VIRTUAL ACCESS
Service Provider Solutions

Service Managed Gateway™

How to Configure and Debug Generic Routing Encapsulation (GRE)

Issue 1.1

Date 14 August 2007

1 About this document

1.1 Scope

This document explains how to:

- configure GRE to route non-sensitive packets from one private network to another without having to go through address translation (section 2.1),
- use GRE with IP Security (IPSec) to provide a secure encrypted connection across IP networks (section 2.2), and
- use the Trace Analyzer tool to debug and trace GRE packets (section 3).

The SMG must be configured to access the Internet before you can configure GRE.

1.2 Readership

This document is for engineers who have previous experience configuring and managing Service Managed Gateways (SMGs).

2 Introduction

Generic Routing Encapsulation (GRE) is a protocol for encapsulating an arbitrary network layer protocol over another arbitrary network layer protocol. GRE is covered in the RFC2784 specification document.

In GRE encapsulation, a packet or *payload* that is being delivered across networks is first encapsulated in a GRE packet. It is then encapsulated in a second protocol known as the *delivery protocol*. GRE can route non-sensitive packets from one private network to another without having to go through address translation.

GRE can also form part of a secure VPN connection. GRE can be used with IP Security (IPSec) to provide a secure encrypted connection across IP networks. It can also be used with an IGMP proxy to carry multicast data. For example, incoming IP data can be encapsulated as GRE packets and carried over a transport-mode IPSec tunnel via the ESP delivery protocol.

You can use the Trace Analyzer tool in the SMG for debugging and tracing GRE packets.

3 Configuring GRE

In the examples in this guide:

- both central and remote SMGs have been configured with normal internet access and with address translation enabled, as illustrated in Figure 1,
- both SMGs use static IP addressing, and
- the IP address of the WAN interface never changes.

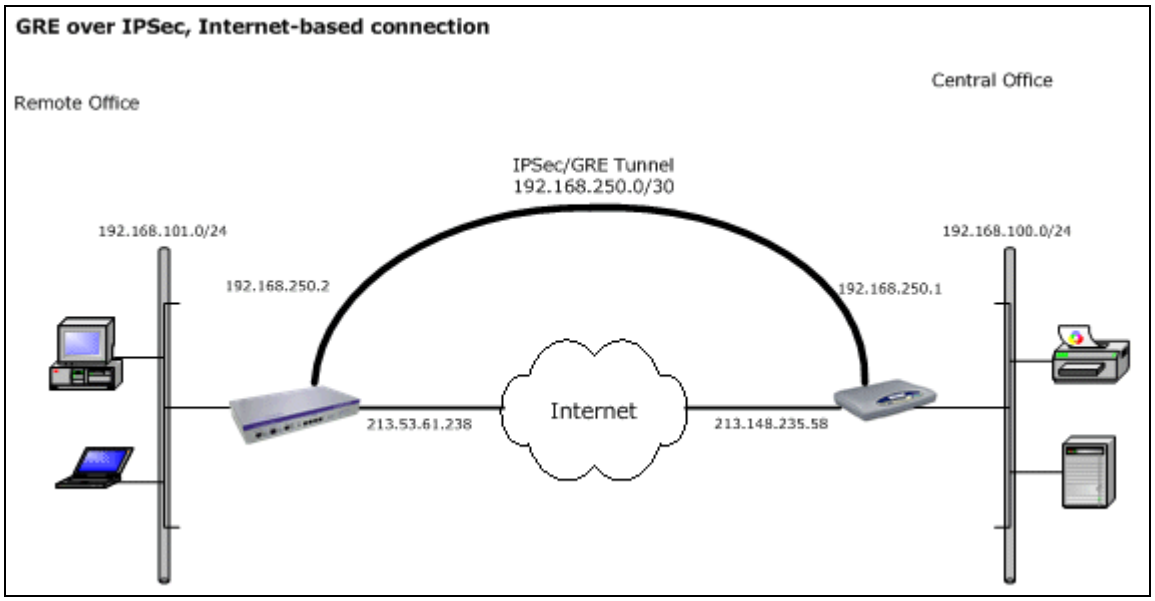

Figure 1: GRE over IPSec on an Internet-based connection

3.1 Configuring GRE using static routing

To configure GRE using static routing, you must:

- configure the GRE parameters,
- configure the IP parameters, and
- set up routing.

3.1.1 Configure GRE parameters

Configure the GRE interface with a remote peer.

1. On the SMG home page, click **Advanced**.
2. In the Advanced menu, click **Expert View**.
3. In Expert View, select **interfaces -> gre-1 -> gre configuration**.
4. Set the configuration parameters as outlined in Table 1 and click **Update**.

Field Name	Explanation
Enabled	Select **yes**.
Name	Type a descriptive name for the link.
Local IP Address	Set the WAN IP address of the local SMG. In the example in Figure 2, 213.148.235.58 is the IP address on the local peer and 213.53.61.238 is the IP address on the remote peer.
Remote IP Address	Set the WAN IP address of the remote SMG. In the example in Figure 3, 213.53.61.238 is the IP address on the local peer and 213.148.235.58 is the IP address on the remote peer.
Timeout	Specifies a period of time after which an inactive GRE tunnel shuts down. When a tunnel is required, it is automatically established. To create a permanent tunnel, set the value to **0**.

Table 1: GRE configuration fields and values

Figure 2 and Figure 3 illustrate examples of a GRE configuration for a central and a remote office.

