Знакомство с IPSEC

IPsec является лучшим набором средств защиты IP данных при прохождении пакета из одного места в другое. IPsec защищает только IP 3й уровень и выше. IPsec использует шифрование данных.

IPsec состоит из следующих наборов протоколов, которые обеспечивают следующие возможности:
Data confidentiality (конфиденциальность данных)
обеспечивает приватность данных между участниками IPsec VPN. Причем эти каналы используются через Inernet. Данные шифруются, что и обеспечивает их конфиденциальность.

Data intergrity (целостность данных)
гарантирует что полученные данные не были изменены или подменены при передаче через IPsec VPN. Обычно используется хэширование данных, и передача хэш ключа.

Data origin authentication (проверка источника данных)
проверяет источник IPsec VPN. Подлинность источников проверяется на каждом конце тунеля.

Anti-replay (проверка подделки данных)
проверяет что пакеты не были дублированы через VPN, используя последовательности (sequence number) и переменное окно (sliding window) принимающей стороной.

SA (security association) IPsec использует три основных протокола:

Internet Key Exchange (IKE)
Encapsulation Security Payload (ESP)
Authentication Header (AH)

IKE Internet Key Exchange - протокол для обмена и договоренности параметров безопасности и ключами аутентификации. Также обменивается ключами для symmetrical encription algoritm внутри IPsec VPN.

ESP Encapsulation Security Payload - протокол обеспечивающий конфиденциальность, целостность, аутентификацию испточника, и anti-replay функции IPsec. К тому же это одновременно и протокол шифрования. Он использует следующие методы шифрования:

AH Authentication Header - обеспечивает целостность данных, проверку источника, опционно функцию anty-replay. Конфиденциальность (шифрование) данных он не обеспечивает.

Оба AH и ESP используют Hash-based Message Authentication Code HMAC для проверки целостности данных и аутентификацию пира.

HMAC алгоритм в IPsec использует следующие алгоритмы:

Хэш алгоритм	Input	Output	Used by IPsec
Message Digest 5 (MD5)	Variable	128 bit	128 bit
Secure Hash Algorithm (SHA-1)	Variable	160 bit	First 96 bit

Оба MD5 и SHA-1 используют shared secret key для генерирования и проверки хэш. Криптографическая стойкость HMAC зависит от свойств хэш функции. Оба MD5 и SHA-1 используют входящие значения переменной длинны и создают хэш фиксированной длинны. **Хотя IPsec использует только 96 бит от 160 битной SHA-1, он считается более секьюрным чем MD5.**

Data Encription Standart (DES) - имеет широкое распространение, довольно старый формат.
Triple Data Encription Standard (3DES) - использует блок DES три раза.
Advanced Encription Standard (AES) - очень популярный симметричный протокол шифрования.

Аутентификация пира

Usernsme and password - пароль и логин должны быть сконфигурированы на обоих пирах. Т.к. пароль и логин не изменяются со временем то этот метод не является безопасным.
Preshared keys - та же концепция что и логин с паролем. В этом случае только одно значение используется на обоих концах
Digital Certificates - очень популярный метод аутентификации пользователей и устройств. Используются сервера аутентификаций, и если устр-во хочет себя идентифицировать оно отсылает сертификат на этот сервер, который и аутентифицирует его.

Internet Key Exchange (IKE)

Защитное соединение IPsec между двумя устройствами в начале может быть установлено по ключам, сохраненным на обоих устройствах. Но если эти ключи не изменять, то сеть может быть подвержена brute-force (перебор паролей) атакам. Постоянная смена ключей в ручном режиме так же невозможна.

IKE протоколы:

Это обмен IPsec параметрами и ключами. IKE автоматизирует процесс обмена ключами, и автоматически создает security assotoation SA. SA являются договоренными параметрами безопасности между пирами. IKE использует другие протоколы для выполнения аутентификации пиров и генерации ключей:
I**SAKMP** - Internet Security Assotiation and Key Management Protocol определяет процседуры о том как установить, согласовать, изменить и удалить SA. Все процессы согласования параметров проходят через ISAKMP, такие как header authentication и payload encapsulation. ISAKMP выполняет аутентификацию пира, но не включает обмен ключами.
Oakley - использует Diffie-Helman алгоритм для управления обмена ключами через IPsec SA. Diffie-Helman это криптографический алгоритм который позволяет двум точкам обмениваться shared ключами через незащищенный канал.

