Establishing IPsec with IKEv2

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

Overview

IKEv1 versus IKEv2

IKEv2 benefits

IKEv2 modes

IKEv2 authentication

IKv2 phases

IKE version 2

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

IKEv1 and IKEv2

IKEv1

Authentication is PSK or PKI

SA lifetime negotiated

Slower negotiation

Stricter traffic selection per SA

Easier to configure

Obsolete version

IKEv2

Authentication is PSK, PKI, or EAP

MOBIKE provides mobility and multihoming

SA lifetime configured locally

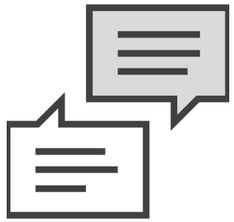
High availability native to protocol

Faster negotiation

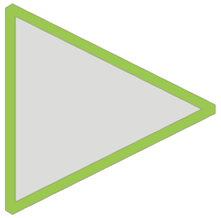
Flexible traffic selection per SA

IKEv2 Benefits

Reliability



Message flow system uses requests followed by responses



Initiator is responsible for ensuring reliability of the traffic being sent

Upon lack of receipt of response after a request, initiator either drops the connection or retransmits the request

IKEv2 Mobility and Multihoming Protocol

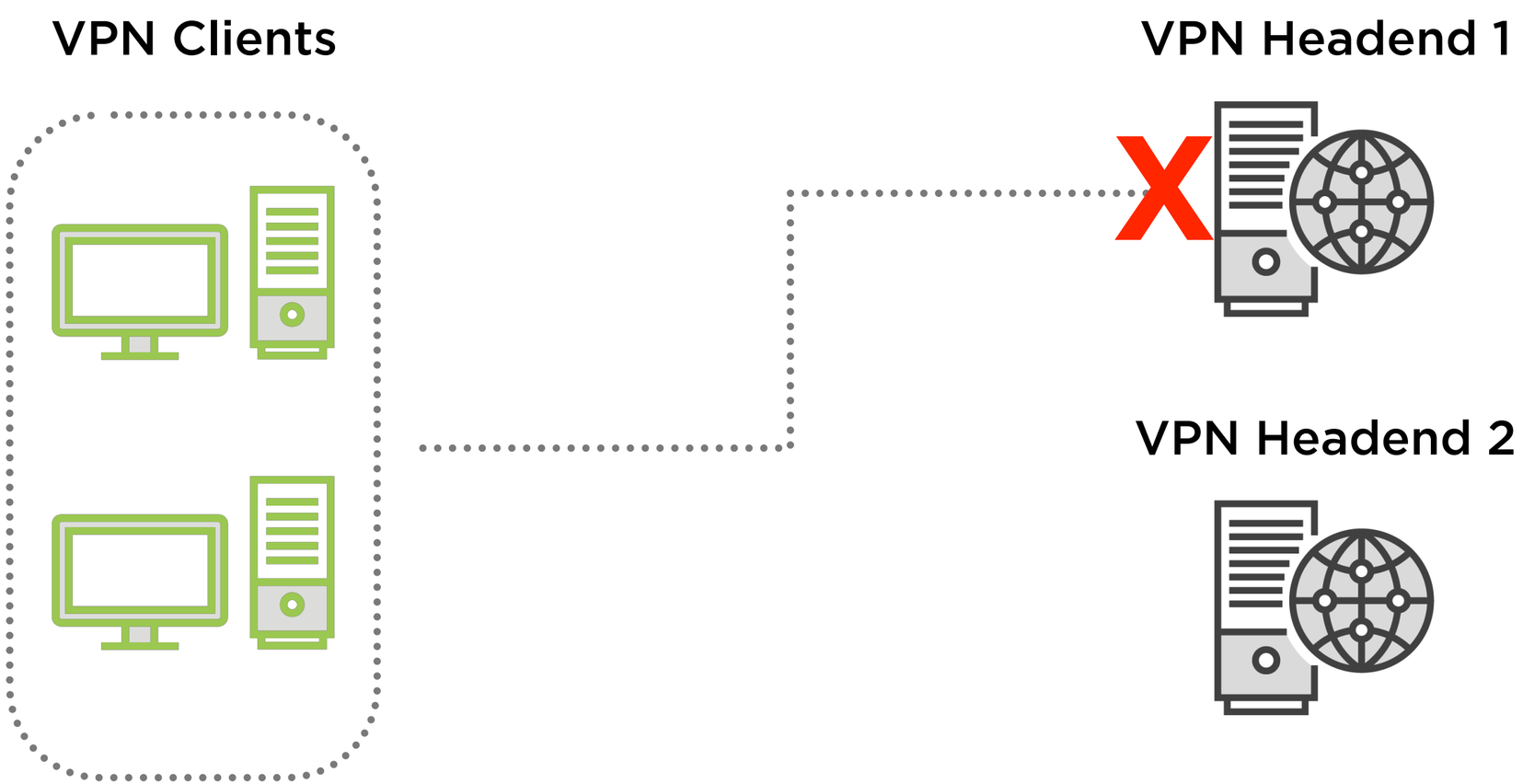
Mobility

Keeps VPN connection active when changing IP addresses

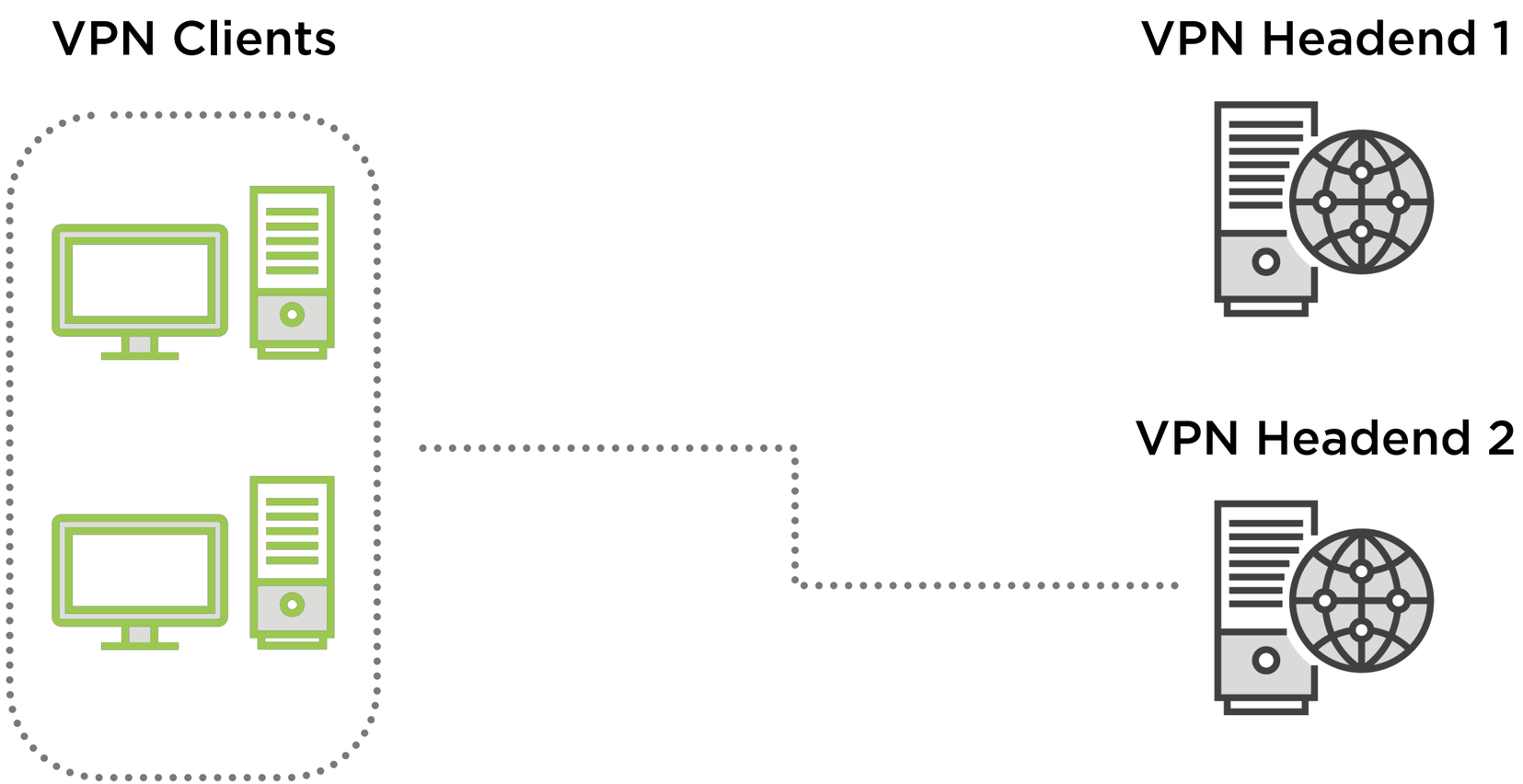
Multihoming

When interface drops, traffic is moved to another interface

High Availability



High Availability



What Traffic to Protect?

IKEv1

Exact parameters must be agreed upon, only one set per SA

IKEv2

Multiple combinations allowed within each SA

Optional IDr Payload

Multiple SAs can be created using the same IP range, port, and protocol combination

Identities let the devices know “who” is talking to “who”

Initiator chooses identity that they want to talk to using the same IP address and other parameters as the other identities

