must create the User before you can add it to the User Group etc.

Because of these dependencies, the order for configuring VPN in the FortiGate is as follows:

- 1) Users
- 2) User Groups
- 3) IPsec Phase 1
- 4) IPsec Phase 2
- 5) Firewall Addresses
- 6) Firewall Policies

Network diagram of example described below:



Additional remote clients that are configured, require unique VIP addresses which don't conflict with each other, but that remain within the appropriate subnets.

FortiGate dial-in gateway configuration: Defined network interfaces.

The screenshot shows the Fortinet Firewall web interface in Microsoft Internet Explorer. The browser address bar displays `https://10.10.1.99/theme1/index?login=1`. The interface features a sidebar menu on the left with categories: System, Firewall, User, VPN, NIDS, Anti-Virus, Web Filter, Email Filter, and Log&Report. The main content area is titled "Zone" and contains a table of defined network interfaces. The table has columns for Name, IP, Netmask, Zone, Access, Status, and Modify. Three interfaces are listed: "internal" (IP: 10.10.1.99, Netmask: 255.255.255.0, Access: HTTPS,PING,SSH), "external" (IP: 62.212.108.181, Netmask: 255.255.255.255, Access: PING), and "dmz" (IP: 10.10.10.1, Netmask: 255.255.255.0, Access: HTTPS,PING,SSH). All interfaces have a green status icon. Below the table is a "New VLAN" button. The browser status bar at the bottom shows "Done" and "Internet".

Name	IP	Netmask	Zone	Access	Status	Modify
internal	10.10.1.99	255.255.255.0		HTTPS,PING,SSH	⬆	
external	62.212.108.181	255.255.255.255		PING	⬆	
dmz	10.10.10.1	255.255.255.0		HTTPS,PING,SSH	⬆	

[New VLAN](#)

Each Locally defined user is configured with a unique name and password (password = Pre-shared key on VPN client), and each user will access a different network on a different interface).

The screenshot shows the Fortinet Firewall management interface in Microsoft Internet Explorer. The browser address bar shows `https://10.10.1.99/theme1/index?login=1`. The interface features a sidebar menu on the left with categories: System, Firewall, User, VPN, NIDS, Anti-Virus, and Web Filter. The 'User' category is expanded, and 'User Group' is selected. The main content area is titled 'User Group' and contains a table with the following data:

Group Name	Members	Modify
vpngroup1	vpnuser1	
vpngroup2	vpnuser2	

Below the table is a 'New' button. The status bar at the bottom of the browser shows 'Done' and 'Internet'.

The screenshot shows the Fortinet Firewall management interface in Microsoft Internet Explorer, displaying the 'Manual Key' configuration page. The browser address bar shows `https://10.10.1.99/theme1/index?login=1`. The sidebar menu is the same as in the previous screenshot, with 'VPN' expanded and 'IPSEC' selected. The main content area has tabs for 'Manual Key', 'Phase 2', 'Phase 1', 'Concentrator', and 'Dialup Monitor'. The 'Manual Key' tab is active, showing a table with the following data:

Gateway Name	Gateway IP	Mode	Encryption Algorithm	Modify
Dial-in-gateway-2	Dialup	Aggressive	3DES-SHA1	
Dial-in-gateway-1	Dialup	Aggressive	3DES-SHA1	

Below the table is a 'New' button. The status bar at the bottom of the browser shows 'Done' and 'Internet'.

Each Phase 1 is linked to a unique User Group, which is in-turn linked to a unique User. The Pre-shared Key field is greyed-out and not used below, since authentication will be done via a dialup group. There is no need to have more than one Encryption/Authentication and DH proposal in both Phase1 and Phase 2, since we will also configure the VPN clients with the same settings.

The screenshot shows the Fortinet management console interface for editing a VPN Gateway. The left sidebar contains a navigation menu with categories: System, Firewall, User, VPN, NIDS, Anti-Virus, Web Filter, Email Filter, and Log&Report. The main content area is titled 'Edit VPN Gateway' and has tabs for Manual Key, Phase 2, Phase 1, Concentrator, and Dialup Monitor. The configuration for 'Dial-in-gateway-1' is as follows:

- Gateway Name:** Dial-in-gateway-1
- Remote Gateway:** Dialup User
- Mode:** Aggressive (selected), Main (ID protection)
- P1 Proposal:** 1 - Encryption: 3DES, Authentication: SHA1
- DH Group:** 1, 2, 5 (all selected)
- Keylife:** 28800 (120-172800 seconds)
- Authentication Method:** Preshared Key
- Pre-shared Key:** [Greyed-out field]
- Local ID:** [Optional field]
- Advanced Options:** (Dialup Group, Peer, XAUTH, Nat Traversal, DPD)
- Peer Options:** Accept peer ID in dialup group (vpngroup1 selected)
- XAuth:** Disable (selected), Enable as Client, Enable as Server
- Nat-traversal:** Enable (checked)
- Keepalive Frequency:** 5 (0-900 seconds)
- Dead Peer Detection:** Enable (checked)

The screenshot shows the Fortinet management console interface for editing a second VPN Gateway. The left sidebar is identical to the first screenshot. The main content area is titled 'Edit VPN Gateway' and has tabs for Manual Key, Phase 2, Phase 1, Concentrator, and Dialup Monitor. The configuration for 'Dial-in-gateway-2' is as follows:

- Gateway Name:** Dial-in-gateway-2
- Remote Gateway:** Dialup User
- Mode:** Aggressive (selected), Main (ID protection)
- P1 Proposal:** 1 - Encryption: 3DES, Authentication: SHA1
- DH Group:** 1, 2, 5 (all selected)
- Keylife:** 28800 (120-172800 seconds)
- Authentication Method:** Preshared Key
- Pre-shared Key:** [Greyed-out field]
- Local ID:** [Optional field]
- Advanced Options:** (Dialup Group, Peer, XAUTH, Nat Traversal, DPD)
- Peer Options:** Accept peer ID in dialup group (vpngroup2 selected)
- XAuth:** Disable (selected), Enable as Client, Enable as Server
- Nat-traversal:** Enable (checked)
- Keepalive Frequency:** 5 (0-900 seconds)
- Dead Peer Detection:** Enable (checked)

Each Phase 2 is linked to a unique Phase 1.

The screenshot shows the Fortinet VPN configuration interface. The left sidebar contains a navigation menu with categories: System, Firewall, User, VPN, NIDS, Anti-Virus, Web Filter, Email Filter, and Log&Report. The VPN section is expanded, showing sub-items: IPSEC, PPTP, L2TP, and Certificates. The main content area is titled 'Manual Key' and contains a tabbed interface with 'Phase 2' selected. A table lists two tunnels:

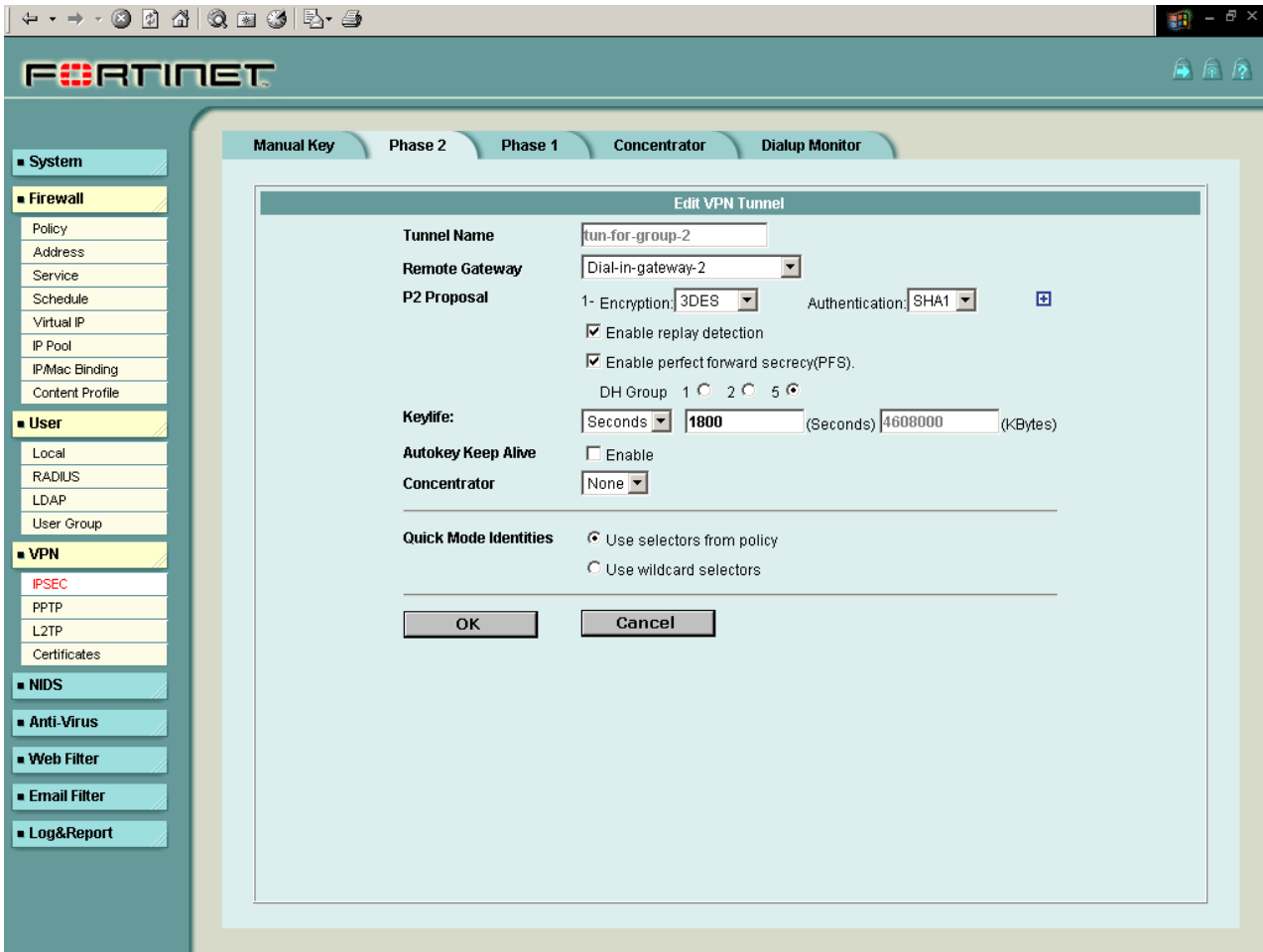
Tunnel Name	Remote Gateway	Lifetime(sec.kb)	Status	Timeout	Modify
tun-for-group-2	Dialup	1800/N/A	N/A	N/A	
tun-for-group-1	Dialup	1800/N/A	N/A	N/A	

Below the table is a 'New' button.

