ISA 2006 Firewall as a VPN Remote Access Server - A Few Tricks

Adrian F. Dimcev www.carbonwind.net
contact@carbonwind.net

29.12.2008
ISA 2006 Firewall as a VPN Remote Access Server - A Few Tricks

---

- 1. How do I restrict from which IP addresses the VPN clients can connect to the ISA VPN Server ?

- 2. How do I specify that ISA will accept PPTP remote access connections from a certain IP address range(s) and L2TP/IPsec remote access connections from another IP address range(s) ?

- 3. How do I restrict on which external IP address ISA listens for incoming VPN remote access connections (for PPTP and L2TP/IPsec) ?

- 4. How do I specify which users can use PPTP and which users can use L2TP/IPsec and adjust the firewall access rules to control access to internal resources in respect with the VPN protocol used by users ?

- 5. How do I specify that users from location X can use only PPTP and that users from location Y can use only L2TP/Psec and adjust the firewall access rules to control access to internal resources in respect with the VPN protocol used by users and the location of these users ?

- 6. How do I specify that a group of users can only connect from location X and another group of users can connect from any location ?

- 7. How do I disable DES and Diffie-Hellman 768-bit MODP group 1 for L2TP/IPsec on the ISA VPN server ?

1. How do I restrict from which IP addresses the VPN clients can connect to the ISA VPN Server ?

As you've noticed, from ISA's GUI we can only specify from which Network ISA will accept incoming VPN remote access connections, we cannot specify a single or a set of IP addresses from which VPN connections can be initiated, see **Figure1**.

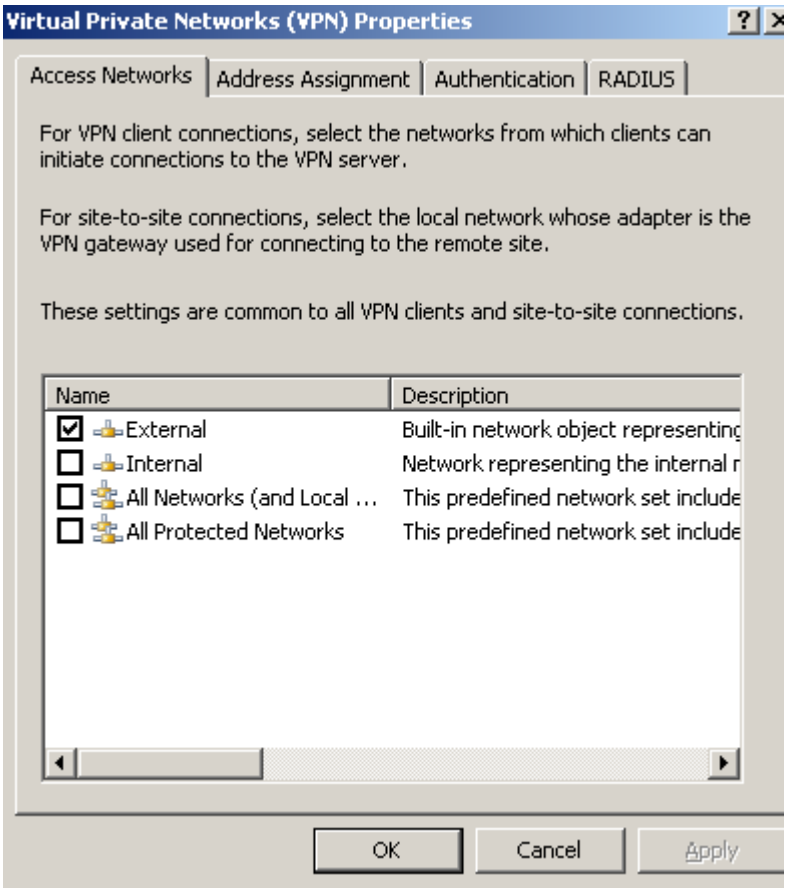


Figure1: VPN - Access Networks: External

So we need a trick, trick found on Microsoft's site, Excluding Specific Addresses from VPN Source Networks in ISA Server 2004.

So what does this trick do ?

Following the article:

Define the Empty Network, see **Figure2**.

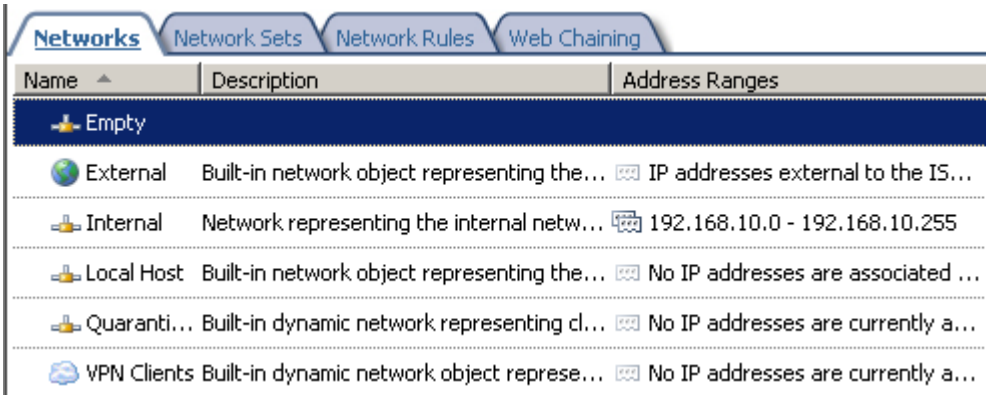


Figure2: An ISA Empty Network

I've created a **Subnet** *Network Object* on ISA, containing the subnet of external IP addresses from which I want to allow VPN clients to create VPN connections for this test (you can use **Computers**, **Computers Sets** or **Address Ranges** *Network Objects*, use what you need), see **Figure3**.

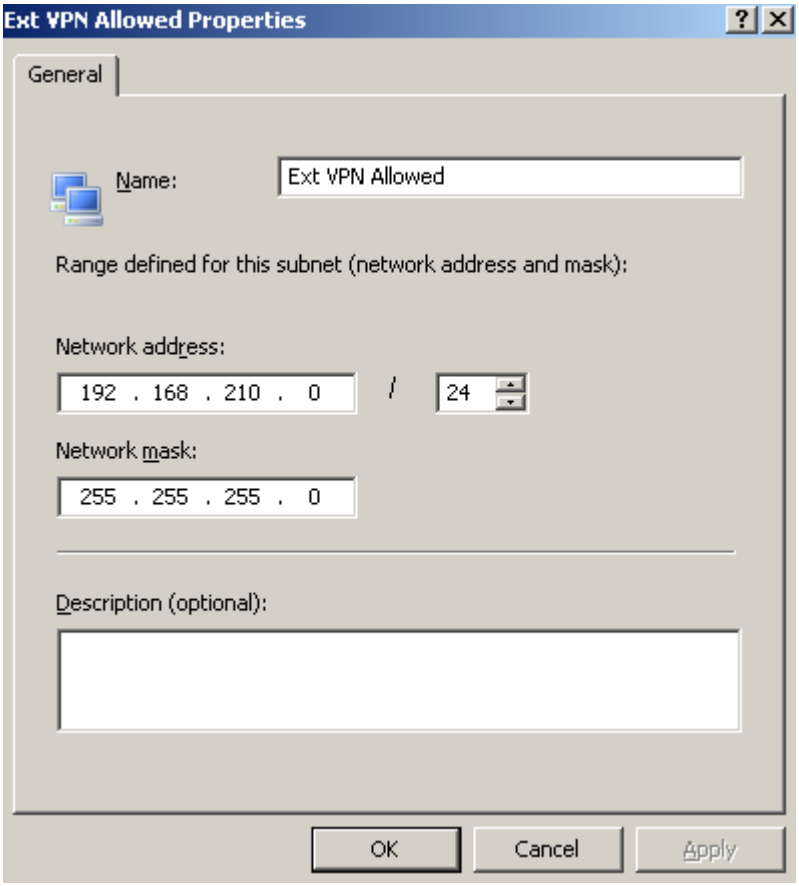


Figure3: An ISA Subnet Network Object

Note that this subnet will typically contain public IP addresses. If your VPN clients are behind NAT devices you do *not* add the private IP addresses of the networks from which they connect, instead you add the public IP addresses of the NAT devices(the source IP address of the VPN packets after NAT occurs).

Configure the Access Networks for the VPN Clients, in this case, to listen on the Empty Network, see **Figure4**.

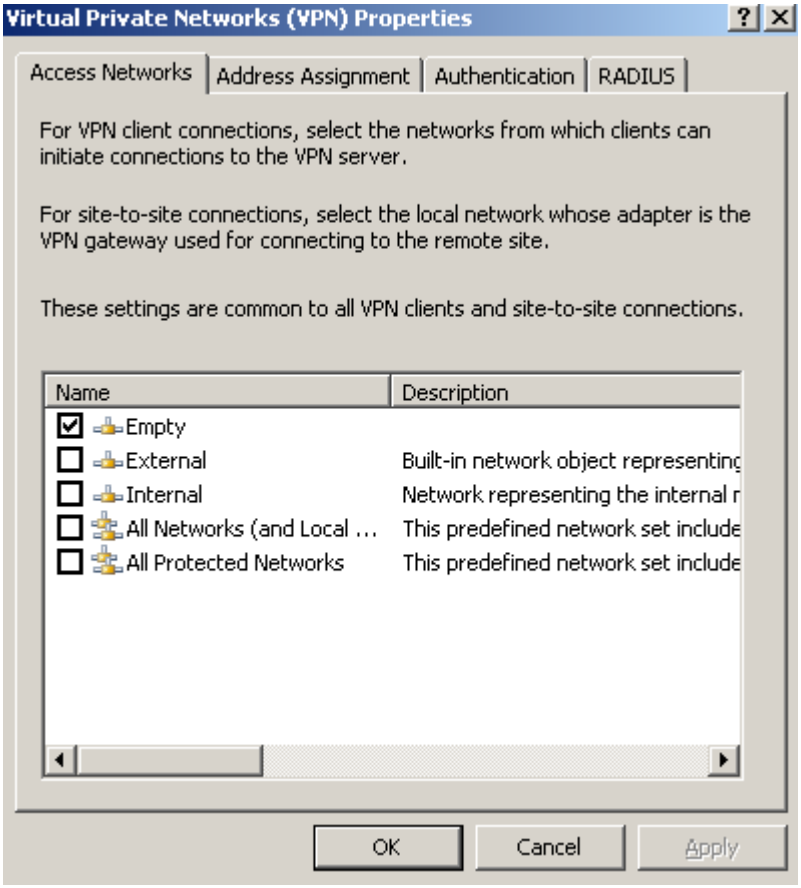


Figure4: VPN - Access Networks: Empty

This will modify **System Policy No. 13**, **Allow VPN client traffic to ISA Server**(ISA 2006 SE). As we can see from **Figure5**, this is an access rule. When we enable the VPN Server on ISA, this access rule will be enabled, allowing VPN traffic from the VPN clients to ISA. As we can see, requests will come from the Empty Network. So basically we've "disabled" this rule, because the Empty Network is empty, so there are no clients from which requests will come.

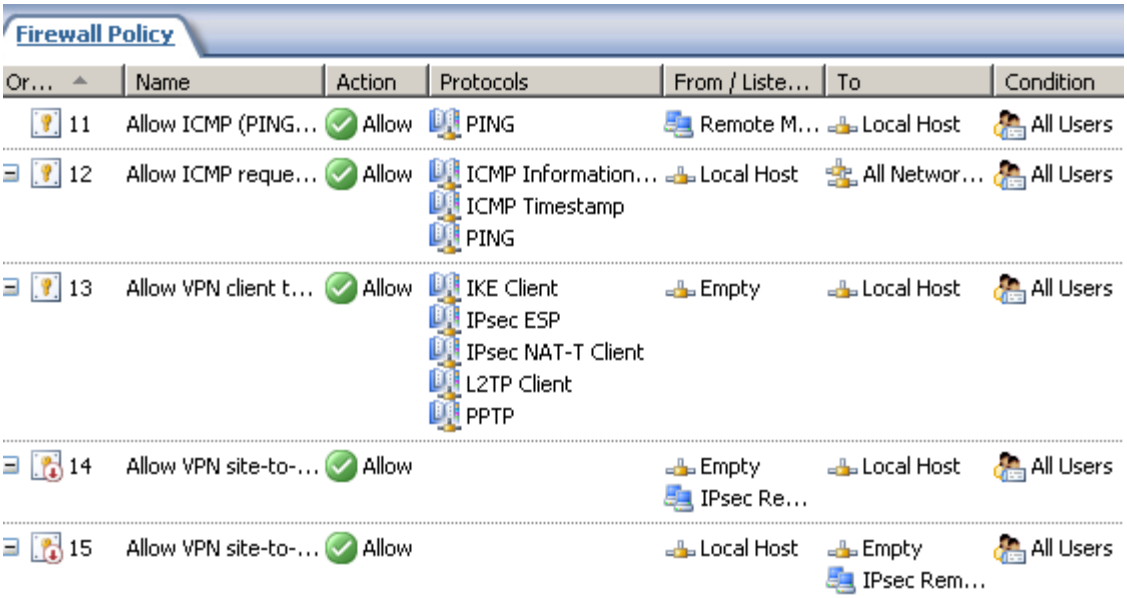


Figure5: ISA - System Policy

Note that ISA as a VPN gateway for the L2TP/IPsec and PPTP site-to-site connections, will also allow the traffic for the incoming(terminated on it) and the outgoing(terminated on it) s2s connections also from/to

the Empty Network(see **System Rules 13** and **15**, **Figure5**). Keep that in mind, otherwise you'll block ISA from intiating and answering to L2TP/IPsec and PPTP s2s connections.

If you use customs access rules based on this trick, you will need to create the needed custom rules for the L2TP/IPsec and PPTP s2s connections.

Next we will define our own custom access rule for VPN requests from the VPN clients(the bellow rule allows both PPTP and L2TP/IPsec) from the needed sources, see **Figure6**.

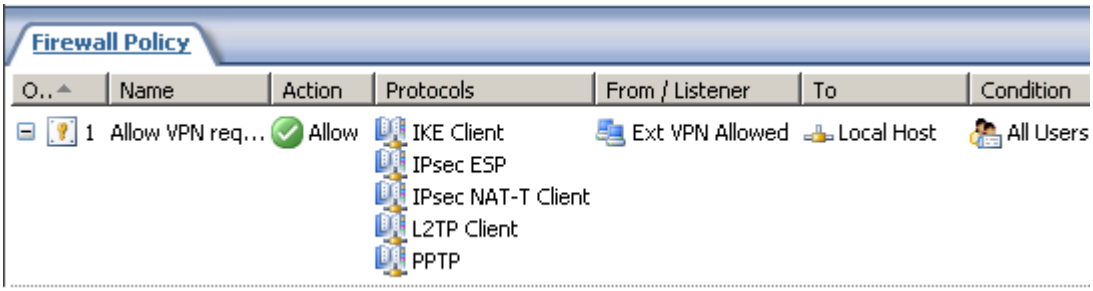


Figure6: ISA - Custom Access Rule

So the long answer:

- The above approach means that the incoming remote access VPN connections will be restricted by firewall rules based on source IP addresses. For L2TP/IPsec connections, the default L2TP/IPsec Main Mode filters are not modified, so the VPN server still accepts IKE messages from any source IP addresses, see **Figure7**, however the firewall will allow IKE "traffic" based on the newly created access rules.

```
C:\>netsh ipsec dynamic show mmfilter all

Main Mode Filters: Generic

-------------------------------------------------------------------

Filter name             : L2TP Server Inbound Filter
Connection Type         : ALL
Source Address          : <Any IP Address>  (0.0.0.0          )
Destination Address     : <My IP Address>   (255.255.255.255)
Authentication Methods  :
        Preshared key
Security Methods        : 5
        3DES/SHA1/DH3/28800/QMlimit=0
        3DES/SHA1/DH2/28800/QMlimit=0
        3DES/MD5/DH2/28800/QMlimit=0
        DES/SHA1/DH1/28800/QMlimit=0
        DES/MD5/DH1/28800/QMlimit=0

-------------------------------------------------------------------

Filter name             : L2TP Server Outbound Filter
Connection Type         : ALL
Source Address          : <My IP Address>   (255.255.255.255)
Destination Address     : <Any IP Address>  (0.0.0.0          )
Authentication Methods  :
        Preshared key
Security Methods        : 5
        3DES/SHA1/DH3/28800/QMlimit=0
        3DES/SHA1/DH2/28800/QMlimit=0
        3DES/MD5/DH2/28800/QMlimit=0
        DES/SHA1/DH1/28800/QMlimit=0
        DES/MD5/DH1/28800/QMlimit=0

2 Generic Filter(s)
```

Figure7: On ISA - netsh ipsec dynamic show mmfilter all

2. How do I specify that ISA will accept PPTP remote access connections from a certain IP address range(s) and L2TP/IPsec remote access connections from another IP address range(s) ?

After we have followed the above steps, we can specify that ISA will accept PPTP connections from a specific IP address range(s) and L2TP/IPsec connections from other IP address range(s) if we need that, simply by using two access rules.

First I've defined the subnet from which I want to allow the L2TP/IPsec VPN clients to connect, see **Figure8** and the subnet from which I want to allow the PPTP VPN clients to connect, see **Figure9**.

As said before, these subnets will typically contain public IP addresses. If your VPN clients are behind NAT devices you do *not* add the private IP addresses of the networks from which they connect, instead you add the public IP addresses of the NAT devices(the source IP address of the VPN packets after NAT occurs).

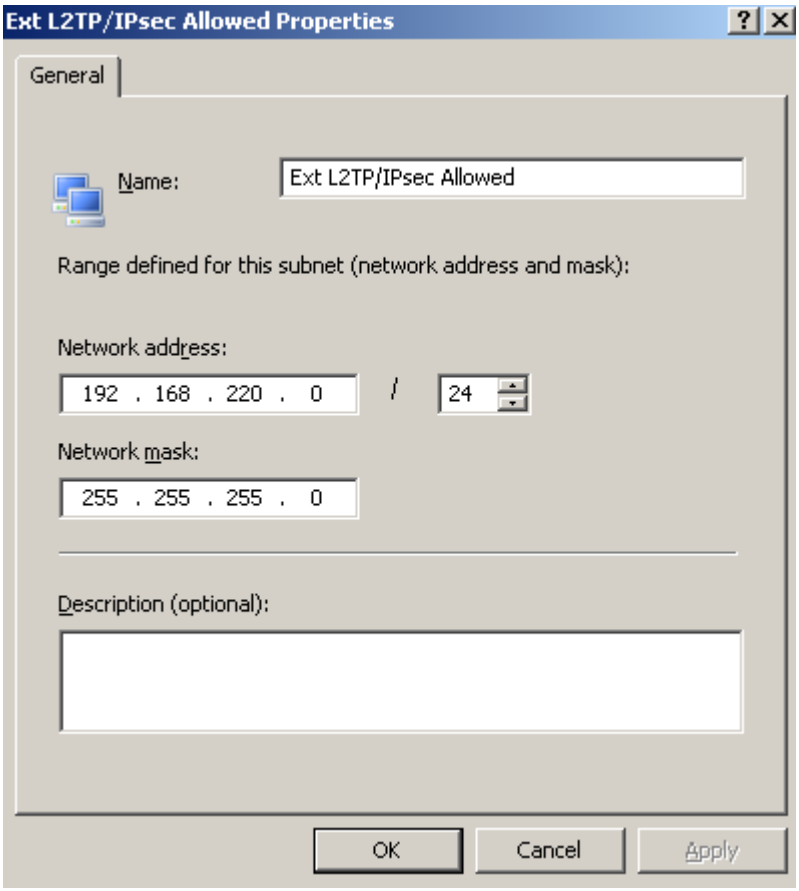


Figure8: ISA - Ext L2TP/IPsec Allowed Subnet Nework Object

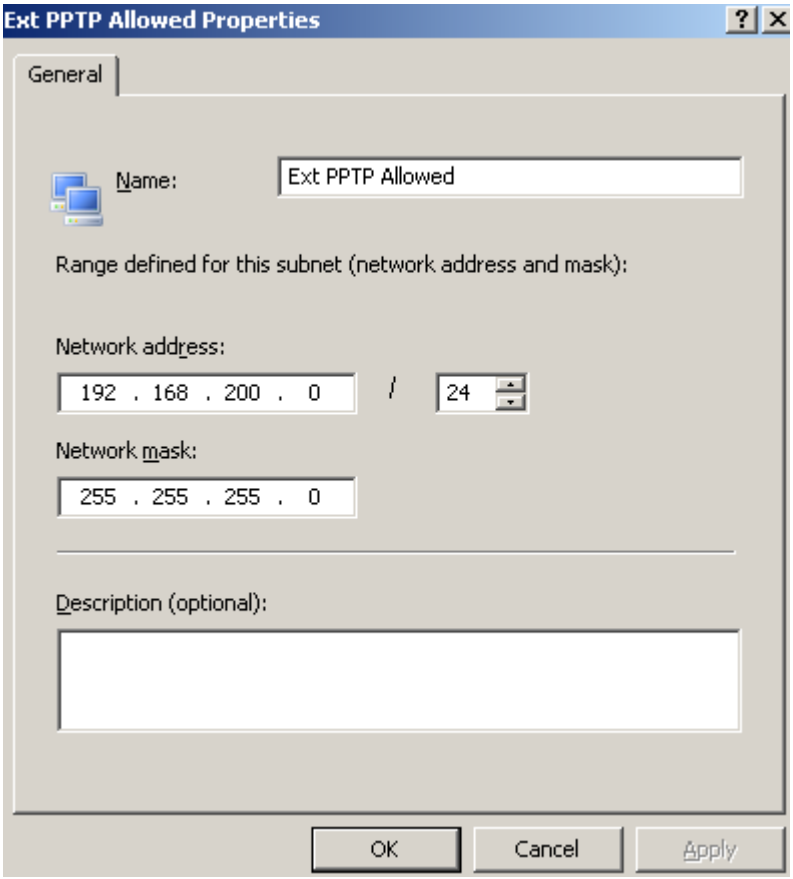


Figure9: ISA - Ext PPTP Allowed Subnet Nework Object

And after that, I've created the two custom access rules. As you can see from **Figure10**, basically I've splitted the access rule from **Figure6** in two rules, and modified the **From** tabs accordingly.

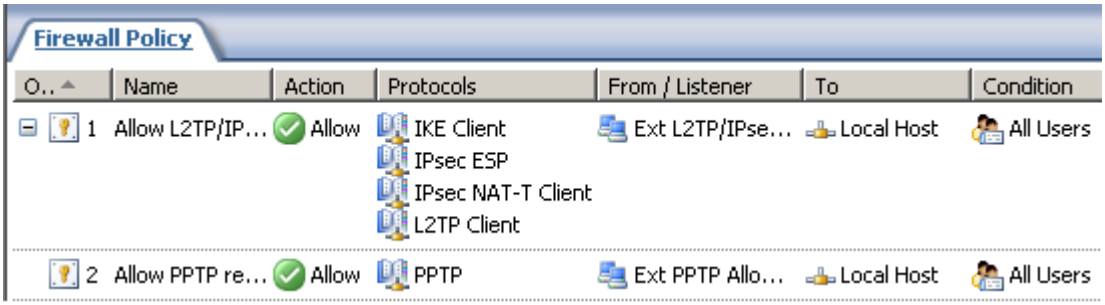


Figure10: ISA - Custom Access Rules

3. How do I restrict on which external IP address ISA listens for incoming VPN remote access connections (for PPTP and L2TP/IPsec) ?

You have an ISA Server 2006 SE. You have multiple public IP addresses on ISA's default interface, IP addresses used to publish various services.
By default when you enable the VPN Server on ISA and specify the External Network as the network from which ISA will accept VPN connections, ISA will accept VPN connections destined to any of the IP addresses configured on its external interface.
You may want to enable ISA to listen on a specific IP address for incoming remote access VPN connections.

Well, I do not have an "official" answer for this, just my answer, so use it on your own risk.

For example, I have the following IP addresses on ISA's external interface, see **Figure11**.

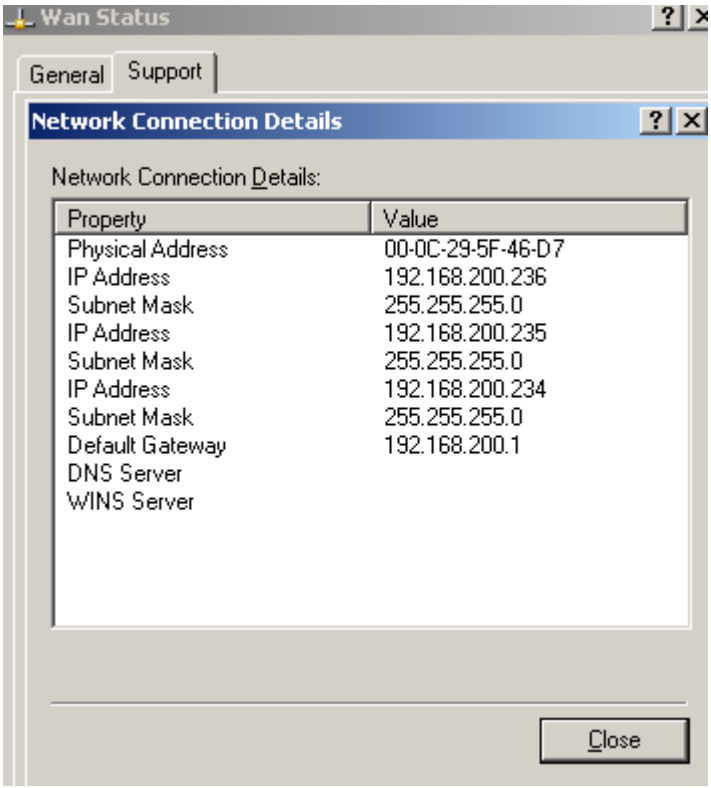


Figure11: ISA's Default External NIC

I want to use the 192.168.200.234 IP address for L2TP/IPsec remote access connections and the 192.168.200.235 IP address for PPTP remote access connections.

Looking at the above two custom created rules(**Figure10**) for L2TP/IPsec and PPTP, we can see that the destination is the Local Host Network.
Searching through Network Concepts in ISA Server 2006, we will learn that this is:

"*A predefined network that represents the ISA Server 2006 firewall. It includes all IP addresses on all network adapters. You do not explicitly define IP addresses on this network. Addresses are added automatically as they are defined on network adapters, including any wide area network (WAN) adapters that are created for VPN connections.*"

Let's initiate an L2TP/IPsec connection, using the default VPN setup of ISA (not the one with the above tricks), and analyze ISA's logs. I want to do that in order to figure it out what access rules we need to specify on which external IP address ISA listens for incoming VPN connections. I want to see what ISA sees, that's why I'm not using Wireshark.

First, IKE negotiations are started, note the source(External Network), the destination(Local Host 192.168.200.235) and the access rule allowing access, see **Figure12**.

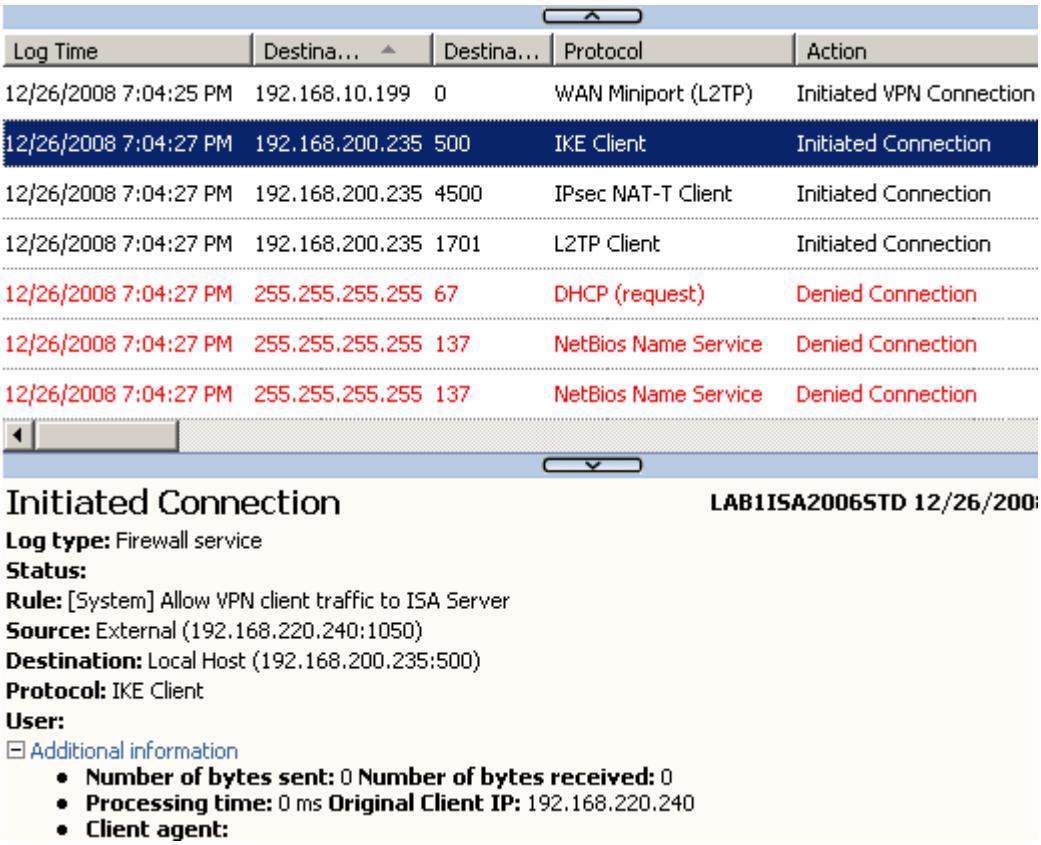


Figure12: ISA Logs - IKE Client

Next, after IKE negotiations were completed successfully, IPsec NAT-T Client traffic appears, note the source(External Network), the destination (Local Host 192.168.200.235) and the access rule allowing access, (the VPN client is behind a NAT device, thus NAT-T is used-UDP encapsulation of ESP packets-, actually IKE MM messages number 5 and the IKE QM messages from the client will also be destined to UDP port 4500 as a NAT device was detected between the two peers), see **Figure13**.

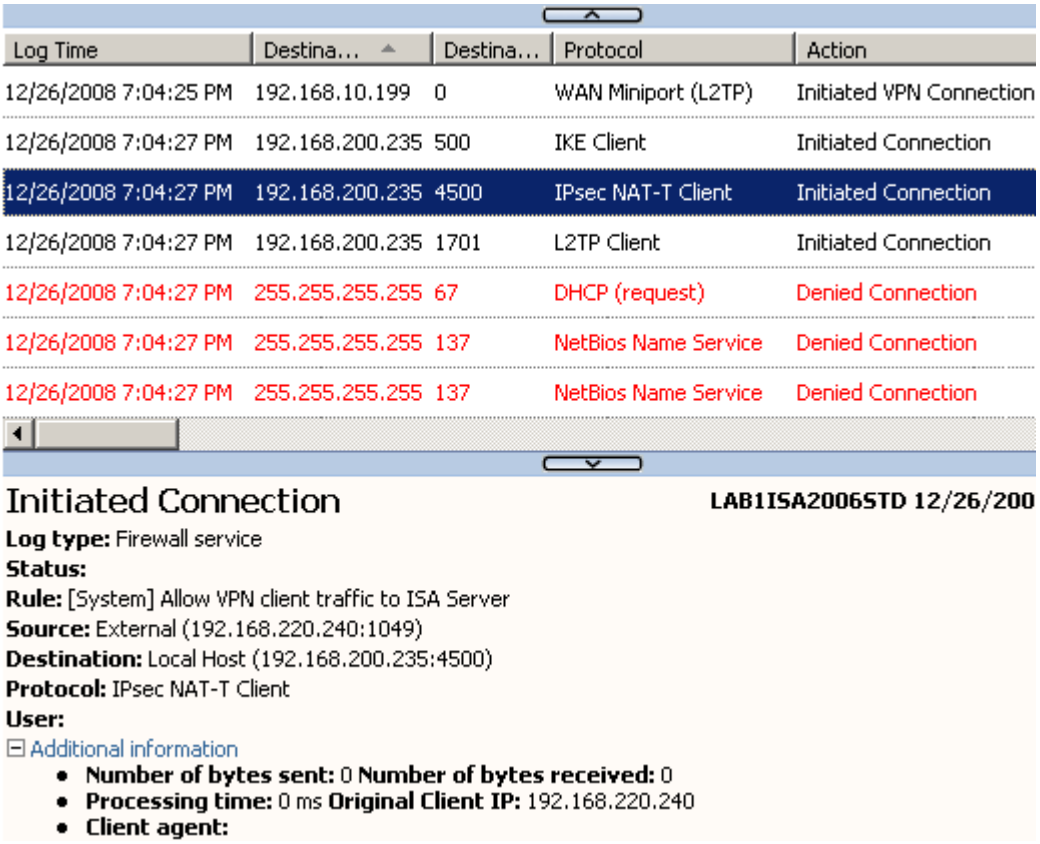


Figure13: ISA Logs - IPsec NAT-T Client

Then, the L2TP tunnel(UDP based implementation as L2TP is ran over IP) will be established, note the source(External Network), the destination(Local Host 192.168.200.235) and the access rule allowing access, see **Figure14**.

