IKEv2 Packet Exchange and Protocol Level Debugging

Document ID: 115936

Contributed by Atri Basu and Jay Young, Cisco TAC Engineers.
Mar 12, 2013

Contents

Introduction

This document describes the advantages of the latest version of Internet Key Exchange (IKE) and the differences between version 1 and version 2.

IKE is the protocol used to set up a security association (SA) in the IPsec protocol suite. IKEv2 is the second and latest version of the IKE protocol. Adoption for this protocol started as early as 2006. The need and intent of an overhaul of the IKE protocol was described in Appendix A of *Internet Key Exchange (IKEv2) Protocol* in RFC 4306.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

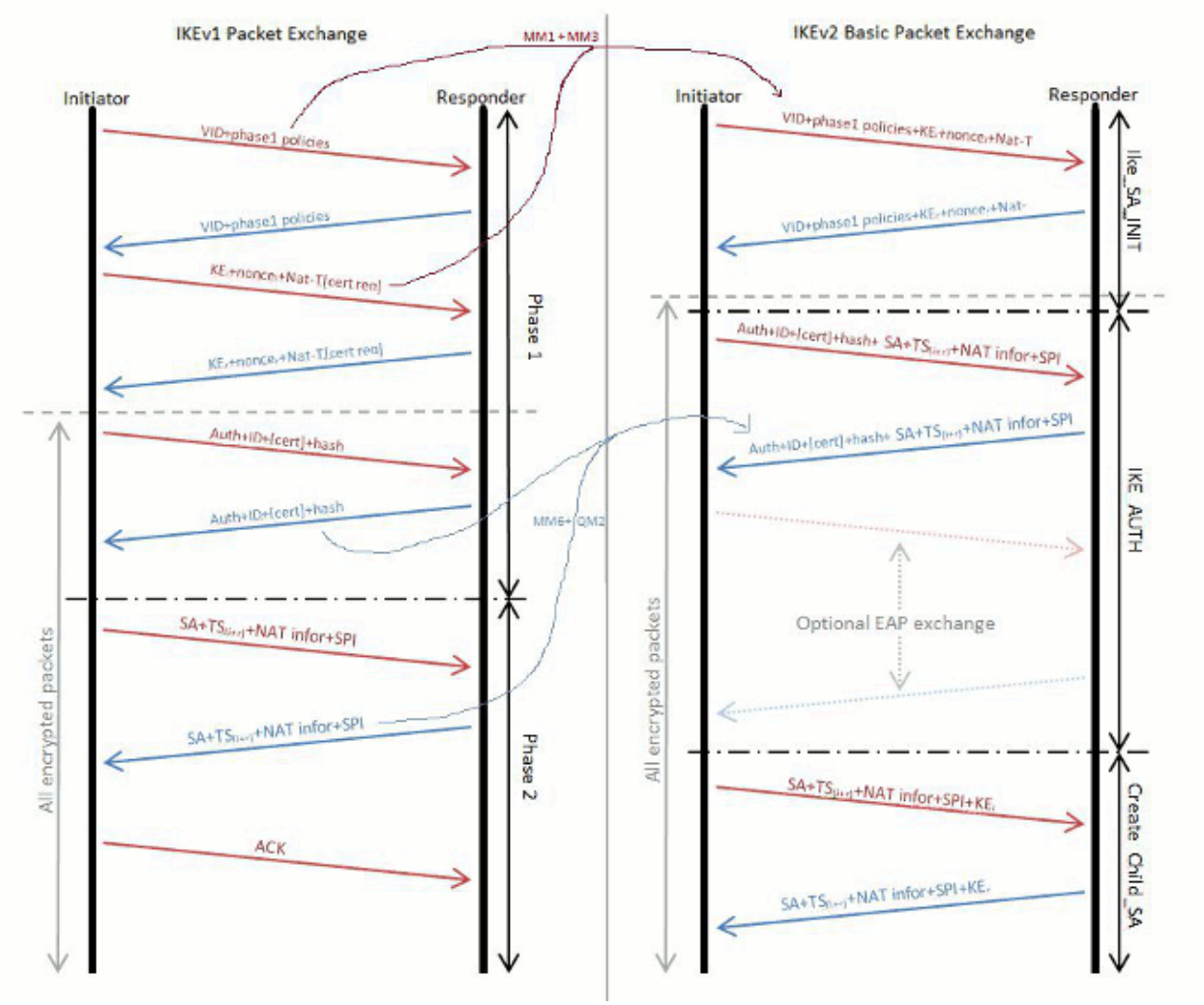
This document is not restricted to specific software and hardware versions.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Differences Between IKEv1 and IKEv2