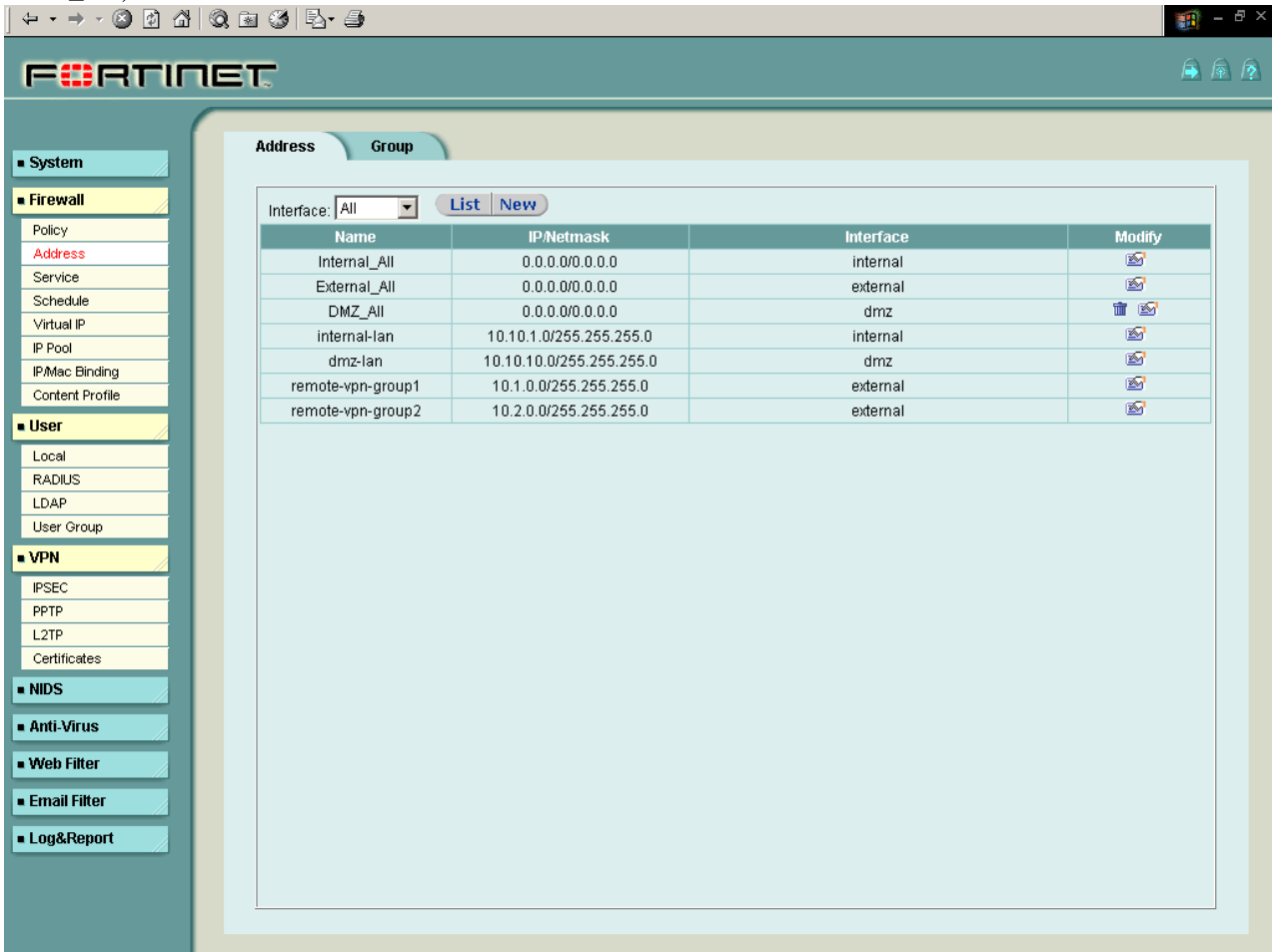
The screenshot shows the 'Edit VPN Tunnel' dialog box in the Fortinet VPN configuration interface. The dialog is titled 'Edit VPN Tunnel' and contains the following fields and options:

- Tunnel Name:** tun-for-group-1
- Remote Gateway:** Dial-in-gateway-1
- P2 Proposal:** 1- Encryption: 3DES, Authentication: SHA1
- Enable replay detection
- Enable perfect forward secrecy(PFS).
- DH Group:** 1 2 5
- Keylife:** Seconds: 1800, (Seconds): 4608000, (KBytes):
- Autokey Keep Alive:** Enable
- Concentrator:** None
- Quick Mode Identities:** Use selectors from policy, Use wildcard selectors

At the bottom of the dialog are 'OK' and 'Cancel' buttons.



Specific Internal, DMZ and External VIP address ranges must be specified (must not use Internal_All, External_All, or DMZ_All).



Each Firewall Policy is linked to a unique Phase 2 and a unique Address range (or interface). Below is the DMZ->External Policy.

Policy

#	ID	Source	Dest	Schedule	Service	Action	Enable	Config
1	3	dmz-lan	remote-vpn-group1	Always	ANY	ENCRYPT	<input checked="" type="checkbox"/>	

Policy

Edit Policy

Source: dmz-lan

Destination: remote-vpn-group1

Schedule: Always

Service: ANY

Action: ENCRYPT

VPN Tunnel: tun-for-group-1

Allow inbound Inbound NAT

Allow outbound Outbound NAT

Traffic Shaping

Guaranteed Bandwidth: 0 (KBytes/s)

Maximum Bandwidth: 0 (KBytes/s)

Traffic Priority: High

Anti-Virus & Web filter

Content Profile: Strict

Log Traffic

Comments: maximum 63 characters

Below is the Internal->External Firewall Policy.

The screenshot shows the Fortinet Firewall web interface in Microsoft Internet Explorer. The browser address bar shows `https://10.10.1.99/theme1/index?login=1`. The interface features a sidebar menu on the left with categories: System, Firewall, User, VPN, NIDS, Anti-Virus, and Web Filter. The 'Firewall' section is expanded, and the 'Policy' tab is selected. The main content area displays a table of policies:

#	ID	Source	Dest	Schedule	Service	Action	Enable	Config
1	4	internal-lan	remote-vpn-group2	Always	ANY	ENCRYPT	<input checked="" type="checkbox"/>	
2	1	Internal_All	External_All	Always	ANY	ACCEPT	<input checked="" type="checkbox"/>	

Below the table is a 'New' button.