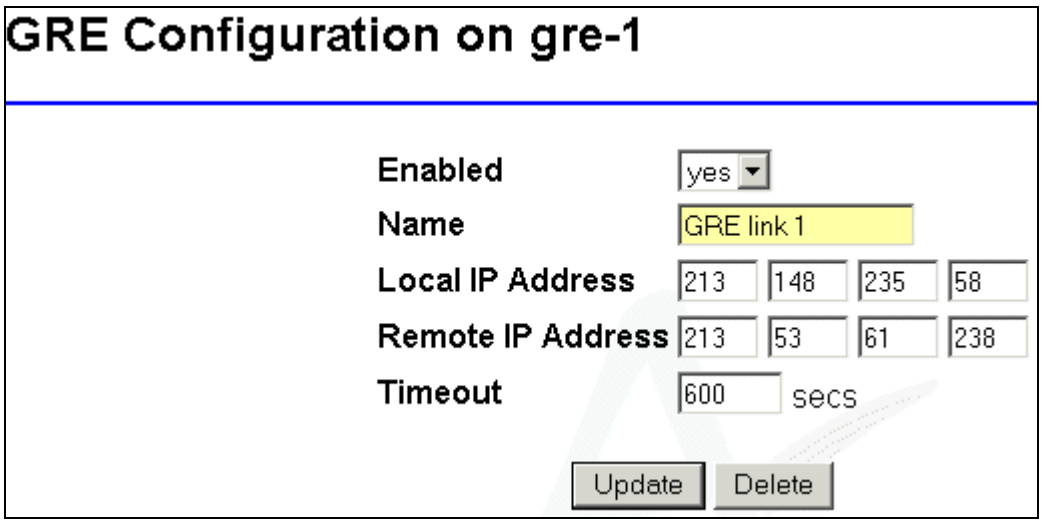

Figure 2: A GRE configuration for a central office

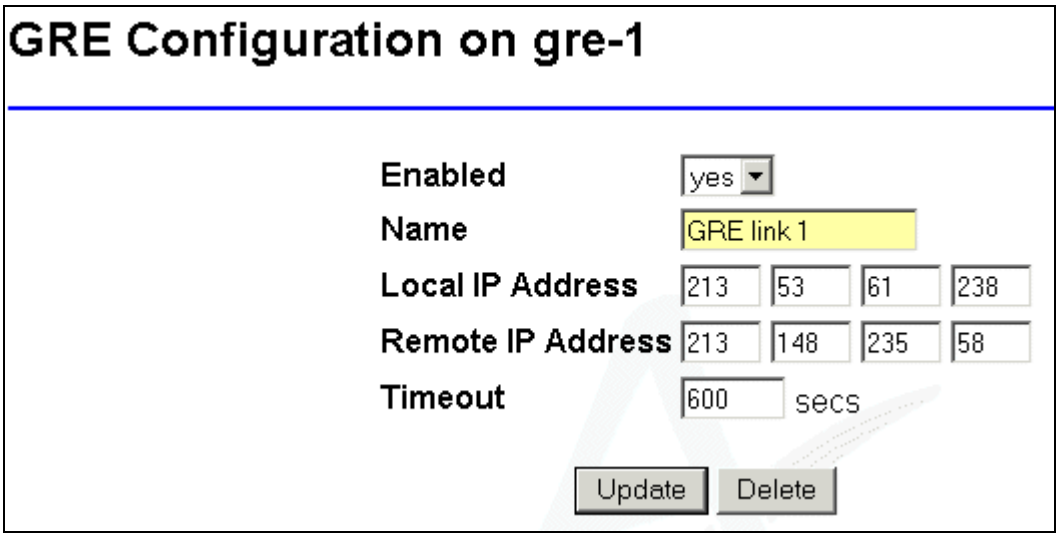

Figure 3: A GRE configuration for a remote office

3.1.2 Configure IP parameters

You must configure the IP details for the GRE interface so that packets can be encapsulated and routed correctly through the SMG. You can choose the IP details from a private address schema. However, the local and remote addresses you choose must be on the same subnet and must not conflict with the private Ethernet address subnet of either SMG.

1. On the SMG home page, click **Advanced**.
2. In the Advanced menu, click **Expert View**.
3. In Expert View, select **interfaces** -> **gre-1** -> **ip** -> **ip**.
4. Set the configuration parameters as outlined in Table 2 and click **Update**.

Field Name	Explanation
Enabled	Select **yes**.
Type	Select **numbered**.
IP Address	Set the IP address of the local SMG. In the example in Figure 4, 192.168.250.1 is the IP address on the local peer and 192.168.250.2 is the IP address on the remote peer.
Mask	Set the IP number of the local subnet mask.
Remote IP Address	Set the IP address of the remote SMG. In the example in Figure 5, 192.168.250.2 is the IP address on the local peer and 192.168.250.1 is the IP address on the remote peer.
Remote Mask	Set the IP number of the remote subnet mask.
MTU	MTU specifies the largest datagram that can be sent by the selected interface. By default, it is set to **1500** bytes. Use the default.
BOOTP	Enables or disables BOOTP. By default, it is set to **no**. Use the default.

Table 2: IP interface configuration fields and values

Figure 4 and Figure 5 illustrate examples of an IP configuration for a central and a remote office.

