BSM 471-AĞ GÜVENLİĞİ

Virtual Private Network (VPN)-IPSec

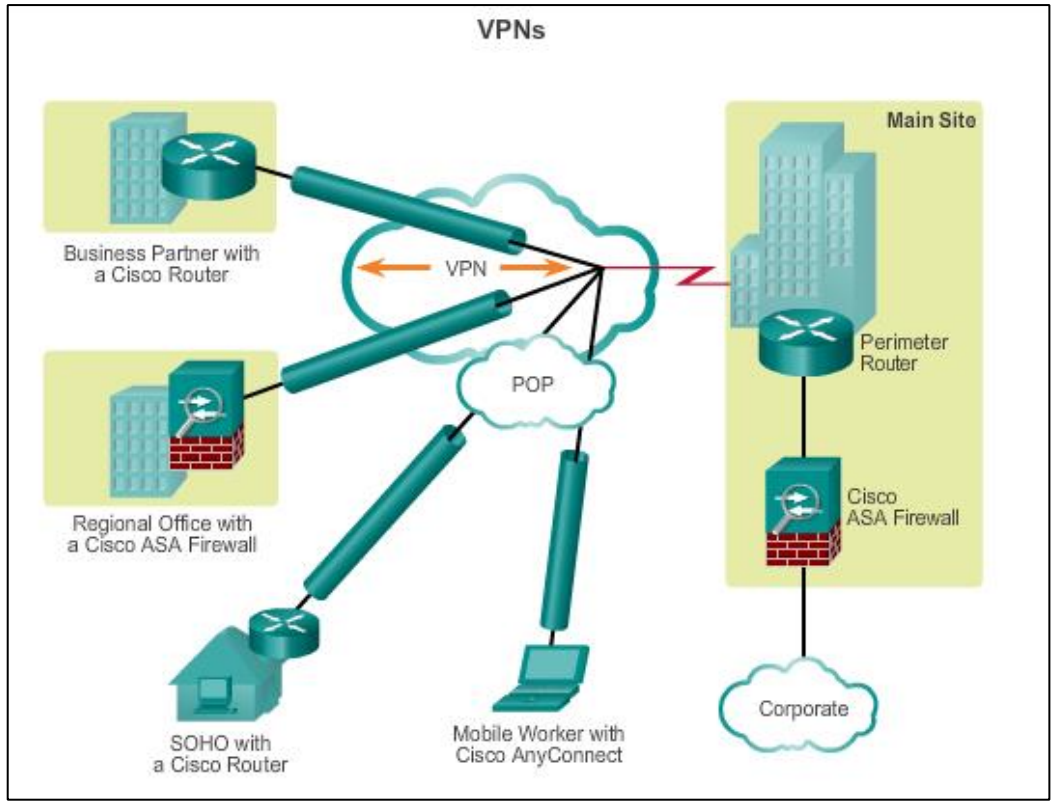
Dr. Öğr. Üyesi Musa BALTA
Bilgisayar Mühendisliği Bölümü
Bilgisayar ve Bilişim Bilimleri Fakültesi

Konu İçeriği

- VPN Kavramı
- Site-to-Site GRE Tünelleme
  - Paket ve Devre Anahtarlama
  - PSTN
  - Frame Relay
  - ISDN
  - PPPs
- Ipsec Tünelleme
- Uzaktan Erişim

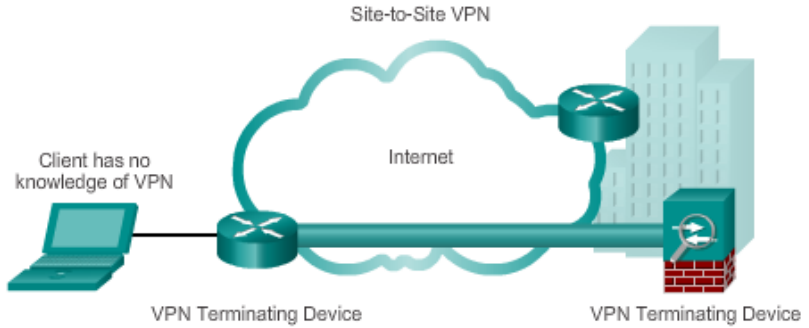
VPN Kavramı

- *İnterneti güvenilir bir kaynak değildir.*
- *VPN'ler, İnternet veya extranetler gibi üçüncü taraf ağlar üzerinden uçtan uca özel ve güvenli ağ bağlantısı oluşturmak için kullanılır.*
- *Genel bir ağ üzerinden özel bir tünel oluşturmak için bir VPN kullanılır.*
- *Veriler, İnternet üzerinden bu tünelde şifreleme kullanılarak ve verileri yetkisiz erişime karşı korumak için kimlik doğrulama kullanılarak güvence altına alınabilir.*



Siteden Siteye VPN

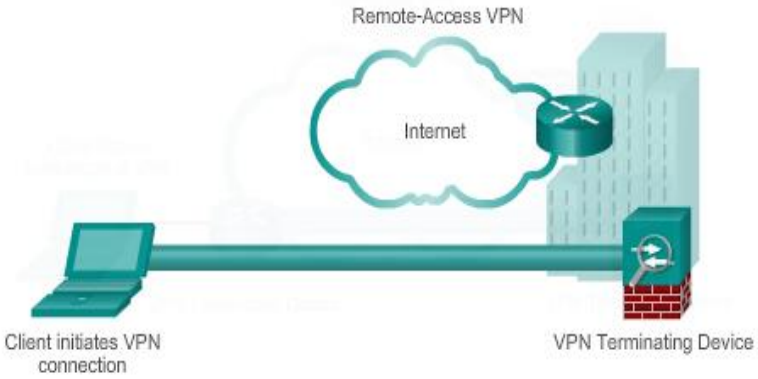
- Tüm ağları birbirine bağlayın, geçmişte siteleri bağlamak için kiralık bir hat veya Frame Relay bağlantısı gerekiyordu, ancak artık çoğu şirketin İnternet erişimi olduğundan, bu bağlantılar siteden siteye VPN'lerle değiştirilebilir.