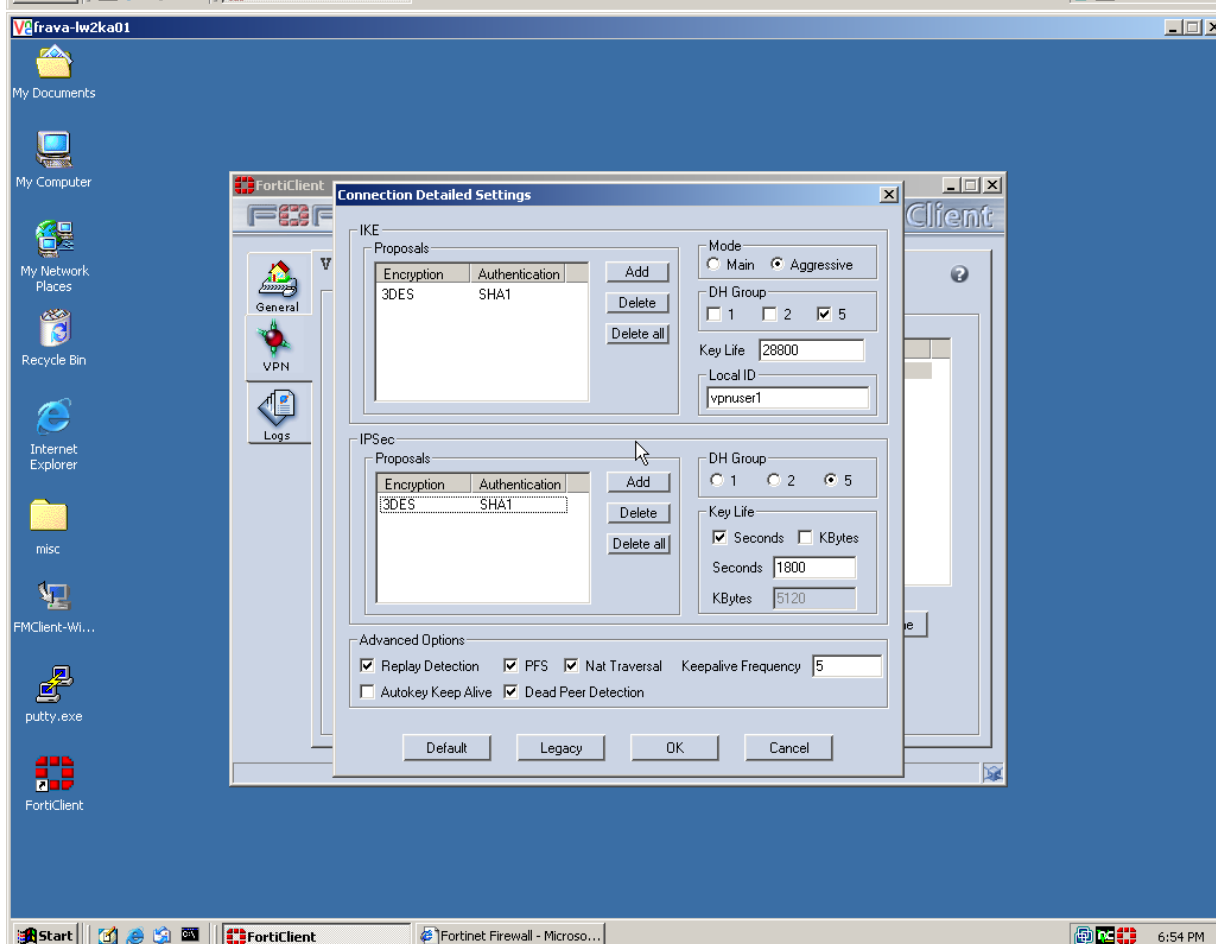
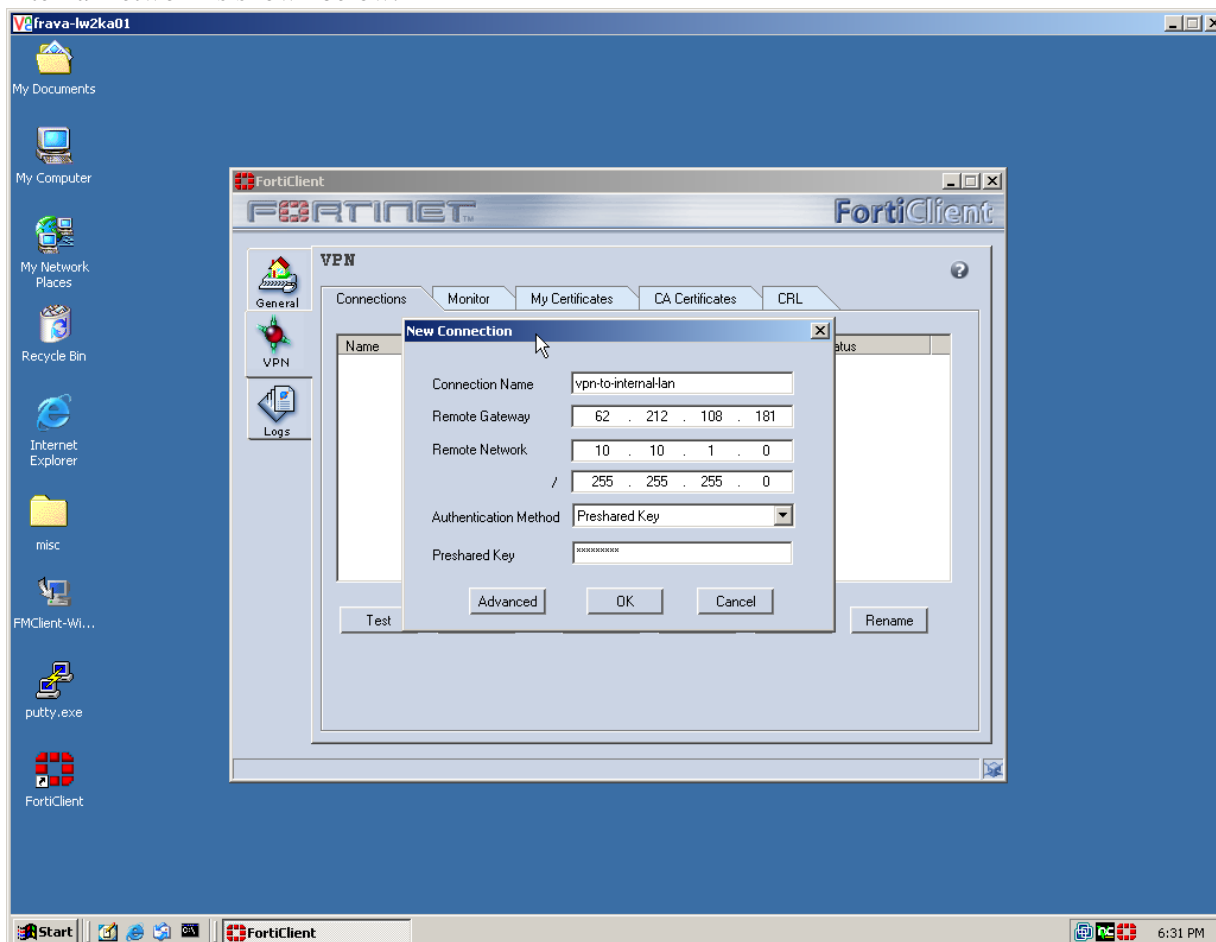
The screenshot shows the 'Edit Policy' configuration window for the selected policy. The window is titled 'Edit Policy' and contains the following settings:

- Source:** internal-lan
- Destination:** remote-vpn-group2
- Schedule:** Always
- Service:** ANY
- Action:** ENCRYPT
- VPN Tunnel:** tun-for-group-2
- Allow inbound
- Inbound NAT
- Allow outbound
- Outbound NAT
- Traffic Shaping
 - Guaranteed Bandwidth: 0 (KBytes/s)
 - Maximum Bandwidth: 0 (KBytes/s)
 - Traffic Priority: High
- Anti-Virus & Web filter
 - Content Profile: Strict
- Log Traffic
- Comments:** maximum 63 characters