Lifetime

IKEv2 allows for local lifetime configuration; no negotiation occurs

IKEv2 Modes

IKEv2 Modes

IKE_SA_INIT

IKE_AUTH

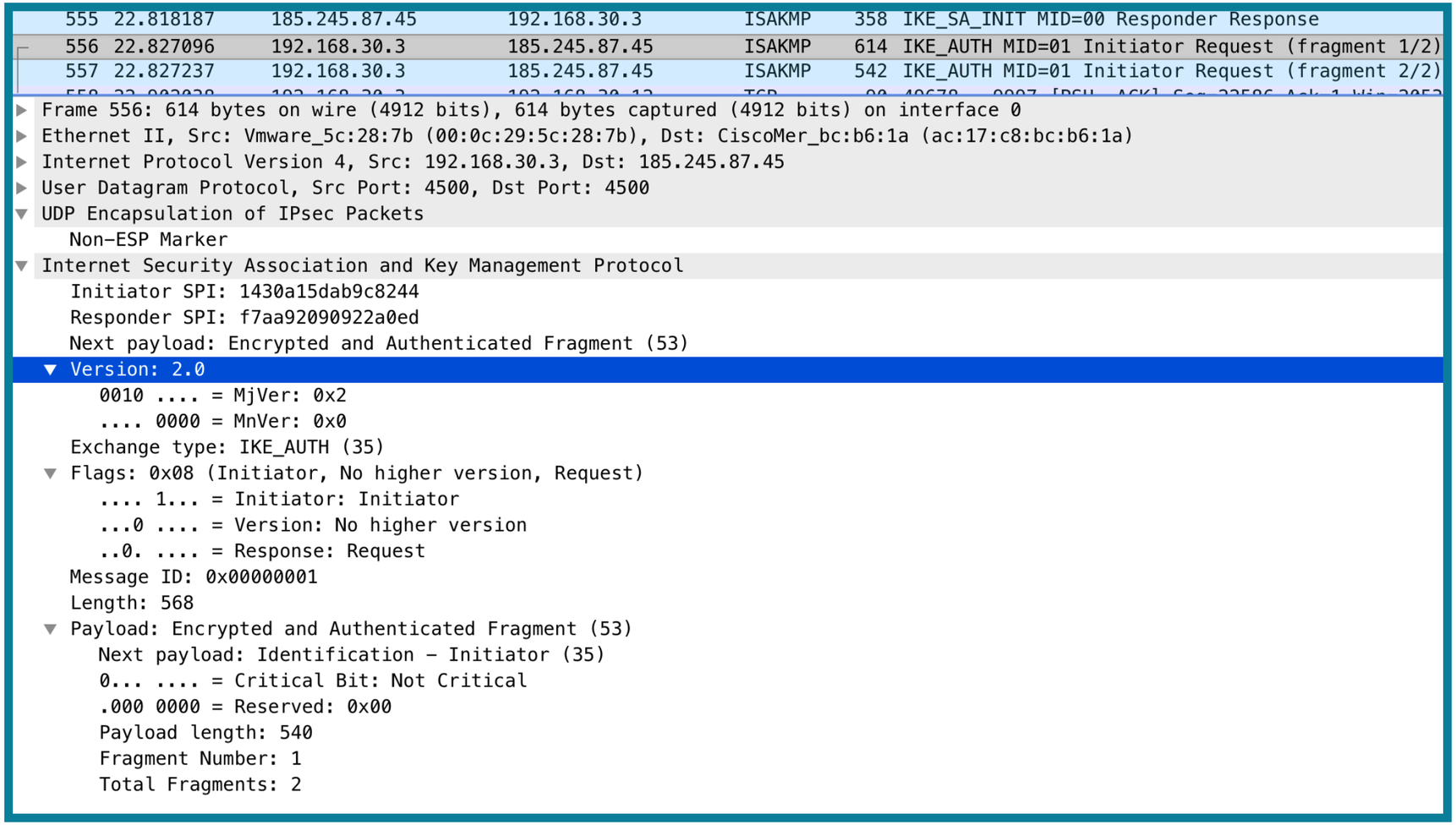
IKEv2 Modes

IKE_SA_INIT replaces purpose of main mode and aggressive mode exchanges from a high level

Proposals containing algorithms, SA parameters, and keying material are sent to confirm available functionality

IKE_SA_INIT exchange takes the place of main mode's first 2 exchanges

IKE_AUTH


555 22.818187 185.245.87.45 192.168.30.3 ISAKMP 358 IKE_SA_INIT MID=00 Responder Response
556 22.827096 192.168.30.3 185.245.87.45 ISAKMP 614 IKE_AUTH MID=01 Initiator Request (fragment 1/2)
557 22.827237 192.168.30.3 185.245.87.45 ISAKMP 542 IKE_AUTH MID=01 Initiator Request (fragment 2/2)
Frame 556: 614 bytes on wire (4912 bits), 614 bytes captured (4912 bits) on interface 0
Ethernet II, Src: Vmware_5c:28:7b (00:0c:29:5c:28:7b), Dst: CiscoMer_bc:b6:1a (ac:17:c8:bc:b6:1a)
Internet Protocol Version 4, Src: 192.168.30.3, Dst: 185.245.87.45
User Datagram Protocol, Src Port: 4500, Dst Port: 4500
UDP Encapsulation of IPsec Packets
Non-ESP Marker
Internet Security Association and Key Management Protocol
Initiator SPI: 1430a15dab9c8244
Responder SPI: f7aa92090922a0ed
Next payload: Encrypted and Authenticated Fragment (53)
