Overlay Tunnel

Overlay Tunnel, tünellenen verinin kurduğu sanal rotaya (Tünelleme dışında kalan fiziksel rota olarak da tanımlanabilir - Tünel kurulan iki cihaz biririne doğudan bağlı gibi kabul edilir) verilen isimdir.

Underlay Tunnel, tünellenen/kapsüllenen verinin internet ortamında takip ettiği fiziksel rotaya verilen isimdir.

GRE (Genetic Routing Encapsulation)

GRE (Genetic Routing Encapsulation), bir tünelleme tekniğidir. İnternet yapısının ilk çıktığı yıllarda kurumlar L3 de farklı protokoller kullanabiliyordu. Günümüzde her ne kadar IPv4 adresler kullanılsa da kurum içinde Private ip adresler kullanılıyor. Bilindiği üzere bu adresler de internete çıkarılamıyor. Yani Private ip adres kullanan iki kurumu birbirine bağlamak içi yine tünellemeye ihtiyaç duyulmaktadır. Bu durum üzerine kurumları internet üzeriden haberleştirebilmek için GRE Tunnel çözümü geliştirilmiştir.

GRE Tunnel çözümü ile kurumlar hangi L3 protokolünü kullanırsa kullansın paketler internete çıkarılacağı zaman internete çıkış yapacağı router üzerinde paket L3 başlık bilgisine kadarki kısım veri olarak kabul ediliyor. Kendi L3 başlık (hangi L3 protokolü kullanılıyorsa) bilgisinin önüne tünellendiğini belirten ek bir GRE başlık bilgisi ve ardına yeni bir L3 başlık bilgisi (internet üzerinde taşınabilmesi için IPv4 başlık bilgisi) ekleniyor. Paket internet üzerinden hedef routera (kurumun ISP'ye bakan routeruna) ulaştığında dekapsüle edilirken paketin internete çıkarılırken eklenen L3 başlık bilgisi çıkarıldığında GRE başlığıyla paketin tünellendiği anlaşılıyor. Paket GRE başlığından da çıkarılarak gönderildiği kurum içerisindeki hedef cihaza iletilir (Konfigürasyonu ve Detaylar için **CCNA - 3.06 - GRE and IPSec VPN** notlarını inceleyebilirsin).

- GRE Tunnel ile Multicast veya Broadcast paketler de taşınabiliyor.
- GRE Tunnel ile veriler taşınırken şifrelenmeden taşınıyor.
- GRE Tunnel kimlik denetimi sağlamamaktadır.

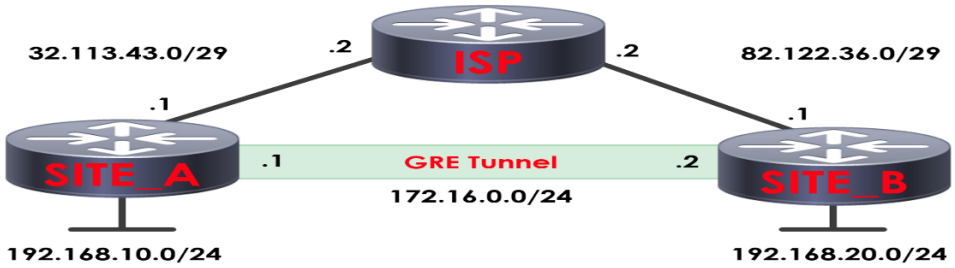
Kimlik denetimi ve şifreleme desteğinin bulunmadığı için alternatif olarak IPsec protokolü kullanılmaktadır. IPsec protokolü ise Multicast yayın desteklemediği için (OSPF Multicast yayın kullanana protokoller için sorun olabiliyor) GRE başlık bilgisinden sonra IPsec başlık bilgisi ekleniyor. Bu sayede hem Multicast yayının desteklemesi hem de paketin hedefe şifreli gönderilmesi sağlanıyor. Paketin internet üzerinde iletilebilmesi için de IPsec başlığından sonra yine ek bir L3 (IPv4 başlık bilgisi) başlık bilgisi ekleniyor ve paket internet ortamına bırakılıyor. IPsec (kullanılan şifreleme algoritmaları göre değişiklik gösterebiliyor) ve GRE Tunnel (24 Byte) kullanımı tek bir paket içerisinde taşınabilecek maksimum veri miktarının (MTU Size) düşmesine neden olmaktadır.

