VPN and IPSec

Cryptography

Bir haberleşmenin güvenli kabul edilebilmesi için Data Integrity, Origin Authentication ve Data Confidentially özelliklerini sağlaması gerekiyor.

|→ Data Confidentially, veriye iletim süresince üçüncü bir kişi tarafından erişilememesinin sağlanmasıdır. Bu özellik şifreleme algoritmaları kullanılarak sağlanıyor.

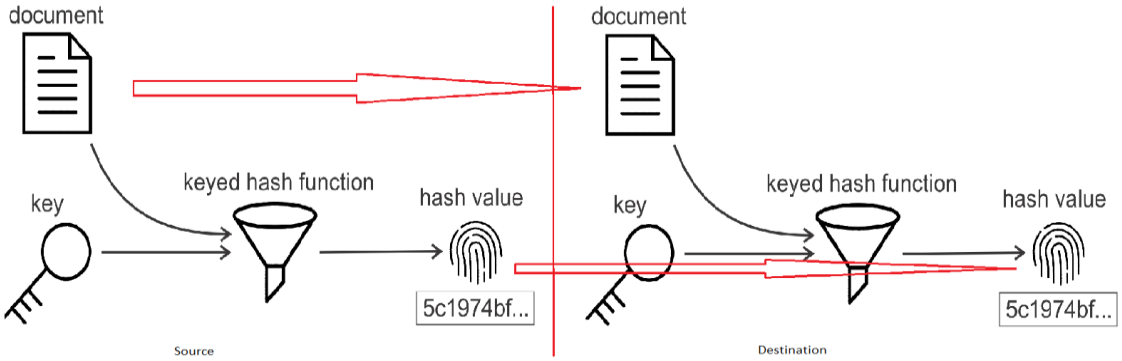
|→ Data Integrity, verinin kaynaktan çıktğı andah ihtibaren iletim süresince herhangi bir değişikliğe uğramadan hedefe ulaşıp ulaşamadığının kontorlüdür. İletim boyunca verinin değişmediğinin kontrolü genelde Hash algoritmalarıyla kontrol edilmektedir.

Hash Algoritmaları, tek yönlü matematik fonksiyonlarıdır. Burada "tek yönlü" kelimesiyle ifade elimek istenen hash agoritmasının sonucu kullanılarak hash algoritmasına verilen veri yeniden elde edilemiyor. Hash algoritmasına verilen veride en küçük bir değişikik dahi yapılması durumunda hash fonksiyonunun çıktısı tamamiyle değişmektedir. Bu nedenle Data Integrity kontrollerinde kullanılmaktadır.

- MD5 (Message Digest), girişine verilen veri boyutu farketmeksizin 128 bit boyutunda çıktı vermektedir. Günümüzde güvenli kabul edilmemektedir.
- SHA-1, girişine verilen veri boyutu farketmeksizin 160 bit boyutunda çıktı vermektedir. Günümüzde güvenli kabul edilmemektedir.
- SHA-2, girişine verien veri boyutu farklemteksizin farklı boyutlarda çıktılar elde edilebilmektedir. SHA-224 (224 bit), SHA-256 (256 bit), SHA-384 (384 bit), SHA-512 (512 bit). Güvenlik açıkları olduğu iddia edilse de günümüzde yaygın kullanılmaktadır.
- SHA-3, yazının hazırlandığı tarihte SHA hash algoritma ailesinin son üyesidir. SHA-2'de olduğu gibi SHA3-224 (224 bit), SHA3-256 (256 bit), SHA3-384 (384 bit), SHA3-512 (512 bit) çıktılar üretilebilmektedir.
- Hash algoritmaları her ne kadar tek yönlü olsa da çıktıları kullanılarak Dictionary Attack ile hash algoritmasının girişine verilen verilen elde edilebiliyor. Hash algoritmalarında çıktı boyutunun büyümesi verinin tespit sürecini zorlaştırdğı için daha güvenli kabul edilmektedir.

|→ Origin Authenticaton, hedefe ulaşan verinin doğru kaynaktan gönderilip gönderilmediğinin kontrol edilmesidir.

