Securing LDAP communications between a FortiGate and Windows Server

March 15, 2006.

FortiGate v2.80 MR11
Windows Server 2003 SP1

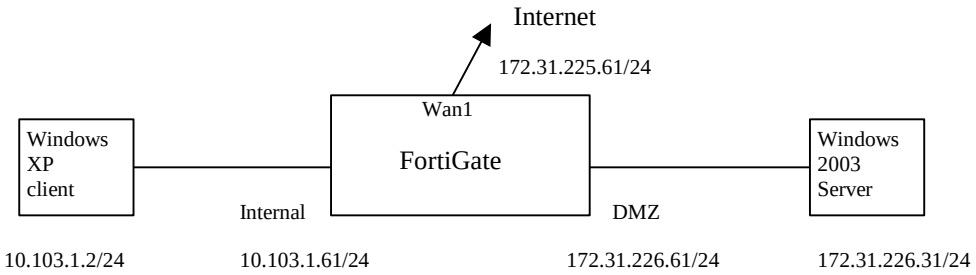
The FortiGate can perform VPN or Firewall authentication using a LDAP server. If the LDAP server is a Windows 2003 Active Directory server, it may be possible to create an IPSec tunnel between the FortiGate and the Windows Server in order to secure the LDAP binding requests and replies.

This article is based on the following Microsoft information:
http://support.microsoft.com/default.aspx?scid=kb;en-us;816514

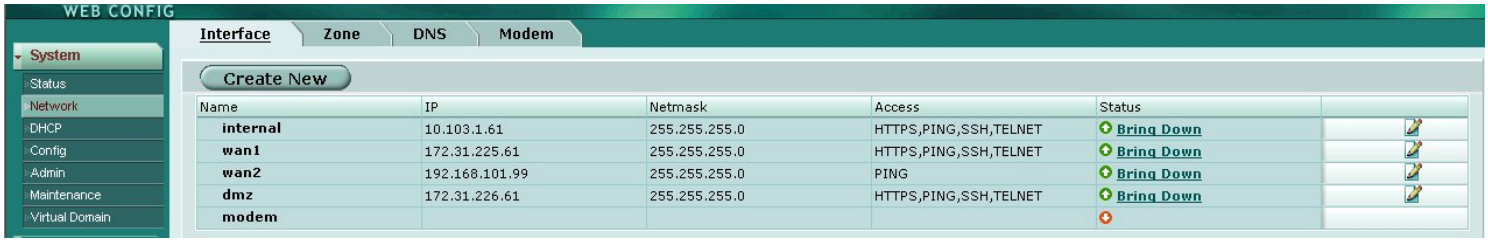
Note: This article describes a method of creating an IPSec tunnel between a Windows 2003 Server and a FortiGate. This information is currently being supplied as is, without the guarantee that this configuration will work in all instances. Fortinet has not verified and tested IPSec compatability between Windows OS and FortiGate devices. No technical support will be provided for this type of configuration.

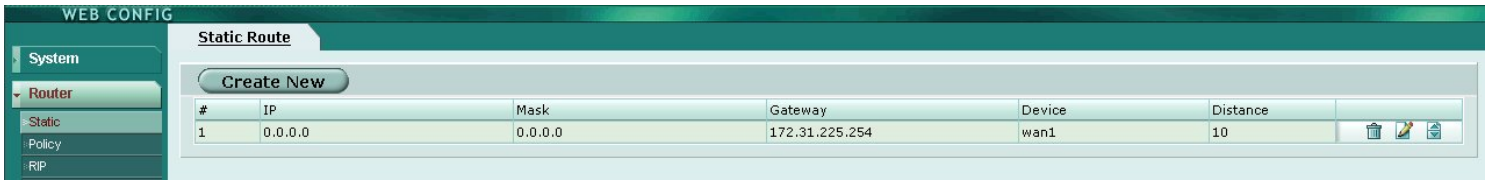
Configuration:

In the configuration shown below, the Windows Server is on a separate FortiGate interface, but it could have been on the Internal interface, alongside the clients. In this example, the client will be authenticated on the FortiGate firewall in order to obtain access to the Internet.

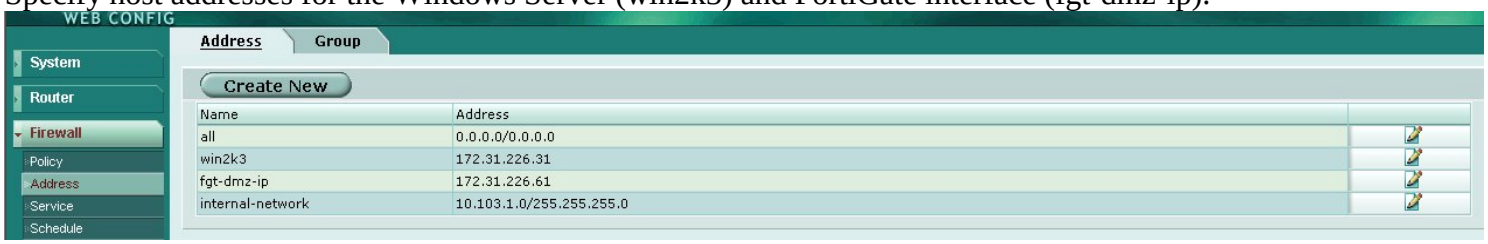


FortiGate:

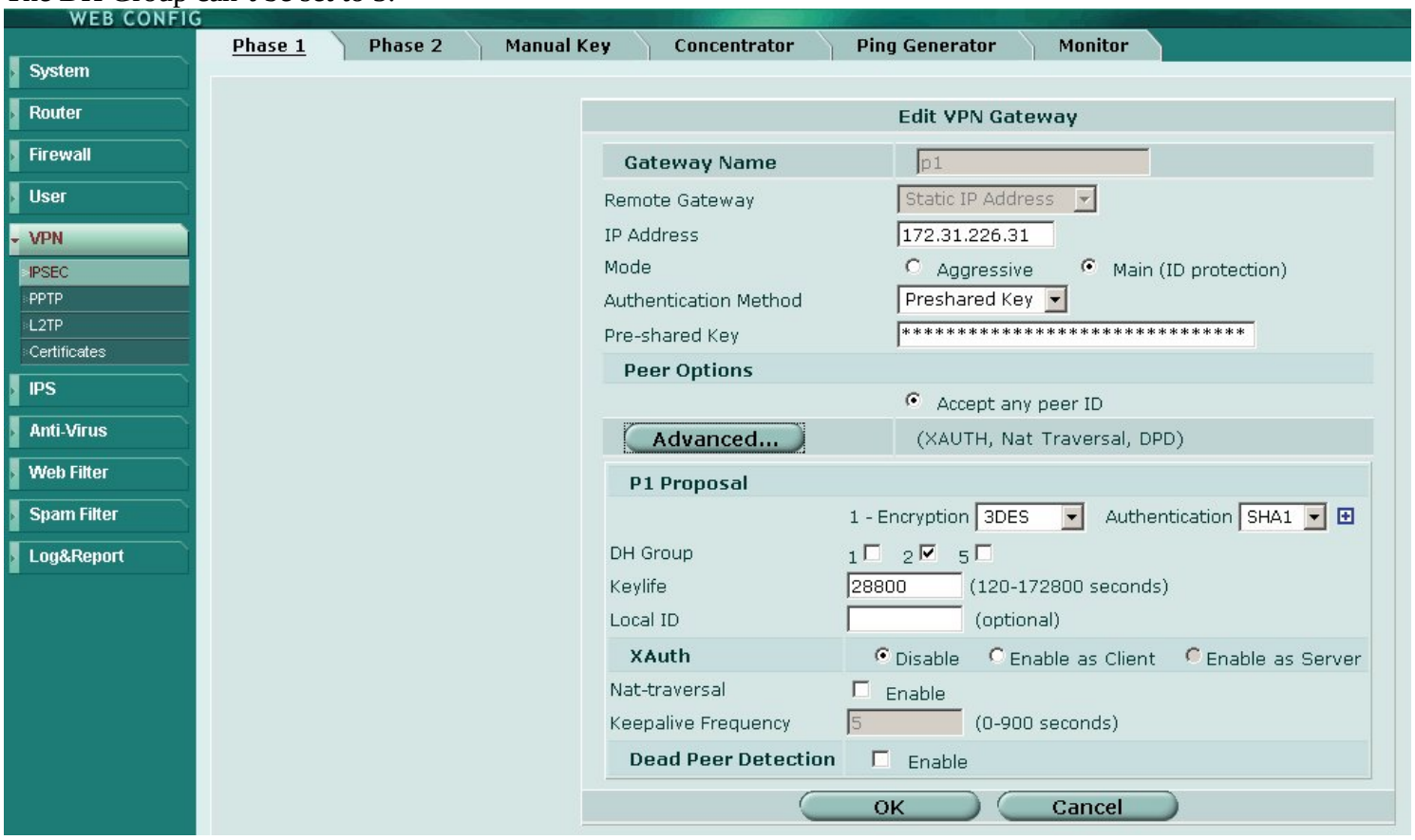


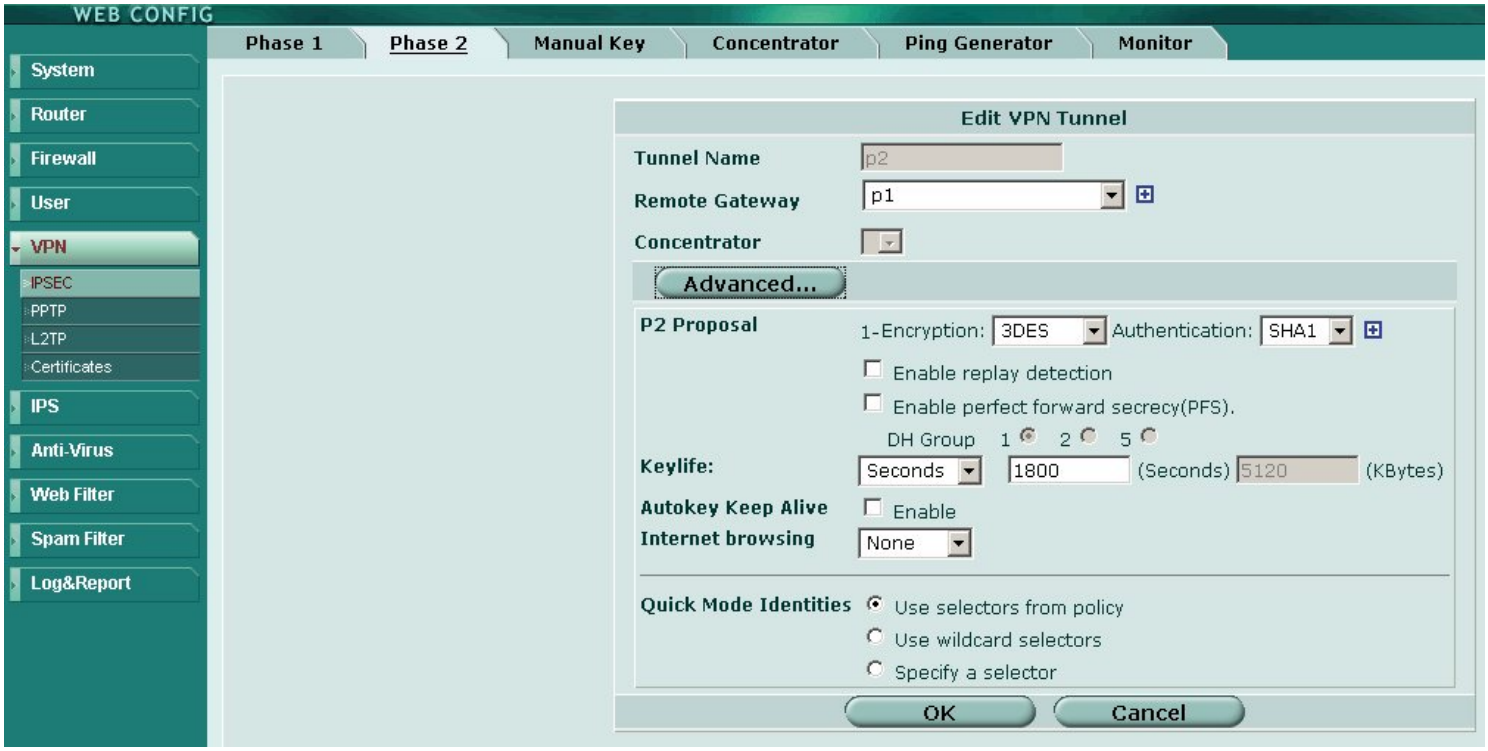


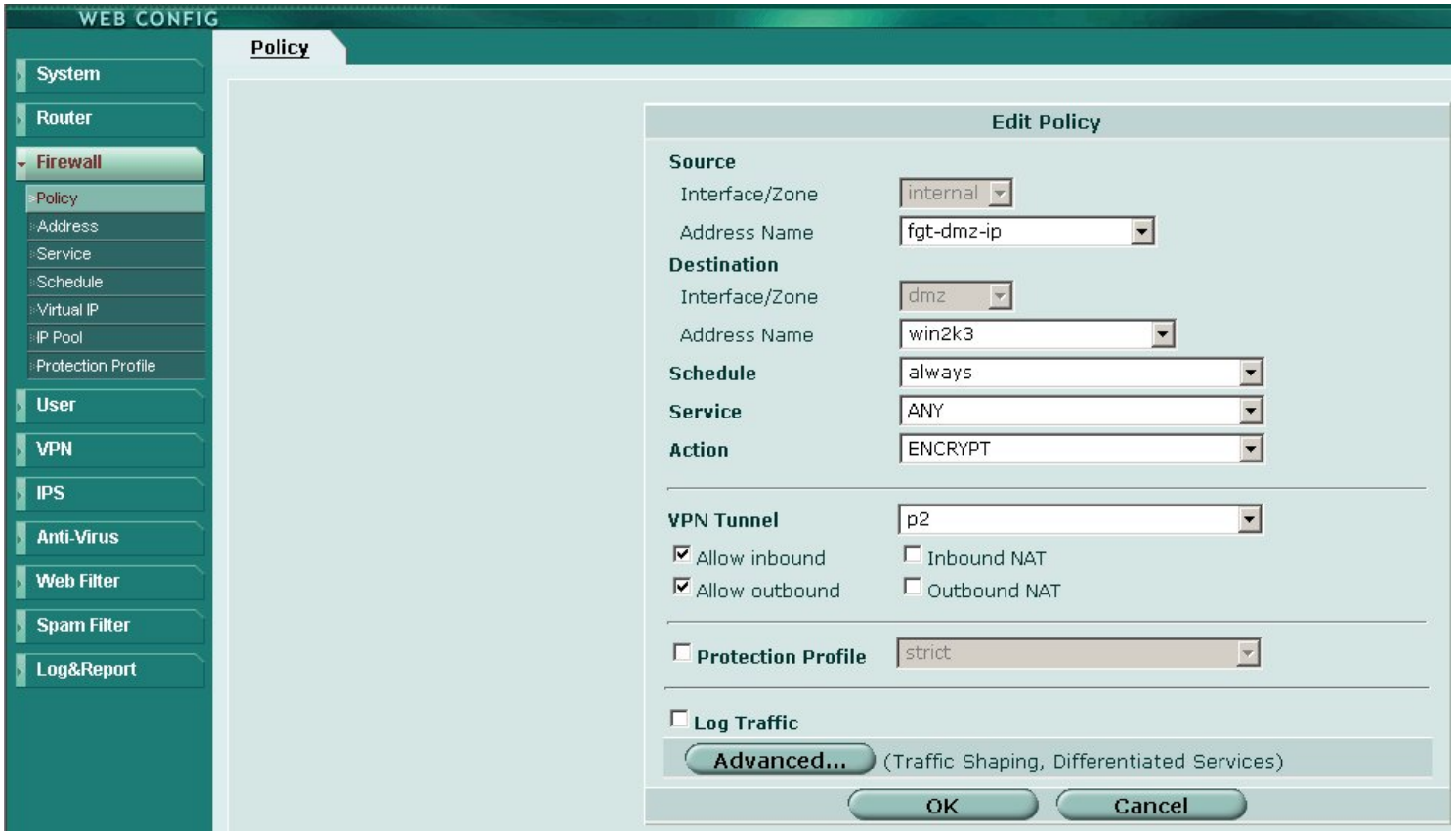
Specify host addresses for the Windows Server (win2k3) and FortiGate interface (fgt-dmz-ip).



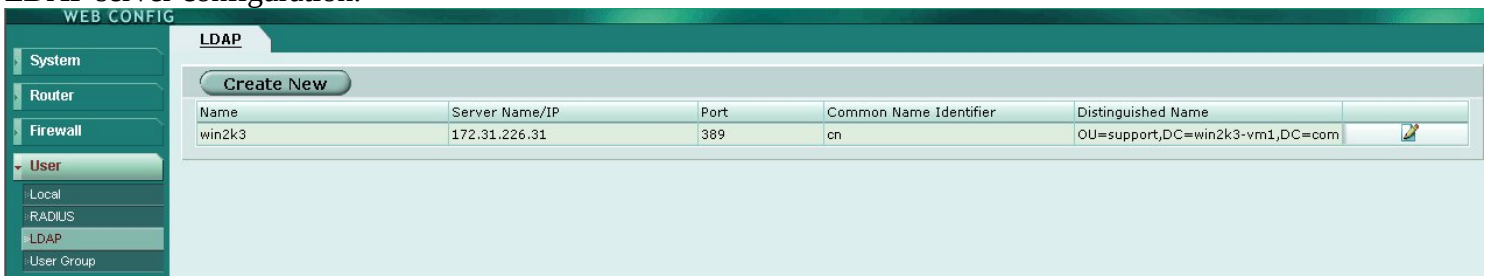
The DH Group can’t be set to 5.