- Dahili ana bilgisayarların bir VPN'in varlığından haberi yoktur.
- VPN bağlantısının her iki tarafındaki cihazlar önceden VPN yapılandırmasından haberdar olduğunda oluşturulur.
- Uç ana bilgisayarlar, bir VPN ağ geçidi üzerinden normal TCP/IP trafiği gönderir ve alır.
- VPN ağ geçidi, belirli bir siteden gelen tüm trafik için giden trafiği kapsüllemek ve şifrelemekten sorumludur.
- VPN ağ geçidi daha sonra onu İnternet üzerinden bir VPN tüneli aracılığıyla hedef sitedeki bir eş VPN ağ geçidine gönderir.
- Alındıktan sonra, eş VPN ağ geçidi başlıkları çıkarır, içeriğin şifresini çözer ve paketi kendi özel ağı içindeki hedef ana bilgisayara iletir.

Uzaktan Erişim VPN

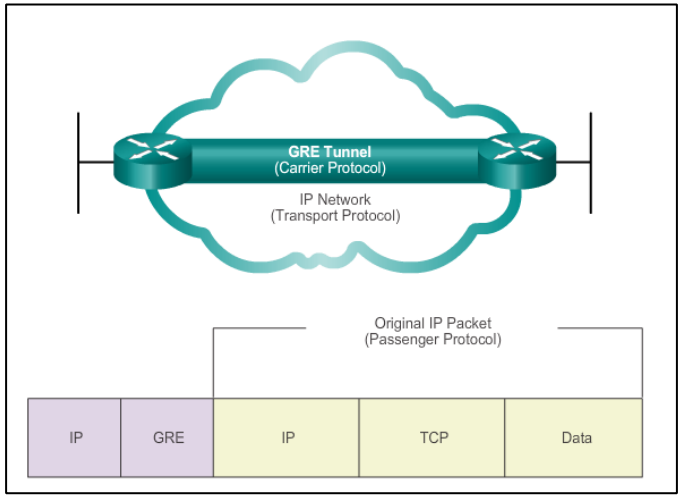
- Evden çalışanlar, mobil kullanıcılar ve extranet, tüketiciden işletmeye trafiğin ihtiyaçlarını destekleme,
- VPN istemcisinin (uzak ana bilgisayar), ağ ucundaki bir VPN sunucu cihazı aracılığıyla kurumsal ağa güvenli erişim kazandığı bir istemci/sunucu mimarisini destekleme,

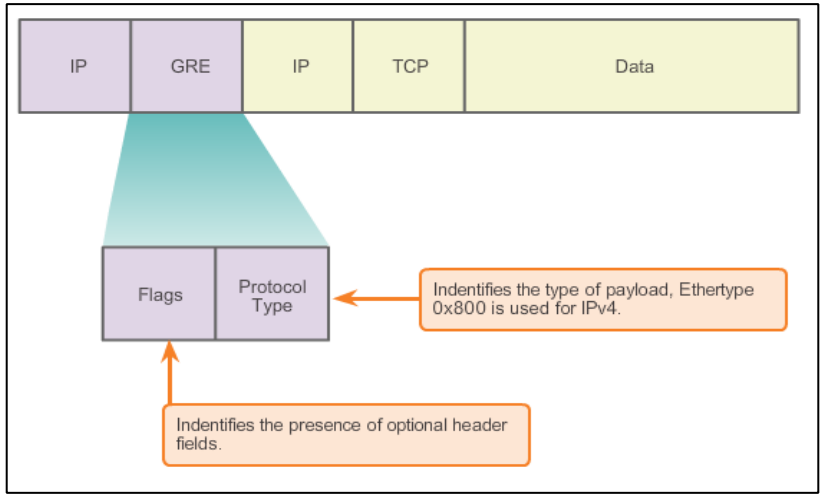


- Şirket ağlarına İnternet üzerinden güvenli bir şekilde erişmesi gereken bireysel ana bilgisayarları bağlamak için kullanılır.
- Mobil kullanıcının uç cihazına (Cisco AnyConnect Güvenli Mobilite İstemcisi) VPN istemci yazılımının yüklenmesi gerekebilir.
- Ana bilgisayar herhangi bir trafik göndermeye çalıştığında, VPN İstemci yazılımı bu trafiği kapsüller ve şifreler ve İnternet üzerinden hedef ağın ucundaki VPN ağ geçidine gönderir.