Verinin iletim boyunca değişikliğe uğrayıp uğramadığını anlamak için hash algoritmaları kullanmak yeteli olmuyor. Veri iletimi sırasında üçüncü bir kişi tarafından veriye ve hash bilgisine müdahale edilebilir (farklı bir veri ve bu verinin hash bilgisi eklenebilir). Bu durumda veri hedefe ulaştığında hash aloritması sonucu aynı çıkacağı için verinin ileitm boyunca değiiştirilip değiştirlmediğini anlamak mümkün olmayacaktır. Bu nedenle veri hash algoritmasına kaynak tarafından belirlenen bir secret key kullanılarak veriliyor (HMAC – Hashed Message Authentication Code).. Ortaya çıkan has bilgisi veri hedefe ulaştıığında kaynağın veriyi hashlemek için kullanıdığı secret key kullanılarak tekrar hash algoritmasına tabi tutulacaktır. Hash algoritmasının sonucunayla kaynağın gönderdiği hash bilgisinin aynı olup olmadığına bakılarak verinin doğru kaynaktan gelip gelmediği ve iletimi boyunca değiştirilip değiştirilmediği anlaşılacaktır.



|→ Secure Key Exchange, verinin iletimi boyunca bir değişikliğe uğramadığını veya doğru kaynaktan gelidiğini kontrol edebilmek için bir secret key kullanılıyordu. Bu key bilgisini aynı zamanda hedefin de bilmesi gerekiyor. Bu süreçte secret key'in hedefle güvenli bir şekilde paylaşılması gerekiyor. Secret key'i hedefe iletilirken asimetrik şifreleme algoritmaları kullanılmaktadır (Secret key hedefe iletildikten sonra veri iletişimi için simetrik şifreleme algoritmaları kullanılmaya başlanıyor). Peki simetrik ve asimetrik şifreleme nedir?

Şifreleme algoritmaları için simetrik ve asimetrik olamk üzere iki farklı mekanizma kullanılmaktadır.

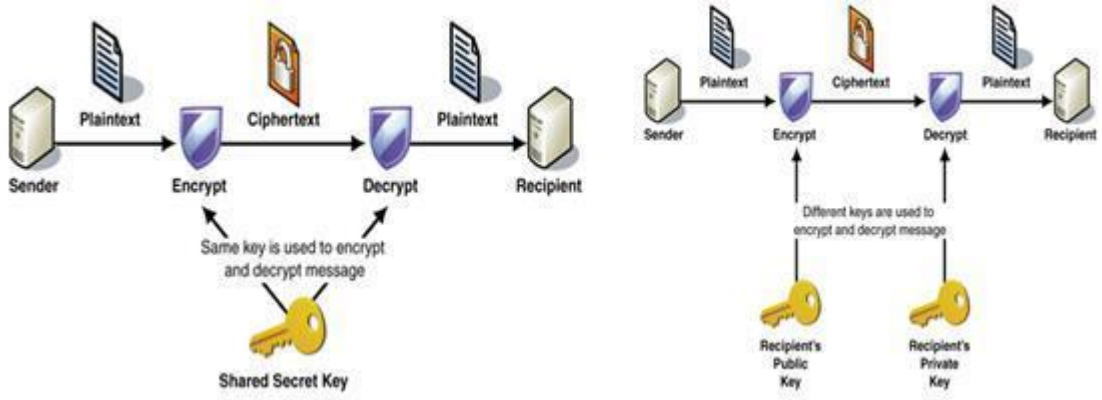
Simetrik şifreleme, bir metnin bir anahtar kelimeyle şifrelenerek hedefe ilrtilir. İletilen şifreli metin hedefte de aynı anahtar kullanılarak deşifre edilir (şifreleme-deşifre işlemleri için tek bir anahtar kullanılıyor). Bunun mekanizmayı kullanabilmek için anahtarın hedef ile güvenli bi r şekilde paylaşılması gerkeiyor. **RC4, AES, DES, 3DES, QUAD, SEAL** algoritmaları simetrik şifreleme algoritmalarına örnek verilebilir.

