ÖZET

SİTEDEN SİTEYE SANAL ÖZEL AĞ VE DİNAMİK ÇOK NOKTALI SANAL ÖZEL AĞ KARŞILAŞTIRMALI İNCELENMESİ

SEYYAR, Yunus Emre
Kırıkkale Üniversitesi
Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı, Yüksek Lisans Tezi
Danışman: Yrd. Doç. Dr. H. Murat ÜNVER
Eylül 2013, 141 sayfa

Günümüzde birçok kullanıcı (bankalar, telekomünikasyon firmaları, birden fazla şubeye sahip kuruluşlar, yurt dışı ofisleri olan firmalar, vs.) çeşitli nedenlerden dolayı (güvenlik, hızlı iletim, vs.) siteden siteye sanal özel ağlar kullanmaktadır. Ancak gelişen koşullarda kullanılan bu yöntem bazı nedenlerinden dolayı çok noktalı kullanıcılar için performans kaybına sebep olmaya başlamıştır. Bunun üzerine çok noktalı sanal özel ağlar geliştirilmiş ve kullanılmaya başlamıştır. Bu çalışma aynı zamanda sanal özel ağların başlangıcından bu zamana kadar gelişimini de göstermektedir.

Bu çalışmada bir ağ benzetim programı (GNS3) kullanılarak iki örnek sanal özel ağ konfigürasyonu oluşturulmuştur ve bir ağ haberleşme simülasyonu koşularak oluşan ağ trafiği gözlemlenmiştir.

Sonuç olarak; bu çalışma ile çok noktası olan firmalar için hem performans açısından hem maliyet açısından hem de konfigürasyon kolaylığı açısından dinamik sanal özel ağın faydalı olduğu gözlemlenmiştir.

Proje uygulama alanları çok geniş olması nedeniyle birkaç örnek ile ele alınmış ve incelenmiş hâlihazırda dinamik çok noktalı sanal özel ağ kullanımının siteden siteye sanal özel ağ kullanımı yerine kullanılmasının faydalı olduğunu ortaya konulmuştur.

Anahtar kelimeler: Siteden siteye, sanal özel ağ, dinamik çok noktalı, internet güvenlik protokolü, çok noktalı genel yönlendirme

ABSTRACT

THE CONFRANTATIVE/CONTRASTIVE STUDY OF SITE TO SITE VIRTUAL PRIVATE NETWORK AND DYNAMIC MULTIPOINT VIRTUAL PRIVATE NETWORK

SEYYAR, Yunus Emre
Graduate School of Natural and Applied Sciences
Department of Computer Engineering, M.Sc. Thesis
Supervisor: Assist. Prof. Dr. H. Murat ÜNVER
September 2013, 141 pages

Today many users (banks,telocomunication companies, firms that have more than one office or offices in abroad, etc.) are using site to site virtual private networks for some reasons (security, fast transmission, etc.). But in current conditions, using this method for multipoint users causes a decrease in performance for some reasons. To cope with this problem multipoint virtual private networks are developed and are being used. This work is also gives to development in virtual private networks up to now.

In this work two sample vitrual private networks were configured using a network simulation program (GNS3), and a network communication simulation was run and the resulting network traffic is obsorved.

As a result; the benefits of dynamical virtual private network for companies that have distrubuted offices were shown according to cost, performance and configuration simplicity.

Because of large application areas, a few samples are handled and it is shown that using dynamical multipoint virtual private network is better than site to site virtual private network.

Key Words: Site to site, vpn, dynamic multipoint, ipsec, mgre

TEŞEKKÜR

Tez çalışmalarım esnasında destek ve yardımlarını hiçbir zaman esirgemeyen, çok değerli hocam sayın Yrd. Doç. Dr. H. Murat ÜNVER' e teşekkür ederim

