GRE and IPSec VPN

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.

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

|→ Data Integrity, verinin kaynaktan çıktğı andah itibaren iletim süresince herhangi bir değişikliğe uğramadan hedefe ulaşıp ulaşamadığının kontorlüdür. İletim boyunca verinin değişmediği Hash algoritmaları kullanılarak kontrol edilmektedir.

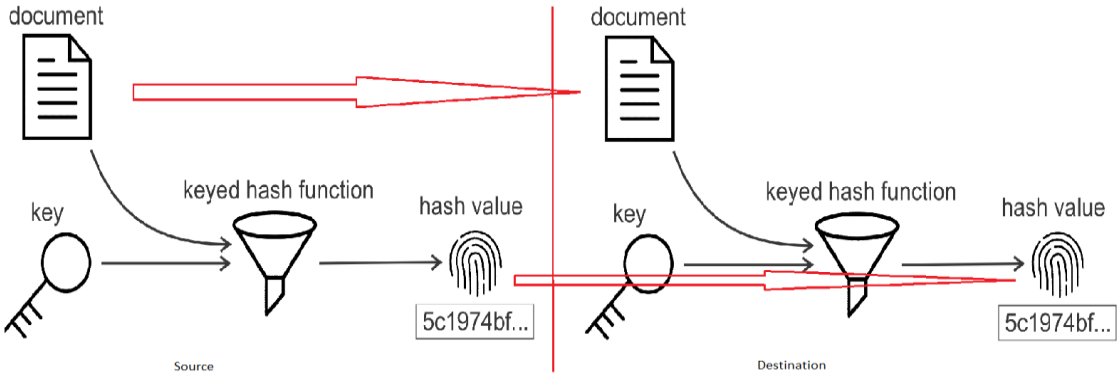
Hash Algoritmaları, tek yönlü matematik fonksiyonlarıdır. Burada "tek yönlü" kelimesiyle ifade elimek istenen Hash agoritmasının sonucu kullanılarak hash algoritmasına verilen veri yeniden elde edilememesidir. Hash algoritmasına verilen veride en küçük bir değişikik dahi yapılması durumunda hash fonksiyonunun 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.

Verinin iletim boyunca değişikliğe uğrayıp uğramadığını anlamak için Hash algoritmaları yeterli olmuyor. Veri iletimi boyunca üçüncü bir kişi tarafından veriye ve Hash bilgisine müdahale edilebilir (bu süreçte 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.

Verinin iletimi boyunca değiştirilip değiştirilmediğini anlamka için veri, Hash algoritmasına kaynak tarafından belirlenen bir Secret Key kullanılarak veriliyor (HMAC – Hashed Message Authentication Code).. Ortaya çıkan Hash bilgisi veri hedefe ulaştıığında kaynağın veriyi Hash'lemek için kullanıdığı Secret Key kullanılarak veri tekrar Hash algoritmasına tabi tutuluyor. Hash algoritmasının sonucuyla kaynağın gönderdiği Hash bilgisi karşılaştırılarak aynı olup olmadığına

bakılıyor. Bu sayede verinin doğru kaynaktan gelip gelmediği ve iletimi boyunca değiştirilip değiştirilmediği anlaşılıyor.



|→ 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?

Simetrik ve Asimetrik Şifreleme

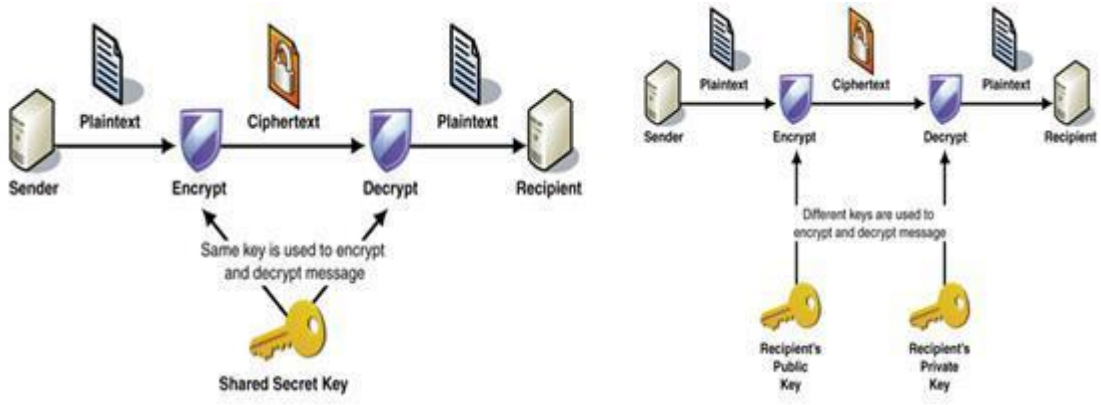
Şifreleme algoritmaları için simetrik ve asimetrik olamk üzere iki farklı mekanizma kullanılmaktadır.