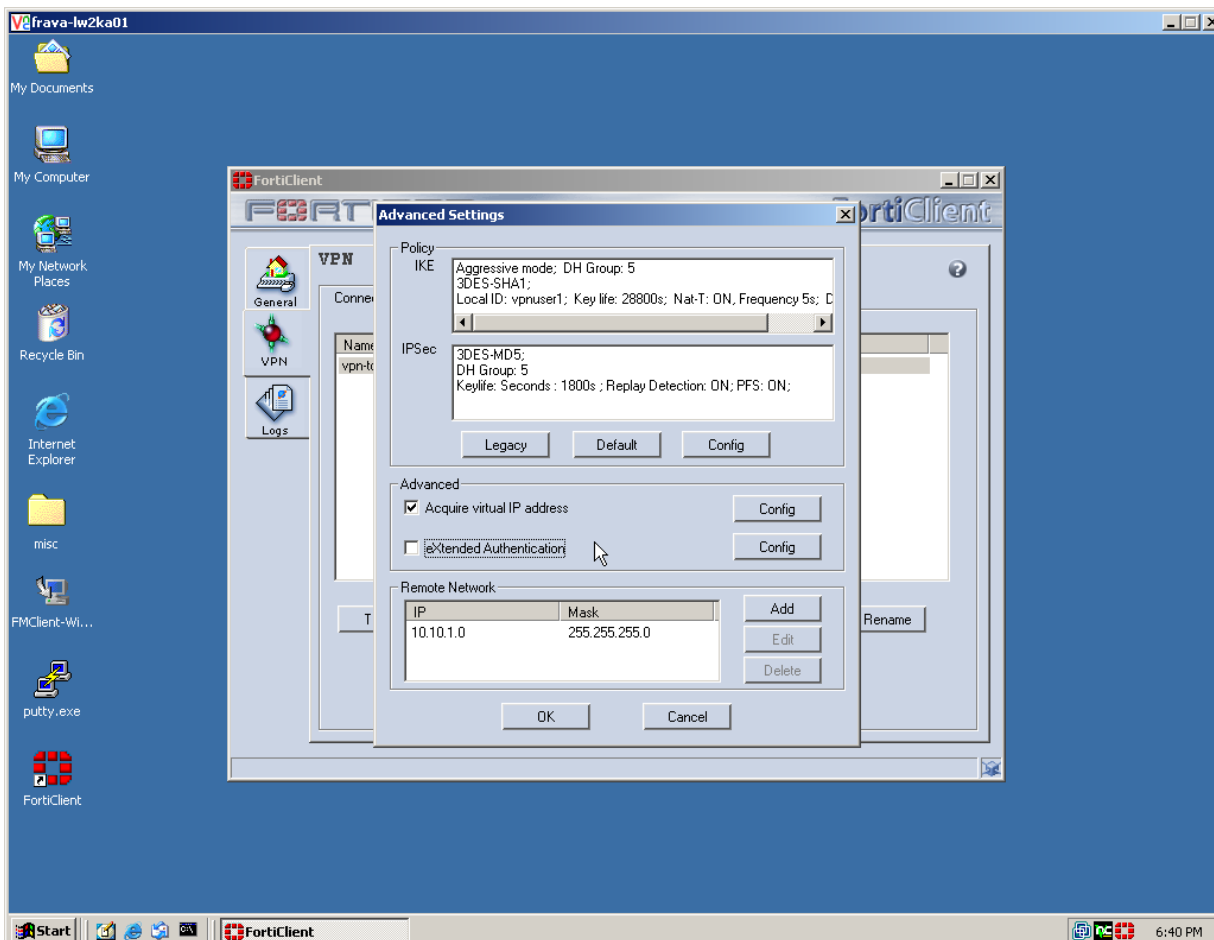
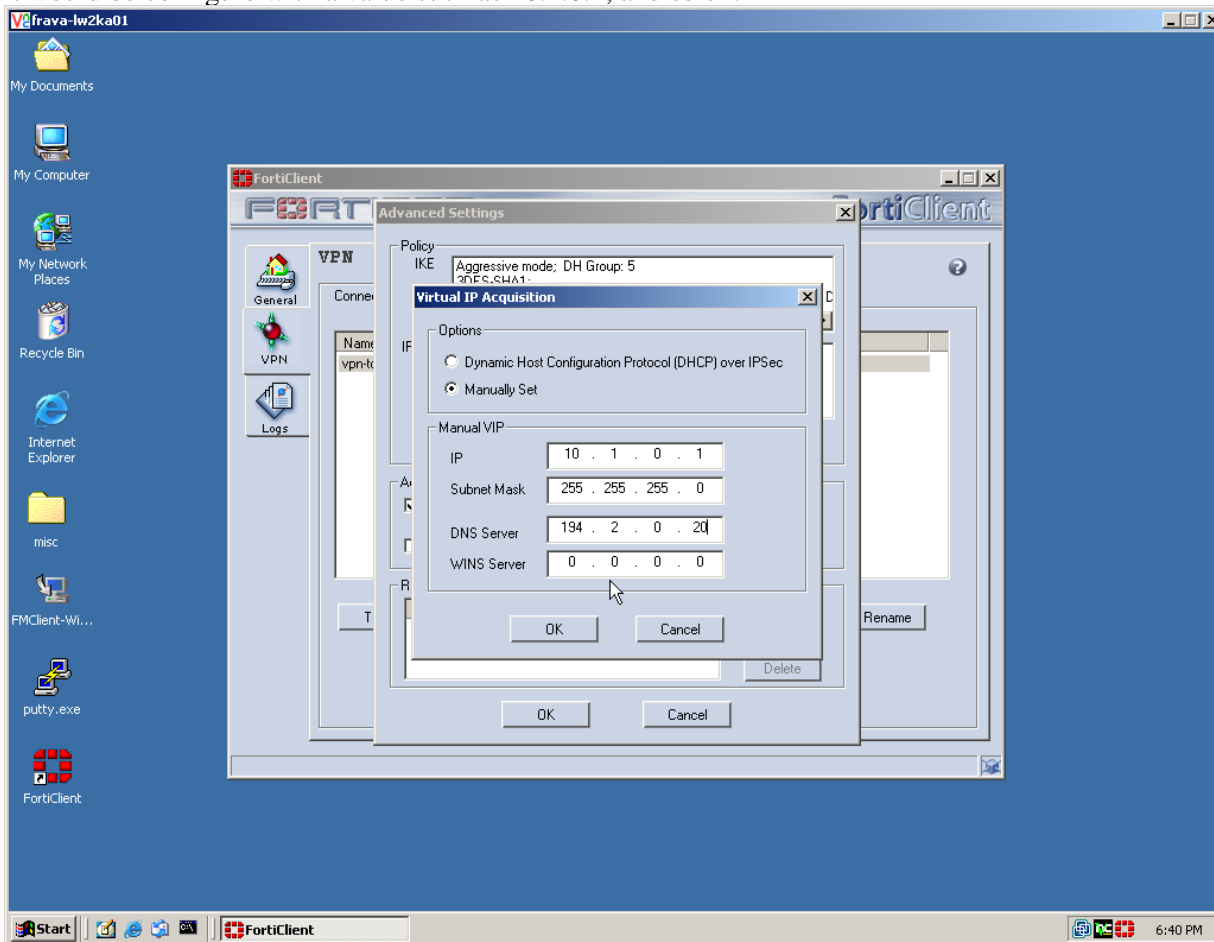
At the bottom of the window are 'OK' and 'Cancel' buttons.

FortiClient remote VPN user configuration:

Finally, each remote VPN user will be defined with a “Virtual IP” (VIP) value which is within the corresponding “remote-vpn-groupx” address range shown above, and a “Remote Access” network value which matches the defined Internal or DMZ network ranges (not Internal_All and not DMZ_All). The example of “vpnuser1” which accesses the Internal network is shown below.



This first user is configured with a VIP of 10.1.0.1. If an additional user is required to access the same internal network, it would be configure with a value such as 10.1.0.2, and so on.



// End of configuration samples.

// FortiClient log outputs collected using the TEST button. FortiClient v1.0.210 is connecting to a FGT200 v2.50-MR8

##1

// Log below is when an incorrect user ID is configured on the FC (ID mismatch)

```
In run_timer_list, jiffies=00000000, skipped = 0
tvecs[1]->bits is 3, tvecs[n]->index is 0
Detect local gateway for peer: 62.212.108.181
Get sa_connect message...10.30.30.8->62.212.108.181:0, natt_mode=0
Using new connection...natt_mode=0
Set connection name = vpn-to-internal-lan.
Adding timer #1... expiry=3600, data=9731984
Adding to bucket 3 at index 1
Tunnel 10.30.30.8 ---> 62.212.108.181:500,natt_en=1 is starting negotiation
Will negotiate a normal SA
Initiator:aggressive mode is sending 1st message...
Initiator:aggressive mode set dh=1536.
Sending DPD VID payload....
Sending VID payload....
Sending NATT VID payload (draft3)...
Sending NATT VID payload (draft3 and draft1)...
Initiator: sent 62.212.108.181 aggressive mode message #1 (OK)
Adding timer #2... expiry=28800, data=9733288
Adding to bucket 4 at index 1
set retransmit: st=1, timeout=10.
Adding timer #2... expiry=10, data=9733288
Adding to bucket 1 at index 10
Next_time = 10 sec
```

```
In run_timer_list, jiffies=0000000A, skipped = 10
tvecs[1]->bits is 3, tvecs[n]->index is 0
No response from the peer, retransmit (st=1)....
set retransmit: st=1, timeout=20.
Adding timer #2... expiry=20, data=9733288
Adding to queue
Adding timer #3... expiry=20, data=9733288
Adding to bucket 1 at index 30
Next_time = 20 sec
```

```
In run_timer_list, jiffies=0000001E, skipped = 20
tvecs[1]->bits is 3, tvecs[n]->index is 0
No response from the peer, retransmit (st=1)....
set retransmit: st=1, timeout=20.
Adding timer #2... expiry=20, data=9733288
Adding to queue
Adding timer #3... expiry=20, data=9733288
Adding to bucket 1 at index 50
Next_time = 20 sec
```

```
In run_timer_list, jiffies=00000032, skipped = 20
tvecs[1]->bits is 3, tvecs[n]->index is 0
Retransmit reaches maximum count (st=1)...delete it!
Next_time = 3550 sec
```

##2

// Log below is when the user ID is OK, but there is a mismatch on the Phase 1 Encryption/Authentication proposals.

```
In run_timer_list, jiffies=00000000, skipped = 0
tvecs[1]->bits is 3, tvecs[n]->index is 0
Detect local gateway for peer: 62.212.108.181
Get sa_connect message...10.30.30.8->62.212.108.181:0, natt_mode=0
Using new connection...natt_mode=0
Set connection name = vpn-to-internal-lan.
Adding timer #1... expiry=3600, data=9731984
Adding to bucket 3 at index 1
Tunnel 10.30.30.8 ---> 62.212.108.181:500,natt_en=1 is starting negotiation
```

Will negotiate a normal SA
Initiator:aggressive mode is sending 1st message...
Initiator:aggressive mode set dh=1536.
Sending DPD VID payload....
Sending VID payload....
Sending NATT VID payload (draft3)....
Sending NATT VID payload (draft3 and draft1)....
Initiator: sent 62.212.108.181 aggressive mode message #1 (OK)
Adding timer #2... expiry=28800, data=9733288
Adding to bucket 4 at index 1
set retransmit: st=1, timeout=10.
Adding timer #2... expiry=10, data=9733288
Adding to bucket 1 at index 10
Next_time = 10 sec

In run_timer_list, jiffies=00000000, skipped = 0
tvecs[1]->bits is 3, tvecs[n]->index is 0
Comes 62.212.108.181:500->10.30.30.8:500,ifindex=0,
Exchange Mode = 5, Message id = 0x75FC11C9, Len = 40
ISAKMP INFO #####
Received Payloads= Notif
-----Receive Information Payload-----
 protocol_id=1, notify_msg=14 (NO_PROPOSAL_CHOSEN), ispi_size=0
Negotiate SA Error: protocol_id=1, notify_msg=14 (NO_PROPOSAL_CHOSEN), ispi_size=0
[43]

Next_time = 10 sec

//#3

// Log below is when the user ID is OK, Phase 1 OK, but a mismatch on the Phase 2 Encryption/Authentication proposals.