İÇİNDEKİLER

Sayfa

ÖZET i

ABSTRACT iii

TEŞEKKÜR iv

İÇİNDEKİLER v

ŞEKİLLER viii

KISALTMALAR xi

1. GİRİŞ 13

2. MATERYAL VE YÖNTEMLER 19

2.1. Genel Ağlara Bakış 20

2.2. Sanal Özel Ağ Kullanım Alanları 22

2.2.1. Sanal Özel Ağ (Uzaktan Erişimli) 22

2.2.2. Sanal Özel Ağ (Intranet) 24

2.2.3. Sanal Özel Ağ (Extranet) 27

2.3. Sanal Özel Ağ Bileşenleri 30

2.3.1. Sanal Özel Ağ Donanım Bileşenleri 31

2.3.2. Sanal Özel Ağ Yazılım Bileşenleri 33

2.4. Sanal Özel Ağlarda Güvenlik 34

2.4.1. Güvenlik Duvarı 35

2.4.2. Ağ Adresi Dönüştürme (NAT) 35

2.4.3. Kimlik Doğrulama 36

2.4.4. Doğrulama Yetkilendirme Aktivite İzlenmesi (AAA) 39

2.5. Sanal Özel Ağ Güvenliği 41

2.5.1. Kimlik Doğrulama ve Erişim 42

2.5.2. Erişim Kontrolü 42

2.5.3. Veri Şifrelenmesi 43
2.5.4. Simetrik Kripto Algoritmaları 44
2.5.5. Asimetrik Kripto Sistemler 46
2.5.6. Açık Anahtar Yapısı 49
2.6. Sanal Özel Ağlarda Tünelleme 53
2.6.1. Tünellemenin Fonksiyonu 53
2.6.2. Tünellemenin Avantajları 55
2.6.3. Tünelleme Tekniğinin Bileşenleri 56
2.6.4. Tünellenen Paket Formatı 57
2.6.5. Tünel Tipleri 58
2.7. Tünelleme Protokolleri 59
2.7.1. Noktadan Noktaya Protokol (PPP) 60
2.7.2. Noktadan Noktaya Tünelleme Protokolü (PPTP) 63
2.7.3. İkinci Katman Yönlendirme Protokolü (L2FP) 71
2.7.4. İkinci Katman Yönlendirme Tünelleme Protokolü (L2TP) 76
2.7.5. Protokollerin Karşılaştırılması 77
3. ARAŞTIRMA BULGULARI 79
3.1. Yönlendirme Protokolleri 91
3.2. Siteden Siteye Sanal Özel Ağ 93
3.2.1. İnternet Güvenlik Protokolü (IPSEC) 99
3.2.2. Kapsülleyen Güvenlik Veri Yükü (ESP) 107
3.3. Dinamik Çok Noktalı Sanal Özel Ağ (DM VPN) 108
3.3.1. Gelecek Durak Karar Protokolü (NHRP) 116
3.3.2. Çok Noktalı Genel Yönlendirme Kapsülü (MGre) 116
3.3.3. İnternet Güvenlik Protokolü (IPSEC) 116
3.4. Siteden Siteye Sanal Özel Ağ Ve Dinamik Çok Noktalı Sanal Özel Ağ Karşılaştırmalı İncelenmesi 116

4. SONUÇLAR 123

KAYNAKLAR 124

EKLER..... 126

ŞEKİLLER

ŞEKİL Sayfa

2.1. Sanal özel ağ olmadığı durumda tipik bir uzaktan erişim yapısı 22
2.2. Sanal özel ağ (Uzaktan Erişimli Yapısı) 23
2.3. Sanal özel ağ olmayan geniş alan ağ 25
2.4. Sanal özel ağ ile intranet bağlantısı 26
2.5. Sanal özel ağ kullanılmayan extranet yapısı 27
2.6. Extranet sanal özel ağ yapısı 28
2.7. Sanal özel ağ bağlantı tipleri 29
2.8. Sanal özel ağ çözümünde kullanılan bileşenler 30
2.9. Sanal özel ağ istemci profilleri 32
2.10. Intranet ve İnternet arasındaki güvenlik duvarı 35
2.11. Ağ adresi dönüştürme yapısı 36
2.12. Radius sunucu 37
2.13. RAS sunucu 38
2.14. Sanal özel ağ doğrulama, yetkilendirme, aktivite izlenme yapısı 40
2.15. Sanal özel ağ senaryosunda kimlik doğrulama 42
2.16. Şifreleme mekanizması 44
2.17. Simetrik şifreleme tekniği 45
2.18. Diffie-Hellman algoritması 47
2.19. RSA algoritma mantığı 48
2.20. Açık anahtar yapısı tabanlı iletim 52
2.21. Sanal özel ağ tüneli 53
2.22. Tünelleme tekniği 55
2.23. Tüneller içinden iki fazda veri iletimi 57
2.24. Tünellenmiş paketin yapısı 58
2.25. İsteğe bağlı olarak oluşturulan tünel yapısı 59
2.26. Sunucular tarafından oluşturulan tüneller 59
2.27. Tünelleme protokolünü kullanan tünellenmiş paketler 60
2.28. Noktadan noktaya protokol bağlantının kurulması 61
2.29. Noktadan noktaya çerçeve formatı 62
2.30. Noktadan noktaya tünelleme protokol paketin yapısı 64