- Simetrik Şifreleme, veriyi şifrelemke için de şifresini çözmek için de tek bir anahtarın kullanıldığı şifreleme mekanizmasıdır. Veri iletiminde ise bir veri bir anahtar kelimeyle şifrelenerek hedefe iletilir. İletilen şifreli veri hedefte de aynı anahtar kullanılarak deşifre edilir (şifreleme-deşifre işlemleri için tek bir anahtar kullanılıyor). Bunun mekanizmayı kullanabilmek için anahtarın hedef ile güvenli bir şekilde paylaşılması gerkeiyor. **RC4, AES, DES, 3DES, QUAD, SEAL** algoritmaları simetrik şifreleme algoritmalarına örnek verilebilir.

- Asimetrik şifreleme, bir veriyi şifrelemek ve deşifre atmak için iki farklı anahtarın kullanıldığı şifreleme mekanizmasıdır. Bir veri asimetrik algoritamlardan biriyle şifrelenmek istendiğinde hedef üzerinde aralarında matematiksel ilişkilerin bulunan iki farklı Key (Public Key, Private Key) oluşturacaktır. Hedefe veri göndermek isteyen kaynaklar, verilerini hedefin belirlediği Public Key'i kullanarak şifrelenecek (Public Key herkesle paylaşılmaktadır) ve hedefe gönderecektir. Şifreli veri hedefe ulaştığında ise yine hedefin belirledği Private Key kullanılarak metin deşifre edilmektedir (Private key sadece hedef tarafından bilinmektedir. Yani verisini Public Key kullanarak şifreleyen kaynak dahi elinde Private Key bulunmadığı için şifrelediği veriyi tekrar deşifre edememektedir). Özetle, Public Key veriyi şifrelemede, Private Key ise şifreli veriyi deşifre etmede kullanılmaktadır**. RSA, Diffie-Hellman- ECC, DSA, El Gamal** asimetrik şifreleme algoritmalarına örnek verilebilir. Bu algoritmaların temeli asal çarpamlara ayırma, eliptik eğriler gibi matematiksel zorluklara dayanmaktadır.

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 simetrik 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 şifreleme 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 az paralar ödeyerek şubeleri arasında bağlantılar kurabilmesini sağlıyor.
- **Güvenlik** ; Şifreleme ve kimlik doğrulama yapılması, kurulan bağlantılara üçüncü bir kişinin eirşim sağlayabilmesine engel oluyor.
- **Ölçeklenebilirlik** ; Kullanıcı sayısı değişiklik gösterdiğinde yeni kullanıcılar için ek bir donanım almaya gerek kalmadan kolaylıkla bağlanabilmeleri sağlanıyor. Bu sayede aynı anda binlerce kullanıcı aynı anda kurum networküne bağlanıp (doğrudan bağlanmış gibi) çalışabiliyor.
- **Uyumluluk** ; farklı marka cihazlar kullanılsa da kullanıcılar bu durumdan etkilenmeden kurum networküne bağlanırken yüksek hızlarda erişim sağlayabiliyorlar.

VPN Bağlantısı

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.

