Configuring a VPN Server Learning Objectives

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

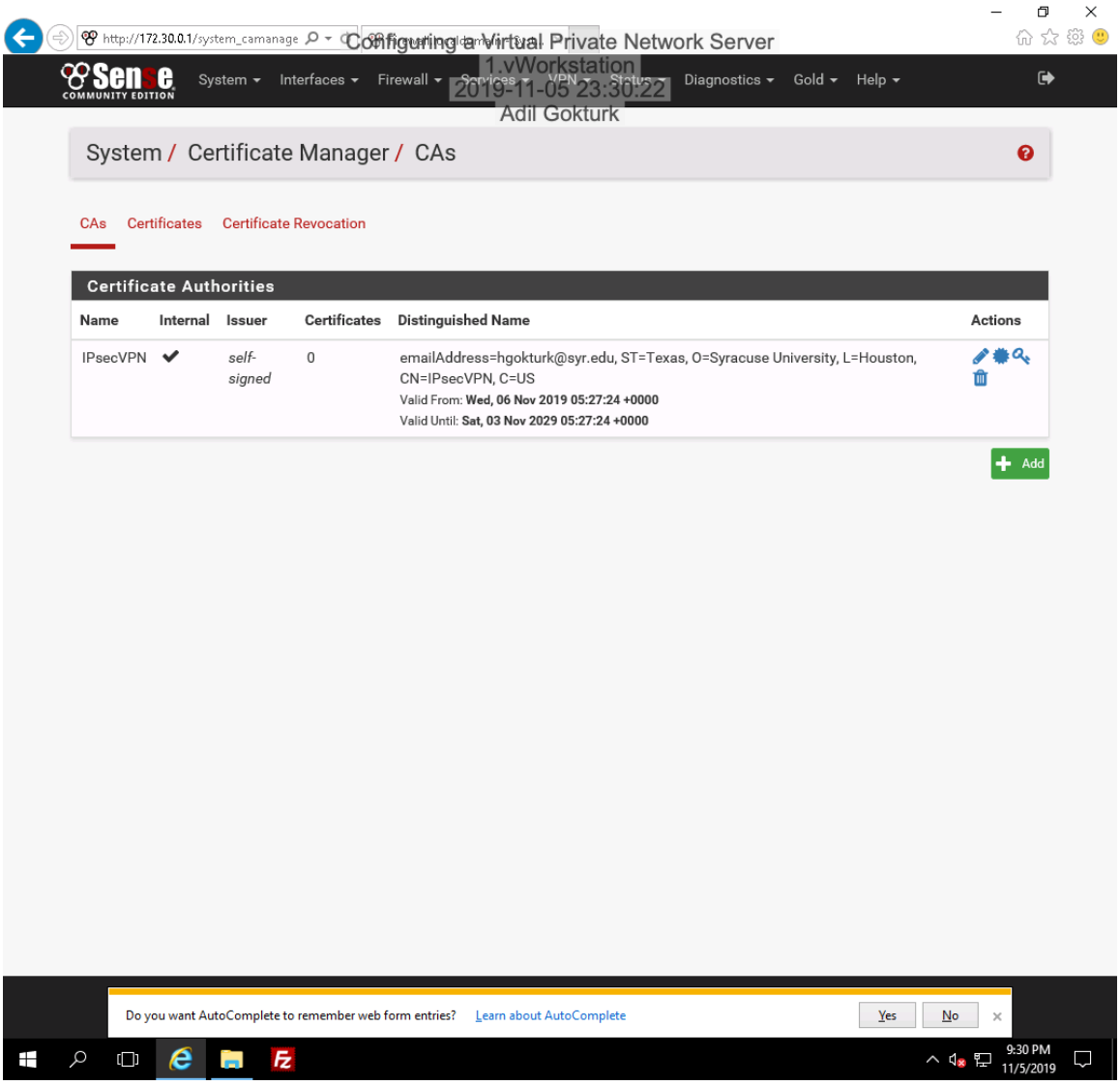
Tools and Software

• pfsense Firewall