Recursive Routing Error

GRE konfigürasyonlarında OSPF gibi dinamik yönlendirme protokolleri kullanırken dikkat edilmesi gerekiyor. Kullanılan dinamik yönlendirme protokolünde kurumun ISP'ye bakan bacağındaki ip adresinin de öğretilmesi için tanım yapıldığında GRE Tunnel hata verecektir. Bu durumu bir örnek üzerinden açıklamak gerekirse;

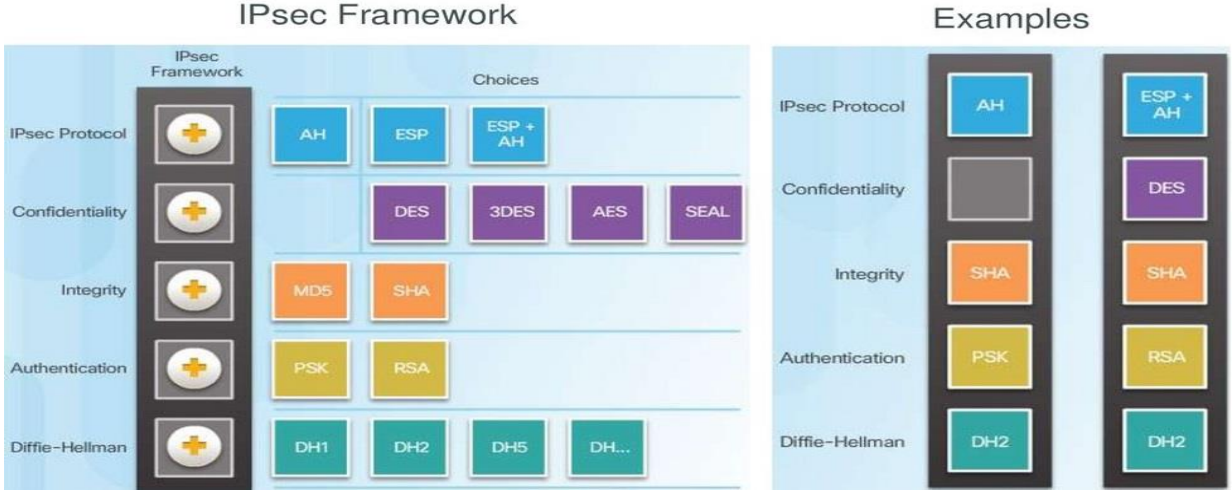
- Dinamik yönlendirme protokolü olarak OSPF kullanıldığını varsayalım. SITE_A router üzerinde OSPF konfigürasyonunda yayınlanacak networkler için tanım yapılırken 92.158.10.0/24 networküyle beraber (yapılmaması gereken) 32.113.43.0/29 networkü için

de tanım yapıldığında SİTE_B routeruna OSPF protokolü ile hem SİTE_A'nın kurum için bakan arayüzüne atanan ip adresinin (192.168.10.0/24) hem de GRE tünel üzerindeki hedef ip adresinin (32.113.43.2) anonsu ulaştırılacaktır. Bu durumda SITE_2'den SITE_1'e paket gönderilmesi gerektiğinde paketin gönderileceği hedef ip adresi GRE Tunnel üzerinden öğrenildiği için paket 32.113.43.2 adresine tünel üzerinden göndermeye çalışılır. GRE Tunnel üzerinde böyle bir ip adresi olmadığı için GRE Tunnel anında Down duruma geçirilecek ve yeniden GRE Tunnel kurulmaya çalıştırılacaktır. GRE Tunnel tekrar oluşturulduğunda ise OSPF ile yine SITE_A'nın ISP'ye bakan arayüzüne atanan ip adresi SİTE_B'ye GRE Tunnel üzerinden anons edileceği için GRE Tunnel tekrar tekrar Down duruma geçecektir. Bu süreç OSPF tanımı düzetilene kadar tekrarlanacaktır.



