

# IPsecLite User Guide

---

A network emulator and visualization tool for teaching network security concepts.

Copyright © ADABTEK, Corp. All rights reserved.

Last updated: March 2010

© 2010 ADABTEK, Corp. All rights reserved.

Trademarks and brands are the property of their respective owners.

The information in this document belongs to ADABTEK, Corp. It may not be used, reproduced or disclosed without the written approval of ADABTEK, Corp.

Notice of non-liability:

ADABTEK, Corp. is providing the information in this document to you “AS-IS” with all faults. ADABTEK, Corp. makes no warranties of any kind (whether express, implied or statutory) with respect to the information contained herein. ADABTEK, Corp. assumes no liability for damages (whether direct or indirect), caused by errors or omissions, or resulting from the use of this document or the information contained in this document or resulting from the application or use of the product described herein. ADABTEK, Corp. reserves the right to make changes to any information herein without further notice.

# Contents

<b>PREFACE .....</b>	<b>5</b>
<b>Intended Audience.....</b>	<b>5</b>
<b>Where to Go for More Information .....</b>	<b>5</b>
<b>Revision History .....</b>	<b>5</b>
<b>SYSTEM REQUIREMENTS .....</b>	<b>6</b>
<b>INSTALLATION .....</b>	<b>7</b>
<b>USING IPSECLITE .....</b>	<b>8</b>
<b>Tutorial 1: Emulating the Network .....</b>	<b>9</b>
Configuring Hosts and Gateways .....	9
Testing the Network.....	11
<b>Tutorial 2: Establishing a Protected Tunnel .....</b>	<b>13</b>
Defining Protection Rules.....	13
Establishing Security Associations.....	14
Verifying Traffic Protection .....	14
<b>Tutorial 3: Simulating Attacks.....</b>	<b>17</b>
<b>COMPLETE REFERENCE.....</b>	<b>19</b>
<b>Attacks .....</b>	<b>20</b>
IP Datagram.....	20
Packet Replay .....	20
Packet Tampering.....	21
Send.....	21
<b>Instance Configuration .....</b>	<b>22</b>
Real Traffic Endpoint .....	22
Network.....	22
Packet Delivery .....	23
Display windows in a frame .....	23
Start.....	23
Exit.....	23
<b>IP Traffic Monitor .....</b>	<b>24</b>
IP Datagram.....	24
Network Data .....	24

<b>Network Traffic Generator .....</b>	<b>26</b>
Packet Delivery .....	26
Ping Request.....	26
Trace.....	27
<b>Main Window .....</b>	<b>28</b>
Traffic Monitors.....	28
Policies and Associations.....	29
Generate Traffic .....	29
Attacks.....	29
Help .....	29
Exit.....	29
<b>Protected Traffic Monitor (Incoming) .....</b>	<b>30</b>
Anti-Replay Window .....	30
ESP .....	30
AH .....	30
Protected Traffic (Incoming) .....	31
Protected Traffic Statistics (Incoming) .....	32
<b>Protected Traffic Monitor (Outgoing) .....</b>	<b>33</b>
ESP .....	33
AH .....	33
Protected Traffic (Outgoing) .....	33
Protected Traffic Statistics (Outgoing) .....	34
<b>Security Policy Database/Security Association Database .....</b>	<b>36</b>
Security Policy Database .....	36
Security Association Database .....	38
<b>UDP Traffic Monitor .....</b>	<b>41</b>
UDP Packet .....	41
Network Data .....	41

## Preface

---

This document describes IPsecLite.

### Intended Audience

This document is intended for educators and students with interest in teaching and learning network security concepts, especially, those pertaining to the Internet Security Protocol (IPsec).

### Where to Go for More Information

For information on IPsecLite application, updates, technical issues, and other you may visit IPsecLite's web page at <http://www.adabtek.com/IPsec/IPsecLite/IPsecLite.aspx>.

### Revision History

Revision history for this document.

Table 1. Revision History

Date	Description
04/01/2010	Complete revision.

## System Requirements

---

The minimum hardware and software requirements for IPsecLite are:

- Microsoft Windows XP<sup>1</sup> Home Edition with SP2
- Microsoft .NET Framework 3.5
- A Network Interface Card (NIC)
- An IP address for each instance of IPsecLite
- An available port (8088 by default)
- About 2 GB of free disk space

---

*You may run multiple instances of IPsecLite on the same system provided that the IP address requirement is met. In an environment where obtaining static IP addresses are not feasible, you can choose to run IPsecLite instances on multiple systems (virtual or physical). Using multiple systems may also provide better teaching/learning experience.*

---

---

<sup>1</sup> Microsoft Windows® is registered trade mark of Microsoft Corporation.

## Installation

---

IPsecLite is a standard Microsoft Windows desktop application. To install IPsecLite simply launch the setup program (setup.exe) and follow the instructions on the screen.

Similarly, to uninstall IPsecLite use the **Add/Remove Programs** in Microsoft Windows XP (**Programs and Feature** in Microsoft Windows Vista) in the Control Panel.

## Using IPsecLite

To assist you with getting started with IPsecLite and demonstrate for you the capabilities of IPsecLite three tutorials are provided in this section. These tutorials use the network in Figure 1.

Tutorial	Description
Emulating a Network	Shows how to use multiple instances of IPsecLite to emulate a network.
Establishing a Protected Tunnel	Shows how to build a tunnel to protect traffic between two gateways in the emulated network.
Simulating Attacks	Shows how to use IPsecLite to simulate attacks and shows IPsec mechanisms to protect against the attacks.

*IPsecLite features are not limited to the demonstrations in the above tutorials. For a more comprehensive approach to use IPsecLite refer to "IPsecLite: A Tool for Teaching Security Concepts (The 41<sup>st</sup> Technical Symposium on Computer Science Education, SIGCSE 2010, Milwaukee, WI, USA)".*

In this network IPsec is used to establish a *protected tunnel* between two gateways **G1** and **G2**. This tunnel protects ALL communications between the two gateways which includes the traffic between hosts **G1H1** and **G2H1**.

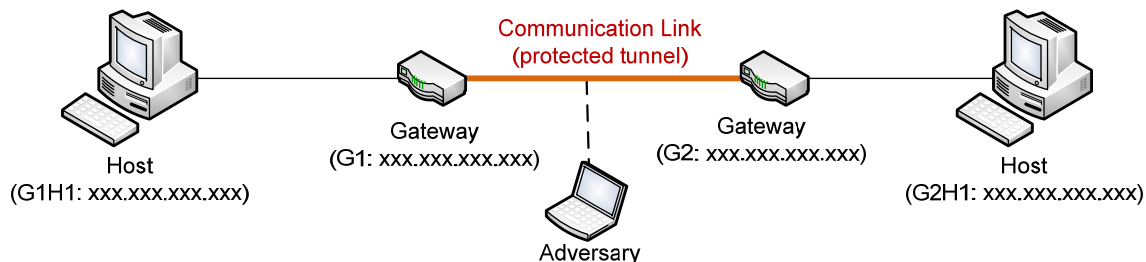


Figure 1. The network used in IPsecLite tutorials

For simplicity this guide assumes that one system is used to implement the network and the NIC is bound by 4 IP addresses.

The IP addresses that are used in tutorials are shown in the following table.

Table 2. Nodes and IP addresses for sample network used in IPsecLite tutorials

Node	Type	IP Address	Gateway/Peer Gateway	Gateway/Peer Gateway IP Address
G1H1	Host	192.168.0.82	G1	192.168.0.81
G1	Gateway	192.168.0.81	G2	192.168.0.91
G2	Gateway	192.168.0.91	G1	192.168.0.81
G2H1	Host	192.168.0.92	G2	192.168.0.91



## Tutorial 1: Emulating the Network

This tutorial helps you learn how to emulate a network consisting of two node types: hosts and gateways. It also shows you how to use IPsecLite tools to send a message from one node to another and how to inspect the corresponding IP datagram along its path to the destination of the message.

---

*To emulate the network in Figure 1 four instances of IPsecLite are used. Each instance requires a unique IP address. The IP address requirement may be fulfilled by using 4 IP addresses on the system, launching IPsecLite on four different systems (virtual or physical), or other combination.*

---

### Configuring Hosts and Gateways

Use **Instance Configuration** window to configure a host. This window is automatically displayed after an instance of IPsecLite is launched. Referring to Table 2, there are two hosts to configure, **G1H1** and **G2H1**.

**Step 1:** To configure an instance of IPsecLite to represent host **G1H1**, launch an instance of IPsecLite. Using **Instance Configuration** window and Table 2, configure **G1H1** as shown in Figure 2. Then, click on **Start** button. The **Main Window** for host **G1H1** is displayed (Figure 3). **IP Traffic Monitor** window is launched within this window by default.

---

*The title bar of each window includes instance configuration information. When multiple IPsecLite instances are running on the same system, this information allows you distinguish between each instance.*

---

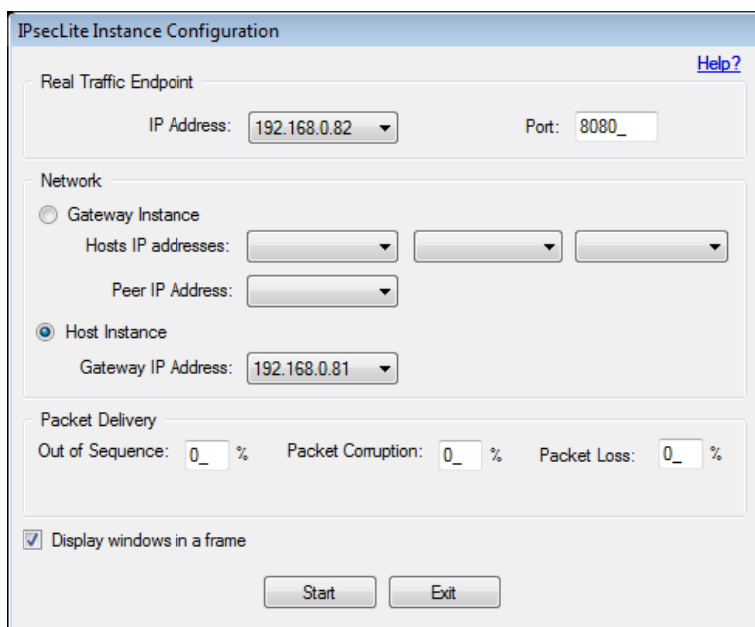


Figure 2. Configuring host G1H1

**Step2:** To configure gateway **G1** launch another IPsecLite instance. Using the information in Table 2 and **Instance Configuration** window, configure **G1** as shown in Figure 4. Then, click on the **Start** button.