IKE фазы

Процесс работы протокола IKE разбит на 2 фазы, по которым устанавливается коммуникационный канал между двумя точками.

IKE phase 1 - главная IKE фаза. Между пирами устанавливается двунаправленное SA. Для приема и передачи используются разные SA. На 1й фазе также происходит и аутентификация пира. Существуют 2 IKE режима для установления двунаправленных SA это: main mode и aggressive mode. На этой фазе происходит согласование параметров, таких как метод хэширования и использование trasform set.

- **Использование pre-shared ключа для аутентификации** - VPN client инициирует aggressive mode. Каждый пир знает ключ другого пира. Этот ключ виден в running-config. Зная это есть дополнительная опция шифрования pre-shared ключей. В конфигурацию VPN клиента необходимо ввести данные о группе, имя и ключ.
- **Использование цифровых сертификатов** - VPN клиент инициирует main mode. Цифровые сертификаты используют RSA подписи на Easy VPN Remote устройстве. Эта поддержка обеспечивается RSA сертификатом сохраненным в центральном репозитории или в самом устройстве. С цифровым сертификатом для определения профайла группы используется специальное distinguished имя. Cisco рекомендует тайм аут в 40 секунд когда используются цифровые сертификаты.

IKE phase 1.5 - опциональная фаза которая обеспечивает дополнительную аутентификацию Xauth или Extended Authentication. IPsec может использовать username и password для установления соединения. Например когда устанавливается IPsec VPN соединение через cisco VPN client, то при настройке групповой аутентификации клиент запрашивает логин и пароль, дак вот эти логин и пароль и являются результатом работы Xauth.

IKE phase 2 - вторая главная IKE фаза, в которой происходит создание однонаправленной SA по параметрам согласованным 1й фазой. Т.е. на второй фазе происходит непосредственно создание SA для пользовательского трафика, а в перфой для служебного трафика. Использование однонаправленной SA означает что раздельный ключевой материал необходим для каждого направления. Фаза 2 использует IKE quick mode для установки каждой unidirectional SA.

IKE режимы

Состоит из трех режимов. На первой фазе IKE происходит происходит выбор одного из двух режимов (main или aggressive), а вторая фаза всегда использует режим quick.

IKE Main Mode

Состоит из обмена 6 сообщениями между пирами.
IPsec параметры и security policy - инициатор соединения шлет один или несколько предложений (proposals) и ответчик выбирает одно из них
Diffie-Helman public key exchange - IPsec пиры обмениваются публичными ключами.
ISAKMP session authentication - Каждый пир аутентифицируется другим пиром.

IKE Aggressive Mode

Состоит из обмена 3 пакетами.
Инициатор шлет все данные включая IPsec параметры, security policy, и Diffie-Helman публичные ключи.
Ответчик аутентифицирует пакет и шлет parameter proposal, key material, identification back.
Инициатор аутентифицирует пакет

IKE Quick Mode

Используется во время IKE фазы 2. Согласование на этом режиме уже проходит в защищенном режиме, установленном в первой фазе. Происходит согласование SA используемых для шифровки данных. А также обмен ключами для этих SAs.

Другие IKE функции

Dead Peer Detection (DPD)

Периодически шлются keepalive пакеты, каждые 10 сек. Если пает не пришел, то пир считается недоступным.

NAT traversal

Решает проблемы связанные с NAT, так как IPsec прячет заголовок L3. Во время первой фазы определяется используется ли NAT. После этого во время IKE фазы 2 решается использовать ли NAT traversal и устанавливается SA. NAT traversal работает путем вставки UDP заголовка до ESP заголовка в IPsec пакете. Этот новый заголовок транспортного уровня имеет незашифрованную информацию о портах, которая сохраняется в таблице трансляции.

Using NAT-T

To use NAT-T, you must perform the following tasks:
Step 1 Enter the following command to enable IPsec over NAT-T globally on the ASA:
crypto isakmp nat-traversal natkeepalive
The range for the natkeepalive argument is 10 to 3600 seconds. The default is 20 seconds.
For example, enter the following command to enable NAT-T and set the keepalive value to one hour.
hostname(config)# crypto isakmp nat-traversal 3600
Step 2 Select the before-encryption option for the IPsec fragmentation policy by entering this command:
hostname(config)# crypto ipsec fragmentation before-encryption
This option lets traffic travel across NAT devices that do not support IP fragmentation. It does not impede the operation of NAT devices that do support IP fragmentation.