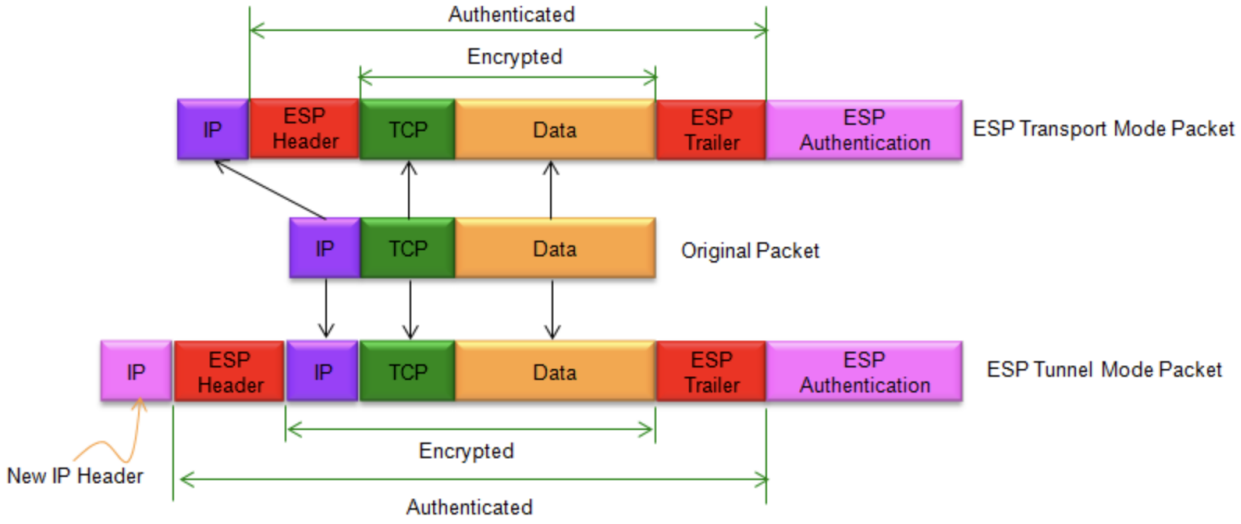
IPsec

IPsec, ip protokollerinin iletim sürecinde güvenliğini sağlayabilmek için geliştirilmiş bir protokol kümesidir. Bu protokol sayesinde paketlerde Authentication, Confidentiality ve Integrity (CIA) gibi özellikler dekteklenebiliyor. Bu özelliklerin içeriğine bakıldığında;
Authentication, tünel kurulacak hedef cihazın doğru cihaz olup olmadığının kontrolü sağlanıyor.
Data Confidentiality, çeşitli şifreleme algoritmaları kullanılarak paketin iletimi boyunca yetkisi olmayan 3. Bir kişi tarafından okunamaması sağlanıyor.
Data Integrity, verinin iletimi süresince değiştirilip değiştirilmediğinin kontrolü sağlanıyor.
Replay Detection, paketlerin (üçüncü bir kişi tarafından/saldırgan tarafından) tekrar tekrar gönderilmesini önleyen özelliktir.
Paketlerin içine bir Sequence Number ekleniyor. Bu sayede aynı Sequence Number'a ait paket ikinci kez gönderilirse paket drop ediliyor.
Bu özellikler IPsec konfigürasyonunda isteğe göre seçilerek özelleştirilebiliyor. Bu süreçte kullanılabilecek özellikler özetlenmek istendiğinde ortaya aşağıdaki gibi bir görsel çıkıyor.



|→ **IPsec Protocol**, bütün özelliklerin bütünleştirilerek tünelleme yapısının oluşturulduğu kısımdır (AH şifreleme yapamadığı için konfigürasyonlarda daha çok ESP kullanılıyor).
|→ **Confidentially**, tünelleme sürecinde kullanılacak şifreleme algoritmasının belirlendiği kısımdır.
|→ **Integrity**, túnel üzerinde verinin değişmeden iletilip iletilmediğini kontrol etmek için kullanılan Hash algoritmasının belirlendiği kısımdır.
|→ **Authentication**, verinin doğru hedef cihaza gönderilip gönderildiğini kontrol etmek için kullanılacak yöntemin seçimi yapılır. Bunun için yaygın kullanıla iki protokol vardır. Bunlar;
PSK (Pre-Shared Key), bir anahtar kelime seçilerek IPsec yapılacak cihazlar arasında paylaşılır.
RSA, dijital sertifika oluşturma tekniklerinden birisidir.
|→ **Diffie-Hellman**, Asimetrik şifreleme algoritmalarından biridir. Tünelleme sürecinde cihazlar arasında Confidentiality ve Authentication gibi işlemlerde güvenli bir şekilde anahtar paylaşımı/değişimi sağlamak için kullanılan kısımdır.