**Step 3:** Launch two more instances and configure **G2H1** and **G2**.

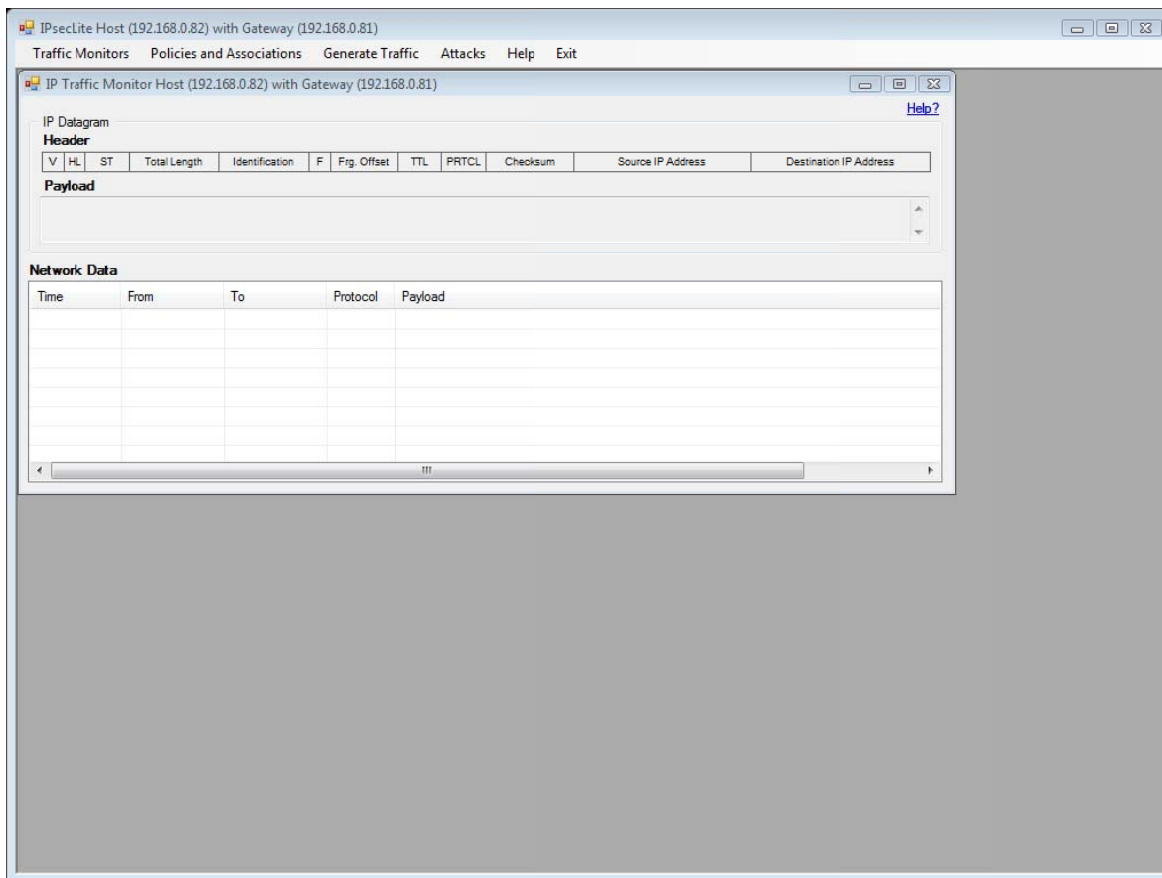
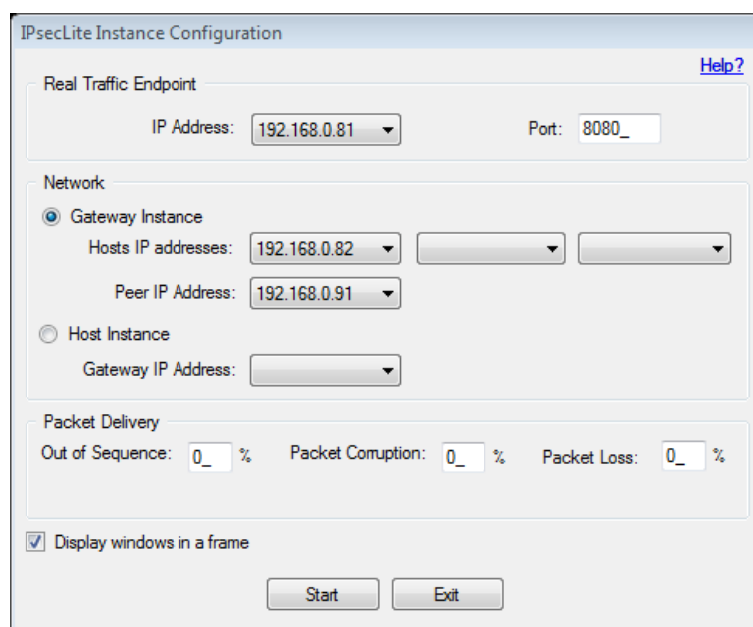


Figure 3. Main window for G1H1



#### Figure 4. Configuring gateway G1

## Testing the Network

Use **Network Traffic Generator** to send a message from **G1H1** to **G2H2** and use **IP Traffic Monitor** to verify the communication.

**Step 1:** In **G1H1** instance select **Generate Traffic** → **ICMP Ping** from the main menu. **Network Traffic Generator** window is displayed.

**Step 2:** Enter **G2H1**'s IP address in **Address** textbox and a message in **Data** textbox and click on **Send** button (Figure 5).

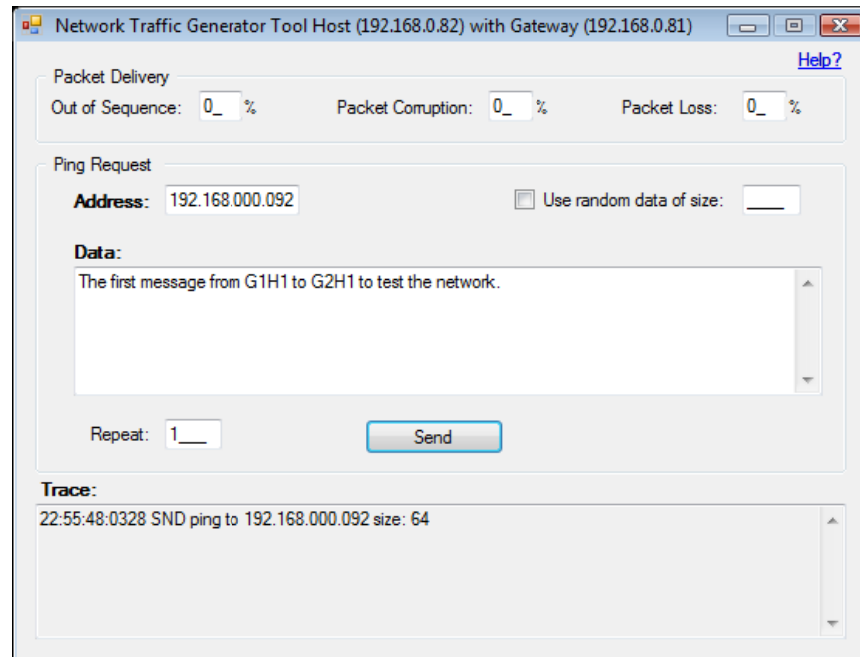


Figure 5. Network Traffic Generator on G1H1

**Step 3:** In **G1H1** instance use **IP Traffic Monitor** to verify that the message was send out (Figure 6).

---

*To inspect an IP datagram, you can select the datagram in the **Network Data** list by clicking on the list item that corresponds to it, then, review its elements in the **IP Datagram** section.*

---

**Step 4:** In **G1** instance use **IP Network Monitor** to verify that the message reached **G1** and that it was routed to **G2** (Figure 7).

---

*Letter "R" in **Send To** column indicates that the datagram was routed. The next item shows the destination address of the routed datagram (**G2** in this tutorial).The list is sorted in reverse chronological order.*

