

Configuring a VPN Server Learning Objectives

In this lab, we will configure the server side of the pfSense VPN.

Tools and Software

- pfsense Firewall




Lab Deliverables

❖ Part 1: Use the ipsec Command

- 19 Certificate Authorities

System / Certificate Manager / CAs

CA's Certificates Certificate Revocation

Name	Internal	Issuer	Certificates	Distinguished Name	Actions
IPsecVPN	✓	self-signed	0	emailAddress=hgokturk@syr.edu, ST=Texas, O=Syracuse University, L=Houston, CN=IPsecVPN, C=US Valid From: Wed, 06 Nov 2019 05:27:24 +0000 Valid Until: Sat, 03 Nov 2029 05:27:24 +0000	  

[+ Add](#)

Do you want AutoComplete to remember web form entries? [Learn about AutoComplete](#)







❖ IKEv2VPN

Configuring a Virtual Private Network Server

1.vWorkstation
2019-11-05 23:40:01
Adil Gokturk

System / Certificate Manager / Certificates

CA's Certificates Certificate Revocation

Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (59399e28df78d) Server Certificate CA: No, Server: Yes	self-signed	emailAddress=admin@pfSense.localdomain, ST=State, O=pfSense webConfigurator Self-Signed Certificate, L=Locality, CN=pfSense-59399e28df78d, C=US Valid From: Thu, 08 Jun 2017 18:57:45 +0000 Valid Until: Tue, 29 Nov 2022 18:57:45 +0000		  
IKEv2VPN Server Certificate CA: No, Server: Yes	IPsecVPN	emailAddress=hgokturk@syr.edu, ST=Texas, O=Syracuse University, L=Houston, CN=172.30.0.1, C=US Valid From: Wed, 06 Nov 2019 05:39:36 +0000 Valid Until: Sat, 03 Nov 2029 05:39:36 +0000		  

+ Add

Do you want AutoComplete to remember web form entries? [Learn about AutoComplete](#) Yes No

9:40 PM 11/5/2019

❖ 51. IPsec Tunnels Page

VPN / IPsec / Tunnels

The changes have been applied successfully.

IPsec Tunnels							
	IKE	Remote Gateway	Mode	P1 Protocol	P1 Transforms	P1 Description	Actions
<input type="checkbox"/>	Disable	V2	WAN Mobile Client	AES (256 bits)	SHA256		

[+ Show Phase 2 Entries \(0\)](#)

[+ Add P1](#) [Delete P1s](#)

Do you want AutoComplete to remember web form entries? [Learn about AutoComplete](#) [Yes](#) [No](#) [x](#)

❖ 62. IPsec Tunnels Page

The screenshot displays the Mikrotik WinBox interface for configuring IPsec tunnels. The breadcrumb navigation shows 'VPN / IPsec / Tunnels'. A green message box indicates 'The changes have been applied successfully.' Below this, the 'IPsec Tunnels' section contains a table with the following data:

	IKE	Remote Gateway	Mode	P1 Protocol	P1 Transforms	P1 Description	Actions
<input type="checkbox"/>	Disable	V2	WAN Mobile Client	AES (256 bits)	SHA256		



Below the table, there is a button '+ Show Phase 2 Entries (1)'. At the bottom right of the table area, there are two buttons: '+ Add P1' and 'Delete P1s'. The Windows taskbar at the bottom shows the time as 9:55 PM on 11/5/2019.

❖ 70. Pre-Shared Keys

The screenshot shows a web browser window displaying the configuration page for a VPN server. The browser's address bar shows the URL `http://172.30.0.1/vpn_ipsec_keys.p`. The page title is "Configuring a Virtual Private Network Server". The browser's status bar shows the date and time "2019-11-06 00:01:22" and the name "Adil Gokturk".