In run_timer_list, jiffies=00000000, skipped = 0
tvecs[1]->bits is 3, tvecs[n]->index is 0
Detect local gateway for peer: 62.212.108.181
Get sa_connect message...10.30.30.8->62.212.108.181:0, natt_mode=0
Using new connection...natt_mode=0
Set connection name = vpn-to-internal-lan.
Adding timer #1... expiry=3600, data=9731984
Adding to bucket 3 at index 1
Tunnel 10.30.30.8 ---> 62.212.108.181:500,natt_en=1 is starting negotiation
Will negotiate a normal SA
Initiator:aggressive mode is sending 1st message...
Initiator:aggressive mode set dh=1536.
Sending DPD VID payload....
Sending VID payload....
Sending NATT VID payload (draft3)....
Sending NATT VID payload (draft3 and draft1)....
Initiator: sent 62.212.108.181 aggressive mode message #1 (OK)
Adding timer #2... expiry=28800, data=9733288
Adding to bucket 4 at index 1
set retransmit: st=1, timeout=10.
Adding timer #2... expiry=10, data=9733288
Adding to bucket 1 at index 10
Next_time = 10 sec

In run_timer_list, jiffies=00000000, skipped = 0
tvecs[1]->bits is 3, tvecs[n]->index is 0
Comes 62.212.108.181:500->10.30.30.8:500,ifindex=0,
Exchange Mode = 4, I_COOKIE = 0x68BEAFBC393FD64E, Len = 440
Received Payloads= SA KE NONCE ID VID VID VID 130 130 HASH
Initiator:aggressive mode get 1st response...
Proposal_id = 1:
 Protocol_id = ISAKMP:
 trans_id = KEY_IKE.
 encapsulation = 0 (unknown)
 type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.

```
type=OAKLEY_HASH_ALG, val=SHA.
type=AUTH_METHOD, val=PRESHARED_KEY.
type=OAKLEY_GROUP, val=1536.
Proposal_id = 1:
Protocol_id = ISAKMP:
trans_id = KEY_IKE.
encapsulation = 0 (unknown)
type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.
type=OAKLEY_HASH_ALG, val=SHA.
type=AUTH_METHOD, val=PRESHARED_KEY.
type=OAKLEY_GROUP, val=1536.
Negotiate Result
Proposal_id = 1:
Protocol_id = ISAKMP:
trans_id = KEY_IKE.
encapsulation = 0 (unknown)
type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.
type=OAKLEY_HASH_ALG, val=SHA.
type=AUTH_METHOD, val=PRESHARED_KEY.
type=OAKLEY_GROUP, val=1536.
Phase1 lifetimes=28800
Negotiate Success.(No echo).
test the peer keepalive status....
The peer is non-keepalive fortigate.
testing the peer DPD status....
The peer supports DPD draft 2.
test the peer natt status....
The peer supports natt draft3.
Using IPS_NAT_MODE_KEEPALIVE.
set gw: 009484A8, timeout=28800.
Adding timer #2... expiry=28800, data=9733288
Adding to bucket 4 at index 1
Adding timer #2... expiry=28800, data=9731984
Adding to bucket 4 at index 1
Initiator: sent 62.212.108.181 aggressive mode message #2 (DONE)
confirmed nat-t draft3
My id: 10.1.0.1 255.255.255.0
Adding timer #3... expiry=28800, data=9736160
Adding to bucket 4 at index 1
Initiator:quick mode set pfs=1536...
Try to negotiate with 1800 life seconds.
confirmed nat-t draft3
Initiator: sent 62.212.108.181 quick mode message #1 (OK)
set retransmit: st=2, timeout=10.
Adding timer #3... expiry=10, data=9736160
Adding to bucket 1 at index 10

Next_time = 10 sec

In run_timer_list, jiffies=00000000, skipped = 0
tvecs[1]->bits is 3, tvecs[n]->index is 0
Comes 62.212.108.181:4500->10.30.30.8:4500,ifindex=0, ....
Exchange Mode = 5, Message id = 0x87D1BBA3, Len = 68
##### ISAKMP INFO #####
Received Payloads= HASH Notif
##### Receive Information Payload(Protected)#####
protocol_id=1, notify_msg=14 (NO_PROPOSAL_CHOSEN), ispi_size=0
Negotiate SA Error: protocol_id=1, notify_msg=14 (NO_PROPOSAL_CHOSEN), ispi_size=0
[43]

Next_time = 10 sec

##4
// Log below is when the user ID is OK, Phase 1 and 2 OK, but a mismatch on the Pre-Shared key
```

In run_timer_list, jiffies=00000000, skipped = 0
tvecs[1]->bits is 3, tvecs[n]->index is 0
Detect local gateway for peer: 62.212.108.181
Get sa_connect message...10.30.30.8->62.212.108.181:0, natt_mode=0
Using new connection...natt_mode=0
Set connection name = vpn-to-internal-lan.
Adding timer #1... expiry=3600, data=9731984
Adding to bucket 3 at index 1
Tunnel 10.30.30.8 ---> 62.212.108.181:500,natt_en=1 is starting negotiation
Will negotiate a normal SA
Initiator:aggressive mode is sending 1st message...
Initiator:aggressive mode set dh=1536.
Sending DPD VID payload....
Sending VID payload....
Sending NATT VID payload (draft3)....
Sending NATT VID payload (draft3 and draft1)....
Initiator: sent 62.212.108.181 aggressive mode message #1 (OK)
Adding timer #2... expiry=28800, data=9733288
Adding to bucket 4 at index 1
set retransmit: st=1, timeout=10.
Adding timer #2... expiry=10, data=9733288
Adding to bucket 1 at index 10
Next_time = 10 sec

In run_timer_list, jiffies=00000001, skipped = 1
tvecs[1]->bits is 3, tvecs[n]->index is 0
Comes 62.212.108.181:500->10.30.30.8:500,ifindex=0,
Exchange Mode = 4, I_COOKIE = 0xA5EE24F2C86F37AA, Len = 440
Received Payloads= SA KE NONCE ID VID VID VID 130 130 HASH
Initiator:aggressive mode get 1st response...

Proposal_id = 1:
Protocol_id = ISAKMP:
trans_id = KEY_IKE.
encapsulation = 0 (unknown)
type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.
type=OAKLEY_HASH_ALG, val=SHA.
type=AUTH_METHOD, val=PRESHARED_KEY.
type=OAKLEY_GROUP, val=1536.

Proposal_id = 1:
Protocol_id = ISAKMP:
trans_id = KEY_IKE.
encapsulation = 0 (unknown)
type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.
type=OAKLEY_HASH_ALG, val=SHA.
type=AUTH_METHOD, val=PRESHARED_KEY.
type=OAKLEY_GROUP, val=1536.

Negotiate Result
Proposal_id = 1:
Protocol_id = ISAKMP:
trans_id = KEY_IKE.
encapsulation = 0 (unknown)
type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.
type=OAKLEY_HASH_ALG, val=SHA.
type=AUTH_METHOD, val=PRESHARED_KEY.
type=OAKLEY_GROUP, val=1536.

Phase1 lifetimes=28800
Negotiate Success.(No echo).
test the peer keepalive status....
The peer is non-keepalive fortigate.
testing the peer DPD status....
The peer supports DPD draft 2.
test the peer natt status....
The peer supports natt draft3.
Using IPS_NAT_MODE_KEEPALIVE.
Negotiate SA Error: Authentication failed for pre-shared key [43]
Initiator: parsed 62.212.108.181 aggressive mode message #1 (ERROR)

Next_time = 3599 sec

//#5

// Log below taken when ID, Phase 1 & 2, and Pre-Shared Key are OK, but the VIP address on FortiClient does not match FGT policy

In run_timer_list, jiffies=00000000, skipped = 0
tvecs[1]->bits is 3, tvecs[n]->index is 0
Detect local gateway for peer: 62.212.108.181
Get sa_connect message...10.30.30.8->62.212.108.181:0, natt_mode=0
Using new connection...natt_mode=0
Set connection name = vpn-to-internal-lan.
Adding timer #1... expiry=3600, data=9731984
Adding to bucket 3 at index 1
Tunnel 10.30.30.8 ---> 62.212.108.181:500,natt_en=1 is starting negotiation
Will negotiate a normal SA
Initiator:aggressive mode is sending 1st message...
Initiator:aggressive mode set dh=1536.
Sending DPD VID payload....
Sending VID payload....
Sending NATT VID payload (draft3)....
Sending NATT VID payload (draft3 and draft1)....
Initiator: sent 62.212.108.181 aggressive mode message #1 (OK)
Adding timer #2... expiry=28800, data=9733288
Adding to bucket 4 at index 1
set retransmit: st=1, timeout=10.
Adding timer #2... expiry=10, data=9733288
Adding to bucket 1 at index 10
Next_time = 10 sec

In run_timer_list, jiffies=00000001, skipped = 1
tvecs[1]->bits is 3, tvecs[n]->index is 0
Comes 62.212.108.181:500->10.30.30.8:500,ifindex=0,
Exchange Mode = 4, I_COOKIE = 0x7C5A0EC363D827CD, Len = 440
Received Payloads= SA KE NONCE ID VID VID VID 130 130 HASH
Initiator:aggressive mode get 1st response...

Proposal_id = 1:

Protocol_id = ISAKMP:

trans_id = KEY_IKE.

encapsulation = 0 (unknown)

type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.

type=OAKLEY_HASH_ALG, val=SHA.

type=AUTH_METHOD, val=PRESHARED_KEY.

type=OAKLEY_GROUP, val=1536.

Proposal_id = 1:

Protocol_id = ISAKMP:

trans_id = KEY_IKE.

encapsulation = 0 (unknown)

type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.

type=OAKLEY_HASH_ALG, val=SHA.

type=AUTH_METHOD, val=PRESHARED_KEY.

type=OAKLEY_GROUP, val=1536.