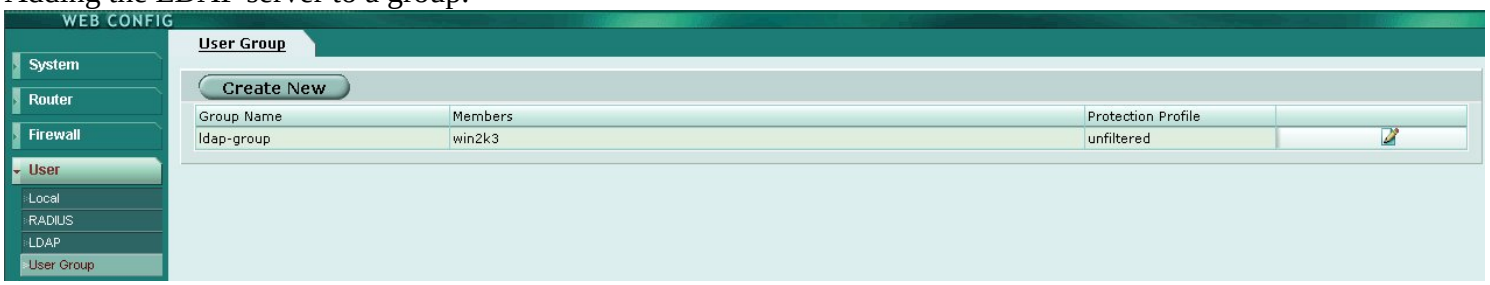




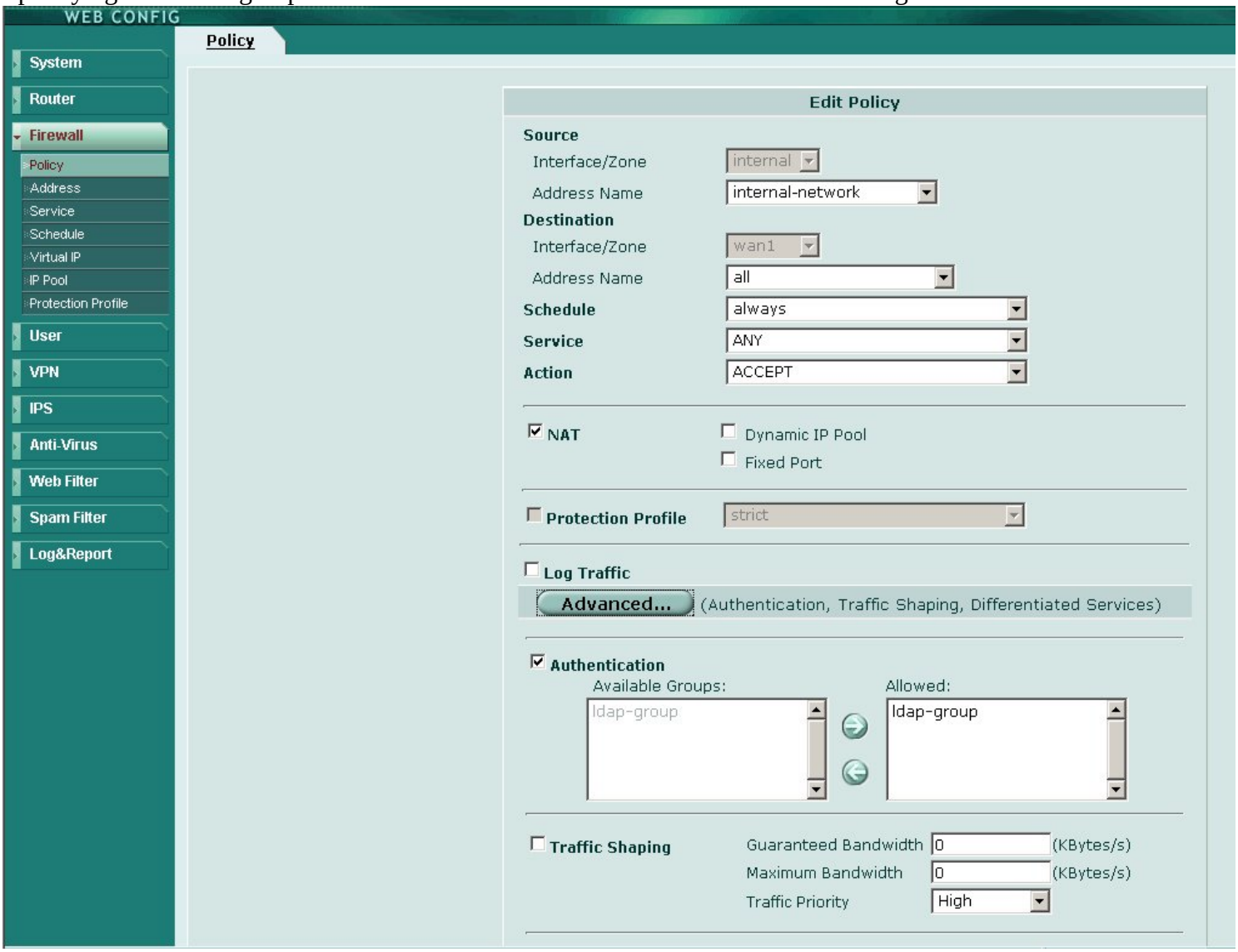
LDAP server configuration.



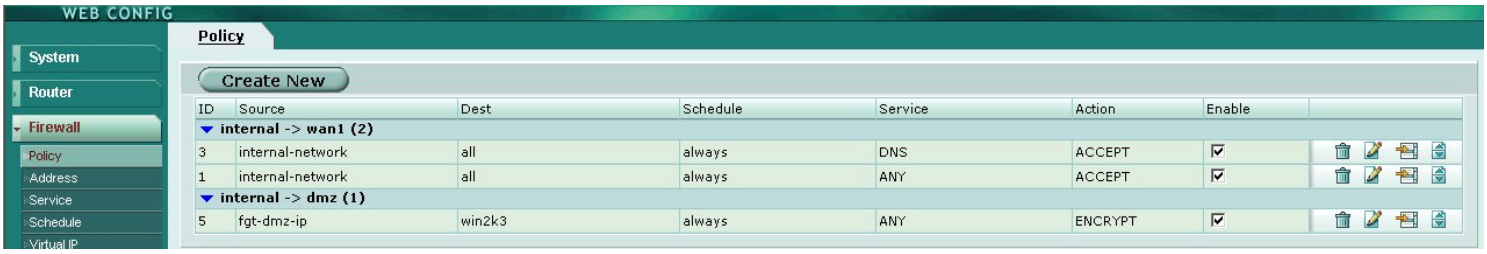
Adding the LDAP server to a group.



Specifying the LDAP group as an Authentication method for internal users accessing the Internet.



Internal -> wan1 policies are for Internet browsing with Authentication. The Internal->dmz policy is the IPSec tunnel to the Windows Server.



The following was also configured via the CLI, in order to properly support a host (i.e. 255.255.255.255) selector in the Firewall Policy:

```
config system global
    set ipsec-host-selector enable
end
```

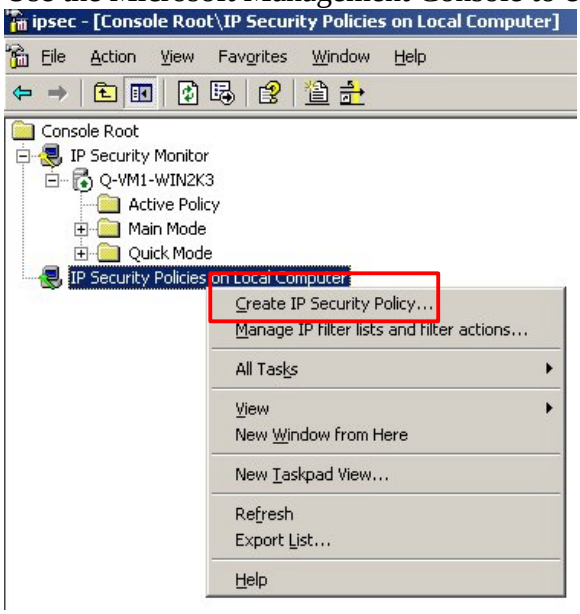
Windows Server 2003 IPSec Configuration:

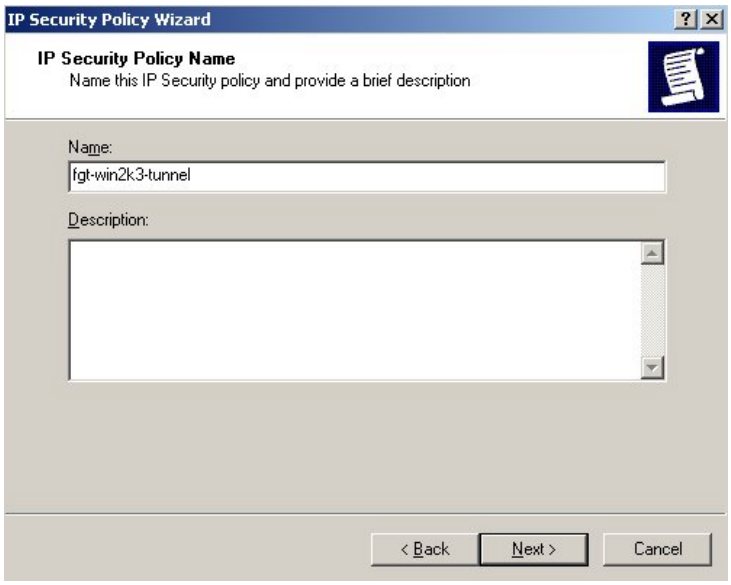
One *IP Security Policy* will be created, and it will contain **two** active *IP Security Rules.* An *IP Security Rule* consists of:

- an *IP Filter List*
- a *Filter Action*
- an *Authentication Method*
- a *Tunnel Endpoint*
- a *Connection Type.*

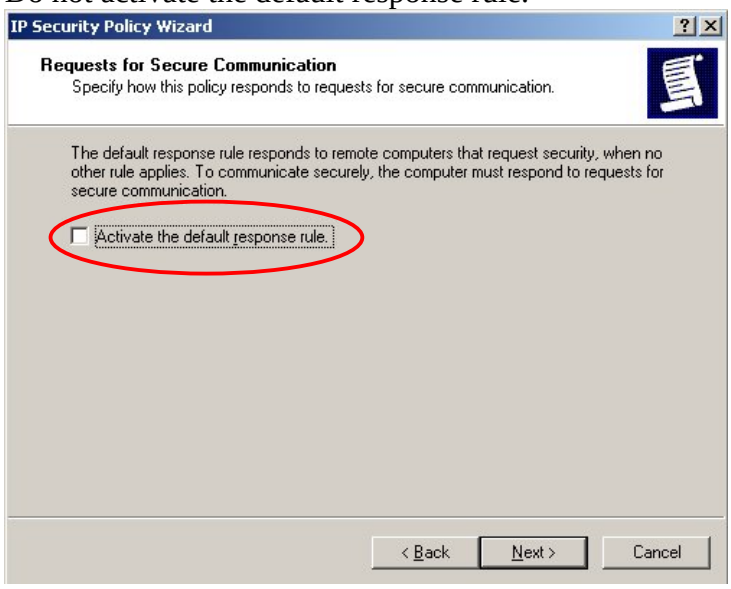
The first rule will specify the FortiGate to Windows Server tunnel and traffic flow, and the second rule will specify the reverse direction. Do not use the "Wizard" nor the "Mirror" options. Everything must be configured manually. The first rule creation will be described step-by-step. The second (opposite) rule must be created with the exact same steps as the first one, but with source and destination information reversed. The second rule creation will not be described step-by-step – only summary snapshots will be displayed.

Use the Microsoft Management Console to configure the IPSec policies.



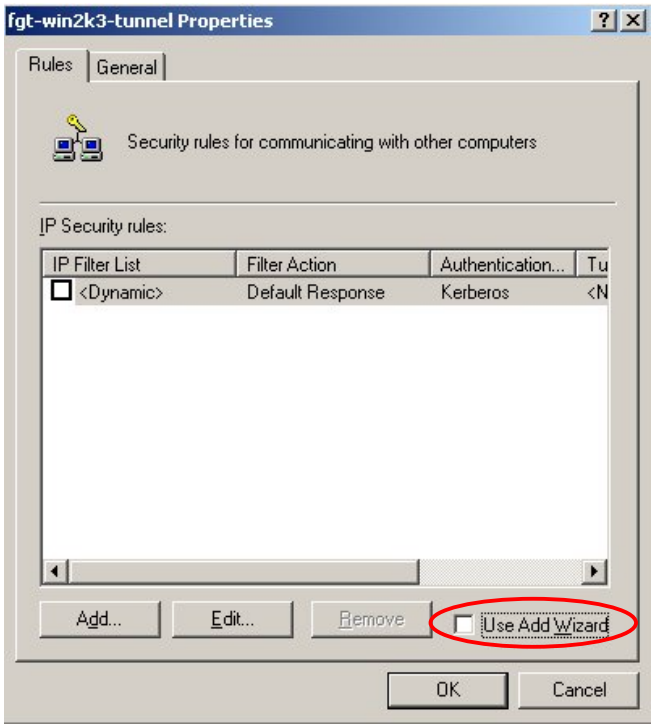


Do not activate the default response rule.

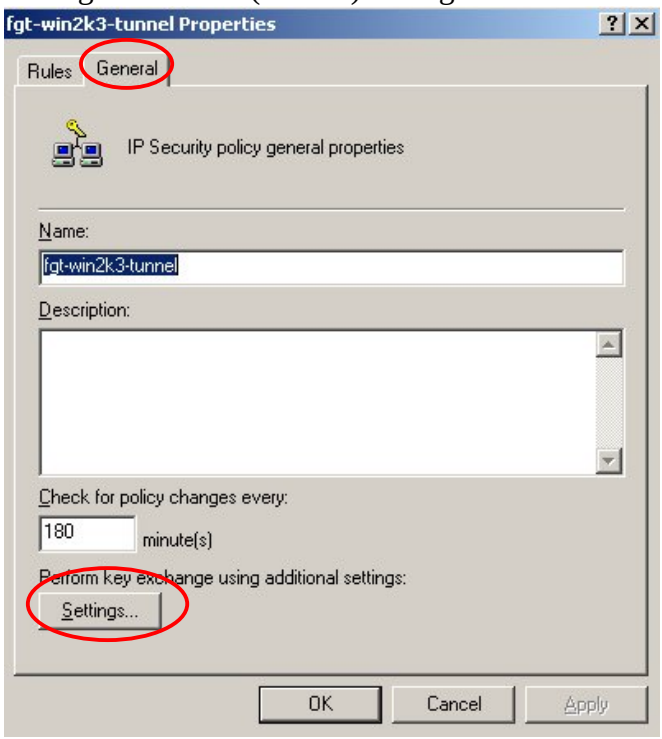


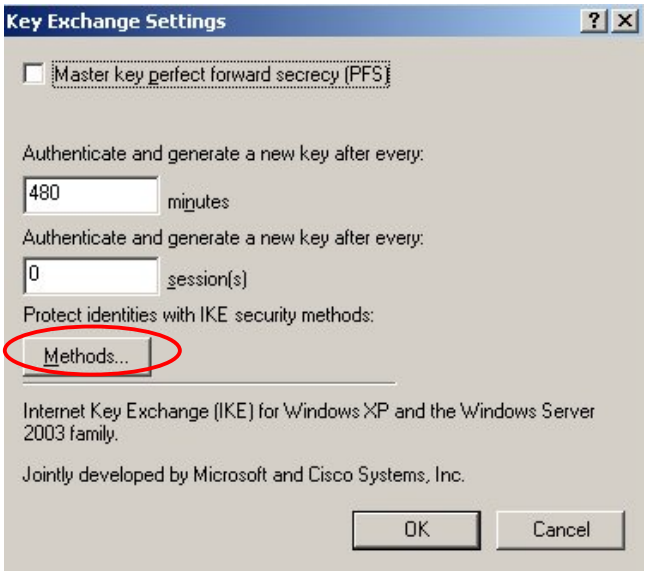
Edit the properties.

Do not use the Wizard.

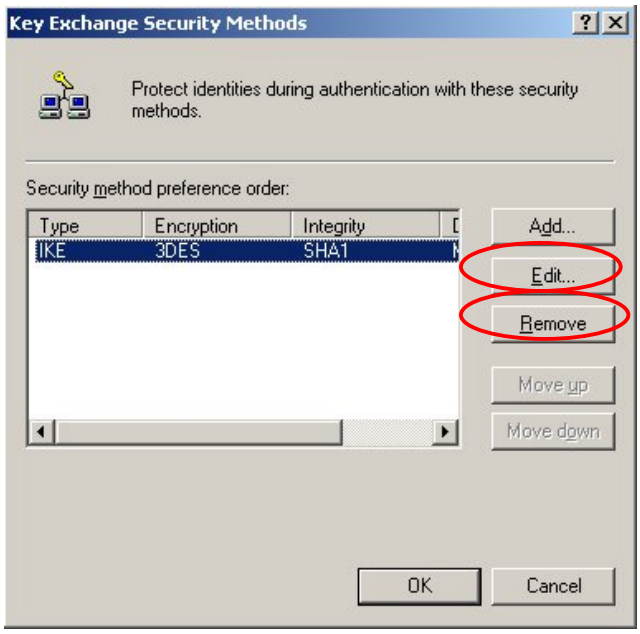


Configure the IKE (Phase1) settings.