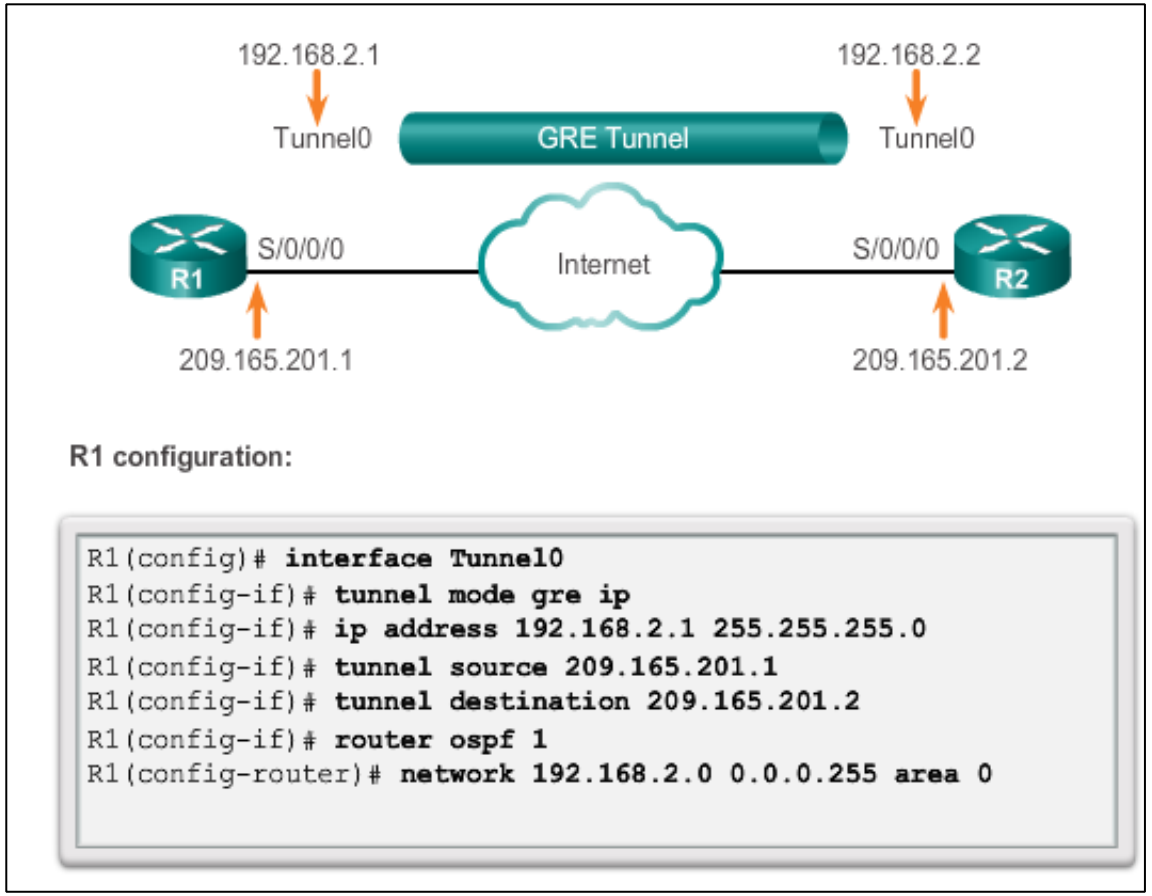
Siteden Siteye GRE Tünelleme

- Cisco tarafından geliştirilen temel, güvenli olmayan, siteden siteye VPN tünel protokolü
- IP tünelleri içinde çok çeşitli protokol paketi türlerini kapsüller
- Bir IP ağı üzerinden uzak noktalardaki yönlendiricilere sanal bir noktadan noktaya bağlantı oluşturur.
- GRE, bir IETF standardı olarak tanımlanır.
- GRE paketlerini tanımlamak için IP protokolü 47 kullanılır.
- GRE kapsülleme, herhangi bir OSI Katman 3 protokolünün kapsüllenmesini desteklemek için GRE başlığında bir protokol türü alanı kullanır.
- GRE'nin kendisi vatansızdır; varsayılan olarak herhangi bir akış kontrol mekanizması içermez.
- GRE, yükünü korumak için herhangi bir güçlü güvenlik mekanizması içermez.
- GRE başlığı, tünelleme IP başlığı ile birlikte, tünellenmiş paketler için en az 24 bayt ek yük oluşturur.





GRE Tünelleme-Örnek

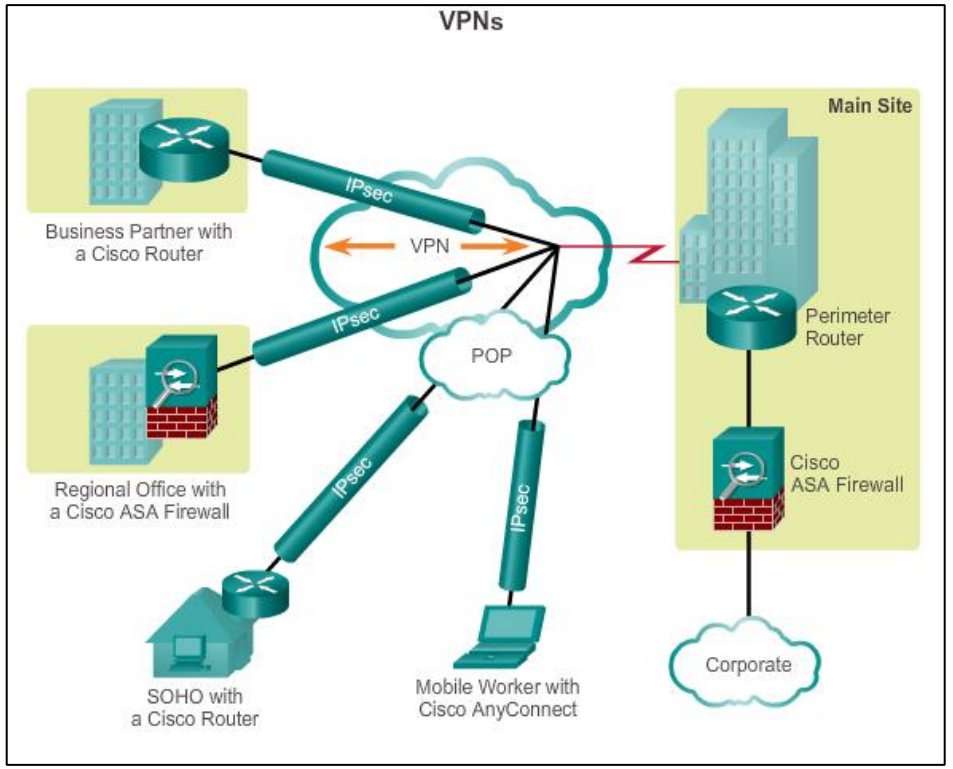


R1 configuration:

```
R1(config)# interface Tunnel0
R1(config-if)# tunnel mode gre ip
R1(config-if)# ip address 192.168.2.1 255.255.255.0
R1(config-if)# tunnel source 209.165.201.1
R1(config-if)# tunnel destination 209.165.201.2
R1(config-if)# router ospf 1
R1(config-router)# network 192.168.2.0 0.0.0.255 area 0
```

Ipsec VPN

- Özel bir ağdan gelen bilgiler, genel bir ağ üzerinden güvenli bir şekilde taşınır.
- Ayrılmış bir Katman 2 bağlantısı kullanmak yerine sanal bir ağ oluşturur.
- Gizli kalmak için, verileri gizli tutmak için trafik şifrelenir.
- Bir VPN'nin IP kullanılarak güvenli bir şekilde nasıl yapılandırılabileceğini tanımlar.
- Güvenli iletişim kurallarını açıklayan açık standartlar çerçevesi.
- Herhangi bir özel şifreleme, kimlik doğrulama, güvenlik algoritması veya anahtarlama teknolojisine bağlı değildir.
- Güvenli iletişim uygulamak için mevcut algoritmalara güvenir.
- Ağ katmanında çalışır, katılımcı IPsec cihazları arasında IP paketlerini korur ve doğrular.
- Bir çift ağ geçidi, bir çift ana bilgisayar veya bir ağ geçidi ile ana bilgisayar arasındaki yolu korur.
- IPsec'in tüm uygulamalarının düz metin Katman 3 başlığı vardır, bu nedenle yönlendirme ile ilgili herhangi bir sorun yoktur.
- Ethernet, ATM veya Frame Relay gibi tüm Katman 2 protokolleri üzerinden çalışır.