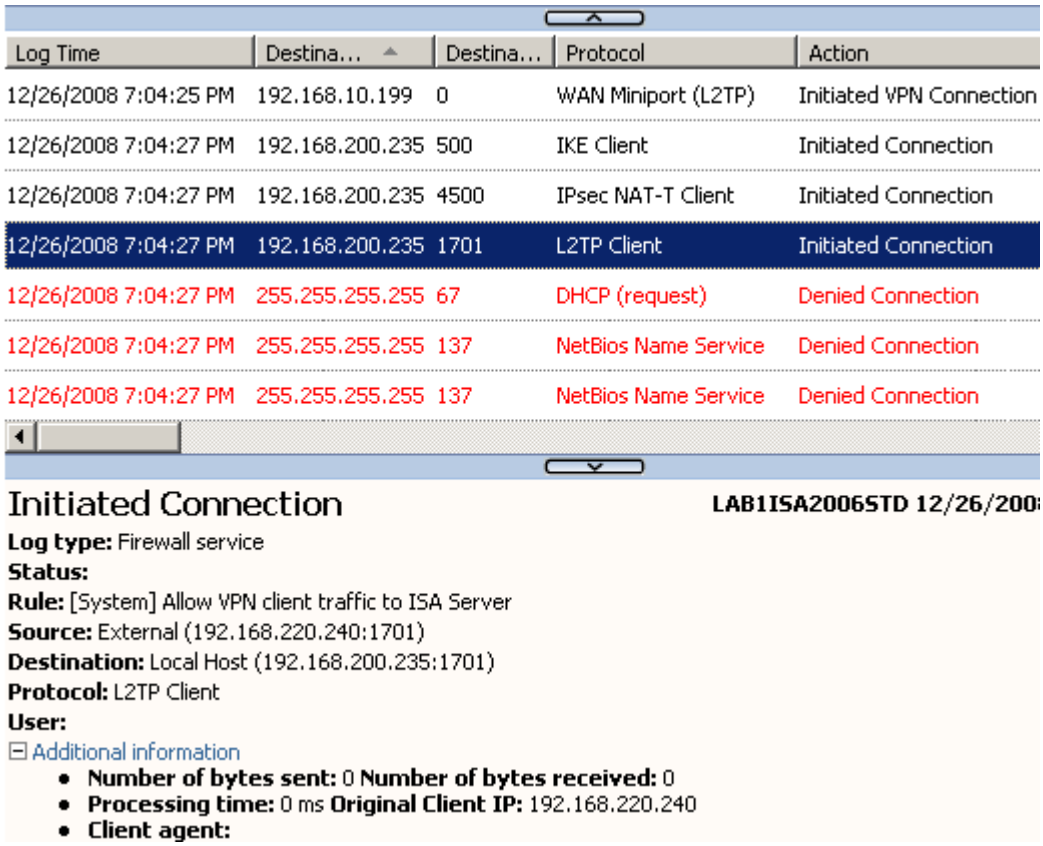
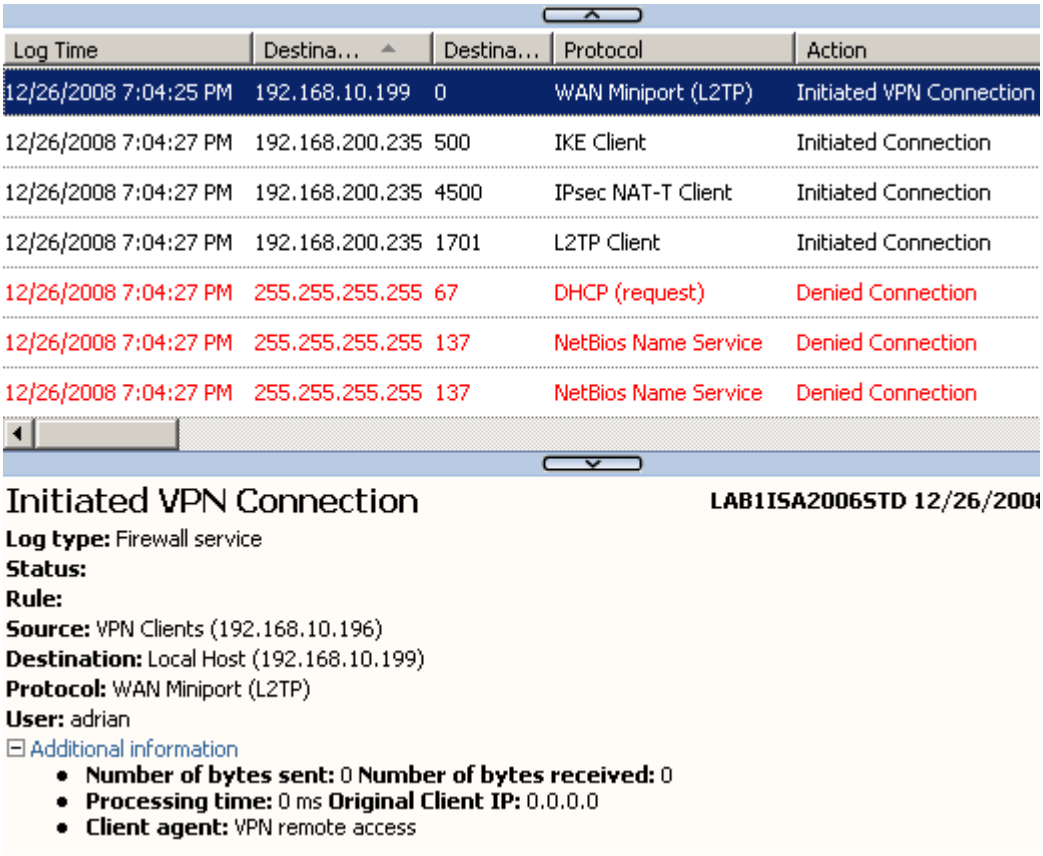


Figure14: ISA Logs - L2TP Client

The L2TP tunnel is used to carry PPP data, note the source(VPN Clients Network, the IP address from client's PPP adapter), destination(Local Host, the IP address from the RAS Server (Dial In) Interface) and the access rule allowing access(none), see **Figure14**.



Log Time	Destina...	Destina...	Protocol	Action
12/26/2008 7:04:25 PM	192.168.10.199	0	WAN Miniport (L2TP)	Initiated VPN Connection
12/26/2008 7:04:27 PM	192.168.200.235	500	IKE Client	Initiated Connection
12/26/2008 7:04:27 PM	192.168.200.235	4500	IPsec NAT-T Client	Initiated Connection
12/26/2008 7:04:27 PM	192.168.200.235	1701	L2TP Client	Initiated Connection
12/26/2008 7:04:27 PM	255.255.255.255	67	DHCP (request)	Denied Connection
12/26/2008 7:04:27 PM	255.255.255.255	137	NetBios Name Service	Denied Connection
12/26/2008 7:04:27 PM	255.255.255.255	137	NetBios Name Service	Denied Connection

Figure15: ISA Logs - WAN Miniport (L2TP)

So it appears that we can use the custom access rules from **Figure6**, this time specifying as destination instead of the Local Network, with a **Computer Network** *Object*, the needed public IP address from ISA's external interface. ISA will know that this IP address belongs to the Local Host Network.

So I've created two new **Computer Network** *Objects* on ISA with the needed IP addresses, see **Figure16** (for L2TP/IPsec) and **Figure17** (For PPTP).

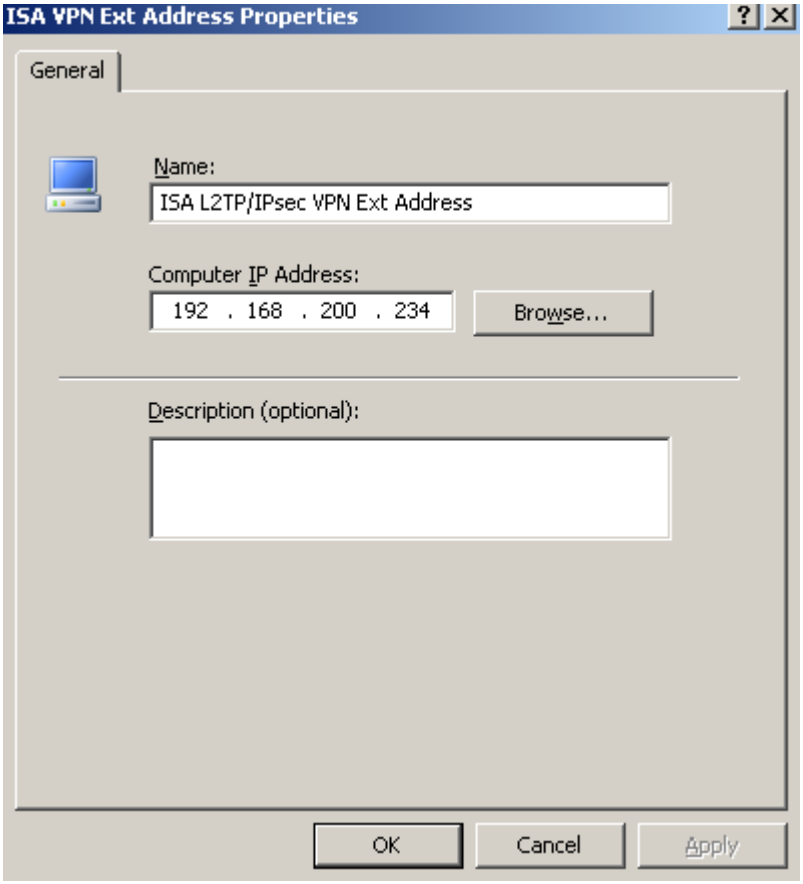


Figure16: ISA - L2TP/IPsec VPN Ext Address

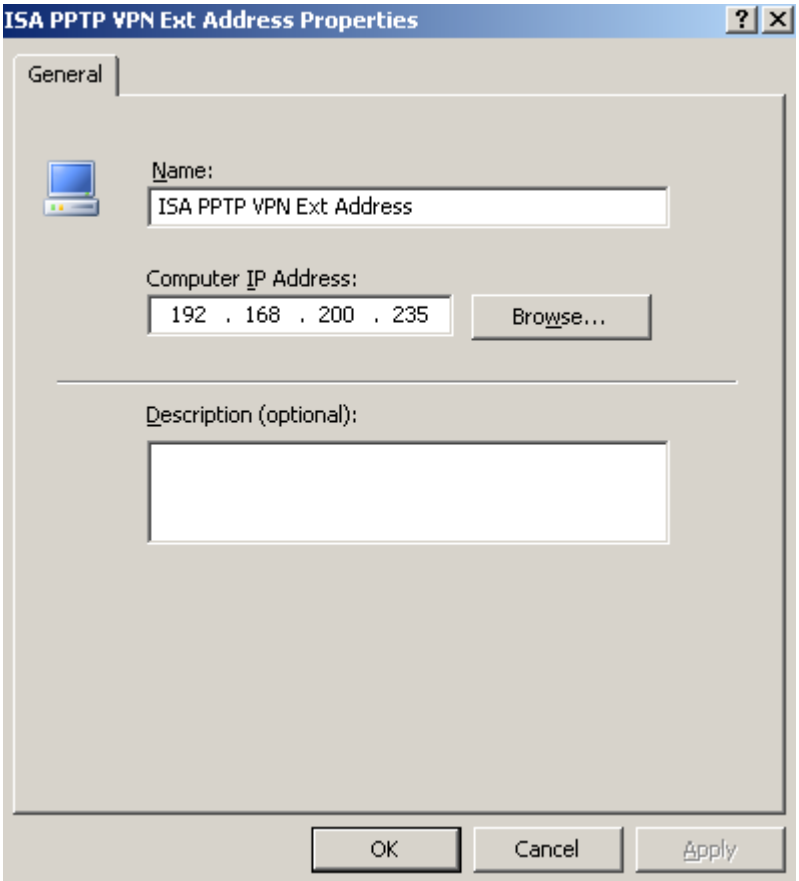


Figure17: ISA - PPTP VPN Ext Address

And I will modify the custom access rules(from **Figure6**) to include as destination the required IP address

for L2TP/IPsec and respectively the one for PPTP, see **Figure18**. Note that naked L2TP connections are not allowed, these packets will be simply dropped by Windows' default IPsec policy for L2TP, since they are not protected by IPsec as they should be(as specified by RFC 3193), you can test that trying to establish an L2TP tunnel from a Windows XP VPN client with the ProhibitIpSec registry value set to 1.

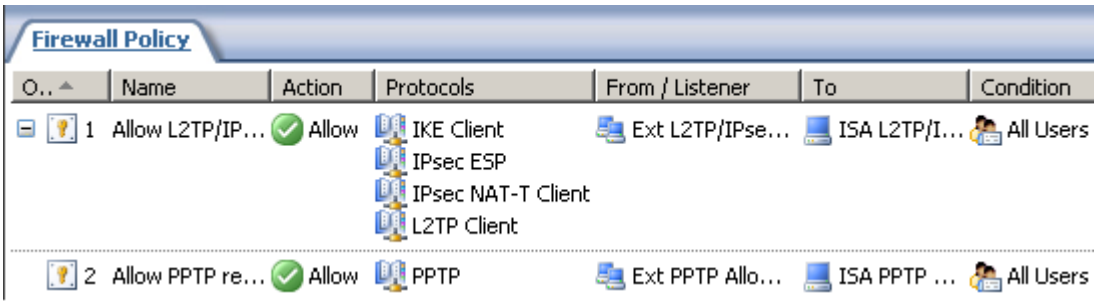


Figure18: ISA - Custom Access Rules

A quick test for PPTP this time to the allowed destination IP address, and the connection is successful, see **Figure19**.

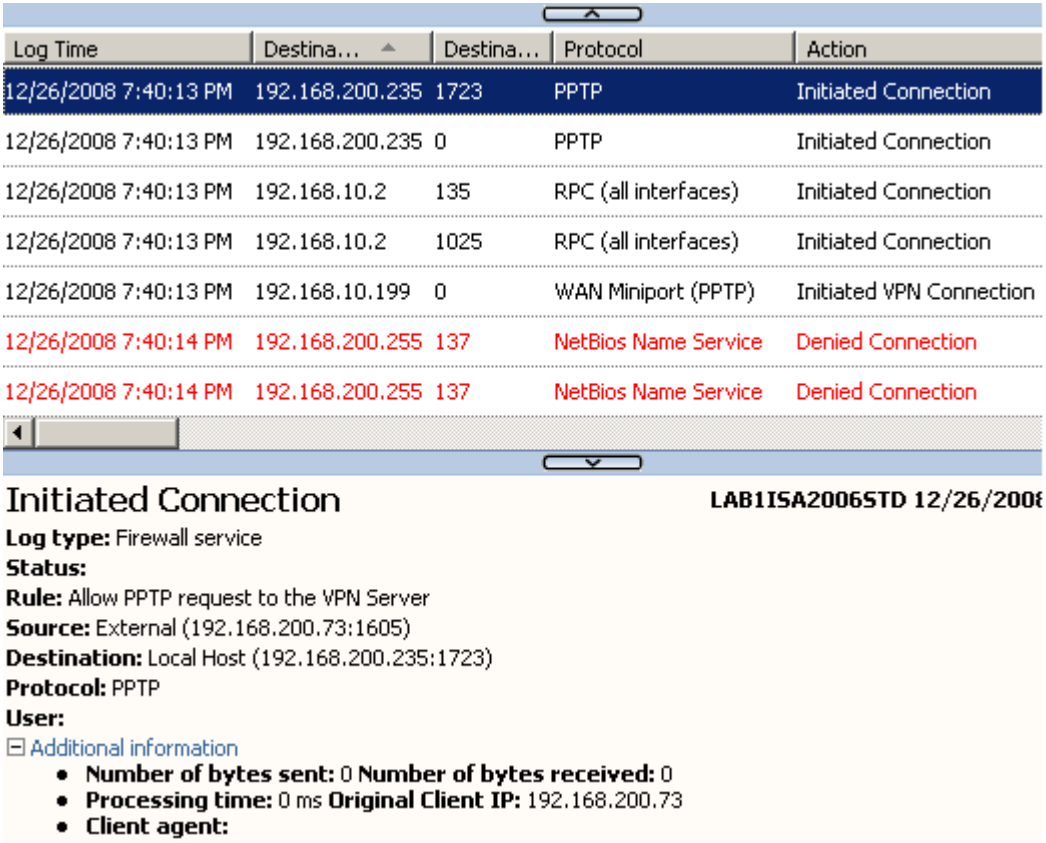


Figure19: ISA - An Allowed PPTP Connection from a PPTP Client

If I attempt to connect with L2TP/IPsec to another IP address(not to the allowed 192.168.200.234 IP address) belonging to ISA's external interface, the firewall will deny this attempt, see **Figure20**.

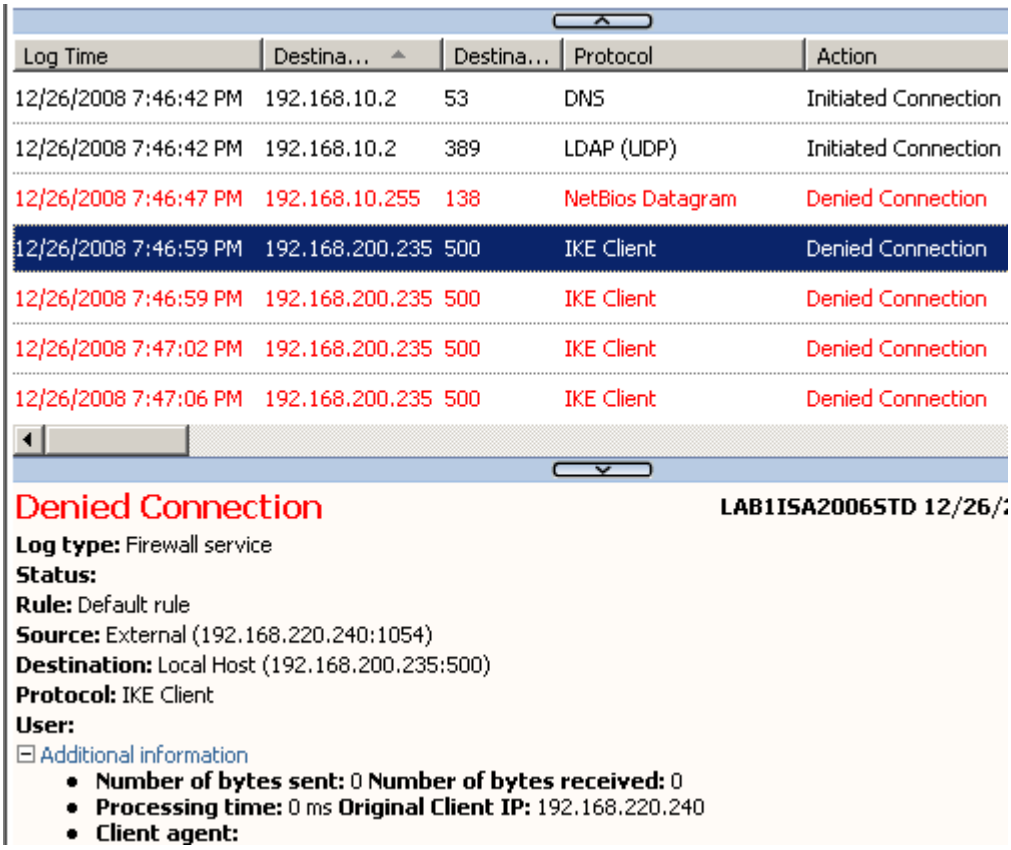


Figure20: ISA - A Denied L2TP/IPsec Connection from an L2TP/IPsec Client

If I attempt to connect with L2TP/IPsec to the allowed 192.168.200.234 IP address, the firewall will allow this attempt, see **Figure21**, and the connection is successful.

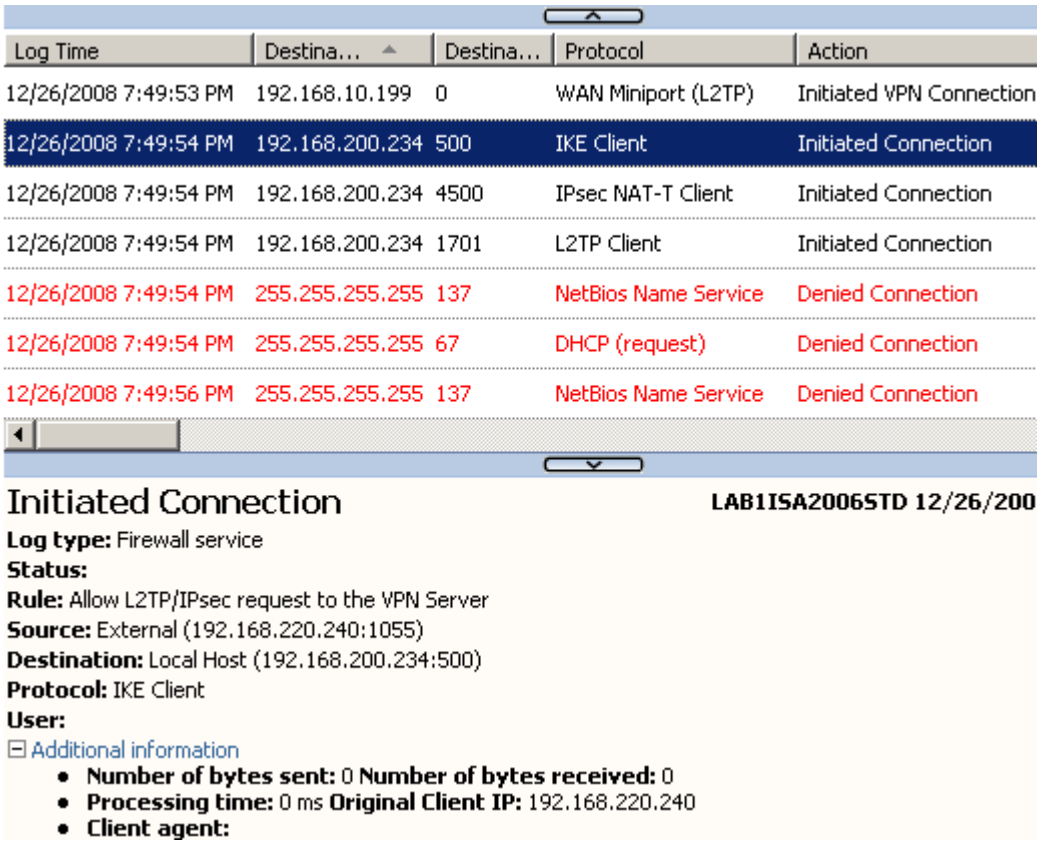


Figure21: ISA - An Allowed L2TP/IPsec Connection from an L2TP/IPsec Client

Note that this approach(with firewall rules) might work for incoming s2s PPTP and L2TP/IPsec connections too, connections for which the local ISA acts as the answering gateway. For s2s PPTP and L2TP/IPsec connections that are initiated by the local ISA(that is, when local ISA acts as the calling gateway), the first IP address from the external NIC will likely be used as the source of the VPN tunnels. We've merely firewalled the "services", we've not specified on which particular IP address the PPTP or L2TP services listen.

4. How do I specify which users can use PPTP and which users can use L2TP/IPsec and adjust the firewall access rules to control access to internal resources in respect with the VPN protocol used by users ?

You may want to enable a certain group of users(for various reasons) to use the weaker PPTP, and another group of users to use the stronger L2TP/IPsec.

We can do that with remote access policies on the RRAS server, however ISA's GUI does not provides us this type of granularity. Since we want to touch as little as possible the RRAS console on ISA, we can easily accomplish this using RADIUS authentication for the VPN clients, IAS Active Directory Integrated as a RADIUS server.

We will configure ISA to use RADIUS authentication for VPN remote access connections, **Figure22**.

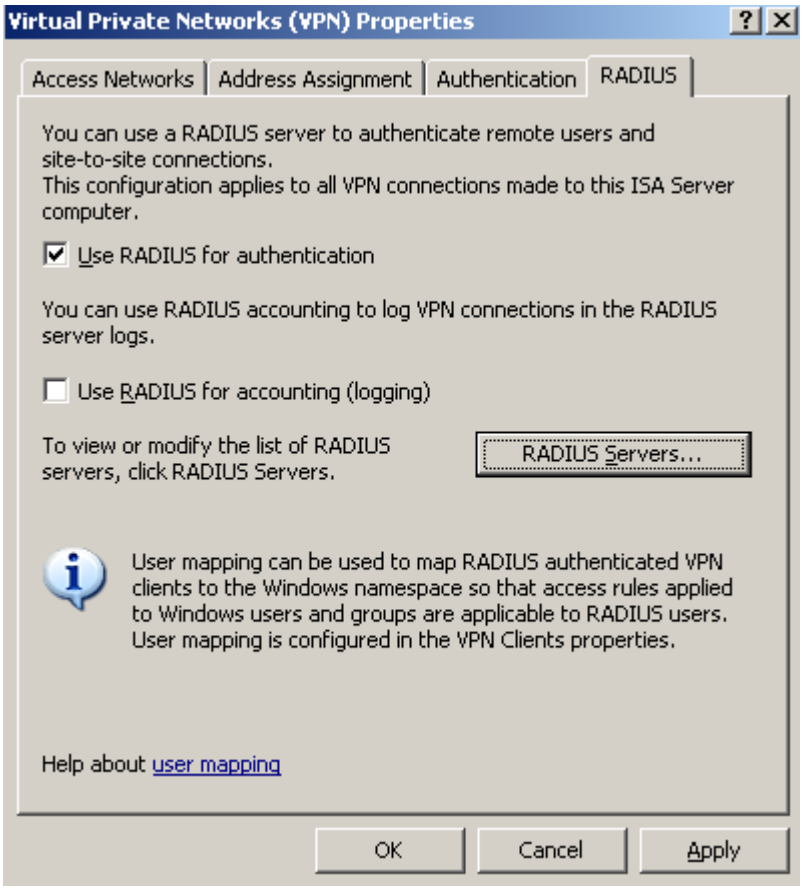


Figure22: ISA VPN Remote Access - Use Radius for Authentication

Specify a RADIUS server on ISA, the IP address of the IAS server, see **Figure23**.

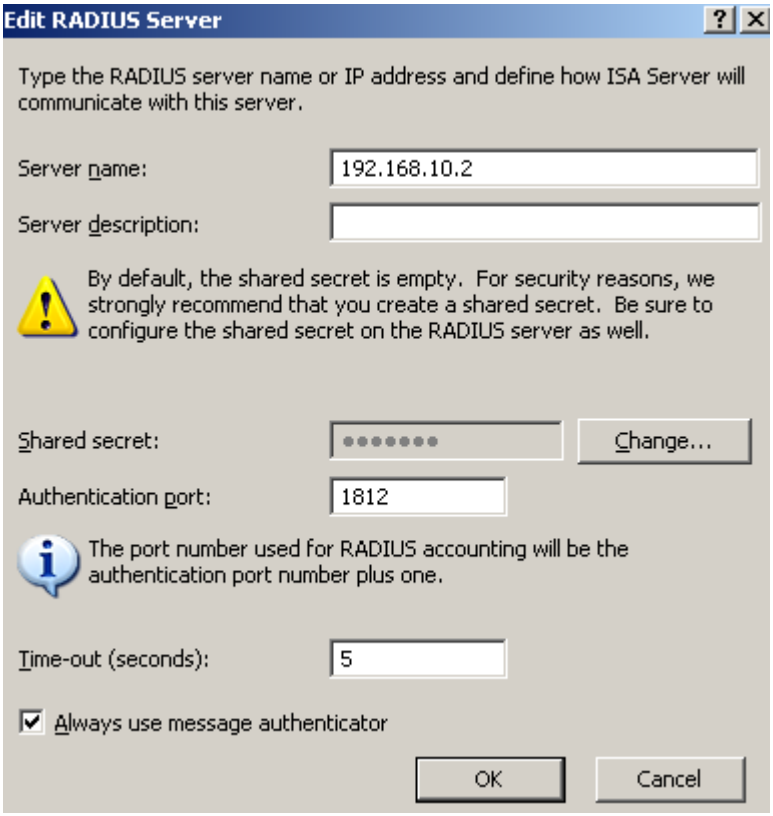


Figure23: ISA - Add A RADIUS Server

When ISA is a domain member(best practice), we can create Active Directory group-based access rules. Since we are using RADIUS for user authentication, we do not want to loose this feature.
And we don't have to, because ISA provides a feature called User Mapping, see **Figure24**. So while ISA is still a domain member(we need to map something to something), and we use RADIUS authentication, we still can use our group-based access rules even when EAP-TLS is used for user authetication.

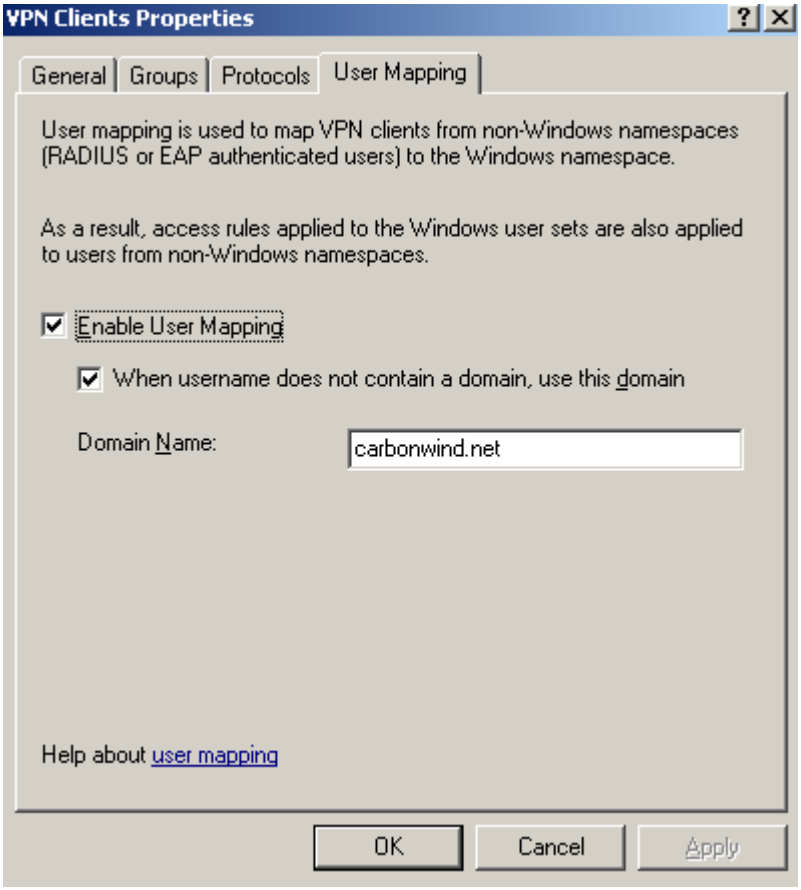


Figure24: ISA VPN Remote Access - Use Radius for Authentication

In Active Directory I've defined two group of users, L2TP VPN Users and PPTP VPN Users, see **Figure25** and **Figure26**. I will make the VPN users members of the required group:
- the L2TP/IPsec users will be members of the L2TP VPN Users group.
- the PPTP users will be members of the PPTP VPN Users group.

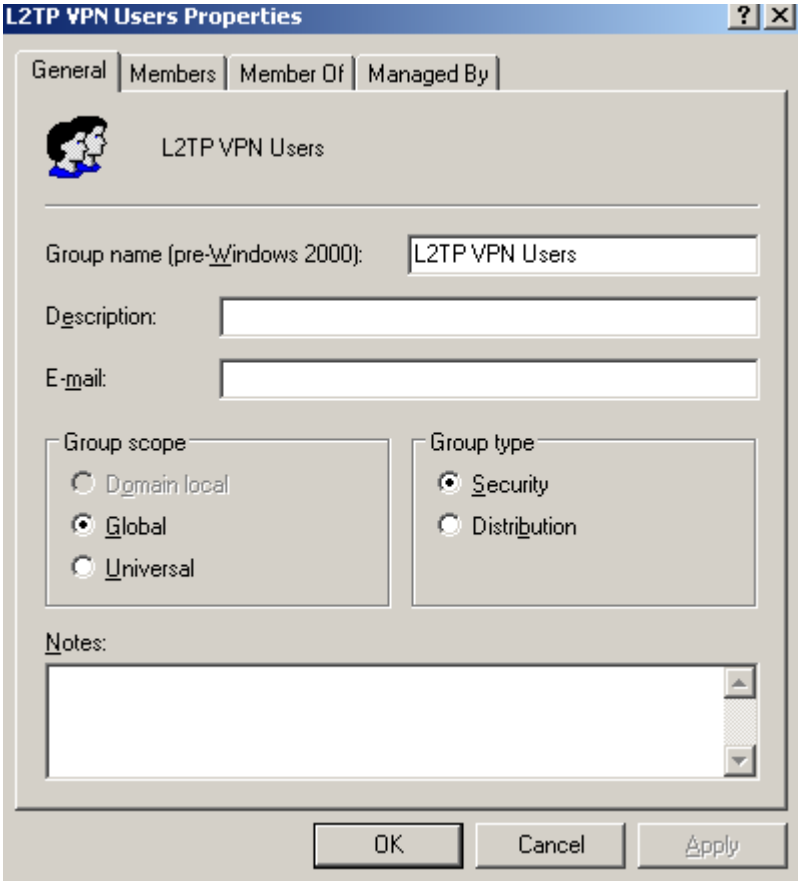


Figure25: Active Directory - L2TP VPN Users Group

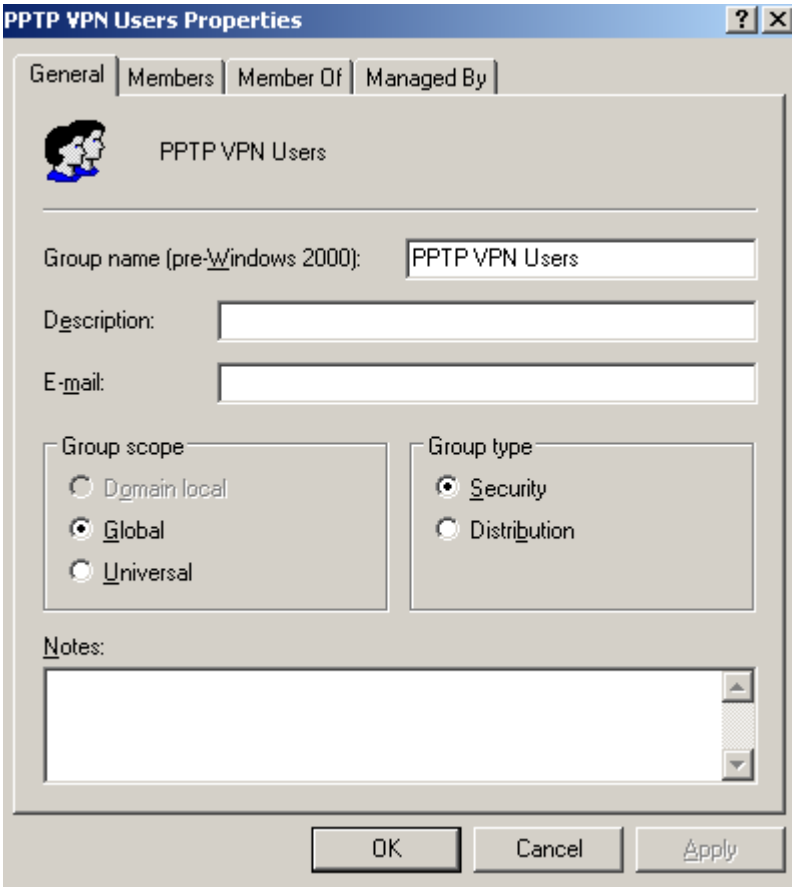


Figure26: Active Directory - PPTP VPN Users Group

The **Remote Access Permissions (Dial-in or VPN)** of the users are set to **Control access through Remote**

Access Policy, see **Figure27**.

We can disable the processing of dial-in properties for a user account, by using the **Ignore-User-Dialin-Properties** attribute on our remote access policy, if we want to. Scroll bellow for more details.