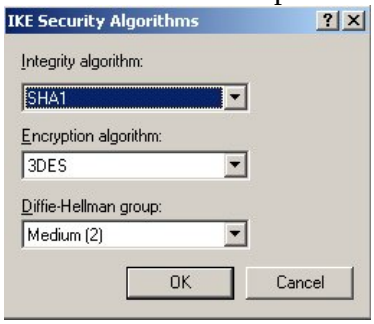




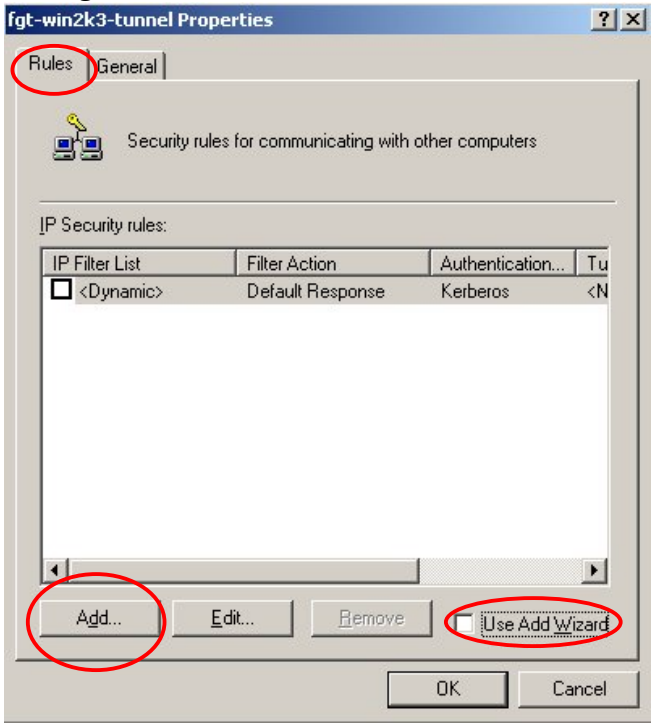
Delete all proposals except for the one that was configured on the FortiGate IPSec Phase1. In this example, keep the 3DES/SHA1 'method'.



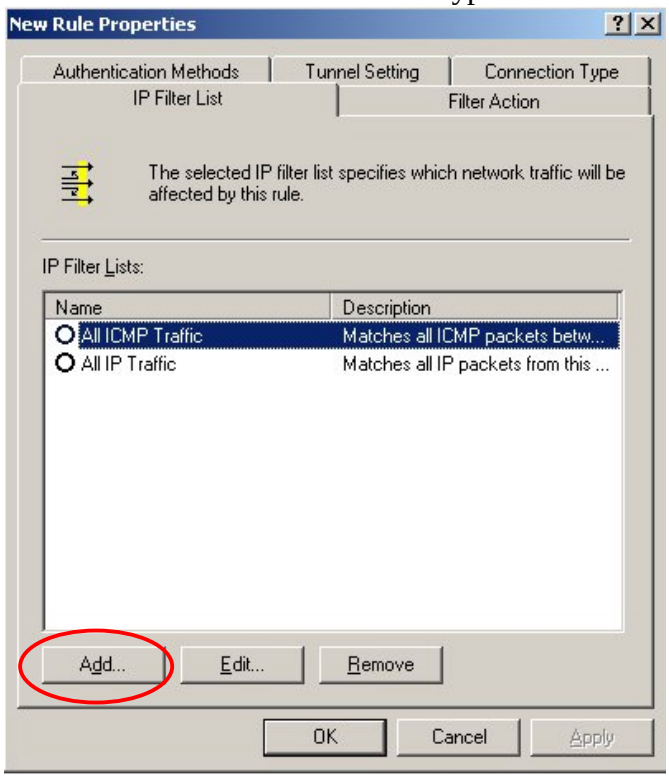
Verify the correct DH setting. The "High (2048)" setting corresponds to Group 14, which is not supported by the FortiGate. Use Group 2 instead.



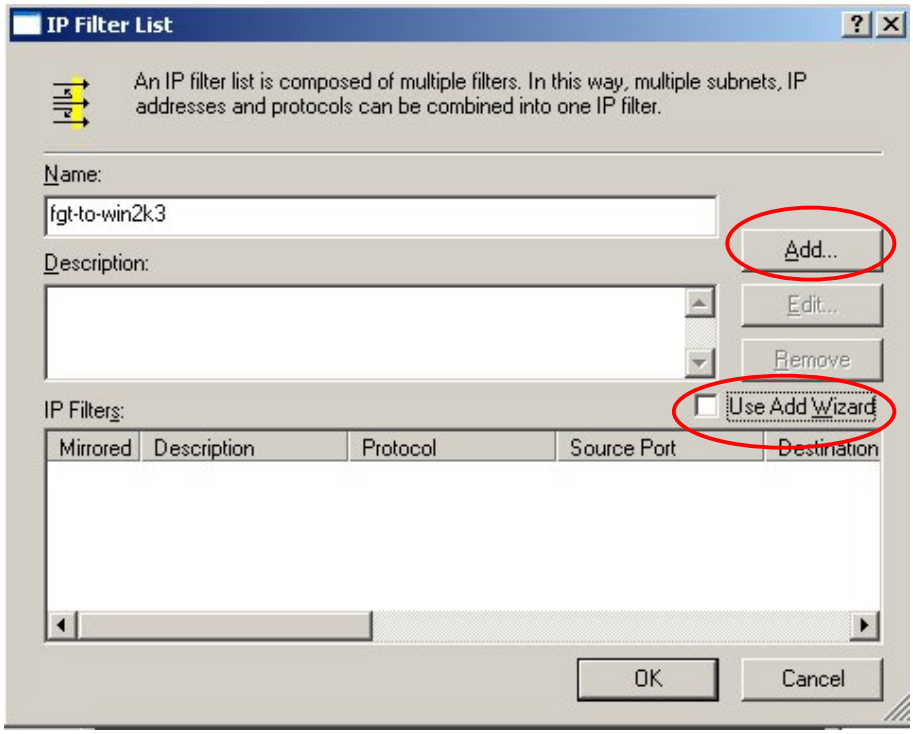
Configure the first Phase2 tunnel rule. Don't use the Wizard.



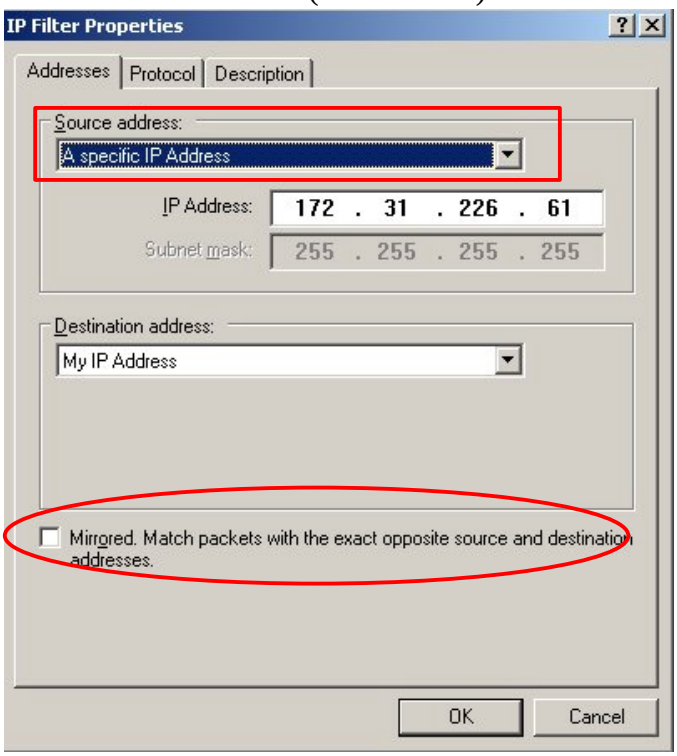
Add a Filter action which will encrypt all traffic between the FortiGate and the Windows Server.



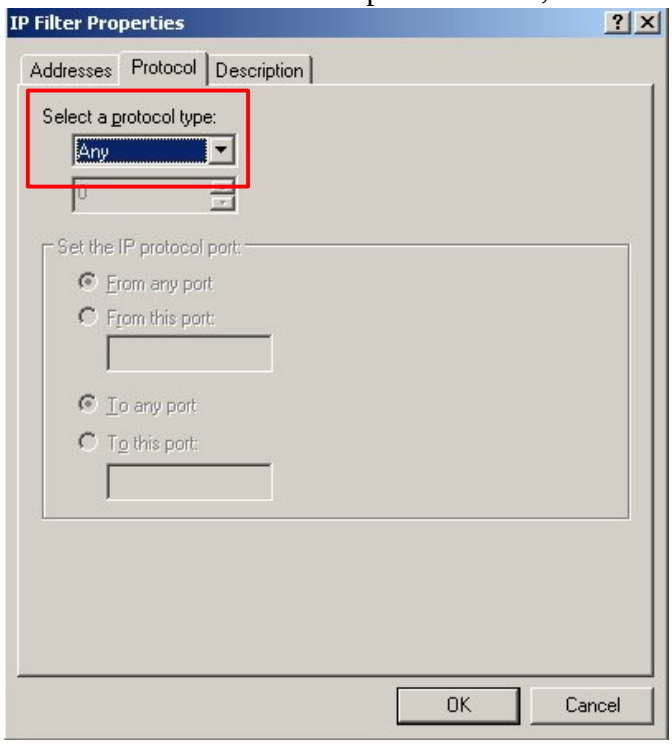
Don’t use the Wizard.

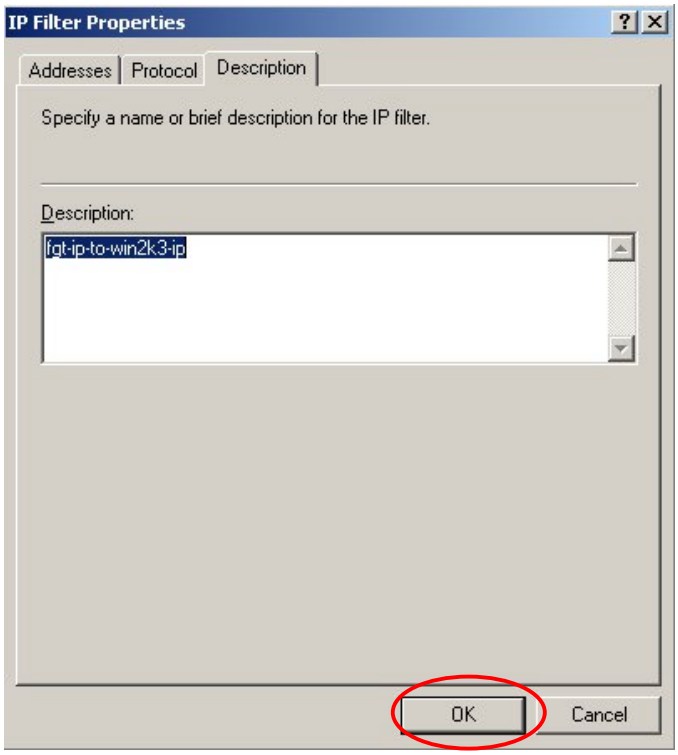


Source is the FortiGate (host address) and the Destination is the Windows Server. Do not enable “Mirrored”

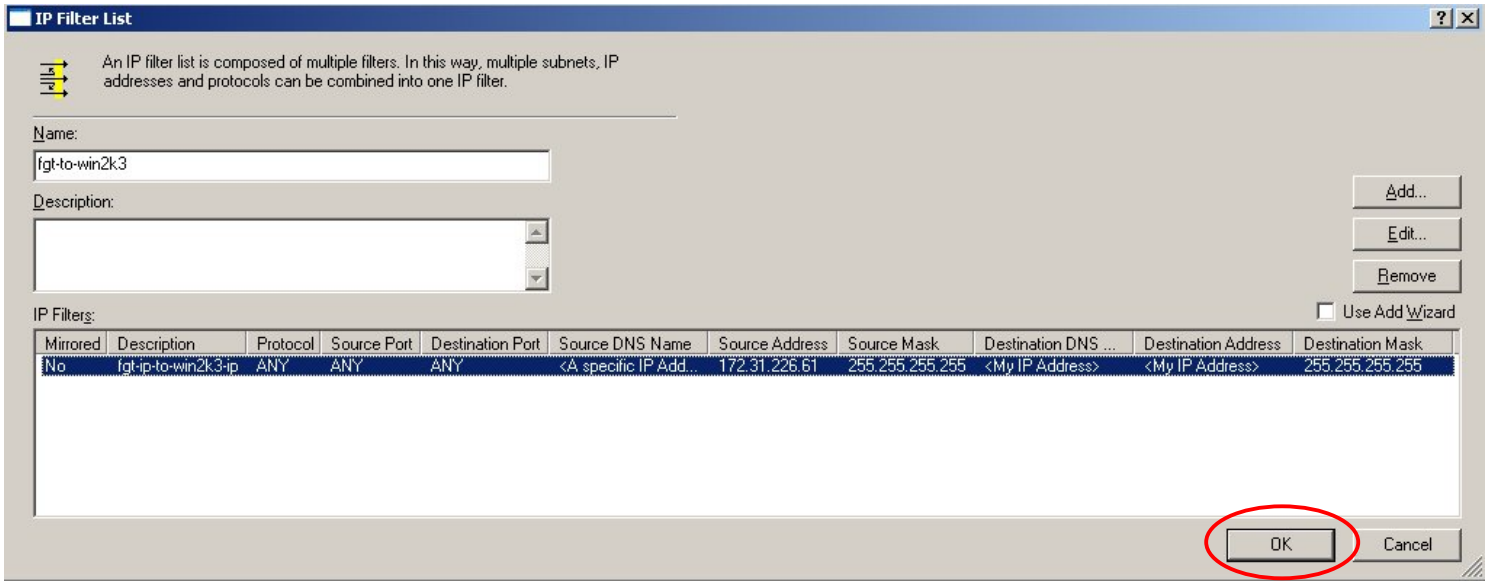


Protocol must be ANY. As per Microsoft, Protocol or Port specific tunnels are not supported.

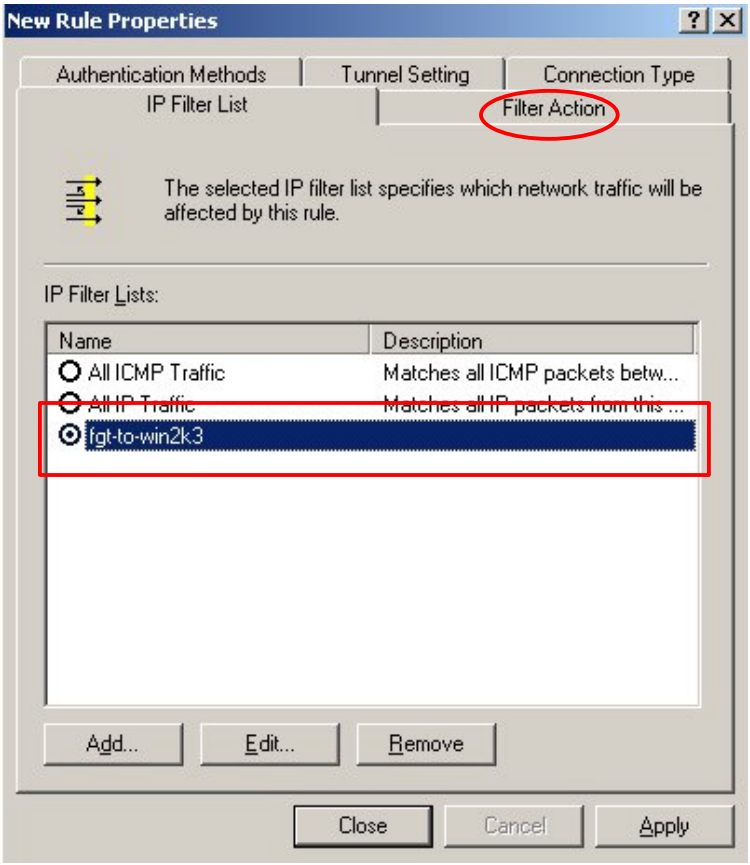




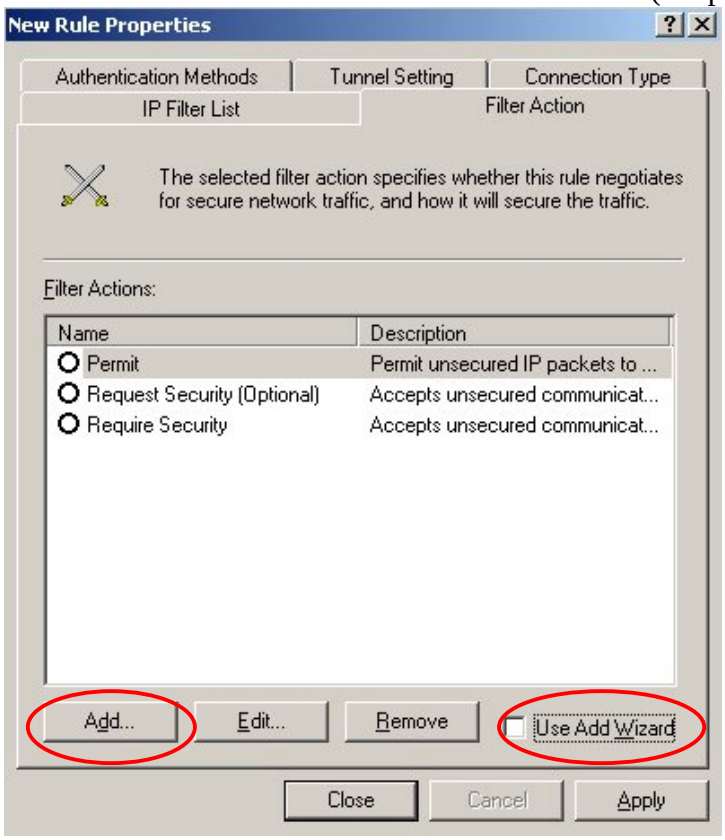
An overview of the IP Filter for this rule.