Asimetrik şifreleme, bir metni şifrelemek ve deşifre atmak için iki farklı anahtarın kullanıldığı şifrelem mekanizmasıdır. Bir metni asimetrik algoritamlardan biriyle şifrelenmek istendiğinde hedef üzerinde aralarında matematiksel ilişkilerin bulunan iki farklı key (public key, private key) oluşturacaktır. Hedefe mesaj iletmek isteyen kaynaklar verilerini hedefin belirlediği Public key'i kullanarak şifrelenecek (Public key herkezle paylaşılmaktadır) ve hedefe gönderecektir. Şifreli metin hedefe ulaştığında ise yine hedefin belirledği Private key kullanılarak metin deşifre edilmektedir (Private key sadece hedef tarafından bilinmektedir). Özetle Public key metni şifrelemede, Private key ise şifreli metni deşifre etmede kullanılmaktadır**. RSA, Diffie-Hellman- ECC, DSA, El Gamal** asimetrik şifreleme algoritmalarına örnek verilebilir.

- Burada önemli kısım kaynak göndereceği metni Public key kullanarak şifreledikten sonra elinde Private key olmadığıi için tekrar deşifre edememektedir.

Characteristic	Symmetric Cryptography	Asymmetric Cryptography
Key used for encryption/decryption	Same key is used	One key is used for encryption and another for decryption
Speed of encryption/decryption	Very fast	Slower
Size of resulting encrypted text	Usually same as or less than the original plaintext size	More than the original plaintext size
Known keys	Both parties should know the key in symmetric key encryption	One of the keys is known by the two parties in public key encryption
Usage	Confidentiality	Confidentiality, Digital signature

- Asimetrik şifrelemede anahtar boyutları simetriş şifrelemeye göre çok daha büyüktür. Bu ve tabloda belirtilen özelliklerden dolayı şifreli haberleşmede öncelikle hedefe secret key iletilirken asimetrik şifreleme algoritmaları kullanılıyor. Secret key hedefe güvenli bir şekilde iletildikten sonra iletişime daha hızlı olan simetrik şifrelem algoritmalarıyla devam ediliyor.
- Asimetrik şifreleme IKE (Internet Key Exchange), SSL (Secure Socket Layer), SSH (Secure Shell) ve PGP (Pretty Good Privacy) gibi daha birçok teknolojide kullanılmaktadır.



- IPSec konfigürasyonunda Diffie-Hellman algoritması kullanılmaktadır.
- KRİPTOGRAFİ ÜZERİNE AYRICA YAZI HAZIRLANACAKTIR.

VPN Teknolojileri

VPN (Virtual Private Network), farklı konumda bulunan networklere internet üzerinden uzaktan erişim yoluyla bağlanmayı sağlayan tenknolojidir. Bu erişim sırasında oluşturulan özel bağlantılar sayesinde kullanıcılar farklı konumda dahi olsalar bağlandıkları networklere güvenli bir şekilde erişip trafik oluşturabiliyorlar.

Service Provider VPNs, bir servis sağlayıcı tarafından oluşturulur ve yönetilir. Servis sağlayıcı, bir kuruluşun şubeleri arasında güvenli kanallar oluşturmak ve trafiği diğer müşteri trafiğinden izole edebilmek için katman 2 veya katman 3'te MPLS kullanır.

Enterprise VPNs, internet üzerinden kurumsal trafiğin güvenliğini sağlamak için kurum tarafından şubeler arası internet üzerinde güvenli bir kanal (ISP'den bağımsız) oluşturma çabasıdır. Site-to-site ve Remote Access VPN'ler kurum tarafından IPsec ve SSL VPN'ler kullanılarak oluşturulur ve yönetilir.