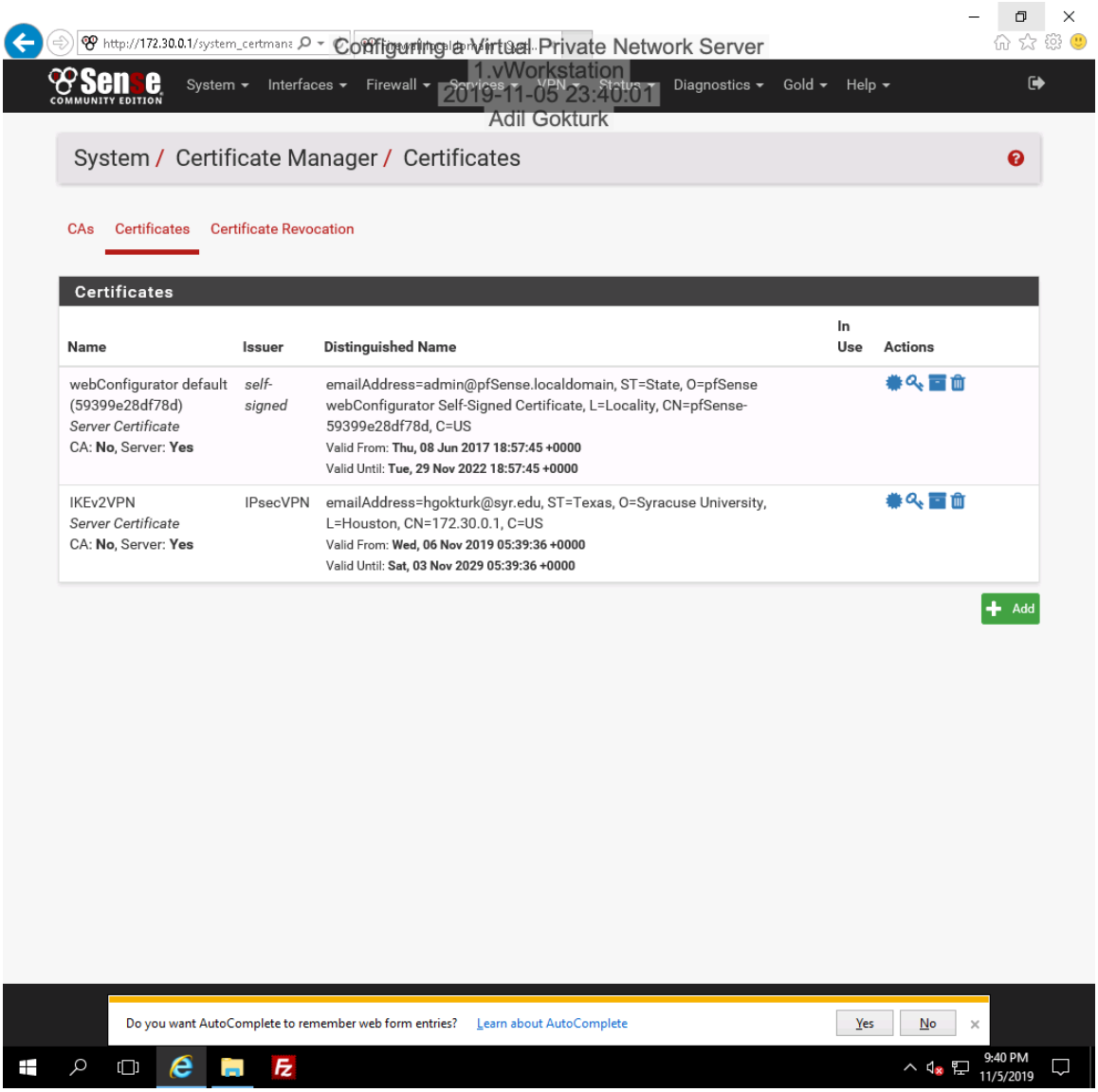
Lab Deliverables

❖ Part 1: Use the ipsec Command

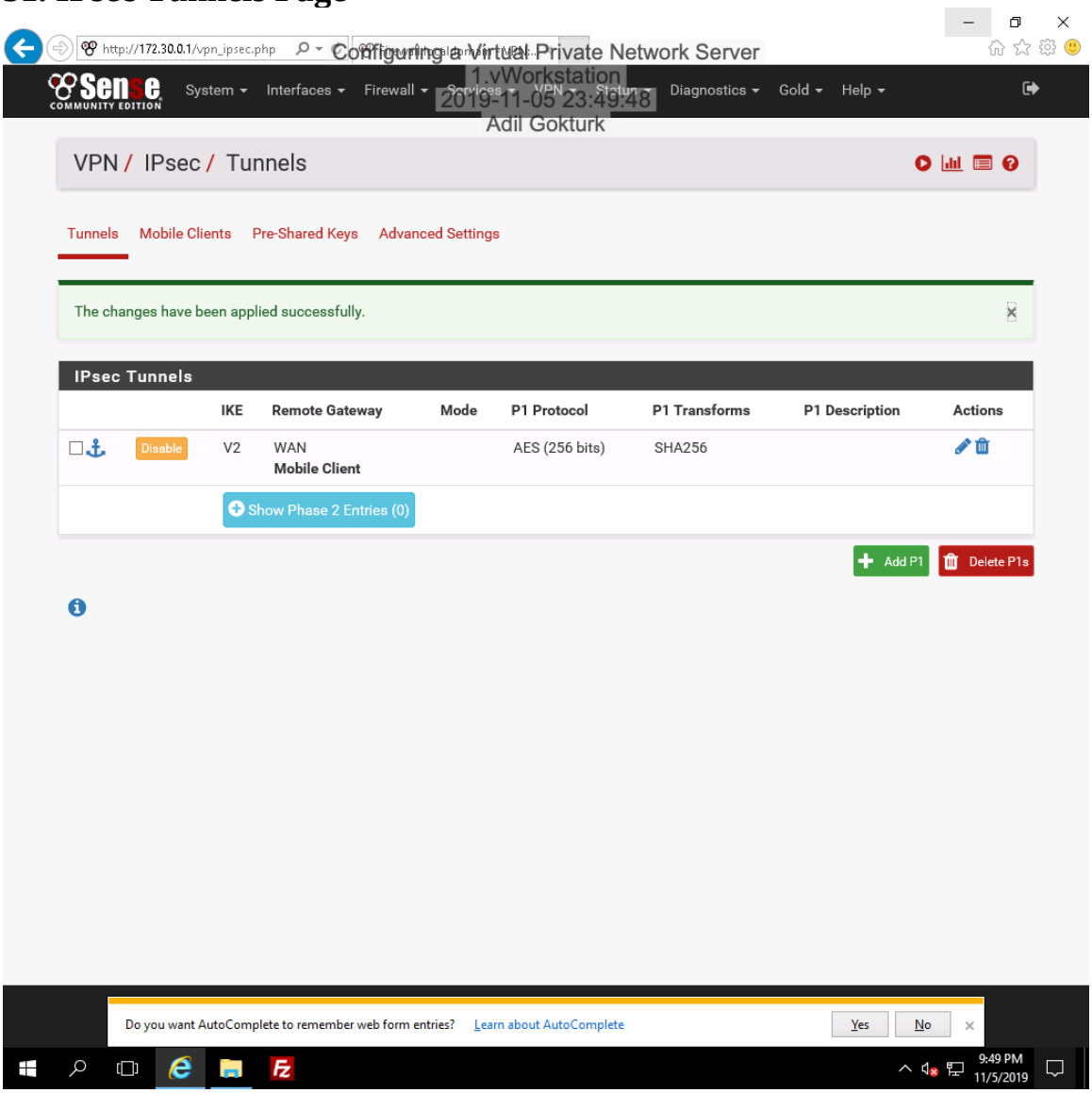
- **19 Certificate Authorities**



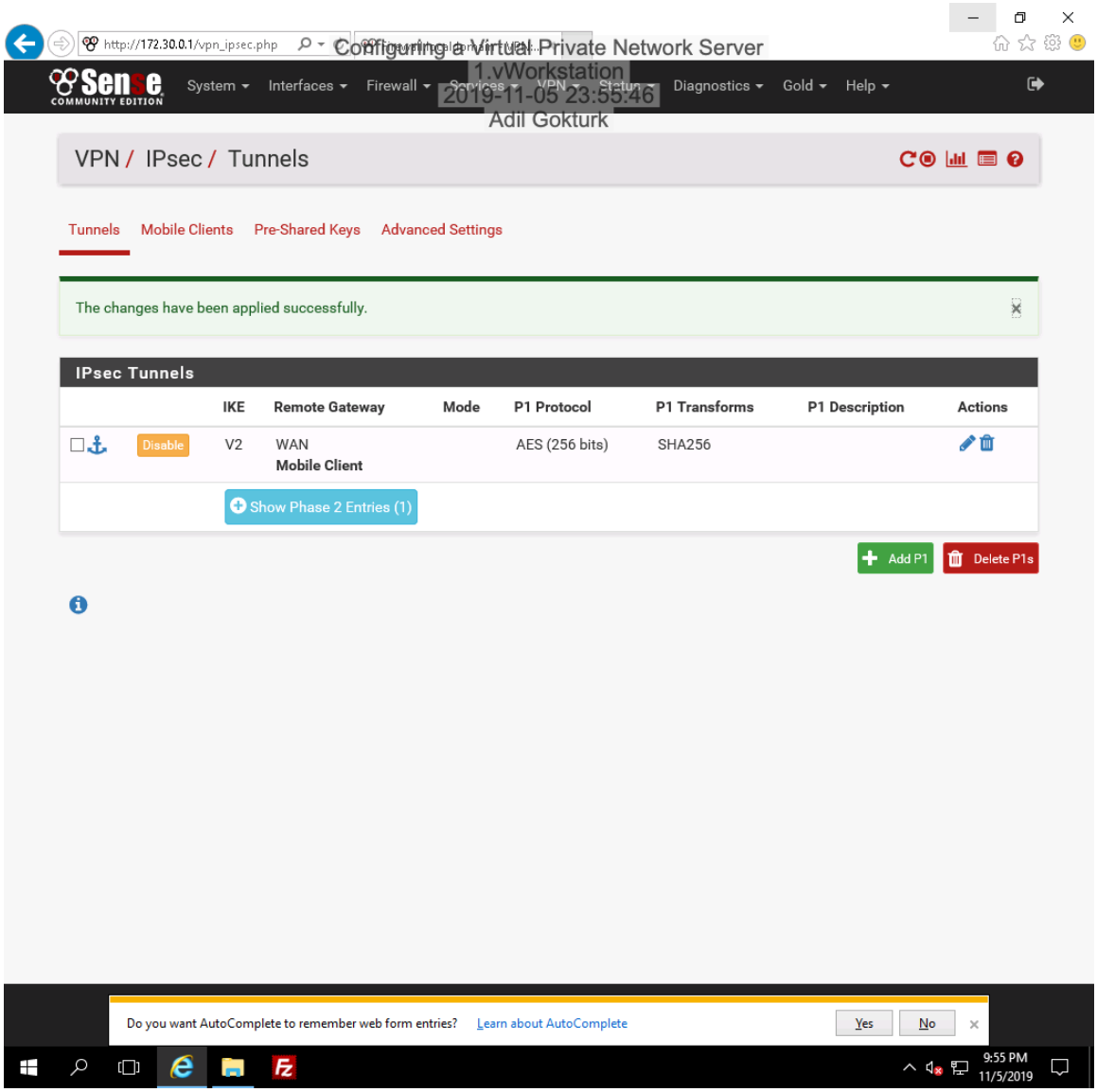
❖ IKEv2VPN


Configuring a Virtual Private Network Server
1.vWorkstation
2019-11-05 23:40:01
Adil Gokturk
http://172.30.0.1/system_certmana
System Interfaces Firewall Services VPN Status Diagnostics Gold Help
System / Certificate Manager / Certificates
CAs Certificates Certificate Revocation
Certificates
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