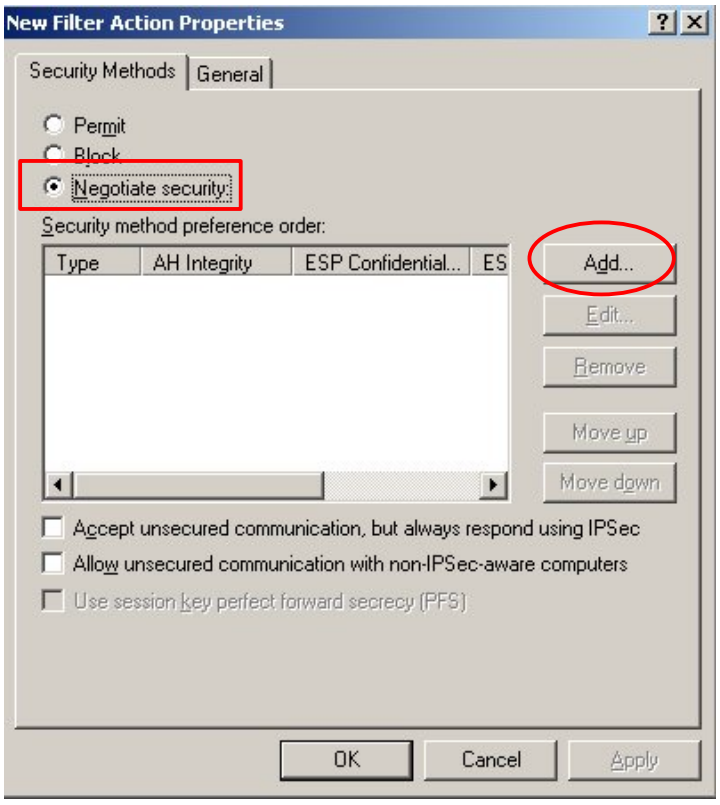


Select the IP Filter rule button and define the Filter Action (i.e. Encryption and Authentication proposals)

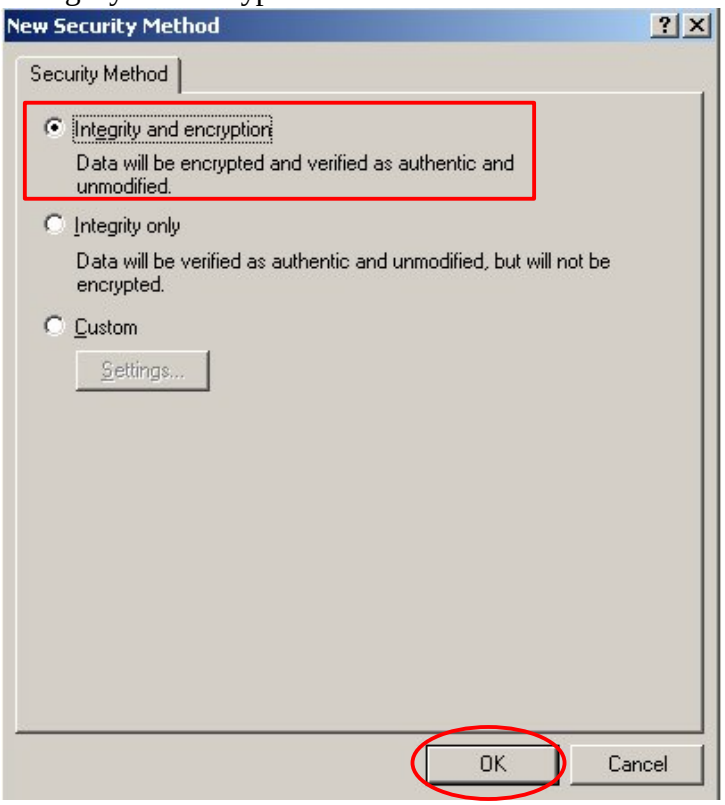


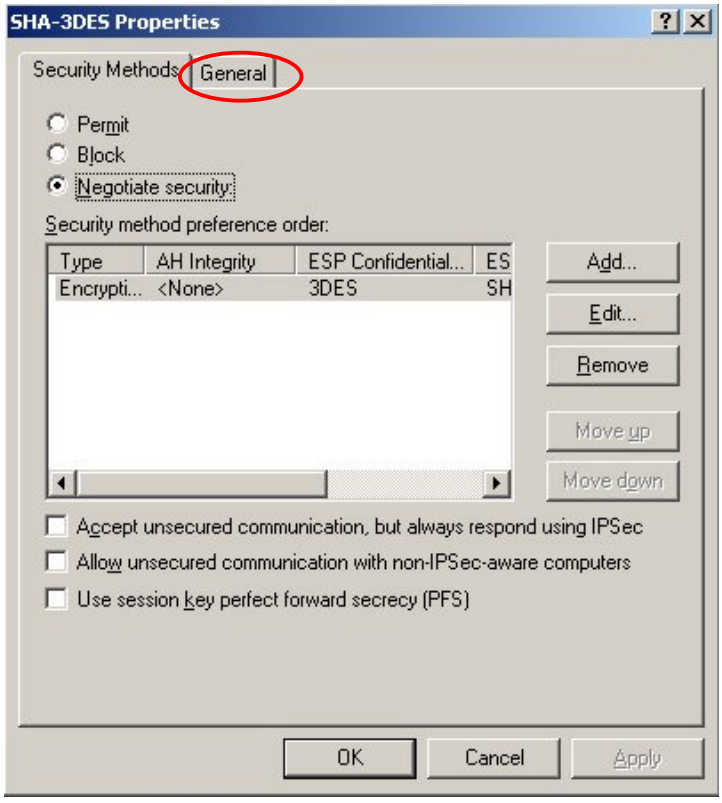
Don’t use the Wizard. Create a new Filter Action (i.e. proposal).

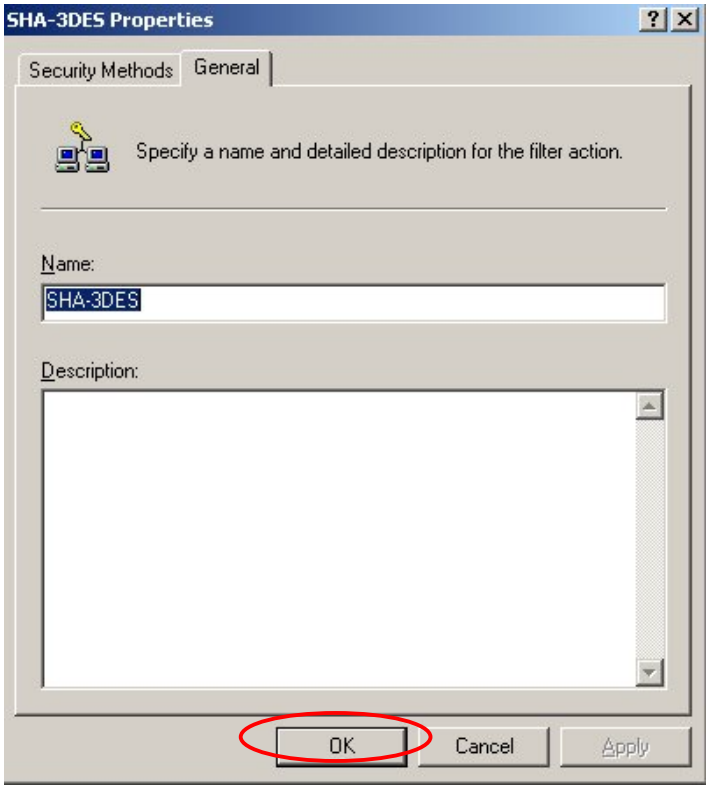




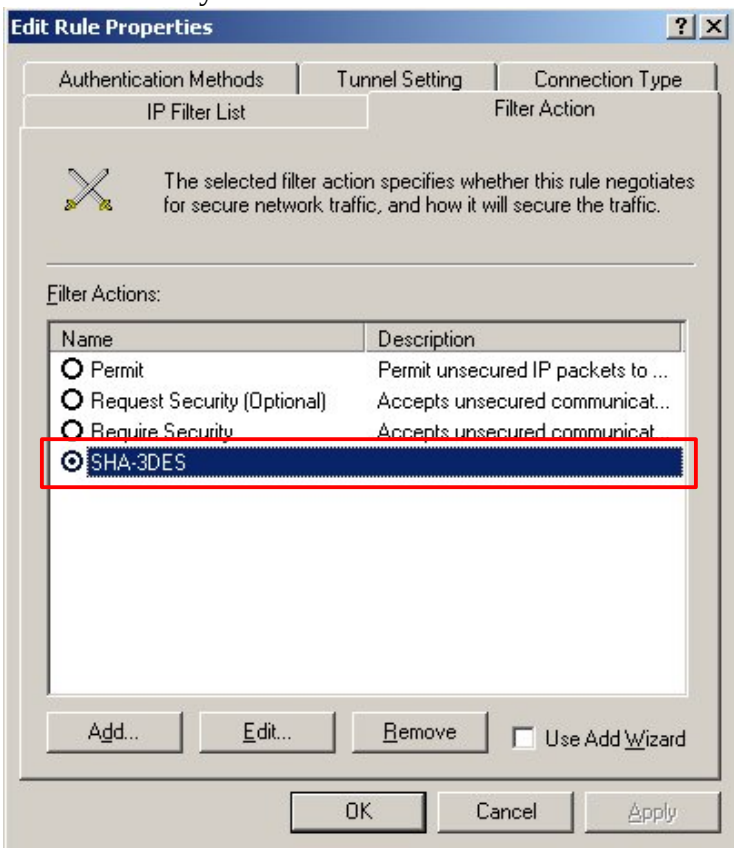
“Integrity and encryption” defaults to 3DES/SHA1.



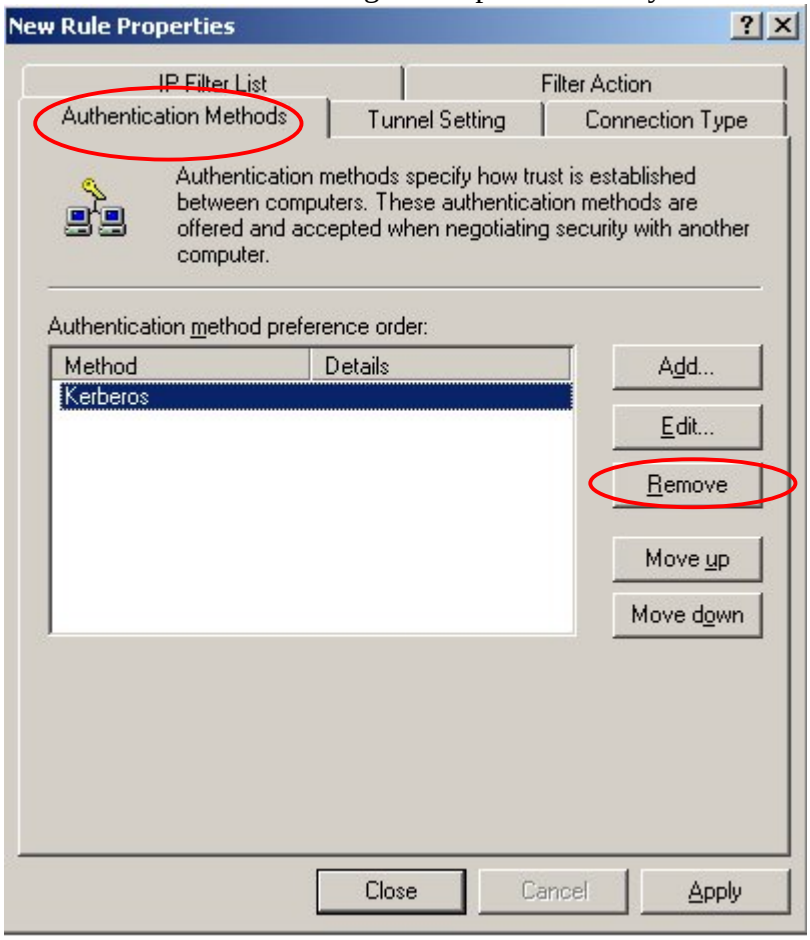


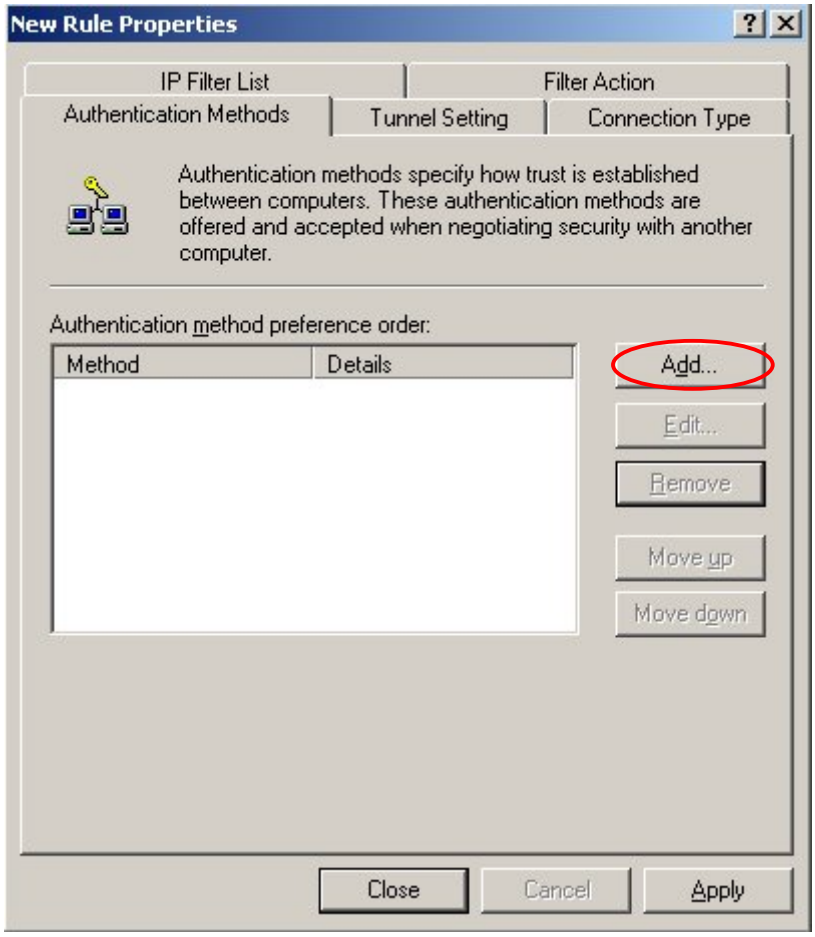


Select the newly created Filter Action for this rule.

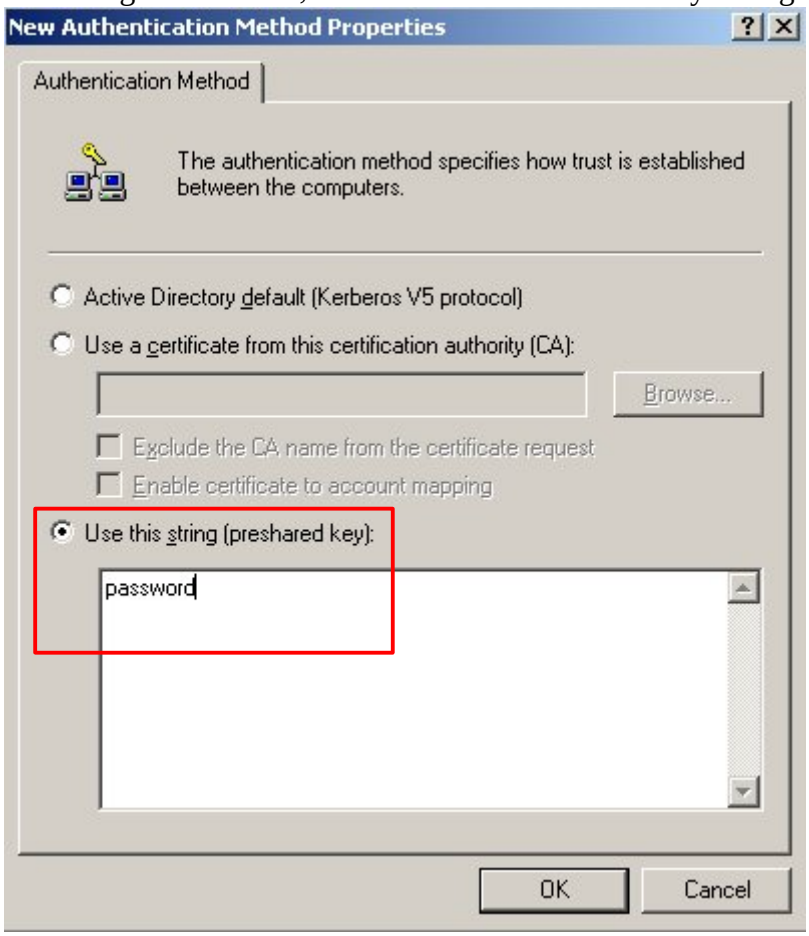


Remove Kerberos and configure the pre-shared key authentication method.

