Protocol Deep Dive: IPsec

LEARNING IPSEC FUNDAMENTALS



Joe Abraham
NETWORK SECURITY CONSULTANT
@joeabrah www.joeabrahamtech.com

How We'll Conduct This Course



Focus on the building blocks of the IPsec protocol suite



Break it down to a low level, then build it back up



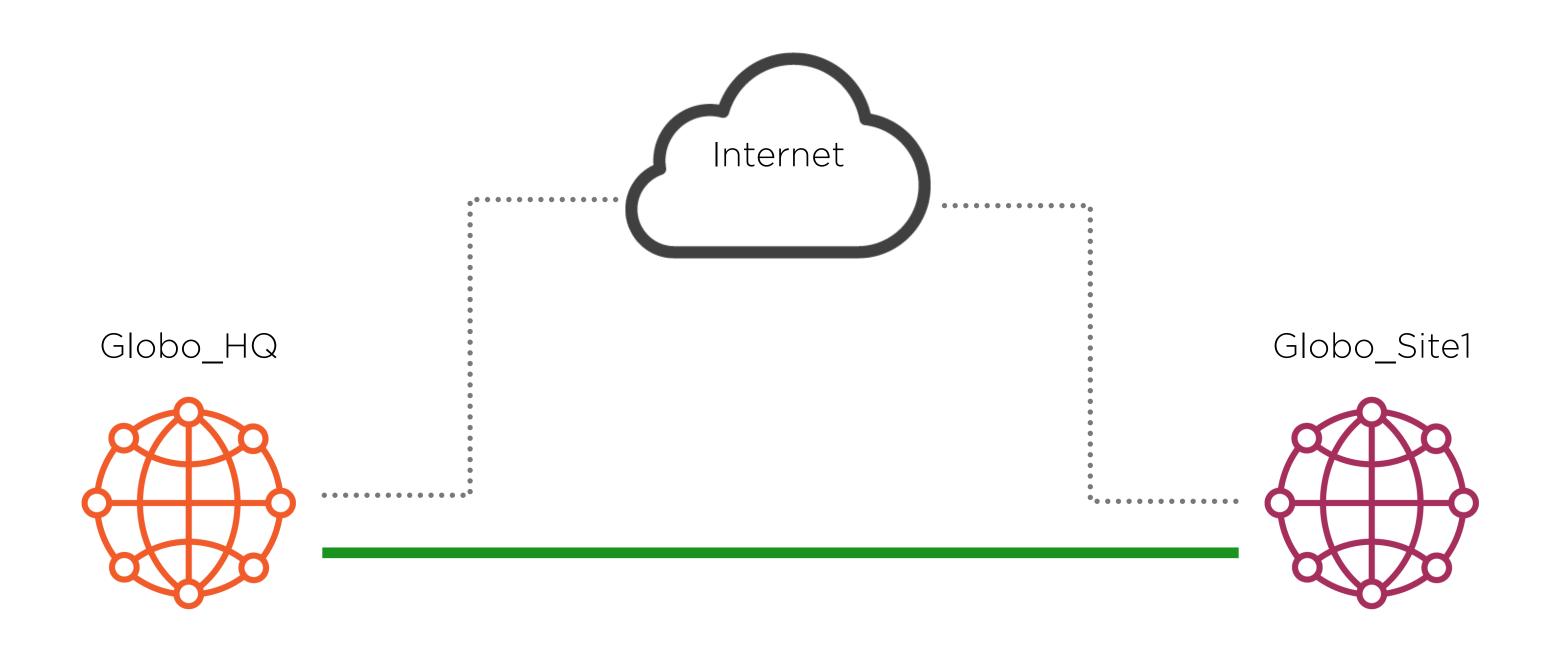
Use implementations such as Dynamic Multipoint VPN (DMVPN) and dynamic Virtual Tunnel Interfaces (dVTI)



Globomantics wants to change their infrastructure

- Remote site users need access to corporate resources
- IPsec is one of the standards for VPN traffic

Globomantics' Network



Overview

What is IPsec?

• History, uses, modes

Building IPsec

 Building blocks, components, authentication

IPsec use cases

IKEv1

IKEv2

IPsec with IPv6

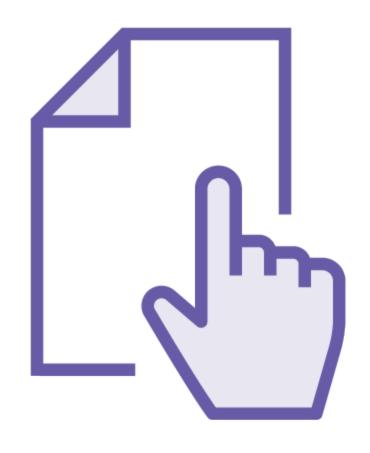
Course Prerequisites

Have good understanding of:

Routing and Switching

Security Threats

Desire to learn about IPsec!