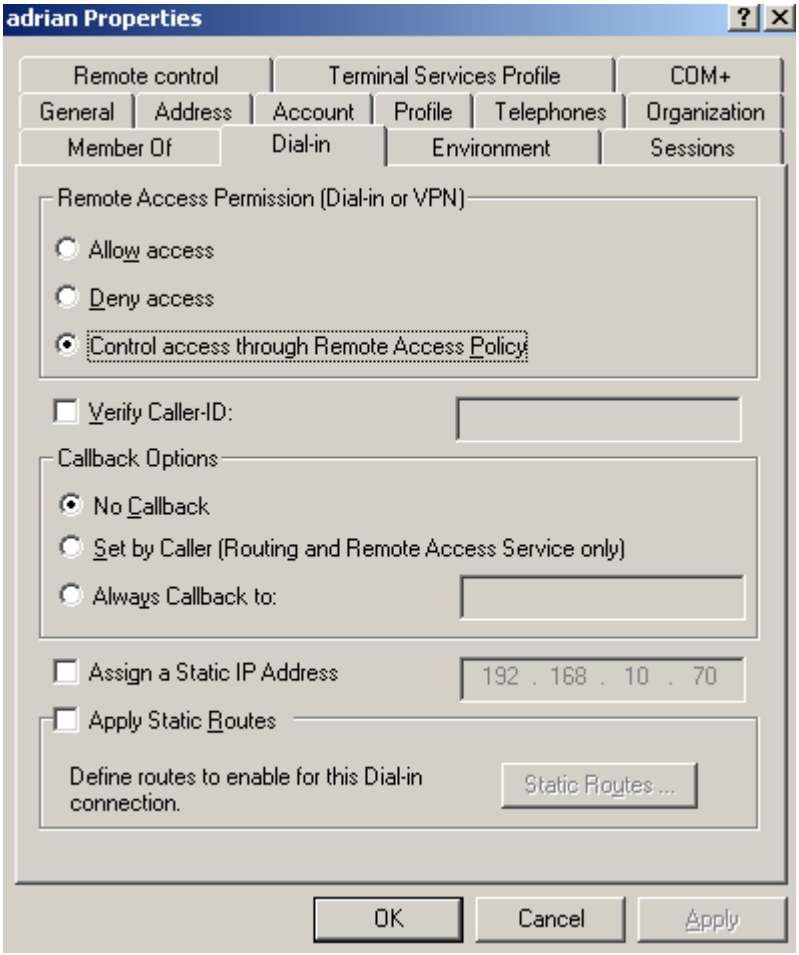


Figure27: Active Directory - User's Dial-in Permissions

Moving and configuring the IAS, I've made ISA a RADIUS client, see **Figure28**.

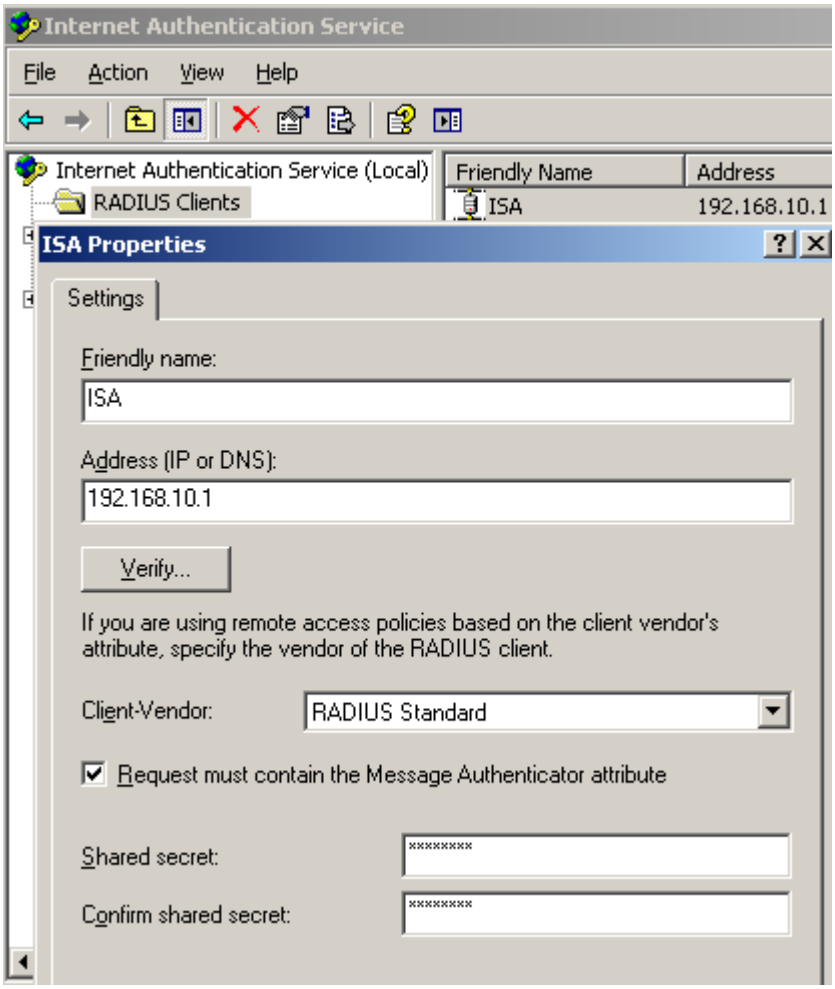


Figure28: IAS - Add ISA as a RADIUS Client

On the IAS, I've added two remote access policies using the wizard for VPN, the settings are based on this article: Force VPN clients to use strongest encryption, see **Figure29**.

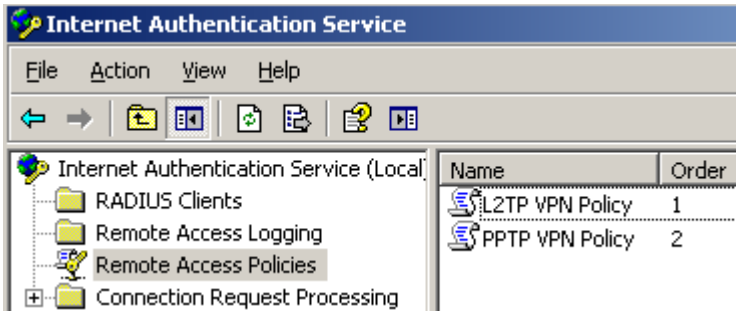


Figure29: IAS Active Directory Integrated - Remote Access Policies

Let's analyze and modify them.

The first one is called L2TP/IPsec VPN Policy, "crafted" for the group of users that will use L2TP/IPsec. As seen from **Figure30**, in the conditions to match area, I've added the **Windows-Groups** attribute matching the L2TP VPN VPN Users group, and the **Tunnel-Type** is set to **Layer Two Tunneling Protocol(L2TP)**.

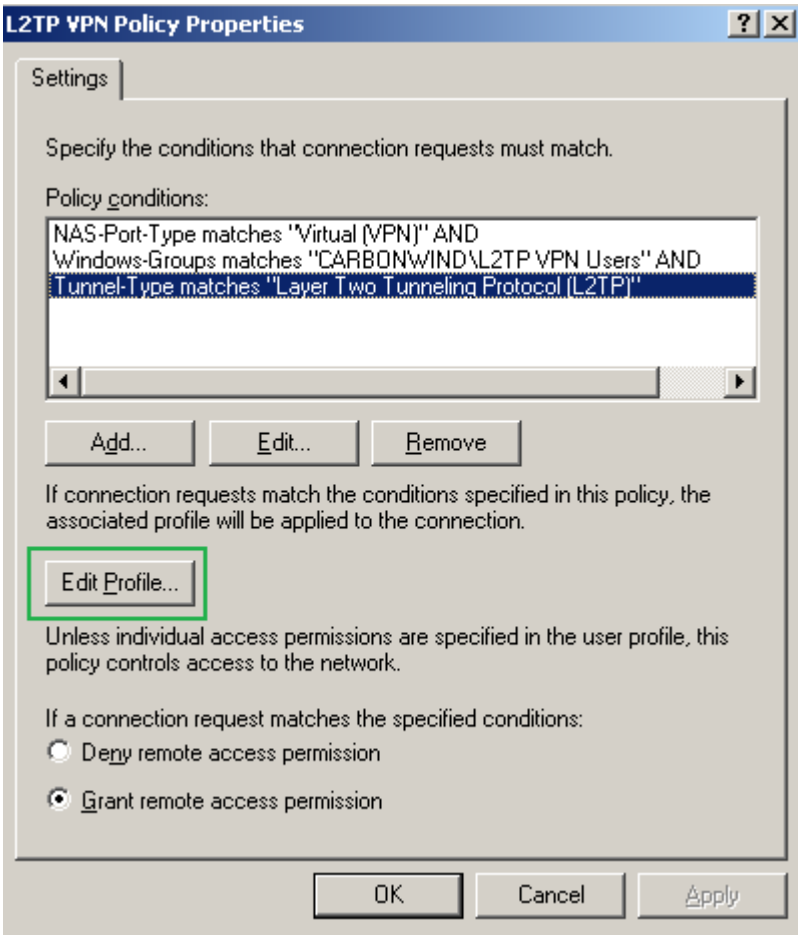


Figure30: IAS Active Directory Integrated - L2TP VPN Remote Access Policy

If we click the **Edit Profile** button, on the **Authentication** tab of the **Edit Dial-in Profile**, for the moment I've selected only MS-CHAPv2(EAP is not configured yet), see **Figure31**, MS-CHAPv2 was selected on ISA too before using RADIUS for VPN remote access user authentication.

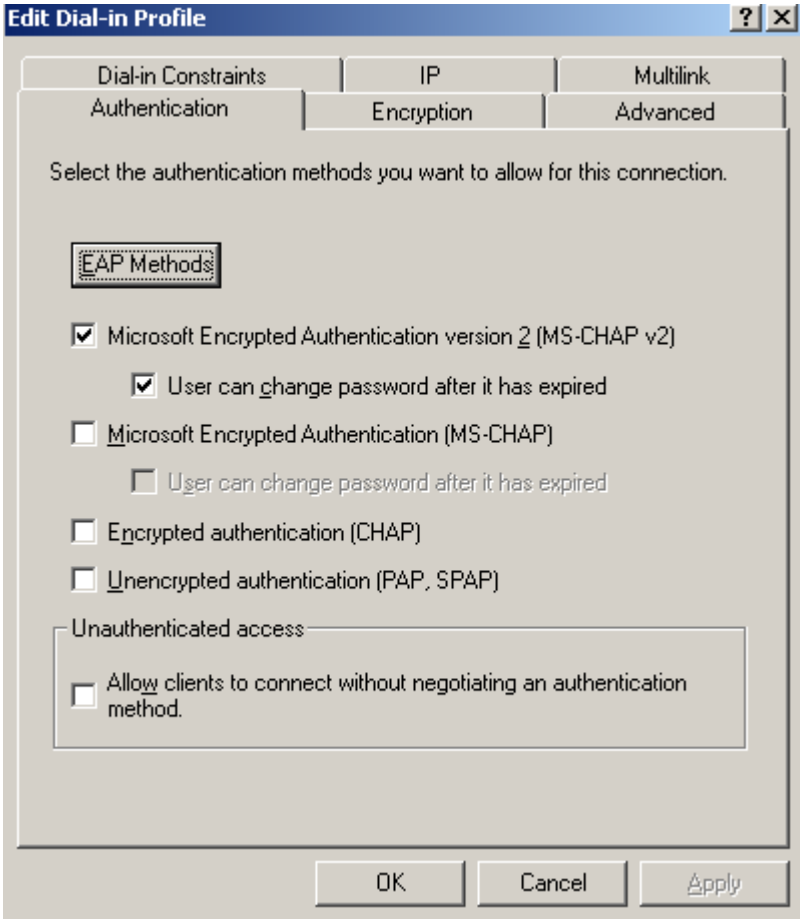


Figure31: IAS Active Directory Integrated - Edit Profile L2TP VPN Remote Access Policy: The Authentication Tab

On the **Encryption** tab of the **Edit Dial-in Profile**, only **Strongest Encryption** is selected, see **Figure32**. If you select for example **No Encryption**, then users can establish L2TP tunnels with ESP confidentiality set to NULL, however ESP integrity will still apply, as per RFC 3193 you cannot set both ESP confidentiality and integrity to NULL, unless AH is used.

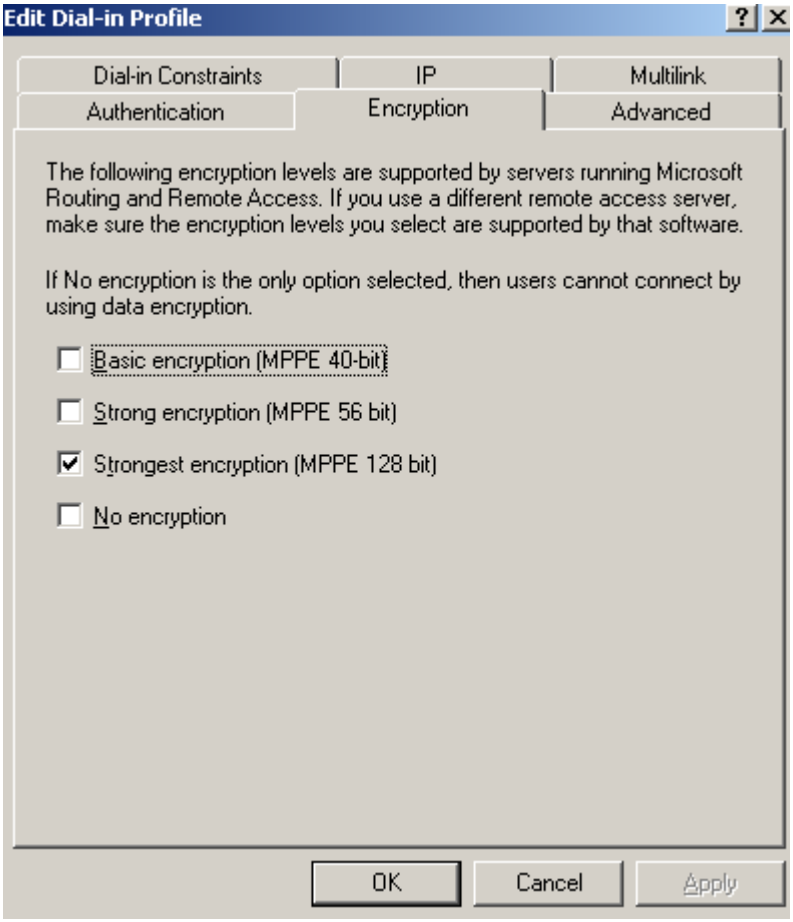


Figure32: IAS Active Directory Integrated - Edit Profile L2TP VPN Remote Access Policy: The Encryption Tab

The **Advanced** tab of the **Edit Dial-in Profile** contains the **Framed-Protocol** and the **Service-Type** attributes, see **Figure33**. Here we can set Microsoft's specific attribute **Ignore-User-Dialin-Properties**, to disable the processing of dial-in properties for users' accounts for this remote access policy, see **Figure34**. Please refer to Dial-in properties of a user account and to Accepting a connection attempt.

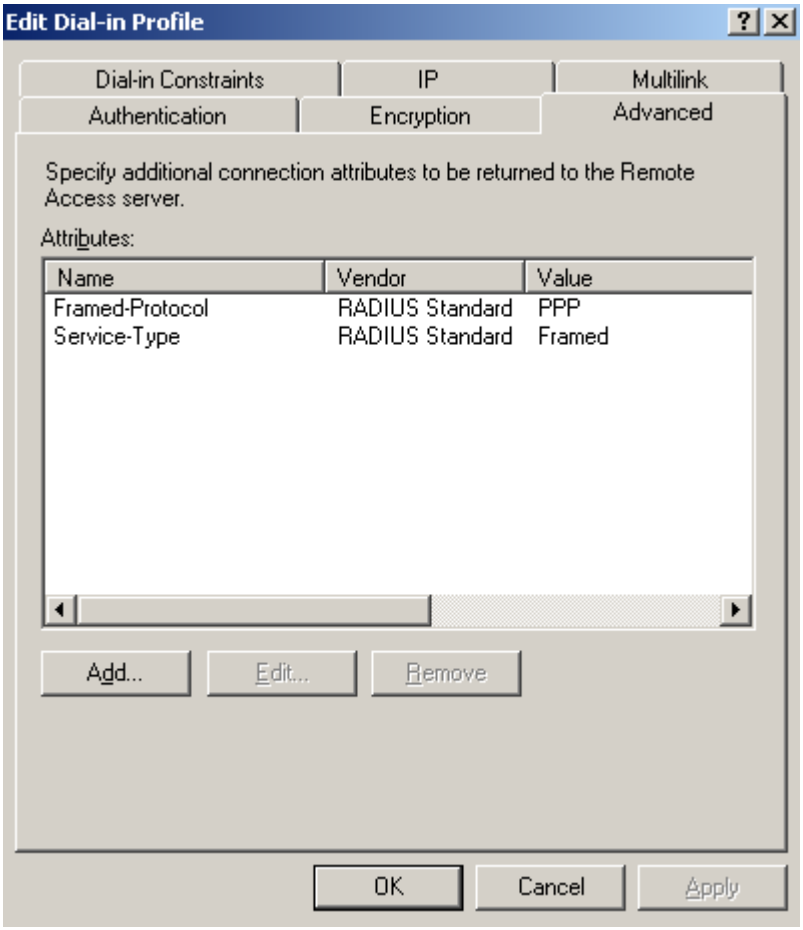


Figure33: IAS Active Directory Integrated - Edit Profile L2TP VPN Remote Access Policy: The Advanced Tab

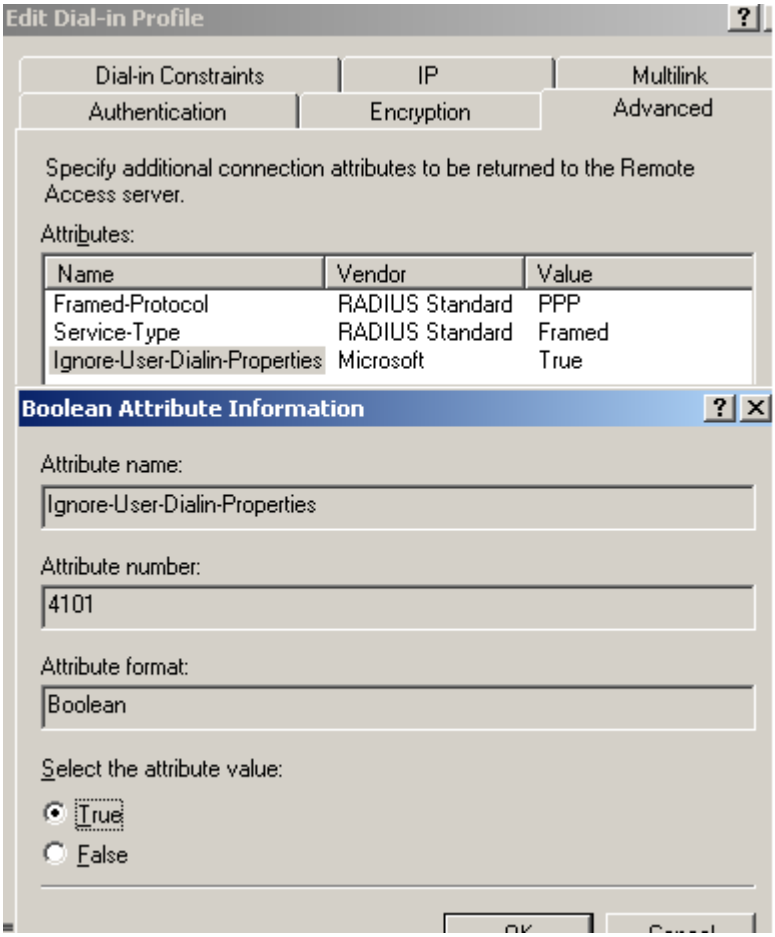


Figure34: IAS Active Directory Integrated - Edit Profile L2TP VPN Remote Access Policy: The Advanced Tab - Ignore-User-Dialin-Properties Attribute

The second remote access policy is called PPTP VPN Policy, this time "crafted" for the group of users that will use PPTP. As seen from **Figure35**, in the conditions to match area, I've added the **Windows-Groups** attribute matching the PPTP VPN Users group, and the **Tunnel-Type** is set to **Point-to-Point Tunneling Protocol(PPTP)**.

The rest of the settings of this remote access policy are identical with the ones from the L2TP VPN Policy, so I will not repeat them.

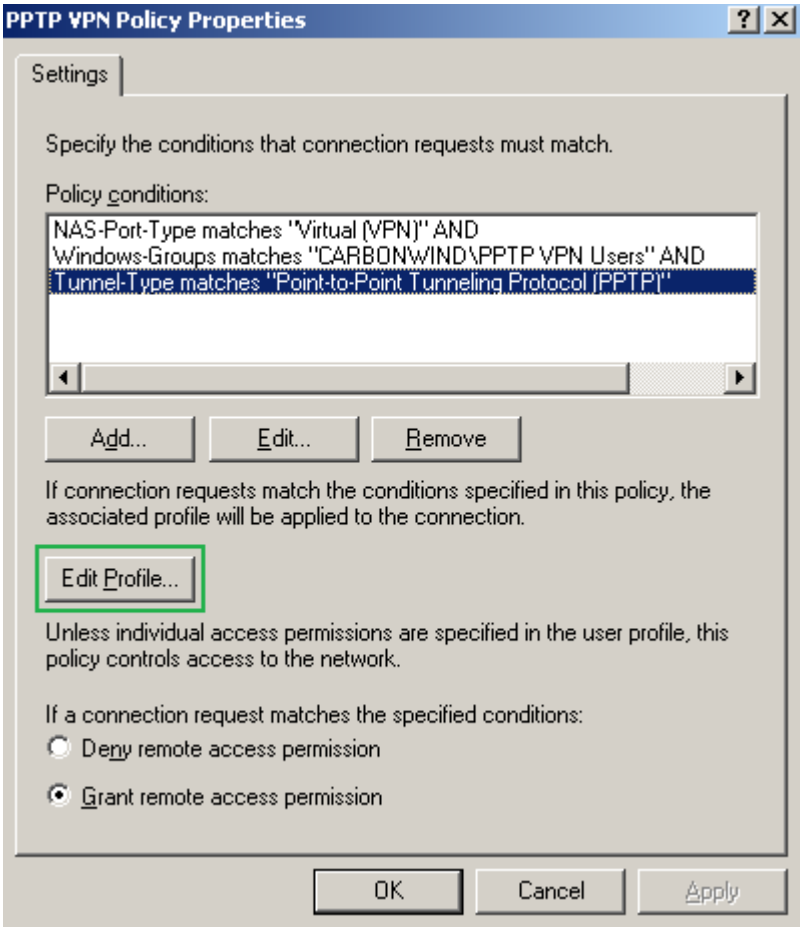


Figure35: IAS Active Directory Integrated - PPTP VPN Remote Access Policy

Going back to ISA, I've defined a test firewall policy, just to show you how easy is to configure granular group-based access rules, while using RADIUS authentication, ISA a domain member, see **Figure36**.

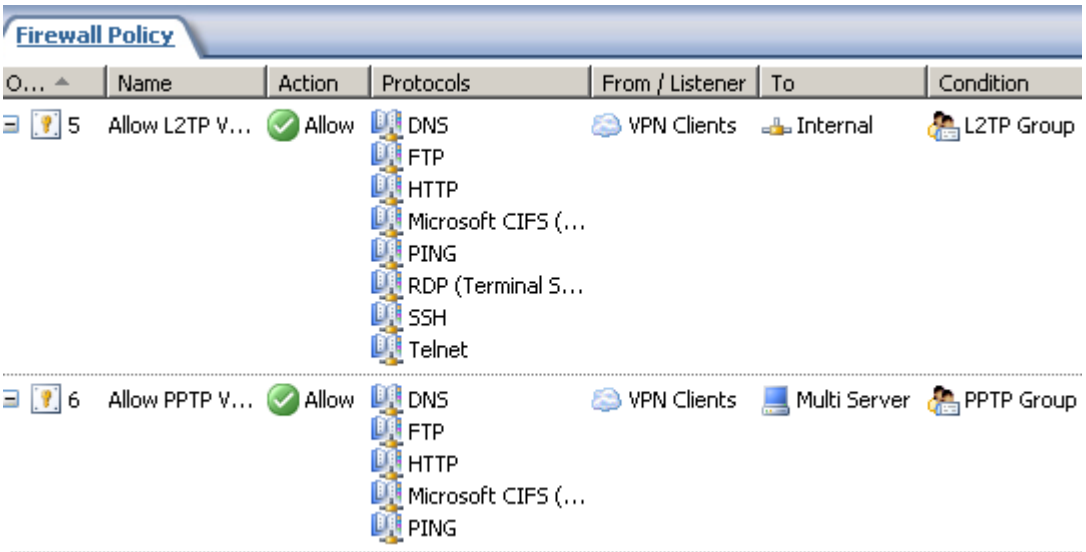


Figure36: ISA - Group Based Access Rules for VPN Clients

The ISA set of users L2TP Group which corresponds to the Windows Active Directory group L2TP VPN Users, see **Figure37**, is allowed to access certain protocols(firewall access rule 5), so in the end the users who can only use L2TP/IPsec(dues to the RADIUS remote access policy) are allowed to access only certain resources, which is what we wanted.

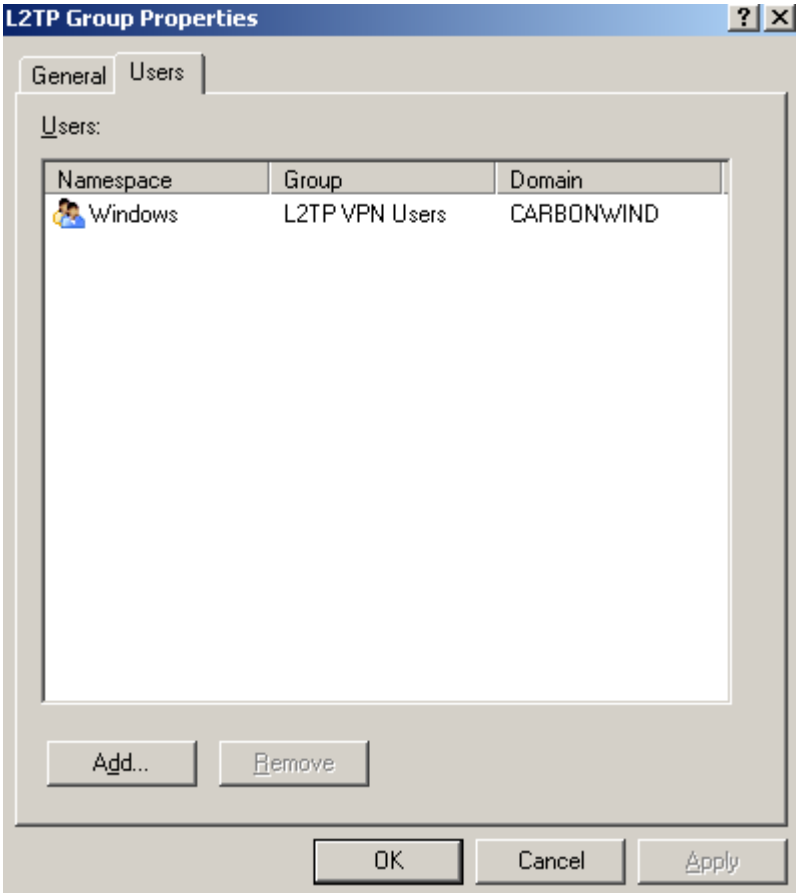


Figure37: ISA Set of Users - L2TP Group

The ISA set of users PPTP Group which corresponds to the Windows Active Directory group PPTP VPN Users, see **Figure38**, is allowed to access certain protocols and hosts located the Internal Network(firewall access rule 6), so in the end the users who can only use PPTP(due to the RADIUS remote access policy) are allowed to access only certain resources, which is what we wanted.

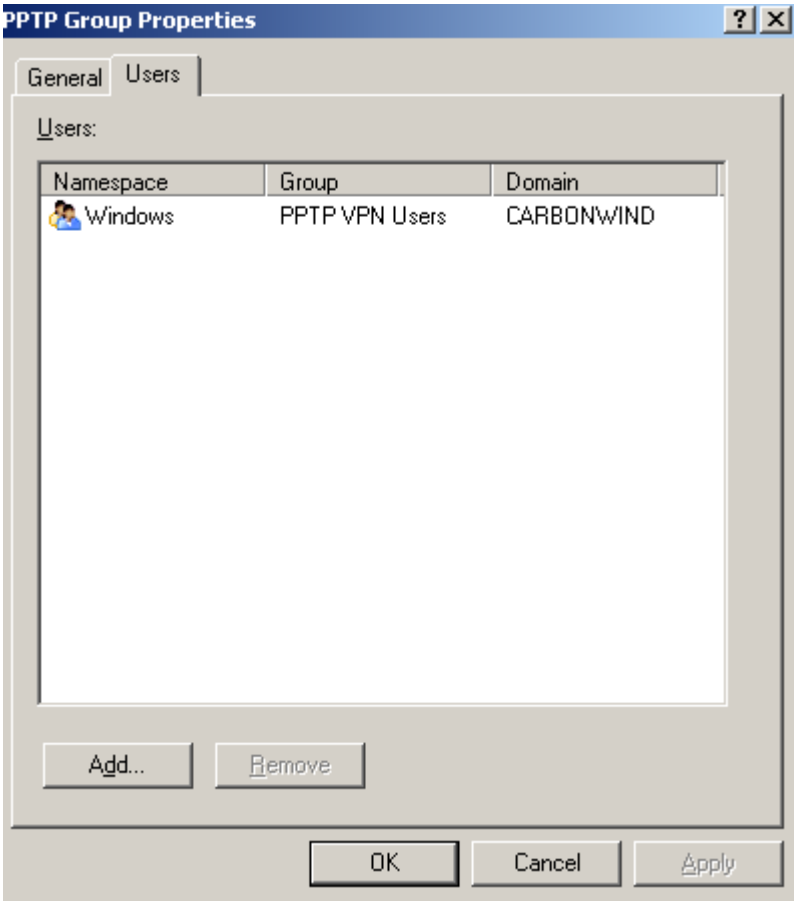


Figure38: ISA Set of Users - PPTP Group

Actually we can get even more granularity. For example we can group the users belonging to the L2TP VPN Users group into smaller different Active Directory groups which we can use for ISA's access rules granting access to the resouces located behind it. Say a couple of users will belong to group AA, and another few users will belong to group BB. Group AA can be allowed to use say RDP to an internal server and group BB to use SSH to an internal server. Since members of both groups belong to the bigger L2TP VPN Users group, they can only use L2TP due to the RADIUS remote access policy.

We can refine the access rules till the user-based level, without having to bind a specific user to a specific IP address, IP address to use with our access rules to control access to internal resources, a feature which represents a huge benefit from the administrative perspective.

To make a quick test, if we connect with the user John who belongs to the PPTP VPN Users group using the PPTP protocol, user John will be granted access, see the IAS log from **Figure39**.

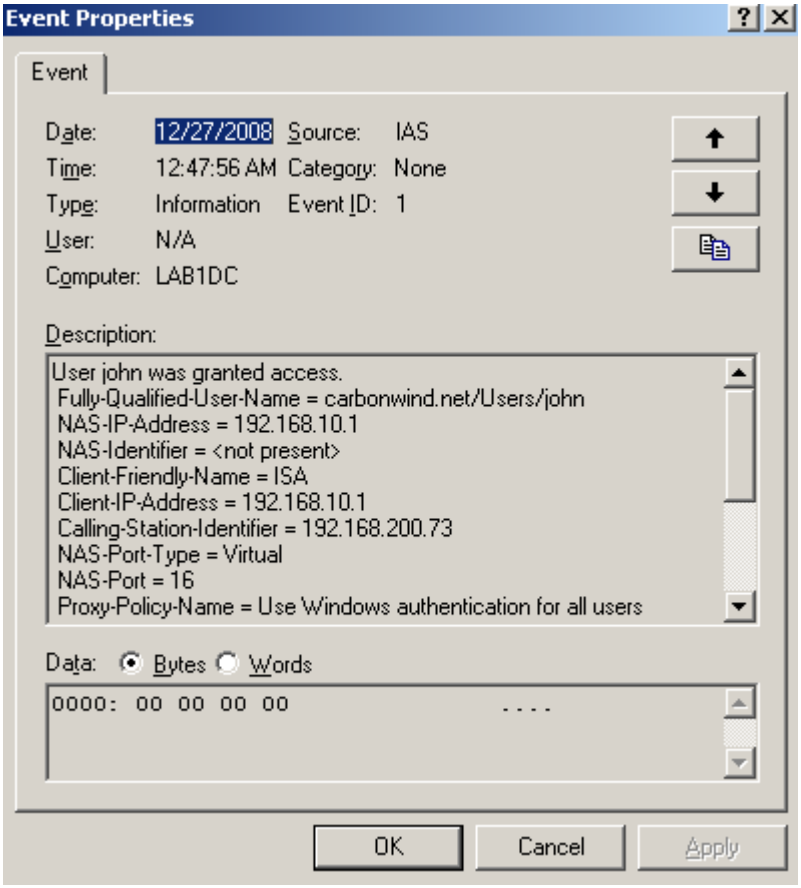


Figure39: IAS - User john was granted access

However, if we connect with the same user John who belongs to the PPTP VPN Users group using the L2TP/ IPsec protocol, user John will be denied access, see the IAS log from **Figure40**.

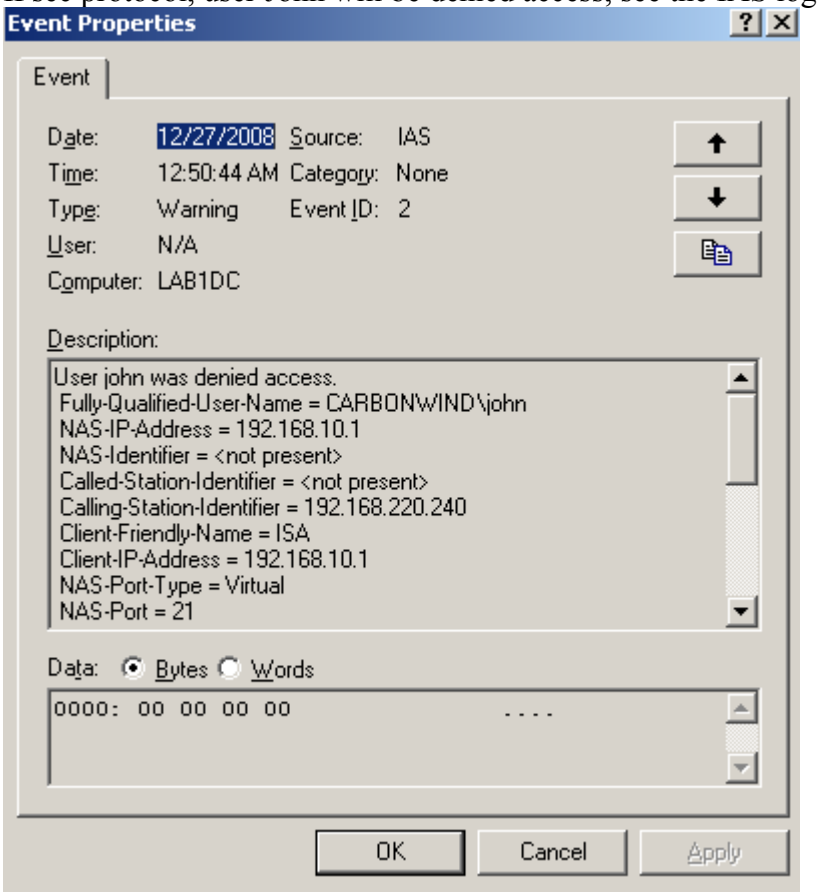


Figure40: IAS - User john was denied access

5. How do I specify that users from location X can use only PPTP and that users from location Y can use only L2TP/Psec and adjust the firewall access rules to control access to internal resources in respect with the VPN protocol used by users and the location of these users ?