---

**Step 5:** Use **IP Network Monitor** on **G2** and **G2H1** to verify that the message reached **G2H1**.

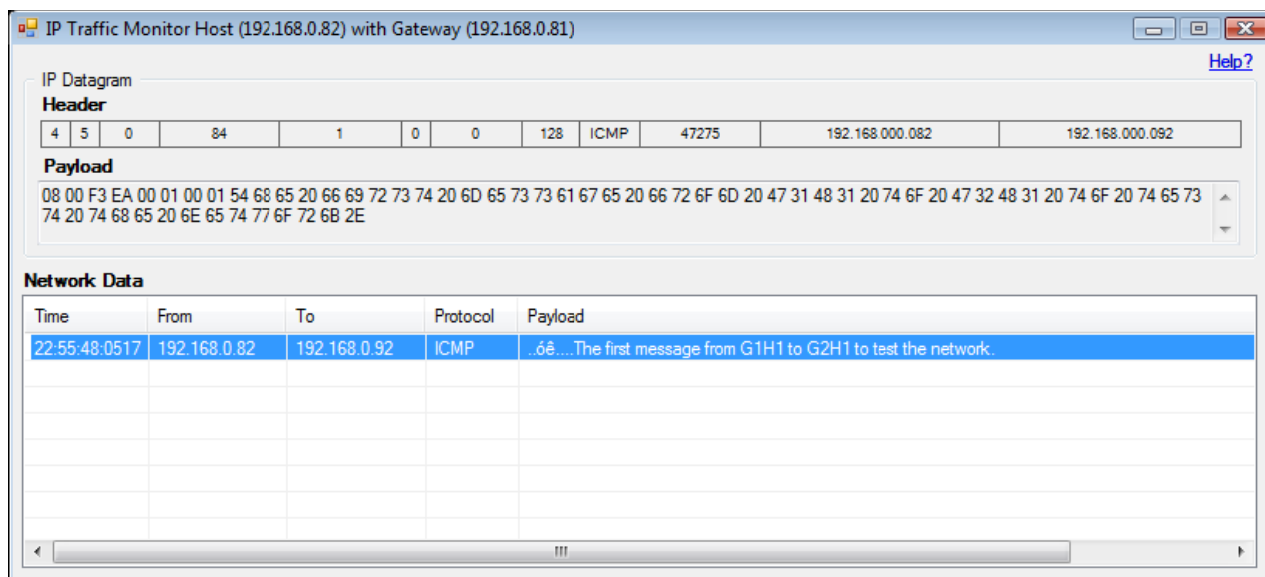


Figure 6. IP Traffic Monitor on G1H1 after sending the first message to G2H1

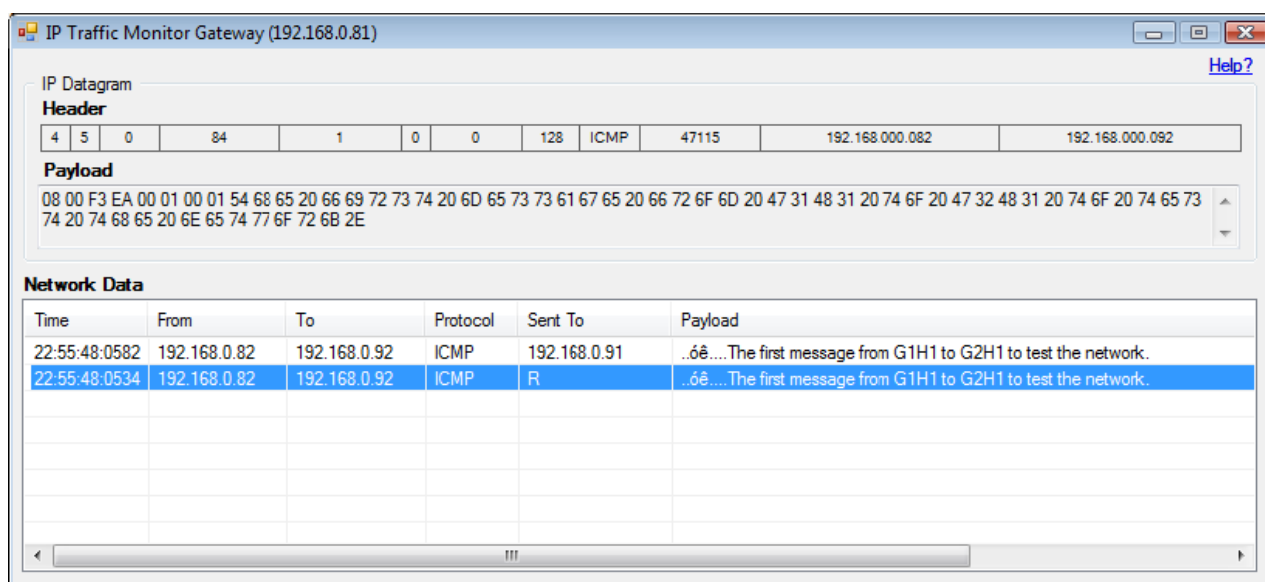


Figure 7. IP Traffic Monitor on G1 after sending the first message to from G1H1 to G2H1

## Tutorial 2: Establishing a Protected Tunnel

Use **Security Policy Database/Security Association Database** window to establish a protected communication channel (tunnel) between gateways **G1** and **G2**. Establishing a protected connection between two nodes involves two tasks: defining protection rules (security policies) and establishing Security Associations (protected connections) (SAs).

### Defining Protection Rules

Configure security policy database (SPD) with a rule to protect the all traffic between **G1** and **G2** using **ESP** protocol in tunnel mode.

**Step 1:** In **G1** instance select **Security Policy Database/Security Association Database**.

**Step 2:** Enter **G2's** IP address in **Destination IP** textbox, select **ESP** from **Protocol** combo box, and select **Tunnel** from **Mode** combo box. Leave the other items unchanged and click on **Add/Update** button.

**Step 3:** Review and verify the rule in the **Security Policy Rules** list (Figure 8).

---

*To update a rule simply re-enter the rule and click on Add/Update button.*

---

The screenshot shows the 'Security Policy Database/Security Association Database Gateway (192.168.0.81)' window. The 'Security Policy Rule' section is active, displaying the following configuration:

- Source IP: 192.168.0.81
- Destination IP: 192.168.0.91
- Application: ANY
- Protocol: ESP
- Confidentiality: AES-CBC-128
- Data Integrity: HMAC-SHA1-96
- PRF: HMAC-SHA1
- DH Group: GROUP 14: 2048 BIT MODP
- Mode: Tunnel
- ESP Integrity Check: ☒

The 'Add/Update' button is highlighted. Below this, the 'Security Policy Rules' table shows the configured rule:

Destination IP	SPI	Applicat...	Mode	Protocol	Confidentiality	Data Integrity	PRF	DH Group
192.168.0.91		ANY	TUNNEL	ESP	ENCR_AES_CBC (128)	AUTH_HMAC_SHA1_...	PRF_HMAC_SHA1	GROUP5_2048BIT_M...

At the bottom of the window, there are 'Connect' and 'Disconnect' buttons.

Figure 8. Security Policy Database after adding a rule to protect the traffic between G1 and G2

## Establishing Security Associations

Start the Internet Key Exchange (IKE) message exchanges to establish four SAs.

**Step 1:** Select the rule created in previous step by clicking on the corresponding list item in **Security Policy Rules** list.

**Step 2:** Click on **Connect** button to start IKE message exchanges. IPsecLite will switch to **Security Association Database** window (Figure 9).

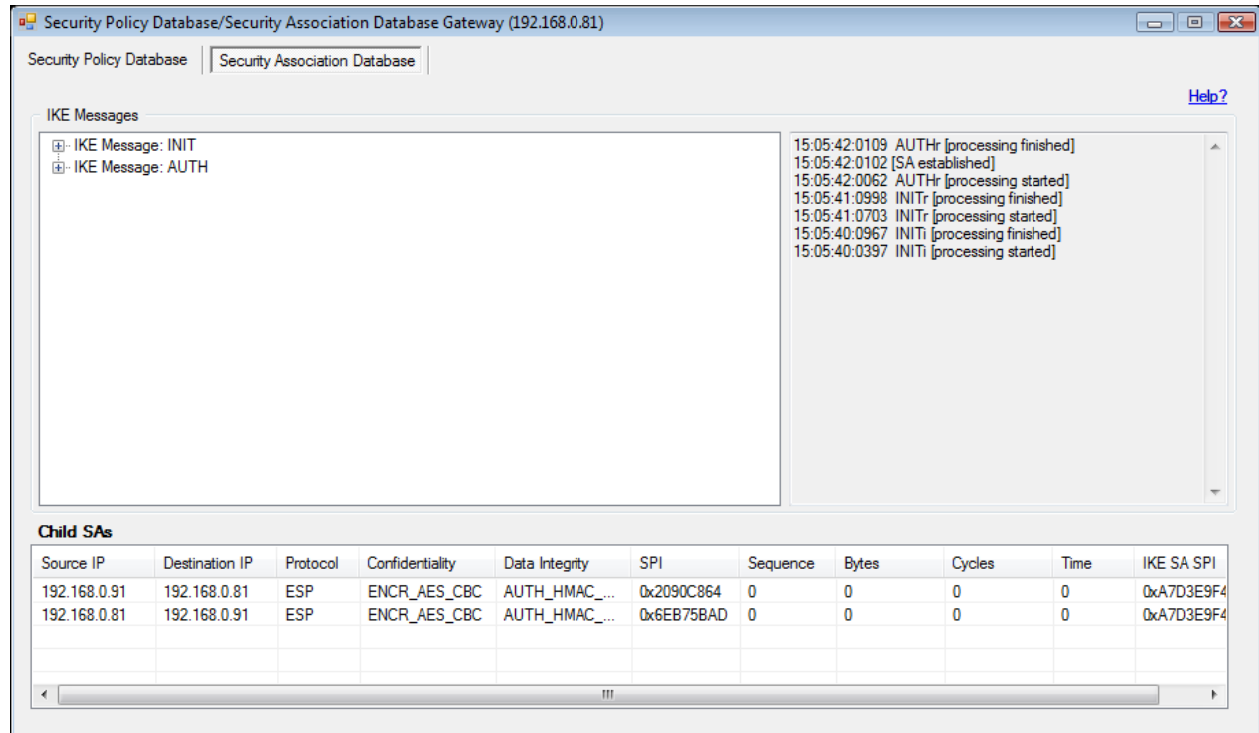


Figure 9. Security Association Database window after successful IKE message exchanges to establish SAs

**Step 3:** Upon successful completion of IKE message exchanges, expand the nodes associated with IKE messages in **IKE Message** section and inspect the **INIT** and **AUTH** messages.

**Step 4:** Verify that two CHILD\_SAs were created. **Child SAs** list should contain two items corresponding to two CHILD\_SAs.

**Step 5:** Verify that two IKE\_SAs were created. **IKE SA SPI** column in **Child SAs** list must contain the Security Parameter Index (SPI) for initiator IKE\_SA. Similarly, this column on **G2** instance must contain an SPI for responder IKE\_SA.

## Verifying Traffic Protection

Send a message from **G1H1** to **G2H1** and verify that the corresponding datagrams between **G1** and **G2** are protected. Also, use the **Protected Traffic (Outgoing)** and **Protected Traffic (Incoming)** windows on **G1** and **G2**, respectively, to examine the protected packets.

**Step 1:** Repeat the steps in Testing the Network subsection (Page 11) to send a message from **G1H1** to **G2H1** and verify that communication between **G1** and **G2** is protected (use **IP Traffic Monitor** on **G1** and **G2** and observe that the content of IP datagram is not in plain-text).

**Step 2:** In **G1** instance select **Traffic Monitors** → **Protected Traffic Monitor (Outgoing)**.

**Step 3:** Send a message from **G1H1** to **G2H1**.

**Step 4:** In **G1** instance view the content of **Protected Traffic (Outgoing)** list on **Protected Traffic Monitor (Outgoing)** window. Click on the list item (ESP packet) and review the details of the ESP packet in **ESP** section of the window (Figure 10).