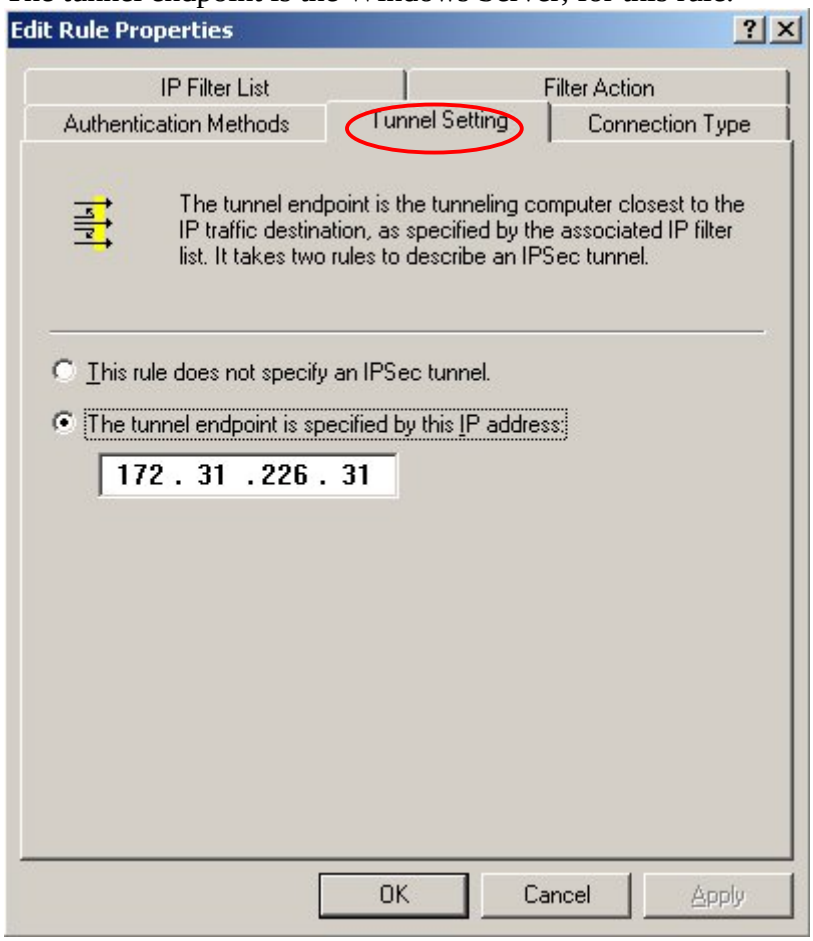


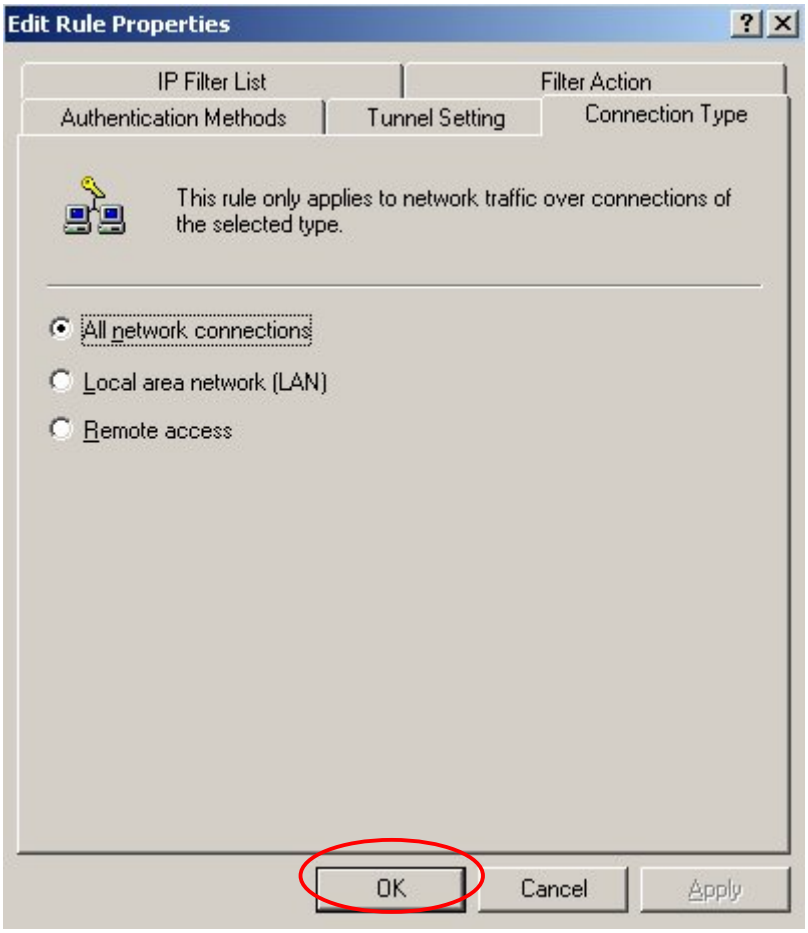


The string entered here, must match the Preshared Key configured on the FortiGate Phase1.

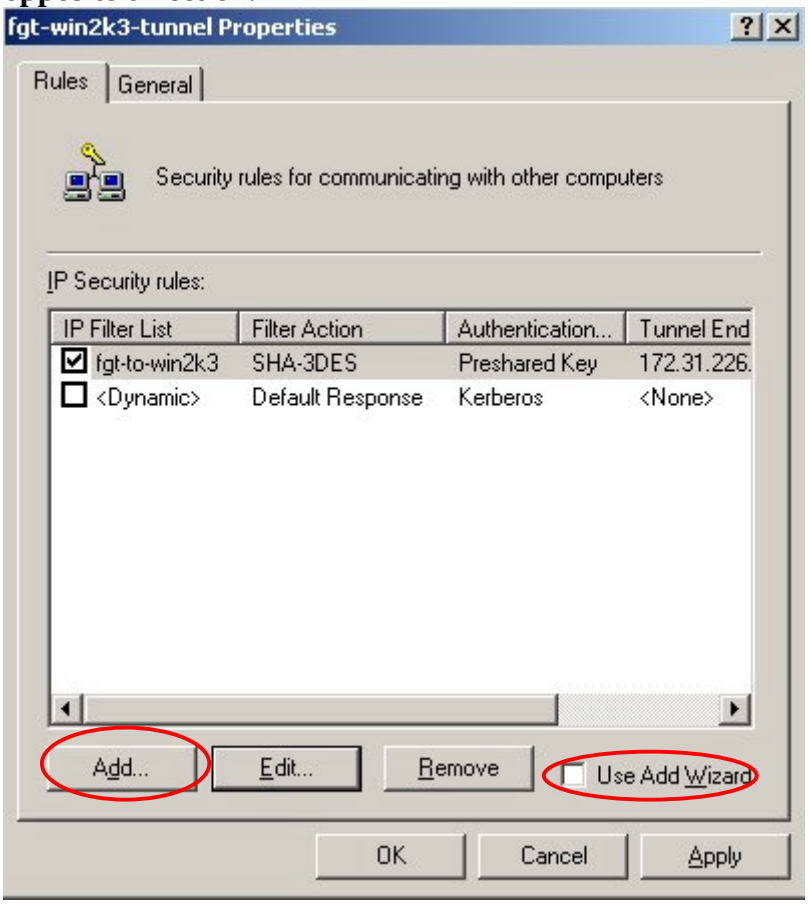


The tunnel endpoint is the Windows Server, for this rule.

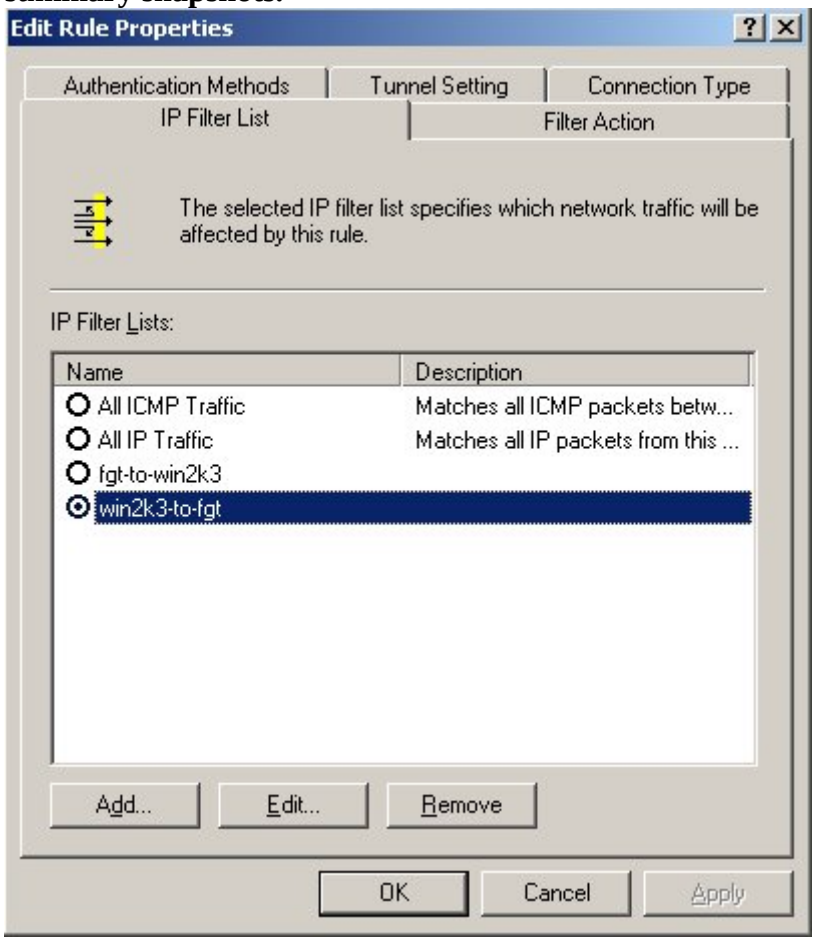


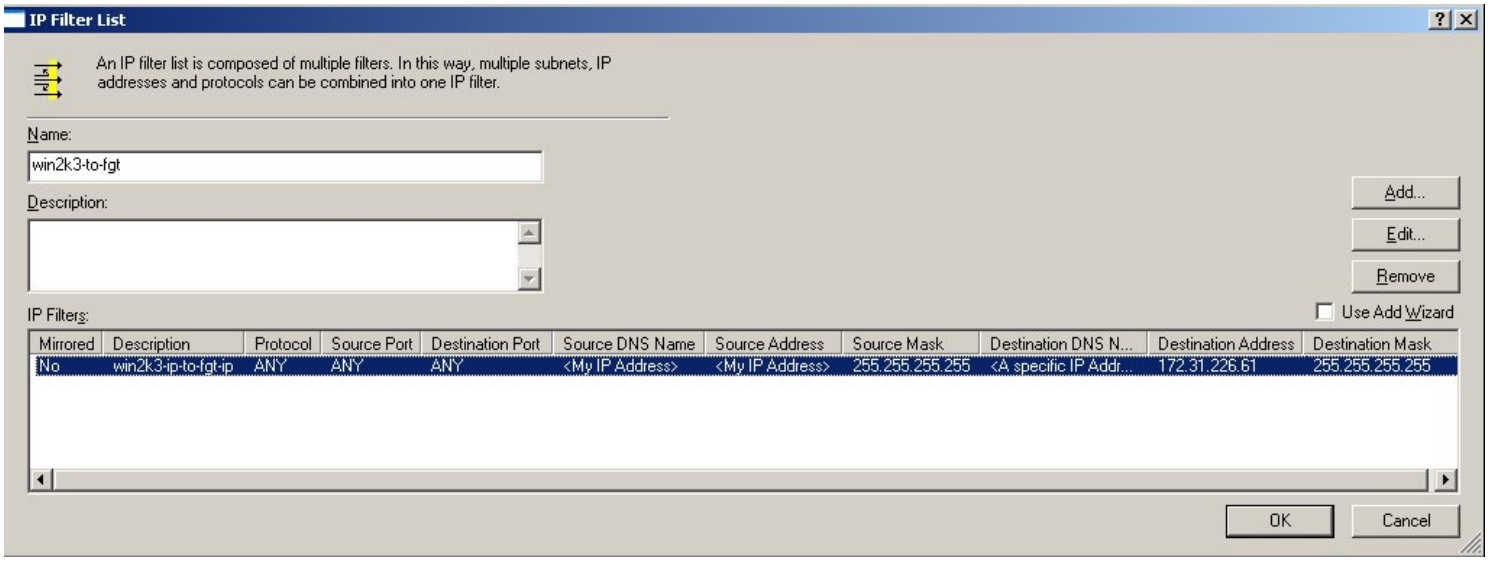


The FortiGate to Windows server tunnel rule has been configured. The same must now be done for the opposite direction.

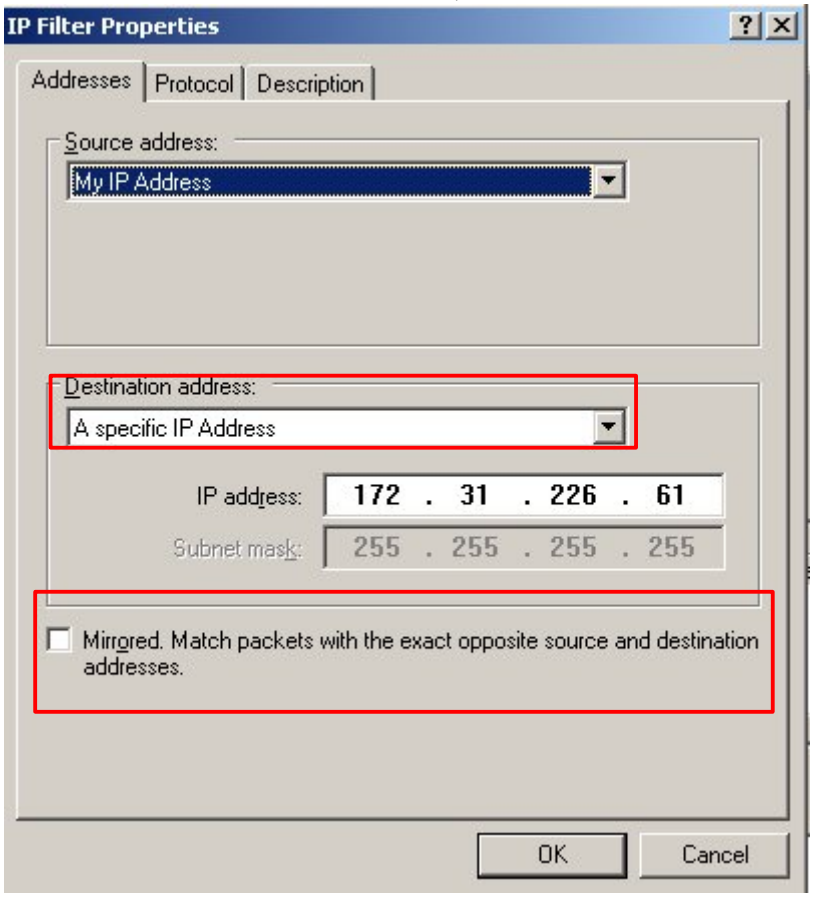


The same previous steps must be followed to create a reverse tunnel rule. Below are only displayed the summary snapshots.

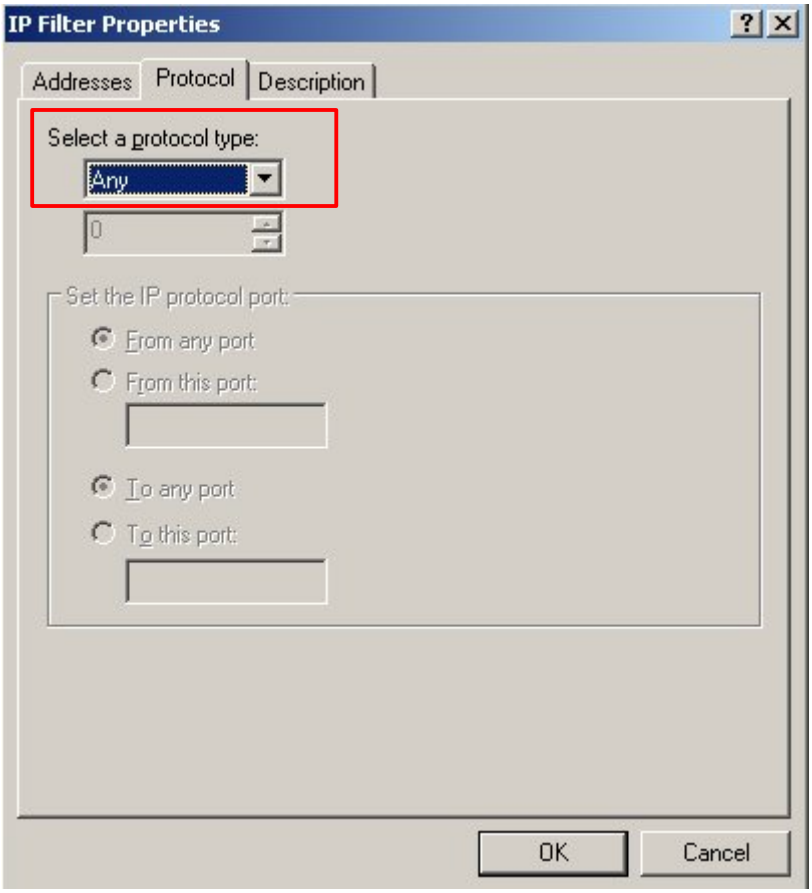


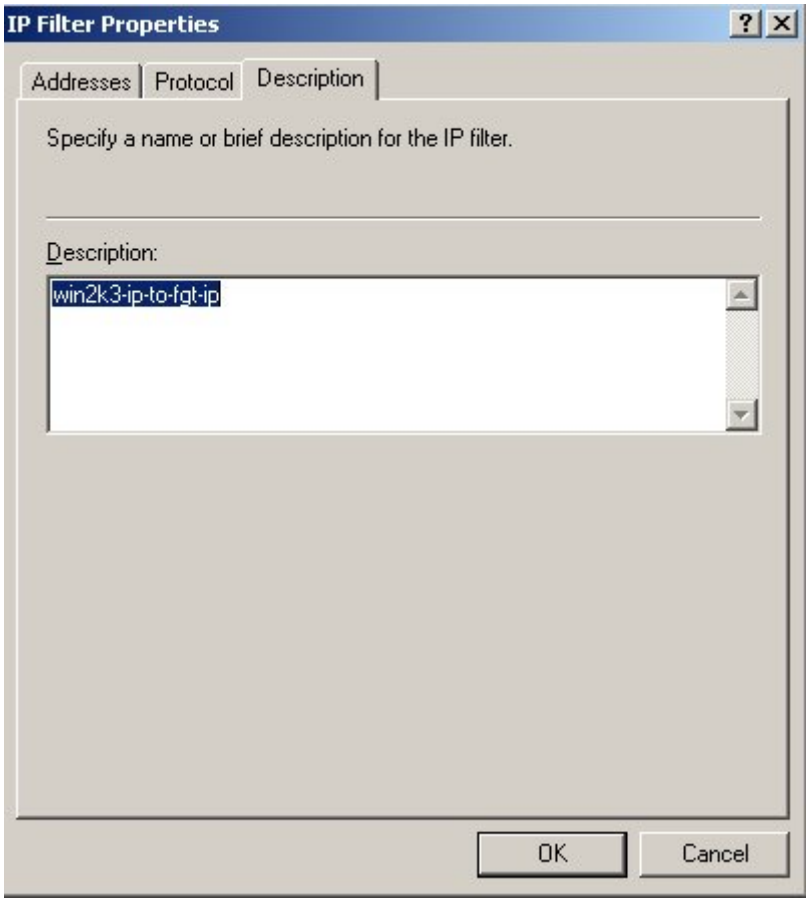


Source is now the Windows Server, and the Destination is the FortiGate. Don’t select Mirror.