For example you have two locations, X and Y. From location X you want to allow only PPTP connections to ISA, and from location Y you want to allow only L2TP/IPsec connections to ISA.

Furthermore, you've decided to group the VPN users from location X into a specific Active Directory group, and to group the VPN users from location Y into another specific Active Directory group because the access rules on ISA are defined based on Active Directory users and groups. You need that the PPTP group to access certain resources, and the L2TP/IPsec group other resources over the VPN tunnel.

This is pretty easy to accomplish, grouping the already used tricks from above.

First we need the trick with the Empty Network on ISA, and the custom access rules for incoming VPN remote access connections, see **Figure41**. You may add the desired IP addresses for location X and location Y.

Doing so we will make sure that ISA will only allow L2TP/IPsec traffic from location Y and only PPTP traffic from location X.

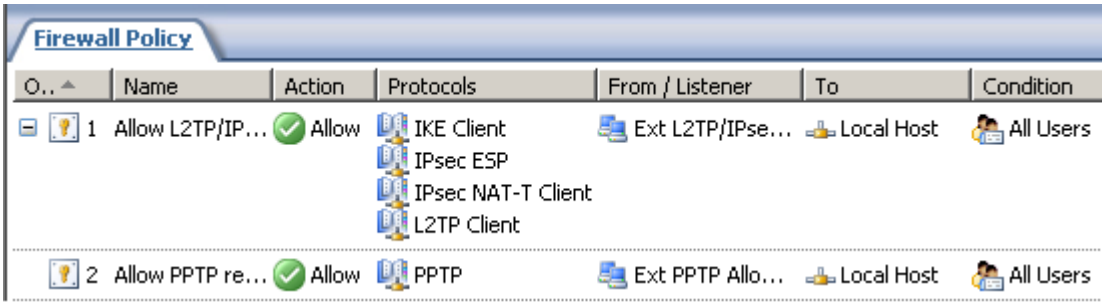


Figure41: ISA - Custom Access Rules

Next, we will use the RADIUS tricks for creating two remote access policies for PPTP and for L2TP/IPsec, see **Figure42** and **Figure43**.

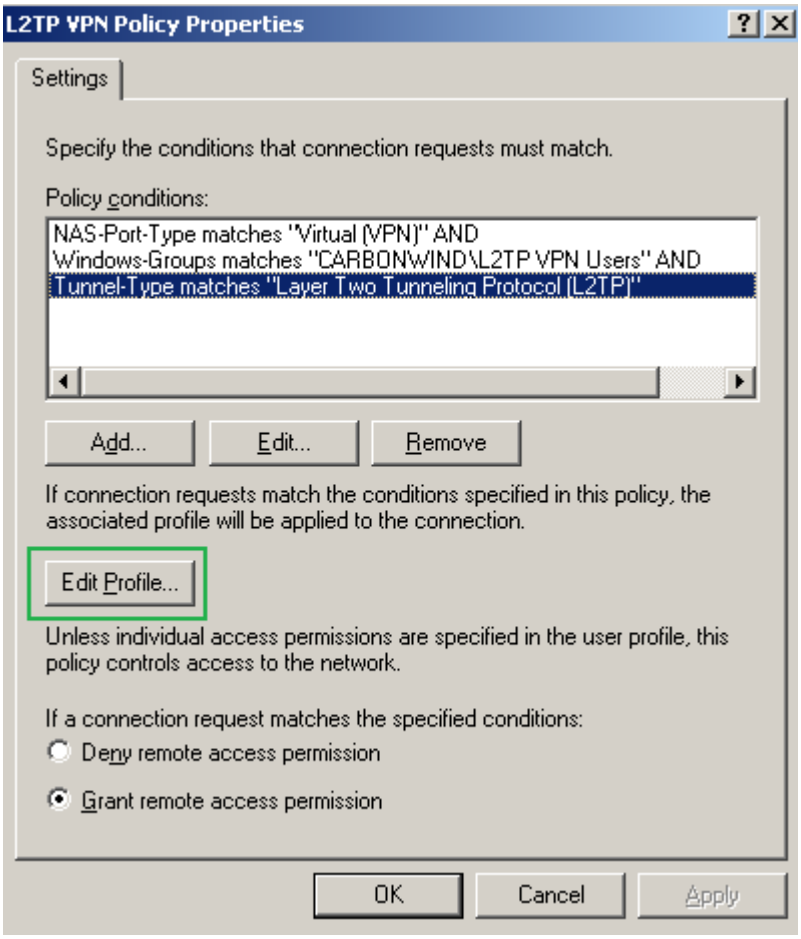


Figure42: IAS Active Directory Integrated - L2TP VPN Remote Access Policy

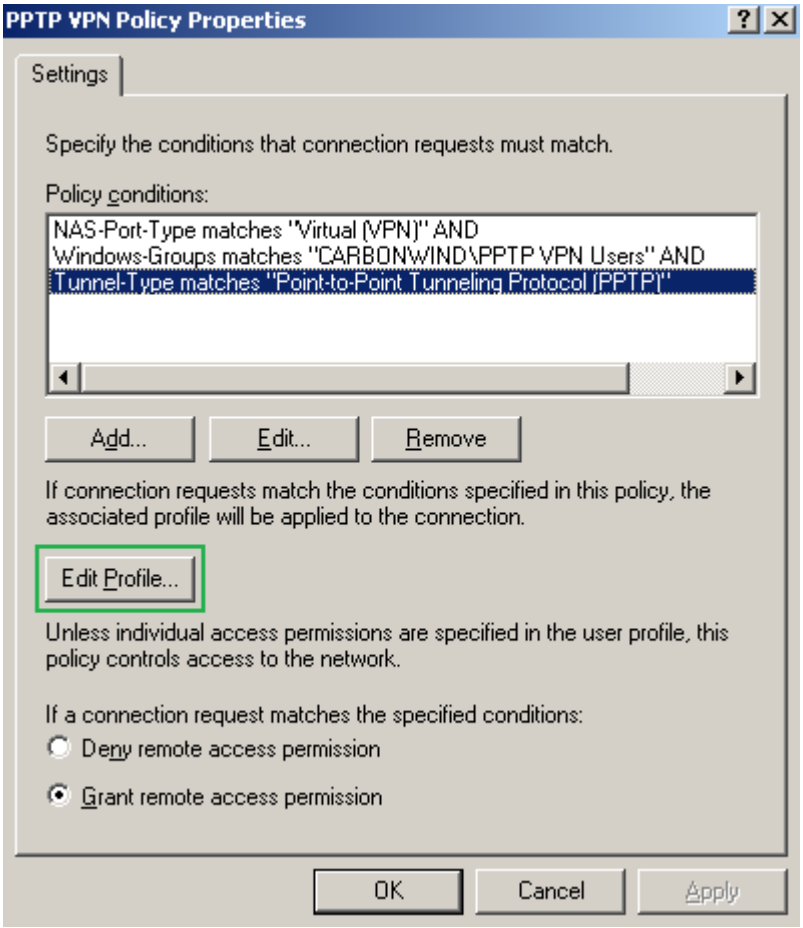


Figure43: IAS Active Directory Integrated - PPTP VPN Remote Access Policy

Putting the pieces together:

- only L2TP/IPsec connections can be initiated from location Y(due to ISA firewall rules). Due to the RADIUS remote access policies only the L2TP VPN Users Active Directory group can use L2TP. Also due to firewall limitations, the L2TP VPN Users Active Directory group can access only certain resources, see **Figure44**. So, indirectly due to the policies defined on the firewall and on the RADIUS server, users from location Y can only access certain resources located behind ISA.

- only PPTP connections can be initiated from location X(due to ISA firewall rules). Due to the RADIUS remote access policies only the PPTP VPN Users Active Directory group can use PPTP. Also due to firewall limitations, the PPTP VPN Users Active Directory group can access only certain resources, see **Figure44**. Again, indirectly due to the policies defined on the firewall and on the RADIUS server, users from location Y can only access certain resources located behind ISA.

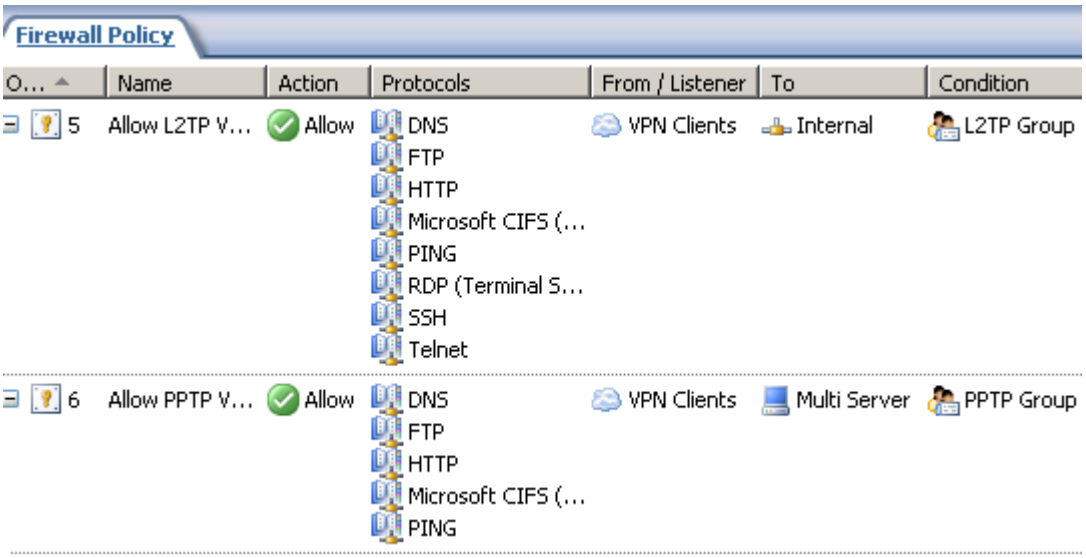


Figure44: ISA - Group Based Access Rules for VPN Clients

As already said, actually we can get even more granularity. For example we can group the users belonging to the L2TP VPN Users into smaller different Active Directory groups which we can use for ISA's access rules allowing access to the resouces located behind it. So a couple of users will belong to group AA, and another few users will belong to group BB. Group AA can be allowed to use say RDP to an internal server and group BB to use SSH to an internal server. Since members of both groups belong to the bigger L2TP VPN Users group, they can only use L2TP due to RADIUS remote access policies.

We can refine the access rules till the user-based level, without having to bind a specific user to a specific IP address, IP address to use with our access rules to control access to internal resources, saving us a lot of administrative overhead.

6. How do I specify that a group of users can only connect from location X and another group of users can connect from any location ?

I saw this one on http://forums.isaserver.org/m_2002071818/mpage_1/key_restrict%2cvpn/tm.htm#2002071818.

It is doable. It's a little unclear what exactly Gatis wants to achieve.

If he wants a group of users from location X(external location) to use only PPTP and a group users from anywhere(external locations) except location X to use L2TP/IPsec, we can use the combination of firewall rules and RADIUS remote access policy, see **Figure45**, **Figure46**, **Figure47** and **Figure48**.

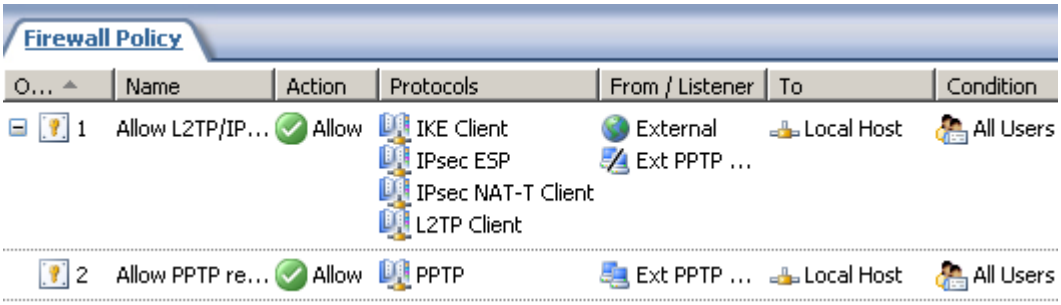


Figure45: ISA Custom Access Rules

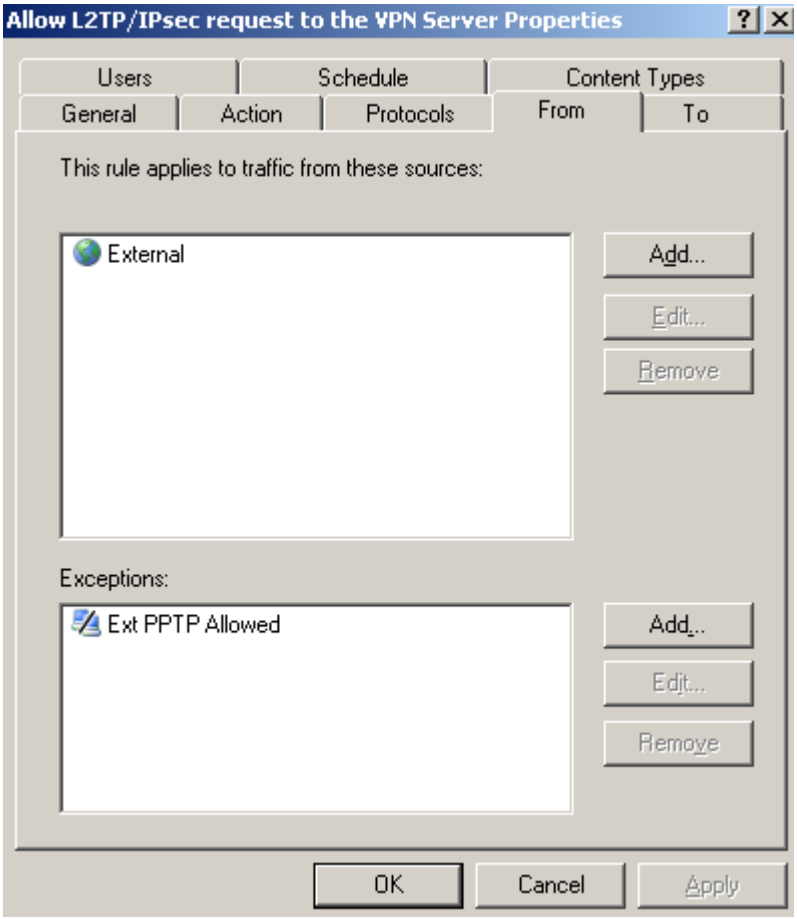


Figure46: ISA Custom Inbound L2TP/IPsec remote Access Access Rule - Exceptions

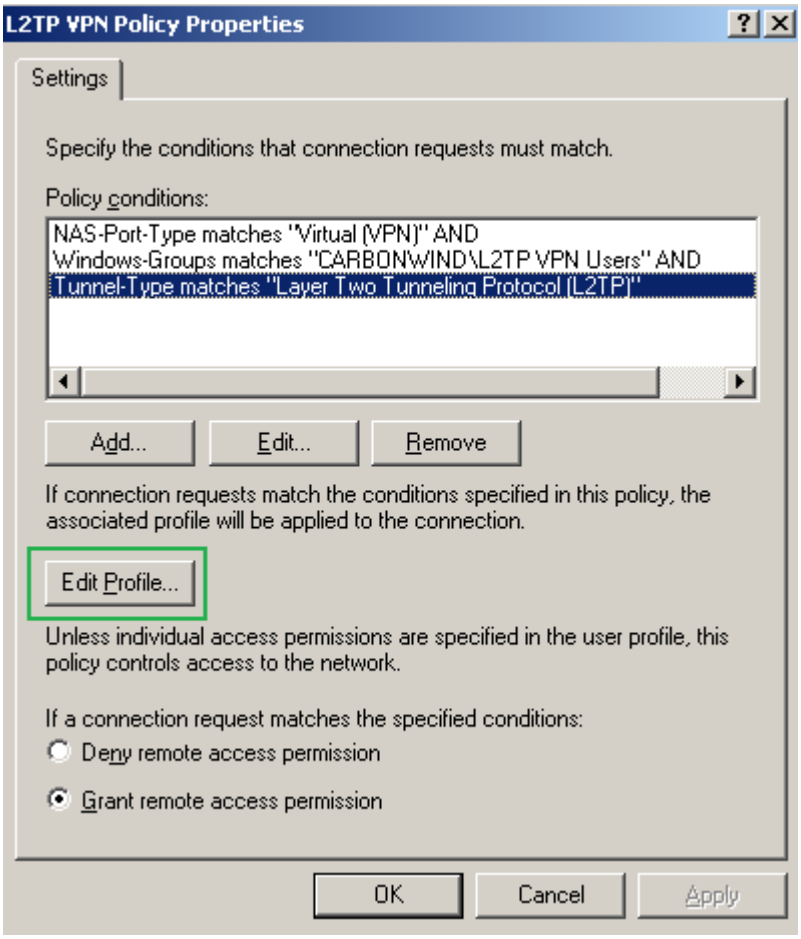


Figure47: IAS Active Directory Integrated - L2TP VPN Remote Access Policy

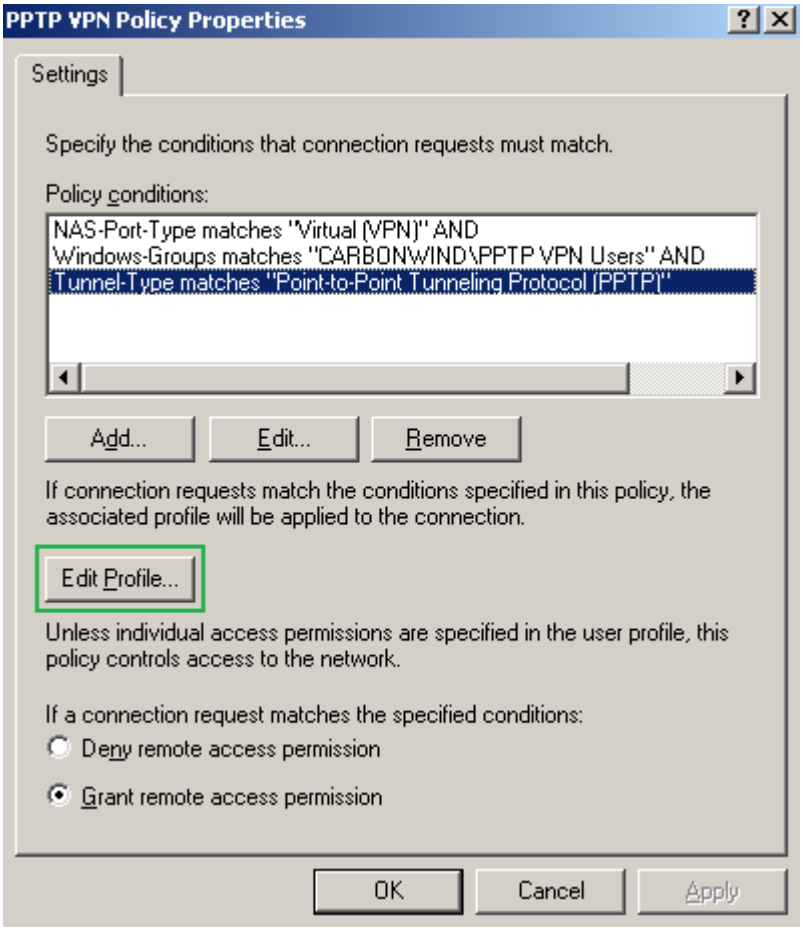


Figure48: IAS Active Directory Integrated - PPTP VPN Remote Access Policy

The first access rule, **Figure45**, allows incoming L2TP/IPsec remote access connections from the External Network with an exception, the location from which only PPTP connections are allowed. The RADIUS policy from **Figure47** allows only the L2TP VPN Users group to use L2TP.

The second access rule, **Figure45**, allows incoming PPTP remote access connections only from location X. The RADIUS policy from **Figure48** allows only the PPTP VPN Users group to use PPTP.

So if a user from location X wants to use L2TP/IPsec, he or she cannot due to the firewall rules, he or she must use only PPTP. Due to the RADIUS remote access policies, he or she must be a member of the PPTP VPN Users group. Access to the resources located behind ISA is controlled based on Active Directory group to which the user belongs, see **Figure49**, so the user is limited to access the resources that the group to which he or she belongs is allowed to access.

If a user from the any external place except location X will connect with L2TP/IPsec, he or she must be a member of the L2TP VPN Users group due to the RADIUS remote access policies restriction which allow only the users belonging to the L2TP VPN Users group to use L2TP. Again, access to the resources located behind ISA is controlled based on Active Directory group to which the user belongs, see **Figure49**, so the user is limited to access the resources that the group to which he or she belongs is allowed to access.

So indirectly we've managed to bind things together in this situation.

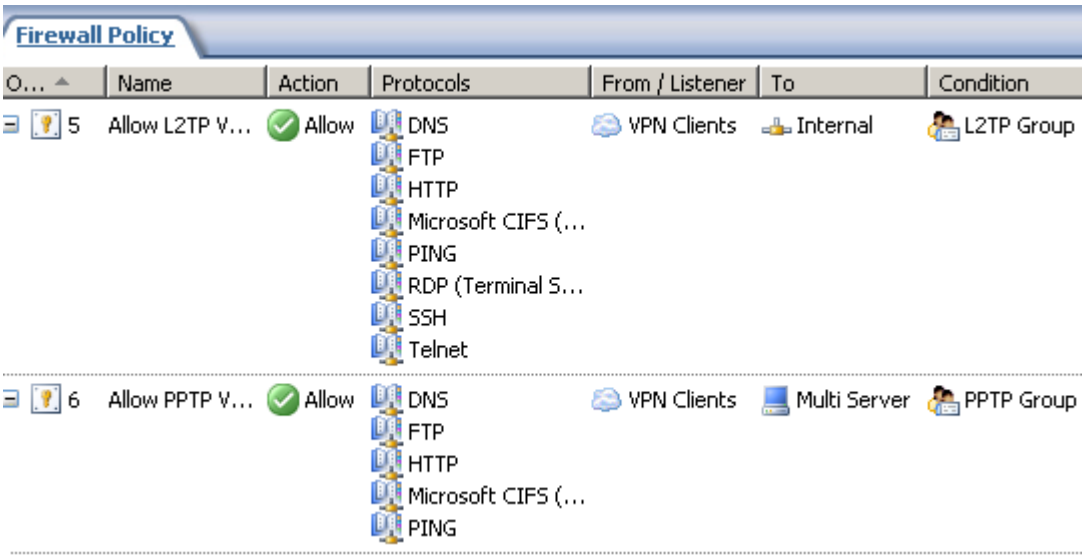


Figure49: ISA - Group Based Access Rules for VPN Clients

Actually, as said before we can get even more granularity. For example we can group the users belonging to the L2TP VPN Users into smaller different Active Directory groups which we can use for ISA's access rules allowing access to the resouces located behind it. So a couple of users will belong to group AA, and another users will belong to group BB. Group AA can be allowed to use say RDP to an internal server and group BB to use SSH to connect to an internal server. Since members of both groups belong to the L2TP VPN Users group, they can only use L2TP due to RADIUS remote access policies, and they can connect from anywhere except from location X.

We can refine the access rules till the user-based level, without having to bind a specific user to a specific IP address, IP address to use with our access rules to control access to internal resources.

However if Gant simply wants that only a certain group of users to connect to ISA only from from location X(external location) using either PPTP or L2TP/IPsec, and another group of users to connect to ISA from

anywhere(external locations) PPTP or L2TP/IPsec, we cannot use the combination of firewall rules for incoming VPN traffic and RADIUS remote access policies.

So we must bind together somehow the location with the group of users. We can do that on the RADIUS server with remote access policies.

I've added in Active Directory two new groups, the VPN Users Location X group which will contain the users from location X allowed to use VPN, see **Figure50**, and the VPN Users Location Anywhere group which will contain the users allowed to use VPN from anywhere, see **Figure51**.

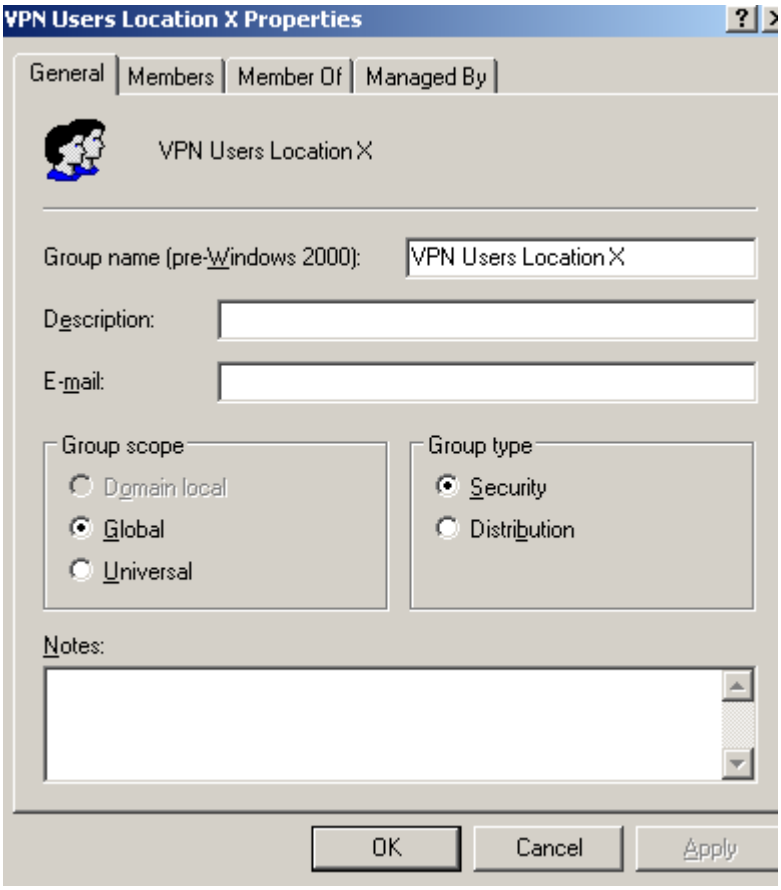


Figure50: Active Directory - VPN Users Location X Group

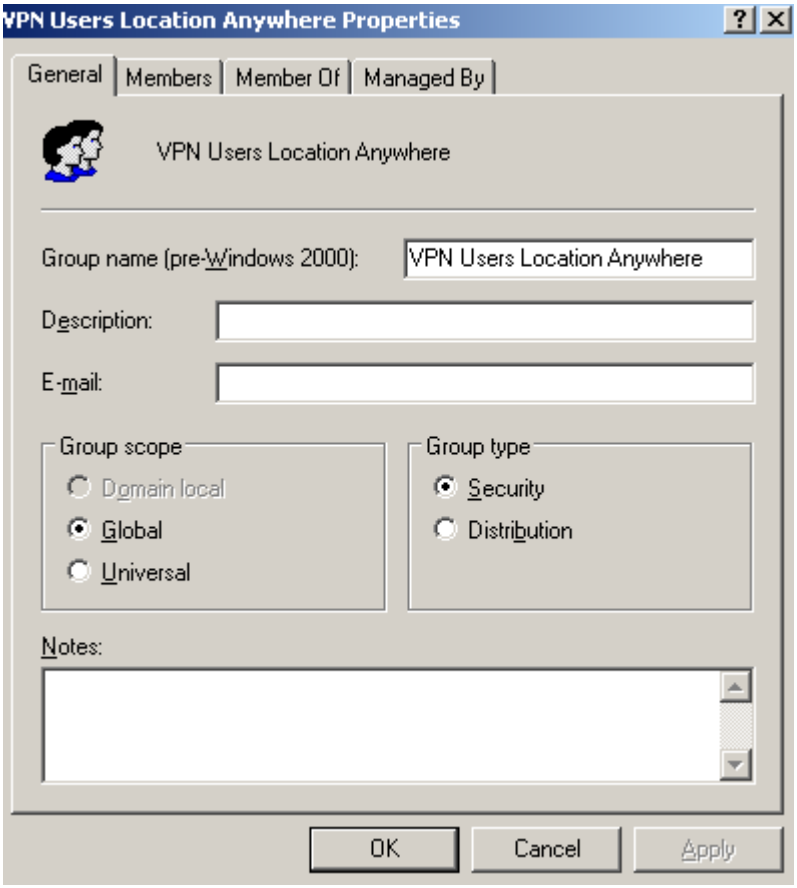


Figure51: Active Directory - VPN Users Location Anywhere Group

As before following the wizard for VPN I've defined two remote access policies on the IAS, the settings being based on this article: Force VPN clients to use strongest encryption, see **Figure52**.

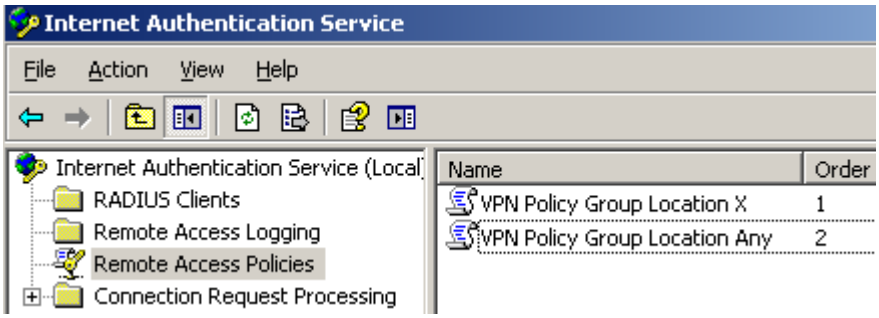


Figure52: IAS Active Directory Integrated - Remote Access Policies

And we will edit them.

The first remote access policy, VPN Policy Group Location X will apply to the group of users VPN Users Location X that are allowed to connect from location X, see **Figure53**. As shown there, I've added a new condition **Calling-Station-Id**, refer to Concepts for IAS. This parameter will allow us to bind a user or group of users with a specific location.

For example let's say that location X uses the "public" subnet 192.168.220.0/24(one more time: in practice this is *not* the private subnet from which VPN clients behind NAT devices will connect).

To know what to enter for the parameter **Calling-Station-Id**, we will take a look at Pattern matching syntax.

For example I've entered: *(192\.168\.220\..*)*.

If we need another subnet too, we can enter: *(192\.168\.220\..*)|(192\.168\.250\..*)*.
If all the VPN clients are behind a NAT device with one public IP address we can enter: *(192\.168\.220\.240)*.
If the NAT devices uses a pool of IP addresses for NAT-ing outbound connections, we can enter: *(192\.168\.220\.240)|(192\.168\.220\.241)|(192\.168\.220\.242)*.

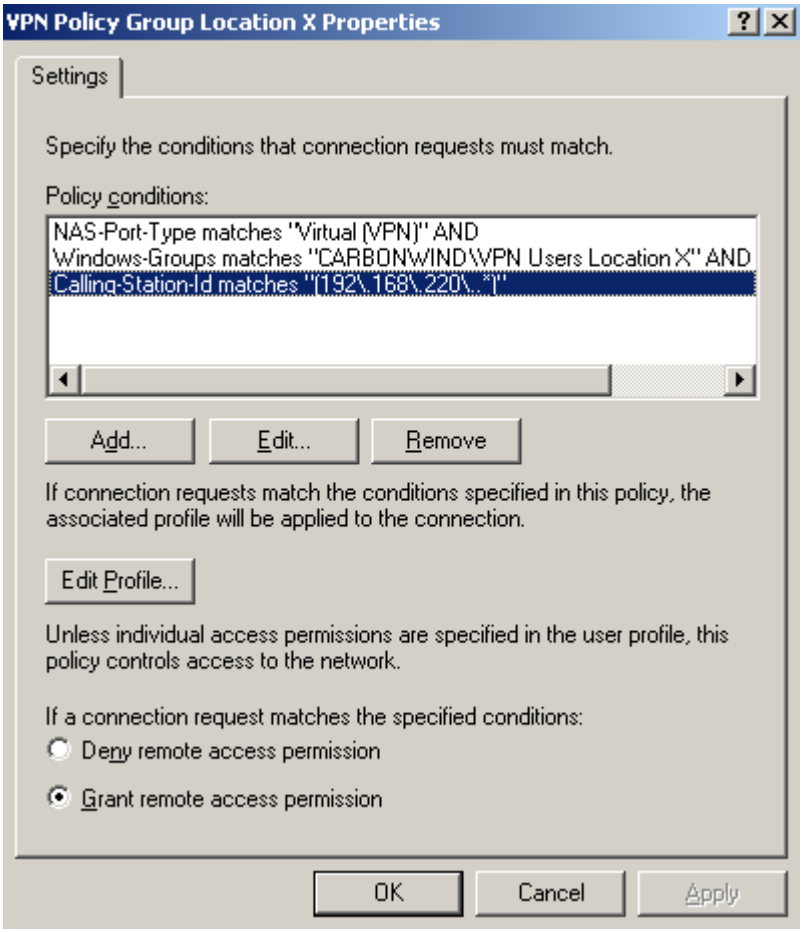


Figure53: IAS Active Directory Integrated Remote Access Policy - VPN Policy Group Location X

The second remote access policy, VPN Policy Group Location Any will apply to the group of users VPN Users Location Anywhere that are allowed to connect from any external location, see **Figure54**.