2.31. Noktadan noktaya protokol işlemleri 65
2.32. Noktadan noktaya tünel protokolü ve bileşenleri..... 66
2.33. Noktadan noktaya tünel protokolü paketi 66
2.34. PPP bağlantı üzerinden PPTP kontrolünün yapılması 67
2.35. Noktadan noktaya tünel prtokolü ile veri tünelleme işlemi 68
2.37. İstemci ve sunucu arasında ikinci katman yönlendirme tünelin kurulması 73
2.38. İkinci katman yönlendirme tünelleme işlemi 74
2.39. İkinci katman yönlendirme paket formatı 74
2.40. İkinci katman yönlendirme tünelleme mesajın yapısı..... 76
2.41. ESP ile şifrelenmiş bir ikinci katman yönlendirme tünelleme paketin yapısı .. 77
3.1. Sanal ağ ayarları..... 80
3.2. Sanal ağ ayarları sanal ethernet kartı ekleme..... 81
3.3. Sanal ağ ayarları sanal ethernet kartı seçimi 82
3.4. Sanal ağ ayarları eklenen ethernet kartları 82
3.5. Sanal bilgisayar ayarı 83
3.6. Sanal bilgisayar ethernet seçimi..... 83
3.7. Sanal bilgisayar ip adresi 84
3.8. Sanal bilgisayar ethernet adresi..... 85
3.9. GNS3 açılış ekranı 86
3.10. GNS3 Cisco yönlendirici IOS seçimi 86
3.11. GNS3 IOS yüklenmesi..... 87
3.12. Cisco IOS kaydedilmesi..... 87
3.13. GNS bölümleri 88
3.14. Sanal yönlendiriciler arasında yapılacak bağlantı için kablolama çeşitleri 89
3.15. Sanal Ethernet kart eklenmesi..... 90
3.16. Sanal ethernet kart seçimi 90
3.17. Sanal ethenert kartının yüklenmesi 91
3.18. Siteden siteye sanal özel ağ..... 94
3.19. Sanal bilgisayarlardan atılan ping ve alınan cevaplar 95
3.20. Sanal bilgisayarlardan atılan ping ve alınan cevaplar 95
3.21. Sanal bilgisayarlardan atılan tracert ve alınan cevap 96
3.22. ANK yönlendiricisinde isakmp doğrulanması..... 96
3.23. IST yönlendiricisinde isakmp tablosu..... 96
3.24. ANK yönlendiricisinde eigrp komşuluğu ve hello paketleri 97

3.25. ANK yönlendiricisinde tünelin başlaması 97
3.26. İnternet güvenlik protokolü mimarisi..... 100
3.27. İnternet güvenlik protokolü iletim modu 101
3.28. İnternet güvenlik protokolü tünel modu..... 101
3.29. Pakete doğrulama başlığı uygulanması 106
3.30. Pakete kapsülleyen güvenlik veri yükü uygulanması 107
3.31. Dinamik Çok Noktalı Sanal Özel Ağ..... 110
3.32. HUB yönlendiricisine ait nhrp tablosu..... 110
3.33. IST yönlendiricisine ait nhrp tablosu 111
3.34. IZM yönlendiricisine ait nhrp tablosu..... 111
3.35. LA yönlendiricisine ait nhrp tablosu..... 111
3.36. HUB yönlendiricisine ait dmvpn tablosu..... 112
3.37. IST yönlendiricisine ait dmvpn tablosu 112
3.38. IZM yönlendiricisine ait dmvpn tablosu 112
3.39. LA yönlendiricisine ait dmvpn tablosu 113
3.40. HUB yönlendiricisine ait isakamp tablosu..... 113
3.41. IST yönlendiricisine ait isakamp tablosu 113
3.42. IZM yönlendiricisine ait isakamp tablosu..... 114
3.43. LA yönlendiricisine ait isakamp tablosu..... 114
3.44. İlgili sanal bilgisayardan diğer bilgisayar ping işlemi 114
3.45. İlgili sanal bilgisayardan diğer bilgisayar "ping" işlemi..... 115
3.46. İlgili sanal bilgisayardan diğer bilgisayar "tracert" işlemi..... 115
3.47. Siteden siteye sanal özel uygulamasına gönderilen paket (ping)..... 118
3.48. Dinamik çok noktalı sanal özel uygulamasına gönderilen paket (ping) 118
3.49. Siteden siteye sanal özel ağ uygulamasında yer alan iki lokasyon arasında mevcut sanal bilgisayarlar arasındaki ping işleminin süresi..... 119
3.50. Dinamik çok noktalı sanal özel uygulamasında yer alan merkez lokasyon ve şube lokasyon arasında mevcut sanal bilgisayarlar arasındaki ping işleminin süresi 119
3.51. Dinamik çok noktalı sanal özel uygulamasında yer alan iki şube lokasyon arasında mevcut sanal bilgisayarlar arasındaki ping işleminin süresi 120
3.52. Dinamik çok noktalı sanal özel uygulamasında yer alan şube ve merkez lokasyon arasında mevcut sanal bilgisayarlar arasındaki ping işleminin süresi 120