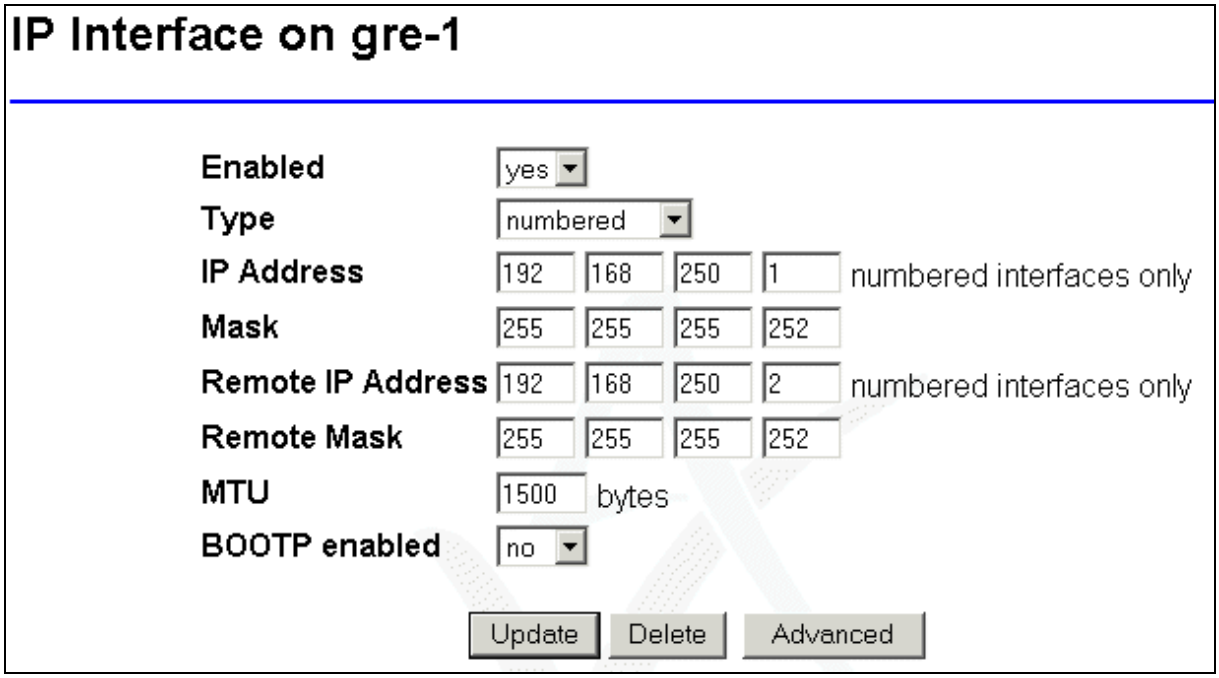

Figure 4: An IP configuration for a central office

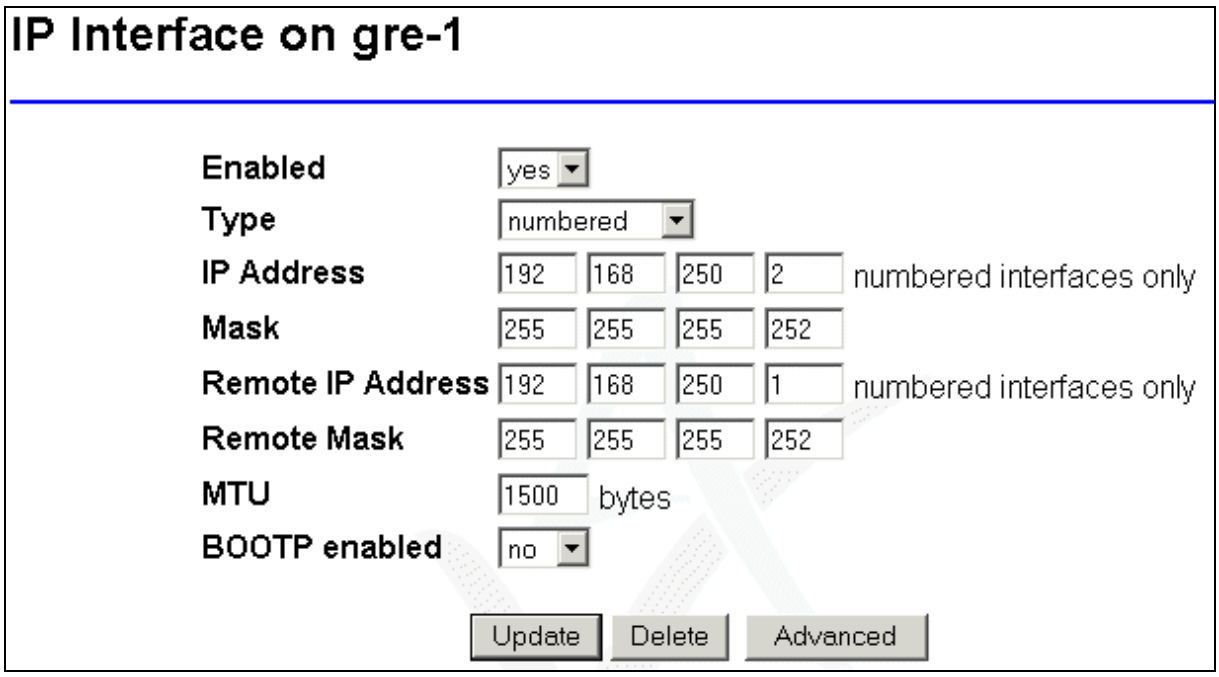

Figure 5: An IP configuration for a remote office

3.1.3 Set up routing

To route packets to the remote private LAN, you must set up a static route. The static route will catch all packets that are destined for the remote LAN and send them to the gre-1 interface. The gre-1 interface then encapsulates the packets and transports them to the remote peer.

1. On the SMG home page, click **Advanced**.
2. In the Advanced menu, click **Expert View**.
3. In Expert View, select **system** -> **ip** -> **static routes**.
4. Click **Add** in the first available row of the table.
5. In the IP Static Route Entry 1 page, set the configuration parameters as outlined in Table 3 and click **Update**.

Field Name	Explanation
Configured	Select **yes**.
Route Type	Select **unnumbered**.
IP Address	Type the LAN IP address of the remote SMG. In the example in Figure 6, the IP address on the local peer is 192.168.101.0 and on the remote peer 192.168.100.0.
Mask	Type the mask of the local or remote LAN subnet. In the examples in Figure 6 and Figure 7, the mask is 255.255.255.0
Next Hop For Numbered Interfaces	Type the numbered interface that packets will be directed to.
Next Hop For Unnumbered Interfaces	Select the unnumbered interface that packets will be directed to. Select **gre-1**.
Metric	The metric is used to determine the best route to a destination when alternate routes are compared. By default, the metric is set to 1500 bytes. Use the default.

Table 3: Static route configuration fields and values

Figure 6 and Figure 7 illustrate examples of static route configuration for a central and a remote office.

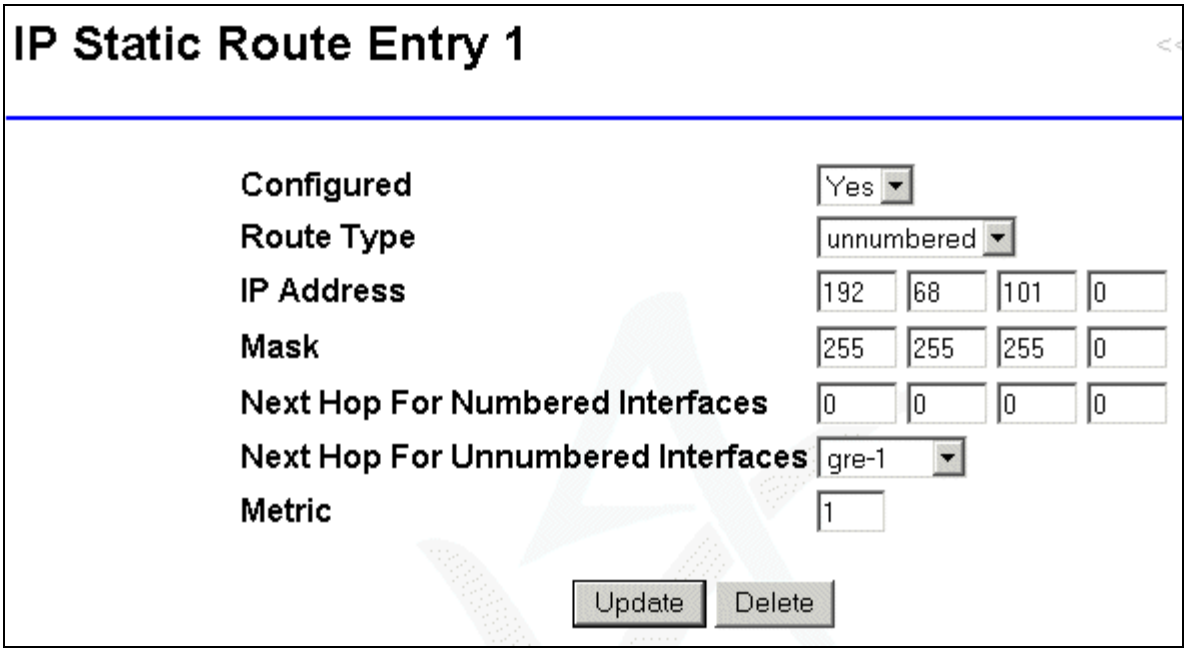

Figure 6: A static routing configuration for a central office

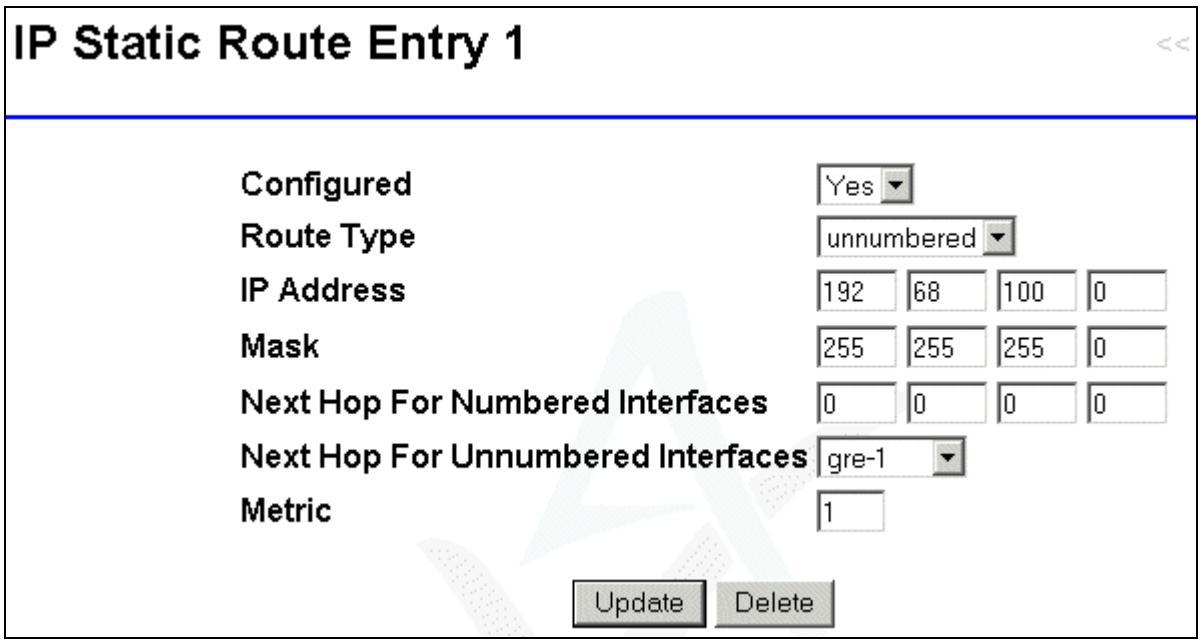

Figure 7: A static routing configuration for a remote office

3.2 Configuring GRE using IPSec

Follow the instructions in this section to provide IPSec encryption of the GRE packets. For more information on IPSec, read the Virtual Access guide **VPN Application and Configuration**.