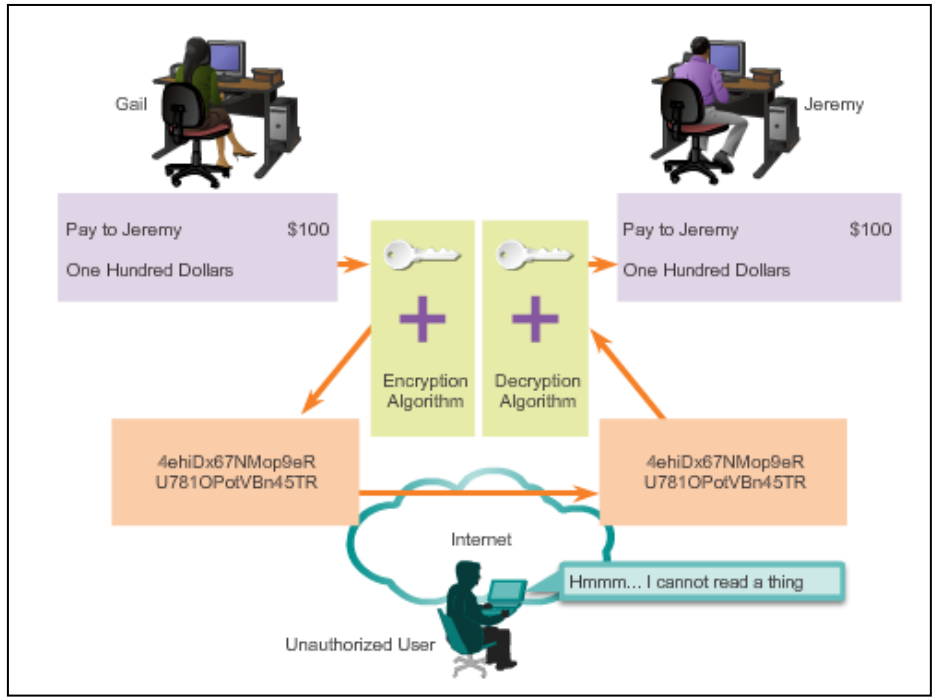


Ipsec VPN-devam

- **Genel karakteristikleri;**
- IPsec, algoritmadan bağımsız bir açık standartlar çerçevesidir.
- IPsec, veri gizliliği, veri bütünlüğü ve kaynak kimlik doğrulaması sağlar.
- IPsec, IP paketlerini koruyarak ve doğrulayarak ağ katmanında hareket eder.
- **Güvenlik karakteristikleri;**
- **Gizlilik (şifreleme)** – Ağ üzerinden iletmeden önce verileri şifreler.
- **Veri bütünlüğü** – Verilerin aktarım sırasında değiştirilmediğini doğrular; değişiklik algılanırsa paket bırakılır.
- **Kimlik Doğrulama** – Gönderilen verilerin kaynağının kimliğini doğrular, istenen iletişim ortağıyla bağlantının yapıldığından emin olur, IPsec, bağımsız olarak iletişim kurabilen kullanıcıların ve cihazların kimliğini doğrulamak için İnternet Anahtar Değişimi'ni (IKE) kullanır.
- **Tekrar Oynatmaya Karşı Koruma** – Yeniden gönderilen paketleri algılayıp reddeder ve sahtekarlığı önlemeye yardımcı olur.

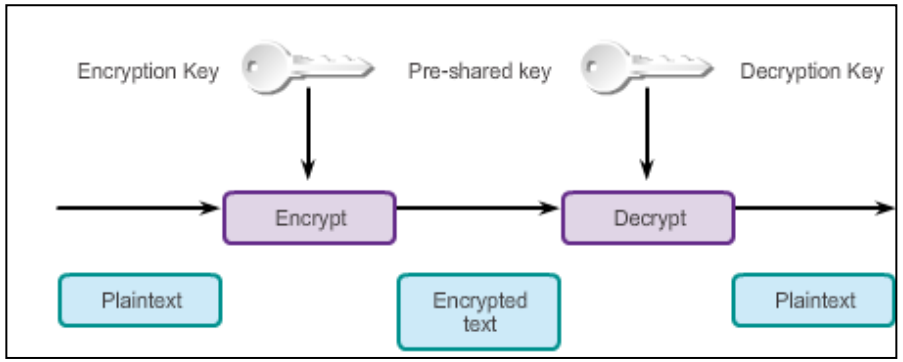
Şifreleme ile Gizlilik

- Şifrelemenin çalışması için hem gönderenin hem de alıcının orijinal mesajı kodlanmış biçimine dönüştürmek için kullanılan kuralları bilmesi gerekir.
- Kurallar, algoritmalara ve ilişkili anahtarlara dayalıdır.
- Doğru anahtar olmadan şifre çözme son derece zordur (veya imkansızdır).
- Anahtar uzunluğu arttıkça şifrelemeyi kırmak zorlaşır. Ancak, daha uzun bir anahtar, verileri şifrelerken ve şifresini çözerken daha fazla işlemci kaynağı gerektirir.
- İki ana şifreleme türü şunlardır:
  - ***Simetrik Şifreleme (gizli anahtarlı)***
  - ***Asimetrik Şifreleme (açık anahtarlı)***



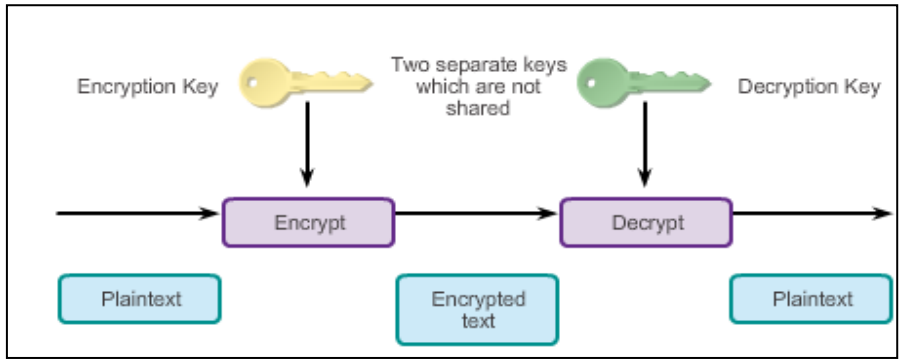
Simetrik Şifreleme

- Şifreleme ve şifre çözme aynı anahtarı kullanır.
- İki ağ aygıtından her biri, bilgilerin kodunu çözmek için anahtarı bilmelidir.
- Her cihaz, bilgiyi ağ üzerinden diğer cihaza göndermeden önce şifreler.
- Genellikle mesajın içeriğini şifrelemek için kullanılır.
- Örnekler: DES ve 3DES (artık güvenli kabul edilmemektedir), Rivest Cipher4 ve AES (IPsec şifrelemesi için 256 bit önerilir).