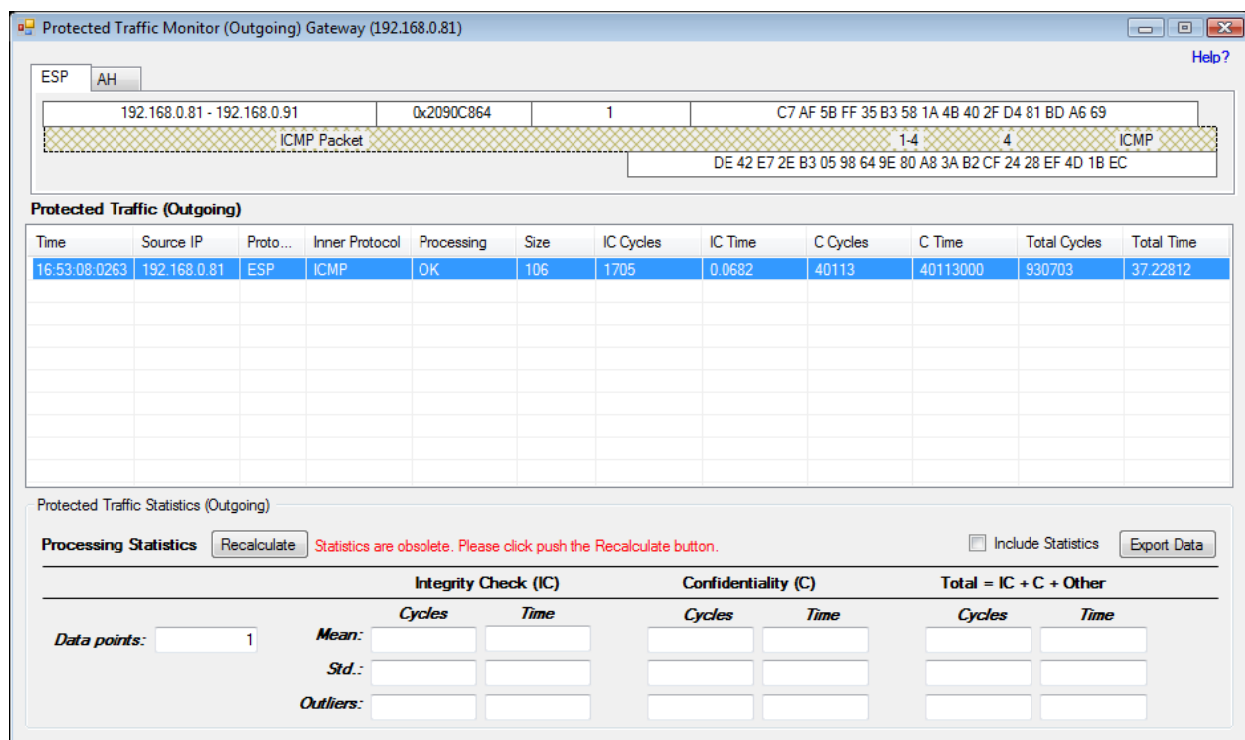


Figure 10. Protected Traffic Monitor (Incoming) in G1 after sending a message from G1H1 to G2H1

**Step 5:** In **G2** instance select **Traffic Monitors** → **Protected Traffic Monitor (Incoming)**.

**Step 6:** Send a message from **G1H1** to **G2H1**.

**Step 7:** In **G2** instance view the content of **Protected Traffic (Incoming)** list on **Protected Traffic Monitor (Incoming)** window. Click on the list item (ESP packet) and review the details of the ESP packet in **ESP** section of the window (Figure 11).

**Step 8:** Review the content of **Anti-Replay Window**. Note that **G2** has received two protected packets so far.

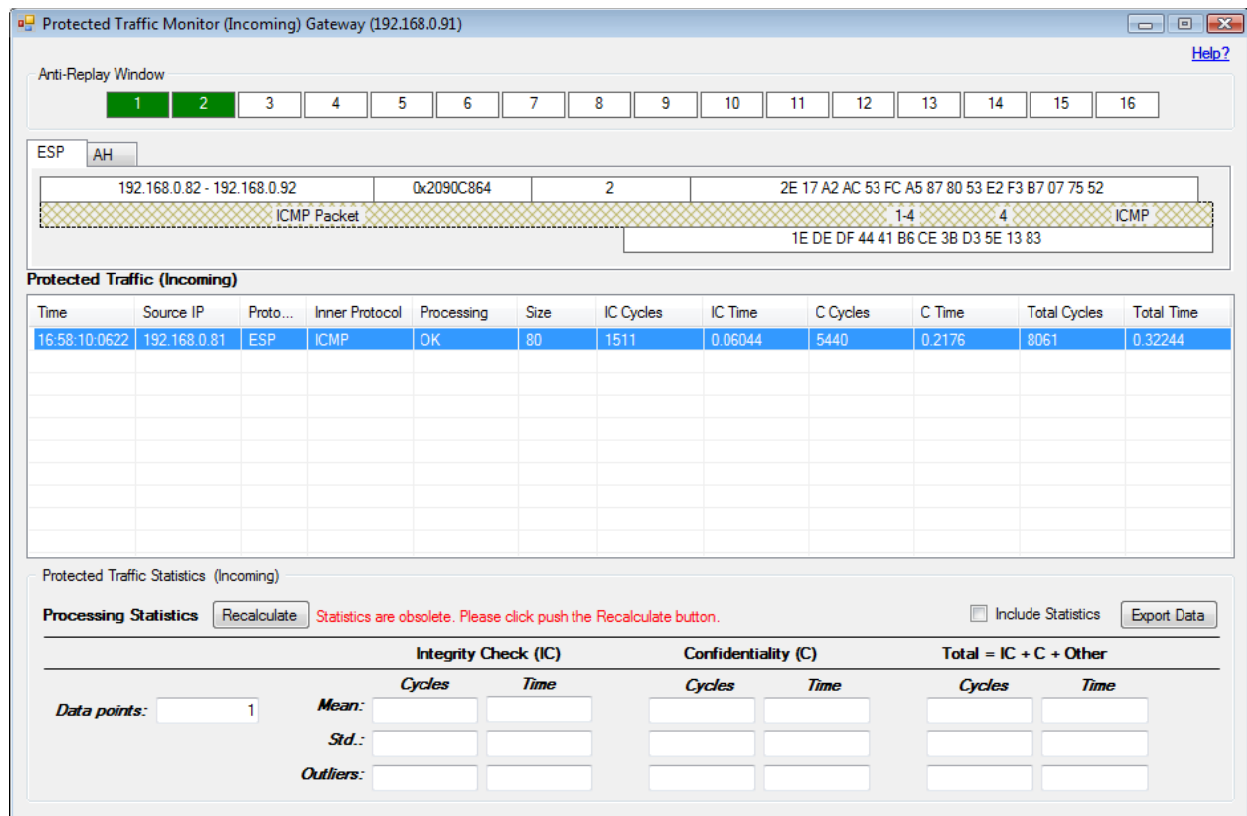


Figure 11. Protected Traffic Monitor (Incoming) on G2 after sending the second message from G1H1 to G2H1



## Tutorial 3: Simulating Attacks

Use **Attacks Simulator** to capture an outgoing IP datagram and resend it to its destination. Depend on what attack to simulate you may change the datagram. Below are the steps to simulate packet-replay and spoofing attacks.

---

*Close all instances of IPsecLite that you used in previous tutorials.*

---

**Step 1:** Launch two IPsecLite instances to emulate **G1** and **G2** listed in Table 2, and establish a protected tunnel between **G1** and **G2**.

**Step 2:** In **G1** instance select **Attacks** → **Packet Replay**. **Attacks Simulator** window is displayed.

**Step 3:** In **G2** instance select **Traffic Monitors** → **Protected Traffic Monitor (Incoming)**.

**Step 4:** Send a message from **G1** to **G2**.

**Step 5:** Observe that the outgoing packet is captured in the **Attack Simulator** window (Figure 12).

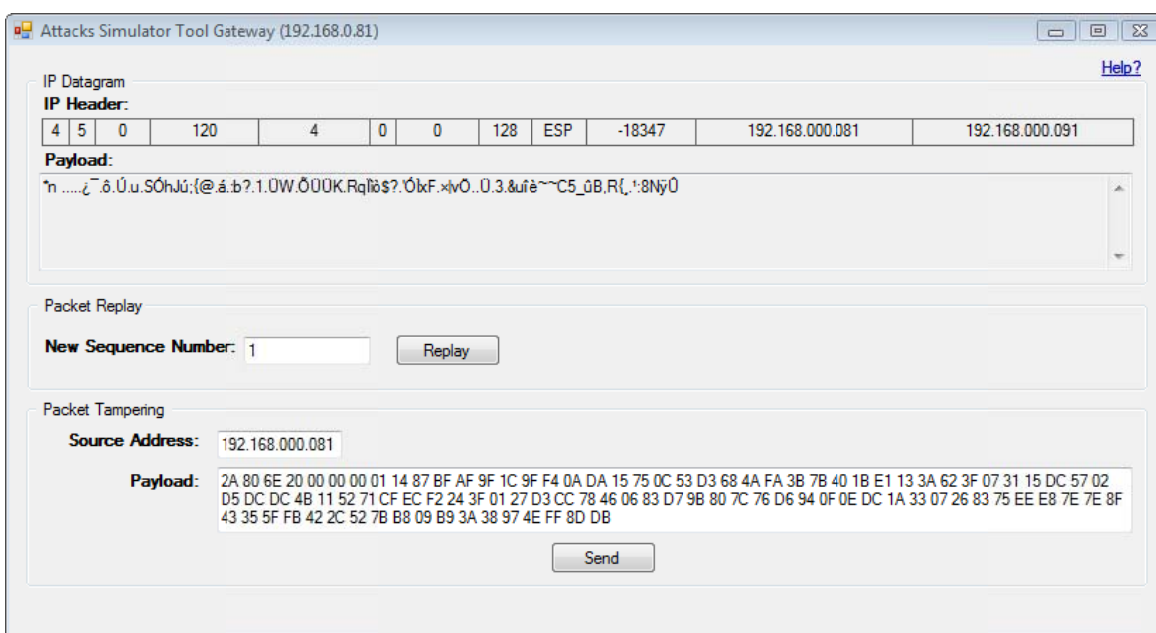


Figure 12. Attacks Simulator window in **G1** instance after sending a message to **G2**

**Step 6:** Verify that the packet arrived at **G2** (use **Protected Traffic Monitor (Incoming)** in **G2** instance).

**Step 7:** In **G1** instance click on **Replay** button in **Attacks Simulator** window to resend the packet.

**Step 8:** In **G2** instance review the content of **Protected Traffic Monitor (Incoming)** window (Figure 13).

**Step 9:** Enter **2** in **New Sequence Number** textbox in **Attacks Simulator** window (**G1** instance), change the IP address in **Source Address** textbox, and click on **Send** button.

