Обмен пакетами IKEv2 и отладка уровня протокола

Содержание

Введение

Этот документ описывает преимущества последней версии Протокола IKE и различий между версией 1 и версией 2.

IKE является протоколом, используемым для устанавливания сопоставления безопасности (SA) в комплекте Протокола IPSec. IKEv2 является второй и последней версией протокола IKE. Принятие для этого протокола запустилось уже в 2006. Потребность и намерение перестройки протокола IKE были описаны в Приложение A *Обмена ключами между сетями (IKEv2) Протокол* в RFC 4306.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

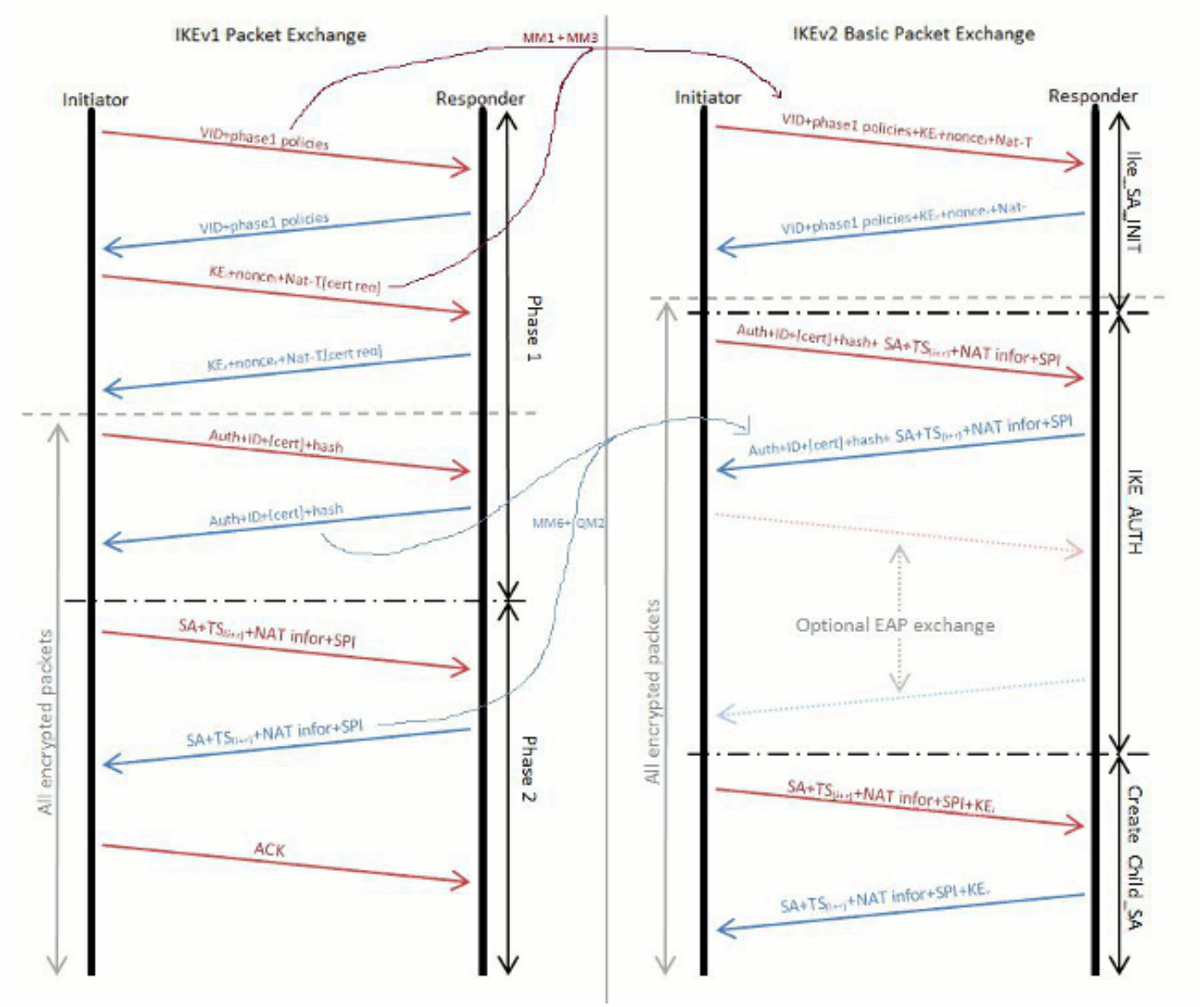
Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные

обозначения технических терминов Cisco.

