Finalizing IPsec Concepts

Joe Abraham
NETWORK SECURITY CONSULTANT

@joeabrah   www.joeabrahamtech.com

Overview

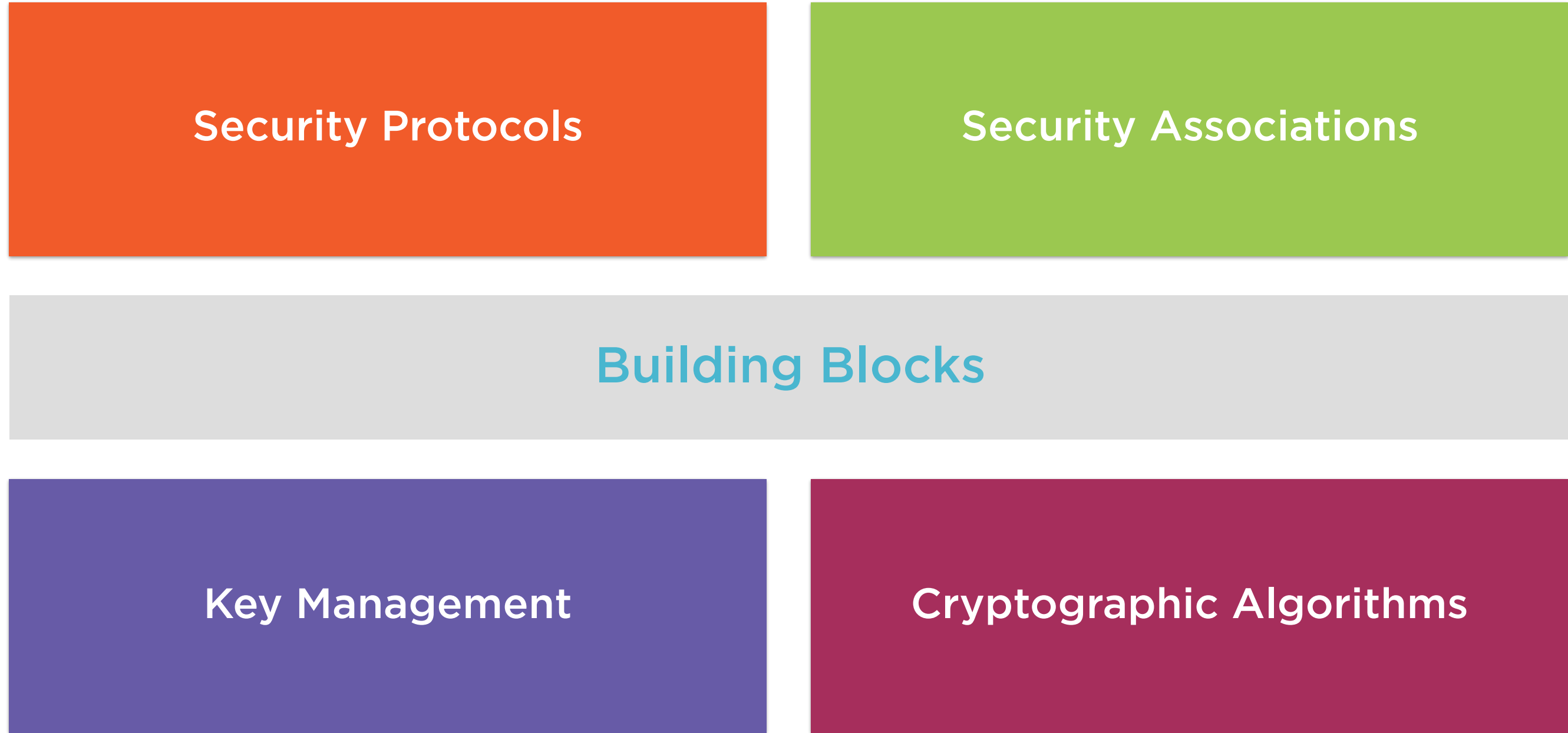IPsec module review

Additional resources

Let's wrap!

Protocol suite

Secures our VPN links

Protects our data

What's IPsec?

IPsec Protocol Suite

Security Protocols

Security Associations

Building Blocks

Key Management

Cryptographic Algorithms

Site-to-Site and Remote Access

Site-to-Site VPN | Remote Access VPN

Site-to-Site VPN

Logically connect sites together

GRE over IPsec (DMVPN)

Protects entire network

Provides corporate resources to other sites

Remote Access VPN

Logically connect endpoint to another network

IPsec using the OS IP stack

Protects individual devices

Provides individuals access to corporate resources

Useful in WiFi hotspots

IKE version 1

Internet Key Exchange; Uses ISAKMP, OAKLEY, and SKEME to help establish SAs for securing network traffic.
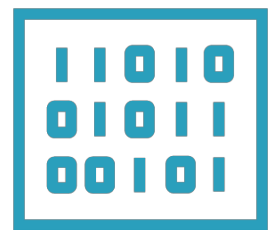
IKE version 2

Internet Key Exchange; Adds enhancements to protocol over version 1, as well as changes to functionality and communications structure.

IPsec in IPv6

Creators wanted security to be something easily implemented in the protocol

Extension headers are used to add new services to IPv6, such as IPsec

Requirement is that IPv6 implementations "should" support IPsec now instead of "must"

The functionality of IPsec in IPv6 doesn't change much from IPv4, only some minor changes and the differences in the packet structures

Let's Wrap!

Pluralsight Courses

IPv6: Introduction to the Protocol

VPN Fundamentals for CCNP Security

Cryptography: The Big Picture

RFC 6071

IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap

Thank You!