Configuring IPsec Prefragmentation Globally

IPsec prefragmentation is globally enabled by default. To enable or disable prefragmentation for IPsec VPNs at the global level, perform this task beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# **crypto ipsec fragmentation before-encryption**	Enables prefragmentation for IPsec VPNs globally.
Step 2	Router(config)# **crypto ipsec fragmentation after-encryption**	Disables prefragmentation for IPsec VPNs globally.

Mode configuration

Позволяет отсылать IPsec атрибуты удаленному IPsec клиенту. IP адрес IPsec соединения, DNS и NETBIOS сервера и т.д. Таким образом работает Cisco VPN client.

Easy VPN Server

Для работы Easy VPN Server необходима поддержка ISAKMP политик с использованием Diffie-Hellman group 2 (1024bit) согласования. Этот протокол используется расширением Cisco Unity. Cisco Unity protocol базируется на идентификации клиентской группы. Клиент должен аутентифицировасть свою группу, а если включен XAUTH еще и себя(логином и паролем). При использовании Easy VPN Remote обязательно должна присутствовать аутентификация и шифрование. Cisco Unity протокол использует только ESP. Если включен режим сплит тунелинга, то NAT не используется, потому что туннель учавствует в маршрутизации.

таблице указаны значения параметров команды применяемых в настройке:

Transform type	IOS Transform	Description
AH Transform	ah-md5-hmac ah-sha-hmac	AH с MD5 аутентификацией AH с SHA аутентификацией
ESP Encription Transform	esp-aes esp-aes 192 esp-aes 256 esp-des esp-3des	ESP с 128 bit AES шифрованием ESP с 192 bit AES шифрованием ESP с 256 bit AES шифрованием ESP с 56 bit DES шифрованием ESP с 168 bit DES шифрованием
ESP Authentication transform	esp-md5-hmac esp-sha-hmac	ESP с MD5 аутентификацией ESP с SHA аутентификацией

DES с 56 битным ключем, может быть взломан в течении 24 часов современными компьютерами.
3DES использует 3 различных 56 битных ключа (DES encrypt, DES decrypt, DES encrypt) для создания цифрового текста.
AES использует от 128 - 256 бит. Также существует Rijndael. Их отличия в том что шаг шифрования в AES 64bit а в Rijndael 32 bit

VPN Ports

PPTP:
To allow PPTP tunnel maintenance traffic, open TCP 1723.
To allow PPTP tunneled data to pass through router, open Protocol ID 47.

L2TP over IPSec
To allow Internet Key Exchange (IKE), open UDP 500.
To allow IPSec Network Address Translation (NAT-T) open UDP 4500.
To allow L2TP traffic, open UDP 1701.

OpenVPN:

OpenVPN uses port 1194 udp and tcp:

Here’s the Cisco access list: (gre=Protocol ID 47, pptp=1723, isakmp=500, non500-isakmp=4500):

permit gre any any
permit tcp any any eq 1194
permit udp any any eq 1194
permit udp any any eq isakmp
permit udp any any eq non500-isakmp
permit udp any any eq 5500
permit tcp any any eq 1723
permit udp any any eq 1701

Table 3 Allowed Transform Combinations

Transform Type	Transform	Description
AH Transform (*Pick only one.*)	**ah-md5-hmac**	AH with the MD5 (Message Digest 5) (an HMAC variant) authentication algorithm. (No longer recommened).
	ah-sha-hmac	AH with the SHA (Secure Hash Algorithm) (an HMAC variant) authentication algorithm.
ESP Encryption Transform(*Pick only one.*)	**esp-aes**	ESP with the 128-bit Advanced Encryption Standard (AES) encryption algorithm.
	esp-gcm **esp-gmac**	The **esp-gcm** and **esp-gmac** transforms are ESPs with either a 128-bit or a 256-bit encryption algorithm. The default for either of these transforms is 128 bits. Both **esp-gcm** and **esp-gmac** transforms cannot be configured together with any other ESP transform within the same crypto IPsec transform set using the **crypto ipsec transform-set** command.
	esp-aes192	ESP with the 192-bit AES encryption algorithm.
	esp-aes256	ESP with the 256-bit AES encryption algorithm.
	esp-des	ESP with the 56-bit Data Encryption Standard (DES) encryption algorithm. (No longer recommended).
	esp-3des	ESP with the 168-bit DES encryption algorithm (3DES or Triple DES). (No longer recommended).
	esp-null	Null encryption algorithm.
	esp-seal	ESP with the 160-bit SEAL encryption algorithm.
ESP Authentication Transform(*Pick only one.*)	**esp-md5-hmac**	ESP with the MD5 (HMAC variant) authentication algorithm. (No longer recommended).
	esp-sha-hmac	ESP with the SHA (HMAC variant) authentication algorithm.
IP Compression Transform	**comp-lzs**	IP compression with the Lempel-Ziv-Stac (LZS) algorithm