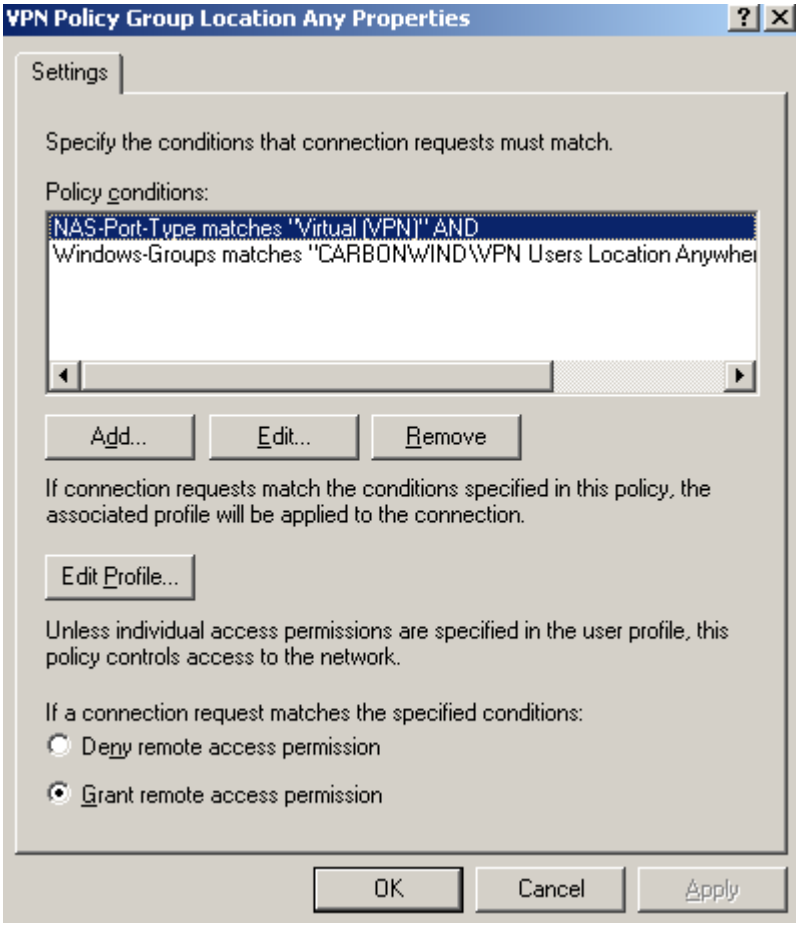


Figure54: IAS Active Directory Integrated Remote Access Policy - VPN Policy Group Location Any

If we want the users from the VPN Users Location Anywhere group to connect from almost anywhere, except say from Location X, we can simply add a new remote access policy which denies access to this group when the connection is initiated from location X, see **Figure55**.

I've added a new remote access policy, VPN Policy Group Location Any Deny Location X, and place this policy above the VPN Policy Group Location Any policy. The VPN Policy Group Location Any Deny Location X policy denies access if a user from the VPN Users Location Anywhere group attempts to establish a VPN connection from location X, see **Figure56**.

The remote access policies are processed in order, so the VPN Policy Group Location Any Deny Location X policy will be matched before the VPN Policy Group Location Any policy, denying the access from location X as required.

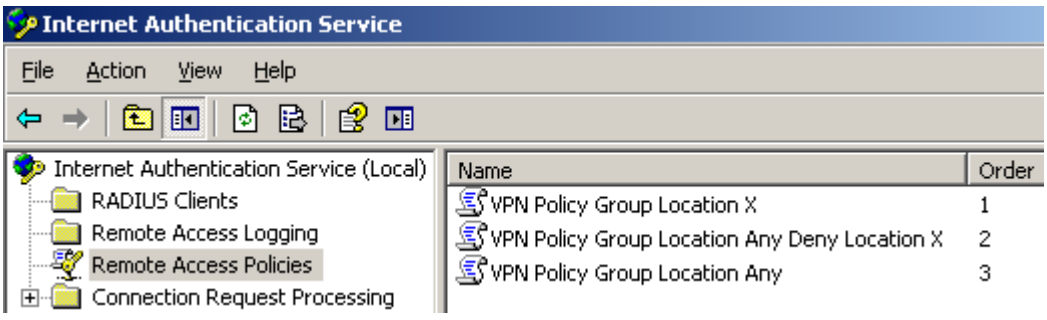


Figure55: IAS Active Directory Integrated - Ordered Remote Access Policies

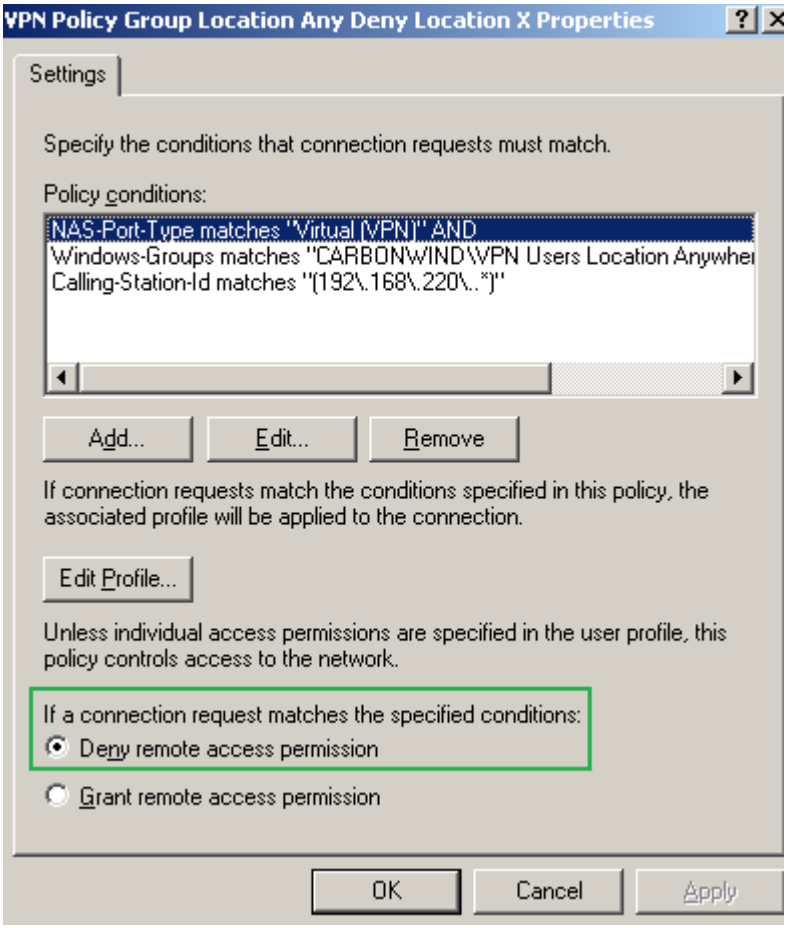


Figure56: IAS Active Directory Integrated Remote Access Policy - VPN Policy Group Location Any Deny Location X

Now, let's create some test group-based access rules on ISA for allowing access to resources for the VPN clients.

On ISA I've added two sets of users see **Figure57** and **Figure58**.

The ISA set of users VPN Users Location X which corresponds to the Windows Active Directory group VPN Users Location X, is allowed to access certain protocols and hosts located the Internal Network see **Figure59** (firewall access rule 5), so in the end the users from location X are allowed to access only certain resources, which is what we might want.

The ISA set of users VPN Users Location Anywhere which corresponds to the Windows Active Directory group VPN Users Location Anywhere, is allowed to access certain protocols and hosts located the Internal Network, see **Figure59** (firewall access rule 6), so in the end the users from the "anywhere group" are allowed to access only certain resources, which is what we might want.

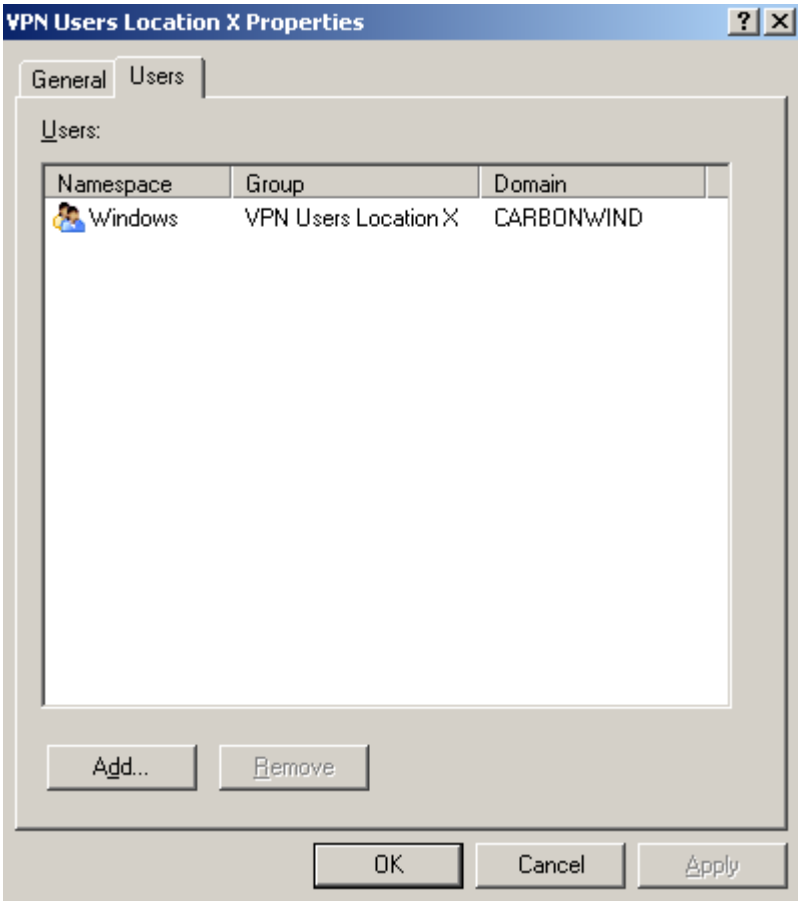


Figure57: ISA Set of Users - VPN Users Location X

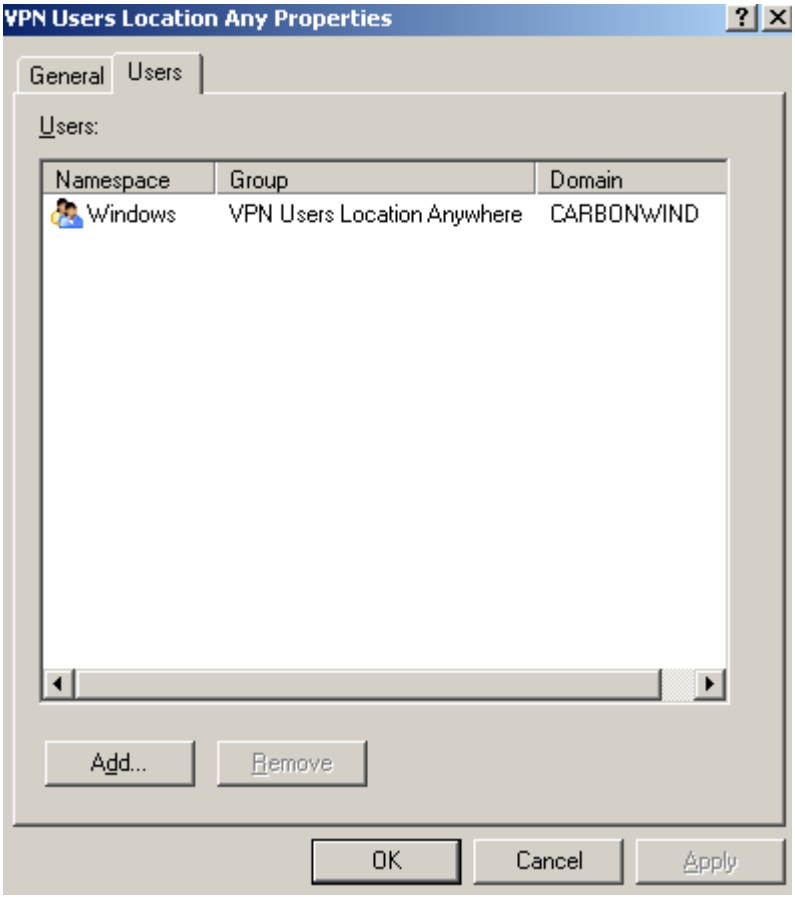


Figure58: ISA Set of Users - VPN Users Location X

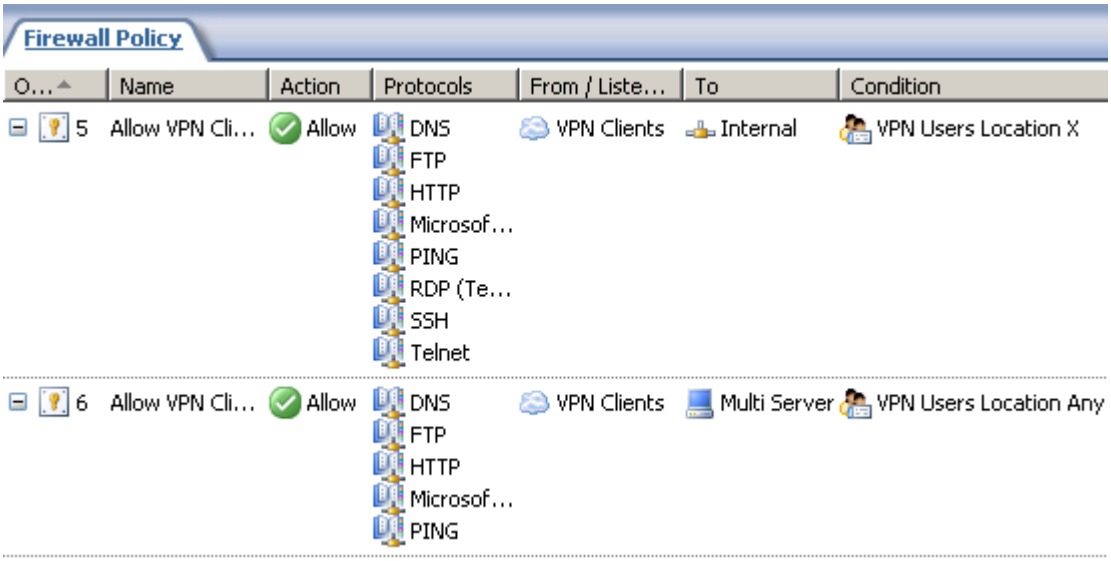


Figure59: ISA - Group-Based Access Rules

And, we can group the users from the VPN Users Location X Active Directory group into smaller Active Directory groups, say group AA and group BB, so that we can refine the group-based access rules on ISA. Members from the group AA will be allowed to use RDP and the members from the group BB to use SSH. Since the members of these both groups belong to the bigger group VPN Users Location X, they will not be able to connect from another location.

Note that this method is not as efficient and secure as the one with firewall rules for incoming VPN remote access connections, as with that approach the connections were not allowed right from the start. In this case, for L2TP/IPsec, the IKE MM and QM negotiations take place, which means that a shared secret DH is computed, and 3DES keys for ESP encryption are derived(system overhead). Then PPP authentication take place. During this phase the RADIUS server will deny access(a failure message), thus after all these steps the connections will be denied. In case of PPTP, the TCP connection is started, some PPP LCP negotiations take place(GRE encapsulated packets), and again during the PPP authentication phase, the RADIUS server will deny access(a failure message).

With the firewall approach the first IKE message from the client used to "start" the L2TP/IPsec connection was denied, respectively the first TCP SYN packet from the client used to "start" the PPTP connection was denied. Unfortunetely we can't apply the firewall approach for this situation.

Let's make some quick tests, connecting with user adrian, a member of the VPN Users Location X Active Directory group. I will connect from an unallowed location, and the IAS will not grant access, note the wrong Calling-Station-Identifier from **Figure60**.

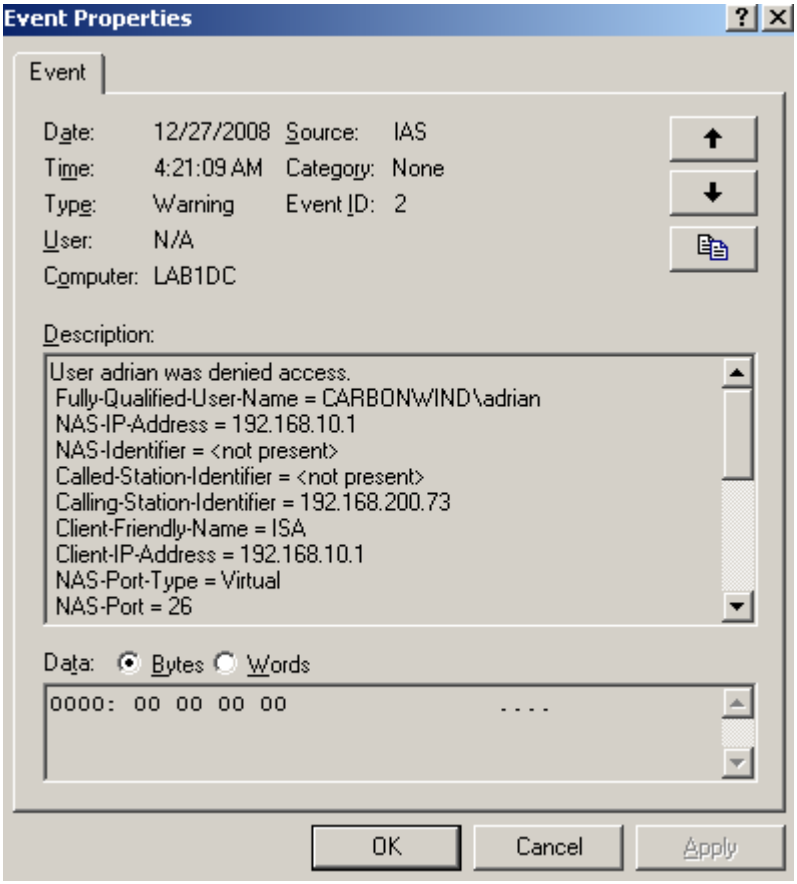


Figure60: IAS - Denied Access

If I will connect with the same user, from an allowed location, IAS will grant access, see the correct Calling-Station-Identifier from **Figure61**.

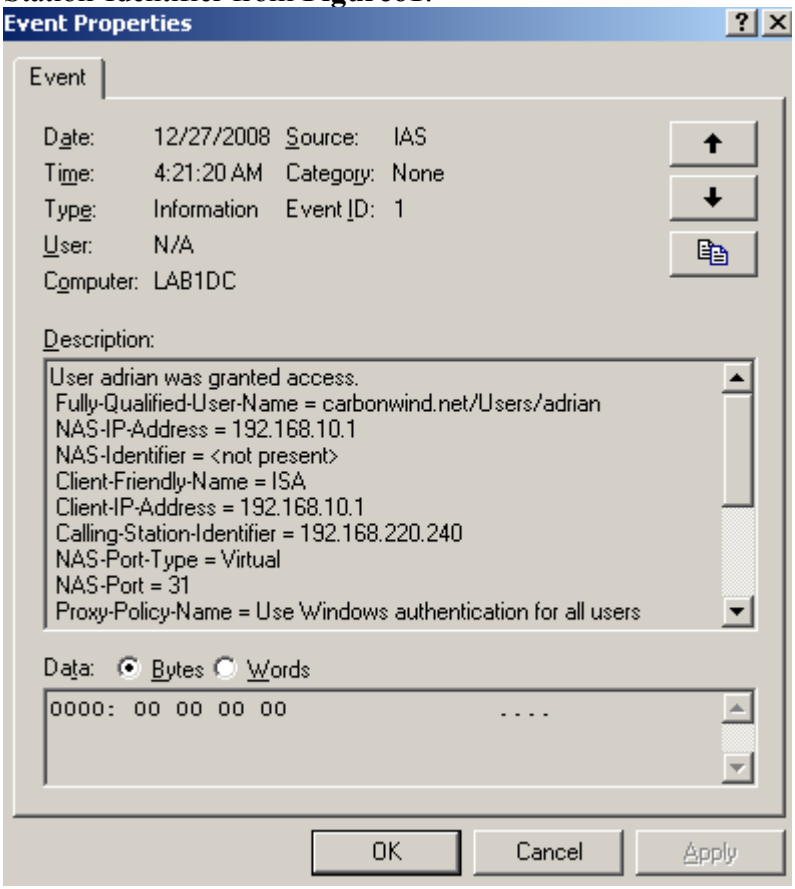


Figure61: IAS - Allowed Access

7. How do I disable DES and Diffie-Hellman 768-bit MODP group 1 for L2TP/IPsec on the ISA VPN server ?

So you may have had a pen test over your VPN server(ISA 2006 SE) and they came up saying that DH 768-bit MODP Group 1 and DES are enabled for IKE MM(that's a pretty standard check). You've been assigned the task to shrink the IKE protection suites.

Unfortunetely there is no simple way to do this(not one that I'm aware of).

For example for SSL and TLS, Microsoft has published a list of registry values that you can use to manage the chiper suites for TLS and to disable for example SSL 2.0, please refer to How to Restrict the Use of Certain Cryptographic Algorithms and Protocols in Schannel.dll.
I'm not saying that this an easy way to to that(as you may want to do it from a GUI), but there is a solution.
And Jason Jones has done a full tutorial on this subject in respect with ISA, please refer to Hardening SSL Cipher Strength and SSL Protocol Support on ISA Servers.

I'm not, for the moment, aware of such similar document(s) specifying some reg values that can be used to enable or disable DES for IKE(for the default L2TP/IPsec Windows policy).
The good news are that for Vista and Windows 2008 L2TP/IPsec connections, DES and DH 768-bit MODP Group 1 are disabled by default.

So what are we going to do ?

First about what are they(pen testers) talking about ?

The default IPsec policy for L2TP is enabled on the VPN server(Windows 2003).

Let's analyze with netsh the available IKE MM protection suites, see **Figure62**.
The encryption and hash algorithms attributes determine which algorithm will be used for message encryption and authentication, that is to protect messages 5 and 6 of MM(when the two peers authenticate each other, providing identity protection), the QM messages and any IKE Informational messages sent after IKE MM was established.
The DH group attribute specifies which DH group will be used for deriving a shared secret from which keys for the symmetric encryption algorithm(like 3DES) will be derived. 3DES will be used to encrypt the above mentioned messages. Also, if PFS is not enabled, the MM DH shared secret will be used to derive keys for the symmetric encryption algorithm(like 3DES) used by IPsec ESP to provide confidentiality and integrity for our data. So the stronger the DH group, the "better", for example DH 2048-bit MODP Group 14 matches 3DES' strength, rated at 112-bits of security. As a comparison, AES with 128-bit keys has 128-bits of security, so we cannot derive keys at "full strength" using a DH MODP Group 14 for it.
Note that the hash function plays a role in the keys derivation process.

It looks that we need to disable the last two proposals from **Figure62** (I've enabled the DH 2048-bit MODP Group 14, please refer to KB 818043). The protection suites are processed from top to down, so the first one is preffered by the VPN server.

Note the Lifetime which specifies how long the IKE SA will last. There is no QM limit per IKE SA.

```
C:\>netsh ipsec dynamic show mmpolicy all

IKE MM Policy Name     : L2TP Main Mode Policy
IKE Soft SA Lifetime   : 28800 secs

Encryption  Integrity  DH    Lifetime (Kb:secs)  QM Limit Per MM
----------  ---------  ----  ------------------  ---------------
 3DES        SHA1      2048       0:28800          0
 3DES        SHA1      2          0:28800          0
 3DES        MD5       2          0:28800          0
 DES         SHA1      1          0:28800          0
 DES         MD5       1          0:28800          0

C:\>
```

Figure62: Default L2TP Main Mode Policy

As said above, the IKE SA will be used to protect the IKE QM negotiations.
IKE QM is used to generate IPsec SAs, in our case we need to use ESP Transport Mode for protecting the L2TP tunnel, ESP will provide both confidentiality and integrity.
As seen from **Figure63**, the default policy contains multiple protection suites. We don't need AH, as AH is incompatible with NAT devices(behind which typically VPN clients connect), and, as just said, ESP will provide both confidentiality and integrity.
For the best security we can afford, we will use ESP, 3DES as the symmetric encryption algorithm and SHA-1 as the hash function. We cannot enable PFS for session keys(as you see it is disabled by default) because the Windows VPN clients do not use PFS by default, if we do so we will endup being unable to complete the QM negotiations. PFS for session keys enhances the security, because a new DH shared secret is derived with each QM negotiation, so our data will be protected with keys derived from this new shared secret.
It's a good idea to disable DES here. The protection suites are processed from top to down, so the first one is preffered by the VPN server, we're going to change the prefered one, as I want to use SHA-1 instead of MD5.

Note the Lifetime which specifies how long the IPsec SA will last.

```
C:\>netsh ipsec dynamic show qmpolicy all

QM Negotiation Policy Name : L2TP Optional Encryption Quick Mode Policy

    Security Methods       Lifetime (Kb:secs)   PFS DH Group
-----------------------  --------------------  ------------
 ESP[3DES,MD5]               250000:3600        <Unassigned>
 ESP[3DES,SHA1]              250000:3600        <Unassigned>
 AH[SHA1]+ ESP[3DES,NONE]    250000:3600        <Unassigned>
 AH[MD5] + ESP[3DES,NONE]    250000:3600        <Unassigned>
 AH[SHA1]+ ESP[3DES,SHA1]    250000:3600        <Unassigned>
 AH[MD5] + ESP[3DES,MD5]     250000:3600        <Unassigned>
 ESP[ DES,MD5]               250000:3600        <Unassigned>
 ESP[ DES,SHA1]              250000:3600        <Unassigned>
 AH[SHA1]+ ESP[ DES,NONE]    250000:3600        <Unassigned>
 AH[MD5] + ESP[ DES,NONE]    250000:3600        <Unassigned>
 AH[SHA1]+ ESP[ DES,SHA1]    250000:3600        <Unassigned>
 AH[MD5] + ESP[ DES,MD5]     250000:3600        <Unassigned>
 ESP[NONE,SHA1]              250000:3600        <Unassigned>
 ESP[NONE,MD5]               250000:3600        <Unassigned>
 AH[SHA1]                    250000:3600        <Unassigned>
 AH[MD5]                     250000:3600        <Unassigned>
```

Figure63: Default L2TP Quick Mode Policy

We're not done yet, not at all. For IKE MM we need to specify an authentication method, pre-shared keys and/or certificates authentication(RSA digital signatures).
From **Figure64**(showing generic filters), we can see that this ISA is using both of them(I've added on ISA a certificate that can be used for IKE authentication from an Enterprise CA).
Also, there are some MM filters that specify from/to which sources/destinations ISA will accept/start IKE negotiations using the specified authentication methods and protection suites.

There is an inbound filter, ISA being a VPN server and an answering gateway(accepting IKE negotiation from any source, as the location of the VPN clients is unknown in advanced, as they are mobile users), and an outbound filter, ISA can act as a calling gateway. ISA's IP address is not specifically configured, as you may enable the VPN server on multiple interfaces(say External and a anonynmous wireless DMZ).
So it looks like a general sort of policy. We don't need to touch these filters.

```
C:\>netsh ipsec dynamic show mmfilter all

Main Mode Filters: Generic

-------------------------------------------------------------

Filter name             : L2TP Server Inbound Filter
Connection Type         : ALL
Source Address          : <Any IP Address>  (0.0.0.0        )
Destination Address     : <My IP Address>   (255.255.255.255)
Authentication Methods  :
        Root CA         : DC=net, DC=carbonwind, CN=Lab1CA
          Exclude CA name     : NO

        Preshared key
Security Methods        : 5
        3DES/SHA1/DH3/28800/QMlimit=0
        3DES/SHA1/DH2/28800/QMlimit=0
        3DES/MD5/DH2/28800/QMlimit=0
        DES/SHA1/DH1/28800/QMlimit=0
        DES/MD5/DH1/28800/QMlimit=0

-------------------------------------------------------------

Filter name             : L2TP Server Outbound Filter
Connection Type         : ALL
Source Address          : <My IP Address>   (255.255.255.255)
Destination Address     : <Any IP Address>  (0.0.0.0        )
Authentication Methods  :
        Root CA         : DC=net, DC=carbonwind, CN=Lab1CA
          Exclude CA name     : NO

        Preshared key
Security Methods        : 5
        3DES/SHA1/DH3/28800/QMlimit=0
        3DES/SHA1/DH2/28800/QMlimit=0
        3DES/MD5/DH2/28800/QMlimit=0
        DES/SHA1/DH1/28800/QMlimit=0
        DES/MD5/DH1/28800/QMlimit=0

2 Generic Filter(s)
```

Figure64: Default L2TP Main Mode Filters

And very very important, we need to closely take a look at the QM filters, see **Figure65**(showing generic filters).
These filters say which traffic, from which source and destination needs to be protected.
We need to protect the L2TP tunnel, an UDP based implementation. L2TP uses UDP port 1701. However, this aspect may vary, as specified in RFC 3193 (see 4.2. IKE Phase 2 Negotiations section). Also this is very important from a compatibility point of view with various VPN clients, which may be kinda' restrictive.
We don't need to touch these filters.

```
C:\>netsh ipsec dynamic show qmfilter all

Quick Mode Filters(Transport): Generic

-------------------------------------------------------------------

Filter name             : L2TP Server Filter1
Connection Type         : ALL
Source Address          : <Any IP Address>  (0.0.0.0        )
Destination Address     : <My IP Address>   (255.255.255.255)
Protocol                : UDP     Src Port: 0      Dest Port: 1701
Mirrored                : yes
Quick Mode Policy       : L2TP Optional Encryption Quick Mode Policy
Inbound Action          : Negotiate
Outbound Action         : Negotiate

-------------------------------------------------------------------

Filter name             : L2TP Server Inbound Filter
Connection Type         : ALL
Source Address          : <Any IP Address>  (0.0.0.0        )
Destination Address     : <My IP Address>   (255.255.255.255)
Protocol                : UDP     Src Port: 1701   Dest Port: 1701
Mirrored                : no
Quick Mode Policy       : L2TP Optional Encryption Quick Mode Policy
Inbound Action          : Negotiate
Outbound Action         : Negotiate

-------------------------------------------------------------------

Filter name             : L2TP Server Inbound Filter
Connection Type         : ALL
Source Address          : <Any IP Address>  (0.0.0.0        )
Destination Address     : <My IP Address>   (255.255.255.255)
Protocol                : UDP     Src Port: 1701   Dest Port: 0
Mirrored                : no
Quick Mode Policy       : L2TP Optional Encryption Quick Mode Policy
Inbound Action          : Negotiate
Outbound Action         : Negotiate

-------------------------------------------------------------------

Filter name             : L2TP Server Outbound Filter
Connection Type         : ALL
Source Address          : <My IP Address>   (255.255.255.255)
Destination Address     : <Any IP Address>  (0.0.0.0        )
Protocol                : UDP     Src Port: 1701   Dest Port: 1701
Mirrored                : no
Quick Mode Policy       : L2TP Optional Encryption Quick Mode Policy
Inbound Action          : Negotiate
Outbound Action         : Negotiate

-------------------------------------------------------------------

Filter name             : L2TP Server Outbound Filter
Connection Type         : ALL
Source Address          : <My IP Address>   (255.255.255.255)
Destination Address     : <Any IP Address>  (0.0.0.0        )
Protocol                : UDP     Src Port: 0      Dest Port: 1701
Mirrored                : no
Quick Mode Policy       : L2TP Optional Encryption Quick Mode Policy
Inbound Action          : Negotiate
Outbound Action         : Negotiate

5 Generic Filter(s)
```

Figure65: Default L2TP Quick Mode Filters

So we need to edit some of these settings. We can use the netsh commands for this. However, our modifications will not stick, they will not be preserved through reboots for example. So we will endup with the default chipers. We might create a script to "keep an eye" on the protection suites, and "adjust" them. But this not quite "ideal", unless assuming you're good at scripting and you can accomplish this task.

Another way of doing this is to disable the default IPsec policy for L2TP and create our own IPsec policy to match the needed changes on the default policy. We know from above how the default policy looks like. We can disable the default IPsec policy used to protect the L2TP tunnels by setting the ProhibitIpSec registry value set to 1. After we do that and reboot ISA, the L2TP tunnels will be established in clear, that is, not

protected by IPsec. You may want to make sure the VPN server is unreacheable from the external network untill you create, enable and test the custom IPsec policy.

So let's proceed(before you may like to read Microsoft's KB 240262 How to configure an L2TP/IPSec connection by using Preshared Key Authentication and maybe this old doc Description of the IPSec policy created for L2TP/IPSec).

Do it enterly on your own risk and pleasure(I don't know what's Microsoft position on doing this on the ISA Server).

Note that this is a very sensible aspect, if you do not configure correctly the custom IPsec policy, in the best case you will block the creating of L2TP/IPsec connections or block other traffic, while in the worst case you will create security breaches by lefting certain traffic unprotected. You will need to double check and double test your final custom IPsec policy.

I've disabled the default IPsec policy used to protect the L2TP tunnels.

From the **Administrative Tools** menu, launch the **Local Security Policy** tool.
Right-click **IP Security Policies on Local Machine**, click **Create IP Security Policy**, see **Figure66**.

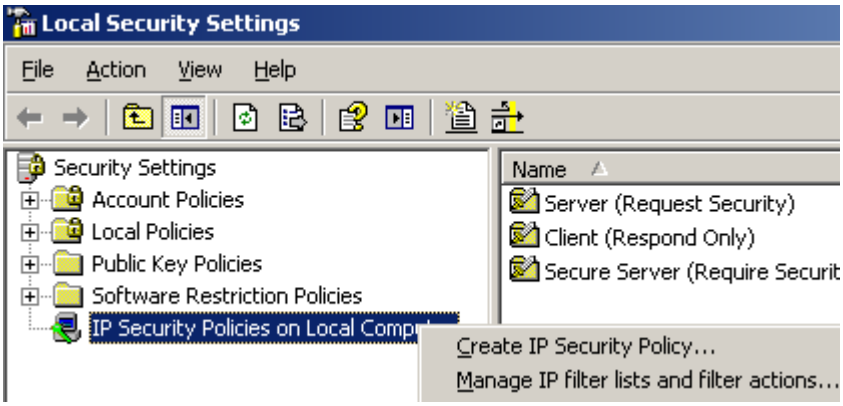


Figure66: Create A New IP Security Policy

Click **Next** on the welcome screen, see **Figure67**.

Figure67: IP Security Policy Wizard - Welcome

Enter a suggestive name on the **IP Security Policy Name** window and click **Next**, see **Figure68**.