VPN Kullanmanın Faydaları

- Düşük Maliyet ; Kurumların çok daha a paralar ödeyerek şubeleri arasında bağlantılar kurabilmesini sağlıyor.
- Güvenlik ; Şifreleme ve kimlik doğrulama yapılması kurulan bağlantılara üçüncü bir kişinin eirşim sağlayabilmesine engel olunuyor.
- Ölçeklenebilirlik ; Kullanıcı sayısı değişiklik gösterdiğinde yeni kullanıcılar için ek bir donanım almaya gerek kalmadan kolaylıkla bağlanabiliyor. Bu sayede aynı anda binlerce kullanıcı aynı anda kurum networkünde bağlanıp (doğrudan bağlanmış gibi) çalışabiliyor.
- Uyumluluk ; farklı marka cihazlar kullanılsa da kullanıcılar bu durumdan etkilenmeden kurum netwrküne bağlanırken yüksek hızlarda erişim sağlayabiliyorlar.

VPN bağlantısı Site-to-site ve Remote Access olmak üzere iki farklı şekilde kurulabiliyor.

|→ Remote Access VPN, özel bir donanım ihtiyaç duyulmadan cihazlara bir yazılım kurularak VPN bağlantısının gerçekleştirilmesidir. Bu kullanımın Client-Based ve Clientless olmak üzere iki tipte kullanımı vardır.

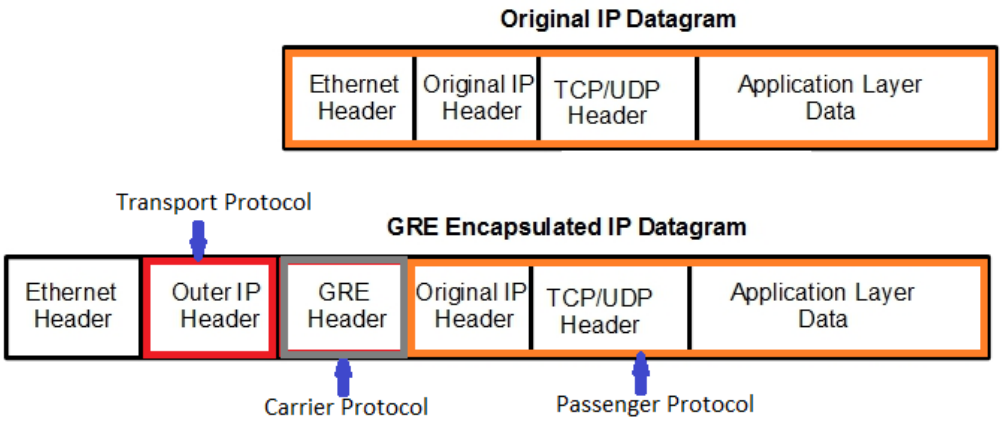
- Clienless VPN Connections, istemcinin browser üzerinden VPN bağlantısının kurulmasıdır.
- Client-Based VPN Connections, istemci bilgisayarıa VPN Client yazılımları kurularak bilgisayar üzerinden kurulan VPN bağlantılarıdır.

|→ Site-to-site VPN, kurumların VPN gateway'ler kurarak istemcilerin bu gateway üzerinden kurum networküne bağlanabilmesiyle verçekleştirilen VPN bağlantısıdır (bu kullanım şeklinde istemci bilgisayarına herhangi bir yazılım kurulmasına gerek kalmıyor - İstemciler paketleri VPN Gateway'e gönderiyor).