IPsec sürecinde Tünel Mode ve Transport Mode olmak üzere iki farklı mod bulunuyor. Bu modların farkına bakıldığında;
|—> **Tunnel Mode**, günümüzde Private ip adresleri kullanılıyor ve bu adreslerle internete çıkılamıyor. Bu nedenle paketlerin internet ortamında iletilebilmesi için IPsec başlığının arkasına paketlerin ek bir ip başlık bilgisi eklenmesi gerekiyor. Paketlerin bu şekilde gönderilmesidir.
|—> **Transport Mode**, hedef ve kaynak cihazlar Public ip adreslerine sahip ise (yani internet üzerinden herhangi ek bir işlem yapmadan doğrudan erişilebiliyorsa) ek bir ip başlık bilgisi eklemden paketin kendi/orjinal ip başlık bilgisi kullanılarak internet ortamına bırakılmasıdır.



IKE (Internet Key Exchange)

IKE, tünelleme sürecinde Authentication işleminin gerçekleştirilmesini sağlayan protokoldür. Cihazların tünelleme işleminde karşılıklı olarak anlaşma sürecini tarif eder . IKEv1 ve IKEv2 olmak üzere iki versiyonu vardır. IKEv1, ISAKMP (Internet Security Association Key Management Protokol) olarak da isimlendirilmektedir.
IKE konfigürasyonu iki fazdan oluşmaktadır. Bunlar;
|—> **Phase 1**, Phase 2' deki haberleşmenin hangi şifreleme algoritmalarıyla yapılacağının tarif edildiği kısımdır. Yani ikinci fazın güvenliğini sağlayabilmek için kullanılan fazdır. Bu süreç ISAKMP SA Phase olarak da isimlendirilir.
|—> **Phase 2**, verinin taşınırken nasıl şifreleneceğinin tarif edildiği kısımdır. Bu süreç IPsec SA olarak da isimlendirilir.

IPsec Konfigürasyonu

Konfigürasyon için öncelikle cihazların arayüzlerine ip adresleri verilerek Up konuma getirilmesi gerekiyor.

Arayüzler Up konuma getirildikten sonra Phase 1 için ilk olarak "**crypto isakmp policy <Policy Number>**" komutuyla politika tanımı yapılıyor. Politika tanımında ise;

- "**authentication <Authentication Algorithm>**" komutuyla kimlik denetiminde kullanılacak teknik seçimi yapılıyor.
    - "**encryption <Encryption Algorithm>**" komutuyla Phase 2 de kullanılacak şifreleme algoritması seçiliyor.
    - "**group <DH Algorithm>**" komutuyla anahtar paylaşımında kullanılacak Diffie-Hellman algoritması seçiliyor.
    - "**hash <Hash Algorithm>**" komutuyla kullanılacak Hash algoritması seçiliyor ve "**exit**" komutuyla tanım arayüzünden çıkılıyor.
    - Son olarak "**crypto isakmp key 0 <Key> address <Dst. Ip Address>**" komutuyla karşı cihaz ile bağlantı sürecide kimlik doğrulama işlemi için kullanılacak ortak anahtarın/Key tanımı ve hedef cihazın ip adresi tanımlanarak ilk faz tamamlanıyor (komuttaki "0" değeri, arkasından yazıla kısmın/anahtarın şifresiz yazıldığını belirtmek için kullanılıyor).