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

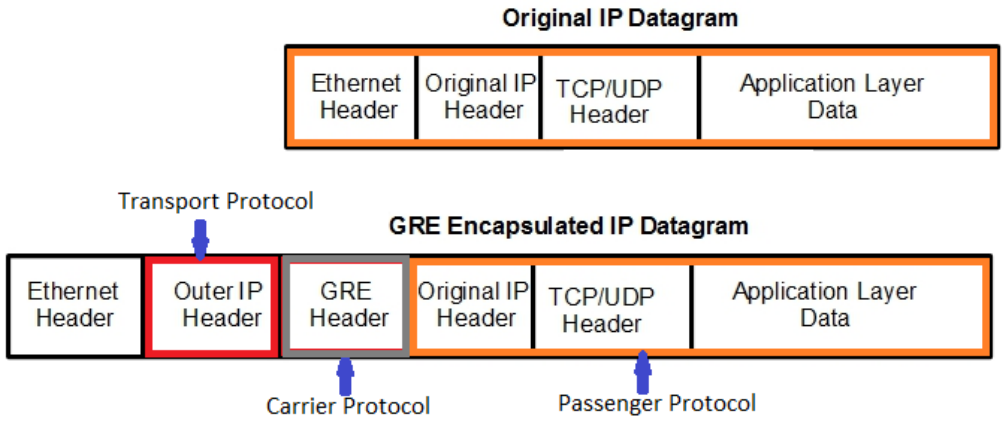
|→ **Site-to-site VPN**, kurumların VPN gateway'ler kurarak istemcilerin bu gateway üzerinden kurum networküne bağlanabilmesiyle gerçekleştirilen VPN bağlantısıdır (bu kullanım şeklinde istemci bilgisayarına herhangi bir yazılım kurulmasına gerek kalmıyor - İstemciler paketleri VPN Gateway'e gönderiyor).

- 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 ediliyor. Bu nedenle Site-to-site VPN kullanılırken Cisco'nun teknolojilerinden olan GRE (Generic Routing Encapsulation) protokolü kullanılarak VPN tunneling yapılmaktadır.

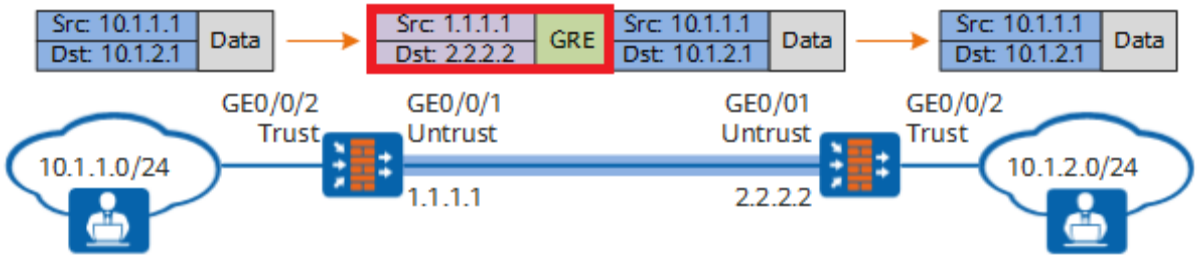
GRE (Generic Routing Encapsulation)

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 ulaştrıldığında 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 oluşturuluyor. Oluşturulan pakete GRE başlık bilgileri eklenerek internet üzerinden 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 (paket orjinalinde – GRE başlığı çıkarıldığında private ip adresine sahip) hedef cihaza yönlendiriliyor.



Her ne kadar GRE farklı tekolojilere sahip paketleri taşımak içim kullanılsa da iletim boyunca bu paketlerin güvenliğini sağlamamaktadır. Yani sadece GRE ile kapsüllenen bir paket iletim boyunca üçüncü bir kişi tarafından müdahaleye açık durumdadır. Bu nedenle iletimin güvenliğini sağlamak için IPSec protokolü kullanıılıyor.