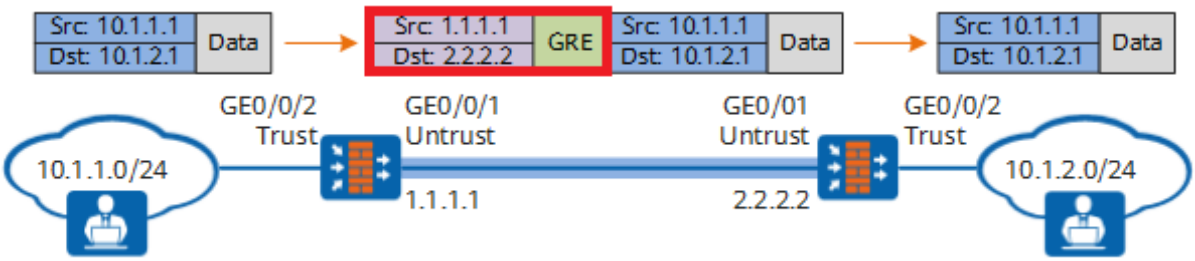
- Siteto-site VPN kullanımında aslında kaynak istemci de VPN Gateway'in kurum içine bakan arayüzü de priavate ip adresine sahiptir ve bilindiği üzere Private ip adresleriyle internete çıkıldığında paket daha ilk routerda drop ediliyordu. Bu nedenle Site-to-site VPN kullanılırken Cisco'nun teknolojilerinden olan GRE (Generic Routing Encapsulation) protokolü kullanılarak VPN tunneling yapılmaktadır.

GRE (Generic Routing Encapsulation), varolan paket başlığına ek L3 başlık bilgisi eklenerek (enkapsüle edilerek) paketin internet üzerinde hedefe ulaşabilmesini sağlayan protokoldür. Cisco tarafından çıkarılmıştır ama günümüze open standard haline gelmiş bir teknolojidir. Bu işlemde kullanılan terminolojilere bakıldığında;

- Passenger Protocol, GRE ile taşınacak verinin kendisidir.
- Carrier Protocol, veri hedefe ulaştırıldığında decapsüle edilirken L3'e GRE protokolünün kullanıldığını belirrtmek için kullanılan başlık alanıdır.
- Transport Protocol, GRE ile taşınacak veriye internet üzerinde kullanılacak ip bilgilerinin (Public Ip) eklendiği başlık alanıdır.



GRE Tünellemede işlem akışına bakıldığında paket istemcide Private kaynak ve hedef ip adresler içerecek şekilde oluşturuuyor. Oluşturulan pakete GRE başlık bilgileri eklenerek internet üzerindne kurumda kurulan VPN Gateway'a kadar iletilmesi sağlanıyor. Paket VPN Gateway'e geldiğinde başlık bilgisindeki Carrier protocol bilgisine bakılıyor ve paketin GRE ile kapsüllendiği anlaşılıyor. Paket dekapsüle edilerek kurum networkündeki (private ip adresine sahip) hedef cihaza yönlendiriliyor.



Her ne kadar GRE farklı tekolojilere sahip paketleri taşımakta kullanılsa da iletim boyunca bu paketlerin güvenliğini sağlamamaktadır. Yani sadece GRE ile kapsüllenen bir paket iletim boyunca üçüncü bir kişi tarafından müdahaleye maruz kalabilir. Bu nedenle IPSec protokolü kullanıılıyor.