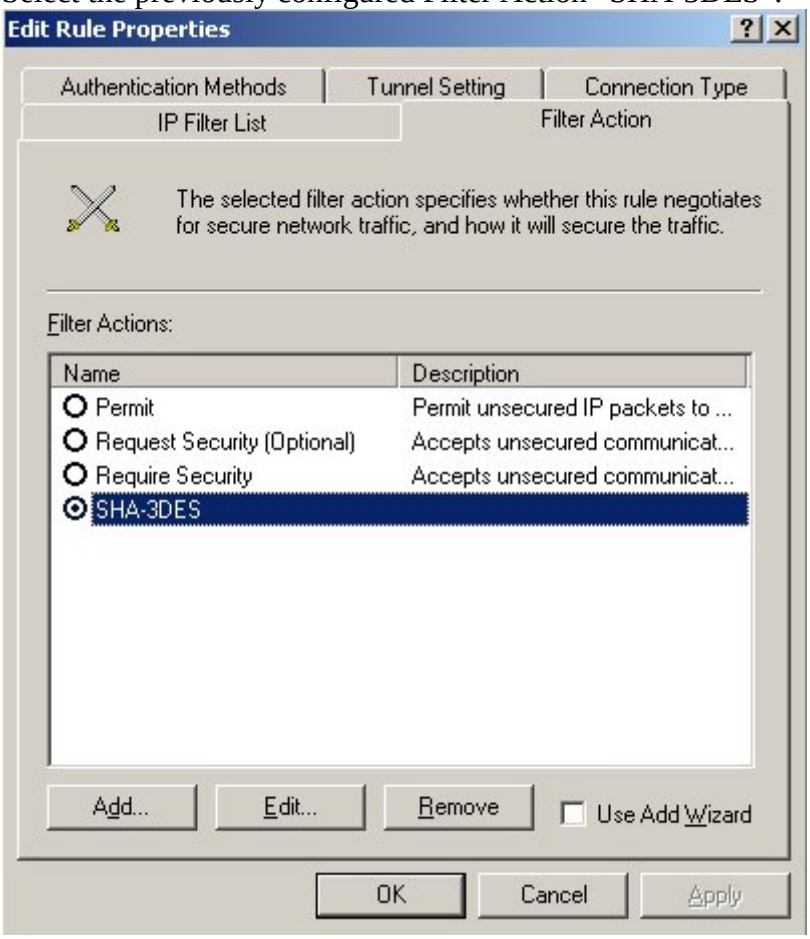


Protocol must be ANY.

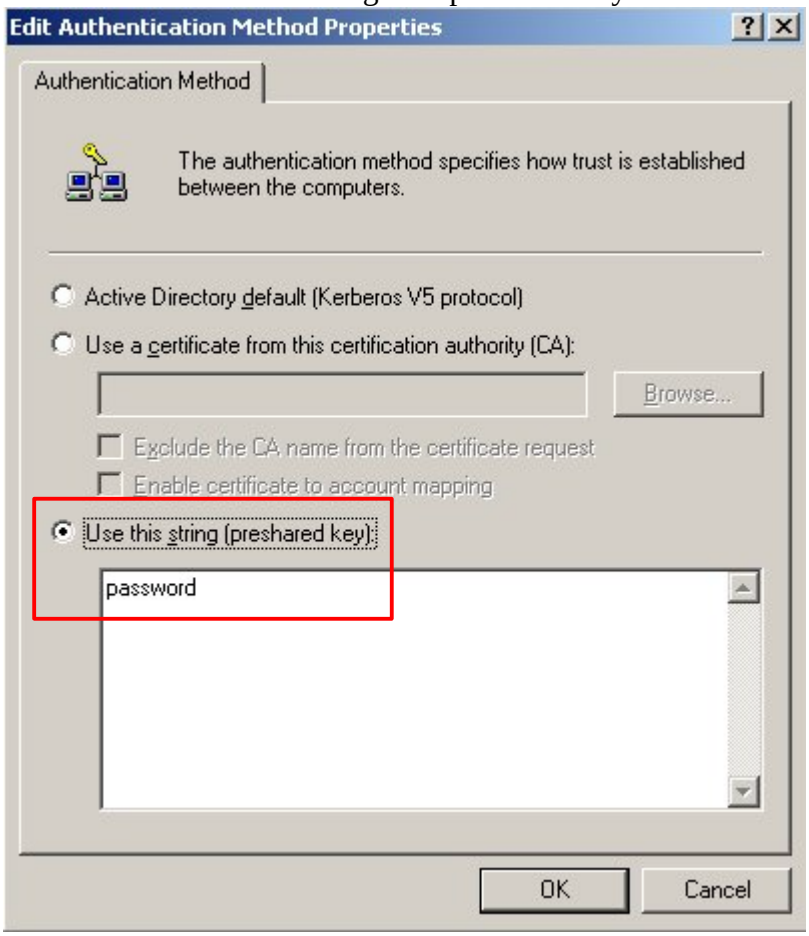


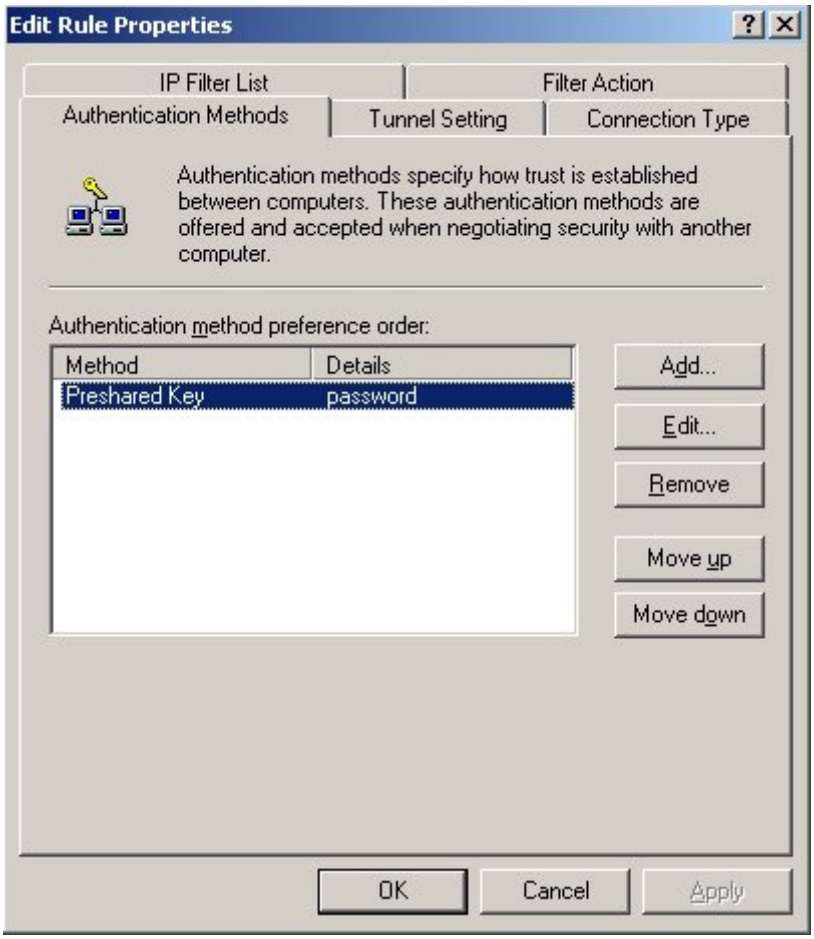


Select the previously configured Filter Action “SHA-3DES”.

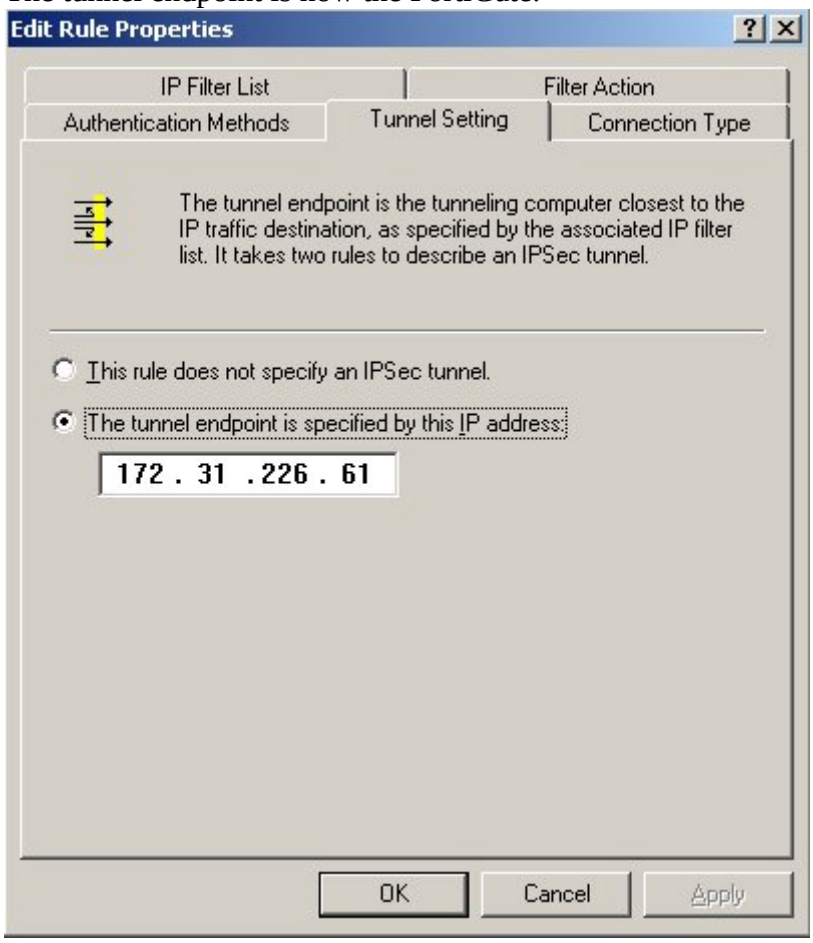


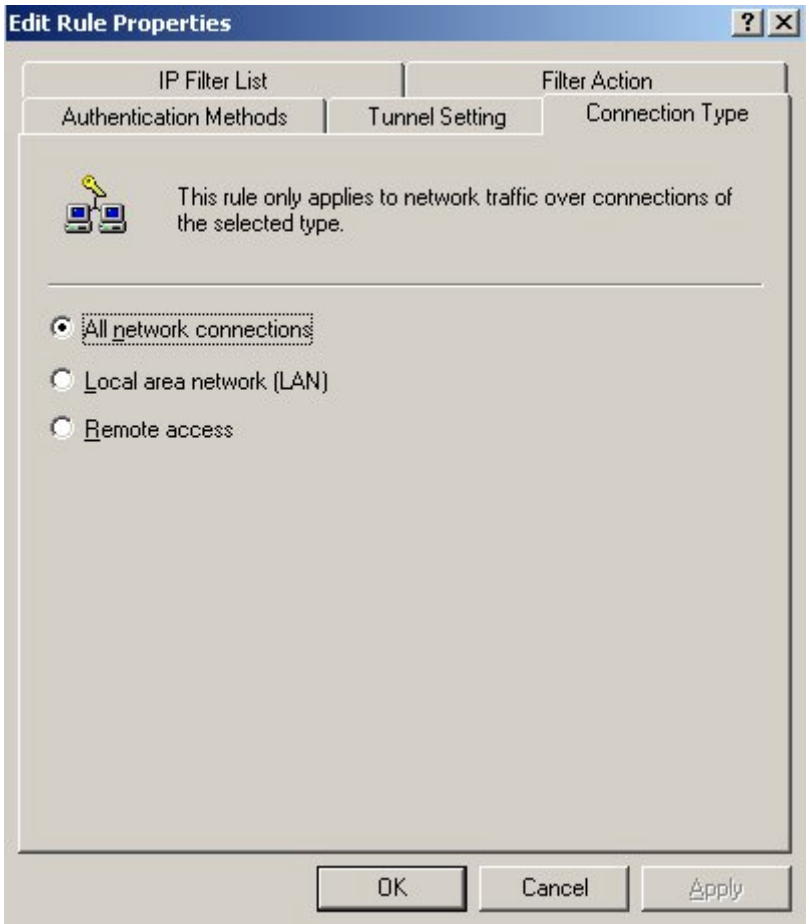
Remove Kerberos and configure a preshared key.



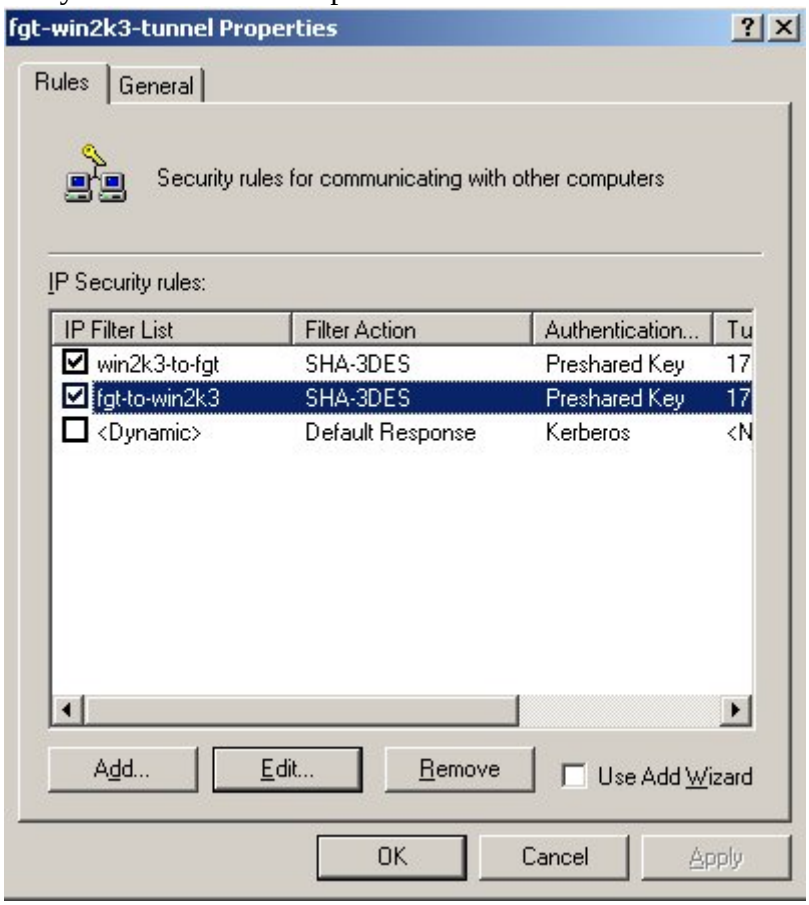


The tunnel endpoint is now the FortiGate.

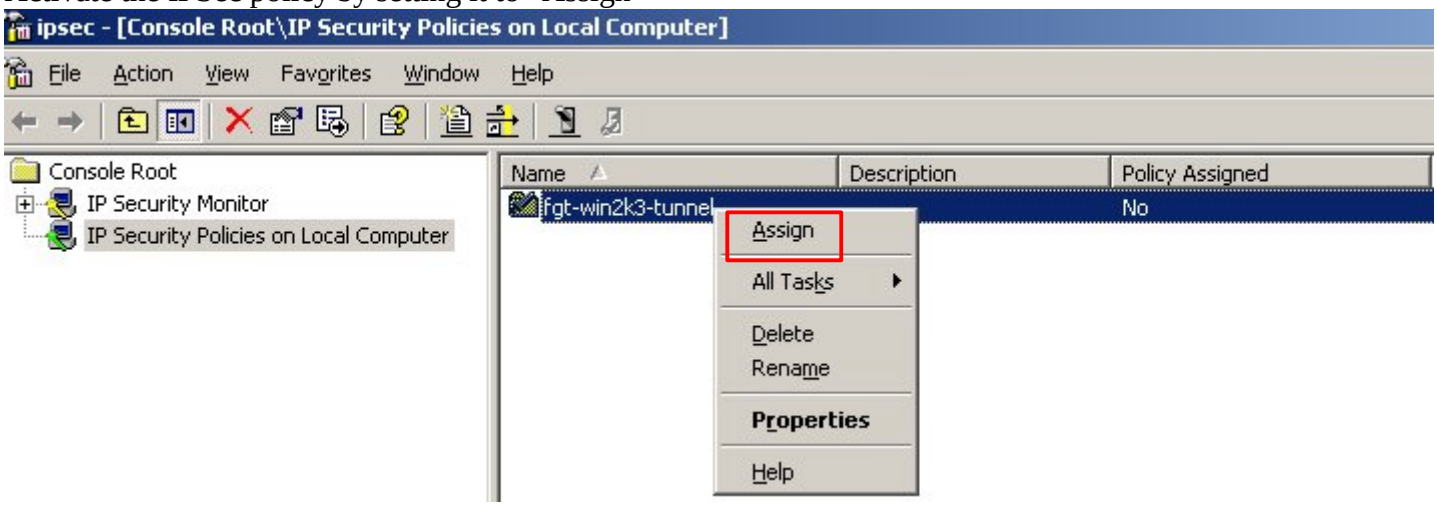




The two *IP Security* rules have been configured and selected for the *IP Security Policy*. Do not select the "<Dynamic> Default Response" one.