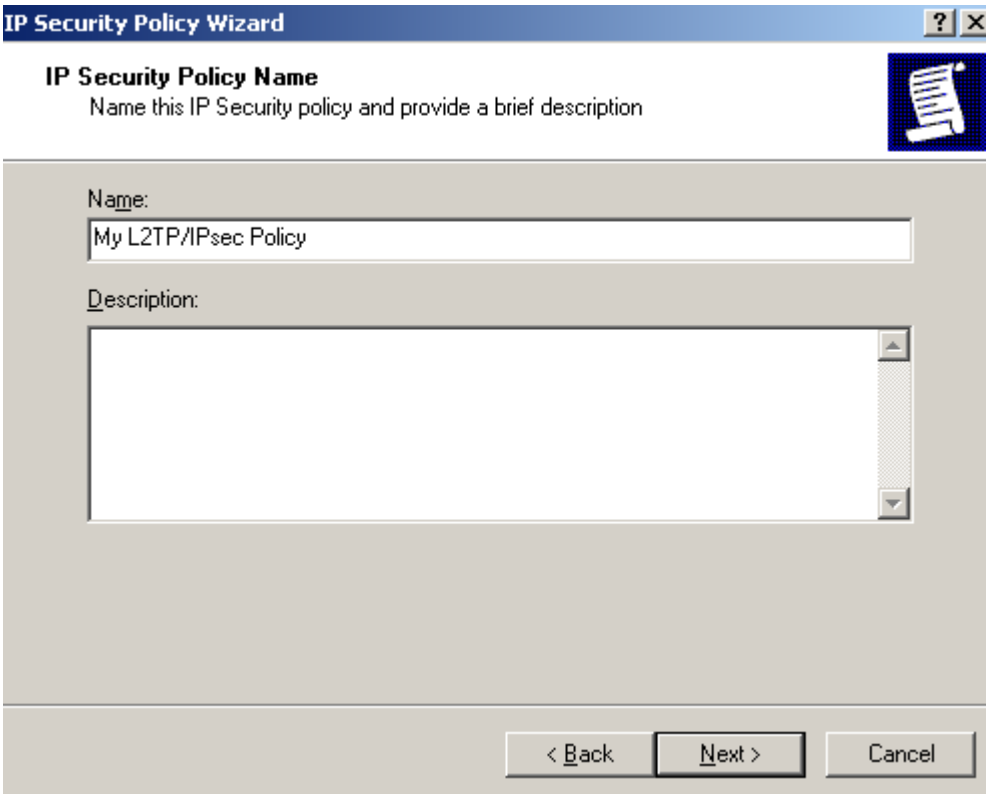


Figure68: IP Security Policy Wizard - Policy Name

On the **Requests for Secure Communication** window, clear the **Activate the default response rule** checkbox and click **Next**, see **Figure69**.

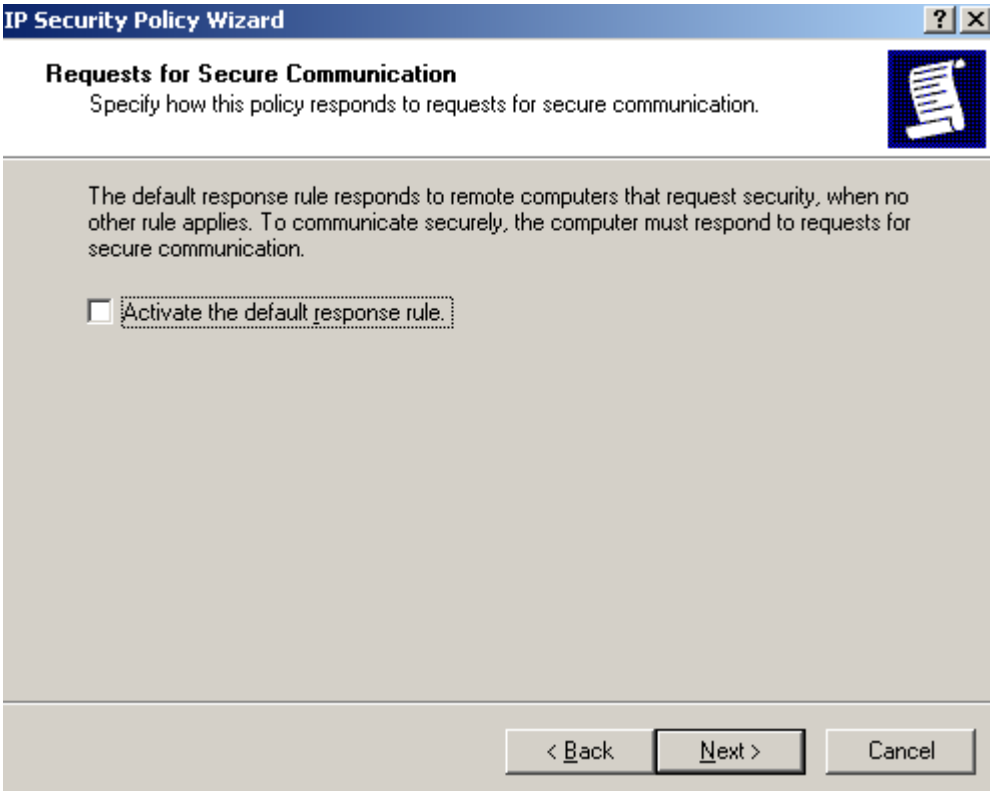


Figure69: IP Security Policy Wizard - Requests for Secure Communication

Make sure the **Edit Properties** checkbox is selected on the **Completing the IP Security Policy Wizard** window and click **Finish**, see **Figure70**.

Figure70: IP Security Policy Wizard - Completing the IP Security Policy Wizard

On the new window click **Add** on the **Rules** tab, see **Figure71**. Do not check the **Use Add Wizard** checkbox.

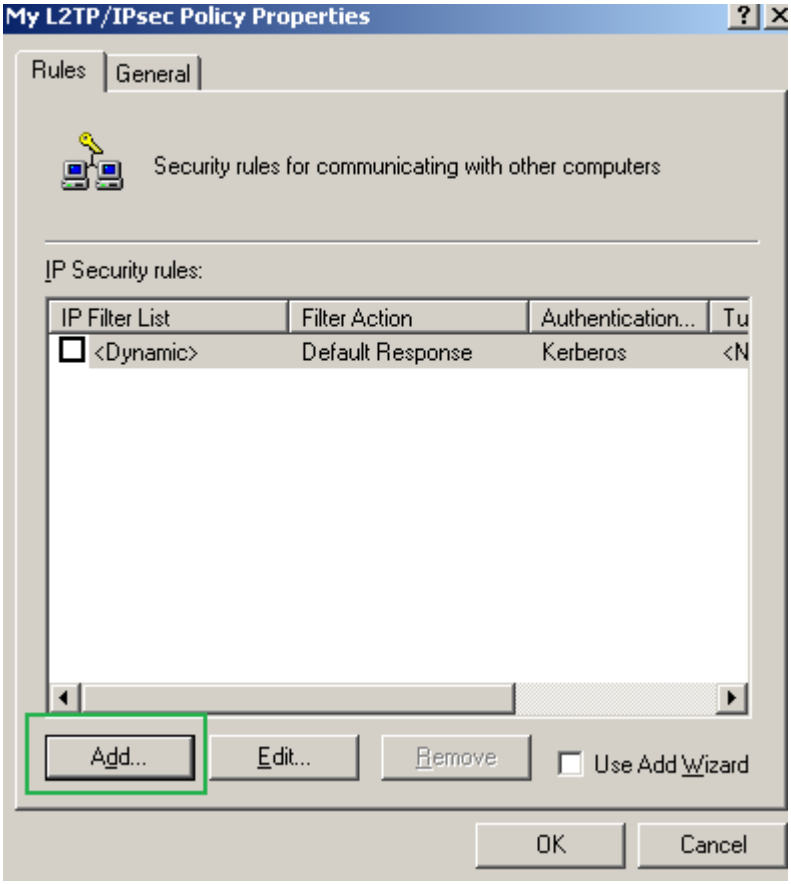


Figure71: Edit My L2TP/IPsec Policy - Add an IP Security Rule

On the **New Rule Properties** window, on the **IP Filter List** tab, click **Add**, see **Figure72**.

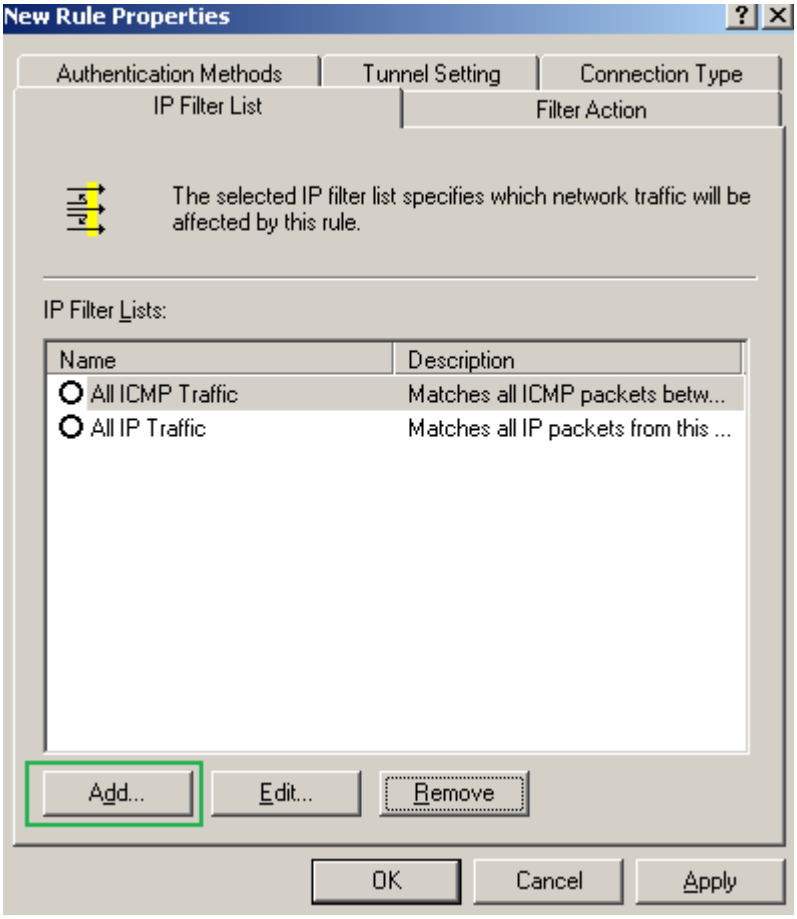


Figure72: Edit My L2TP/IPsec Policy - New Rule Properties: IP Filter tab - Add An IP Filter List

Enter a suggestive name for this **IP Filter List** and click **Add**, see **Figure73**. Now we will add one by one the QM filters that will dictate what traffic needs to be protected by IPsec, remember from **Figure65** that there were five of them. Do not check the **Use Add Wizard** checkbox.

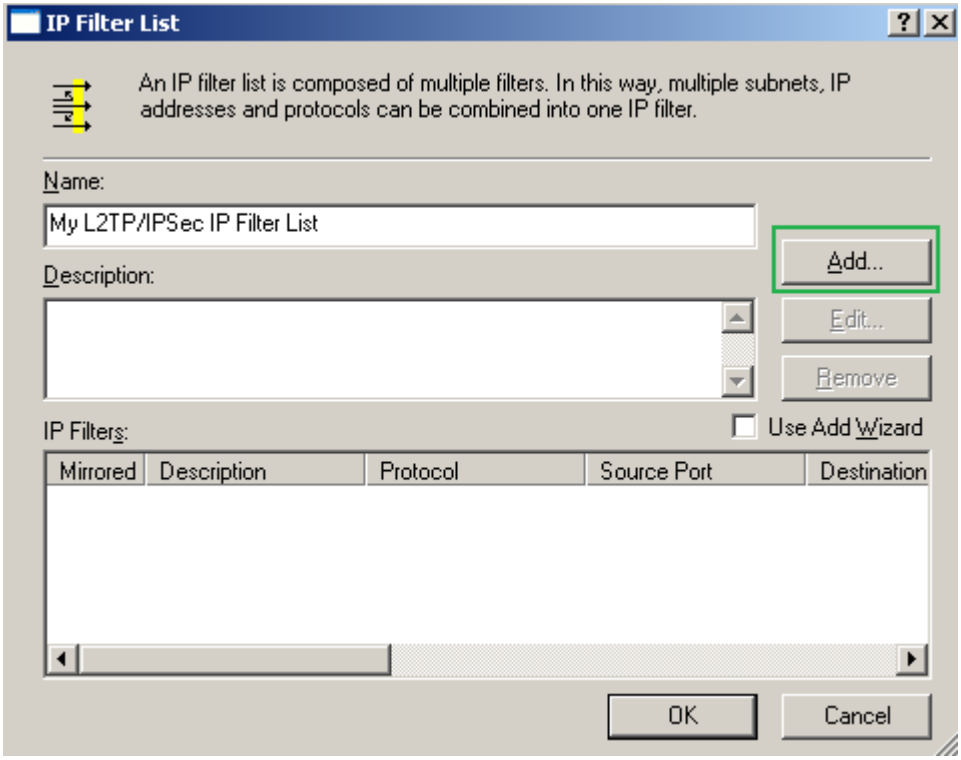


Figure73: Edit My L2TP/IPsec Policy - Add My L2TP/IPsec IP Filter List

To get the filters in the order listed by the netsh command in **Figure65**, we will start adding the last filter from that printscreen, giving it a suggestive description, see **Figure74**(**Addresses** tab), **Figure75**(**Protocol** tab) and **Figure76**(**Description** tab).
Leave in the **Addresses** tab, as ISA's address the "My IP Address" option, just as in the default policy, as if you have multiple IP addresses on ISA's external NIC or enable the VPN server on multiple interfaces you might get into troubles if you only specify one IP address, that is, only L2TP traffic to and from this IP address will be protected by IPsec(unless you firewall the other IP addresses by the trick described before in this article to drop unwanted packets).

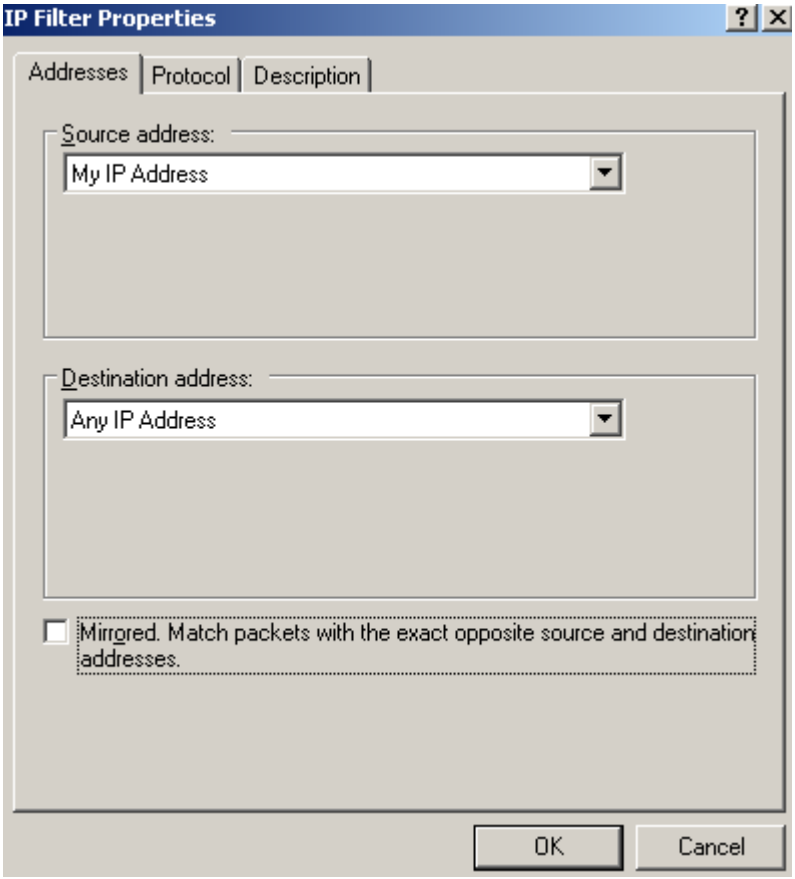


Figure74: Edit My L2TP/IPsec Policy - Add the first My L2TP Server Outbound Filter: Addresses

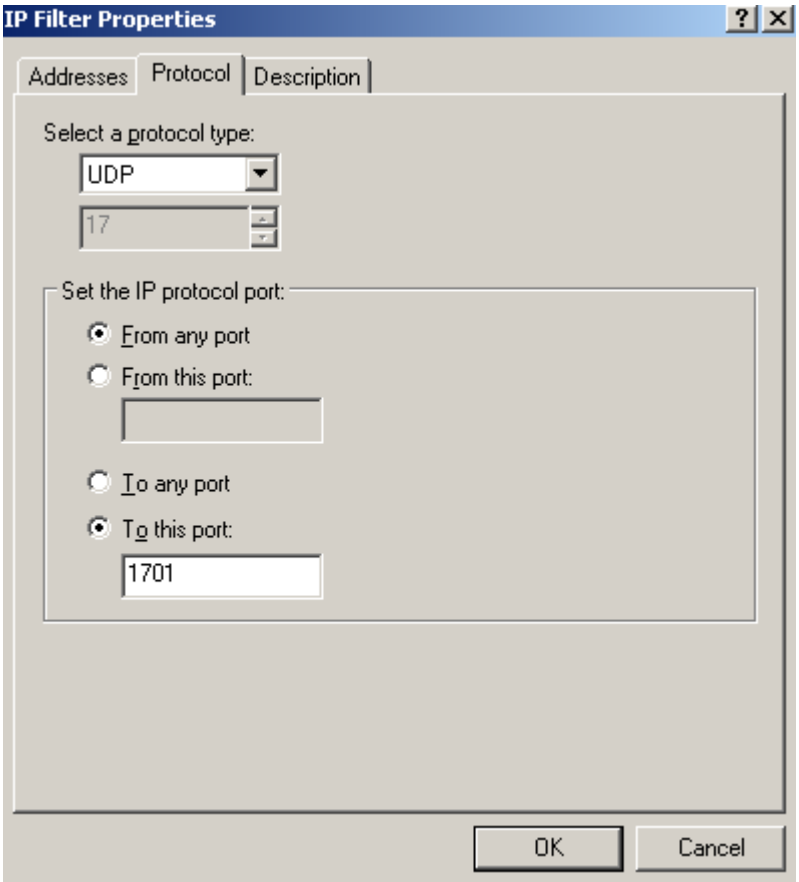


Figure75: Edit My L2TP/IPsec Policy - Add the first My L2TP Server Outbound Filter: Protocol

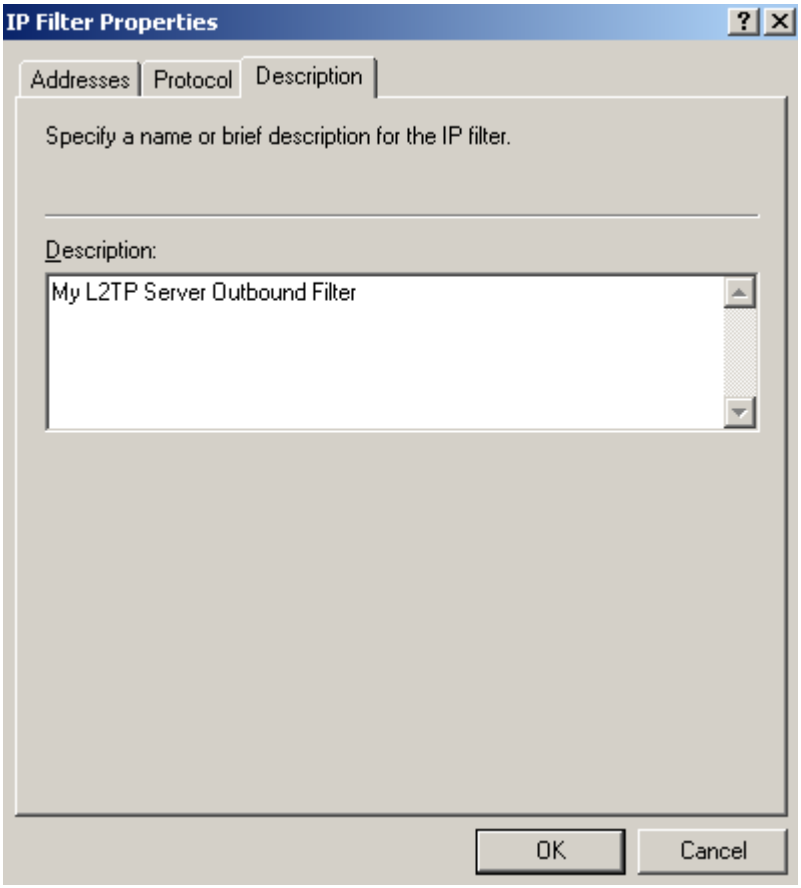


Figure76: Edit My L2TP/IPsec Policy - Add the first My L2TP Server Outbound Filter: Description

Add the second filter from down to top from **Figure65**, see **Figure77**(**Addresses** tab), **Figure78**(**Protocol** tab) and **Figure79**(**Description** tab).

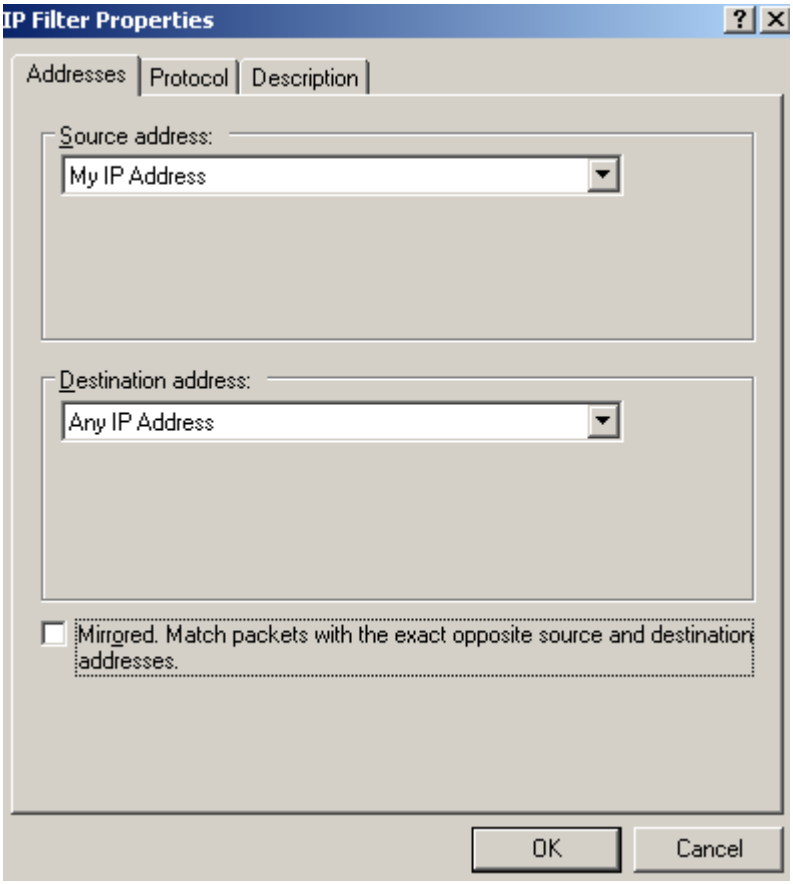


Figure77: Edit My L2TP/IPsec Policy - Add the second My L2TP Server Outbound Filter: Addresses

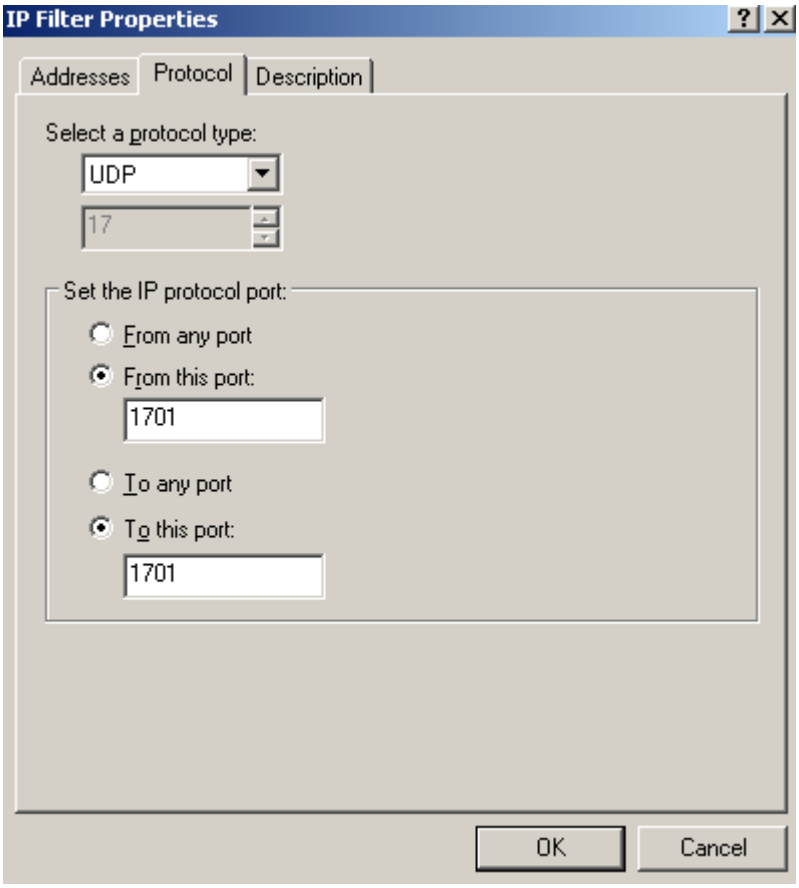


Figure78: Edit My L2TP/IPsec Policy - Add the second My L2TP Server Outbound Filter: Protocol

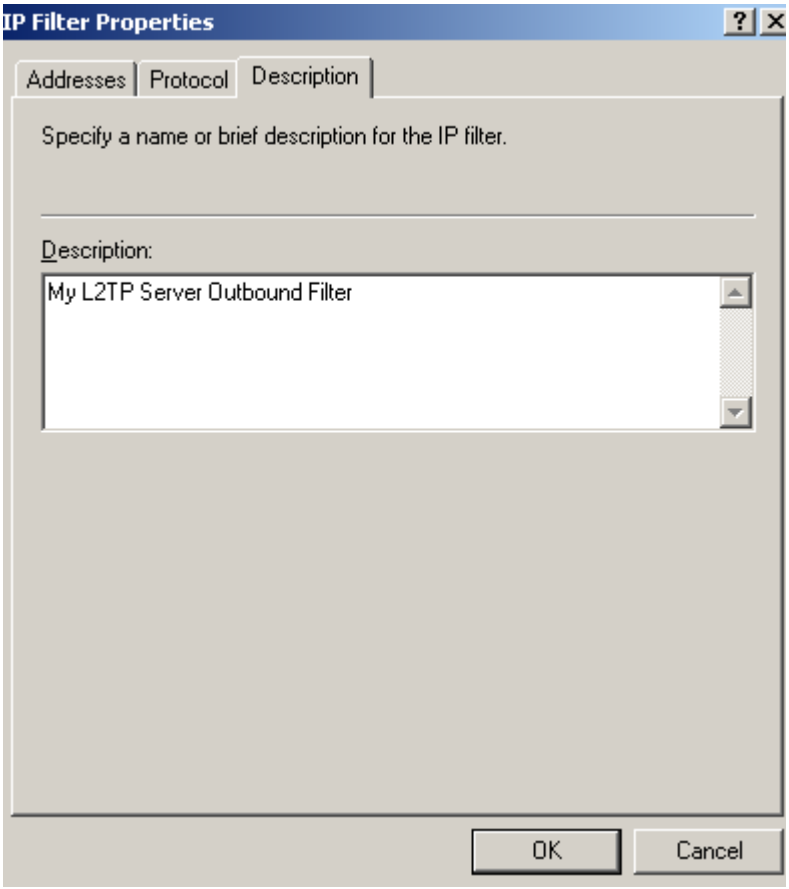


Figure79: Edit My L2TP/IPsec Policy - Add the second My L2TP Server Outbound Filter: Description

Add the third filter from down to top from **Figure65**, see **Figure80**(**Addresses** tab), **Figure81**(**Protocol** tab) and **Figure82**(**Description** tab).

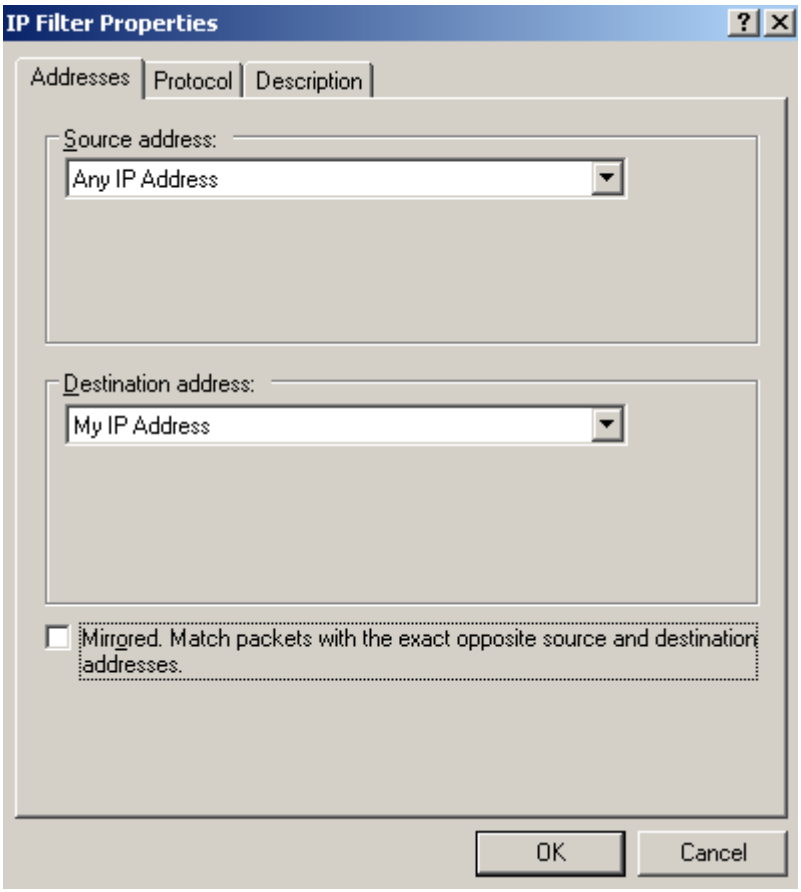


Figure80: Edit My L2TP/IPsec Policy - Add the first My L2TP Server Inbound Filter: Addresses

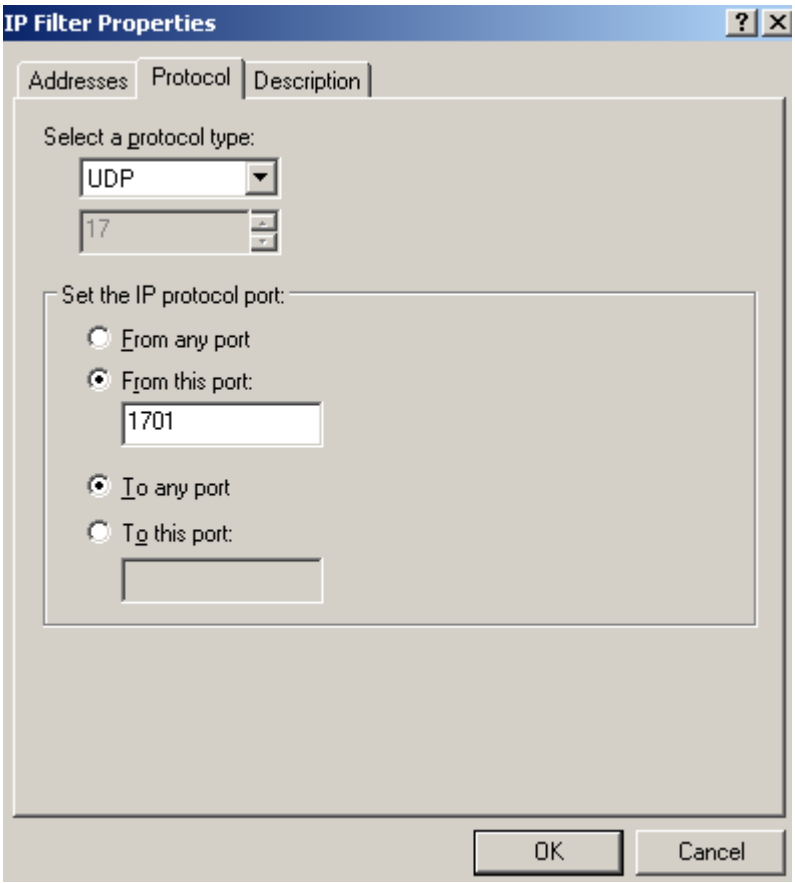


Figure81: Edit My L2TP/IPsec Policy - Add the first My L2TP Server Inbound Filter: Protocol

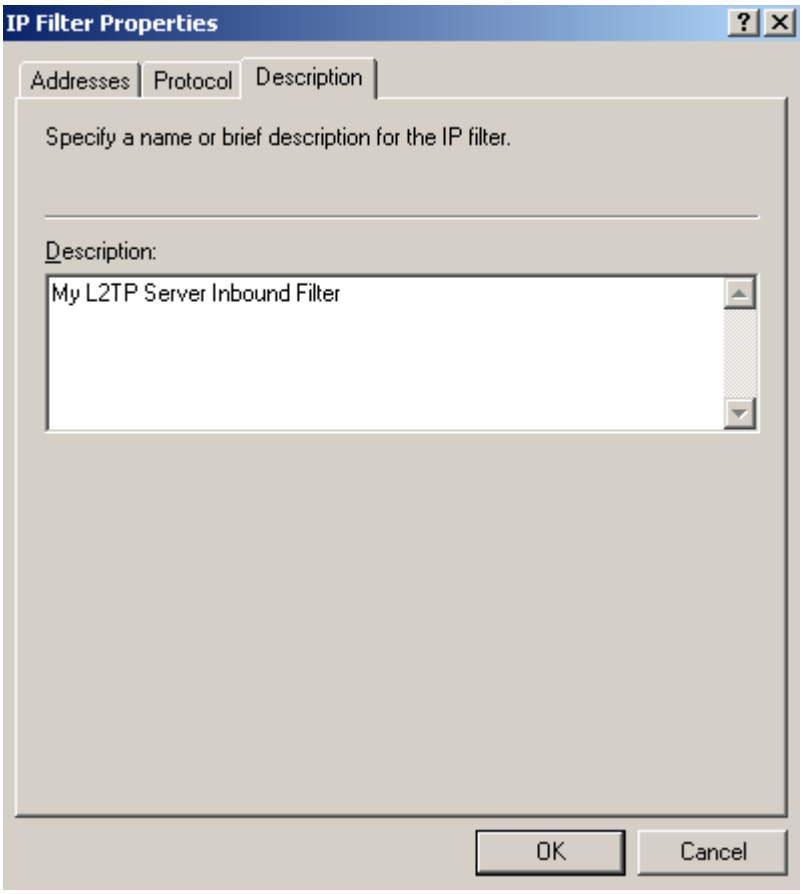


Figure82: Edit My L2TP/IPsec Policy - Add the first My L2TP Server Inbound Filter: Description

Add the fourth filter from down to top from **Figure65**, see **Figure83**(**Addresses** tab), **Figure84**(**Protocol** tab) and **Figure85**(**Description** tab).