The web application interface has a dark header with the "Sensei COMMUNITY EDITION" logo and a navigation menu with items: System, Interfaces, Firewall, Sources, VPN, Status, Diagnostics, Gold, and Help. The main content area has a breadcrumb trail "VPN / IPsec / Pre-Shared Keys" and a success message: "The changes have been applied successfully." Below this is a tabbed interface with "Tunnels", "Mobile Clients", "Pre-Shared Keys" (selected), and "Advanced Settings".

The "Pre-Shared Keys" section contains a table with the following data:

Identifier	Type	Pre-Shared Key	Actions
adilgokturk	EAP	password1	 

Below the table is a green "+ Add" button. At the bottom of the browser window, a Windows taskbar is visible with icons for the Start menu, search, task view, Edge, File Explorer, and Firefox. A system tray notification asks "Do you want AutoComplete to remember web form entries?" with "Yes" and "No" buttons. The system clock shows "10:01 PM 11/5/2019".

❖ Part 2: Configuring Firewall Rule for VPN Traffic

• 9. IPsec Rules Table

Configuring a Virtual Private Network Server

1.vWorkstation
2019-11-06 00:07:02
Adil Gokturk

Firewall / Rules / IPsec

The settings have been applied. The firewall rules are now reloading in the background.
[Monitor the reload progress.](#)

Floating WAN LAN **IPsec**

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/0 B	IPv4 *	*	*	*	*	none		IPsec Open	Anchor Edit Copy Delete

[Add](#) [Add](#) [Delete](#) [Save](#) [Separator](#)

Do you want AutoComplete to remember web form entries? [Learn about AutoComplete](#) [Yes](#) [No](#)

10:07 PM
11/5/2019

❖ Part 2: Challenge Questions

- IPsec can provide two different modes: Tunnel Mode and Transport Mode.
Explain how each mode works and discuss their tradeoffs. Considering the tradeoffs, what would be the optimum solution? Should we choose one or the other?
 - Firewall.cx (2019) argues that the IPsec's protocol goal is to provide security services for IP packets such as encrypting sensitive data, authentication protection against replay and data confidentiality.
- **IPsec Tunnel Mode**
 - The Tunnel Mode is IPsec default mode and with this model entire original IP packet is protected, which means IPsec wraps the original packet, encrypts it, adds a new IP header and delivers it to the other side of the VPN tunnel as shown below the diagram.1 (Firewall.cx, 2019).

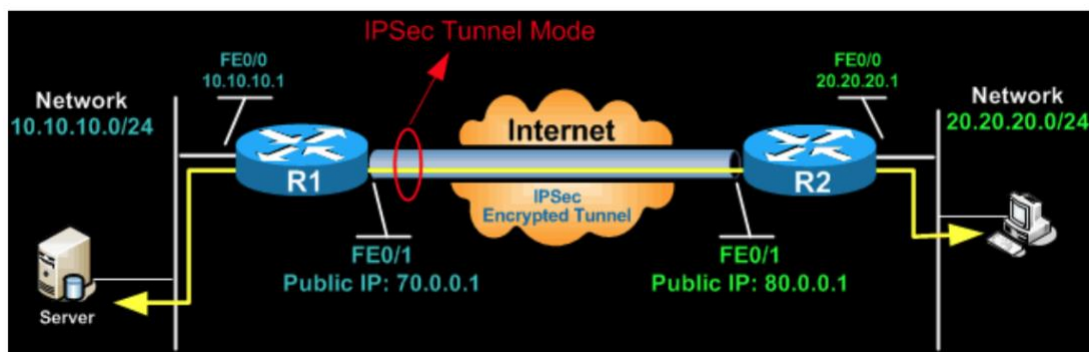


Diagram.1 IPsec Tunnel mode (Firewall.cx, 2019)

In tunnel mode, an IPsec header—AH or ESP header is inserted between the IP header and the upper layer protocol (Firewall.cx, 2019). Between AH and ESP, ESO is most commonly used in IPsec VPN Tunnel configuration as shown in the diagram.2.