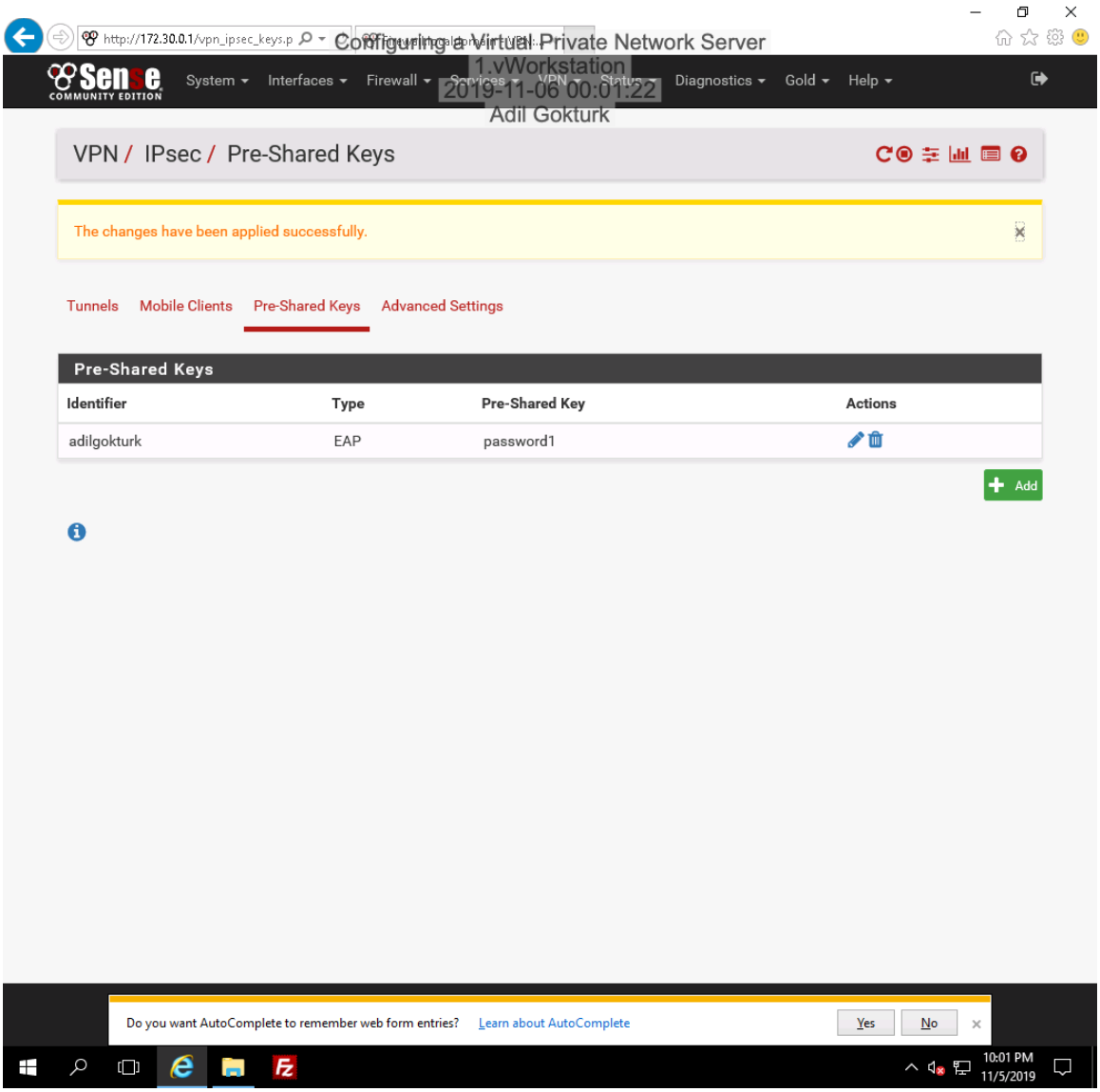
❖ 51. IPsec Tunnels Page



❖ 62. IPsec Tunnels Page

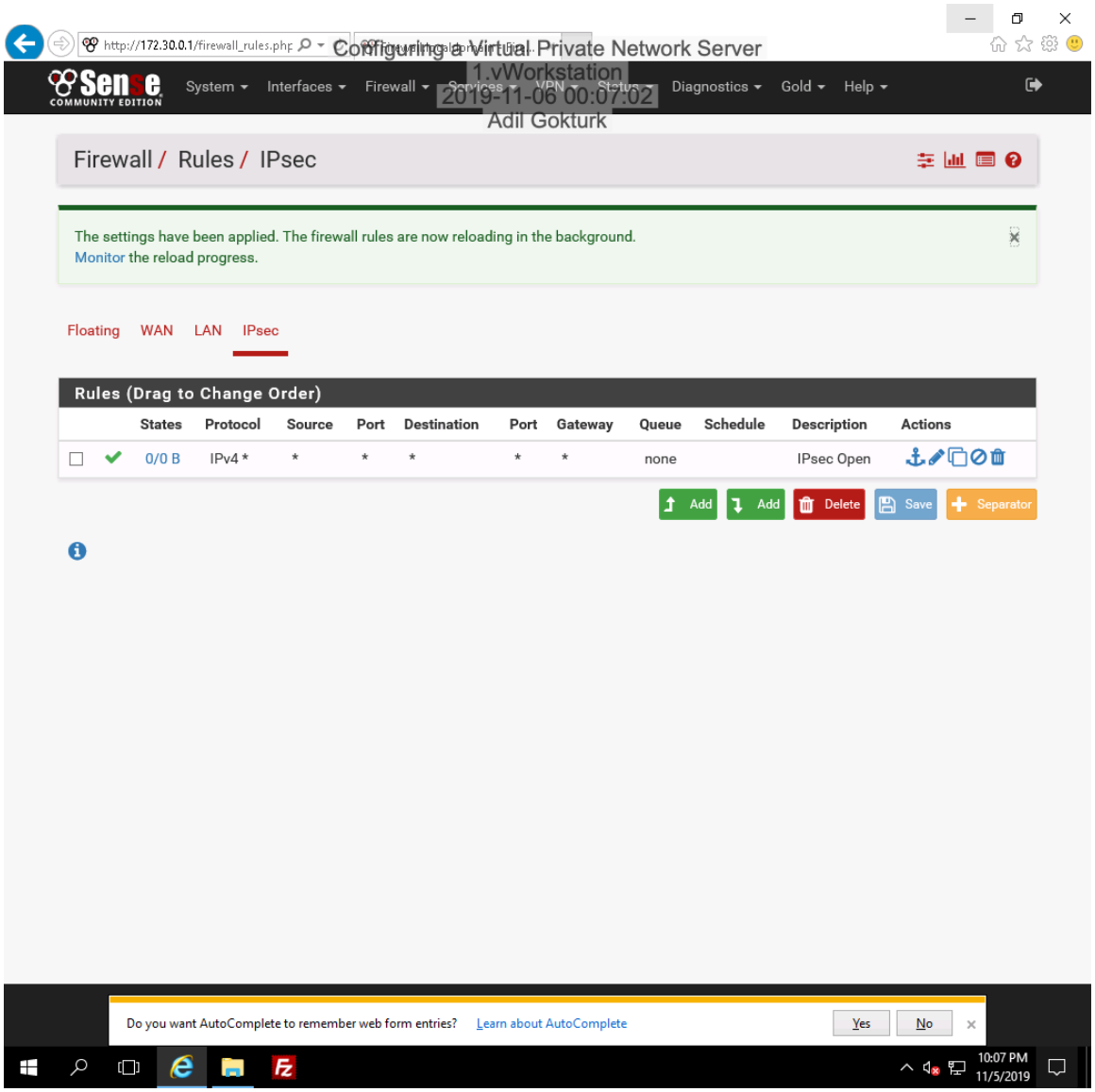


❖ 70. Pre-Shared Keys



❖ Part 2: Configuring Firewall Rule for VPN Traffic

- **9. IPsec Rules Table**



❖ 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) .