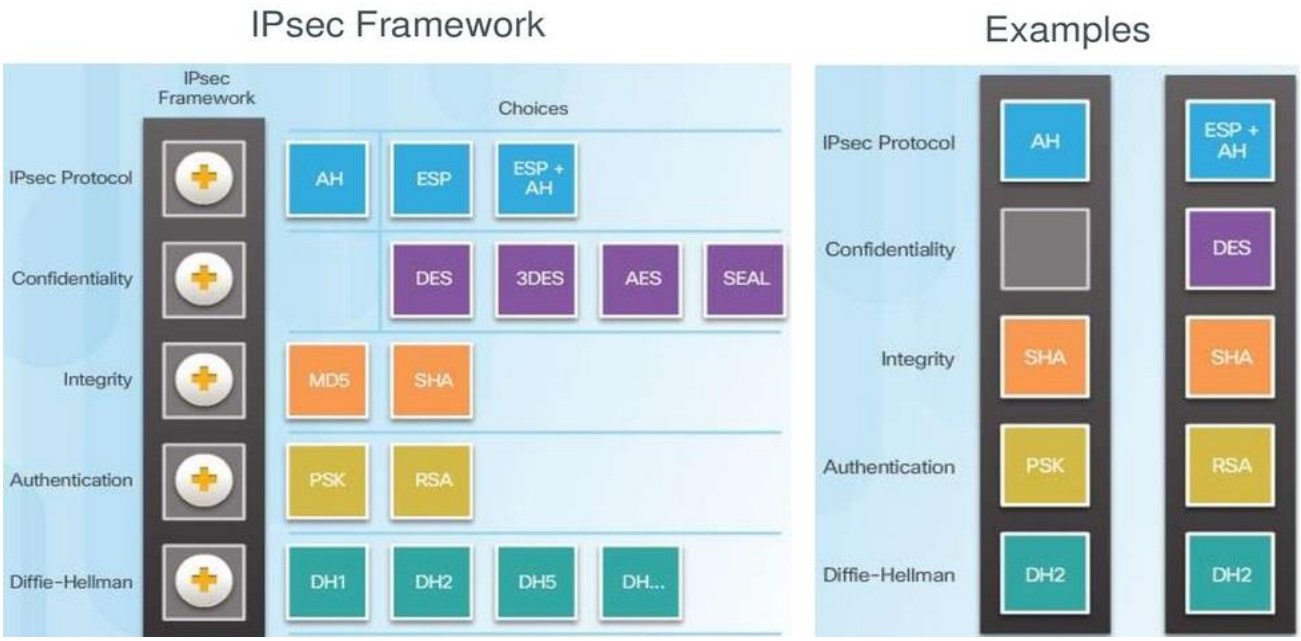
IPSec VPNs

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 kullanılarak verinin iletim boyunca değiştirilip değiştirilmediği tespitedilebilir.
- Kimlik denetimi yapılmaktadır (IKE – Internet Key Exchange).
- Diffi-Hellman algoritması kullanılarak Secure Key Exchange işlemi gerçekleştiriliyor.

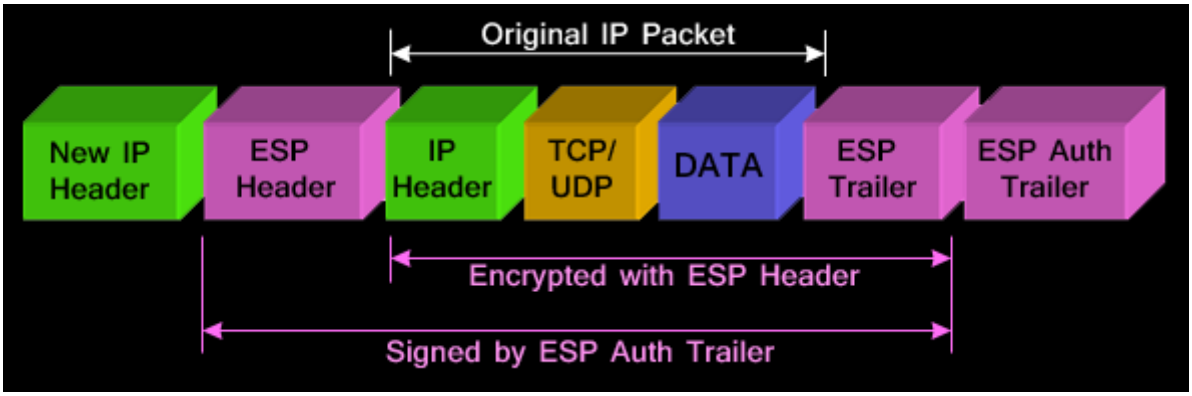
IPSec özellikleri listelenirken bağlantıların şifrelendiğinden, Diffi-Hellman algoritaması kulanıldığından, Hash algoritmalarının kullanıldığından bahsedildi ama herhangi bir algoritma/teknoloji özellikle belirtilmedi. Nedeni, IPSec sürecinde bu özellikler olabildiğince esnek bırakılmıştır. Yani IPSec 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. AES algoritmasında sadece kullanılacak anahtar boyutunun seçimi yapılıyor (128, 192 veya 256 bit).