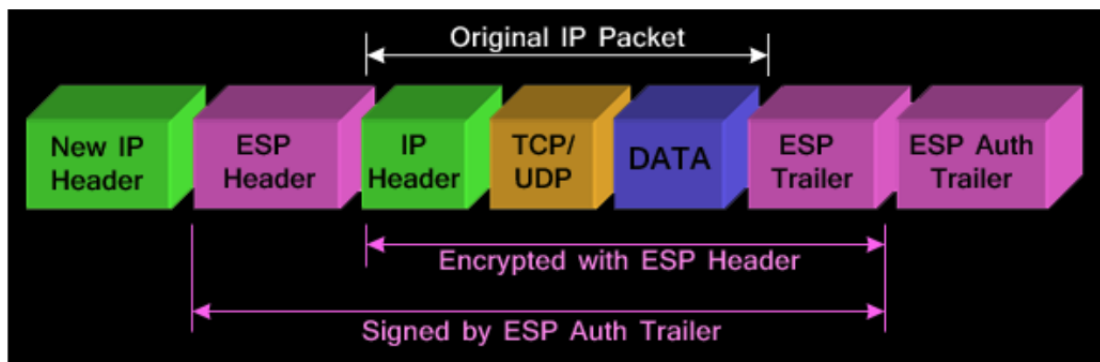


Diagram.2 IPsec Tunnel mode with ESP header (Firewall.cx, 2019)

As show below in the diagram.3, ESP is identified in the New IP header with an IP protocol ID of 50, which is commonly used between a Cisco VPN client and an IPsec Gateway(Firewall.cx, 2019)

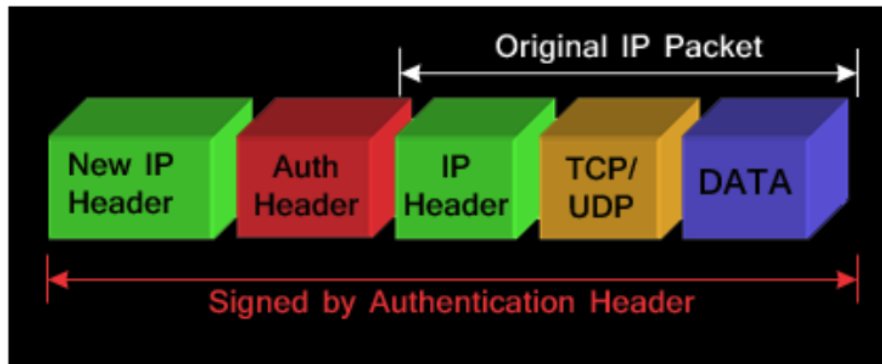


Diagram.3 IPsec Tunnel mode with AH header (Firewall.cx, 2019)

IPsec tunnel mode allows to the AH to work alone or together with the ESP.

- **IPsec Transport Mode**

IPsec Transport model is a great option for end-to-end communications, as shown below in the diagram.4. The communication between a client and a server or a between a workstation and a gateway are some of the most common applications.