Phase 1 tamamlandıktan sonra Phase 2 konfigürasyonu için;

- "**crypto ipsec transform-set <Transform Set Name> <Using Crypto Algorithm>**" komutuyla ilk olarak bir Transform-set ismi oluşturularak bu set içerisinde veriyi şifreleme sürecinde kullanılacak algoritmaların tanımı yapılıyor.
    - "**mode <IPsec Mode>**" komutuyla bu süreçte kullanılacak mode tanımlanıyor. Tanımlanmadığı taktirde varsayılanda Tunnel Mode seçili oluyor ve "**exit**" komutuyla Transform-set arayüzünden çıkılır.
- IPsec tüneline girecek verilerin belirlenmesi için (sonuçta internete çıkış arayüzünde tünele girecek trafiğin ayıklanması gerekiyor) "**access-list <ACL Number> permit <Source Ip Address> <Source Wildcard Mask> <Destination Ip Address> <Destination Wildcard Mask>**" komutuyla hedef ve kaynak ip adres bilgilerinin belirtildiği bir Extended ACL yazılarak tünel kurulacak arayüze uygulanıyor.
- Phase 2 sürecinde gerçekleşirilen şifreleme ve ACL tanımlarının bir bütün olarak çalışabilmesi için Crypto Map tanımı yapılması gerekiyor. Crypto-Map tanımı için "**crpyto-map <Crypto-Map Name> <Crypto Map Sequence Number> ipsec-isakmp**" komutuyla bir Crypto Map ismi ve Phase 2'de tanımlanan özelliklerin (Tünelleme bilgileri ve ACL tanımı) Crypto Map yapısının 10 satırında yer alacağı belirtiliyor (Sequence Number aslında kurulan her Birr ipsec tüneli için bir satır tanımı olarak tanımlanabilir. Örnek olarak kurum A şubesine ipsec tüneli kurmak için tanımladığı özellikler ve ACL yapısını sequence Number 10 satırıyla, B şubesine ipsec tüneli kurmak için tanımladığı özellikler ve ACL yapısını sequence Number 20 satırıyla tanımlayabilir).
- "**match address <ACL Number/Name>**" komutuyla tünellenmesi istenen trafiği temsil eden ACL belirtiliyor.
- "**set transform-set <Transform Set Name>**" komutuyla Phase 2'de oluşturulan Transform Set tanımı belirtiliyor.
- "**set peer <Destination Ip Address>**" komutuyla hedef networkün ip adresi belirtilerek Phase 2 tamamlanıyor.

- Son adımda ise oluşturulan Crypto Map tanımının ilgili arayüze uygulanması gerekiyor. Bunun için "**int <Interface Id>**" komutuyla ilgili arayüze girilerek "**crypto map <Crypto Map Name>**" komutuyla arayüze uygulanıyor.

ÖNEMLİ: IPsec konfigürasyonundan sonra paketi tünelin sonlanacağı routerun internete bakan arayüzüne gönderilebilmesi için dinamik olarak ya da statik olarak Private ip adres için rota tanımının yapılması gerekiyor. Aksi taktirde Private ip adresine sahip paketlerin gönderileceği bir spnraki ip adresi belirli olmayacağından paketler drop edilecektir.

```
R1(config)#crypto isakmp policy 4
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#encryption aes 128
R1(config-isakmp)#group 2
R1(config-isakmp)#hash sha256
R1(config-isakmp)#exit
R1(config)#crypto isakmp key 0 MyPass1 address 30.0.0.4
R1(config)#
R1(config)#crypto ipsec transform-set TS1 esp-aes esp-sha-hmac
R1(cfg-crypto-trans)#mode tunnel
R1(cfg-crypto-trans)#exit
R1(config)#$ 102 permit ip 192.168.1.0 0.0.0.255 192.168.4.0 0.0.0.255
R1(config)#crypto map CM1 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R1(config-crypto-map)#match address 102
R1(config-crypto-map)#set transform-set TS1
R1(config-crypto-map)#set peer 30.0.0.4
R1(config-crypto-map)#exit
R1(config)#
R1(config)#int fa 1/0
R1(config-if)#crypto map CM1
R1(config-if)#exit
R1(config)#
R1(config)#ip route 192.168.4.0 255.255.255.0 30.0.0.4
R1(config)#
```

|→ Uygulamalarını Lab dizini altında bulabilirisin.