3.2.1 Enable VPN

1. Ensure that the GRE interface is configured. If the GRE interface is not configured, follow the steps in section 3.1.1 and 3.12.
2. On the SMG homepage, click **Advanced**.
3. In the Advanced menu, click **Expert View**.
4. In Expert View, select **system -> vpn -> system**.
5. Set Enable VPN to **yes** and click **Update**.
6. Repeat steps 2–5 on the peer SMG.

Figure 8 illustrates an example of a VPN configuration for both a central and a remote office.

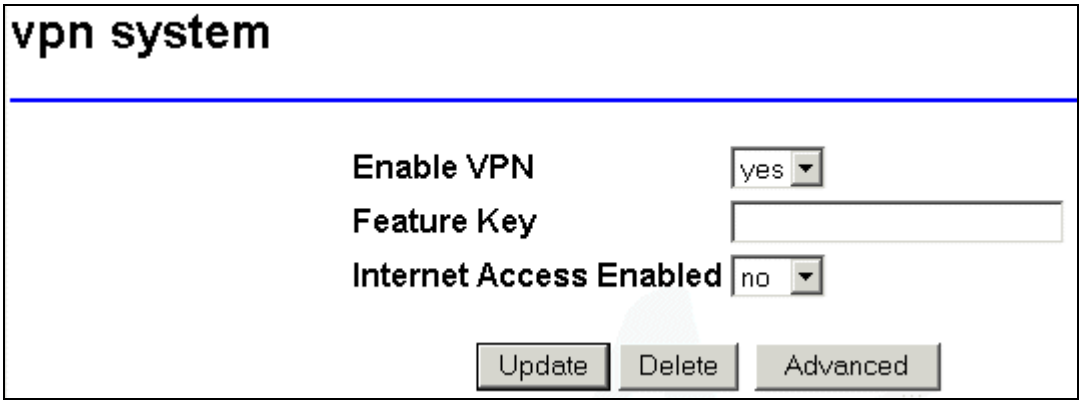

Figure 8: VPN is enabled

3.2.2 Set IKE parameters

Set the IKE parameters to set up the IPSec tunnel between the two peer devices.

1. On the SMG home page, click **Advanced**.
2. In the Advanced menu, click **Expert View**.
3. In the Expert View, select **system -> vpn -> ike**.
4. Click **Add** in the first available row of the table.
5. In the IKE Policy Configuration Entry 1 page, set the configuration parameters as outlined in Table 4 and click **Update**.

Field Name	Explanation
Enabled	Select **yes**.
Name	Type a descriptive name for the policy.
Response Type	Defines the role of the router in the IKE negotiation. By default, it is set to **both**. Use the default.
Exchange Type	Defines the security and speed of the exchange. Select **Main**.
Local Identifier Type	Defines the type of data that is used to identify the packet to the peer. Select **IP Address**.
Local Identifier Data	Type the local WAN IP address. In the examples in Figure 9 and Figure 10, **213.148.235.58** is the WAN IP address on the local peer and **213.53.61.238** is the WAN IP address on the remote peer.
Remote Identifier Type	Select **IP Address**.
Remote Identifier Data	Type the remote WAN IP address. In the examples in Figure 9 and Figure 10, **213.53.61.238** is the WAN IP address on the local peer and **213.148.235.58** is the WAN IP address on the remote peer.
Local Address	Type the local WAN IP address. In the examples in Figure 9 and Figure 10, **213.148.235.58** is the local WAN IP address on the local peer and **213.53.61.238** is the local WAN IP address on the remote peer.
Peer Address	Type the remote WAN IP address. In the examples in Figure 9 and Figure 10, **213.53.61.238** is the remote WAN IP address on the local peer and **213.148.235.58** is the remote WAN IP address on the remote peer.
Preshared Key	This password must be the same on both peers. For security, it should be greater than 16 characters.
Preshared Key Confirm	Retype the password for the Preshared Key.
Perfect Forward Secrecy (PFS)	Enables or disables PFS. By default, it is set to **no**.
DH Group	By default, the DH Group set to **1 (768)**. Use the default.
Authorisation Mode	Select **Preshared Key**.
Encryption Algorithm	Select **3DES**.
Authentication Algorithm	By default, the Authentication Algorithm is set to **md5**. Use the default.
Life (KB) and Life (seconds)	Use the default values.

Table 4: Parameters for setting the IKE

Figure 9 and Figure 10 illustrate examples of the IKE configuration for a central and a remote office.