Asimetrik Şifreleme

- Şifreleme ve şifre çözme için farklı anahtarlar kullanır.
- Anahtarlardan birini bilmek, saldırganın ikinci anahtarı çıkarmasına ve bilgilerin kodunu çözmesi için yeterli değildir.
- Bir anahtar mesajı şifrelerken, ikinci bir anahtar mesajın şifresini çözer.
- Genel anahtar şifreleme, bir özel anahtar ve bir genel anahtarın bir kombinasyonunu kullanan bir asimetrik şifreleme çeşididir.
- Genellikle dijital sertifika ve anahtar yönetiminde kullanılır; Örnek: RSA (Rivest Shamir Adleman)



Gizli Anahtar vs Açık Anahtar

- Hem gizli anahtarlı kriptografinin hem de açık anahtarlı kriptografinin güçlü ve zayıf yönleri vardır:
- Gizli anahtarlı kriptografi ile veriler hızlı bir şekilde şifrelenebilir ve şifresi çözülebilir, ancak iletişim kuran her iki tarafın da aynı gizli anahtar bilgisini paylaşması gerektiğinden, anahtar alışverişinin lojistiği sorun olabilir.
- Açık anahtarlı kriptografide, anahtar değişimi bir sorun değildir çünkü açık anahtarın gizli tutulması gerekmez, ancak verileri şifrelemek ve şifresini çözmek için kullanılan algoritmalar kapsamlı hesaplamalar gerektirir ve bu nedenle çok yavaştır.

Açık Anahtar Sertifikaları

- Bir açık anahtar sertifikası, bir varlığın asimetrik kriptografide kullanılmak üzere kendi genel anahtarını iletmesi için güvenli bir yol sağlar. Açık anahtar sertifikası aşağıdaki durumu önler:
  - Charlie kendi genel anahtarını ve özel anahtarını oluşturursa, kendisinin Alice olduğunu iddia edebilir ve genel anahtarını Bob'a gönderebilir. Bob, Charlie ile iletişim kurabilecektir, ancak Bob, verilerini Alice'e gönderdiğini düşünecektir.
- Açık anahtar sertifikası, **pasaportun dijital eşdeğeri** olarak düşünülebilir. Güvenilir bir kuruluş tarafından verilir ve hamiline kimlik sağlar.
- Ortak anahtar sertifikaları veren güvenilir bir kuruluş, **Sertifika Yetkilisi (CA)** olarak bilinir. CA notere benzetilebilir.
- Bir CA'dan sertifika almak için, kişinin kimlik kanıtı sağlaması gerekir. CA, başvuranın temsil ettiğini söylediği kuruluşu temsil ettiğinden emin olduktan sonra, CA, sertifikada yer alan bilgilerin geçerliliğini onaylayan sertifikayı imzalar.

Açık Anahtar Sertifikaları-devam

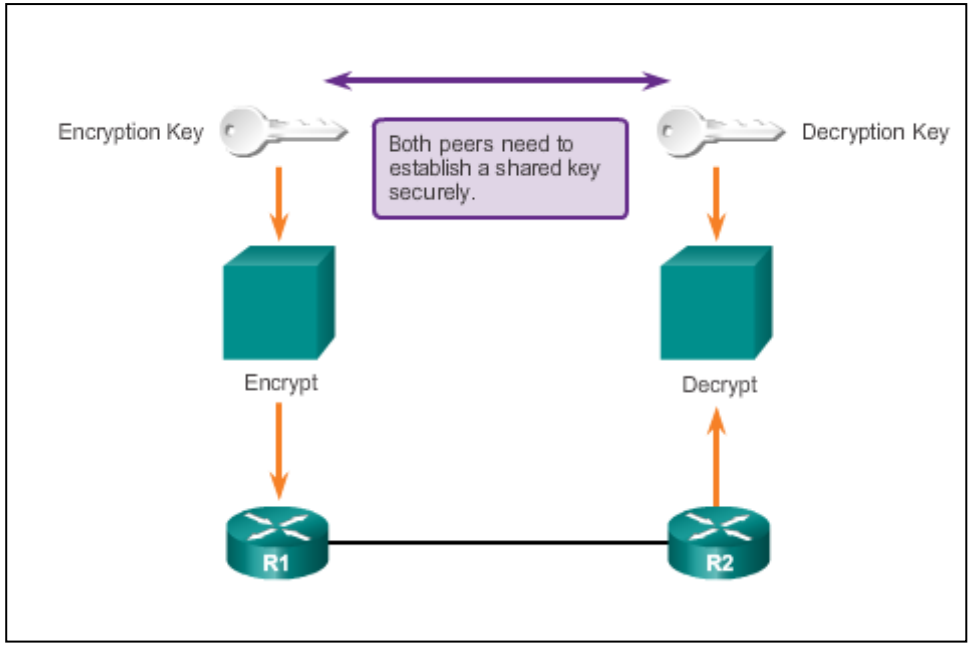
- *Bir açık anahtar sertifikası aşağıdaki alanları içerir:*
  - **Issuer**; Sertifikayı veren CA. Kullanıcı, sertifikayı veren CA'ya güveniyorsa ve sertifika geçerliyse, kullanıcı sertifikaya güvenebilir.
  - **Period of validity**; Sertifikanın bir son kullanma tarihi vardır. Bir sertifikanın geçerliliği doğrulanırken bu tarih kontrol edilmelidir.
  - **Subject**; Sertifikanın temsil ettiği varlık hakkında bilgi içerir.
  - **Subject's public key**; Sertifikanın sağladığı birincil bilgi, öznenin genel anahtarıdır. Diğer tüm alanlar, bu anahtarın geçerliliğini sağlamak için sağlanmıştır.
  - **Signature**; Sertifika, sertifikayı veren CA tarafından dijital olarak imzalanır. İmza, CA'nın özel anahtarı kullanılarak oluşturulur ve sertifikanın geçerliliğini sağlar. TLS işleminde gönderilen veriler değil sadece sertifika imzalandığı için, TLS inkar edilemezlik sağlamaz.