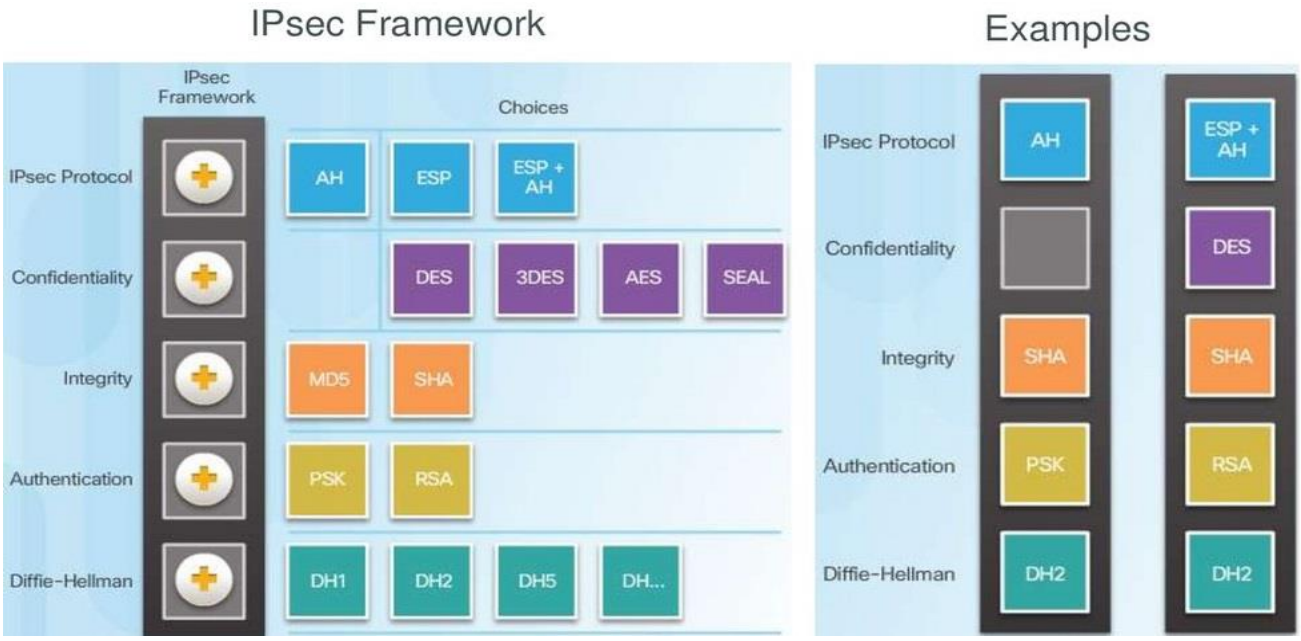
IPSec VPNs

IPSec protokolü GRE teknolojisinde olduğu gibi paketi enkapsüle etmektedir ama bunun için Carrier Protocol kısmında GRE kullanmak yerine AH, ESP gibi farklı bir protokol kullanmaktadır. Ayrıca paketi şifreleyerek iletim boyunca üçüncü bir kişinin erişimini de engellemektedir. Özetle IPSec için bir protokol kümesi denilebilir. Birçok protokolün kullanıldığı bir teknolojidir.

IPSec protokolü open standard protokol olduğu için farklı marka cihazlar kullanılsa dahi sorunsuzca IPSec tünelleri kurulabilmektedir. IPSec protokolü;

- Bağlantı şifrelendiği için gizlilik sağlamaktadır.
- Hash algoritmaları kullanılaark verinin iletim boyunca değiştirilip değiştirilmediği tespit edilebiliyor.
- Kimlik denetimi yapılmaktadır (IKE – Internet Key Exchange).
- Diffi-Hellman algoritması kullanılarak Secure Key Exchange işlemi gerçekleştiriliyor.