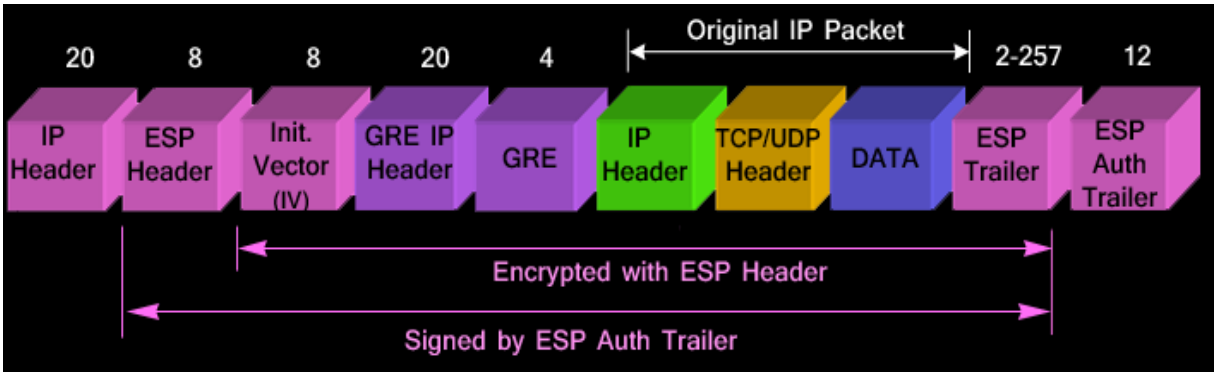


GRE over IPSec

IPSec teknolojisi, Multicast paketleri desteklemiyor. Bu durumada oluşabilecek sorunlara bir örnek verilmek istendiğinde, kurumlarda şubeler arasında yaygın kullanılan dinamik yönlendirme protokollerinden biri olan OSPF protokolünde routerlar aralarında haberleşirken (Hello paketiyle komşuluk kurma sürecinde dahi) Multicast adresler kullanıyor. Multicast adresler sayesinde routerlar aralarında hem komşuluk kuruyor hem de karşılıklı olarak durumlarını kontrol ediyorlar. IPSec

protokolü Multicast destekelmediği için routerlar arasında komşuluk dahi kurulamayacaktır. Benzer şekilde Multicast yayın kullanan teknolojiler de kullanılamayacaktır.

IPSec protokolünün Multicast adres desteklememesi durumu paketlerin 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 sağlanırken IPSec ile iletişimin güvenliği sağlanmaktadır.



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

|→ IPSec yapabilmek için routerların ISP/Internet kısmına bakan arayüzlerde 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).

GRE Konfigürasyonu

- Router genelinde (yönlendirme protokolleri – rota tanımları gibi) ve routerların internete bakan arayüzlerinde gerekli konfigürasyonlar (ip adres ataması ve portun açılması gibi) yapıldıktan sonra "**interface tunnel <Tunnel Number>**" komutuyla bir Tunnel arayüzüne giriş yapılıyor.
    - Tunnel değeri routerlarda karşılıklı olarak farklı seçilebilir.
- Tunnel arayüzünde ilk olarak "**ip address <Network Address> <Subnet Mask>**" komutuyla Tunnel üzerinde kullanılmak üzere routera Private ip adres tanımı yapılıyor.
- Private ip adres tanımından sonra GRE Tunnel'ın kullanılacağı kaynak ve hedef routerların Public ip adresleri "**tunnel source <Interface ID | Ip Address >**" ve "**tunnel destination <Ip Address>"** komutlarıyla tanımlanıyor.
    - ISP'ye bağlı arayüzlerde ip değişikliği olması ihtimaline karşı kaynak ip bilgisi olarak Exit Interface de belirtilebiliyor ama bu durumda ARP sorgusu yapılmadığı için routerlarda Proxy ARP özelliğinin devrede olması gerekiyor.
- Son olarak hedef networke gönderilecek paketlerin GRE Tunnel'a yönelendirilmesi için "**ip route <Dest Networ Address> <Subnet Mask> <Next Hop (GRE Private Ip Address) Ip Address>"** komutuyla statik rota tanımı yapılması gerekiyor. Bu adımdan sonra paketler GRE Tunnel üzerinden kapsüllenerek gönderilecektir.
- İsteğe bağlı olarak "**ip mtu <MTU Size>**" komutuyla kullanılacak MTU (Maximum Trasmission Unit) boyutu veya "**ip tcp adjust-miss <MISS Size>**" komutuyla MSS (Maximum Segment Size) değeri belirlenebiliyor.