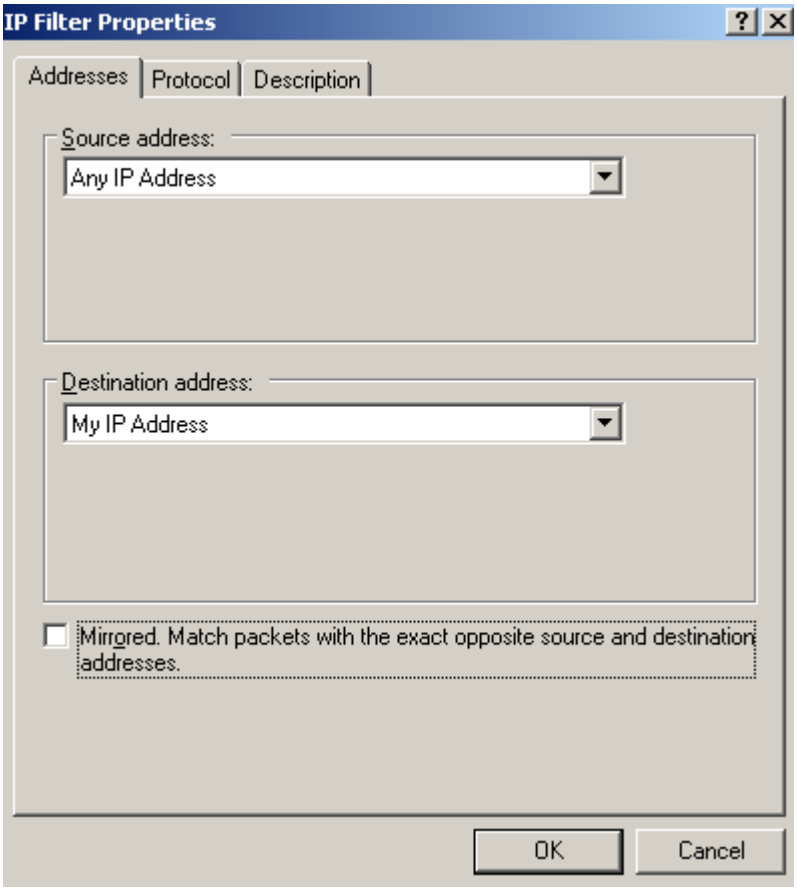


Figure83: Edit My L2TP/IPsec Policy - Add the second My L2TP Server Inbound Filter: Addresses

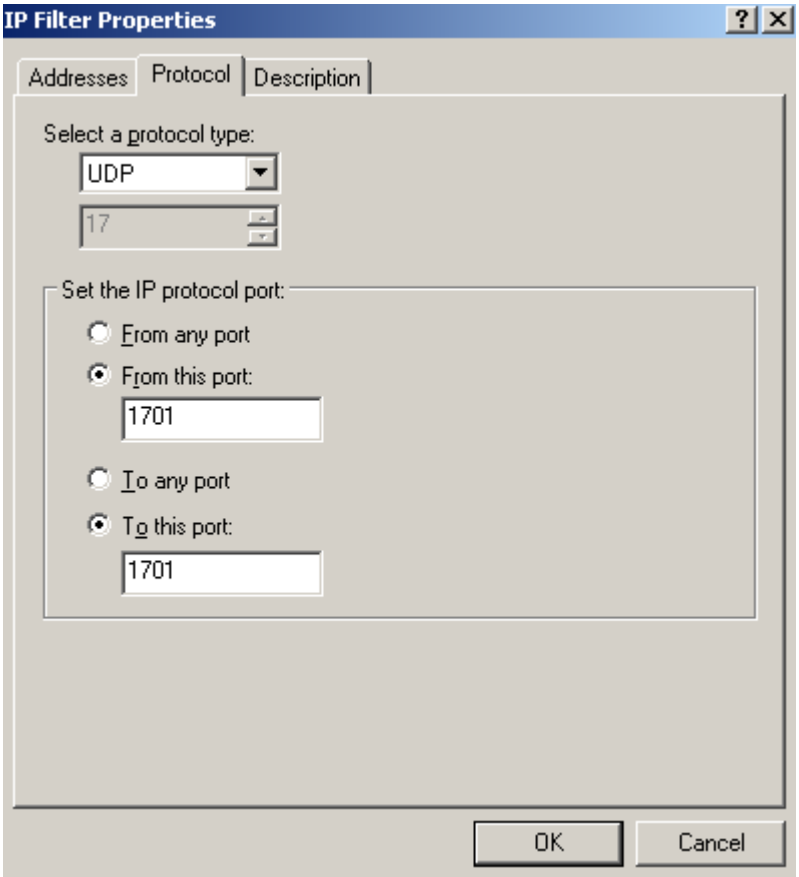


Figure84: Edit My L2TP/IPsec Policy - Add the second My L2TP Server Inbound Filter: Protocol

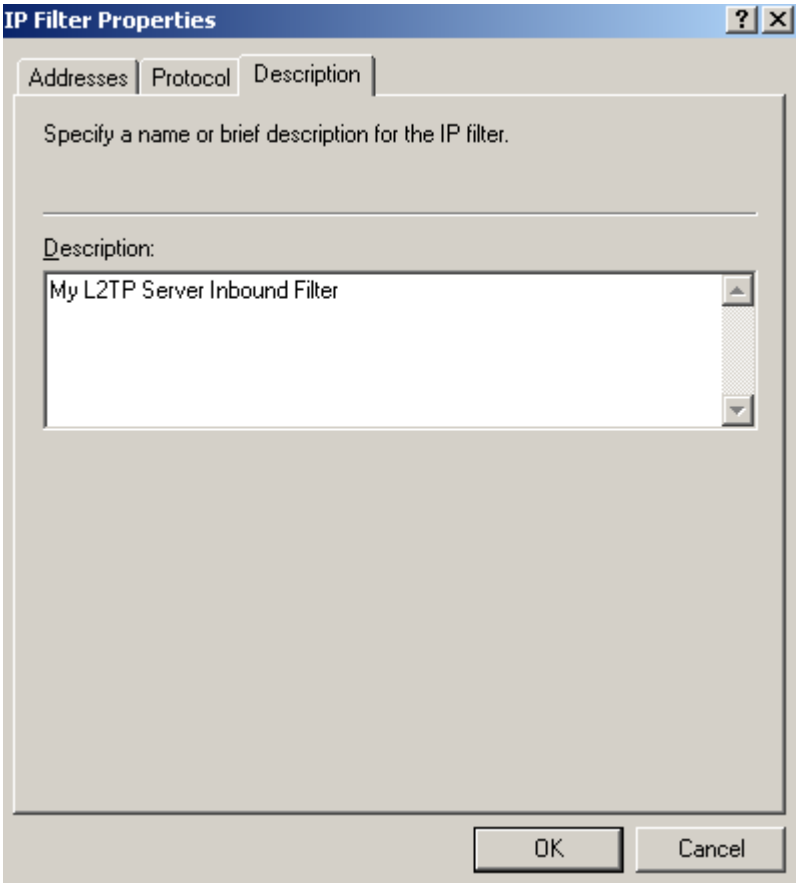


Figure85: Edit My L2TP/IPsec Policy - Add the second My L2TP Server Inbound Filter: Description

Add the last filter from down to top from **Figure65**, see **Figure86**(**Addresses** tab), **Figure87**(**Protocol** tab) and **Figure88**(**Description** tab).

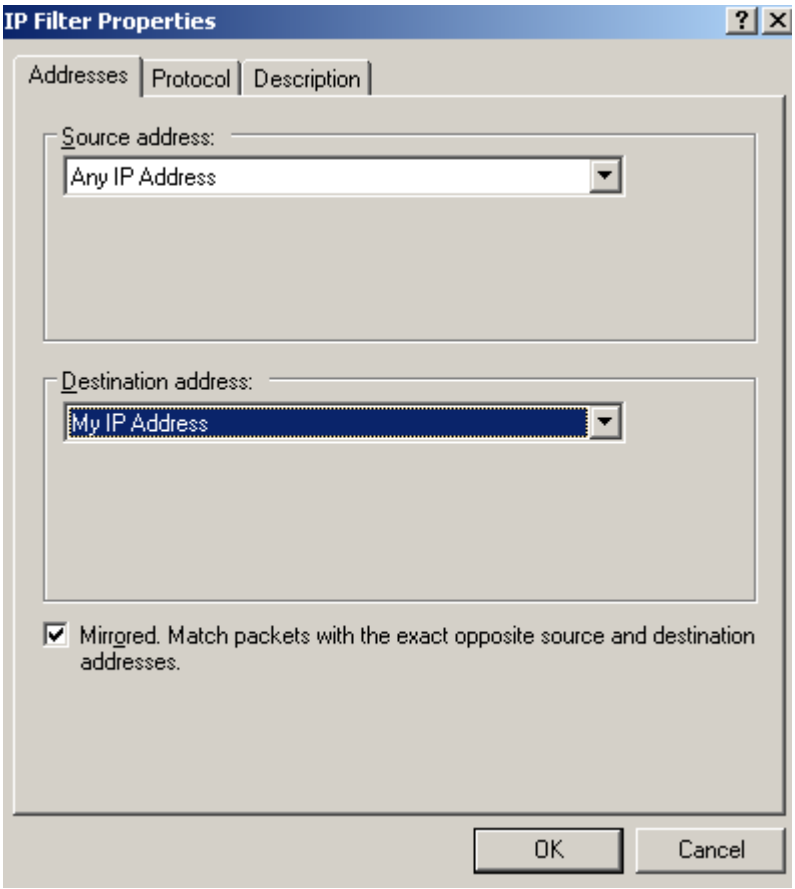


Figure86: Edit My L2TP/IPsec Policy - Add the My L2TP Server Filter1: Addresses

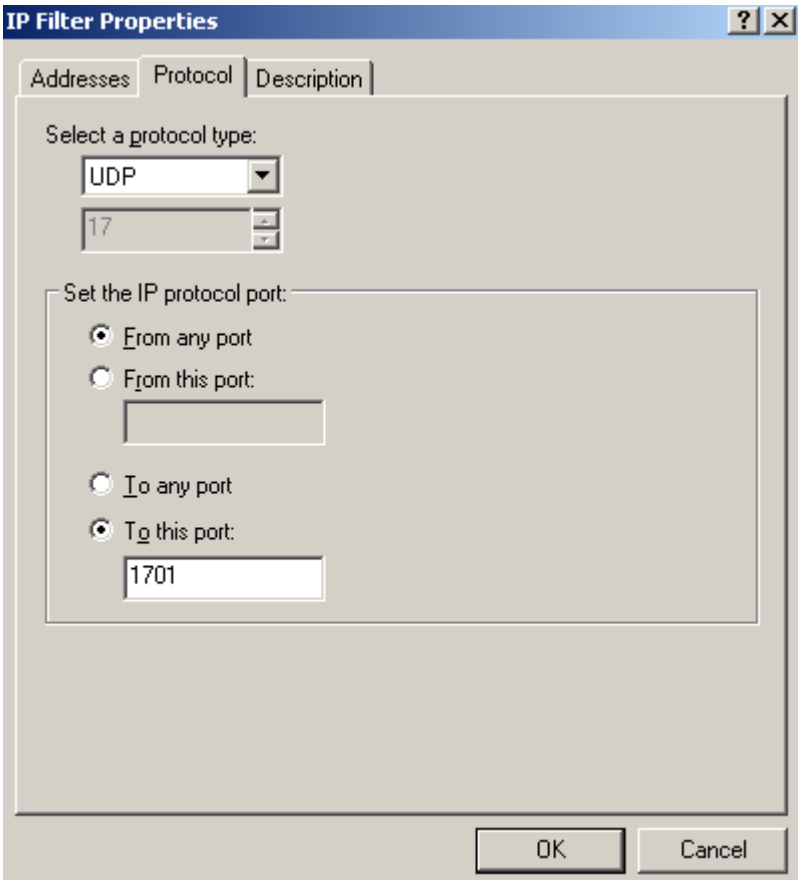


Figure87: Edit My L2TP/IPsec Policy - Add the My L2TP Server Filter1: Protocol

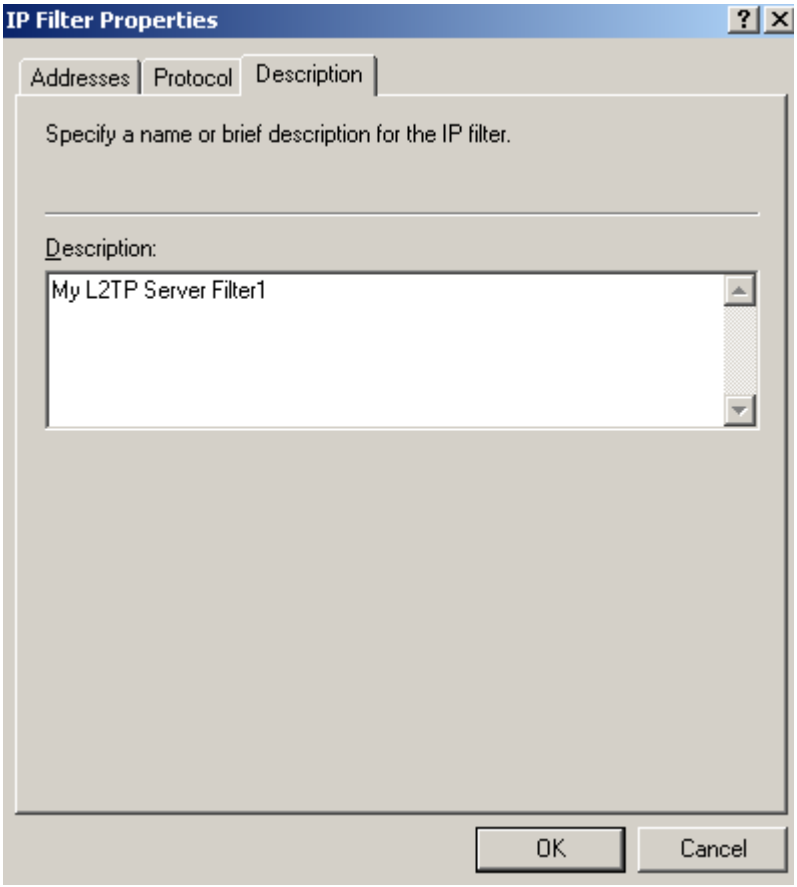


Figure88: Edit My L2TP/IPsec Policy - Add the My L2TP Server Filter1: Description

So now we're done entering all the five filters, see **Figure89**. Click **OK** to close this window.

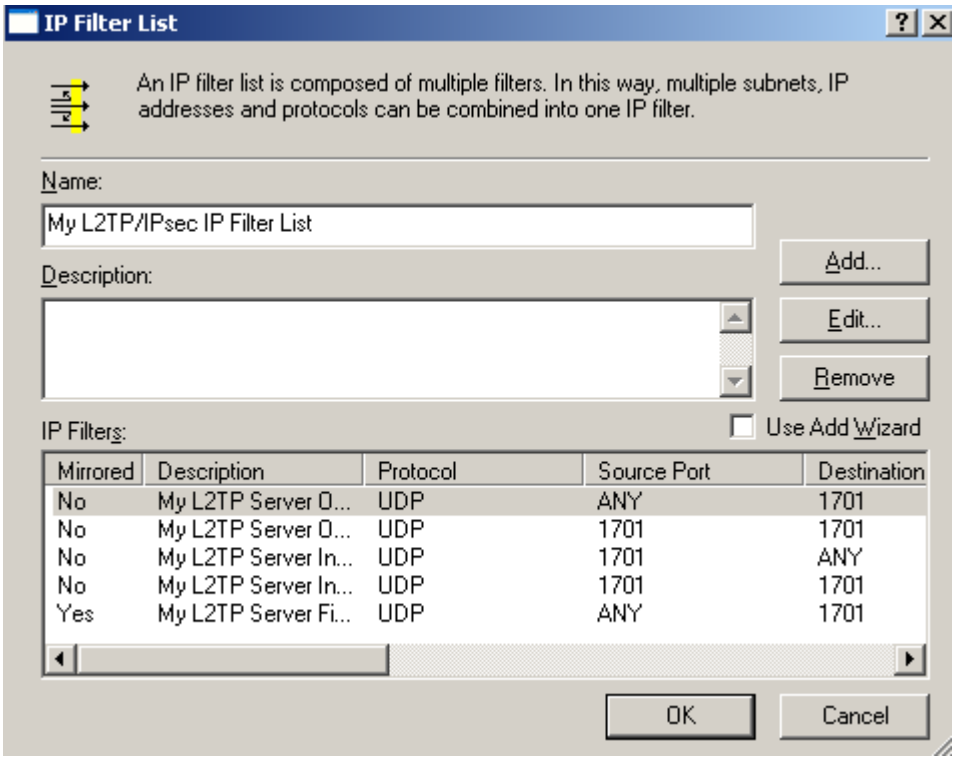


Figure89: Edit My L2TP/IPsec Policy - My L2TP/IPsec IP Filter List Completed

Coming back on the **New Rule Properties** window, on the **IP Filter List** tab, we will select our newly created custom IP Filter List, see **Figure90**.

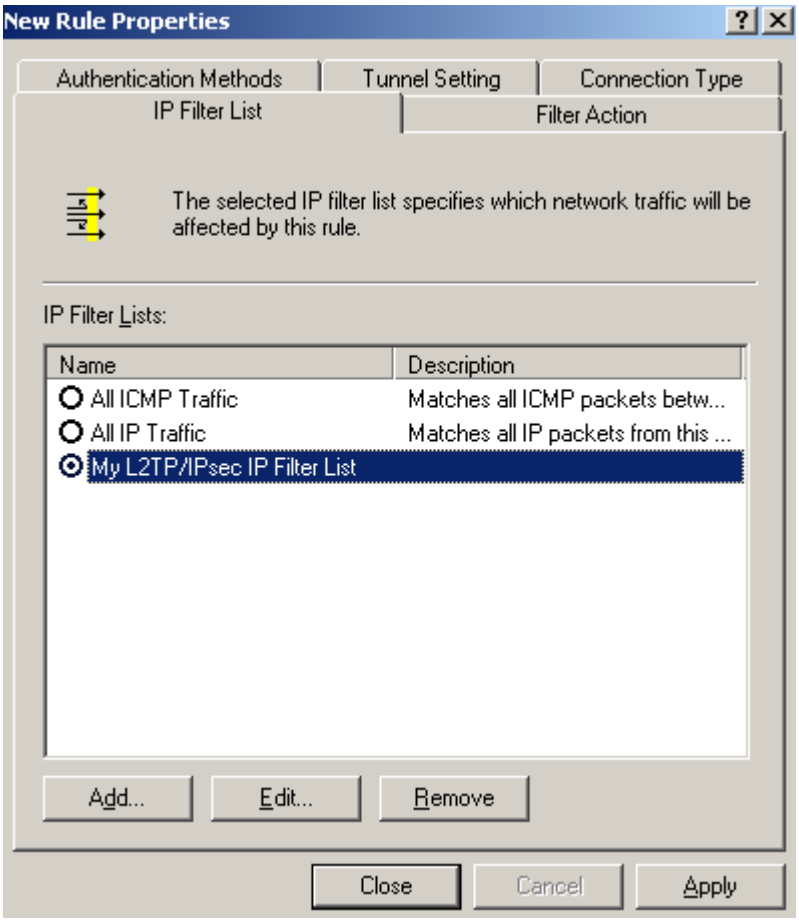


Figure90: Edit My L2TP/IPsec Policy - New Rule Properties: IP Filter List tab

On the **New Rule Properties** window, click the **Filter Action** tab, see **Figure91**. Click the **Add** buton, make sure the **Use Add Wizard** checkbox is not selected.

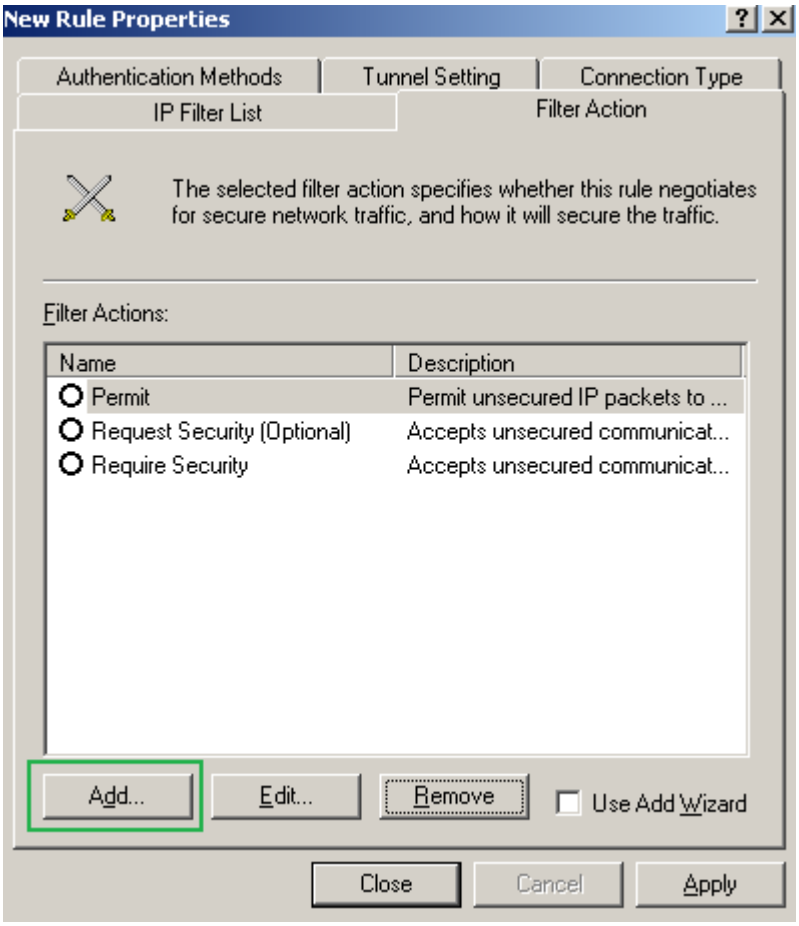


Figure91: Edit My L2TP/IPsec Policy - New Rule Properties: Filter Action tab

On the **New Filter Action Properties** window, on the **Security Methods** tab, select **Negotiate Security**, remove any **Security Methods**(if any) and click the **Add** button, see **Figure92**.

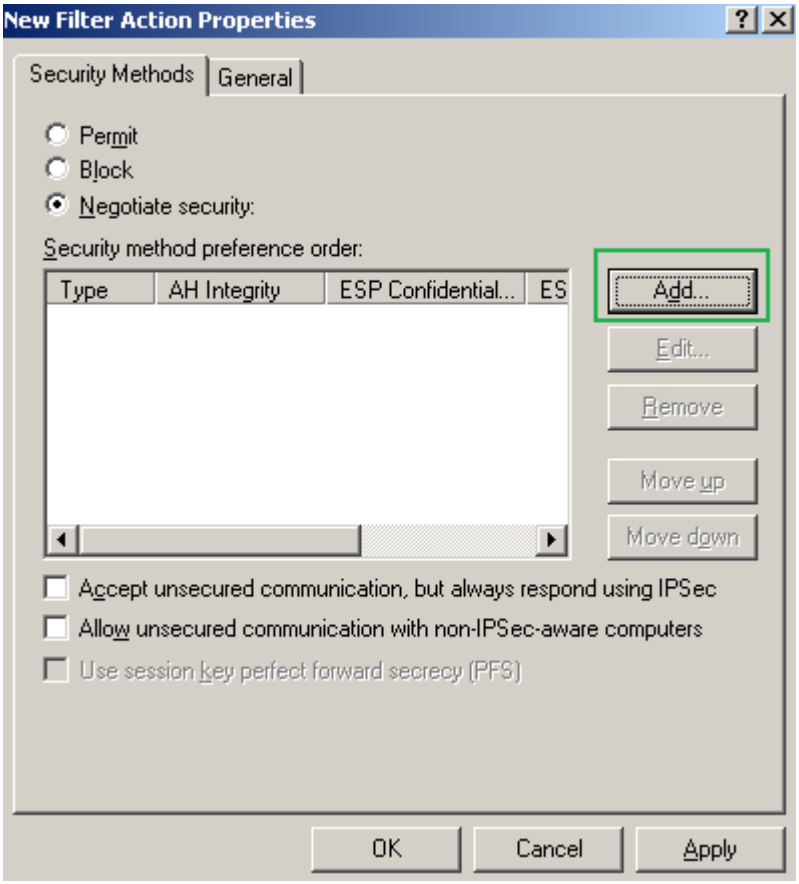


Figure92: Edit My L2TP/IPsec Policy - New Filter Action Properties: Security Methods tab

On the **New Security Method** window select **Custom** and click the **Settings**... button.
Put a checkmark into the **Data integrity and encryption(ESP)** checkbox -remember that we wanted this type of protection for our L2TP tunnels-, select SHA-1, 3DES.
In the **Session key settings** area, check the **Generate a new key every** checkboxes and enter **250000 Kbytes** and **3600 seconds**, see **Figure93**.

As you have noted we've defined the protection suite to be negotiated during IKE QM for our L2TP tunnels.
Click OK to add this custom security method.

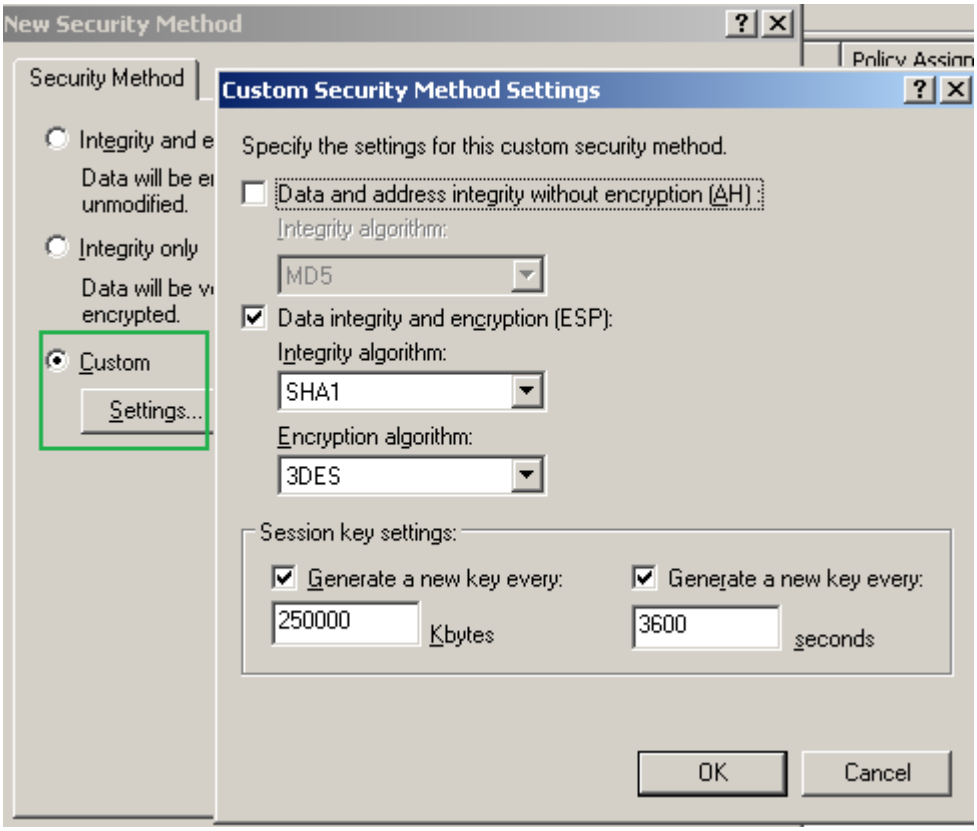


Figure93: Edit My L2TP/IPsec Policy - New Security Method: Add a Custom Security Method

On the **New Filter Action Properties** window, on the **Security Methods** tab we can see the custom security method we've added, **Figure94**. Leave unchecked the three checkboxes found in the lower section of the **New Filter Action Properties** window.

Note the PFS options for session keys. Remember, as tempted as may be, we cannot use this setting, as by default Windows VPN clients do not support it. Unless you define custom IPsec policies too on the VPN clients, do not check this checkbox.

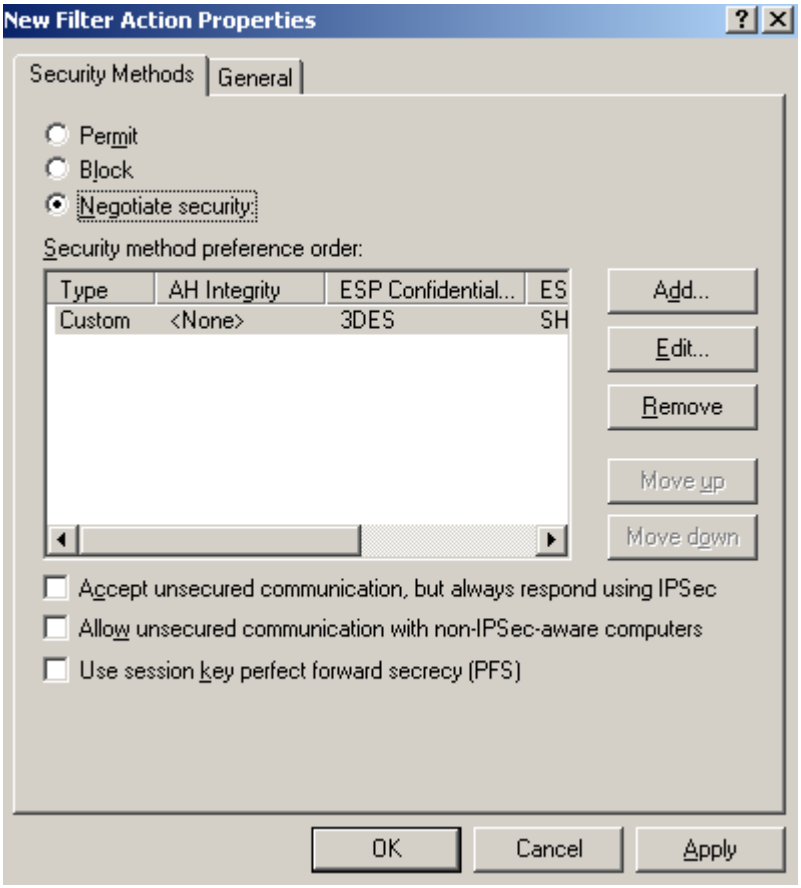


Figure94: Edit My L2TP/IPsec Policy - New Filter Action Properties: Security Methods tab - Added Custom Security Method

On the **New Filter Action Properties** window, click the **General Methods** tab and enter a suggestive name for the New Filter Action, see **Figure95**. Click **OK** to close the **New Filter Action Properties** window.

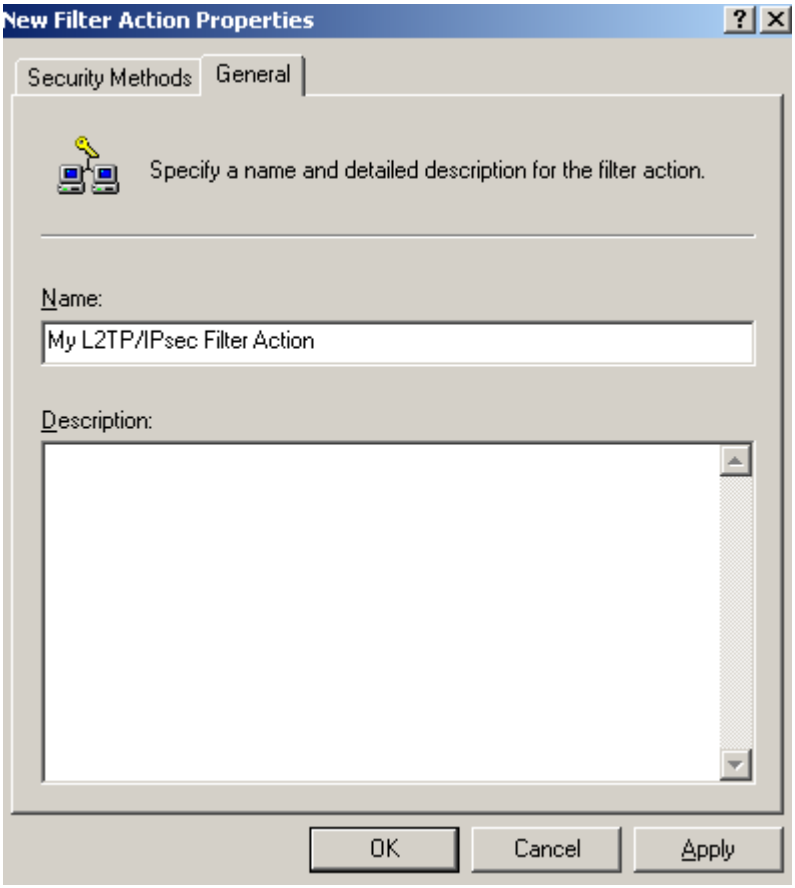


Figure95: Edit My L2TP/IPsec Policy - New Filter Action Properties: General tab - Enter A Name

On the **New Rule Properties** window, on the **New Filter Action** tab, select the newly created Filter Action, see **Figure96**.