**Step 10:** In **G2** instance review the content of **Protected Traffic Monitor (Incoming)** window.

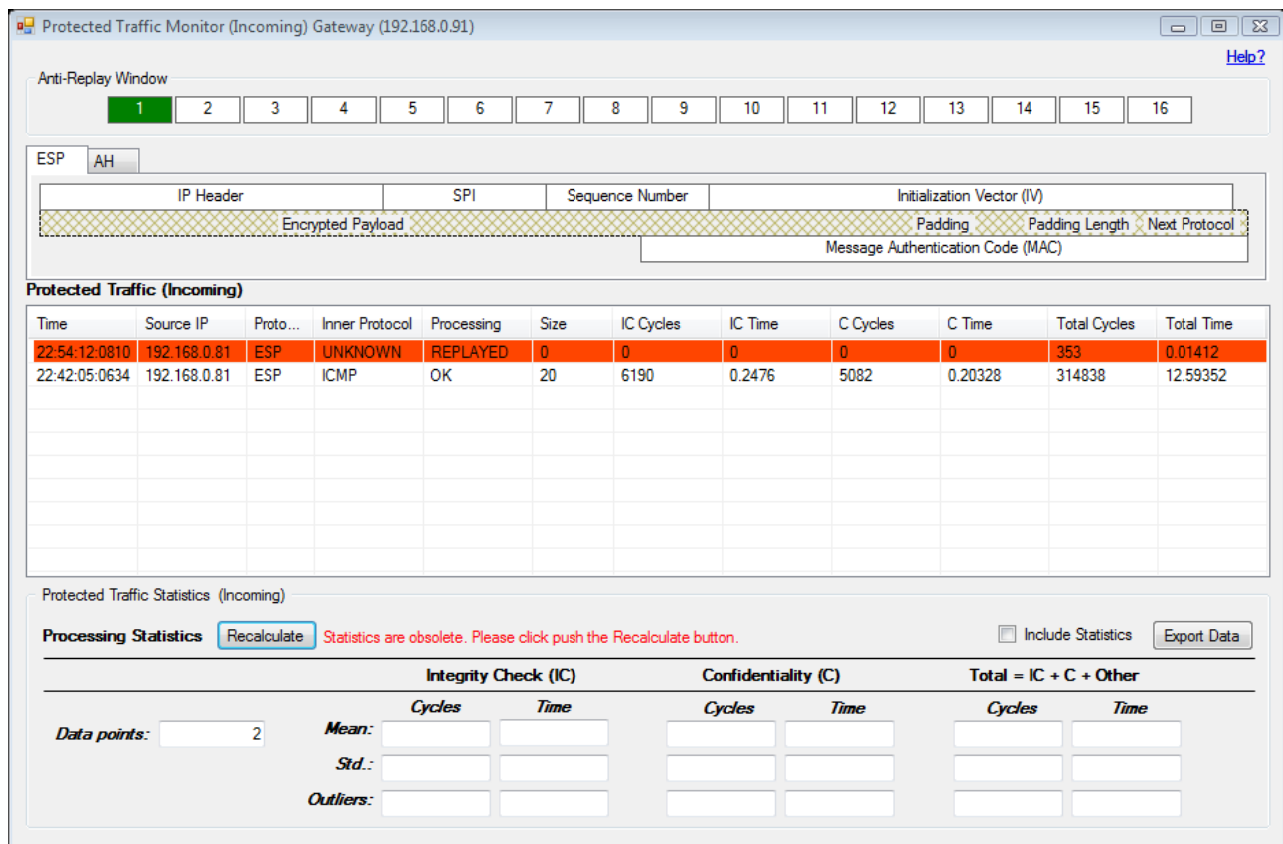


Figure 13. Protected Traffic Monitor (Incoming) in G2 instance after receiving a replayed packet

## Complete Reference

---

This chapter contains references for all IPsecLite tools, functions, and features. The main sections of this reference are organized in alphabetical order.

## Attacks

**Attacks Simulator** (Figure 14) is used to simulate *packet replay* attacks and *packet tampering* attacks. This window captures outgoing IP datagrams.

Attacks Simulator Tool Host (192.168.0.81) with Gateway (192.168.0.82)

IP Datagram [Help?](#)

IP Header:

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

Payload:

Packet Replay

New Sequence Number:

Packet Tampering

Source Address:

Payload:

Figure 14. Attacks Simulator

### IP Datagram

This section shows an outgoing IP datagram.

#### IP Header

Header of the latest outgoing IP datagram.

#### Payload

Payload of the latest outgoing IP datagram in network byte order.

### Packet Replay

Use this section to simulate a *packet replay* attack.

#### New Sequence Number

The sequence number that should be used to replay a protected packet. This textbox shows the sequence number of the latest outgoing protected packet.

#### Replay

Causes the replay of the latest outgoing protected packet.

## Packet Tampering

Use this section to simulate a *packet tampering* attack such as a *spoofing attack*.

### *Source Address*

Source IP address that should be used to resend an IP datagram whose payload includes the latest outgoing protected packet.

### *Payload*

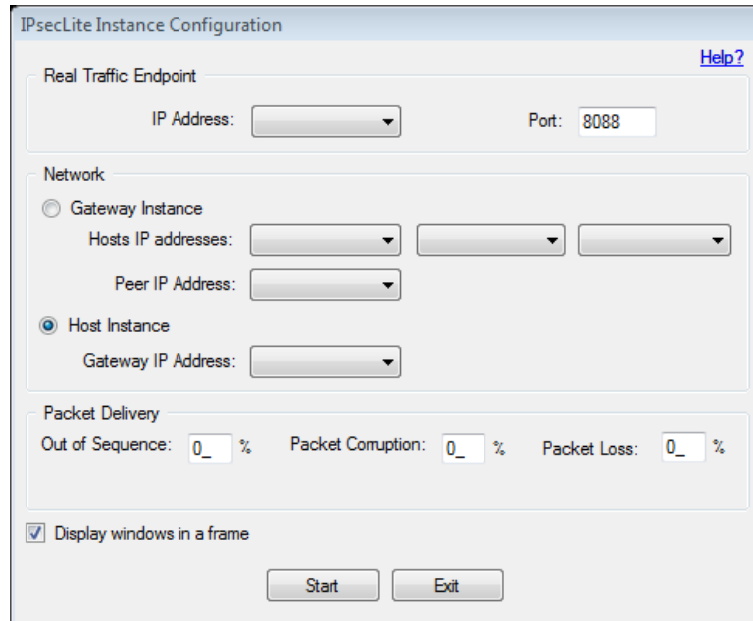
The payload for the IP datagram to be resent.

### **Send**

Button to use to resend the IP datagram.

## Instance Configuration

**Instance Configuration** window (Figure 14) is used to configure one IPsecLite instance to emulate one node in a network. Each instance can be configured to represent a Host or a Gateway.



The figure shows a software window titled "IPsecLite Instance Configuration". It contains several sections: "Real Traffic Endpoint" with fields for "IP Address" (a dropdown menu) and "Port" (a text box containing "8088"); "Network" with two radio buttons, "Gateway Instance" and "Host Instance" (the latter is selected), and associated IP address fields; "Packet Delivery" with three percentage fields for "Out of Sequence", "Packet Corruption", and "Packet Loss", all set to "0\_"; and a checked checkbox for "Display windows in a frame". At the bottom are "Start" and "Exit" buttons. A "Help?" link is in the top right corner.

Figure 15. Instance Configuration

### Real Traffic Endpoint

Use this section to define a communication end-point that an IPsecLite instance must use for communication with other IPsecLite instances.

#### IP Address

The end-point's IP address.

#### Port

The end-point's port number.

---

*Communicating IPsecLite instances must use the same port number. Also, firewalls must be configured to allow for this communication.*

---

### Network

Use this section to select the role of a node in the network (Host or Gateway) and to configure other nodes that are directly linked to it.

#### Gateway Instance

Select this option to configure an IPsecLite instance as a gateway. A gateway instance must be linked to another gateway and, at least, one host.

## Hosts IP Addresses

IP addresses for hosts, represented by other IPsecLite instances, which are directly linked to the current gateway.

---

*Each IP address can be associated with only one instance that represents a node in the network.*

---

## Peer IP Address

IP address of a gateway, represented by another IPsecLite instance, which is directly linked to the current gateway.

## Host Instance

Select this option to configure an IPsecLite instance as a host. A host must be linked to a gateway.

## Gateway IP Address

IP address of the gateway, represented by an IPsecLite instance, to which this host is directly linked.

## Packet Delivery

Use this section to control the behavior of the emulated network environment.

### Out of Sequence

A number between 0 and 99 and defines percentage of packets that are delivered out-of-sequence.

### Packet Corruption

A number between 0 and 99 and defines percentage of the packets that are corrupted during transmission.

### Packet Loss

A number between 0 and 99 and defines percentage of the packets that are lost during transmission.

## Display windows in a frame

When this checkbox is checked IPsecLite tools are contained within the **Main** window (Figure 17). When the checkbox is not checked the tool windows can be freely moved around.

## Start

Starts the IPsec instance.

## Exit

Aborts the configuration and exits the instance.

## IP Traffic Monitor

Use **IP Traffic Monitor** (Figure 15) to monitor incoming and outgoing IP datagrams related to the current instance of IPsecLite.