Açık Anahtar Sertifikaları-devam

- Bir sertifika zincirinde birden çok sertifika birbirine bağlanabilir. Bir sertifika zinciri kullanıldığında, ilk sertifika her zaman gönderene ait olur. Sonraki, gönderenin sertifikasını veren kuruluşun sertifikasıdır.
- Zincirde daha fazla sertifika varsa, her biri bir önceki sertifikayı veren yetkiliye aittir. Zincirdeki son sertifika, bir kök CA'nın sertifikasıdır. Bir kök CA, yaygın olarak güvenilen bir genel Sertifika Yetkilisidir.
- Birkaç kök CA'ya ilişkin bilgiler genellikle müşterinin İnternet tarayıcısında depolanır. Bu bilgiler, CA'nın genel anahtarını içerir. İyi bilinen CA'lar arasında ***DigiCert, Entrust*** ve ***GlobalSign*** bulunur.

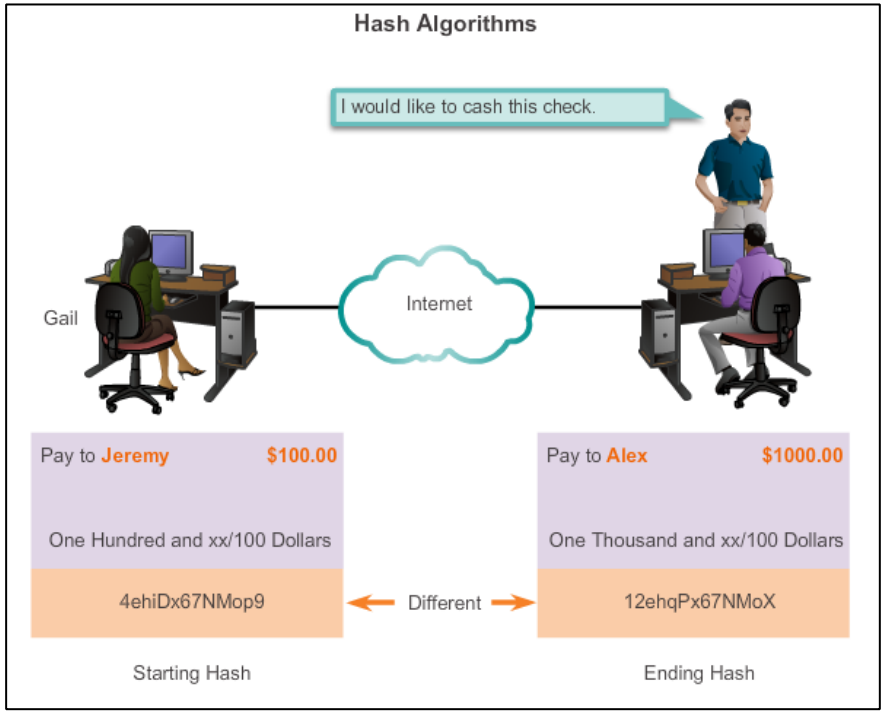
Diffie-Hellman Key Exchange

- Diffie-Hellman (DH) bir şifreleme mekanizması değildir ve genellikle verileri şifrelemek için kullanılmaz.
- DH, verileri şifreleyen anahtarları güvenli bir şekilde değiştirmek için kullanılan bir yöntemdir.
- DH algoritmaları, iki tarafın şifreleme ve karma algoritmalar tarafından kullanılan paylaşılan bir gizli anahtar oluşturmasına izin verir.
- DH, IPsec standardının bir parçasıdır.
- DES, 3DES ve AES gibi şifreleme algoritmalarının yanı sıra MD5 ve SHA-1 karma algoritmaları, şifreleme ve şifre çözmeyi gerçekleştirmek için simetrik, paylaşılan bir gizli anahtar gerektirir.
- DH algoritması, iki eşin güvenli olmayan bir kanal üzerinden iletişim kurmalarına rağmen yalnızca kendilerinin bildiği paylaşılan bir gizli anahtar oluşturması için bir yol sağlayan bir genel anahtar değişim yöntemini belirtir.



Hash Algoritmalarıyla Bütünlük

- Orijinal gönderen, mesajın bir karmasını oluşturur ve mesajın kendisiyle birlikte gönderir.
- Alıcı, mesajı ve hash'i ayrıştırır, alınan mesajdan başka bir hash üretir ve iki hash'i karşılaştırır.
- Aynı iseler, alıcı orijinal mesajın bütünlüğünden makul ölçüde emin olabilir.
- Karma tabanlı Mesaj Kimlik Doğrulama Kodu (HMAC), karma işlevlerini kullanan mesaj kimlik doğrulaması için bir mekanizmadır.
- HMAC'ın iki parametresi vardır: Bir mesaj girişi ve yalnızca mesajı gönderen ve amaçlanan alıcılar tarafından bilinen bir gizli anahtar.
- Mesaj gönderen, gizli anahtarın ve mesaj girişinin yoğunlaştırılmasıyla oluşturulan bir değer (mesaj doğrulama kodu) üretmek için bir HMAC işlevi kullanır.
- Mesaj doğrulama kodu, mesajla birlikte gönderilir.
- Alıcı, kullanılan gönderici ile aynı anahtarı ve HMAC işlevini kullanarak, alınan mesajdaki mesaj kimlik doğrulama kodunu hesaplar.
- Alıcı, hesaplanan sonucu alınan mesaj doğrulama koduyla karşılaştırır.
- İki değer eşleşirse, mesaj doğru bir şekilde alınmıştır ve alıcı, gönderenin anahtarı paylaşan bir kullanıcı topluluğu üyesi olduğundan emin olur.