While *Internet Key Exchange (IKEv2) Protocol* in RFC 4306 describes in great detail the advantages of IKEv2 over IKEv1, it is important to note that the entire IKE exchange was overhauled. This diagram provides a comparison of the two exchanges:



In IKEv1, there was a clearly demarcated Phase 1 exchange, which contains six packets followed by a Phase 2 exchange is made up of three packets; the IKEv2 exchange is variable. At best, it can exchange as few as four packets. At worst, this can increase to as many as 30 packets (if not more), depending on the complexity of authentication, the number of Extensible Authentication Protocol (EAP) attributes used, as well as the number of SAs formed. IKEv2 combines the Phase 2 information in IKEv1 into the IKE_AUTH exchange, and it ensures that after the IKE_AUTH exchange is complete, both peers already have one SA built and ready to encrypt traffic. This SA is only built for the proxy identities that match the trigger packet. Any subsequent traffic that matches other proxy identities then triggers the CREATE_CHILD_SA exchange, which is the equivalent of the Phase 2 exchange in IKEv1. There is no Aggressive Mode or Main Mode.

Initial Phases in IKEv2 Exchange

In effect, IKEv2 has only two initial phases of negotiation:

- IKE_SA_INIT Exchange
- IKE_AUTH Exchange

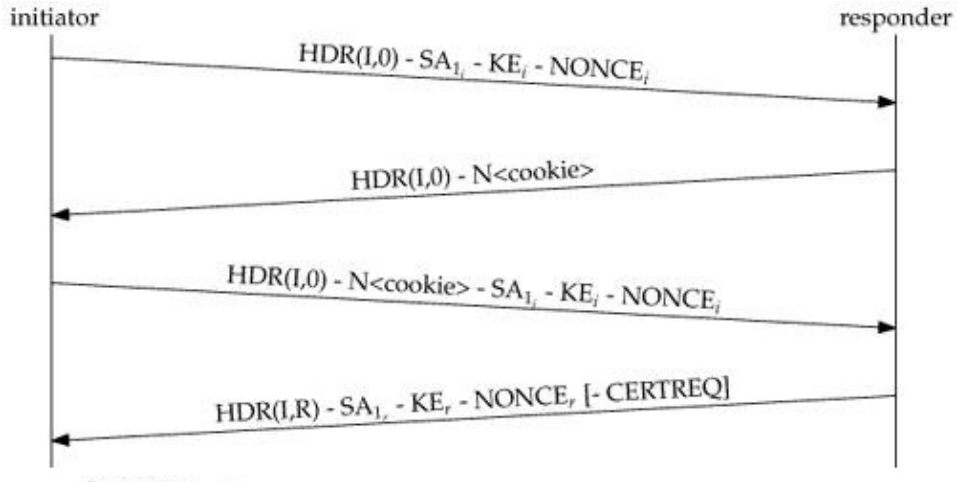
IKE_SA_INIT Exchange

IKE_SA_INIT is the initial exchange in which the peers establish a secure channel. After it completes the initial exchange, all further exchanges are encrypted. The exchanges contain only two packets because it combines all the information usually exchanged in MM1−4 in IKEv1. As a result, the responder is computationally expensive to process the IKE_SA_INIT packet and can leave to process the first packet; it

leaves the protocol open to a DOS attack from spoofed addresses.

In order to protect from this kind of attack, IKEv2 has an optional exchange within IKE_SA_INIT to prevent against spoofing attacks. If a certain threshold of incomplete sessions is reached, the responder does not process the packet further, but instead sends a response to the Initiator with a cookie. For the session to continue, the Initiator must resend the IKE_SA_INIT packet and include the cookie it received.