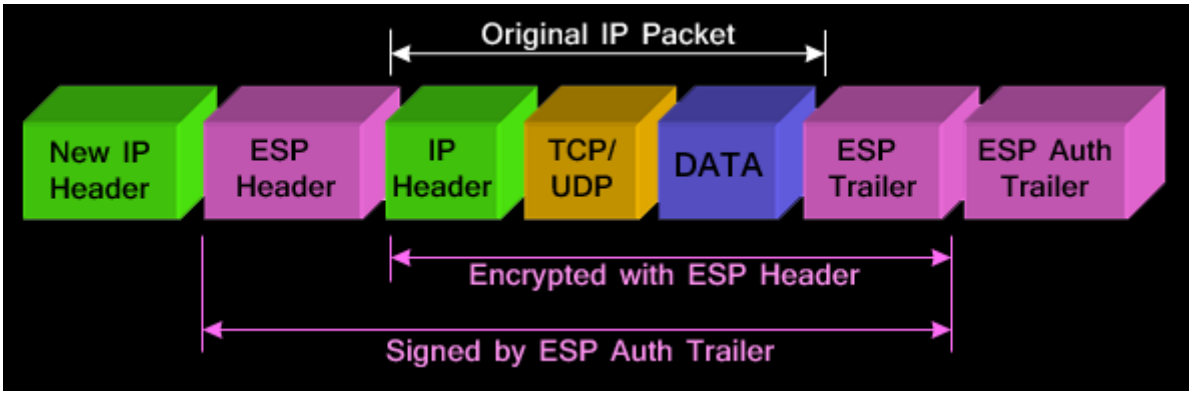
IPSec özellikleir listelenirken bağlantıalrın şifrelendiğinden, Diffi-Hellman algoritamsı kulanıldığından, hash algoritmalarının kullanıldığından bahsedildi ama herhangi bir algoritma/teknoloji özellikle belirtilmedi. Çünkü IPSec sürecinde bu özellikler olabildiğince esnek bırakılmıştır. Yani IPSec sürecinde kullanılacak algoritmalar/teknolojiler isteğe bağlı seçilebilmektedir.



|→ DH1, DH2... Diffie-Hellman algoritmasında kullanılan anahtar boyutunu belirliyor.

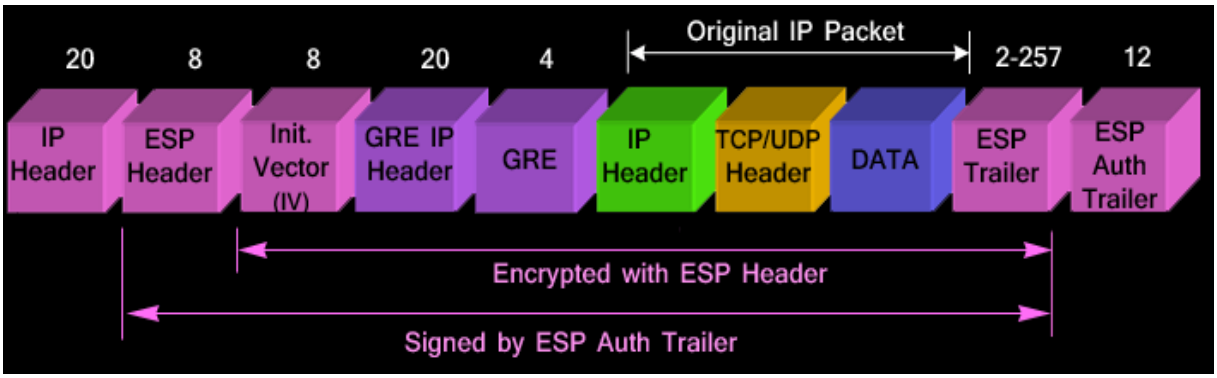
|→ IPSec protokol olarak AH (Authentication Header) veya ESP (Encapsulation Security Payload) kullanılabiliyor. AH gizlilik sağlamadığı (iletişimi şifrelemiyor) için günümüzde kullanılmamaktadır.

|→ IPSec için karşılıklı olarak cihazlarda seçilen şifreleme algoritmasının aynı olması gerkeiyor. Aksi taktirde bağlantı kurulamaz. Genelde günümüzde güvenli kabul edildiği için AES seçiliyor. Sadece AES algoritmasında kullanılacak anahtar boyutunun seçimi yapılıyor (128, 192 veya 256 bit).