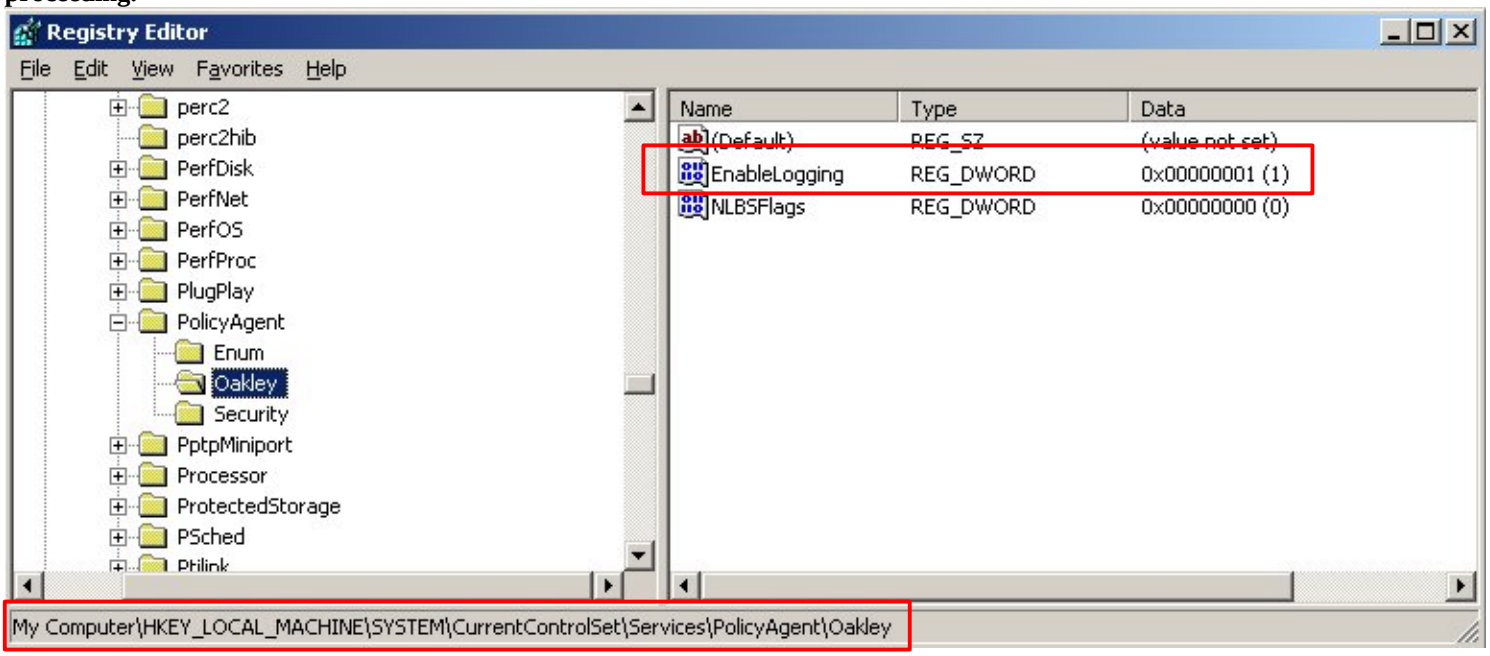
Activate the IPSec policy by setting it to "Assign"



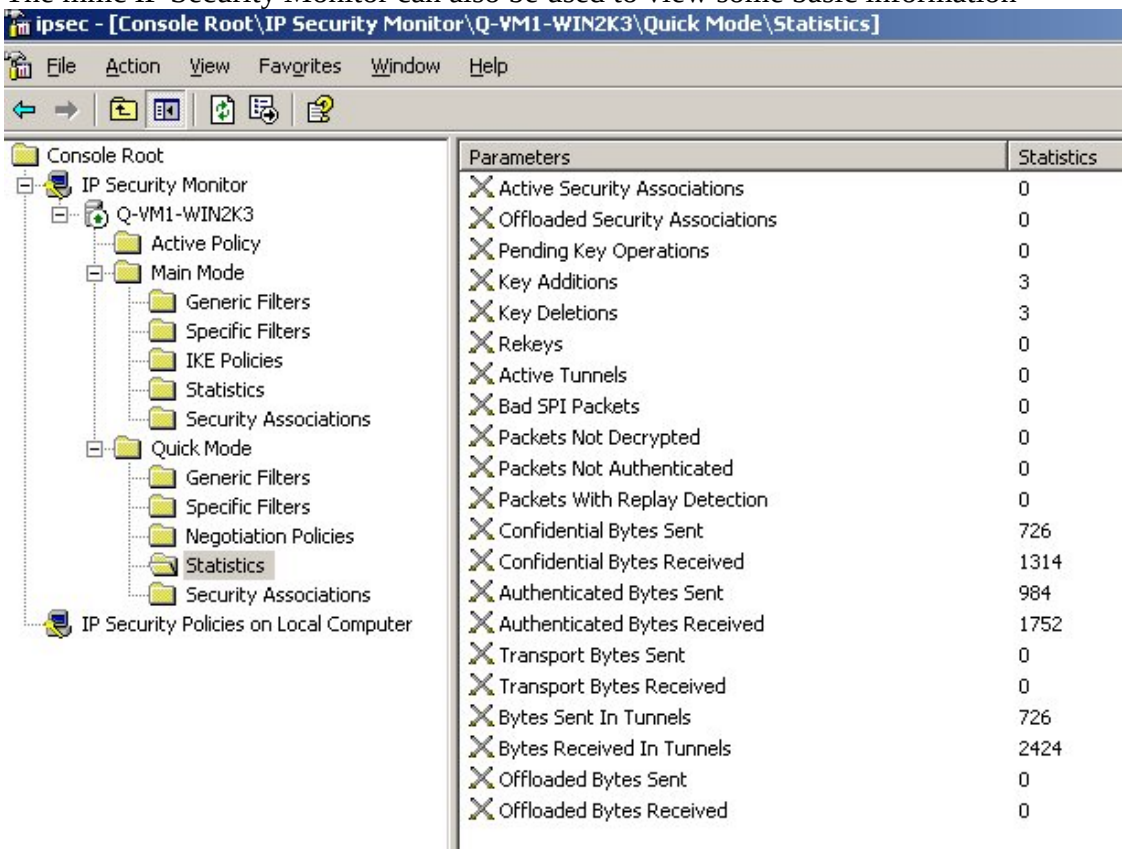
IPSec debugging:

On Windows Server perform the following registry modification, and view the C:\windows\debug\oakley.log file.

WARNING: The incorrect usage of the Windows Registry Editor can cause serious problems requiring the re-installation of your operating system and possible loss of data. Use the Registry Editor at your own risk. Please ensure that you have a backup before proceeding.



The mmc IP Security Monitor can also be used to view some basic information



On the FortiGate, enable the following CLI commands:

```
diag deb en
diag deb appl ike 2
```

The following can also be used:

```
diag vpn tun list
diag vpn gw list
```

Example debug log outputs:

Windows oakley.log:

```
3-14: 18:01:40:687:780 Receive: (get) SA = 0x00000000 from 172.31.226.61.500
 3-14: 18:01:40:687:780 ISAKMP Header: (V1.0), len = 100
 3-14: 18:01:40:687:780   I-COOKIE afda38a347aaed8c
 3-14: 18:01:40:687:780   R-COOKIE 0000000000000000
 3-14: 18:01:40:687:780   exchange: Oakley Main Mode
 3-14: 18:01:40:687:780   flags: 0
 3-14: 18:01:40:687:780   next payload: SA
 3-14: 18:01:40:687:780   message ID: 00000000
 3-14: 18:01:40:687:780 Filter to match: Src 172.31.226.61 Dst 172.31.226.31
 3-14: 18:01:40:687:780 MM PolicyName: 3
 3-14: 18:01:40:687:780 MMPolicy dwFlags 2 SoftSAExpireTime 28800
 3-14: 18:01:40:687:780 MMOffer[0] LifetimeSec 28800 QMLimit 0 DHGroup 2
 3-14: 18:01:40:687:780 MMOffer[0] Encrypt: Triple DES CBC Hash: SHA
 3-14: 18:01:40:687:780 Auth[0]:PresharedKey KeyLen 16
 3-14: 18:01:40:687:780 Responding with new SA 40d0bb0
 3-14: 18:01:40:687:780 processing payload SA
 3-14: 18:01:40:687:780 Received Phase 1 Transform 1
 3-14: 18:01:40:687:780      Life type in Seconds
 3-14: 18:01:40:687:780      Life duration of 28800
 3-14: 18:01:40:687:780      Encryption Alg Triple DES CBC(5)
 3-14: 18:01:40:687:780      Hash Alg SHA(2)
 3-14: 18:01:40:687:780      Auth Method Preshared Key(1)
 3-14: 18:01:40:687:780      Oakley Group 2
 3-14: 18:01:40:687:780 Phase 1 SA accepted: transform=1
 3-14: 18:01:40:687:780 SA - Oakley proposal accepted
 3-14: 18:01:40:687:780 processing payload VENDOR ID
 3-14: 18:01:40:687:780 ClearFragList
 3-14: 18:01:40:687:780 constructing ISAKMP Header
 3-14: 18:01:40:687:780 constructing SA (ISAKMP)
 3-14: 18:01:40:687:780 Constructing Vendor MS NT5 ISAKMPOAKLEY
 3-14: 18:01:40:687:780 Constructing Vendor FRAGMENTATION
 3-14: 18:01:40:687:780 Constructing Vendor draft-ietf-ipsec-nat-t-ike-02
 3-14: 18:01:40:687:780
 3-14: 18:01:40:687:780 Sending: SA = 0x040D0BB0 to 172.31.226.61:Type 2.500
 3-14: 18:01:40:687:780 ISAKMP Header: (V1.0), len = 148
 3-14: 18:01:40:687:780   I-COOKIE afda38a347aaed8c
 3-14: 18:01:40:687:780   R-COOKIE 01a1ed1c3b47d706
 3-14: 18:01:40:687:780   exchange: Oakley Main Mode
 3-14: 18:01:40:687:780   flags: 0
 3-14: 18:01:40:687:780   next payload: SA
 3-14: 18:01:40:687:780   message ID: 00000000
 3-14: 18:01:40:687:780 Ports S:f401 D:f401
 3-14: 18:01:40:718:780
 3-14: 18:01:40:718:780 Receive: (get) SA = 0x040d0bb0 from 172.31.226.61.500
 3-14: 18:01:40:718:780 ISAKMP Header: (V1.0), len = 180
 3-14: 18:01:40:718:780   I-COOKIE afda38a347aaed8c
 3-14: 18:01:40:718:780   R-COOKIE 01a1ed1c3b47d706
 3-14: 18:01:40:718:780   exchange: Oakley Main Mode
 3-14: 18:01:40:718:780   flags: 0
 3-14: 18:01:40:718:780   next payload: KE
 3-14: 18:01:40:718:780   message ID: 00000000
 3-14: 18:01:40:718:780 processing payload KE
 3-14: 18:01:40:781:780 processing payload NONCE
 3-14: 18:01:40:781:780 ClearFragList
 3-14: 18:01:40:781:780 constructing ISAKMP Header
 3-14: 18:01:40:781:780 constructing KE
 3-14: 18:01:40:781:780 constructing NONCE (ISAKMP)
```

```
 3-14: 18:01:40:781:780
 3-14: 18:01:40:781:780 Sending: SA = 0x040D0BB0 to 172.31.226.61:Type 2.500
 3-14: 18:01:40:781:780 ISAKMP Header: (V1.0), len = 184
 3-14: 18:01:40:781:780   I-COOKIE afda38a347aaed8c
 3-14: 18:01:40:781:780   R-COOKIE 01a1ed1c3b47d706
 3-14: 18:01:40:781:780   exchange: Oakley Main Mode
 3-14: 18:01:40:781:780   flags: 0
 3-14: 18:01:40:781:780   next payload: KE
 3-14: 18:01:40:781:780   message ID: 00000000
 3-14: 18:01:40:781:780 Ports S:f401 D:f401
 3-14: 18:01:40:812:780
 3-14: 18:01:40:812:780 Receive: (get) SA = 0x040d0bb0 from 172.31.226.61.500
 3-14: 18:01:40:812:780 ISAKMP Header: (V1.0), len = 92
 3-14: 18:01:40:812:780   I-COOKIE afda38a347aaed8c
 3-14: 18:01:40:812:780   R-COOKIE 01a1ed1c3b47d706
 3-14: 18:01:40:812:780   exchange: Oakley Main Mode
 3-14: 18:01:40:812:780   flags: 1 ( encrypted )
 3-14: 18:01:40:812:780   next payload: ID
 3-14: 18:01:40:812:780   message ID: 00000000
 3-14: 18:01:40:812:780 processing payload ID
 3-14: 18:01:40:812:780 processing payload HASH
 3-14: 18:01:40:812:780 AUTH: Phase I authentication accepted
 3-14: 18:01:40:812:780 processing payload NOTIFY
 3-14: 18:01:40:812:780 Unknown Notify Message 24578
 3-14: 18:01:40:812:780 ClearFragList
 3-14: 18:01:40:812:780 constructing ISAKMP Header
 3-14: 18:01:40:812:780 constructing ID
 3-14: 18:01:40:812:780 MM ID Type 1
 3-14: 18:01:40:812:780 MM ID ac1fe21f
 3-14: 18:01:40:812:780 constructing HASH
 3-14: 18:01:40:812:780 MM established.  SA: 040D0BB0
 3-14: 18:01:40:828:780
 3-14: 18:01:40:828:780 Sending: SA = 0x040D0BB0 to 172.31.226.61:Type 2.500
 3-14: 18:01:40:828:780 ISAKMP Header: (V1.0), len = 68
 3-14: 18:01:40:828:780   I-COOKIE afda38a347aaed8c
 3-14: 18:01:40:828:780   R-COOKIE 01a1ed1c3b47d706
 3-14: 18:01:40:828:780   exchange: Oakley Main Mode
 3-14: 18:01:40:828:780   flags: 1 ( encrypted )
 3-14: 18:01:40:828:780   next payload: ID
 3-14: 18:01:40:828:780   message ID: 00000000
 3-14: 18:01:40:828:780 Ports S:f401 D:f401
 3-14: 18:01:40:828:780
 3-14: 18:01:40:828:780 Receive: (get) SA = 0x040d0bb0 from 172.31.226.61.500
 3-14: 18:01:40:828:780 ISAKMP Header: (V1.0), len = 148
 3-14: 18:01:40:828:780   I-COOKIE afda38a347aaed8c
 3-14: 18:01:40:828:780   R-COOKIE 01a1ed1c3b47d706
 3-14: 18:01:40:828:780   exchange: Oakley Quick Mode
 3-14: 18:01:40:828:780   flags: 1 ( encrypted )
 3-14: 18:01:40:828:780   next payload: HASH
 3-14: 18:01:40:828:780   message ID: be2ae44f
 3-14: 18:01:40:828:780 processing HASH (QM)
 3-14: 18:01:40:828:780 ClearFragList
 3-14: 18:01:40:828:780 processing payload NONCE
 3-14: 18:01:40:828:780 processing payload ID
 3-14: 18:01:40:828:780 processing payload ID
 3-14: 18:01:40:828:780 processing payload SA
 3-14: 18:01:40:828:780 Negotiated Proxy ID: Src 172.31.226.61.0 Dst 172.31.226.31.0
 3-14: 18:01:40:828:780 Checking Proposal 1: Proto= ESP(3), num trans=1 Next=0
 3-14: 18:01:40:828:780 Checking Transform # 1: ID=Triple DES CBC(3)
 3-14: 18:01:40:828:780  tunnel mode is Tunnel Mode(1)
 3-14: 18:01:40:828:780  SA life type in seconds
 3-14: 18:01:40:828:780  SA life duration 1800
 3-14: 18:01:40:828:780  HMAC algorithm is SHA(2)
 3-14: 18:01:40:828:780 Finding Responder Policy for SRC=172.31.226.61.0000 DST=172.31.226.31.0000,
SRCMask=255.255.255.255, DSTMask=255.255.255.255, Prot=0 InTunnelEndpt 1fe21fac OutTunnelEndpt
3de21fac
 3-14: 18:01:40:828:780 QM PolicyName: SHA-3DES dwFlags 1
 3-14: 18:01:40:828:780 QMOffer[0] LifetimeKBytes 0 LifetimeSec 0
 3-14: 18:01:40:828:780 QMOffer[0] dwFlags 0 dwPFSGroup 0
 3-14: 18:01:40:828:780  Algo[0] Operation: ESP Algo: Triple DES CBC HMAC: SHA
 3-14: 18:01:40:828:780 Phase 2 SA accepted: proposal=1 transform=1
 3-14: 18:01:40:828:780 GetSpi: src = 172.31.226.61.0000, dst = 172.31.226.31.0000, proto = 00,
context = 00000000, srcMask = 255.255.255.255, destMask = 255.255.255.255, TunnelFilter 1
```

```
 3-14: 18:01:40:843:780 Setting SPI  3540032480
 3-14: 18:01:40:843:780 constructing ISAKMP Header
 3-14: 18:01:40:843:780 constructing HASH (null)
 3-14: 18:01:40:843:780 constructing SA (IPSEC)
 3-14: 18:01:40:843:780 constructing NONCE (IPSEC)
 3-14: 18:01:40:859:780 constructing ID (proxy)
 3-14: 18:01:40:859:780 constructing ID (proxy)
 3-14: 18:01:40:859:780 constructing HASH (QM)
 3-14: 18:01:40:859:780
 3-14: 18:01:40:859:780 Sending: SA = 0x040D0BB0 to 172.31.226.61:Type 2.500
 3-14: 18:01:40:859:780 ISAKMP Header: (V1.0), len = 156
 3-14: 18:01:40:859:780   I-COOKIE afda38a347aaed8c
 3-14: 18:01:40:859:780   R-COOKIE 01a1ed1c3b47d706
 3-14: 18:01:40:859:780   exchange: Oakley Quick Mode
 3-14: 18:01:40:859:780   flags: 3 ( encrypted commit )
 3-14: 18:01:40:859:780   next payload: HASH
 3-14: 18:01:40:859:780   message ID: be2ae44f
 3-14: 18:01:40:859:780 Ports S:f401 D:f401
 3-14: 18:01:40:859:780
 3-14: 18:01:40:859:780 Receive: (get) SA = 0x040d0bb0 from 172.31.226.61.500
 3-14: 18:01:40:859:780 ISAKMP Header: (V1.0), len = 52
 3-14: 18:01:40:859:780   I-COOKIE afda38a347aaed8c
 3-14: 18:01:40:859:780   R-COOKIE 01a1ed1c3b47d706
 3-14: 18:01:40:859:780   exchange: Oakley Quick Mode
 3-14: 18:01:40:859:780   flags: 1 ( encrypted )
 3-14: 18:01:40:859:780   next payload: HASH
 3-14: 18:01:40:859:780   message ID: be2ae44f
 3-14: 18:01:40:859:780 processing HASH (QM)
 3-14: 18:01:40:859:780 ClearFragList
 3-14: 18:01:40:859:780 Adding QMs: src = 172.31.226.31.0000, dst = 172.31.226.61.0000, proto = 00,
context = 00000009, my tunnel = 172.31.226.31, peer tunnel = 172.31.226.61, SrcMask = 0.0.0.0,
DestMask = 0.0.0.0 Lifetime = 1800 LifetimeKBytes 100000 dwFlags 1 Direction 1 EncapType 1
 3-14: 18:01:40:859:780  Algo[0] Operation: ESP Algo: Triple DES CBC HMAC: SHA
 3-14: 18:01:40:859:780  Algo[0] MySpi: 3540032480 PeerSpi: 3894842112
 3-14: 18:01:40:859:780 Encap Ports Src 500 Dst 500
 3-14: 18:01:40:859:780 isadb_set_status sa:040D0BB0 centry:000EBB40 status 0
 3-14: 18:01:40:859:780 Constructing Commit Notify
 3-14: 18:01:40:859:780 constructing ISAKMP Header
 3-14: 18:01:40:859:780 constructing HASH (null)
 3-14: 18:01:40:859:780 constructing NOTIFY 16384
 3-14: 18:01:40:859:780 constructing HASH (QM)
 3-14: 18:01:40:859:780
 3-14: 18:01:40:859:780 Sending: SA = 0x040D0BB0 to 172.31.226.61:Type 4.500
 3-14: 18:01:40:859:780 ISAKMP Header: (V1.0), len = 76
 3-14: 18:01:40:859:780   I-COOKIE afda38a347aaed8c
 3-14: 18:01:40:859:780   R-COOKIE 01a1ed1c3b47d706
 3-14: 18:01:40:859:780   exchange: Oakley Quick Mode
 3-14: 18:01:40:859:780   flags: 3 ( encrypted commit )
 3-14: 18:01:40:859:780   next payload: HASH
 3-14: 18:01:40:859:780   message ID: be2ae44f
 3-14: 18:01:40:859:780 Ports S:f401 D:f401
 3-14: 18:02:32:156:780 CE Dead. sa:040D0BB0 ce:000EBB40 status:35f0
```