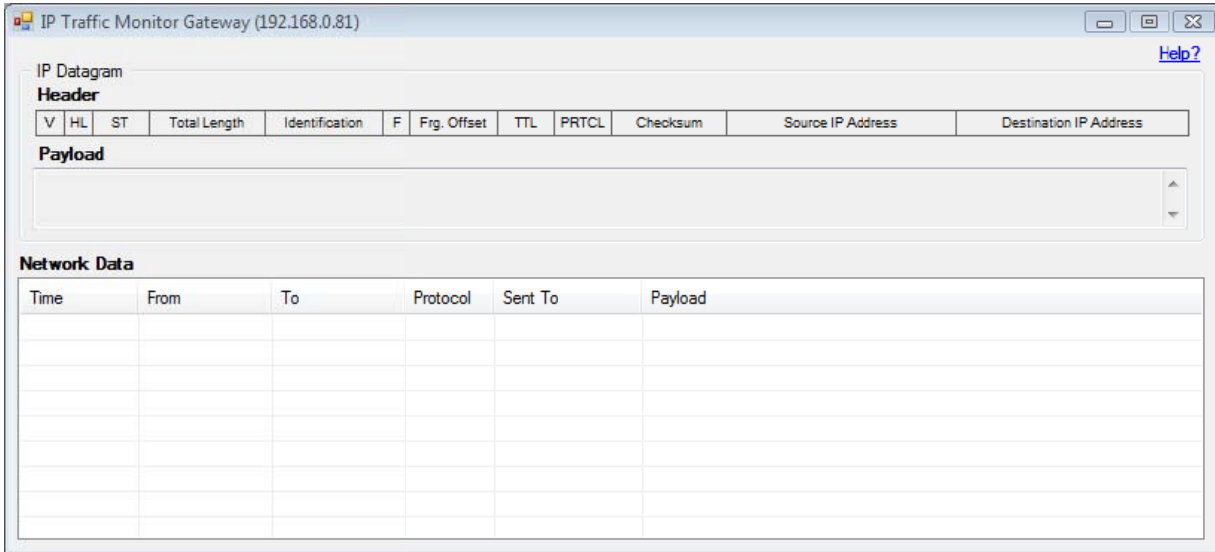


Figure 16. IP Traffic Monitor

### IP Datagram

Use this section to visualize an IP datagram and to view its payload in network byte order.

---

*To visualize an IP datagram select it from the **Network Data** list by clicking on the corresponding list item.*

---

#### Header

IP datagram header.

---

*When an IP datagram is selected this section shows the corresponding values in the selected IP datagram.*

---

#### Payload

IP datagram payload in network byte order.

#### Network Data

Shows the list of incoming and outgoing IP datagrams in reverse chronological order.

#### Time

Arrival or departure time of IP datagrams.



***From***

Source address of IP datagrams.

***To***

Destination address of IP datagrams.

***Protocol***

Packet types of the encapsulated packets.

***Send To***

Shows if the IP datagrams are routed.

---

*This column is only available IPsecLite instances configured as gateway. A routed IP datagram is indicated by "R" and the next row shows the IP address of the gateway receiving the datagram (the peer gateway).*

---

***Payload***

IP datagram payloads.

## Network Traffic Generator

Use Network Traffic Generator (Figure 16) to generate and send messages to other nodes in the network.

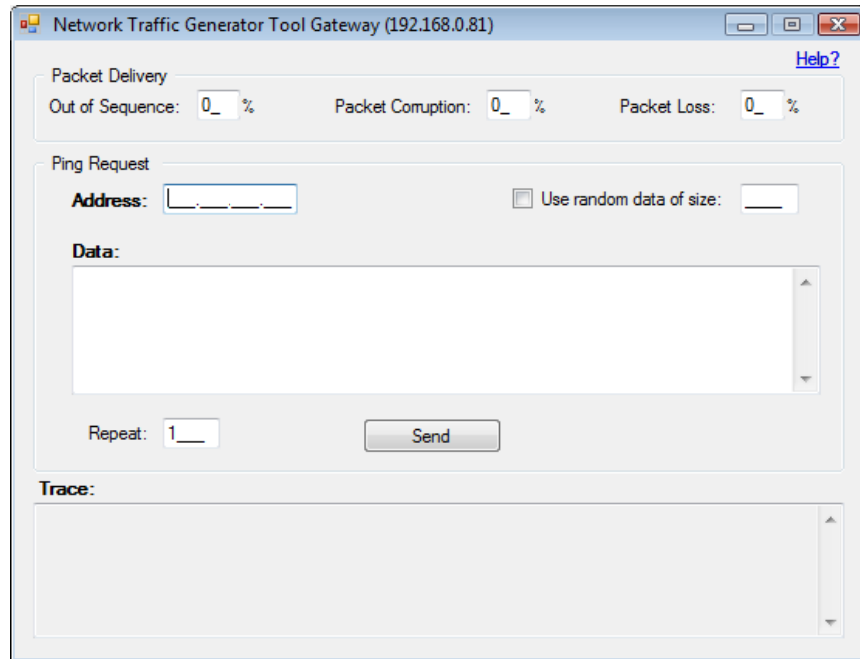


Figure 17. Network Traffic Monitor

### Packet Delivery

Use this section to control the behavior of the emulated network environment.

#### *Out of Sequence*

A number between 0 and 99 and defines percentage of packets that are delivered out-of-sequence.

#### *Packet Corruption*

A number between 0 and 99 and defines percentage of the packets that are corrupted during transmission.

#### *Packet Loss*

A number between 0 and 99 and defines percentage of the packets that are lost during transmission.

### Ping Request

Use this section to send messages to other instances. Messages are formatted using ICMP Ping request.

#### *Address*

Destination IP address for messages.

### *Use random data of size*

Check this checkbox to generate random data of specified size.

### *Data*

Data to use as the payload of the Ping request.

### *Repeat*

Number of times the message must be sent.

### *Send*

Click on this button to send the message(s).

### *Trace*

Log of messages that were sent.

## Main Window

Upon configuring an IPsecLite instance the **Main Window** (Figure 17) is displayed.

---

When **Display window in a frame** (page 23) checkbox is checked, this window functions as a container for displaying IPsecLite tools.

---

Use the menu bar in the **Main Window** to access different tools.

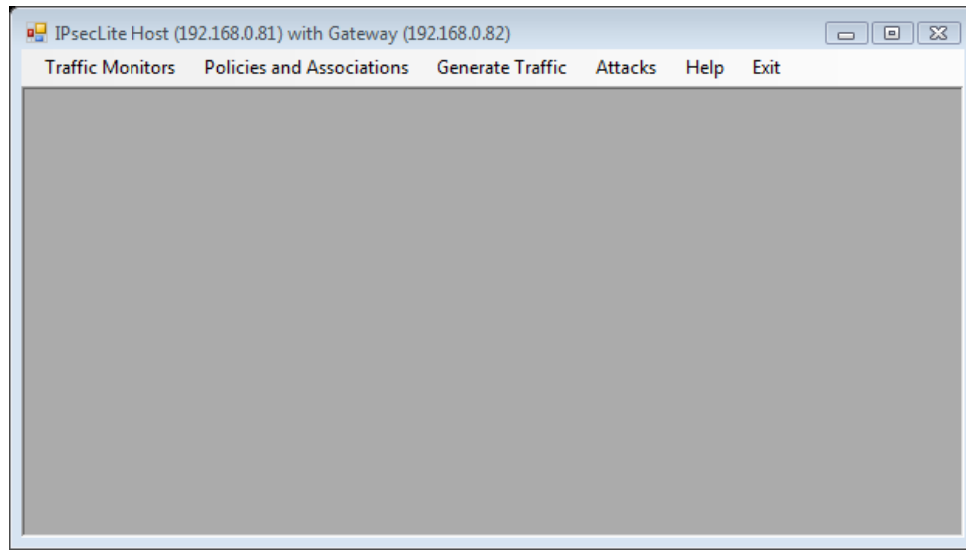


Figure 18. Main Window

### Traffic Monitors

Use this menu item to access a set of network traffic monitoring tools.

#### *IP Datagrams*

Use this menu item to access **IP Traffic Monitor** (Page 24) for monitoring the incoming and outgoing IP datagrams.

#### *UDP Packets*

Use this menu item to access **UDP Traffic Monitor** (Page 41) for monitoring the incoming and outgoing UDP packets.

#### *Protected Packets (Incoming)*

User this menu item to access **Protected Traffic Monitor (Incoming)** (Page 30) for monitoring incoming protected (ESP and AH) packets.

#### *Protected Packets (Outgoing)*

Use this menu item to access **Protected Traffic Monitor (Outgoing)** (Page 33) for monitoring outgoing protected (ESP and AH) packets.

## Policies and Associations

Use this menu item to access **Security Policies/Security Associations** (Page 36) for managing security policies and security associations.

## Generate Traffic

Use this menu item to access a set of tools for generating network traffic<sup>2</sup>.

### ICMP

Use this menu item to access **Network Traffic Generator** (Page 26) for sending messages to other nodes in the network.

## Attacks

Use this menu item to access a set of tools for simulating network attacks.

### Packet Replay

Use this menu item to access **Attacks Simulator** (Figure 14) for simulating a packet replay attack.

### Packet Tampering

Use this menu item to access **Attacks Simulator** (Figure 14) for simulating attacks that are based on modifications to authentic packets and resending them to their destinations.

## Help

Use this menu item to access help features and to access **About** IPsecLite page.

### Online Help

Use this menu item to go to IPsecLite support page on the web.

### Home Page

Use this menu item to go to the IPsecLite's home page on the web.

### About

Use this menu item to launch the about page.

## Exit

Use this menu item to end an instance and exit.

---

*It is strongly recommended that you use the Exit menu item to exit IPsecLite. Failing to do so may cause the instance to stay resident in the memory.*

---

---

<sup>2</sup> Current version of IPsecLite supports only one packet format (ICMP) at this time.

## Protected Traffic Monitor (Incoming)

Use **Protected Traffic Monitor (Incoming)** (Figure 18) to monitor and view the incoming protected packets and collect detailed data on overhead of IPsec services.