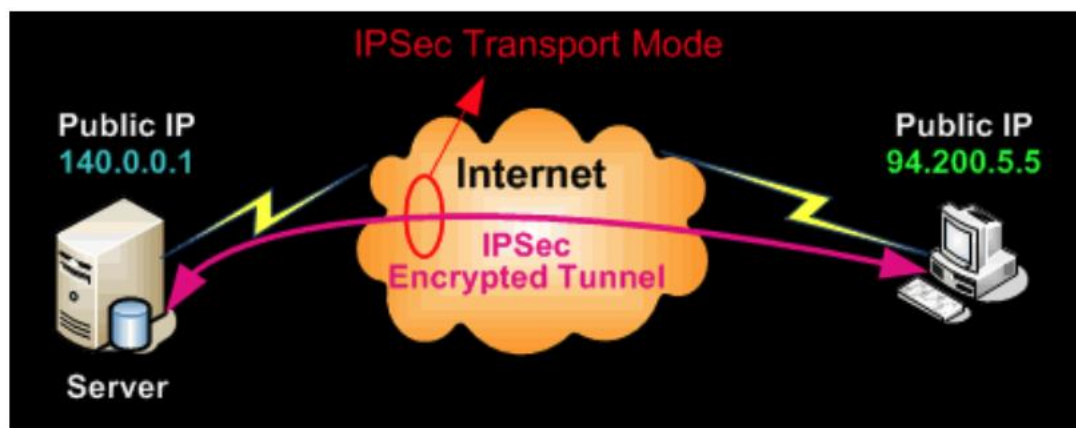


Diagram.4 IPsec Transport mode, end-to-end communication (Firewall.cx, 2019)

IPsec transport mode, also known as IP Payload, provides protection to data, and consists of TCP?UDP header + Data, through an AH or ESP header. The payload is encapsulated by the IPsec headers and trailers as shown below in the diagram.5 (Firewall.cx, 2019).

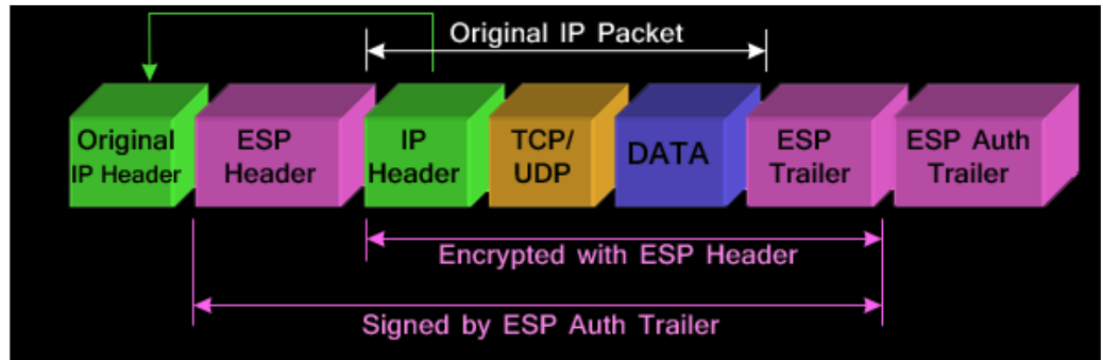


Diagram.5 IPsec Transport mode with ESP header (Firewall.cx, 2019)

The original IP header is moved to the front and placing the sender's IP header at the front proves that transport mode does not provide protection and encryption to the original IP header as illustrated in the diagram below (Firewall.cx, 2019)

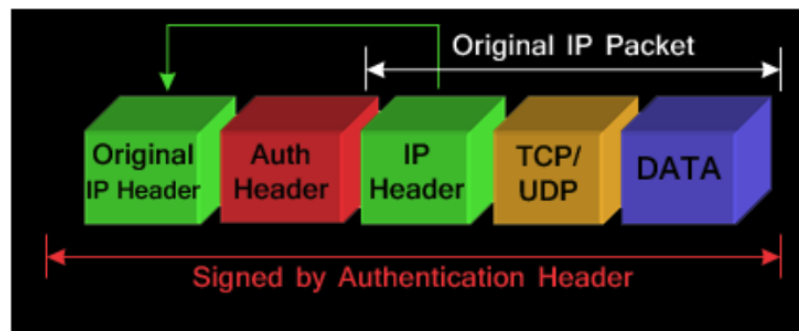


Diagram.6 IPsec Transport mode with AH header (Firewall.cx, 2019)

The AH can be applied alone or together with ESP when IPsec is in transport mode.

- IPsec can be configured to operate either Tunnel or Transport mode. The preference of either one of these modes depends on the requirements and the implementation of IPsec application (Firewall.cx, 2019).

References

- Firewall.cx (Producer). (2019). UNDERSTANDING VPN IPSEC TUNNEL MODE AND IPSEC TRANSPORT MODE - WHAT'S THE DIFFERENCE? Retrieved from <http://www.firewall.cx/networking-topics/protocols/870-ipsec-modes.html>