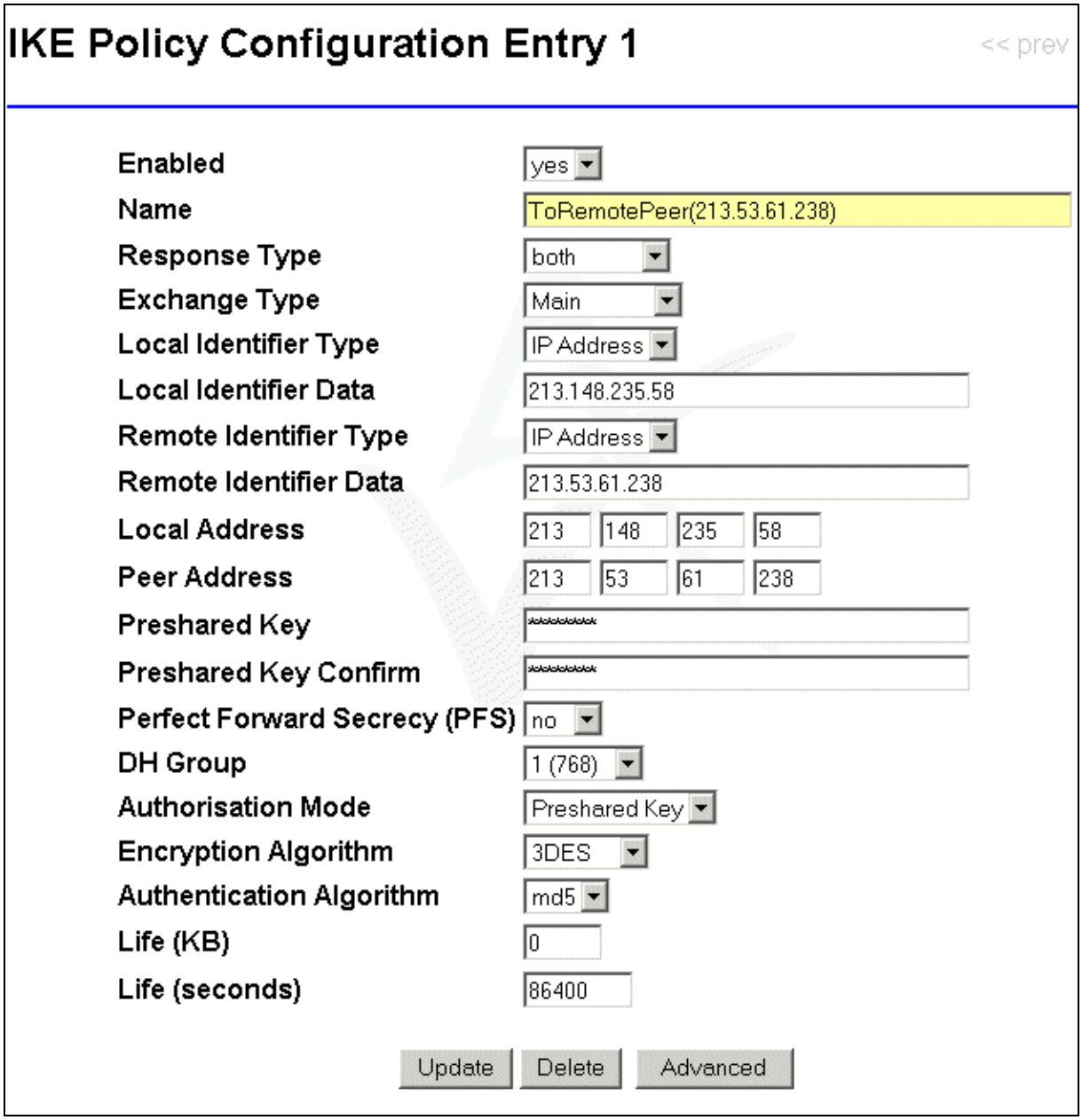

Figure 9: An IKE configuration for a central office

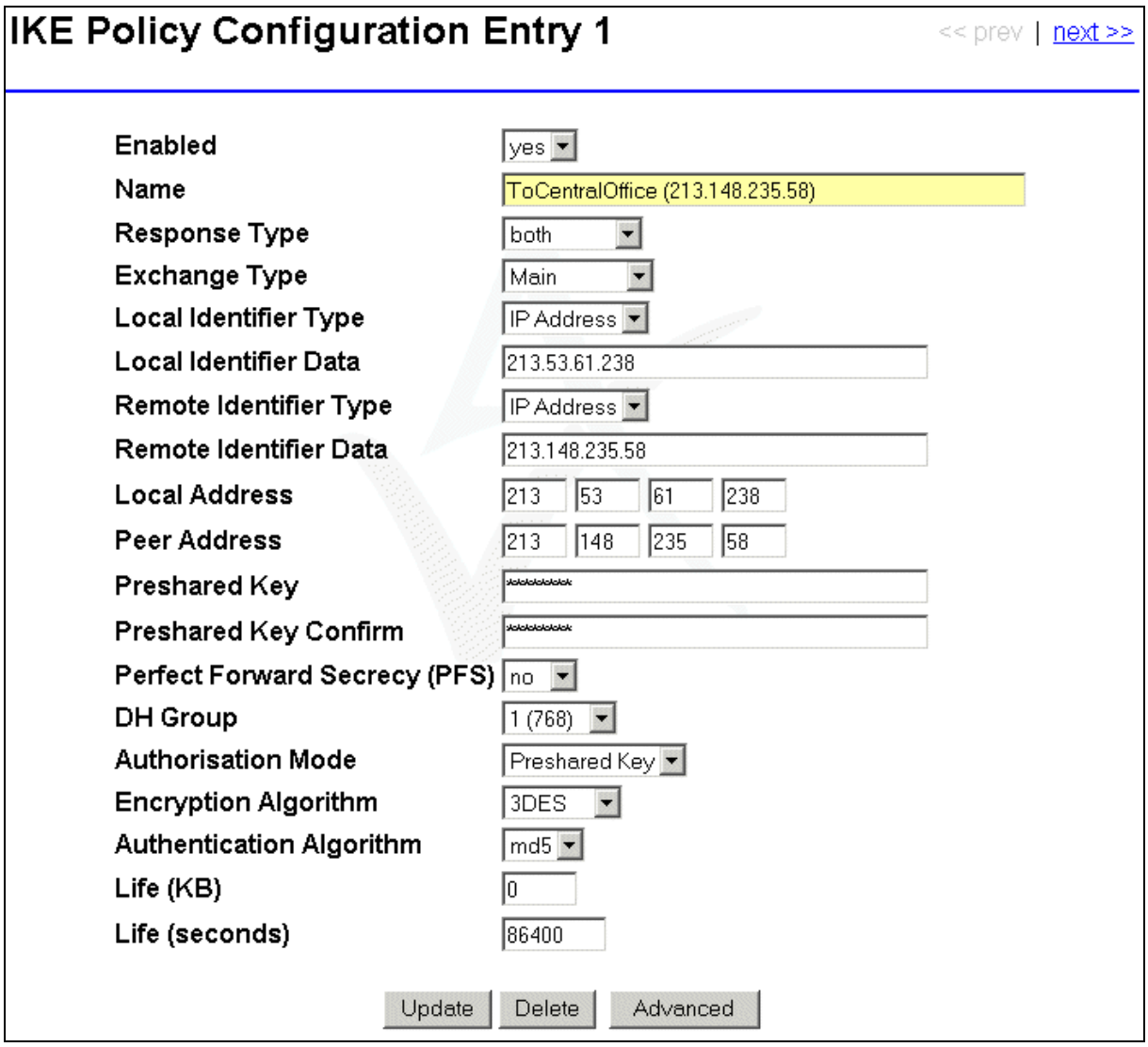

Figure 10: An IKE configuration for a remote office

3.2.3 Set SPD parameters

Configure the SPD parameters to catch matching GRE packets, encrypt them using IPSec, and deliver them across the IPSec tunnel. You need to configure **two** SPD policies for each peer. An apply policy encrypts the data for delivery across the tunnel. A bypass policy allows the encrypted data in from the remote peer.

	Local peer	Remote peer
Bypass policy	•	•
Apply policy	•	•

Table 5: Bypass and apply policies apply to both peers

1. On the SMG home page, click **Advanced**.
2. In the Advanced menu, click **Expert View**.

3. In Expert View, select **system** -> **vpn** -> **spd 1-100**.
4. Click **Add** to add a new policy.
5. In the SPD Policy Configuration Entry page, set the configuration parameters as outlined in Table 6 and click **Update**.

Field Name	Explanation
Enabled	Select **yes**.
Name	Type a name for the policy.
Process	Determines what will happen to the packets that match this policy. Select **apply** for an apply policy and **bypass** for a bypass policy.
Priority	Assigns a priority to policies. Assign a higher priority number to apply policies than to bypass policies.
Protocol	Select **gre**.
Source Start Address and Source End Address	For an apply policy, type the local GRE IP address in both fields. In the examples in Figure 11 and Figure 13, **213.148.235.58** is the source address on the local peer and **213.53.61.238** is the source address on the remote peer. For a bypass policy, type the remote GRE IP address in both fields. In the examples in Figure 12 and Figure 14, **213.53.61.238** is the source address on the local peer and **213.148.235.58** is the source address on the remote peer.
Source Mask	Type **255.255.255.255**.
Source Port	By default, the source port is **0**.
Destination Start Address and Destination End Address	For an apply policy, type the remote GRE IP address in both fields. In the examples in Figure 11 and Figure 12, **213.53.61.238** is the destination address on the local peer and **213.148.235.58** is the destination address on the remote peer. For a bypass policy, type the local GRE IP address in both fields. In the examples in Figure 11 and Figure 12, **213.148.235.58** is the destination address on the local peer and **213.53.61.238** is the destination address on the remote peer.
Destination Mask	Type **255.255.255.255**.
Destination Port	By default, the destination port is **0**. Use the default.
Security Protocol	By default, the security protocol is **esp**. Use the default.
Security Gateway	For apply policies, type the remote peer WAN IP address. In the examples in Figure 11 and Figure 13, **213.53.61.238** is the WAN IP address on the local peer and **213.148.235.58** is the WAN IP address on the remote peer.
Authentication in ESP	By default, the authentication in ESP is set to **yes**. Use the default.
Encryption Algorithm	By default, the encryption algorithm is set to **yes**. Use the default.
Authentication Algorithm	By default, the authentication algorithm is set to **md5**. Use the

	default.
Encapsulation Mode	Select **transport**.
Life (KB) and Life (seconds)	Use the default values.