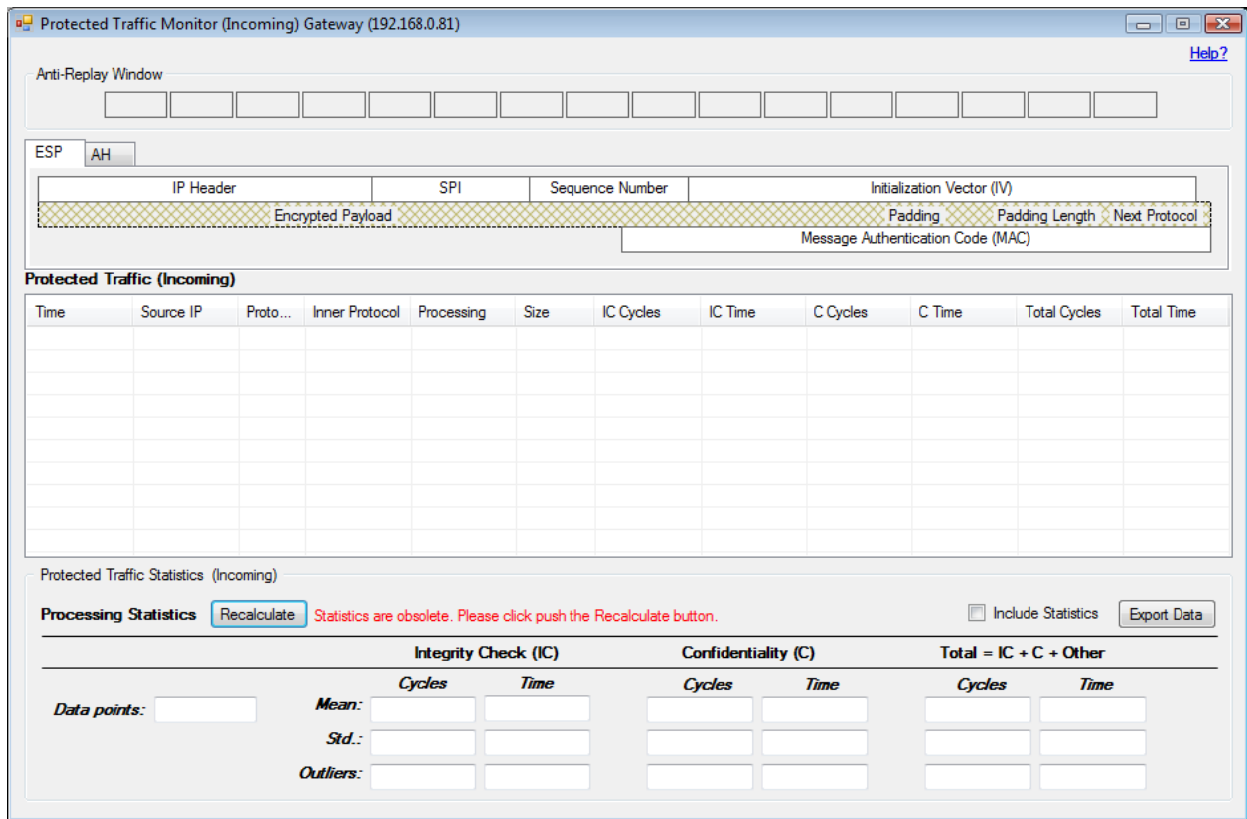


Figure 19. Protected Traffic Monitor (Incoming)

### Anti-Replay Window

This window of size 16 shows, in green, the protected packets that have already arrived. Each element of the window corresponds to a protected packet identified by its sequence number.

### ESP

Use this section to view the elements of a packet protected by ESP protocol.

*To view the elements of a protected packet you need to select it from the **Protected Traffic (Incoming)** list by clicking on the corresponding list item.*

### AH

Use this section to view the elements of a packet protected by AH protocol.

*To view the elements of a protected packet you need to select it from the **Protected Traffic (Incoming)** list by clicking on the corresponding list item.*

## Protected Traffic (Incoming)

This list view shows a list of incoming protected packets in reverse chronological order.

### *Time*

Arrival times of incoming protected packets.

### *Source IP*

Source addresses of incoming protected packets.

### *Protocol*

Protocols used to protect packets.

### *Inner Protocol*

Packet type of packets encapsulated in payload of protected packets.

### *Processing*

IPsec processing results as listed in the following table.

**Table 3. Protected Packets Processing Status**

Processing	Description	Color Code
OK	Packet was successfully processed	White
INVALID_MAC	Packet was not authentic or was corrupted	Red
REPLAYED	Packet was replayed	Orange-Red
TOO_OLD	Packet did not arrive in a timely manner	Pink
INVALID_PAD	Packet did not include invalid padding	Chocolate
NO_SA	Packet was associated with no CHILD_SA for traffic protection	Coral

### *Size*

Shows the original packet sizes when processing is OK. Otherwise, shows the size of protected packets.

### *IC Cycles*

Overhead of data integrity check service in CPU cycles.

### *IC Time*

Overhead of data integrity check service in milliseconds.

### *C Cycles*

Overhead of data confidentiality service (decryption) in milliseconds.

### *C Time*

Overhead of data confidentiality service (decryption) in milliseconds.

### *Total Cycles*

Total overhead of protected packet processing in CPU cycles. This is the overhead of data integrity check service, data confidentiality service, and other operations such as maintenance of anti-replay window.

### *Total Time*

Total overhead of protected packet processing in milliseconds. This is the overhead of data integrity check service, data confidentiality service, and other operations such as maintenance of anti-replay window.

### **Protected Traffic Statistics (Incoming)**

Use this section to obtain overhead statistics.

#### *Recalculate*

Use this button to recalculate the statistics.

#### *Export Data*

Use this button to export the data in **Protected Traffic (Incoming)** list to a file.

#### *Include Statistics*

Check this checkbox to include the statistics when the data in **Protected Traffic (Incoming)** list is exported to a file.

#### *Data Points*

Number of packets in **Protected Traffic (Incoming)** list.

#### *Integrity Check (IC)*

Statistics on data integrity check processing overhead after eliminating outliers.

#### *Confidentiality (C)*

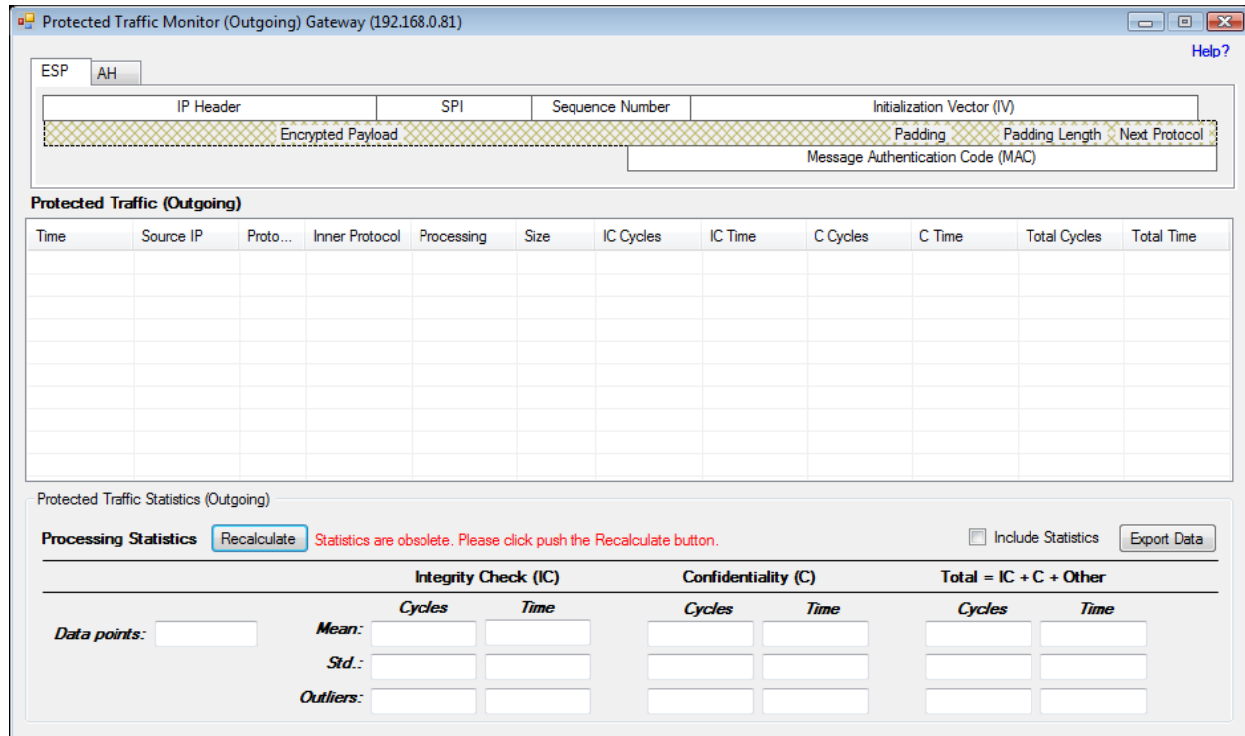
Statistics on data confidentiality processing (decryption) overhead after eliminating outliers.

#### *Total = IC + C + Other*

Statistics on total overhead of data protection services.



Use **Protected Traffic Monitor (Outgoing)** (Figure 19) to monitor and view the incoming protected packets and collect detailed data on overhead of IPsec services.



**Figure 20. Protected Traffic Monitor (Outgoing)**

ESP

Use this section to view the elements of a packet protected by ESP protocol.

To view the elements of a protected packet you need to select it from the **Protected Traffic (Outgoing)** list by clicking on the corresponding list item.

AH

Use this section to view the elements of a packet protected by AH protocol.

To view the elements of a protected packet you need to select it from the **Protected Traffic (Outgoing)** list by clicking on the corresponding list item.

### Protected Traffic (Outgoing)

This list view shows a list of outgoing protected packets in reverse chronological order.

## Time

Arrival times of incoming protected packets.

### ***Source IP***

Source addresses of outgoing protected packets.

### ***Protocol***

Protocols used to protect the packets.

### ***Inner Protocol***

Packet types of encapsulated packets.

### ***Processing***

IPsec processing results.

### ***Size***

Packet size.

### ***IC Cycles***

Overhead of data integrity check service in CPU cycles.

### ***IC Time***

Overhead of data integrity check service in milliseconds.

### ***C Cycles***

Overhead of data confidentiality service (encryption) in milliseconds.

### ***C Time***

Overhead of data confidentiality service (encryption) in milliseconds.

### ***Total Cycles***

Total overhead of protected packet processing in CPU cycles. This is the overhead of data integrity check service, data confidentiality service, and other operations such as SA lookup.

### ***Total Time***

Total overhead of protected packet processing in milliseconds. This is the overhead of data integrity check service, data confidentiality service, and other operations such as SA lookup.

### ***Protected Traffic Statistics (Outgoing)***

Use this section to obtain overhead statistics.

### ***Recalculate***

Use this button to recalculate the statistics.