Table 23-1 ISAKMP Policy Keywords for CLI Commands

Command	Keyword	Meaning	Description
isakmp policy authentication	rsa-sig	A digital certificate with keys generated by the RSA signatures algorithm	Specifies the authentication method the security appliance uses to establish the identity of each IPsec peer.
	dsa-sig	A digital certificate with keys generated by the DSA signatures algorithm	Specifies Digital Signature Algorithm signatures as the authentication method.
	pre-share (default)	Preshared keys	Preshared keys do not scale well with a growing network but are easier to set up in a small network.
isakmp policy encryption	des 3des (default)	56-bit DES-CBC 168-bit Triple DES	Specifies the symmetric encryption algorithm that protects data transmitted between two IPsec peers. The default is 168-bit Triple DES.
	aes aes-192 aes-256		The Advanced Encryption Standard supports key lengths of 128, 192, 256 bits.
isakmp policy hash	sha (default)	SHA-1 (HMAC variant)	Specifies the hash algorithm used to ensure data integrity. It ensures that a packet comes from where it says it comes from, and that it has not been modified in transit.
	md5	MD5 (HMAC variant)	The default is SHA-1. MD5 has a smaller digest and is considered to be slightly faster than SHA-1. A successful (but extremely difficult) attack against MD5 has occurred; however, the HMAC variant IKE uses prevents this attack.
isakmp policy group	1	Group 1 (768-bit)	Specifies the Diffie-Hellman group identifier, which the two IPsec peers use to derive a shared secret without transmitting it to each other. With the exception of Group 7, the lower the Diffie-Hellman group no., the less CPU time it requires to execute. The higher the Diffie-Hellman group no., the greater the security. Cisco VPN Client Version 3.x or higher requires a minimum of Group 2. (If you configure DH Group 1, the Cisco VPN Client cannot connect.) AES support is available on security appliances licensed for VPN-3DES only. To support the large key sizes required by AES, ISAKMP negotiation should use Diffie-Hellman (DH) Group 5. Designed for devices with low processing power, such as PDAs and mobile telephones, Group 7 provides the greatest security. The Certicom Movian Client requires Group 7.
	2 (default)	Group 2 (1024-bit)	
	5	Group 5 (1536-bit)	
	7	Group 7 (Elliptical curve field size is 163 bits.)	
isakmp policy lifetime	integer value (86400 = default)	120 to 2147483647 seconds	Specifies the SA lifetime. The default is 86,400 seconds or 24 hours. As a general rule, a shorter lifetime provides more secure ISAKMP negotiations (up to a point). However, with shorter lifetimes, the security appliance sets up future IPsec SAs more quickly.

IPSec
Стандарт IPSec был разработан для повышения безопасности IP-протокола. Это достигается за счет дополнительных протоколов, добавляющих к IP- пакету собственные заголовки. Т.к. IPSec - стандарт Интернет, то для него существуют RFC (Requests For Comments). Если есть интерес покопаться во внутренностях IPSec, то следующие RFC могут оказаться полезными:
- RFC 2401 IPSec;
- RFC 2402 AH;
- RFC 2406 ESP;
- RFC 2409 IKE.
Приведем краткое описание каждого дополнительного протокола. Начнем с сокращений, а затем посмотрим, как они укладываются в общую картину создания виртуальной частной сети.

AH (Authentication Header) - протокол заголовка идентификации. Обеспечивает целостность путем проверки того, что ни один бит в защищаемой части пакета не был изменен во время передачи. Не будем вдаваться в подробности, какая часть пакета защищается и где находятся данные AH-заголовка, так как это зависит от используемого типа шифрования и в деталях, с диаграммами описывается в соответствующем RFC. Отметим лишь, что использование AH может вызвать проблемы, например, при прохождении пакета через NAT-устройство. NAT меняет IP-адрес пакета, чтобы, например, разрешить доступ в Интернет с закрытого локального адреса. Так как пакет в таком случае изменится, контрольная сумма AH станет неверной. Также стоит отметить, что AH разрабатывался только для обеспечения целостности. Он не гарантирует конфиденциальности путем шифрования содержимого пакета.

