Securing the Network with IKEv1

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

Overview

Detail IKE

IKEv1 authentication mechanisms

IKEv1 phases

IKv1 modes

IKE version 1

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

IKEv1 is still being used today!

IKEv1 Authentication

Pre-shared key

Uses shared passwords to authenticate peers

Public Key Infrastructure

Uses certificates to authenticate peers based on CA trust points

Using Pre-shared Keys

IKE uses preconfigured key to authenticate with peer

Peers compute and send hashes for authentication

How do you get the password to the other side securely?

This doesn't scale well!

PKI

Uses certificate authority for authentication

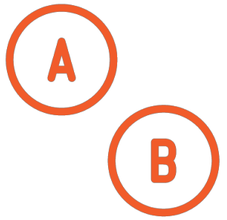
- No passwords shared
- More secure, cannot forge
- Built-in expiration dates

IKEv1 Phases

IKEv1 Phase 1

IKE SAs are being established to form the secure tunnel

Authenticates IPsec devices, negotiates SA policies, and exchanges keys securely



Two modes: main mode and aggressive mode

IKEv1 Phase 2

- Negotiates and establishes IPsec SAs
- IPsec tunnels are established
- Uses security policies defined in device configuration
- Interesting packets are encrypted/ decrypted once this phase is finished

IKE Main Mode

Main Mode Exchanges

Exchange 1: Protocol, SA attributes, algorithms, hashes are exchanged and agreed upon

Exchange 2: Key generation and hashing occurs, for secure verification of the authentication data

Exchange 3: Authentication occurs and the signatures are verified using agreed upon authentication algorithm

Demo

Configure and test main mode

Analyze the packets

Move on to aggressive mode

IKEv1 Aggressive Mode

Only 1 exchange

Everything possible is crammed into first exchange

Diffie-Hellman key and identity are in this exchange

Builds the IKE SA quickly

How do you secure the information if it's all sent in one exchange, before the security is negotiated?

IKE Quick Mode

Demo

Analyze previously configured IPsec connections

Discuss the exchanges and processes for quick mode

Summarizing IKEv1

Summary

What is IKE?

IKEv1 authentication mechanisms

IKEv1 phases

IKEv1 phase 1 modes

IKEv1 phase 2 mode

Get ready for IKEv2!