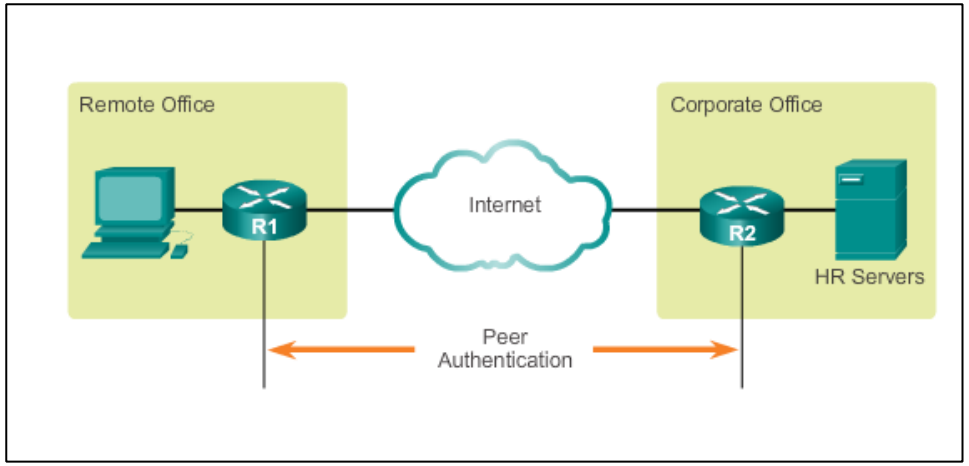


Hash Algoritmalarıyla Bütünlük-devam

- İki yaygın HMAC algoritması vardır:
- **MD5** – 128 bitlik paylaşılan bir gizli anahtar kullanır. Değişken uzunluklu mesaj ve 128 bit paylaşılan gizli anahtar birleştirilir ve HMAC-MD5 karma algoritması aracılığıyla çalıştırılır. Çıktı, 128 bitlik bir karmadır. Karma, orijinal mesaja eklenir ve uzak uca iletilir.
- **SHA** – SHA-1, 160 bitlik bir gizli anahtar kullanır. Değişken uzunluklu mesaj ve 160 bitlik paylaşılan gizli anahtar birleştirilir ve HMAC-SHA1 hash algoritması aracılığıyla çalıştırılır. Çıktı 160 bitlik bir karmadır. Karma, orijinal mesaja eklenir ve uzak uca iletilir.

IPsec Doğrulama

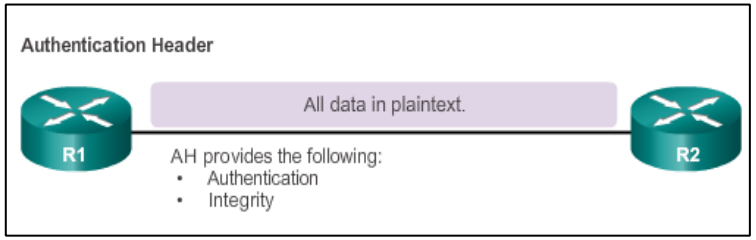
- IPsec VPN'ler kimlik doğrulamayı destekler.
- İletişim yolunun güvenli kabul edilmesi için VPN tünelinin diğer ucundaki cihazın kimliğinin doğrulanması gerekir.
- İki eş kimlik doğrulama yöntemi vardır, PSK ve RSA imzaları vardır:



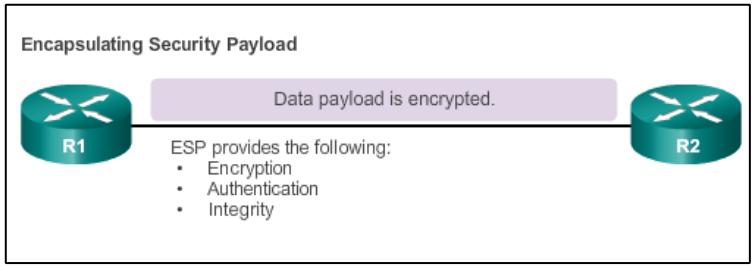
- **PSK**
  - Kullanılması gerekmeden önce güvenli bir kanal kullanılarak iki taraf arasında paylaşılan gizli bir anahtar.
  - Simetrik anahtar şifreleme algoritmaları kullanın.
  - Her eşe manuel olarak bir PSK girilir ve eşin kimliğini doğrulamak için kullanılır.
- **RSA**
  - Eşlerin kimliğini doğrulamak için dijital sertifikalar değiştirilir.
  - Yerel cihaz bir hash türetir ve bunu kendi özel anahtarıyla şifreler. Şifrelenmiş karma veya dijital imza, mesaja eklenir ve uzak uca iletilir.
  - Uzak uçta, şifrelenmiş hash'in şifresi, yerel ucun genel anahtarı kullanılarak çözülür.
  - Şifresi çözülmüş hash, yeniden hesaplanan hash ile eşleşirse, imza gerçektir.

IPsec Protokol Çerçevesi

- **Kimlik Doğrulama Başlığı (AH)**
- Gizliliğin gerekli olmadığı veya buna izin verilmediği durumlarda kullanılacak uygun protokol.
- İki sistem arasında iletilen IP paketleri için veri doğrulama ve bütünlük sağlar.
- Paketlerin veri gizliliğini (şifrelemesini) sağlamaz.

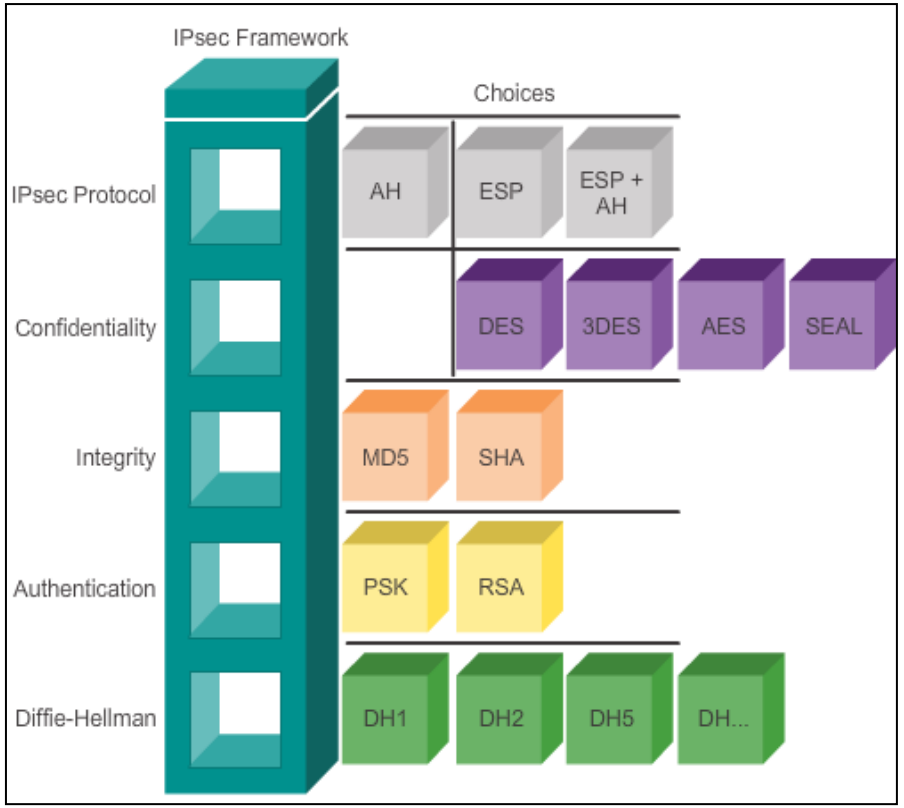


- **Kapsülleyen Güvenlik Yükü (ESP)**
- IP paketini şifreleyerek gizlilik ve kimlik doğrulama sağlayan bir güvenlik protokolü.
- İç IP paketini ve ESP başlığını doğrular.
- ESP'de hem şifreleme hem de kimlik doğrulama isteğe bağlıdır, en azından bunlardan biri seçilmelidir.