ESP (Encapsulating Security Protocol) - инкапсулирующий протокол безопасности, который обеспечивает и целостность и конфиденциальность. В режиме транспорта ESP-заголовок находится между оригинальным IP-заголовком и заголовком TCP или UDP. В режиме туннеля заголовок ESP размещается между новым IP-заголовком и полностью зашифрованным оригинальным IP-пакетом.

Так как оба протокола - AH и ESP - добавляют собственные заголовки, они имеют свой ID протокола, по которому можно определить, что последует за заголовком IP. Каждый тип заголовка имеет собственный номер. Например, для TCP это 6, а для UDP - 17. При работе через firewall важно не забыть настроить фильтры, чтобы пропускать пакеты с ID AH-и/или ESP-протокола. Для AH номер ID - 51, а ESP имеет ID протокола равный 50. При создании правила не перепутайте случайно ID протокола с номером порта.

Третий протокол, используемый IPSec - это IKE или Internet Key Exchange protocol. Как следует из названия, он предназначен для обмена ключами между двумя узлами VPN. Насмотря на то, что генерировать ключи можно вручную, лучшим и более масштабируемым вариантом будет автоматизация этого процесса с помощью IKE. Помните, что ключи должны часто меняться, и вам наверняка не хочется полагаться на свою память, чтобы найти время для совершения этой операции вручную. Главное - не забудьте настроить правило на файрволе для UDP-порта с номером 500, так как именно этот порт используется IKE.

SA (Security Association), что можно приближенно перевести как "связь или ассоциация безопасности" - это термин IPSec для обозначения соединения. При настроенном VPN, для каждого используемого протокола создается одна SA-пара (то есть одна для AH и одна для ESP). SA создаются парами, так как каждая SA - это однонаправленное соединение, а данные необходимо передавать в двух направлениях. Полученные SA-пары хранятся на каждом узле. Если ваш узел имеет SA, значит VPN-туннель был установлен успешно.

Так как каждый узел способен устанавливать несколько туннелей с другими узлами, каждый SA имеет уникальный номер, позволяющий определить, к какому узлу он

относится. Это номер называется SPI (Security Parameter Index) или индекс параметра безопасности.
SA хранятся в базе данных с названием - кто бы подумал ;) - SAD (Security Association Database) или БД ассоциаций безопасности.
Каждый узел IPSec также имеет вторую БД - SPD или Security Policy Database (БД политики безопасности). Она содержит настроенную вами политику узла. Большинство VPN-решений разрешают создание нескольких политик с комбинациями подходящих алгоритмов для каждого узла, с которым нужно установить соединение.

Фаза Один и Фаза Два
Теперь давайте посмотрим как все это работает вместе. Установка и поддержка VPN-туннеля происходит в два этапа. На первом этапе (фазе) два узла договариваются о методе идентификации, алгоритме шифрования, хэш-алгоритме и группе Diffie Hellman. Они также идентифицируют друг друга. Все это может пройти в результате обмена тремя нешифрованными пакетами (так называемый агрессивный режим) или через обмен шестью нешифрованными пакетами (стандартный режим - main mode). При успешном завершении операции создается SA первой Фазы - Phase 1 SA (также называемый IKE SA) и процесс переходит к Фазе Два.

На втором этапе генерируются данные ключей, узлы договариваются насчет используемой политики. Этот режим, называемый быстрым режимом (quick mode), отличается от первой фазы тем, что может установиться только после первого этапа, когда все пакеты второй фазы шифруются. Такое положение дел усложняет решение проблем в случае неполадок на второй фазе при успешном завершении первой. Правильное завершение второй фазы приводит к появлению Phase 2 SA или IPSec SA, и на этом установка туннеля считается завершенной.

Когда же это все происходит? Сначала на узел прибывает пакет с адресом назначения в другом домене шифрования, и узел инициирует Фазу Один с тем узлом, который отвечает за другой домен. Допустим, туннель между узлами был успешно установлен и ожидает пакетов. Однако, узлам необходимо переидентифицировать друг друга и сравнить политику через определенное время. Это время известно как время жизни Phase One или IKE SA lifetime. Узлы также должны сменить ключ для шифрования данных через другой отрезок времени, который называется временем жизни Phase Two или IPSec SA lifetime. Phase Two lifetime короче, чем у первой фазы, так как ключ необходимо менять чаще. Типичное время жизни Phase Two - 60 минут. Для Phase One оно равно 24 часам.