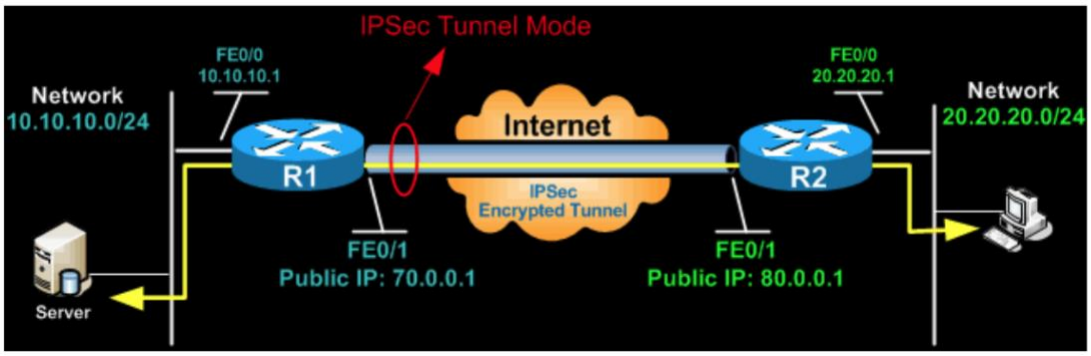


Diagram.1 IPsec Tunnel mode (Firewall.cx, 2019)

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.

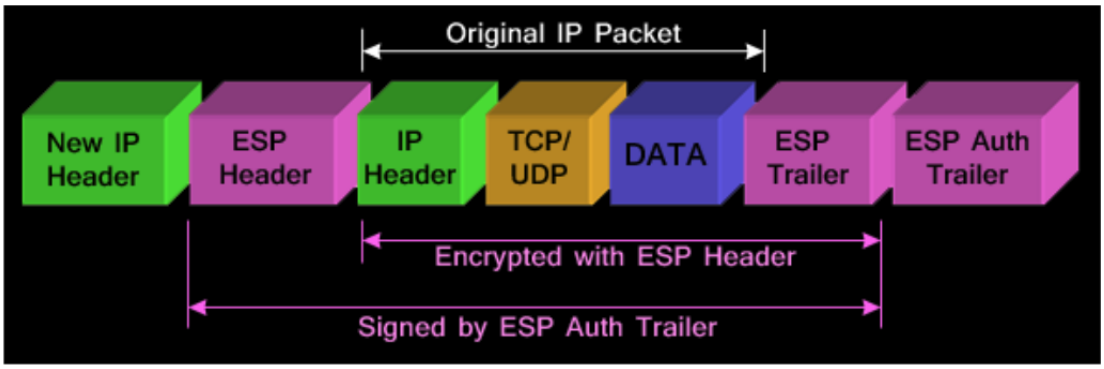


Diagram.2 IPsec Tunnel mode with ESP header (Firewall.cx, 2019)

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)

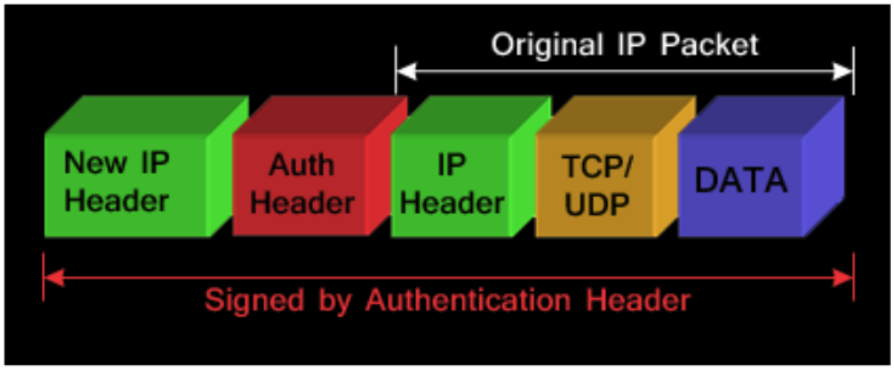


Diagram.3 IPsec Tunnel mode with AH header (Firewall.cx, 2019)

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.