How You Can Follow Along

What is in the course materials?

- Initial lab configurations
- Packet captures

What should you have?

- Equipment/virtualization
- Wireshark for analysis

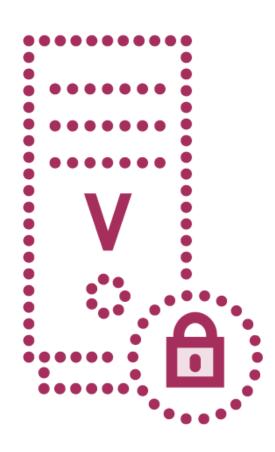
Virtualization Options:

Cisco VIRL

GNS3

EVE-NG

Virtual Box



What Is IPsec?

Short IPsec History

1988

Vendors come together to create a network encryption device

1995

IETF IP Security Working Group Formed

RFC-1825 through 1827 Published

1970's

ARPANET Encryption Devices

Experimental encryption for TCP/IP and ARPANET packets

1994

Trusted Information Service

Enhanced IP security protocols and developed DES drivers

IPsec Information

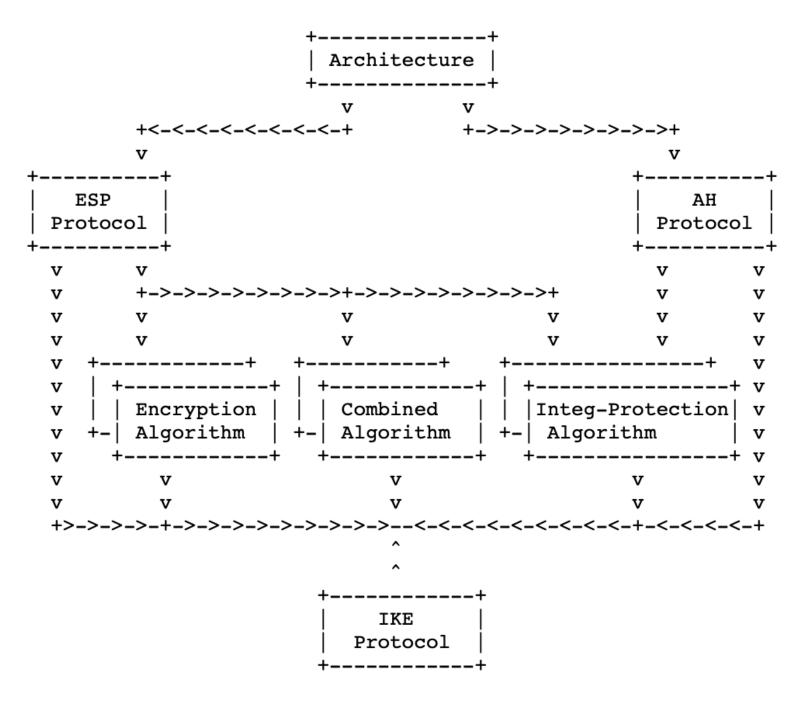


Figure 1. IPsec/IKE Document Interrelationships

Copyright © The Internet Society (2005)

IPsec Datagrams

AH Tunnel Mode

ESP Tunnel Mode

AFTER APPLYING ESP

Pv4	new IP hdr*	 ESP	orig	IP hdr* options)	 TCP	 Data	ESP Trailer	ESP ICV
		<	<	encr	 yptio ity -	on	> >	

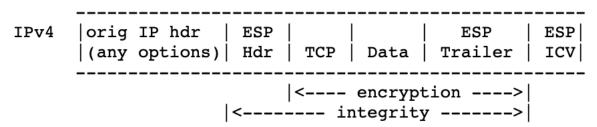
AH Transport Mode

AFTER APPLYING AH

IPv4	original IP hdr (any options) AH TCP Data
	<pre> <- mutable field processing -> <- immutable fields -> < authenticated except for mutable fields> </pre>

ESP Transport Mode

AFTER APPLYING ESP



Why IPsec?

Attack Mitigation

Data Corruption

Theft

Replay Attacks

Eavesdropping



CIA Triad

The combination of the principles of confidentiality, integrity, and availability that must be maintained to ensure an adequate security posture for organizations.

IPsec RFCs

RFC 6071 (IP Security and Internet Key Exchange Document Roadmap)

Summary

Course introduction and overview

What is IPsec?

Why use IPsec?

RFCs

Lab exploration