The Initiator resends the initial packet along with the Notify payload from the responder that proves the original exchange was not spoofed. Here is a diagram of IKE_SA_INIT exchange with cookie challenge:



IKE_AUTH Exchange

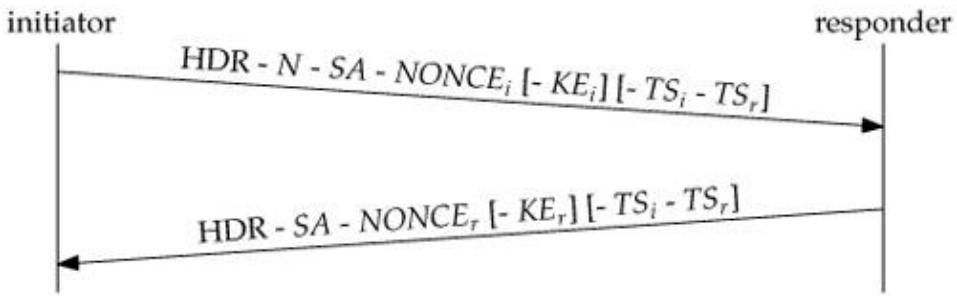
After the IKE_SA_INIT exchange is complete, the IKEv2 SA is encrypted; however, the remote peer has not been authenticated. The IKE_AUTH exchange is used to authenticate the remote peer and create the first IPsec SA.

The exchange contains the Internet Security Association and Key Management Protocol (ISAKMP) ID along with an authentication payload. The contents of the authentication payload is dependent on the method of authentication, which can be Pre−Shared Key (PSK), RSA certificates (RSA−SIG), Elliptic Curve Digital Signature Algorithm certificates (ECDSA−SIG), or EAP. In addition to the authentication payloads, the exchange includes the SA and Traffic Selector payloads that describe the IPsec SA to be created.

Later IKEv2 Exchanges

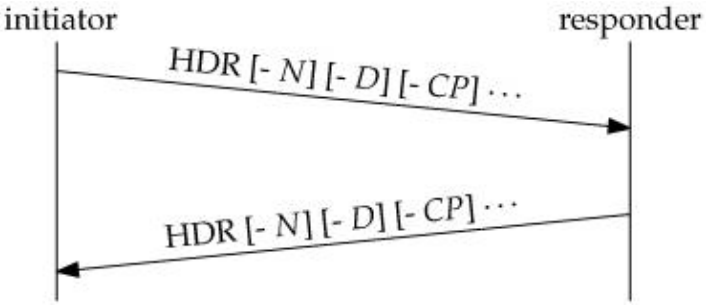
CREATE_CHILD_SA Exchange

If additional child SAs are required, or if the IKE SA or one of the child SAs needs to be re−keyed, it serves the same function that the Quick mode exchange does in IKEv1. As shown in the this diagram, there are only two packets in this exchange; however, the exchange repeats for every rekey or new SA:



INFORMATIONAL Exchange

As it is in all IKEv2 exchanges, each INFORMATIONAL Exchange request expects a response. Three types of payloads can be included in an INFORMATIONAL exchange. Any number of any combination of payloads can be included, as shown in the this diagram:



- The Notify payload (N) has already been seen in conjunction with cookies. There are several other types as well. They carry error and status information, as they do in IKEv1.
- The Delete payload (D) informs the peer that the sender has deleted one or more of its incoming SAs. The responder is expected to delete those SAs and usually includes Delete payloads for the SAs that correspond in the other direction in its response message.
- The Configuration payload (CP) is used to negotiate configuration data between the peers. One important use of the CP is to request (request) and assign (response) an address on a network protected by a security gateway. In the typical case, a mobile host establishes a Virtual Private Network (VPN) with a security gateway on its home network and requests that it be given an IP address on the home network.

  Note: This eliminates one of the problems that the combined use of Layer 2 Tunneling Protocol (L2TP) and IPsec is intended to solve.

Related Information

- **ASA IKEv2 Debugs for Site−to−Site VPN with PSKs TechNote**
- **ASA IPsec and IKE debugs (IKEv1 Main Mode) Troubleshooting TechNote**
- **IOS IPSec and IKE debugs − IKEv1 Main Mode Troubleshooting TechNote**
- **ASA IPSec and IKE debugs − IKEv1 Aggressive Mode TechNote**
- **Cisco ASA 5500 Series Adaptive Security Appliances**
- **Cisco ASA 5500 Series Adaptive Security Appliances Software Downloads**
- **IPSec Negotiation/IKE Protocols**
- **Cisco IOS Firewall**
- **Cisco IOS Software**
- **Secure Shell (SSH)**
- **IPSec Negotiation/IKE Protocols**
- **Technical Support & Documentation − Cisco Systems**

Updated: Mar 12, 2013 Document ID: 115936