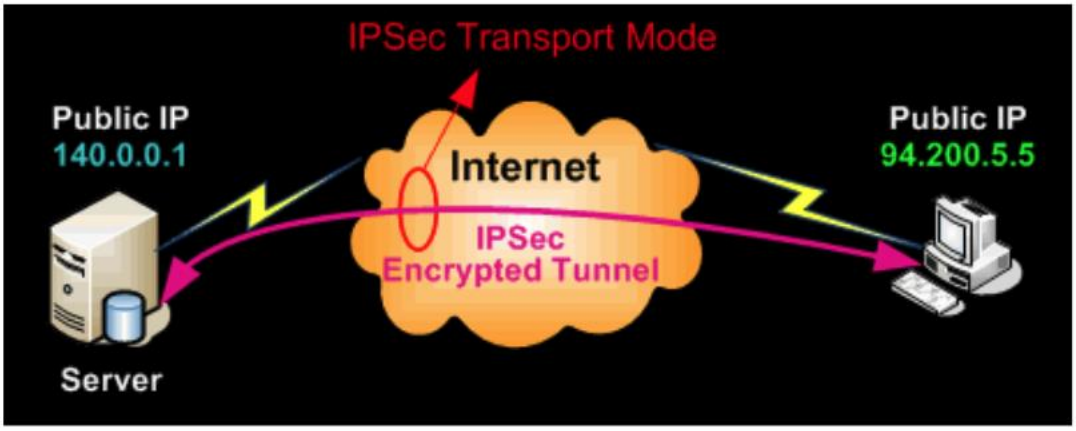


Diagram.4 IPsec Transport mode, end-to-end communication (Firewall.cx, 2019)

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).

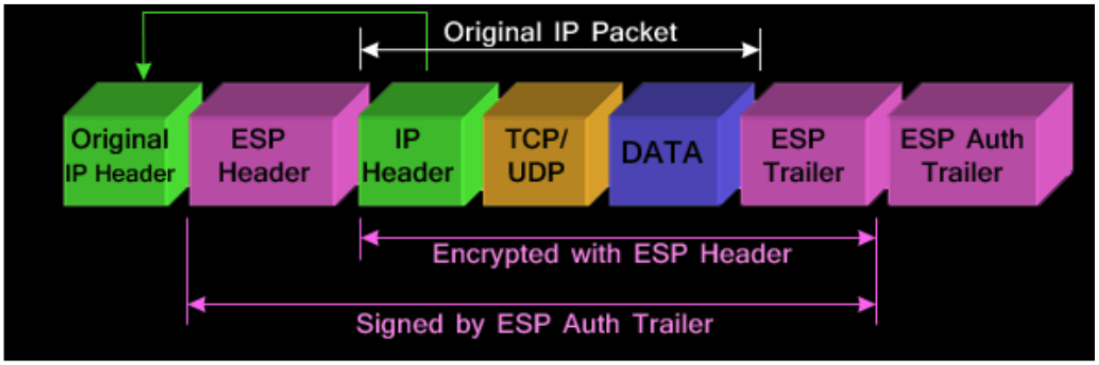


Diagram.5 IPsec Transport mode with ESP header (Firewall.cx, 2019)

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)

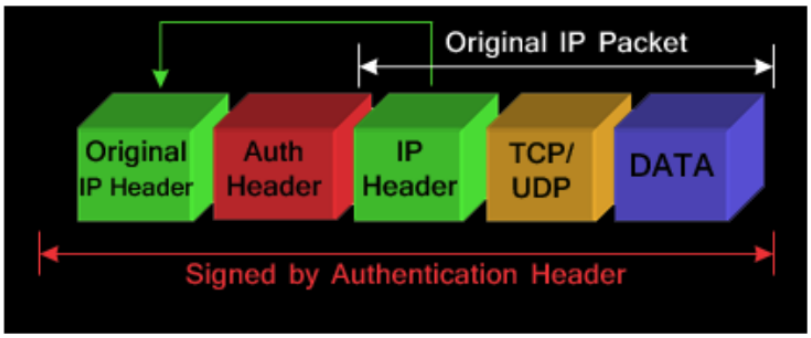


Diagram.6 IPsec Transport mode with AH header (Firewall.cx, 2019)
The AH can be applied alone or together with ESP when IPsec is in transport mode.

- 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