Negotiate Result

Proposal_id = 1:

Protocol_id = ISAKMP:

trans_id = KEY_IKE.

encapsulation = 0 (unknown)

type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.

type=OAKLEY_HASH_ALG, val=SHA.

type=AUTH_METHOD, val=PRESHARED_KEY.

type=OAKLEY_GROUP, val=1536.

Phase1 lifetimes=28800

Negotiate Success.(No echo).

test the peer keepalive status....

The peer is non-keepalive fortigate.

testing the peer DPD status....

The peer supports DPD draft 2.
test the peer natt status....
The peer supports natt draft3.
Using IPS_NAT_MODE_KEEPALIVE.
set gw: 009484A8, timeout=28800.
Adding timer #2... expiry=28800, data=9733288
Adding to bucket 4 at index 1
Adding timer #2... expiry=28800, data=9731984
Adding to bucket 4 at index 1
Initiator: sent 62.212.108.181 aggressive mode message #2 (DONE)
confirmed nat-t draft3
My id: 10.1.0.1 255.255.255.0
Adding timer #3... expiry=28800, data=9736160
Adding to bucket 4 at index 1
Initiator: quick mode set pfs=1536...
Try to negotiate with 1800 life seconds.
confirmed nat-t draft3
Initiator: sent 62.212.108.181 quick mode message #1 (OK)
set retransmit: st=2, timeout=10.
Adding timer #3... expiry=10, data=9736160
Adding to bucket 1 at index 11

Next_time = 10 sec

##6

// Log below is when everything is OK. A successful VPN test connection.

In run_timer_list, jiffies=00000000, skipped = 0
tvecs[1]->bits is 3, tvecs[n]->index is 0
Detect local gateway for peer: 62.212.108.181
Get sa_connect message...10.30.30.8->62.212.108.181:0, natt_mode=0
Using new connection...natt_mode=0
Set connection name = vpn-to-internal-lan.
Adding timer #1... expiry=3600, data=9731984
Adding to bucket 3 at index 1
Tunnel 10.30.30.8 ---> 62.212.108.181:500,natt_en=1 is starting negotiation
Will negotiate a normal SA
Initiator: aggressive mode is sending 1st message...
Initiator: aggressive mode set dh=1536.
Sending DPD VID payload....
Sending VID payload....
Sending NATT VID payload (draft3)....
Sending NATT VID payload (draft3 and draft1)....
Initiator: sent 62.212.108.181 aggressive mode message #1 (OK)
Adding timer #2... expiry=28800, data=9733288
Adding to bucket 4 at index 1
set retransmit: st=1, timeout=10.
Adding timer #2... expiry=10, data=9733288
Adding to bucket 1 at index 10
Next_time = 10 sec

In run_timer_list, jiffies=00000000, skipped = 0
tvecs[1]->bits is 3, tvecs[n]->index is 0
Comes 62.212.108.181:500->10.30.30.8:500,ifindex=0,
Exchange Mode = 4, I_COOKIE = 0xCB18DD8CF237CE0D, Len = 440
Received Payloads= SA KE NONCE ID VID VID VID 130 130 HASH
Initiator: aggressive mode get 1st response...
Proposal_id = 1:
 Protocol_id = ISAKMP:
 trans_id = KEY_IKE.
 encapsulation = 0 (unknown)
 type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.
 type=OAKLEY_HASH_ALG, val=SHA.
 type=AUTH_METHOD, val=PRE_SHARED_KEY.
 type=OAKLEY_GROUP, val=1536.
Proposal_id = 1:

Protocol_id = ISAKMP:
trans_id = KEY_IKE.
encapsulation = 0 (unknown)
type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.
type=OAKLEY_HASH_ALG, val=SHA.
type=AUTH_METHOD, val=PRESHARED_KEY.
type=OAKLEY_GROUP, val=1536.

Negotiate Result

Proposal_id = 1:

Protocol_id = ISAKMP:
trans_id = KEY_IKE.
encapsulation = 0 (unknown)
type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.
type=OAKLEY_HASH_ALG, val=SHA.
type=AUTH_METHOD, val=PRESHARED_KEY.
type=OAKLEY_GROUP, val=1536.

Phase1 lifetimes=28800

Negotiate Success.(No echo).

test the peer keepalive status....

The peer is non-keepalive fortigate.

testing the peer DPD status....

The peer supports DPD draft 2.

test the peer natt status....

The peer supports natt draft3.

Using IPS_NAT_MODE_KEEPALIVE.

set gw: 009484A8, timeout=28800.

Adding timer #2... expiry=28800, data=9733288

Adding to bucket 4 at index 1

Adding timer #2... expiry=28800, data=9731984

Adding to bucket 4 at index 1

Initiator: sent 62.212.108.181 aggressive mode message #2 (DONE)

confirmed nat-t draft3

My id: 10.1.0.1 255.255.255.0

Adding timer #3... expiry=28800, data=9736160

Adding to bucket 4 at index 1

Initiator:quick mode set pfs=1536...

Try to negotiate with 1800 life seconds.

confirmed nat-t draft3

Initiator: sent 62.212.108.181 quick mode message #1 (OK)

set retransmit: st=2, timeout=10.

Adding timer #3... expiry=10, data=9736160

Adding to bucket 1 at index 10

Next_time = 10 sec

In run_timer_list, jiffies=00000001, skipped = 1

tvecs[1]->bits is 3, tvecs[n]->index is 0

Comes 62.212.108.181:4500->10.30.30.8:4500,ifindex=0,

Exchange Mode = 32, Message id = 0xD6E01AF3, Len = 348

Received Payloads= HASH SA NONCE KE ID ID

Initiator:quick mode get 1st response

Proposal_id = 1:

Protocol_id = IPSEC_ESP:
trans_id = ESP_3DES.
encapsulation = UDP_ENCAPSULATION_MODE_TUNNEL
type=AUTH_ALG, val=SHA1.

Proposal_id = 1:

Protocol_id = IPSEC_ESP:
trans_id = ESP_3DES.
encapsulation = 0 (unknown)
type=AUTH_ALG, val=SHA1.

Negotiate Result

Proposal_id = 1:

Protocol_id = IPSEC_ESP:
trans_id = ESP_3DES.
encapsulation = UDP_ENCAPSULATION_MODE_TUNNEL
type=AUTH_ALG, val=SHA1.

Phase2 esp lifetimes=1800
Using udp tunnel mode.
Negotiate Success.(No echo).
Initiator:Prepare to install sa.
Set sa life soft seconds=1777.
Set sa life hard seconds=1800.
dport = 4500. tunnel.name = vpn-to-internal-lan.
Detect local gateway for peer: 62.212.108.181. Next hop: 10.30.30.1
Initializing sa OK.
Initiator: sent 62.212.108.181 quick mode message #2 (DONE)
expire: st=2, timeout=120.
Adding timer #3... expiry=120, data=9736160
Adding to bucket 1 at index 121
confirmed nat-t draft3
confirmed nat-t draft3

Next_time = 120 sec

In run_timer_list, jiffies=00000001, skipped = 0
tvecs[1]->bits is 3, tvecs[n]->index is 0
confirmed nat-t draft3

IKE daemon stopped

// FortGate v2.50-MR8 debug outputs collected using "diag debug appli ike 2". FortiClient v1.0.210 is connecting to this unit.

##1

// Debug below is when an incorrect user ID is configured on the FC (ID mismatch)

Fortigate-200 #

Fortigate-200 # Comes 81.255.3.99:53522->62.212.108.181:500,ifindex=8, ppp0, vf_id=0....
Exchange Mode = 4, I_COOKIE = 0x8995EF78BC454916, Len = 388
The peer id is joe.
Can not find the remote_gwy, exit.

Comes 81.255.3.99:53522->62.212.108.181:500,ifindex=8, ppp0, vf_id=0....
Exchange Mode = 4, I_COOKIE = 0x8995EF78BC454916, Len = 388
The peer id is joe.
Can not find the remote_gwy, exit.

Comes 81.255.3.99:53522->62.212.108.181:500,ifindex=8, ppp0, vf_id=0....
Exchange Mode = 4, I_COOKIE = 0x8995EF78BC454916, Len = 388
The peer id is joe.
Can not find the remote_gwy, exit.

##2

// Debug below is when the user ID is OK, but there is a mismatch on the Phase 1 Encryption/Authentication proposals.

Fortigate-200 # Comes 81.255.3.99:54164->62.212.108.181:500,ifindex=8, ppp0, vf_id=0....
Exchange Mode = 4, I_COOKIE = 0x9D7B55324D933E35, Len = 392
The peer id is vpnuser1.
Set connection name = Dial-in-gateway.
Received Payloads= SA KE NONCE ID VID VID VID VID
Responder:aggressive mode get 1st message...
test the peer keepalive status....
test the peer natt status....
The peer supports natt draft3.
testing the peer DPD status....
The peer supports DPD draft 2.

Incoming proposal:
Proposal_id = 1:

Protocol_id = ISAKMP:
trans_id = KEY_IKE.
encapsulation = 0 (unknown)
type=OAKLEY_ENCRYPT_ALG, val=DES_CBC.
type=OAKLEY_HASH_ALG, val=MD5.
type=AUTH_METHOD, val=PRESHARED_KEY.
type=OAKLEY_GROUP, val=1536.