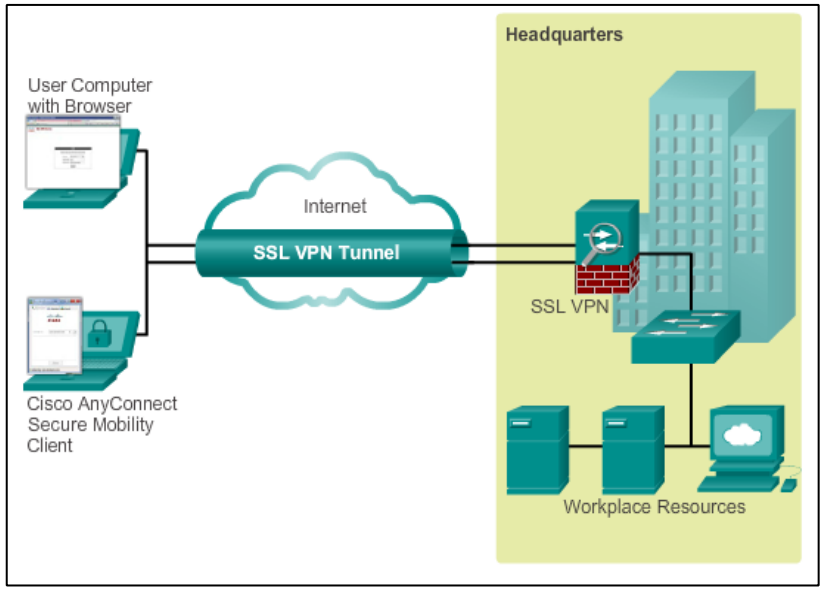
IPsec Protokol Çerçevesi-devam

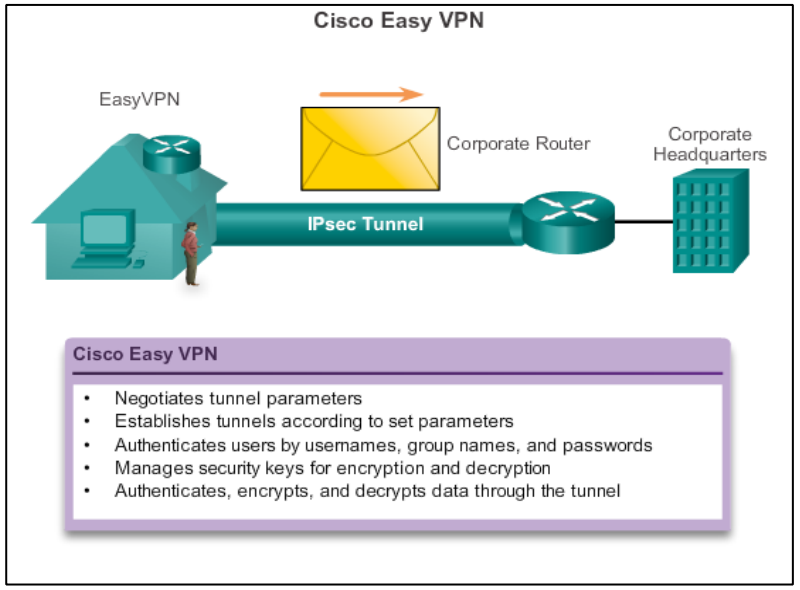
- **IPsec çerçeve protokolü** – AH'nin kendisi şifreleme sağlamadığından, ESP ve AH, ESP veya ESP+AH seçeneklerinin bir kombinasyonu neredeyse her zaman seçilir.
- **Gizlilik (IPsec ESP ile uygulanıyorsa)** – DES, 3DES veya AES, en yüksek güvenliği sağladığı için AES kesinlikle önerilir.
- **Bütünlük** – Karma algoritmalar (MD5 veya SHA) kullanılarak içeriğin aktarım sırasında değiştirilmediğini garanti eder.
- **Kimlik doğrulama** – VPN tünelinin her iki ucundaki cihazların nasıl doğrulandığını (PSK veya RSA) temsil eder.
- **DH algoritma grubu** – Eşler arasında paylaşılan bir gizli anahtarın nasıl oluşturulduğunu temsil eder, DH24 en yüksek güvenliği sağlar.



Uzaktan Erişim VPN

- Uzaktan erişim VPN'lerini dağıtmak için iki temel yöntem vardır:
  - Güvenli Yuva Katmanı (SSL)
  - IP Güvenliği (IPsec)
- Kullanıcıların erişim gereksinimlerine ve kuruluşun BT süreçlerine dayalı VPN yöntemi türü.
- Her iki tür de neredeyse tüm ağ uygulamalarına veya kaynaklarına erişim sunar.





Uzaktan Erişim VPN-devam

Parametre	SSL VPN	IPsec VPN
Uygulamalar	Web temelli uygulamalar, dosya paylaşımı, Email	Tüm IP temelli uygulamalar
Şifreleme	**Orta-Güçlü** Anahtar uzunluğu 40 bit--256 bit	**Güçlü** Anahtar uzunluğu 56 bit--256 bit
Kimlik Doğrulama	**Orta** Tek yönlü veya çift yönlü kimlik doğrulama	**Güçlü** Paylaşımlı-Dijital sertifika kullanarak çift yönlü kimlik doğrulama
Bağlantı Karmaşıklığı	**Zayıf** Sadece bir web tarayıcı	**Orta** Teknik olmayan kullanıcılar için zorlayıcı
Bağlantı Seçenekleri	Herhangi bir cihaz bağlantı kurabilir.	Sadece özel ayarlama yapılan cihazlar bağlantı kurabilir.