Version: 2.0
0010 .... = MjVer: 0x2
.... 0000 = MnVer: 0x0
Exchange type: IKE_AUTH (35)
Flags: 0x08 (Initiator, No higher version, Request)
.... 1... = Initiator: Initiator
...0 .... = Version: No higher version
..0. .... = Response: Request
Message ID: 0x00000001
Length: 568
Payload: Encrypted and Authenticated Fragment (53)
Next payload: Identification - Initiator (35)
0... .... = Critical Bit: Not Critical
.000 0000 = Reserved: 0x00
Payload length: 540
Fragment Number: 1
Total Fragments: 2

IKEv2 Authentication

IKEv2 Authentication

Pre-shared key

Uses shared passwords to authenticate peers

Public Key Infrastructure

Uses certificates to authenticate peers based on CA trust points

Available in both versions

Built into IKEv2

Efficient

Quick computation

Extensible Authentication Protocol

Provides flexible authentication mechanisms

Method of authentication for 802.1x/NAC

Asymmetric keys

Passwords

Symmetric keys

IKEv2 Phases

IKEv2 Phases

Phase 1

IKE_SA_INIT

Establishes ISAKMP SAs

Phase 2

IKE_AUTH

Establishes IPsec SAs

Demo

Configure and test IKEv2

Analyze the packets

Summarizing IKEv2

Summary

IKEv1 versus IKEv2

IKEv2 benefits

IKEv2 modes

IKEv2 authentication

IKEv2 phases

Demo

Here comes IPv6!