My proposal:

Proposal_id = 1:

Protocol_id = ISAKMP:
trans_id = KEY_IKE.
encapsulation = 0 (unknown)
type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.
type=OAKLEY_HASH_ALG, val=SHA.
type=AUTH_METHOD, val=PRESHARED_KEY.
type=OAKLEY_GROUP, val=1536.

Cannot negotiate successfully

Negotiate SA Error: No proposal can be chosen. [2361]

Negotiate Error.

sending INFO message NO_PROPOSAL_CHOSEN to peer

Send IKE Packet(Info Mode):62.212.108.181:500(if8) -> 81.255.3.99:54164, len=40

transmitted 40 bytes

Responder: parsed 81.255.3.99 aggressive mode message #1 (ERROR)

Comes 81.255.3.99:54164->62.212.108.181:500,ifindex=8, ppp0, vf_id=0....

Exchange Mode = 4, I_COOKIE = 0x9D7B55324D933E35, Len = 392

The peer id is vpnuser1.

Received Payloads= SA KE NONCE ID VID VID VID VID

Responder:aggressive mode get 1st message...

test the peer keepalive status....

test the peer natt status....

The peer supports natt draft3.

testing the peer DPD status....

The peer supports DPD draft 2.

Incoming proposal:

Proposal_id = 1:

Protocol_id = ISAKMP:
trans_id = KEY_IKE.
encapsulation = 0 (unknown)
type=OAKLEY_ENCRYPT_ALG, val=DES_CBC.
type=OAKLEY_HASH_ALG, val=MD5.
type=AUTH_METHOD, val=PRESHARED_KEY.
type=OAKLEY_GROUP, val=1536.

My proposal:

Proposal_id = 1:

Protocol_id = ISAKMP:
trans_id = KEY_IKE.
encapsulation = 0 (unknown)
type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.
type=OAKLEY_HASH_ALG, val=SHA.
type=AUTH_METHOD, val=PRESHARED_KEY.
type=OAKLEY_GROUP, val=1536.

Cannot negotiate successfully

Negotiate SA Error: No proposal can be chosen. [2361]

Negotiate Error.

sending INFO message NO_PROPOSAL_CHOSEN to peer

Send IKE Packet(Info Mode):62.212.108.181:500(if8) -> 81.255.3.99:54164, len=40

transmitted 40 bytes

Responder: parsed 81.255.3.99 aggressive mode message #1 (ERROR)

Comes 81.255.3.99:54164->62.212.108.181:500,ifindex=8, ppp0, vf_id=0....

Exchange Mode = 4, I_COOKIE = 0x9D7B55324D933E35, Len = 392

The peer id is vpnuser1.

Received Payloads= SA KE NONCE ID VID VID VID VID
Responder:aggressive mode get 1st message...
test the peer keepalive status....
test the peer natt status....
The peer supports natt draft3.
testing the peer DPD status....
The peer supports DPD draft 2.

Incoming proposal:

Proposal_id = 1:

Protocol_id = ISAKMP:

trans_id = KEY_IKE.

encapsulation = 0 (unknown)

type=OAKLEY_ENCRYPT_ALG, val=DES_CBC.

type=OAKLEY_HASH_ALG, val=MD5.

type=AUTH_METHOD, val=PRESHARED_KEY.

type=OAKLEY_GROUP, val=1536.

My proposal:

Proposal_id = 1:

Protocol_id = ISAKMP:

trans_id = KEY_IKE.

encapsulation = 0 (unknown)

type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.

type=OAKLEY_HASH_ALG, val=SHA.

type=AUTH_METHOD, val=PRESHARED_KEY.

type=OAKLEY_GROUP, val=1536.

Cannot negotiate successfully

Negotiate SA Error: No proposal can be chosen. [2361]

Negotiate Error.

sending INFO message NO_PROPOSAL_CHOSEN to peer

Send IKE Packet(Info Mode):62.212.108.181:500(if8) -> 81.255.3.99:54164, len=40

transmitted 40 bytes

Responder: parsed 81.255.3.99 aggressive mode message #1 (ERROR)

##3

// Debug below is when the user ID is OK, Phase 1 OK, but a mismatch on the Phase 2 Encryption/Authentication proposals.

Fortigate-200 # Comes 81.255.3.99:54164->62.212.108.181:500,ifindex=8, ppp0, vf_id=0...

Exchange Mode = 4, I_COOKIE = 0x68BEAFBC393FD64E, Len = 392

The peer id is vpnuser1.

Set connection name = Dial-in-gateway.

Received Payloads= SA KE NONCE ID VID VID VID VID

Responder:aggressive mode get 1st message...

test the peer keepalive status....

test the peer natt status....

The peer supports natt draft3.

testing the peer DPD status....

The peer supports DPD draft 2.

Negotiate Result

Proposal_id = 1:

Protocol_id = ISAKMP:

trans_id = KEY_IKE.

encapsulation = 0 (unknown)

type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.

type=OAKLEY_HASH_ALG, val=SHA.

type=AUTH_METHOD, val=PRESHARED_KEY.

type=OAKLEY_GROUP, val=1536.

Phase1 lifetimes=28800

Sending DPD VID payload....

Sending VID payload....

Sending NATT VID payload (draft3)....

Responder: sent 81.255.3.99 aggressive mode message #1 (OK)

Send IKE Packet(STF_REPLY):62.212.108.181:500(if8) -> 81.255.3.99:54164, len=440

set retransmit: st=16, timeout=10.

Comes 81.255.3.99:54256->62.212.108.181:4500,ifindex=8, ppp0, vf_id=0...
Exchange Mode = 4, I_COOKIE = 0x68BEAFBC393FD64E, Len = 100
Received Payloads= 130 130 HASH
Responder:aggressive mode get 2nd response...
Using IPS_NAT_MODE_SILENT.
set gw: 0x8137208, timeout=28800.
Responder: parsed 81.255.3.99 aggressive mode message #2 (DONE)

Comes 81.255.3.99:54256->62.212.108.181:4500,ifindex=8, ppp0, vf_id=0...
Exchange Mode = 32, Message id = 0x490C22CC, Len = 348
Received Payloads= HASH SA NONCE KE ID ID
Responder:quick mode get 1st message...
his proposal ids: peer:10.1.0.1(255.255.255.255), me:10.10.1.0(255.255.255.0)
my policy ids: src:10.10.1.0(255.255.255.0), dst:10.1.0.0(255.255.255.0)
Got it
Found Dial-in-gateway:0.0.0.0.
Matched an IPsec tunnel(tunnel-to-internal), kernel_comm.c,440
Dialup tunnel-to-internal.
Dialup proxyid: peer:10.1.0.1(255.255.255.255),me:10.10.1.0(255.255.255.0)

Incoming proposal:
Proposal_id = 1:
Protocol_id = IPSEC_ESP:
trans_id = ESP_DES.
encapsulation = UDP_ENCAPSULATION_MODE_TUNNEL
type=AUTH_ALG, val=MD5.

My proposal:
Proposal_id = 1:
Protocol_id = IPSEC_ESP:
trans_id = ESP_3DES.
encapsulation = 0 (unknown)
type=AUTH_ALG, val=SHA1.

Cannot negotiate successfully
Negotiate SA Error: No proposal can be chosen. [2361]
Negotiate Error.
sending INFO message NO_PROPOSAL_CHOSEN to peer
confirmed nat-t draft3
Send IKE Packet(Info Mode):62.212.108.181:4500(if8) -> 81.255.3.99:54256, len=68
transmitted 68 bytes
Responder: parsed 81.255.3.99 quick mode message #1 (ERROR)

Comes 81.255.3.99:54256->62.212.108.181:4500,ifindex=8, ppp0, vf_id=0...
Exchange Mode = 32, Message id = 0x490C22CC, Len = 348

Comes 81.255.3.99:54256->62.212.108.181:4500,ifindex=8, ppp0, vf_id=0...
Exchange Mode = 5, Message id = 0x663E4B0F, Len = 84
ISAKMP INFO #####
Received Payloads= HASH Delete
Receive Information Payload(Protected)#####
spi_size=16, spi_number=1
No. 0 spi=68beafbc393fd64e07ee417c0c3e09a8
confirmed nat-t draft3
Send IKE Packet(delete notify):62.212.108.181:4500(if8) -> 81.255.3.99:54256, len=84

##4
// Debug below is when the user ID is OK, Phase 1 and 2 OK, but a mismatch on the Pre-Shared key

Fortigate-200 # Comes 81.255.3.99:54164->62.212.108.181:500,ifindex=8, ppp0, vf_id=0...
Exchange Mode = 4, I_COOKIE = 0xA5EE24F2C86F37AA, Len = 392
The peer id is vpnuser1.
Set connection name = Dial-in-gateway.
Received Payloads= SA KE NONCE ID VID VID VID VID
Responder:aggressive mode get 1st message...

test the peer keepalive status....
test the peer natt status....
The peer supports natt draft3.
testing the peer DPD status....
The peer supports DPD draft 2.
Negotiate Result
Proposal_id = 1:
 Protocol_id = ISAKMP:
 trans_id = KEY_IKE.
 encapsulation = 0 (unknown)
 type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.
 type=OAKLEY_HASH_ALG, val=SHA.
 type=AUTH_METHOD, val=PRESHARED_KEY.
 type=OAKLEY_GROUP, val=1536.
Phase1 lifetimes=28800
Sending DPD VID payload....
Sending VID payload....
Sending NATT VID payload (draft3)....
Responder: sent 81.255.3.99 aggressive mode message #1 (OK)
Send IKE Packet(STF_REPLY):62.212.108.181:500(if8) -> 81.255.3.99:54164, len=440
set retransmit: st=18, timeout=10.

sched: timer is overdue by 1 seconds.
No response from the peer, retransmit (st=18)....
Send IKE Packet(EVENT_RETRANSMIT):62.212.108.181:500(if8) -> 81.255.3.99:54164, len=440
set retransmit: st=18, timeout=20.
No response from the peer, retransmit (st=18)....
Send IKE Packet(EVENT_RETRANSMIT):62.212.108.181:500(if8) -> 81.255.3.99:54164, len=440
set retransmit: st=18, timeout=40.
Retransmit reaches maximum count (st=18)...delete it!