Table 6: An SPD policy configuration

Figure 11 and Figure 12 illustrate examples of the SPD configuration for an apply policy and a bypass policy for a central office.

Figure 13 and Figure 14 illustrate examples of the SPD configuration for an apply policy and a bypass policy for a remote office.

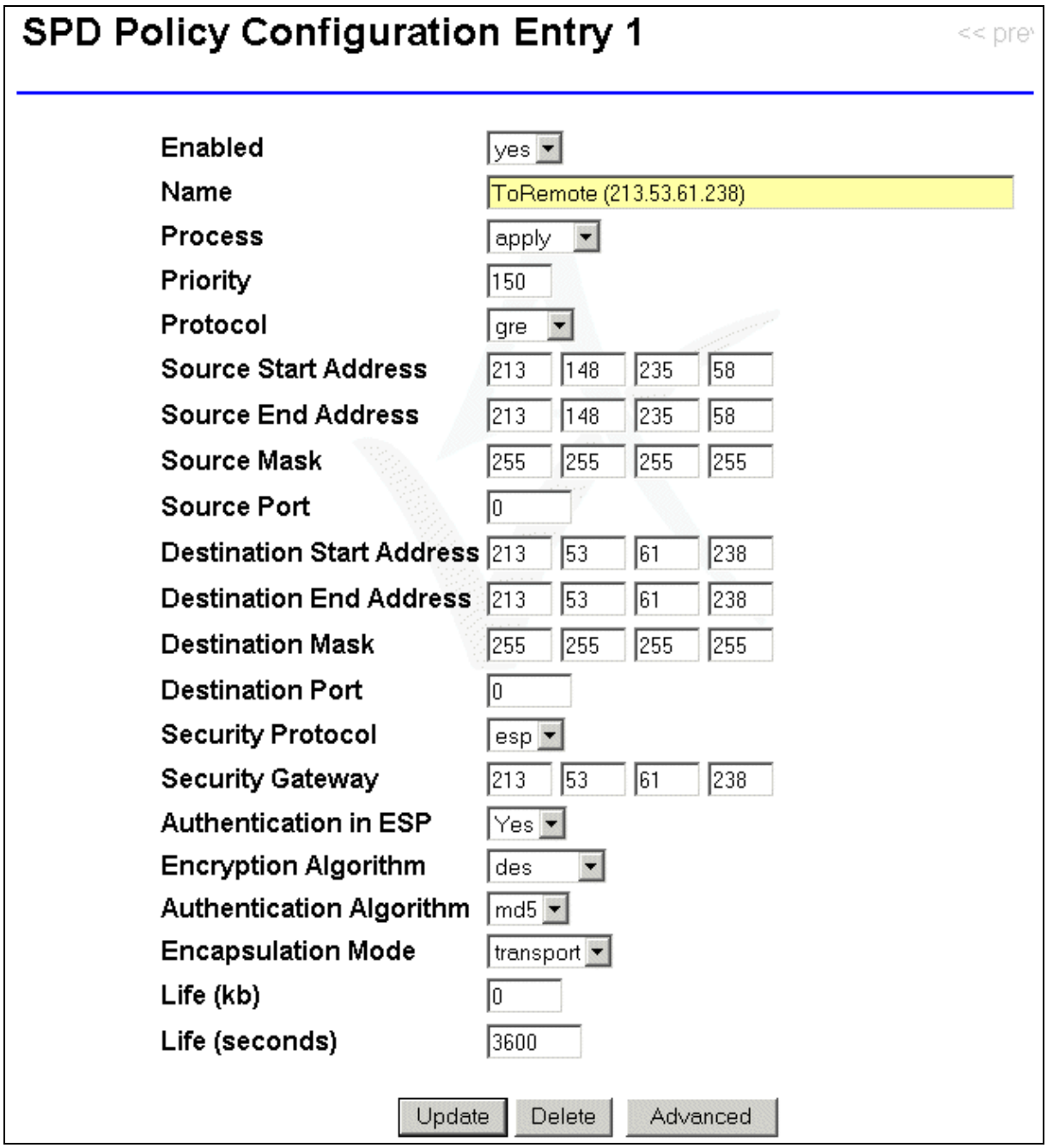

Figure 11: An apply policy for a central office