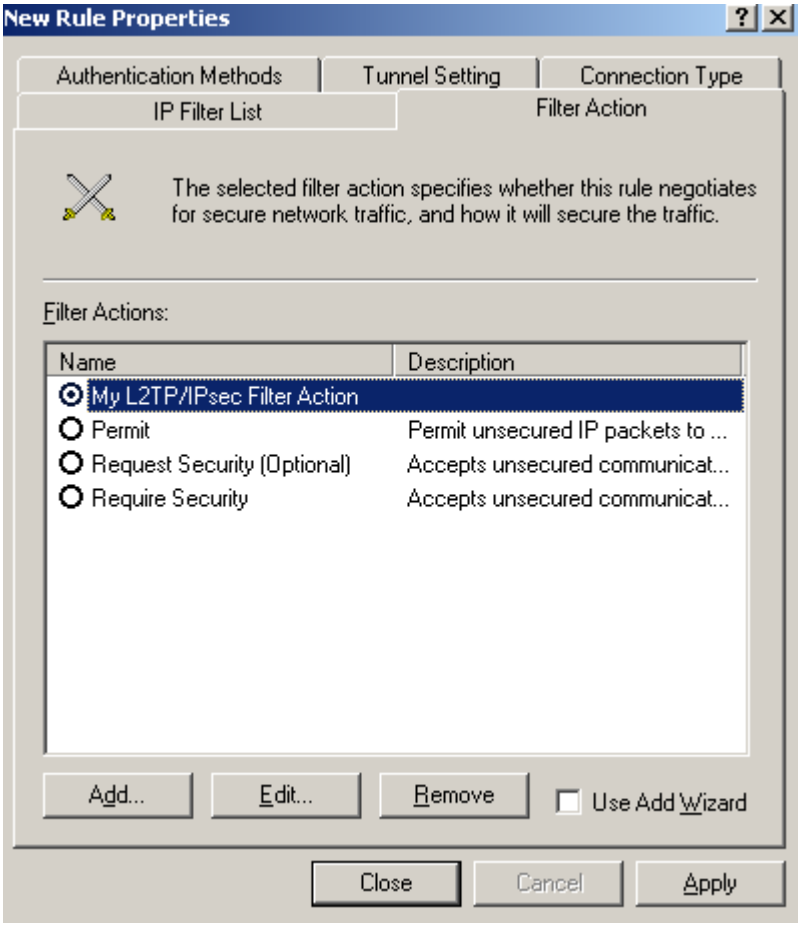


Figure96: Edit My L2TP/IPsec Policy - New Rule Properties: Filter Action tab - Newly Added Filter Action

On the **New Rule Properties** window, on the **Connection Type** tab, select **All network connections**, see **Figure97**.

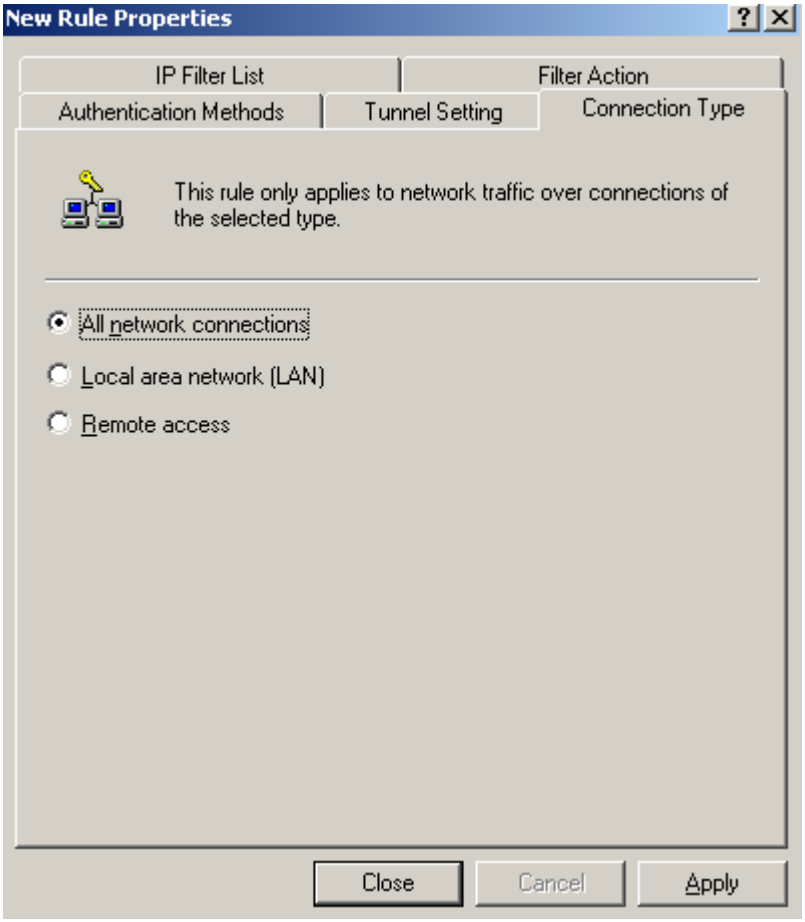


Figure97: Edit My L2TP/IPsec Policy - New Rule Properties: Connection Type tab

On the **New Rule Properties** window, on the **Tunnel Settings** tab, select **This rule does not specify an IPsec tunnel**, as we are not using IPsec tunnel mode, see **Figure98**.

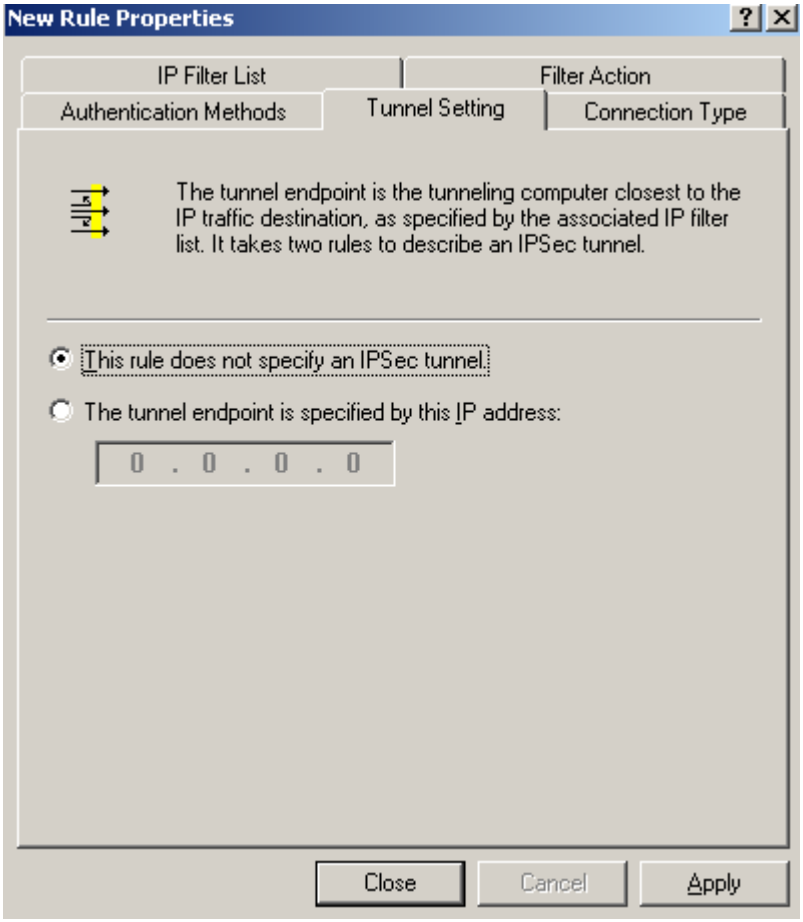


Figure98: Edit My L2TP/IPsec Policy - New Rule Properties: Tunnel Settings tab

On the **New Rule Properties** window, on the **Authentication Methods** tab, I've added two authentication methods for IKE MM, with certificates and with a pre-shared key, see **Figure99**.
Use the pre-shared key only for testing. If you do not need it, remove it from this policy. Remember that the pre-shared key entered on ISA's GUI for the VPN clients does not matter anymore, if you want to use a pre-shared key, you need to enter it here.

For the IKE authentication with certificates I've specified that a certificate from my Enterprise CA to be used, see **Figure100**. It appears that the Windows 2003 API or so is unable to be manually configured(from GUI or CLI) to use a specific certificate for IKE authentication. Please refer to this Microsoft article Public Key Certificate, section **IKE certificate selection process**.

The authentication methods are processed from top to down, so the authentication method with certificates is prefered.

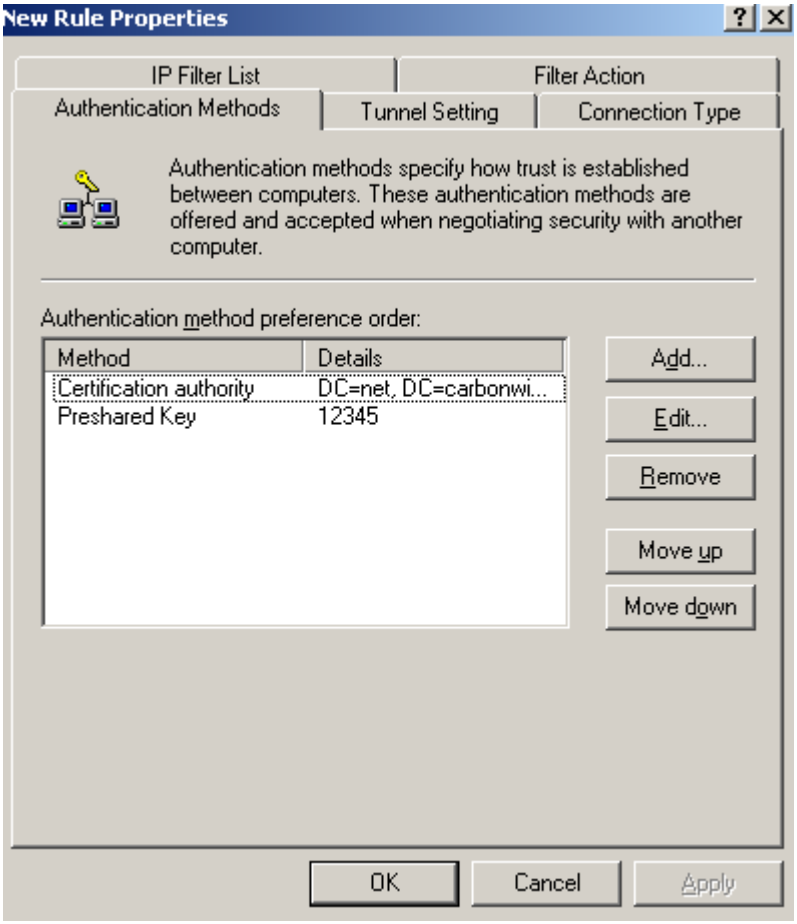


Figure99: Edit My L2TP/IPsec Policy - New Rule Properties: Authentication Methods tab - Two Authentication Methods Added

Note from **Figure100** that there is an option, **Exclude the CA name from the certificate request**, this option is disabled on the default policy. The VPN server requests a certificate from the client during IKE authentication with certificates, and specifies which CA has issued this certificate. By default on ISA, if multiple certificates from different CAs can be used for IKE authentication, ISA will ask the client to provide a cerytificate issued by one of this CAs. Some may feel, that if a private CA is used, certain information may leak, so they may enable the **Exclude the CA name from the certificate request** option. Doing that indeed they may enhance security, however, they may also introduce certain issues, for example the VPN client may have multiple certificates from different CAs that can be used for IKE authentication(say if the VPN client belongs to one of your business partners, as they may have their own private CA) and this L2TP/IPsec VPN client cannot be configured with which certificate to use when connecting to a certain L2TP/IPsec server(the case of the Windows L2TP/IPsec VPN clients) or some L2TP/IPsec VPN clients might not respond to a certificate request that does not include a CA name(Windows L2TP/IPsec VPN clients do respond to such a request).

Click **OK** to close the **Edit Authentication Method Property** window.

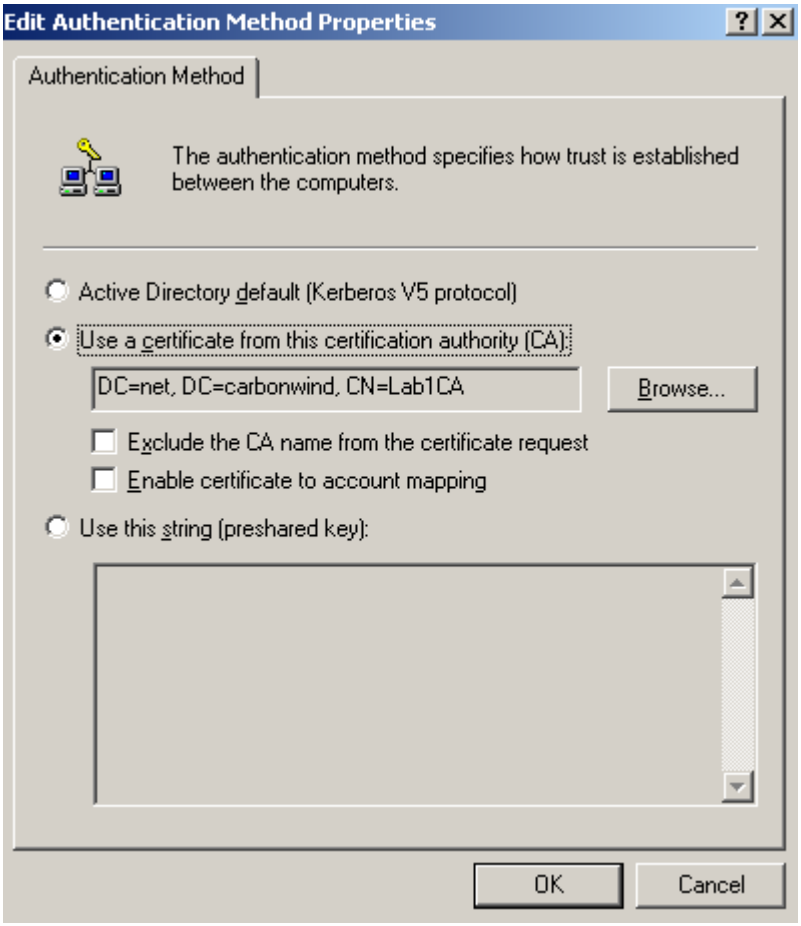


Figure100: Edit My L2TP/IPsec Policy - New Rule Properties: Authentication Methods tab - Add an Authentication Method: Use a certificate from this CA

Click **OK** to close the **New Rule Properties** window, and on the **Rules** tab select the newly created rule, see **Figure101**.

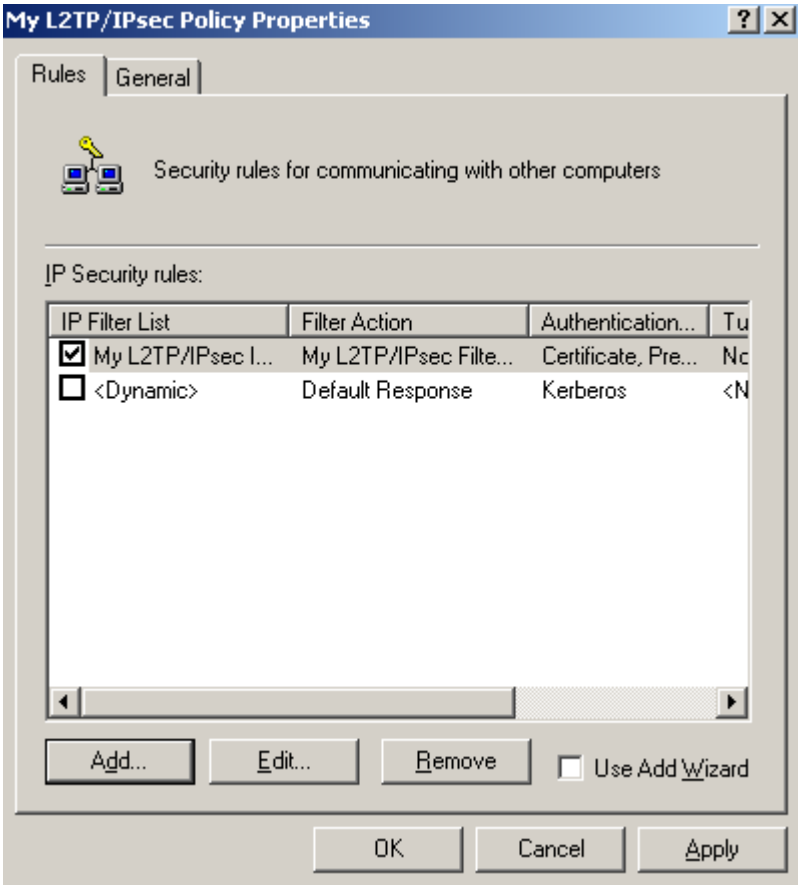


Figure101: Edit My L2TP/IPsec Policy - Rules tab: Newly Added Rule

We're not done yet. We need to enter the protection suites for IKE MM.

On the **My L2TP/IPsec Policy Properties** window, select the **General** tab, and click the **Settings...** button, see **Figure102**.

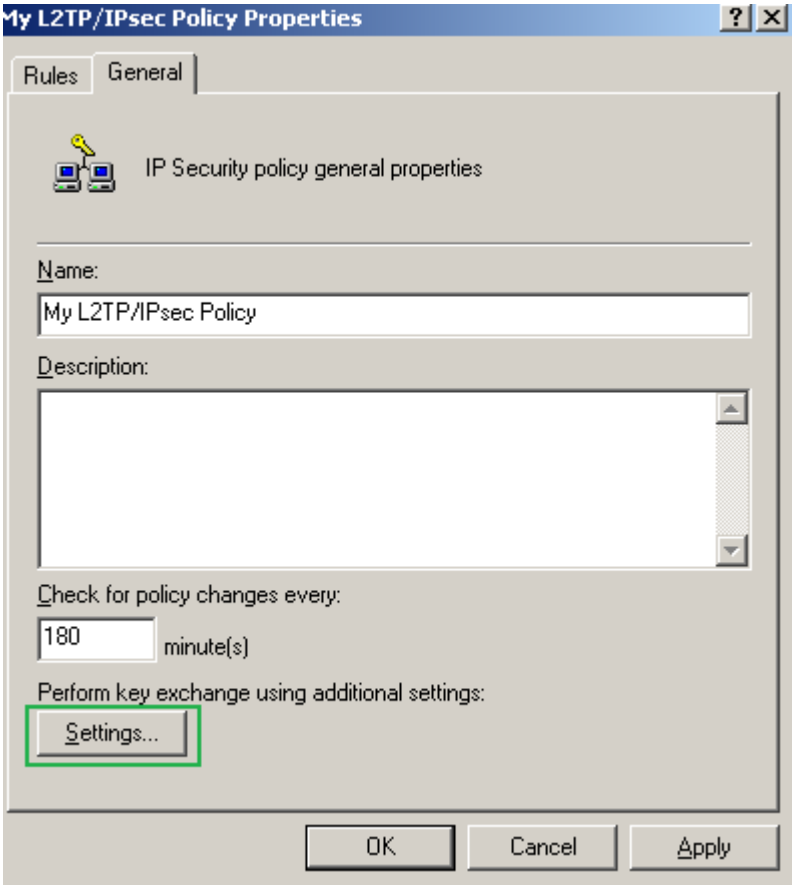


Figure102: Edit My L2TP/IPsec Policy - General tab

The **Key Exchange Settings** window appears, see **Figure103**.
Leave unchecked the **Master key perfect forward secrecy (PFS)** checkbox.
The **Authenticate and generate a new key after every** text boxes are correct, 480 minutes equals 28800 seconds(the IKE SA lifetime from the default MM policy).

Click the **Methods...** button.

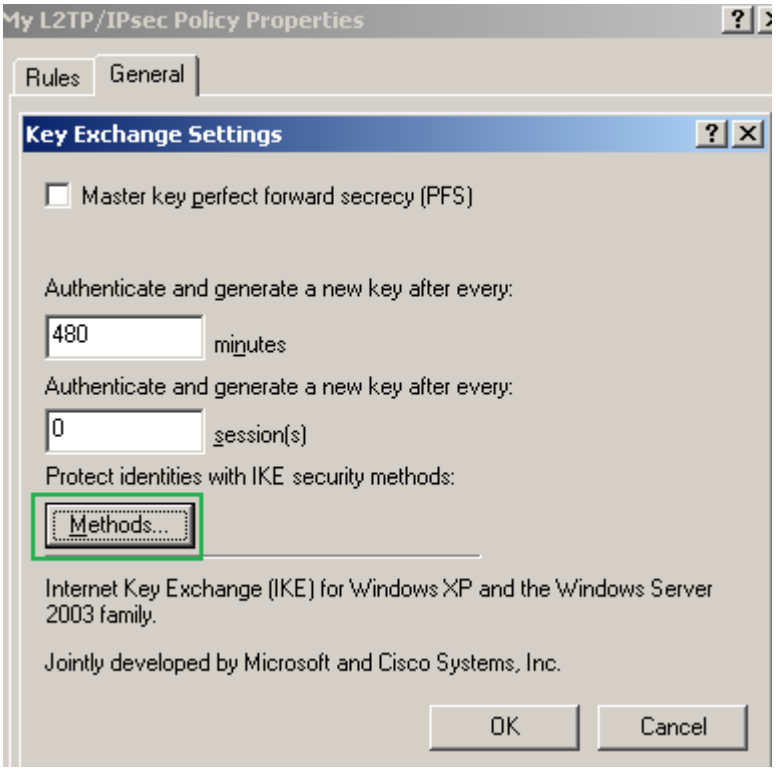


Figure103: Edit My L2TP/IPsec Policy - General tab: Key Exchange Settings

On the **Key Exchange Security Methods** window, remove the default Security Methods(if any) and click the **Add** button, then add the two security methods specified in **Figure104** and **Figure105**.
The first method specifies a high security protection suite, due to the stronger DH group. For example Windows Vista L2TP/IPsec VPN clients by default can use this stronger group. For compatibility reasons I've added the second security method(for example I did not notice that the Mac OS X L2TP/IPsec VPN client is capable of using this group), if you don't need it, as you are really sure that all of your L2TP/IPsec VPN clients or VPN gateways are capable of using the stronger DH group, you may remove the second security method.

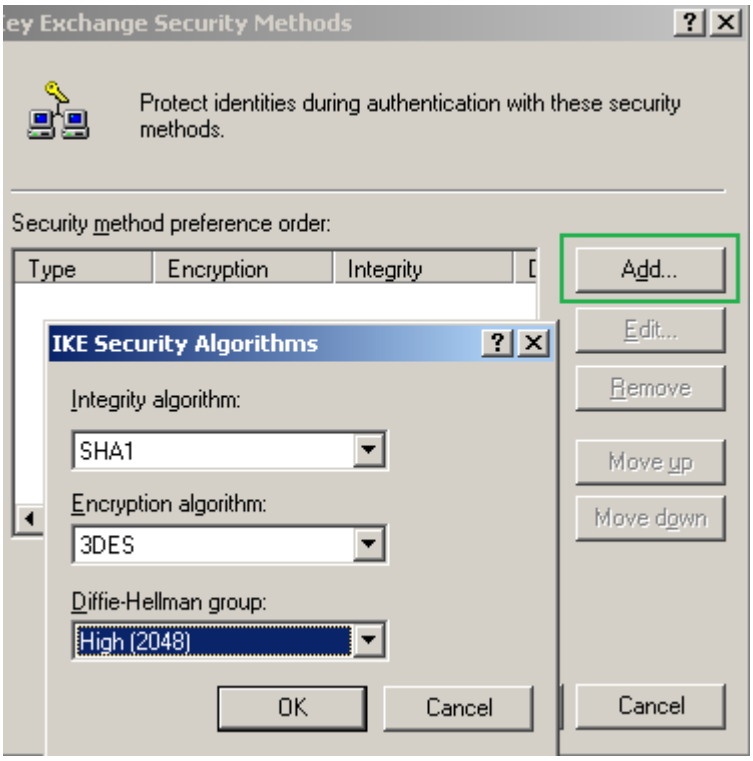


Figure104: Edit My L2TP/IPsec Policy - Key Exchange Security Methods - Add the first Security

Method

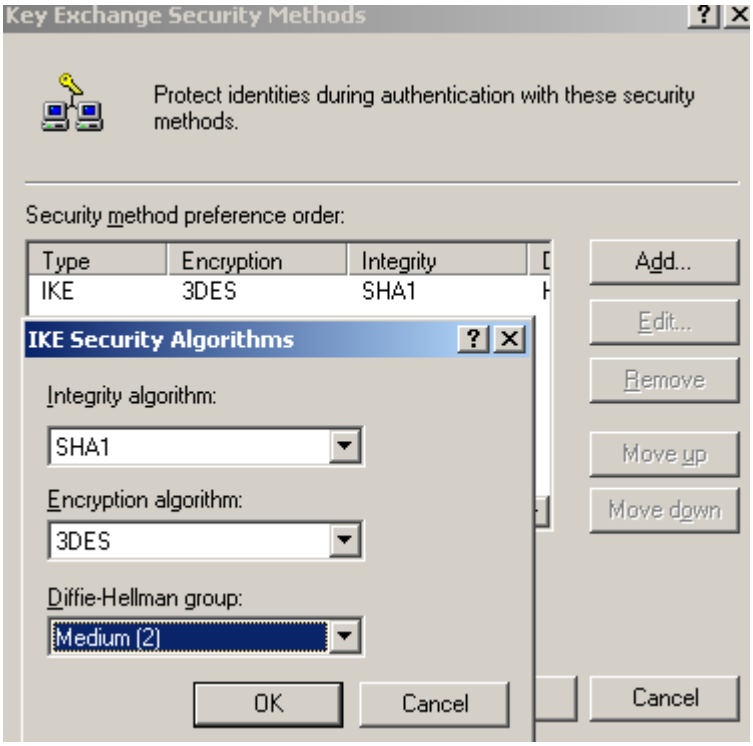


Figure105: Edit My L2TP/IPsec Policy - Key Exchange Security Methods - Add the second Security Method

Figure106 shows the added security methods. They are processed from top to down, so the stronger suite(the one with DH 2048) is prefered.

Figure106: Edit My L2TP/IPsec Policy - Key Exchange Security Methods - Added Key Security

Methods

Click **OK** to close the **Key Exchange Security Methods** window.
Click **OK** to close the **My L2TP/IPsec Policy Properties** window.

And we've created our custom IPsec policy to protect the L2TP tunnels.

Time to assign this custom IPsec policy. Right-click it and click **Assign**, see **Figure107**.

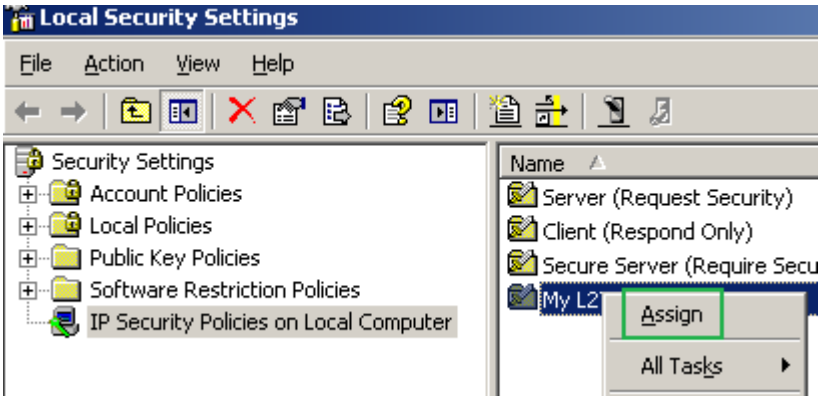


Figure107: Local Security Settings - Assign The Newly Created IPsec Policy

Once it was assigned, see **Figure108**, we can use the netsh commands to analyze it and compare it with the default one.

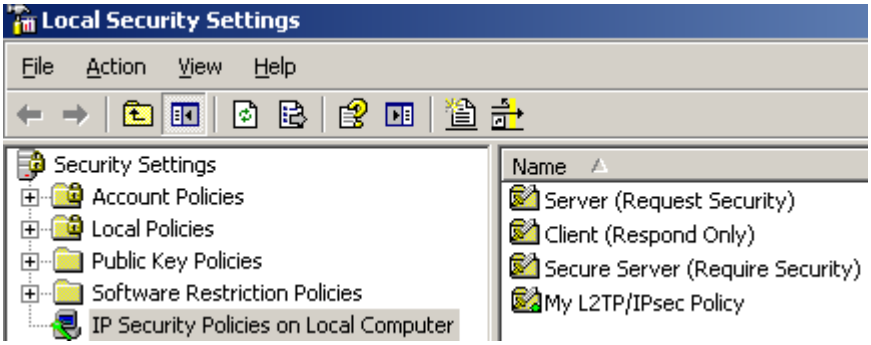


Figure108: Local Security Settings - The Newly Created IPsec Policy Was Assigned

Let's analyze the newly created MM and QM policies and generic filters, see **Figure109**(Custom L2TP Main Mode Policy), **Figure110**(Custom L2TP Quick Mode Policy), **Figure111**(Custom L2TP Main Mode Filters) and **Figure112**(Custom L2TP Quick Mode Filters).

Don't forget to compare them side-by-side with the ones from **Figure62**(Default L2TP Main Mode Policy), **Figure63**(Default L2TP Quick Mode Policy), **Figure64**(Default L2TP Main Mode Filters) and **Figure64**(Default L2TP Quick Mode Filters).

```
C:\>netsh ipsec dynamic show mmpolicy all

IKE MM Policy Name     : 9
IKE Soft SA Lifetime   : 28800 secs

Encryption Integrity  DH   Lifetime (Kb:secs)  QM Limit Per MM
---------- ---------- ----  ------------------  ---------------
 3DES       SHA1      2048       0:28800          0
 3DES       SHA1      2          0:28800          0
```

Figure109: Custom L2TP Main Mode Policy

```
C:\>netsh ipsec dynamic show qmpolicy all

QM Negotiation Policy Name : My L2TP/IPsec Filter Action

    Security Methods       Lifetime (Kb:secs)   PFS DH Group
------------------------ --------------------- ------------
 ESP[3DES,SHA1]               250000:3600       (Unassigned)
```

Figure110: Custom L2TP Quick Mode Policy

```
C:\>netsh ipsec dynamic show mmfilter all

Main Mode Filters: Generic

-------------------------------------------------------------

Filter name             : My L2TP Server Inbound Filter
Connection Type         : ALL
Source Address          : (Any IP Address)  (0.0.0.0        )
Destination Address     : (My IP Address)   (255.255.255.255)
Authentication Methods  :
        Root CA         : DC=net, DC=carbonwind, CN=Lab1CA
          Certmapping enabled : NO
          Exclude CA name     : NO

        Preshared key
Security Methods        : 2
        3DES/SHA1/DH3/28800/QMlimit=0
        3DES/SHA1/DH2/28800/QMlimit=0

-------------------------------------------------------------

Filter name             : My L2TP Server Outbound Filter
Connection Type         : ALL
Source Address          : (My IP Address)   (255.255.255.255)
Destination Address     : (Any IP Address)  (0.0.0.0        )
Authentication Methods  :
        Root CA         : DC=net, DC=carbonwind, CN=Lab1CA
          Certmapping enabled : NO
          Exclude CA name     : NO

        Preshared key
Security Methods        : 2
        3DES/SHA1/DH3/28800/QMlimit=0
        3DES/SHA1/DH2/28800/QMlimit=0

2 Generic Filter(s)
```

Figure111: Custom L2TP Main Mode Filters

```
C:\>netsh ipsec dynamic show qmfilter all

Quick Mode Filters(Transport): Generic

-------------------------------------------------------------------

Filter name             : My L2TP Server Filter1
Connection Type         : ALL
Source Address          : <Any IP Address>  (0.0.0.0        )
Destination Address     : <My IP Address>   (255.255.255.255)
Protocol                : UDP     Src Port: 0      Dest Port: 1701
Mirrored                : yes
Quick Mode Policy       : My L2TP/IPsec Filter Action
Inbound Action          : Negotiate
Outbound Action         : Negotiate

-------------------------------------------------------------------

Filter name             : My L2TP Server Inbound Filter
Connection Type         : ALL
Source Address          : <Any IP Address>  (0.0.0.0        )
Destination Address     : <My IP Address>   (255.255.255.255)
Protocol                : UDP     Src Port: 1701   Dest Port: 1701
Mirrored                : no
Quick Mode Policy       : My L2TP/IPsec Filter Action
Inbound Action          : Negotiate
Outbound Action         : Negotiate

-------------------------------------------------------------------

Filter name             : My L2TP Server Inbound Filter
Connection Type         : ALL
Source Address          : <Any IP Address>  (0.0.0.0        )
Destination Address     : <My IP Address>   (255.255.255.255)
Protocol                : UDP     Src Port: 1701   Dest Port: 0
Mirrored                : no
Quick Mode Policy       : My L2TP/IPsec Filter Action
Inbound Action          : Negotiate
Outbound Action         : Negotiate

-------------------------------------------------------------------

Filter name             : My L2TP Server Outbound Filter
Connection Type         : ALL
Source Address          : <My IP Address>   (255.255.255.255)
Destination Address     : <Any IP Address>  (0.0.0.0        )
Protocol                : UDP     Src Port: 1701   Dest Port: 1701
Mirrored                : no
Quick Mode Policy       : My L2TP/IPsec Filter Action
Inbound Action          : Negotiate
Outbound Action         : Negotiate

-------------------------------------------------------------------

Filter name             : My L2TP Server Outbound Filter
Connection Type         : ALL
Source Address          : <My IP Address>   (255.255.255.255)
Destination Address     : <Any IP Address>  (0.0.0.0        )
Protocol                : UDP     Src Port: 0      Dest Port: 1701
Mirrored                : no
Quick Mode Policy       : My L2TP/IPsec Filter Action
Inbound Action          : Negotiate
Outbound Action         : Negotiate

5 Generic Filter(s)
```

Figure112: Custom L2TP Quick Mode Filters

As said before, with this custom IPsec policy in place, the pre-shared keys we configure on ISA, either for VPN clients(incoming L2TP/IPsec connections, which include the ones from the calling VPN gateways too) or for s2s L2TP/IPsec connections outgoing connections(when the local ISA acts as the calling gateway) will not count anymore, a single pre-shared key will exist for all of them, the one from our custom policy.

I've tested this policy with Windows XP and Vista L2TP/IPsec VPN clients, L2TP/IPsec VPN clients behind NAT devices(to see if NAT-T works), with multiple L2TP/IPsecVPN clients behind the same NAT device at a time, with VPN clients connecting directly when there is no NAT device between the VPN client and ISA

or when ISA was behind a NAT device, using IKE authentication with certificates or with a pre-shared key.

This custom policy is usable for s2s L2TP/IPsec VPN connections too, either using IKE authentication with certificates or with a pre-shared key, due to the nature of the custom MM and QM filters, which accept connections from any source IP addresses. I did not encounter any issues during some tests, when ISA acted either as a calling gateway or as an answering gateway.
ISA will know if it's an incoming VPN client or a VPN gateway based on the "user" credentials presented by this(PPP authentication), the name of the remote site is mapped with a local user name(that's why when you add a remote L2TP/IPsec site called say Branch, a local user named Branch with the Dial-in permissions set to allow must exist).
When acting as a calling gateway, based on the DoD from RRAS created from ISA's GUI, an L2TP tunnel needs to be started to the remote VPN gateway. Due to our custom IPsec policy, this L2TP tunnel must be protected, so IKE MM and QM negotiation will take place, and an IPsec SA will be established to protect this tunnel.

I highly recommend you to start a Wireshark or Netmon capture on ISA's external interface or on the interface on which the VPN server listens for incoming VPN L2TP/IPsec connections to see if the L2TP traffic is protected as expected. Also a look over the Oakley.log may gave you extra information about how things are working. And make a test from a VPN client on which you've disabled the default IPsec policy for L2TP, just to make sure ISA does not respond to naked L2TP tunnels.