Различия между IKEv1 и IKEv2

В то время как *Обмен ключами между сетями (IKEv2), Протокол* в RFC 4306 описывает очень подробно преимущества IKEv2 по IKEv1, важно обратить внимание, что был перестроен весь обмен IKE. Эта схема предоставляет сравнение двух обменов:



В IKEv1 был ясно разграниченный обмен Фазы 1, который содержит шесть пакетов, придерживавшихся обменом Фазы 2, составлен из трех пакетов; обмен IKEv2 является переменным. В лучшем случае это может обмениваться только четырьмя пакетами. В худшем случае это может увеличиться до целых 30 пакетов (если не больше), в зависимости от сложности аутентификации, количества атрибутов Протокола EAP, используемых, а также количества сформированных SA. IKEv2 комбинирует информацию о Фазе 2 в IKEv1 в обмен IKE_AUTH, и это гарантирует, что после того, как обмен IKE_AUTH завершен, обоим узлам уже создали один SA и готовый зашифровать трафик. Этот SA только создан для идентичности прокси, которая совпадает с триггерным пакетом. Любой последующий трафик, который совпадает с другой идентичностью прокси тогда, инициирует обмен CREATE_CHILD_SA, который является эквивалентом обмена Фазы 2 в IKEv1. Нет никакого Агрессивного режима или Основного режима.

Начальные фазы в IKEv2 Exchange

В действительности IKEv2 имеет только две начальных фазы согласования:

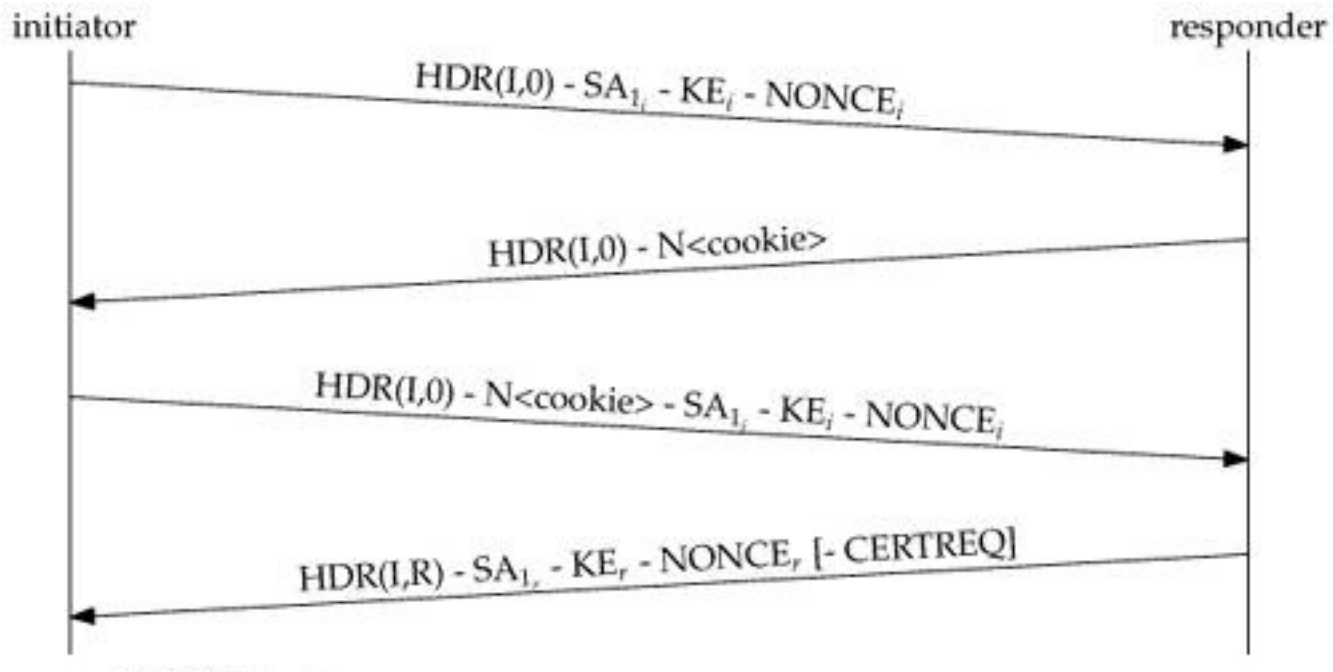
- Exchange IKE_SA_INIT
- Exchange IKE_AUTH