FortiGate debug output:

```
Fortigate # diag deb en

Fortigate # diag deb appl ike 2

Fortigate # diag test auth ldap win2k3 user1 pass1


Get sa_connect message...172.31.226.61->172.31.226.31:500, natt_mode=0
Using new connection...natt_mode=0
Set connection name = p1.
Tunnel 172.31.226.61 ---> 172.31.226.31:500,natt_en=0 is starting negotiation
Initiator: main mode is sending 1st message...
Sending VID payload....
Send IKE Packet(main_outI1):172.31.226.61:500(if4) -> 172.31.226.31:500, len=100
Initiator: sent 172.31.226.31 main mode message #1 (OK)
```

```
set retransmit: st=1, timeout=6.


Comes 172.31.226.31:500->172.31.226.61:500,ifindex=4, dmz, vf_id=0....
Exchange Mode = 2, I_COOKIE = 0xAFDA38A347AAED8C, Len = 148
Received Payloads= SA VID VID VID
Initiator: main mode get 1st response...
parse all vendor ids...
- Private vendor id (20): 1E2B516905991C7D7C96FCBFB587E46100000004
- found fragmentation avoidance
- found NAT-T v2
---
Negotiate Result
Proposal_id = 1:
   Protocol_id = ISAKMP:
      trans_id = KEY_IKE.
      encapsulation = IKE/none
         type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.
         type=OAKLEY_HASH_ALG, val=SHA.
         type=AUTH_METHOD, val=PRESHARED_KEY.
         type=OAKLEY_GROUP, val=1024.
Phase1 lifetimes=28800
Negotiate Success.(No echo).
Initiator: sent 172.31.226.31 main mode message #2 (OK)
Send IKE Packet(STF_REPLY):172.31.226.61:500(if4) -> 172.31.226.31:500, len=180
set retransmit: st=1, timeout=6.


Comes 172.31.226.31:500->172.31.226.61:500,ifindex=4, dmz, vf_id=0....
Exchange Mode = 2, I_COOKIE = 0xAFDA38A347AAED8C, Len = 184
Received Payloads= KE NONCE
Initiator:main mode get 2nd response...
Sending initial contact
Responder: sent 172.31.226.31 main mode message #3 (OK)
Send IKE Packet(STF_REPLY):172.31.226.61:500(if4) -> 172.31.226.31:500, len=92
set retransmit: st=1, timeout=6.


Comes 172.31.226.31:500->172.31.226.61:500,ifindex=4, dmz, vf_id=0....
Exchange Mode = 2, I_COOKIE = 0xAFDA38A347AAED8C, Len = 68
Received Payloads= ID HASH
Initiator: main mode get 3rd response...
set gw: 0x80bd810, timeout=28800.
Initiator: parsed 172.31.226.31 main mode message #3 (DONE)
Initiator:quick mode: pfs is not enabled
Try to negotiate with 1800 life seconds.
Initiate an SA with selectors:
 172.31.226.61->172.31.226.31
Send IKE Packet(quick_outI1):172.31.226.61:500(if4) -> 172.31.226.31:500, len=148
Initiator: sent 172.31.226.31 quick mode message #1 (OK)
set retransmit: st=2, timeout=6.


Comes 172.31.226.31:500->172.31.226.61:500,ifindex=4, dmz, vf_id=0....
Exchange Mode = 32, Message id = 0xBE2AE44F, Len = 156
Received Payloads= HASH SA NONCE ID ID
Initiator:quick mode get 1st response
Negotiate Result
Proposal_id = 1:
   Protocol_id = IPSEC_ESP:
      trans_id = ESP_3DES.
      encapsulation = ENCAPSULATION_MODE_TUNNEL
         type=AUTH_ALG, val=SHA1.
Using tunnel mode.
Negotiate Success.(No echo).
Initiator:Prepare to install sa.
Set sa life soft seconds=1750.
Set sa life hard seconds=1800.
dport = 500.Initializing sa OK.
Initiator: sent 172.31.226.31 quick mode message #2 (DONE)
expire: st=2, timeout=120.
Send IKE Packet(STF_REPLY):172.31.226.61:500(if4) -> 172.31.226.31:500, len=52
```

```
Comes 172.31.226.31:500->172.31.226.61:500,ifindex=4, dmz, vf_id=0....
Exchange Mode = 32, Message id = 0xBE2AE44F, Len = 76
Demux: Bad syntax, 1343, payload=8.


autheticate 'user1' against 'win2k3' succeeded!


Fortigate # diag vpn tun list
tunnel[5]:p2, gateway:172.31.226.31:500, hub=, option=0
   eroute[2]:{[172.31.226.61]}->{[172.31.226.31]}
   channel[2]:172.31.226.61,natt=0,state=2,keepalive=0,oif=4
     sa[4]:mtu=1434, cur_bytes=1050, timeout=1792
     itdb[1]:mtu=1434, cur_bytes=264, cur_packets=4, spi=e8269300, replay=0
          3DES=e174dac95674a36b611e55c5ead8e7e26fdc25caa29e772f
          iv=0000000000000000
          SHA1_HMAC=2c7513c6fa9248a8a5a057cbb0cfcb251a06a2dc
     otdb[1]:mtu=1434, cur_bytes=472, cur_packets=7, spi=d3009be0, replay=0
          3DES=e18dae7ec0fbe8936a91ce6a9b6e2205f24aa239bd8648b5
          iv=ffabb29decad735d
          SHA1_HMAC=d32a95d097aae94b98df86939a5a7d161a1d91fb


Fortigate # diag vpn gw list

Fortigate #            vike_count=1
gw:172.31.226.31:500/172.31.226.61(4), rekey time=28488, connected
   cookies: afda38a347aaed8c/01a1ed1c3b47d706
```

FortiGate CLI configuration file:

```
config system global
    set ipsec-host-selector enable
end
config system interface
    edit "internal"
        set ip 10.103.1.61 255.255.255.0
        set allowaccess ping https ssh telnet
    next
    edit "wan1"
        set ip 172.31.225.61 255.255.255.0
        set allowaccess ping https ssh telnet
    next
    edit "dmz"
        set ip 172.31.226.61 255.255.255.0
        set allowaccess ping https ssh telnet
    next
end
config system console
    set output more
end
exec enter root
config firewall address
    edit "win2k3"
        set subnet 172.31.226.31 255.255.255.255
    next
    edit "fgt-dmz-ip"
        set subnet 172.31.226.61 255.255.255.255
    next
    edit "internal-network"
        set subnet 10.103.1.0 255.255.255.0
    next
end
config user ldap
    edit "win2k3"
        set cnid "cn"
        set dn "OU=support,DC=win2k3-vm1,DC=com"
        set server "172.31.226.31"
    next
end
```

```
config user group
    edit "ldap-group"
            set member "win2k3"
        set profile "unfiltered"
        set types-in-group 4
    next
end
config vpn ipsec phase1
    edit "p1"
        set dhgrp 2
        set proposal 3des-sha1
        set remotegw 172.31.226.31
        set psksecret password
    next
end
config vpn ipsec phase2
    edit "p2"
        set dhgrp 2
        set phase1name "p1"
        set proposal 3des-sha1
    next
end
config firewall policy
    edit 3
        set srcintf "internal"
        set dstintf "wan1"
        set srcaddr "internal-network"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "DNS"
        set nat enable
    next
    edit 1
        set srcintf "internal"
        set dstintf "wan1"
        set srcaddr "internal-network"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ANY"
        set nat enable
        set groups "ldap-group"
    next
    edit 5
        set srcintf "internal"
        set dstintf "dmz"
        set srcaddr "fgt-dmz-ip"
        set dstaddr "win2k3"
        set action encrypt
        set schedule "always"
        set service "ANY"
        set inbound enable
        set outbound enable
        set vpntunnel "p2"
    next
end
config router static
    edit 1
        set gateway 172.31.225.254
    next
end
```

Windows Server IPSec overview configuration:

```
C:\Program Files\Support Tools>netsh ipsec static show all


Policy Name            : fgt-win2k3-tunnel
Description            : NONE
Store                  : Local Store <Q-VM1-WIN2K3>
```

```
Last Modified          : 15/March/2006 10:23:38
GUID                   : {F6806B8D-149C-4E3D-AF28-A193075A826A}
Assigned               : YES
Polling Interval       : 180 minutes
MainMode LifeTime      : 480 minutes / 0 Quick Mode sessions
Master PFS             : NO
Main Mode Security Method Order
  Encryption     Integrity      DH Group
  ----------     ---------      --------
    3DES          SHA1          Medium(2)

No. of Rules           : 3

Rule Details
------------


Rule ID                : 1,  GUID = {62A8D558-831D-47B7-A730-BCB4D0FB2125}
Rule Name              : NONE
Description            : NONE
Last Modified          : 14/March/2006 17:59:38
Activated              : YES
Tunnel Dest IP Address : 172.31.226.61
Connection Type        : ALL
Authentication Methods(1)

      Preshared Key : password

FilterList Details
------------------

FilterList Name        : win2k3-to-fgt
Description            : NONE
Store                  : Local Store <Q-VM1-WIN2K3>
Last Modified          : 10/March/2006 13:04:09
GUID                   : {8BCC6F59-B6BA-4895-BE82-6A64D0922C8E}
No. of Filters         : 1
Filter(s)
---------
Description            : win2k3-ip-to-fgt-ip
Mirrored               : NO
Source IP Address      : <My IP Address>
Source Mask            : 255.255.255.255
Source DNS Name        : <My IP Address>
Destination IP Address : 172.31.226.61
Destination Mask       : 255.255.255.255
Destination DNS Name   : <A Specific IP Address>
Protocol               : ANY
Source Port            : ANY
Destination Port       : ANY

FilterAction Details
----------------------

FilterAction Name      : SHA-3DES
Description            : NONE
Store                  : Local Store <Q-VM1-WIN2K3>
Action                 : NEGOTIATE SECURITY
AllowUnsecure(Fallback): NO
Inbound Passthrough    : NO
QMPFS                  : NO
Last Modified          : 14/March/2006 17:59:22
GUID                   : {62AD8B57-D9FD-4BCE-95D3-86257A325B85}
Security Methods
  AH       ESP             Seconds          kBytes
  --       ---             -------          ------
[NONE] [SHA1 , 3DES]     0               0


Rule ID                : 2,  GUID = {8AD76C9A-AEC1-4A97-BBFD-A03523C616FE}
Rule Name              : NONE
Description            : NONE
Last Modified          : 15/March/2006 10:23:38
```

```
Activated              : YES
Tunnel Dest IP Address : 172.31.226.31
Connection Type        : ALL
Authentication Methods(1)

       Preshared Key : password

FilterList Details
------------------

FilterList Name        : fgt-to-win2k3
Description            : NONE
Store                  : Local Store <Q-VM1-WIN2K3>
Last Modified          : 10/March/2006 13:04:32
GUID                   : {B9B78CFB-399A-4C2C-8687-6FB1AD8539F1}
No. of Filters         : 1
Filter(s)
---------
Description            : fgt-ip-to-win2k3-ip
Mirrored               : NO
Source IP Address      : 172.31.226.61
Source Mask            : 255.255.255.255
Source DNS Name        : <A Specific IP Address>
Destination IP Address : <My IP Address>
Destination Mask       : 255.255.255.255
Destination DNS Name   : <My IP Address>
Protocol               : ANY
Source Port            : ANY
Destination Port       : ANY

FilterAction Details
--------------------

FilterAction Name      : SHA-3DES
Description            : NONE
Store                  : Local Store <Q-VM1-WIN2K3>
Action                 : NEGOTIATE SECURITY
AllowUnsecure(Fallback): NO
Inbound Passthrough    : NO
QMPFS                  : NO
Last Modified          : 14/March/2006 17:59:22
GUID                   : {62AD8B57-D9FD-4BCE-95D3-86257A325B85}
Security Methods
  AH       ESP             Seconds          kBytes
  --       ---             -------          ------
[NONE] [SHA1 , 3DES]     0               0


Rule ID                : 3,  GUID = {CBC51CFF-9DD3-4785-BA7D-13E073B28E16}
Rule Name              : NONE
Description            : NONE
Last Modified          : 09/March/2006 17:25:42
Activated              : NO
Connection Type        : ALL
Authentication Methods(1)

       KERBEROS

No FilterList exists in Default Response Rule

FilterAction Details
--------------------

FilterAction Name      : NONE
Description            : NONE
Store                  : Local Store <Q-VM1-WIN2K3>
AllowUnsecure(Fallback): NO
Inbound Passthrough    : NO
QMPFS                  : NO
Last Modified          : 09/March/2006 17:25:42
GUID                   : {F4F5E737-5C78-46E6-9304-33ACCA14C35C}
Security Methods
  AH       ESP             Seconds          kBytes
```

```
  --       ---             -------          ------
[NONE] [SHA1 , 3DES]     0               0
[NONE] [MD5  , 3DES]     0               0
[NONE] [SHA1 , DES ]     0               0
[NONE] [MD5  , DES ]     0               0
[SHA1] [NONE , NONE]     0               0
[MD5 ] [NONE , NONE]     0               0


No. of policies        : 1


Stand Alone FilterAction(s)
---------------------------

FilterAction Name      : Request Security (Optional)
Description            : Accepts unsecured communication, but requests clien...
Store                  : Local Store <Q-VM1-WIN2K3>
Action                 : NEGOTIATE SECURITY
AllowUnsecure(Fallback): YES
Inbound Passthrough    : YES
QMPFS                  : NO
Last Modified          : 01/March/2006 19:22:48
GUID                   : {72385233-70FA-11D1-864C-14A300000000}
Security Methods
  AH       ESP             Seconds          kBytes
  --       ---             -------          ------
[NONE] [SHA1 , 3DES]    900           100000
[NONE] [SHA1 , DES ]    900           100000
[SHA1] [NONE , NONE]    300           100000
[MD5 ] [NONE , NONE]    300           100000

FilterAction Name      : Permit
Description            : Permit unsecured IP packets to pass through.
Store                  : Local Store <Q-VM1-WIN2K3>
Action                 : PERMIT
AllowUnsecure(Fallback): NO
Inbound Passthrough    : NO
Last Modified          : 01/March/2006 19:22:48
GUID                   : {7238523B-70FA-11D1-864C-14A300000000}

FilterAction Name      : Require Security
Description            : Accepts unsecured communication, but always require...
Store                  : Local Store <Q-VM1-WIN2K3>
Action                 : NEGOTIATE SECURITY
AllowUnsecure(Fallback): NO
Inbound Passthrough    : NO
QMPFS                  : NO
Last Modified          : 09/March/2006 17:19:45
GUID                   : {7238523F-70FA-11D1-864C-14A300000000}
Security Methods
  AH       ESP             Seconds          kBytes
  --       ---             -------          ------
[NONE] [SHA1 , 3DES]     0               0

No. of Standalone FilterActions   3


Stand Alone FilterList(s)
-------------------------

FilterList Name        : All ICMP Traffic
Description            : Matches all ICMP packets between this computer and ...
Store                  : Local Store <Q-VM1-WIN2K3>
Last Modified          : 09/March/2006 10:11:36
GUID                   : {72385235-70FA-11D1-864C-14A300000000}
No. of Filters         : 0

FilterList Name        : All IP Traffic
Description            : Matches all IP packets from this computer to any ot...
Store                  : Local Store <Q-VM1-WIN2K3>
Last Modified          : 09/March/2006 11:40:43
GUID                   : {7238523A-70FA-11D1-864C-14A300000000}
```

No. of Filters : 0

No. of Standalone FilterLists 2