(Özetle bir router üzerinde aynı özellikler kullanılarak birden fazla ipsec tünel kurulacağı zaman değişen tek kısım yeni bir ACL tanımı, Sequence Number ve son adımda yapılan Peer kısımları oluyor.)

IPsec konfigürasyonunun Phase 1 safhasında cihazlar karşılıklı olarak birbirlerine paketler gönderip anlaşıyorlar. Bu süreçte iki farklı **Main Mode** ve **Aggressive Mode** olmak üzere iki fraklı mod kullanıyor.

- **Main Mode**, Phase 1 safhasında 6 farklı paket kullanılarak cihazlar aralarında anlaşır. Yaygın olarak kullanılan moddur. Bu modda kullanılan paketlere bakıldığında (R1 ve R2 adında IPsec tunnel kurulacak iki cihaz olduğunu varsayalım);
    - MM1, anlaşma sürecinde gönderilen ilk pakettir. R1 kendi üzerinde Phase 1 safhasında tanımlanan özellikleri/güvenlik bilgilerini karşı cihaza teklif olarak gönderdiği/bildirdiği pakettir.
    - MM2, R2 R1'in kendisine gönderdiği MM1 paketi içerisindeki tanımların kendi ü zerinde Phase 1 safhasındaki tanımlarla eşleşip eşleşmediğini bildirdiği pakettir.
    - MM3, R1 ve R2 arasındaki konfigürasyonlar uyuşuyorsa Diffie-Hellman anahtar değişim süreci başlatılıyor ve R1 kendi anahtarını R2 ile paylaşıyor.
    - MM4, R2 kendi anahtarını R1 ile paylaşıyor ve bu aşamadan sonraki kısımda iletişim şifreli olarak devam ediyor.

- MM5, R1 kendi kimlik denetimi bilgilerini R2 ile paylaşıyor.
- MM6, R2 kendi kimlik denetimi bilgilerini R1 ile paylaşıyor ve ISAKMP SA kurulumu tamamlanıyor.

- **Aggressive Mode**, Main Mode'a kıyasla Plase 1 safhasını daha hızlı kurulduğu mod olarak tanımlanabilir. Bu işlem için 3 farklı paket kullanılıyor. Bunlar;
  - **AM1**, Main Mode'daki MM1, MM3 ve MM5 paketlerinin tek seferde gönderildiği pakettir (R1'in R2'ye gönderdiği bütün paketler tek seferde gönderiliyor yani).
  - **AM2**, Main Mode'daki MM2, MM4 ve MM6 paketlerinin tek seferde gönderildiği pakettir.
  - **AM3**, Main Mode'daki MM5 paketinin gönderildiği pakettir.

  Zorunda kalınmadığı sürece Aggressive Mode kullanılması tavsiye edilmiyor. Çünkü, paketler Main Mode'a kıyasla toplu olarak gönderildiği için kimlik denetimi bilgilerinin paylaşıldığı (MM5 ve MM6 paketleri) paketlerin tamamı şifrelenmeden gönderiliyor (Main Mode'da MM4'den sonraki kısım şifreli gönderiliyordu). Bu durumda tünel oluşturulurken bir saldırgan araya girip trafiği dinleyerek tünelleme sürecindeki hassas/kritik bilgileri elde edebilir.

IPsec konfigürasyonunun Phase 2 safhasında cihazların aralarında anlaşma sürecinde ise Quick Mode adı verilen mod kullanılıyor. Bu modda kullanılan paketlere bakıldığında;

- **QM1**, R1 R2 ile güvenlik bilgilerini/kullanacağı teknolojileri paylaşıyor.
- **QM2**, R2 R1'in gönderdiği güvenlik bilgilerinin eşleşip eşleşmediğini bildiren yanıt paketidir.
- **QM3**, bu paket ile R1 ve R2 arasında veri transferini başlatmak üzere iki bağlantı oluşturulur. (Buradaki ilk bağlantı R1'den R2'ye, ikinci bağlantı ise R2'den R1'e veri göndermek için kullanılır).