Exchange IKE_SA_INIT

IKE_SA_INIT является начальным обменом, в котором узлы устанавливают безопасный канал. После того, как это завершит начальный обмен, все дальнейшие обмены зашифрованы. Обмены содержат только два пакета, потому что это комбинирует всю информацию, которой обычно обмениваются в MM1-4 в IKEv1. В результате респондент является в вычислительном отношении дорогим для обработки пакета IKE_SA_INIT и может уехать для обработки первого пакета; это оставляет протокол открытым для DOS - атаки от поддельных адресов.

Для защиты от этого вида атаки IKEv2 имеет дополнительный обмен в IKE_SA_INIT для предотвращения против спуфинговых атак. Если определенный порог неполных сеансов достигнут, респондент не обрабатывает пакет далее, но вместо этого передает ответ Инициатору с cookie. Для сеанса для продолжения Инициатор должен повторно передать пакет IKE_SA_INIT и включать cookie, который это получило.

Инициатор повторно передает начальный пакет наряду с Уведомлять информационным наполнением от респондента, который доказывает, что не имитировался исходный обмен. Вот схема обмена IKE_SA_INIT с проблемой cookie:



Exchange IKE_AUTH

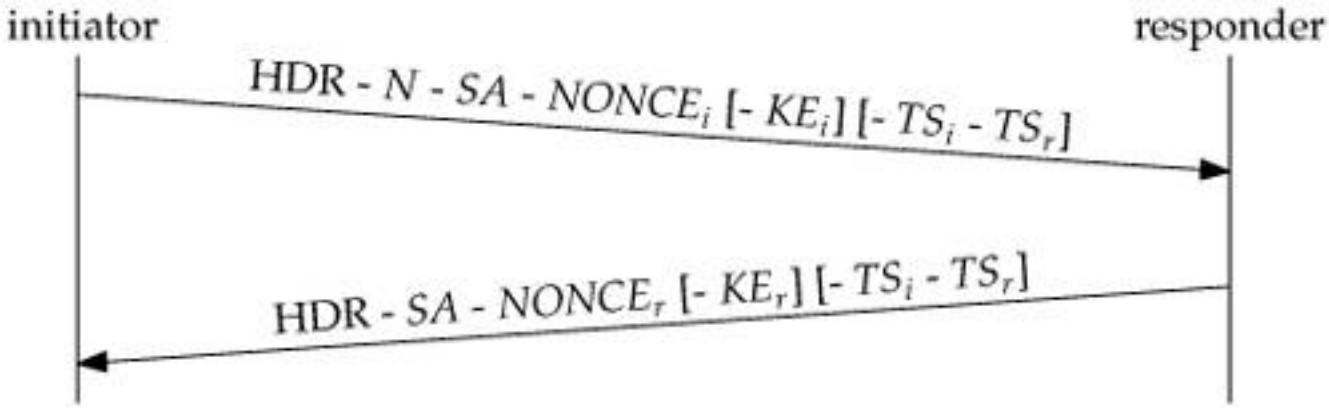
После того, как обмен IKE_SA_INIT завершен, IKEv2 SA зашифрованы; однако, удаленный узел не аутентифицировался. Обмен IKE_AUTH используется, чтобы аутентифицировать удаленный узел и создать первый контекст безопасности IPSec.

Обмен содержит ID Протокола ISAKMP наряду с опознавательным информационным наполнением. Содержание опознавательного информационного наполнения зависит от метода проверки подлинности, который может быть Предварительным общим ключом (PSK), сертификаты RSA (RSA-СИГНАЛ), сертификаты Алгоритма цифровой подписи Эллиптической кривой (ECDSA-SIG) или EAP. В дополнение к опознавательным информационным наполнениям обмен включает SA и информационные наполнения Селектора трафика, которые описывают контекст безопасности IPSec, который будет создан.