##5

// Debug below taken when ID, Phase 1 & 2, and Pre-Shared Key are OK, except that the VIP address on FortiClient does not match FGT policy

Fortigate-200 # Comes 81.255.3.99:36374->62.212.108.181:500,ifindex=8, ppp0, vf_id=0....
Exchange Mode = 4, I_COOKIE = 0x7C5A0EC363D827CD, Len = 392
The peer id is vpnuser1.
Set connection name = Dial-in-gateway-1.
Received Payloads= SA KE NONCE ID VID VID VID VID
Responder:aggressive mode get 1st message...
test the peer keepalive status....
test the peer natt status....
The peer supports natt draft3.
testing the peer DPD status....
The peer supports DPD draft 2.
Negotiate Result
Proposal_id = 1:
 Protocol_id = ISAKMP:
 trans_id = KEY_IKE.
 encapsulation = 0 (unknown)
 type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.
 type=OAKLEY_HASH_ALG, val=SHA.
 type=AUTH_METHOD, val=PRESHARED_KEY.
 type=OAKLEY_GROUP, val=1536.
Phase1 lifetimes=28800
Sending DPD VID payload....
Sending VID payload....
Sending NATT VID payload (draft3)....
Responder: sent 81.255.3.99 aggressive mode message #1 (OK)
Send IKE Packet(STF_REPLY):62.212.108.181:500(if8) -> 81.255.3.99:36374, len=440
set retransmit: st=180, timeout=10.

Comes 81.255.3.99:36375->62.212.108.181:4500,ifindex=8, ppp0, vf_id=0....
Exchange Mode = 4, I_COOKIE = 0x7C5A0EC363D827CD, Len = 100

Received Payloads= 130 130 HASH
Responder:aggressive mode get 2nd response...
Using IPS_NAT_MODE_SILENT.
set gw: 0x8137208, timeout=28800.
Responder: parsed 81.255.3.99 aggressive mode message #2 (DONE)

Comes 81.255.3.99:36375->62.212.108.181:4500,ifindex=8, ppp0, vf_id=0...
Exchange Mode = 32, Message id = 0xECD9037F, Len = 348
Received Payloads= HASH SA NONCE KE ID ID
Responder:quick mode get 1st message...
his proposal ids: peer:10.1.0.1(255.255.255.255), me:10.99.99.0(255.255.255.0)
my policy ids: src:10.10.1.0(255.255.255.128), dst:10.1.0.0(255.255.255.0)
Got it failure
No matching IPsec tunnel found, kernel_comm.c,435
retrieve_ike_policy error.
sending INFO message INVALID_ID_INFORMATION to peer
confirmed nat-t draft3
Send IKE Packet(Info Mode):62.212.108.181:4500(if8) -> 81.255.3.99:36375, len=68
transmitted 68 bytes
Responder: parsed 81.255.3.99 quick mode message #1 (ERROR)

Comes 81.255.3.99:36375->62.212.108.181:4500,ifindex=8, ppp0, vf_id=0...
Exchange Mode = 32, Message id = 0xECD9037F, Len = 348

Comes 81.255.3.99:36375->62.212.108.181:4500,ifindex=8, ppp0, vf_id=0...
Exchange Mode = 32, Message id = 0xECD9037F, Len = 348

//#6

// Debug below is when everything is OK. A successful VPN dial-in connection.

Fortigate-200 # Retransmit reaches maximum count (st=19)...delete it!
Comes 81.255.3.99:54164->62.212.108.181:500,ifindex=8, ppp0, vf_id=0...
Exchange Mode = 4, I_COOKIE = 0xCB18DD8CF237CE0D, Len = 392
The peer id is vpnuser1.
Received Payloads= SA KE NONCE ID VID VID VID VID
Responder:aggressive mode get 1st message...
test the peer keepalive status....
test the peer natt status....
The peer supports natt draft3.
testing the peer DPD status....
The peer supports DPD draft 2.
Negotiate Result
Proposal_id = 1:
 Protocol_id = ISAKMP:
 trans_id = KEY_IKE.
 encapsulation = 0 (unknown)
 type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.
 type=OAKLEY_HASH_ALG, val=SHA.
 type=AUTH_METHOD, val=PRESHARED_KEY.
 type=OAKLEY_GROUP, val=1536.
Phase1 lifetimes=28800
Sending DPD VID payload....
Sending VID payload....
Sending NATT VID payload (draft3)....
Responder: sent 81.255.3.99 aggressive mode message #1 (OK)
Send IKE Packet(STF_REPLY):62.212.108.181:500(if8) -> 81.255.3.99:54164, len=440
set retransmit: st=20, timeout=10.

Comes 81.255.3.99:54695->62.212.108.181:4500,ifindex=8, ppp0, vf_id=0...
Exchange Mode = 4, I_COOKIE = 0xCB18DD8CF237CE0D, Len = 100
Received Payloads= 130 130 HASH
Responder:aggressive mode get 2nd response...
Using IPS_NAT_MODE_SILENT.

set gw: 0x8137208, timeout=28800.
Responder: parsed 81.255.3.99 aggressive mode message #2 (DONE)

Comes 81.255.3.99:54695->62.212.108.181:4500,ifindex=8, ppp0, vf_id=0...
Exchange Mode = 32, Message id = 0xD6E01AF3, Len = 348
Received Payloads= HASH SA NONCE KE ID ID
Responder:quick mode get 1st message...
his proposal ids: peer:10.1.0.1(255.255.255.255), me:10.10.1.0(255.255.255.0)
my policy ids: src:10.10.1.0(255.255.255.0), dst:10.1.0.0(255.255.255.0)
Got it
Found Dial-in-gateway:0.0.0.0.
Matched an IPsec tunnel(tunnel-to-internal), kernel_comm.c,440
Dialup tunnel-to-internal.
Dialup proxyid: peer:10.1.0.1(255.255.255.255),me:10.10.1.0(255.255.255.0)
Negotiate Result
Proposal_id = 1:
 Protocol_id = IPSEC_ESP:
 trans_id = ESP_3DES.
 encapsulation = UDP_ENCAPSULATION_MODE_TUNNEL
 type=AUTH_ALG, val=SHA1.
Phase2 esp lifetimes=1800
negotiate:set pfs=1536.
Using udp tunnel mode.
Responder:quick mode set pfs=1536.
quick mode:idci type=1, len=4, chunk=0a010001
quick mode:idcr type=4, len=8, chunk=0a0a0100ffff00
Responder: sent 81.255.3.99 quick mode message #1 (OK)
confirmed nat-t draft3
Send IKE Packet(STF_REPLY):62.212.108.181:4500(if8) -> 81.255.3.99:54695, len=348
set retransmit: st=21, timeout=10.

Comes 81.255.3.99:54695->62.212.108.181:4500,ifindex=8, ppp0, vf_id=0...
Exchange Mode = 32, Message id = 0xD6E01AF3, Len = 52
Received Payloads= HASH
Replay protection enable.
Set sa life soft seconds=1750.
Set sa life hard seconds=1800.
dport = 54695.adding dialup. peer:10.1.0.1(255.255.255.255), me:10.10.1.0(255.255.255.0)
Add dialup tunnel.tun=tunnel-to-internal, remote_gwy=81.255.3.99
Initializing sa OK.
Responder:quick mode done !

Responder: parsed 81.255.3.99 quick mode message #2 (DONE)
expire: st=21, timeout=120.

Comes 81.255.3.99:54695->62.212.108.181:4500,ifindex=8, ppp0, vf_id=0...
Exchange Mode = 5, Message id = 0x1BCFA1EA, Len = 76
ISAKMP INFO #####
Received Payloads= HASH Delete
Receive Information Payload(Protected)#####
 spi_size=4, spi_number=2
 No. 0 spi=9e54da5a
 No. 1 spi=37692f07
Deleting: dst=81.255.3.99,spi=9e54da5a
Deleting: dst=81.255.3.99,spi=37692f07

Comes 81.255.3.99:54695->62.212.108.181:4500,ifindex=8, ppp0, vf_id=0...
Exchange Mode = 5, Message id = 0x1FA0A422, Len = 84
ISAKMP INFO #####
Received Payloads= HASH Delete
Receive Information Payload(Protected)#####
 spi_size=16, spi_number=1
 No. 0 spi=cb18dd8cf237ce0dac56f63b544ea211

confirmed nat-t draft3

Send IKE Packet(delete notify):62.212.108.181:4500(if8) -> 81.255.3.99:54695, len=84

SA hard expired. 81.255.3.99:54695

// Note: Debug output below is caused by NATT Keepalives. This is normal.

Comes 62.212.107.74:41051->62.212.108.181:4500,ifindex=8, ppp0, vf_id=0...
packet is bad: len=1.

Comes 62.212.107.74:41051->62.212.108.181:4500,ifindex=8, ppp0, vf_id=0...
packet is bad: len=1.