Perfect Forward Secrecy (PFS), Phase 2'de güvenliği arttıran ekstra bir özelliktir. Diffie-Hellman algoritmasıyla karşılıklı anahtar değişim sürecinde cihazların birbirlerine gönderdikleri anahtarların farklı seçilmesi (daha önce seçilen anahtarlardan farklı olması) istenir. Çünkü, aynı anahtarlar kullanılarak şifrelenmiş belirli miktarda trafik ele geçirildiği taktirde anahtarın kırılabilme ihtimali var. PFS özelliği sayesinde cihazların seçtikleri anahtarların daha önce seçilmemiş olması sağlanıyor (Normalde seçilen anahtarların aynı olması düşük bir ihtimal ama PFS özelliği sayesinde bu ihtimal ortadan kaldırılıyor - Bu işlem de ek CPU tüketimine neden oluyor). Konfigürasyonunda dikkat edilmesi gereken nokta IPsec yapılacak cihazlarda karşılıklı olarak açılması gerekiyor.

IKEv2

IKEv2 sürümünde ise Phase 1 ve Phase 2 safhaları yerini IKE_SA_INIT ve IKE_AUTH adı verilen paketlere bırakıyor. Bu yapıların içeriğine bakıldığında;

- **IKE_SA_INIT**, IKEv1 sürümünün MM1 ve MM4 arasındaki paketlerin tek parçada iletildiği paket yapısıdır (R1 R2'ye Request olarak, R2 R1'e Response olarak gönderir yani bu yapıda toplam 2 paket gönderilir).
- **IKE_AUTH**, IKEv1 sürümünün MM5 ve MM6 ile QM1ve QM2 paketlerinin tek parçada iletildiği paket yapısıdır (R1 R2'ye Request olarak, R2 R1'e Response olarak gönderir yani bu yapıda toplam 2 paket gönderilir).

  Özetle; IKE_SA_INIT (2), IKE_AUTH (2) olacak şekilde toplamda 4 paket ile IPsec Tunnel kurulur.

IKEv1'e kıyasla IKEv2'de yeni nesil şifreleme algoritmaları (Eliptic Curve Diffie-Hellman gibi) ve saldırı koruma mekanizmaları (Anti-DDoS Protection, MitM Potection, Evasrdropping Protection) da eklenmiştir.

IPsec VPN Solutions

Site to Site (LAN to LAN) IPsec VPN dışındaki diğer çözümler adından da anlaşılacağı gibi Cisco çözümüdür ve sadece Cisco marka cihazlar arasında kurulabilir.

- **Site to Site (LAN to LAN) IPsec VPN**, farklı marka cihazlar üzerinde konfigüre edilebiliyor.

- **Cisco Dynamic Multipoint VPN (DMVPN)**, IPsec konfigürasyonunu kolaylaştırmak üzerine geliştirilen bir çözümdür. Bir kurumun merkez routerunda her şubesi için ayrı ayrı Transform-Set, ACL ve Crypto-Map tanımı yapılması gerekir. Bu şekilde yapıldığında ise herhangi iki şube arasında haberleşme sürecini kurumun merkez routeru üzerinden gerçekleştirebilir (Hub and Spoke Topology). Şubeler arası doğrudan iletişim kurulabilmesi için her şube routerunda da ayrı ayrı her şube için tanımlamalar yapmak gerekecektir. Topolojideki en küçük bir değişim için bile her şube üzerinde düzenlemeler yapmak gerekecektir.

  DMVPN ile sadece kurumun merkez routerunda DMVPN merkez konfigürasyonu yapılarak şubelerde sadece merkez router tarif ediliyor/konfigürasyonu yapılıyor. Bu adımdan sonra herhangi bir şube, bir başka şube ile iletişime geçmek istediğinde merkez routerdan tünel kurmak istediği şubenin Public ip adresini öğrenerek şubeler arası otomatik olarak IPsec VPN tüneli oluşturulması sağlanıyor (Spoke to Spoke Topology).
  DMVPN ile aynı zamanda GRE desteği de bulunmaktadır. Yani Multicast yayın da desteklenmektedir. Muadili Open Standard protokoller de bulunmaktadır (IKEv1 süürümünü kullanmaktadır).