Позже обмены IKEv2

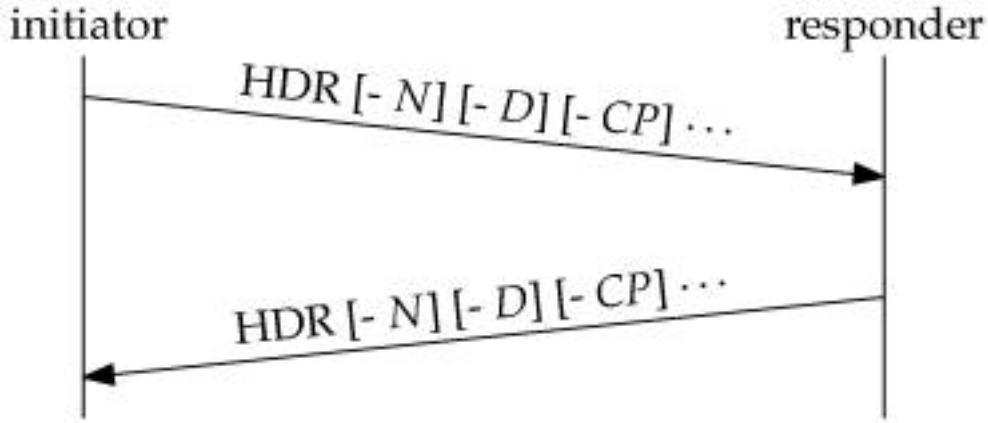
Exchange CREATE_CHILD_SA

Если дополнительные дочерние SA требуются, или если IKE SA или один из дочерних SA должны быть повторно введены, это служит той же функции, которую обмен Быстрого режима делает в IKEv1. Как показано в этой схеме, в этом обмене существует только два пакета; однако, обмен повторяется для каждого повторно вводить или новый SA:



ИНФОРМАЦИОННЫЙ Exchange

Поскольку это находится во всех обменах IKEv2, каждый ИНФОРМАЦИОННЫЙ запрос Exchange ожидает ответ. Три типа информационных наполнений могут быть включены в ИНФОРМАЦИОННЫЙ обмен. Любое количество любой комбинации информационных наполнений может быть включено, как показано в этой схеме:



- Уведомлять информационное наполнение (N) было уже замечено в сочетании с cookie. Также существует несколько других типов. Они несут ошибку и сведения о статусе, как они делают в IKEv1.

- Удалить информационное наполнение (D) сообщает узлу, что отправитель удалил один или больше его входящих SA. Респондент, как ожидают, удалит те SA и обычно включает, Удаляют информационные наполнения для SA, которые соответствуют в другом направлении в его ответном сообщении.
- Информационное наполнение конфигурации (CP) используется для согласования о данных о конфигурации между узлами. Одно важное использование CP должно запросить (запрашивают) и назначают (ответ) адрес в сети, защищенной шлюзом безопасности. В типичном случае мобильный хост устанавливает Виртуальную частную сеть (VPN) со шлюзом безопасности в его домашней сети и запрашивает, чтобы этому дали IP-адрес в домашней сети.**Примечание:** Это устраняет одну из проблем, которые объединенное использование протокола туннелирования на уровне 2 (L2TP) и IPsec предназначено для решения.

Дополнительные сведения

- Отладки ASA IKEv2 для сквозного VPN-соединение с PSK TechNote
- IPsec ASA и отладки IKE (Основной режим IKEv1) Технические примечания по поиску и устранению проблем
- IPSec IOS и отладки IKE - Технические примечания по поиску и устранению проблем Основного режима IKEv1
- IPSec ASA и отладки IKE - Агрессивный режим IKEv1 TechNote
- CISCO ASA 5500 SERIES ADAPTIVE SECURITY APPLIANCES
- Загрузки программного обеспечения многофункциональных устройств защиты Cisco ASA серии 5500
- Согласование IPsec/Протоколы IKE
- (межсетевой экран Cisco IOS)
- ПО Cisco IOS)
- Secure Shell (SSH)
- Согласование IPsec/Протоколы IKE
- Cisco Systems – техническая поддержка и документация