Uygulamasını "Lab -> Çalışamlar -> GRE" dizini altında bulabilirsin.

```
R1(config)#interface tunnel 0

R1(config-if)#ip address 192.168.3.1 255.255.255.0
R1(config-if)#tunnel source gi 0/0
R1(config-if)#tunnel destination 20.0.0.3
R1(config-if)#tunnel mode gre ip
R1(config-if)#exit
R1(config)#ip route 192.168.2.0 255.255.255.0 192.168.3.3
```

```
R1#sh int tun 0
Tunnel0 is up, line protocol is up (connected)
  Hardware is Tunnel
  Internet address is 192.168.3.1/24
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 10.0.0.1 (GigabitEthernet0/0), destination
20.0.0.3
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255
  Fast tunneling enabled
  Tunnel transport MTU 1476 bytes
```

IPSec Konfigürasyonu

IPSec konfigürasyonu üç ayrı adımda/fazda gerçekleştiriliyor (Konfigürasyon öncesinde "sh licanse feature" komutuyla securityk9 özelliğinin aktif olup olmadığı kontrol edilmelidir. Securityk9 özelliği devrede değilse IPSec konfigürasyonu yapılamıyor. Securityk9 özelliğini açmak için Global konfigürasyon modunda "**license boot module <Router Series> technology-package securityk9"** komutu kullanılıyor. Ardından "**do wr**" ve "**do reload**" komutlarıyla cihazın yeniden başlatılması gerekiyor). Bunlar;

1- IPSec konfigürasyonunda ilk adım olarak cihazdan gönderilecek paketler için kullanılacak politikaların belirlenmesi gerekiyor. Bunun için ilk olarak Policy tanımı yapılması gerekliyor. Bunun için "**crypto isakmp policy <Policy Number>**" komutuyla tanımların yapılacağı arayüze giriş yapılıyor.
   - Bu arayüzde ilk olarak "**authentication pre-share**" komutuyla kullanılacak kimlik doğrulama mekanizması tanımlanıyor.
   - Veri bütünlüğünü sağlamak için "**hash >Hash Algorithm>**" komutuyla kullanılacak hash algorimtası belirleniyor.
   - Gizlilik sağlamak için "**encryption <Encryption Algorithm>**" komutuyla kullanılacak şifreleme algritması seçiliyor.
   - Kullanılacak Diffie-Heliman algoritmasını "**group <DH-Number>**" komutuyla seçiliyor.
   - Son olarak da "**lifetime <Time>**" komutuyla kullanılan şifrenin geçerlilik süresi belirtiliyor.

```
crypto isakmp policy 11
encryption aes
hash sha
authentication pre-share
group 2
lifetime 8640
crypto isakmp key MyPass address 20.0.0.3
exit

crypto ipsec transform-set TS1 esp-aes esp-sha-hmac


access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255

crypto map CM1 11 ipsec-isakmp
set peer 20.0.0.3
set transform-set TS1
match address 110
exit

int s 0/3/0
crypto map CM1
exit
```

- İlk adımda son olarak tünelleme yapılan her iki routerda da kimlik doğrulama sürecinde kullanılacak parola "**crypto isakmp key <Password> address <Dst Global Ip Address>** " komutuyla tanımlanıyor.

2- İkinci adımda (negotiation da deniyor) ilk olarak "**crypto ipsec transform-set <Transdorm Set Name> <Encryption Algorithm> <Hash Alorithm**" komutuyla transform-set tanımı yapılıyor (Burada isakmp politikası belirlerken kullanılan şifreleme ve hash algıritmaları kullanılıyor). |→ İkinci adım verinin nasıl şifreleneceğini ve Hash'inin nasıl alınacağını tanımlar. Birinci adımda kullanılan tanımlar da yönetim trafiğinin nasıl şifreleneceğini ve Hash'inin nasıl alınacağıyla ilgili tanımlardır.