GRE over IPSec

IPSec teknolojisi, Multicast paketleri desteklemiyor. Bu durumada oluşabilecek sorunalra bir örnek verilmek istenirse kurumlarda şubeler arasında yaygın kullanılan dinamik yönlendirme protokollerinden biri olan OSPF protokolünde ise en iyi rota seçimi yapılırken routerlar aralarında Multicast yayın kullanarak birbirlerine Hello paketleri gönderior ve bu sayede hem komşuluk kuruyor hem de durumlarını kontrol ediyorlardı. IPSec protokolü Multicast destekelmediği için routerlar arasında komşuluk dahi kurulamayacaktır. Benzer şekilde Multicast yayın kullanan teknolojiler de kullanılamayacaktır. Bu sorun paket IPSec ile kapsüllenmeden önce GRE protokolü ile kapsüllenerek giderilmiştir. GRE Multicast yayın desteklediği için paket IPSec protokolüyle kapsüllenmeden önce GRE protokolü ile kapsüllenerek Multicast adresleri destekler duruma gelmiştir. Özetle GRE ile Multicast desteği sağğlanıtken IPSec ile iletişimin güvenliği sağlanmaktadır.



|→ Paket başlığı büyüdüğü için doğal olarak taşınabilecek veri miktarı da azalmaktadır.

|→ IPSec yapabilmek için statik ip kullanılması gerekiyor.

DMVPN (Dynamic Multipoint VPNs)

IPSec her ne kadar esnek olsa da beraberinde çok fazla sorun da getirmektedir. Bu sorunlara karşılık oalrak Cisco DMVPN çözümünü geliştirmiştir.

DMVPN konfigürasyonunda sadece merkezdeki routera Hub konfigürasyonu yapılıyor. Merkezi routerda sadece tek bir Crypto Map tanımı yapılıyor. Burada sadece merkez routerun statik ip adresine sahip olması yeterli oluyor. Ardından Spoke (şube) cihazlarda da tek bir Crypto Map tamnımı yapılarak merkez routerun statik ip adresi tanıtılıyor. Konfigürasyon sonunda merkeze bağlanmak isteyen Spokes (şubeler) merkeze private ip adresleriyle bağlantı isteğinde bulunuyorlar. Merkez routerda bu private ip adres aralık bilgisi bir tabloda dinamik olarak tutuluyor. Merkez routera gelen paketler hangi şubeye iletilecekse tablodan private ip adres aralığı bilgisine bakılarak paket hedef şubeye yönlendiriyor.

- Bu sayede şubelerin ip adresler değiştiği zaman merkez routera yeniden istek talebinde bulunarak yeni ip adresini otomatik olarak öğretebiliyor.
- Merkez routerda her Spoke için ayrıca konfigürasyon yapmaya gerek kalmıyor.
- Spoke'lar merkez routerdan farklı Spoke'lara ait ip adresleri öğrenerek Spoke-to-Spoke bağlantı da kurabiliyorlar (kullandıkları şifreleme algoritmaları birbirini karşılıyorsa).

|→ DMVPN'de Multicas desteği vardır (Aslında IPSec'de olduğu gibi içerisinde GRE tunnel yapmaktadır ama bunun için ayrıca konfigürasyon yapılamasın gerek kalmıyor).

NOT

- Evlerde kullnaılan Wireless cihazlarının belirli bir sayıda kullnaıcı destekleyebilmesinin nedeni wifi'a bağlanan her kullanıcı için (hava ortamında verilerin şifreli aktarılabilmesi için) simetrik şifreleme algoritmaları kullanılarak şifreleme ve deşifre etme işlmeleri yapılıyor. Bu işlemler çok fazla CPU gerketirdiği için Wireless üzerindeki CPU'yu çatlatabiliyor.
- **GRE ile sadece Ethernet değil daha birçok teknolojinin pakettlerini kapsülleyerek internet üzerinde taşınabilmesini sağlıyor.**
- IPSec ile bir kurumun şubeleri arasında paketlerini merkeze gönderekre gerçekleştirebiliyor. Bunun için konfigürasyonlar sadece merkezde yapılıyor (Buna Hub and Spoke yapı deniliyor). Eğer ki şubelerin merkeze gelmeden doğrudan haberleşebilmesi isteniyorsa IPSec konfigürasyonu bütün şubelerde uygulanıyor (Spoke-to-Spoke). Uzun tanımlamalar yapıldığı için konfigürasyonu çok zahmetli olabiliyor).