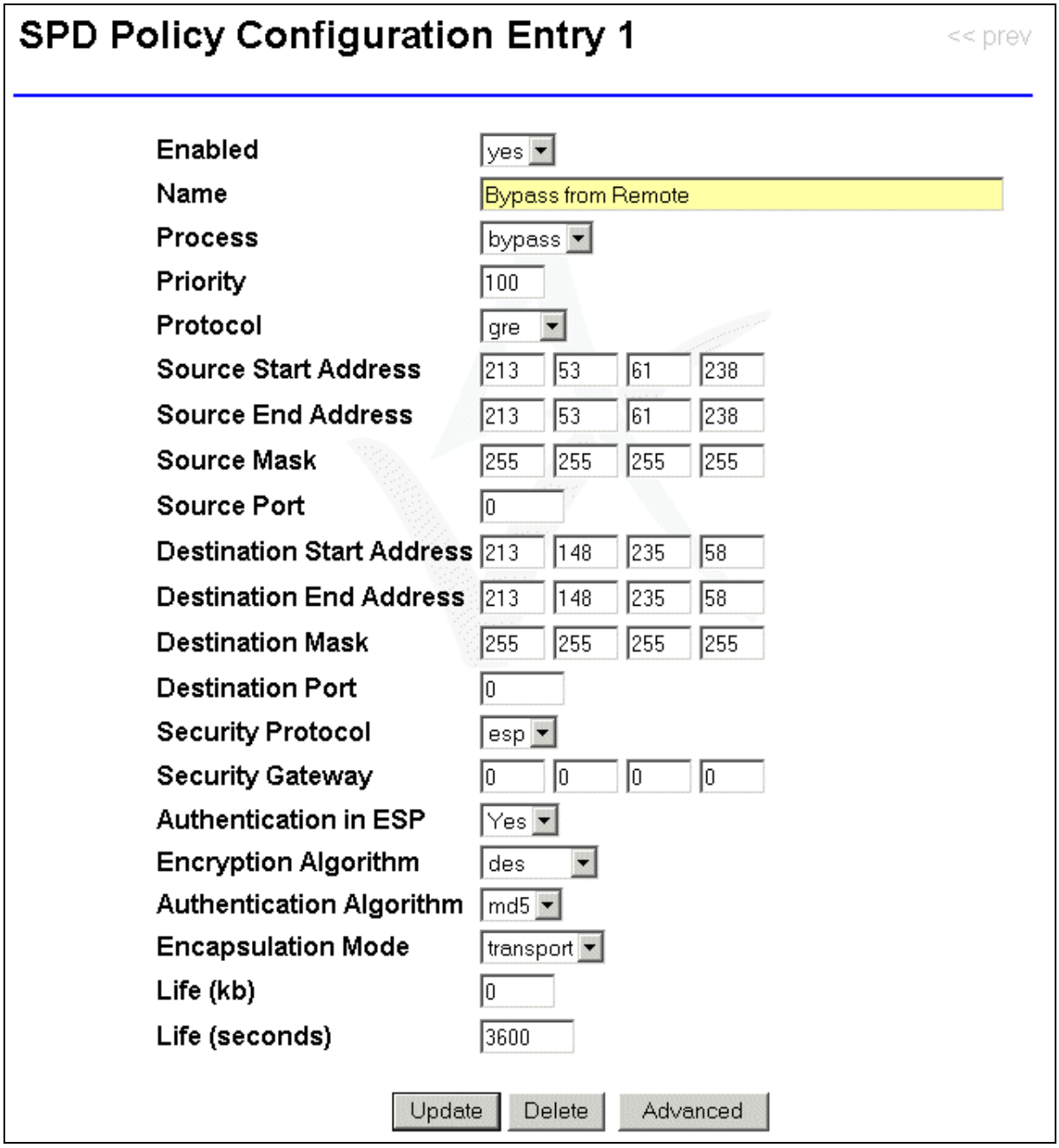

Figure 12: A bypass policy for a central office

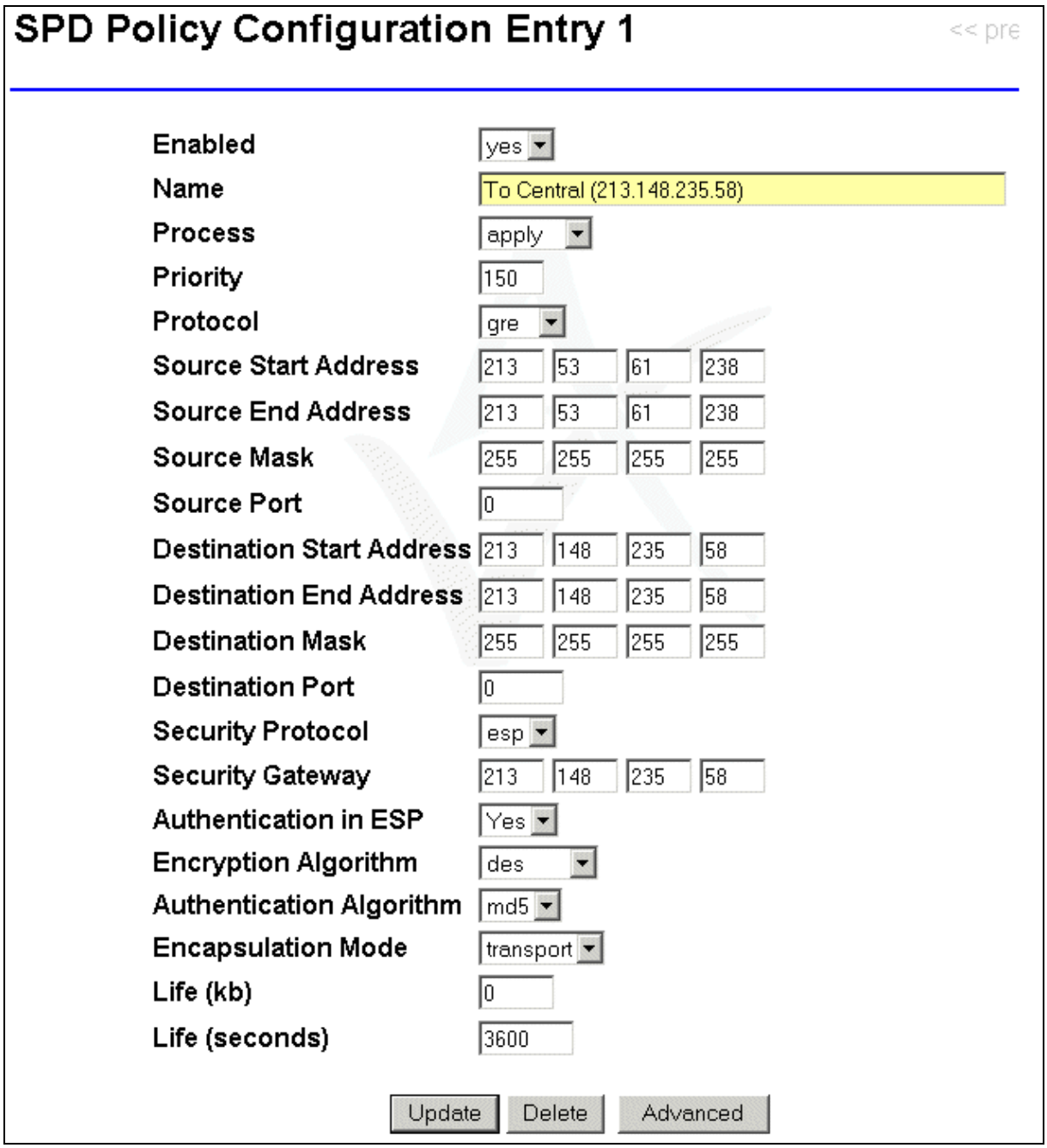

Figure 13: An apply policy for a remote office

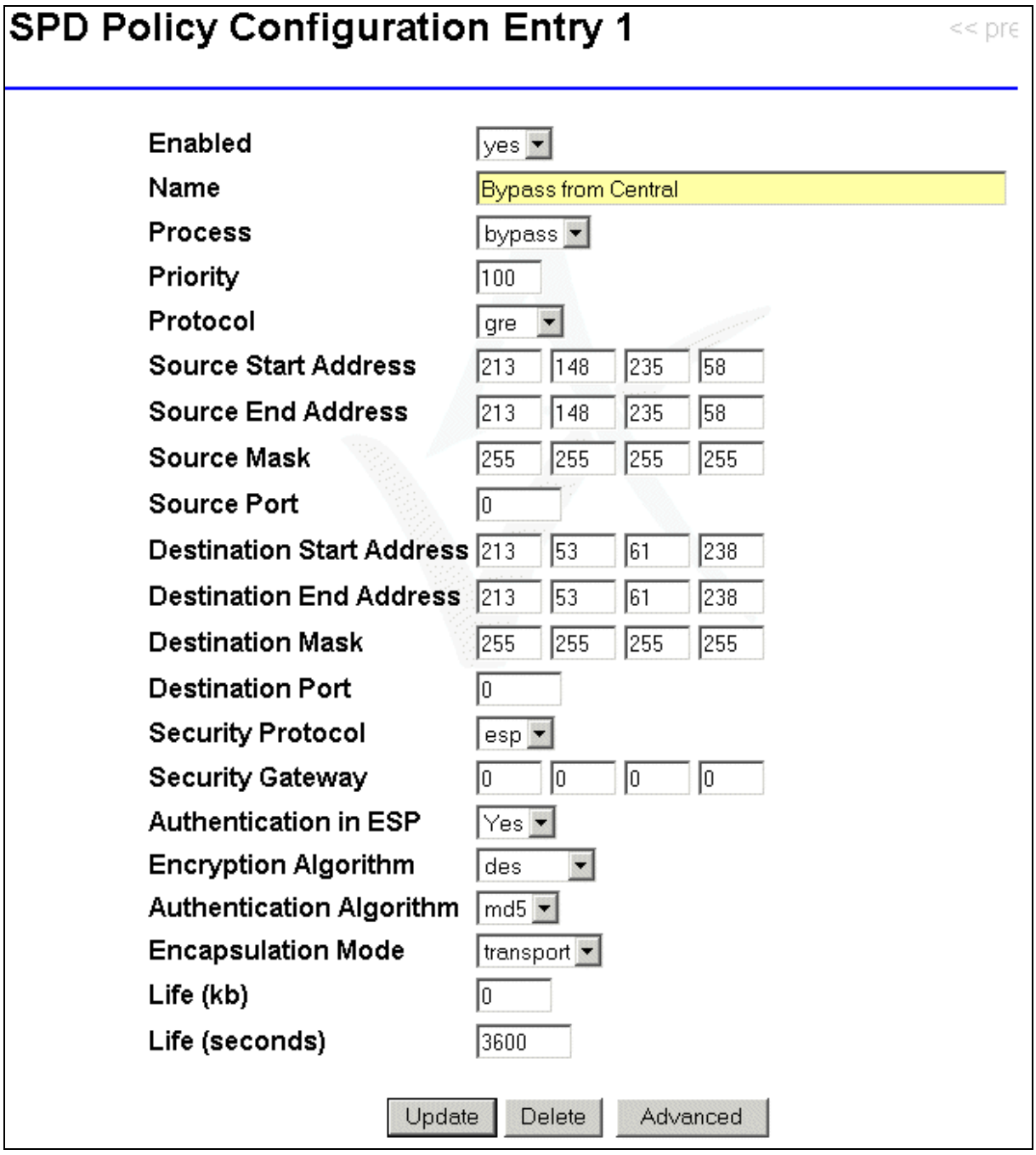

Figure 14: A bypass policy for a remote office

3.2.4 Set up routing

To set up routing, follow the steps in section 3.1.3.