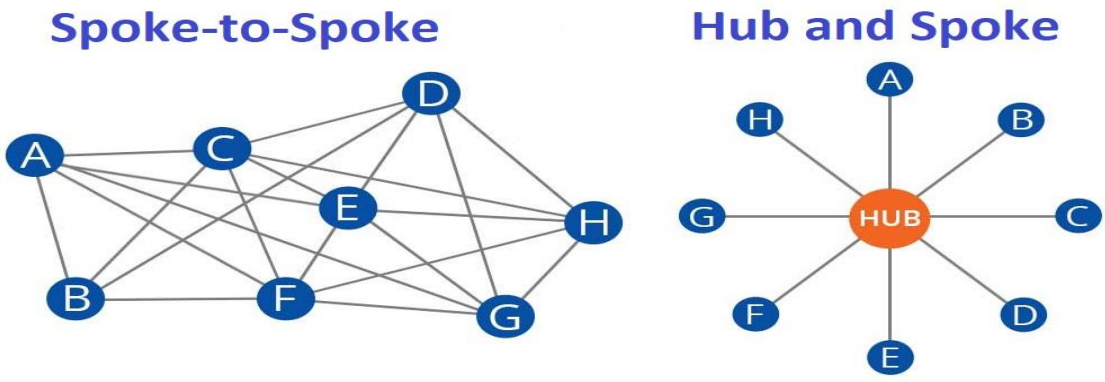
3- Üçüncü adımda öncelikle tünellenecek trafiğin tünele girişini sağalmak için bir ACL tanımı yapılması gerekiyor. Bunun için örnek olarak "**access-list <Extended ACL Number> permit ip <Src Private Ip Address> <Src Wildcard Mask> <Dst Private Ip Address> <Dst Wildcard Mask>**" formatı kulanılabilir.

- Oluşturulan yapıların bir ara yüzüne uygulanması gerekiyor. Bunun için oluşturulan yapıların hepsini bir Crypto Map tanımında toplaması gerekiyor. Crypto Map sayesinde IPSec VPN yaparken hangi IP adresiyle VPN tüneli kurulacağı, hangi trafiğin tünele yönlendirileceği ve hangi Transfor Set'in kullanılacağı belirlenecektir. Bunun için "**crypto map <Crypto Map Name> <ISAKMP Policy Number> ipsec-isakmp**" komutu kullanılıyor.
    - "**set peer <DST Global Ip Address>**" komutuyla hedef routerun global ip adresi tanımlanıyor.
    - Oluşturulan Transfor Set'i uygulamak için "**set transform-set <Transform Set Name>**" komutu kullanılıyor.
    - Oluşturulan ACL'i (Tünele girecek trafiği filtrelemek için tanımlanmıştı) uygulamak için "**match address <ACL Number or Name>**" komutu kullanılıyor. Bu adımdan sorna Crypto Map tanımı tamamlanıyor.
- Oluşturulan Crypto Map'i routerun internete bakan arayüzüne uygulamak için ilgili arayüzlere girilerek "**crypto map <Crypto Map Name>**" komutu kullanılıyor.

Uygualmasını "Lab -> Çalışmalar -> IPSec" dizini altında bulabilirsin :D .

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 olabilyor).



- GRE veya IPSec gibi tünelleme protkollerinin konfigürasyonu yapılırken, NAT gibi adres dönüşümü yapılan noktalarda dikkatli olunmalıdır. Yanlış ip bilgilerin girilmesi durumunda bağlantı kurulamayacaktır.

- SEC-K9 (Securityk9) lisansı, tüm ülkelere küresel dağıtım için hem yerel hem de ABD ihracat gerekliliklerine uyacak şekilde tasarlanmıştır. Bu lisans, ISR G2 platformlarında maksimum şifreli tünel sayısı (225 tünel) ve maksimum şifreli verim (85 Mbps) üzerinde bir kısıtlama uygular.

Kontrol Komutları

- sh int tunnel <Tunnel Number>
- sh crypto isakmp all