### *Export Data*

Use this button to export the data in **Protected Traffic (Outgoing)** list to a file.

### *Include Statistics*

Check this checkbox to include the statistics when the data in **Protected Traffic (Outgoing)** list is exported to a file.

### *Data Points*

Number of packets in **Protected Traffic (Outgoing)** list.

### *Integrity Check (IC)*

Statistics on data integrity check processing overhead after eliminating outliers.

### *Confidentiality (C)*

Statistics on data confidentiality processing (encryption) overhead after eliminating outliers.

### *Total = IC + C + Other*

Statistics on total overhead of data protection services.

## Security Policy Database/Security Association Database

Use Security Policy Database/Security Association Database to manage security policies and security associations, including establishing and ending protected connections.

### Security Policy Database

Use **Security Policy Database** tool (Figure 20) to manage security policies and to establish or end protected connections associated with policies.

Security Policy Database/Security Association Database Gateway (192.168.0.81)

Security Policy Database | Security Association Database

Security Policy Rule

Source IP: 192.168.0.81 Destination IP: \_\_\_\_\_ Protocol: AH Confidentiality: AES-CBC-128

Application: ANY ESP Integrity Check: ☐ Data Integrity: HMAC-SHA1-96

Mode: Transport PRF: HMAC-SHA1

DH Group: GROUP 14: 2048 BIT MODP

Add

Security Policy Rules

Destination IP	SPI	Applicat...	Mode	Protocol	Confidentiality	Data Integrity	PRF	DH Group

Connect Disconnect

Figure 21. Security Policy Database

### Security Policy Rule

Use this section to define a security policy.

#### Source IP

Address of the current instance. This will be the initiator address for the corresponding protected connection.

#### Destination IP

IP address of the responder for establishing a protected connection.

#### Protocol

IPsec protocol to use to protect traffic between the initiator and responder in both directions.

### ESP Integrity Check

If checked the ESP will include integrity check service by adding a trailer (MAC) to each packet.

### Application

Type of traffic to protect.

### Mode

IPsec mode, i.e., Transport or Tunnel.

### Confidentiality

The encryption algorithm to use when ESP is selected.

### Data Integrity

The data integrity algorithm to use.

### PRF

The Pseudo-Random Function to use to compute cryptographic keys.

### DH Group

The Diffie-Helman group to use when exchanging IKE INIT messages.

## *Security Policy Rules*

List the security policy rules. This can be considered as the security policy database.

### Destination IP

IP address of the responder for establishing a protected connection.

### SPI

The Security Parameter Index of the IKE-SA associated with the corresponding rule.

### Protocol

IPsec protocol to use to protect traffic between the initiator and responder in both directions.

### ESP Integrity Check

If checked the ESP will include integrity check service by adding a trailer (MAC) to each packet.

### Application

Type of traffic that will be protected under this security policy rule.

## Mode

IPsec mode, i.e., Transport or Tunnel.

## Confidentiality

The encryption algorithm to use when ESP is selected.

## Data Integrity

The data integrity algorithm to use.

## PRF

The Pseudo-Random Function to use to compute cryptographic keys.

## DH Group

The Diffie-Helman group to use when exchanging IKE INIT messages.

## *Connect*

Use this button to start a protected connection between the instance and the instance identified by the selected security policy.

## *Disconnect*

Use this button to end the protected connection between the instance and the instance identified by the selected security policy.

## **Security Association Database**

This tool (Figure 21) shows detailed information about IKE message exchanges and security associations.

## *IKE Messages*

The section consists of two panes. The right pane provides a list of IKE message exchanges. The left page provides, in tree view format, the details of IKE message exchanges that occur between the current instance and other instances.

## *Child SAs*

Shows the CHILD\_SAs established for different protected connections.

## Source IP

Source address of the protected connection.

## Destination IP

Destination address of the protected connection.

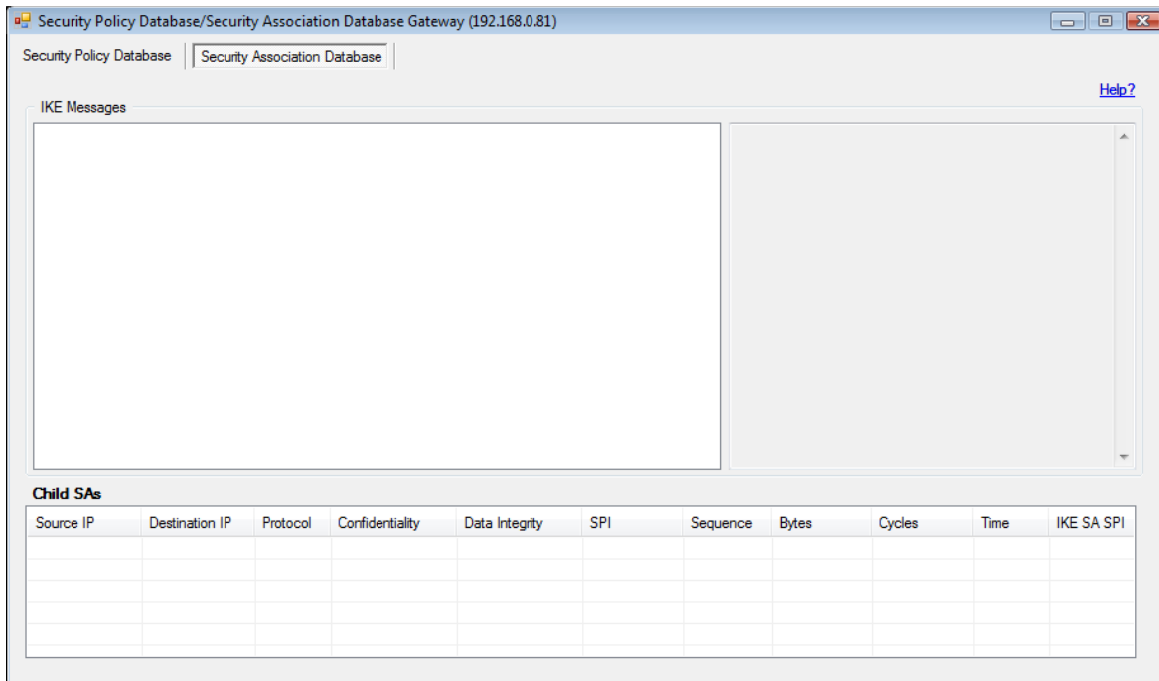


Figure 22. Security Association Database

### Protocol

Protocol to use for traffic protection.

### Confidentiality

Encryption/Decryption algorithm to use for traffic protection.

### Data Integrity

Data integrity algorithm that is used to protect the corresponding traffic.

### SPI

Security Parameter Index for the CHILD-SA.

### Sequence

The last protected packet's sequence number protected by the CHILD-SA.

### Bytes

Number of bytes that were processed using the CHILD-SA.

### Cycles

Number of CPU cycles that were consumed to process traffic associated with the CHILD-SA.

Time

Time in millisecond that elapsed to process traffic associated with the CHILD-SA.

IKE-SA SPI

IKE Security Parameter Index associated with the CHILD-SA.



## UDP Traffic Monitor

Use **UDP Traffic Monitor** (Figure 22) to monitor the incoming and outgoing UDP datagrams flowed between the instance and other instances.

---

*UDP packets are used in IKE message exchanges.*

---

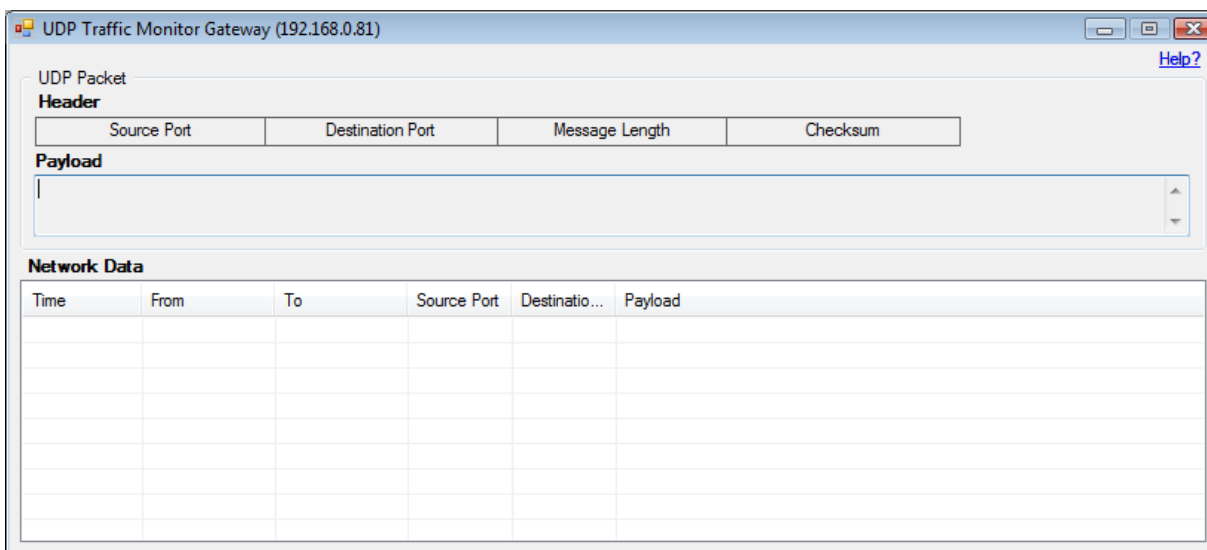


Figure 23. UDP Traffic Monitor

### UDP Packet

Use this section to view the elements of a UDP packet and its payload of in network byte order.

---

*To view a UDP packet you need to select it from the **Network Data** list by clicking on the corresponding list item.*

---

#### Header

This section shows the elements of a UDP packet header. When a UDP packet is selected this section shows the corresponding values in the selected UDP packet.

#### Payload

For a selected UDP packet this section shows its payload in network byte order.

#### Network Data

This list view shows a list of incoming and outgoing UDP packets in reverse chronological order.

#### Time

Arrival/Departure times of UDP packets.

***From***

Source addresses of corresponding IP datagrams.

***To***

Destination addresses of corresponding IP datagrams.

***Source Port***

Source ports of the UDP packets.

***Destination Port***

Destination ports of the UDP packets.

***Payload***

Payloads of the UDP packets.