- **Cisco Group Encrypted Transport VPN (GETVPN)**, DMVPN çözümünün farklı bir versiyonu olarak görülebilir. Farklı olarak paketlerin internet ortamına çıkarılmsı gerekmediği durumlarda/Private networklerde paketlere ek bi ip adres başlık bilgisi eklenmeden (Overlay Tunnel oluşturulmasına gerek duyulmayan) gönderilmesini sağlayan teknolojidir. Tünelleme yapılmadığı için bu süreçte Traceroute yapılarak paketlerin geçtiği her bir güzergah açıkça görülecektir.

- **Cisco Flex VPN**, DMVPN çözümünün IKEv2 sürümünü kullanan versiyonudur.

- **Remote Access VPN**, Site to Site VPN network cihazları arasında (Firewall, Router) gerçekleştiriliyordu. Günümüzde ise bilgisayarlar gibi end device üzerine yazılımlar yüklenerek end-device ile network cihazları arasında VPN bağlantısı kurulabiliyor (SSL VPN). Bu sayede son kullanıcının bağlı olduğu network ortamı veya sahip olduğu ip adresi farkletmeksizin kurum ağlarına bağlanabilmesi ve güvenli bir şekilde iletişim kurabilmesi sağlanıyor.

VTI (Virtual Tunnel İnterface)

Normalde IPsec teknolojisinde Multicast yayın desteği olmadığı için paketler GRE ve IPsec teknolojisiyle birlikte kullanılarak kapsüllenir (IPsec konfigürasyonunda GRE başlığı default olarak ekleniyor). Bu süreçte GRE başlığıyla beraber paket içerisinde taşınabilecek veri miktarı da azalmaktadır. IPsec konfigürasyonunda GRE başlığı eklenmeden kullanıldığı yapıdır (Detaylar ve

konfiigürasyon için
https[:]//www.cisco.com/c/en/us/td/docs/security/asa/asa97/configuration/vpn/asa-97-vpn-config/vpn-vti.pdf dökümanını inceleyebilrisin).

NOTLAR

- Tünelleme yapıldığında asıl paket farklı protokoller kullanılarak kapsüllenip internet üzerinde iletildiği için asıl paketin TTL değeri değişmeyecektir. Sadece internete çıkacağı router ve dekapsüle edileceği router üzerinde TTL değeri değişeceği içi paket hedefe ulaştığında TTL değeri 2 azalacaktır (y ani Traceroute yapıldığında iki hop görünecektir). Bu çıktı aynı zamanda Overlay Tunnel çıktısıdır.
- Tünelleme kurulan cihazlar arasında Underlay üzerinde bir kesinti olduğunda bu anlaşılmaz. Bu nedenle eğer ki etek bir hat varsa yedek hatta geçiş yapılmaz. Bu gibi durumların kontrol edilmesi için Keep Alive özelliği devreye alınabiliyor. Konfigürasonu için "**keepalive [Second <retries>]**" komutu kullanılıyor. Sadece "**keepalive**" komutu kullanıldığında varsayılanda 10 sn aralıklarla Keepalive paketi göndererek bağlantıyı kontrol eder. Gönderdiği paketlerin ardından hedeften yanıt bekler. Gönderilen 3 Keepalive paketine karşılık gelmezse bağlantının kesildiği anlaşılarak port kapatılır.
- Tünelleme sürecinde bant genişliğini konfigüre etmek için "**bandwidth <Bandwidth>**" komutu kullanılıyor. Bant genişliğinin belirtilmesi QoS (Load Balance) veya OSPF gibi bant genişliğini baz alarak işlem yapan protokollerin doğru çalışması için önemlidir.
- IPsec kullanılan cihazlarda seçilen teknolojilerinde aynı olması gerekiyor. Aksi taktirde tünel kurulamaz.
- IPsec'in başlaması için mutlaka trafik oluşturulması gerekiyor. Aksi taktirde IPsec başlamaz (Basitçe tüneli kullanacak bir ping atılabilir).
- Cisco marka cihazlarda IPsec Tunnel kurabilmek için Security lisansı gerekiyor.

Kullanılan Komutlar

- sh int tunnel 100
- sh crypto isakmp policy
- sh crypto ipsec sa. //Phase 1 kontrolü
- sh crypto ipsec transform-set < Transform Set Name> //Phase 2 kontrolü