4 Debugging GRE

4.1 Viewing interface statistics

1. On the SMG home page, click **Advanced**.
2. In the Advanced menu, click **Expert View**.
3. In Expert View, click **Operations**.
4. Select **status** -> **interface summary**.

Figure 15 shows an example of the status summary page for the interfaces.

Interface Status Summary

Index	Name	Ad State	Op State	InOctets	outOctets
01	eth-0	up	up	64091	77255
81	eth-1	up	up	9500	9012
82	eth-2	up	up	344601	372453
83	eth-3	up	down	0	0
111	gre-1	up	up	312	474
112	gre-2	down	down	0	0
113	gre-3	down	down	0	0
114	gre-4	down	down	0	0
115	gre-5	down	down	0	0
116	gre-6	down	down	0	0
117	gre-7	down	down	0	0
118	gre-8	down	down	0	0
440	t1e1-0	up	down	0	0

Figure 15: A status summary for interfaces

4.2 Tracing GRE

4.2.1 Trace GRE

1. Open the Trace analyzer tool.
    1. On the SMG home page, click **Advanced**.
    2. Click Diagnostics
    3. In the Diagnostics form, click **Trace Analyzer**.
2. Trace a GRE packet.
    1. Select the **IP** debugging checkbox.
    2. Type **gre** in the Event Filter field.
    3. Click **Start Trace**.

4.2.2 Customise the GRE trace information

You can customise the information that is returned by the trace by combining the GRE event filter with other protocols.

The steps below explain how to trace a detailed flow of a ping received on eth-0, encapsulated by GRE, and sent out on eth-3 as an encrypted ESP packet.

1. On the SMG home page, click **Advanced**.
2. In the Advanced menu, click **Diagnostics**.
3. In the Diagnostics form, click **Trace Analyzer**.
4. Select the **IP** checkbox.
5. Type **gre|icmp|esp** in the Event Filter field.
6. Click **Start Trace**.

Note: The string gre|icmp|esp specifies IP packets containing GRE **or** ICMP **or** ESP in the event string. If you want to trace packets that use all these protocols, use the & symbol instead of the pipe (|) symbol.

Figure 16 illustrates the trace information for the example trace on gre|icmp|isp.

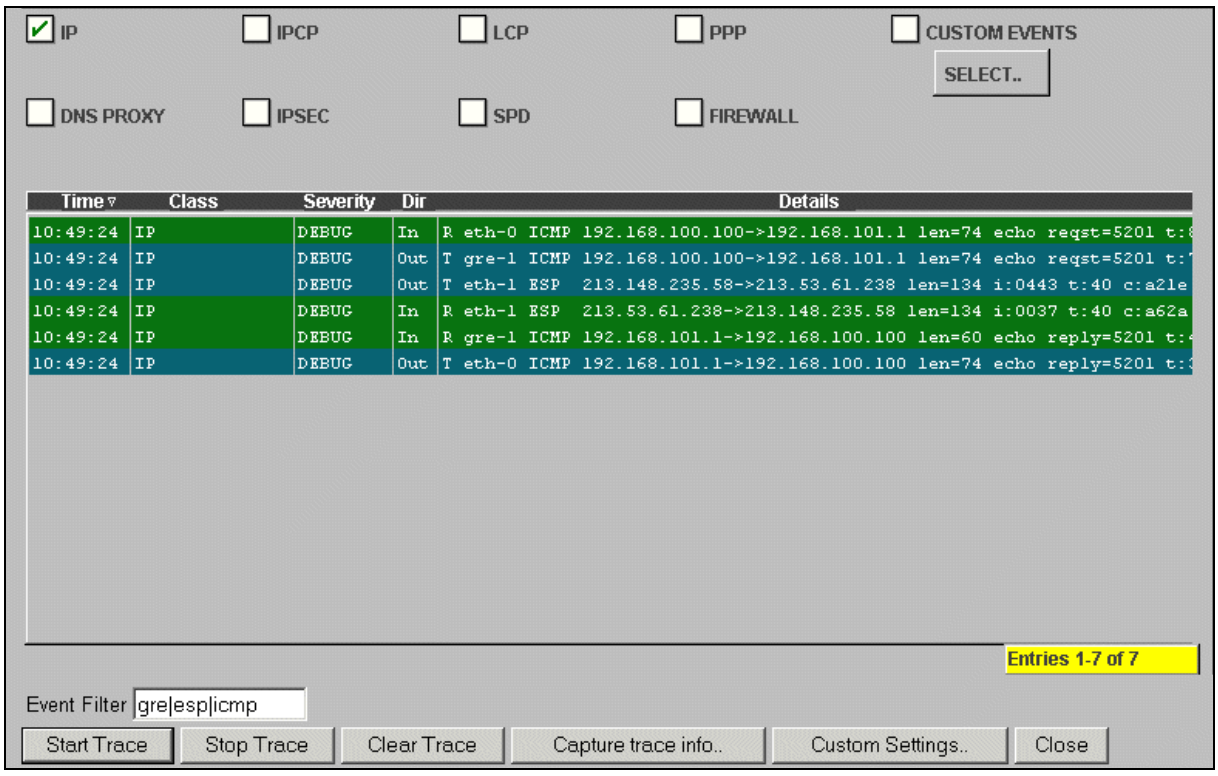

Figure 16: Results in the Trace Analyzer interface

4.2.3 Capture trace information

Click **Capture trace info**. The output appears in a browser window. You can save, print, or cut and paste the output.

Figure 17 illustrates the output for an ICMP ping across the example GRE connection from PC 192.168.101.2 to server 192.168.100.2.

Trace Analyser Logfile

You may save, print or cut & paste from this window to another application.

```
1.    10:49:24 Jan-15-2004   IP      DEBUG   In    R eth-0 ICMP 192.168.100.100->192.168.10
2.    10:49:24 Jan-15-2004   IP      DEBUG   Out   T gre-1 ICMP 192.168.100.100->192.168.10
3.    10:49:24 Jan-15-2004   IP      DEBUG   Out   T eth-1 ESP  213.148.235.58->213.53.61.2
4.    10:49:24 Jan-15-2004   IP      DEBUG   In    R eth-1 ESP  213.53.61.238->213.148.235.
5.    10:49:24 Jan-15-2004   IP      DEBUG   In    R gre-1 ICMP 192.168.101.1->192.168.100.
6.    10:49:24 Jan-15-2004   IP      DEBUG   Out   T eth-0 ICMP 192.168.101.1->192.168.100.
7.    10:49:24 Jan-15-2004   IP      DEBUG   In    R eth-1 ICMP 213.53.61.238->213.148.235.

Trace capture complete.
```

Figure 17: Trace Analyzer output