KISALTMALAR

AAA	Authentication Authorization Accounting
ADSL	Asymmetric Digital Subscriber Line
AES	Advance Encryption Standart
AH	Authentication Header
ATM	Asynchronous Transfer Mode
AURP	Apple Talk Routing
CA	Certification Authority
CDS	Certificate Distribution System
CHAP	Challenge-Handshake Authentication Protocol
DES	Data Encryption Standart
EIGRP	Enhanced Interior Gateway Routing Protocol
ESP	Encapsulating Security Payload
FA	Foreign Agent
FCS	Frame Check Sequence
FDDI	Fiber Distributed Data Interface
GRE	Generic Routing Encapsulation
HA	Home Agent
HDLC	High Level Data Link Control
HMAC	Keyed-Hashing for Message Authentication Code
ID	Identity
IETF	Internet Engineering Task Force
IGRP	Interior Gateway Routing Protocol
IKE	Internet Key Exchange
IP	Internet Protocol
IPSEC	IP Security
ISAKMP	Internet Security Association and Key Management Protocol
ISDN	Integrated Services Digital Network
L2FP	Layer 2 Forwarding Protocol
LAN	Local Area Network
LCP	Link Control Protocol

MAC	Message Authentication Code
MD	Message Digest
MGRE	Multipoint Generic Routing Encapsulation
MPPE	Microsoft Point-to-Point Encryption
NAS	Network Access Server
NAT	Network Address Translation
NCP	Network Control Protocol
NHRP	Next Hop Resolution Protocol
PKI	Public Key Infrastructure
POP	Point of Presence
POTS	Plain Old Telephone Service
PPP	Point to Point Protocol
PPTP	Point to Point Tunnel Protocol
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RA	Registration Authority
RAS	Remote Access Server
RIP	Router Information Protocol
RSA	Rivest-Shamir-Adleman Güvenlik Firması
SA	Security Association
SHA	Secure Hash Algorithm
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VPN	Virtual Private Network, Sanal Özel Ağ
WAN	Wide Area Network

1. GİRİŞ

Günümüzde internet hayatımızın vazgeçilmez bir parçası olma yolunda hızla ilerlemektedir. Büyüyen firmalar merkez ofisleri dışında şube açmak zorunda kalmaktadır. Eskiden şubeler arası iletişimler noktadan noktaya hat (leased line vb.) hizmeti alınarak sağlanmaktaydı. Gelişen teknoloji ile birçok firma tarafından tercih edilen; Sanal özel ağ (VPN, Virtual Private Network) teknolojisi ortaya çıktı. Bu yeni teknoloji daha esnek ve en önemlisi çok daha düşük maliyetler ile geleneksel çözümlerinin tüm işlevlerini yerine getirmektedir.

Ağ teknolojilerindeki düzenli gelişmelere rağmen, kurumların hedefi daha hızlı ve daha verimli haberleşme olanaklarını kullanabilmektir. Personel ve yöneticiler dünyanın neresinde olurlarsa olsunlar, yerel ağlarına sanki ofislerindeymiş gibi erişebilmek isterler.

1980 ortalarında ve 1990 başlarında uzak erişim için telefon hatları kullanılıyordu. Şirketler, yöneticilerinin taşınabilir bilgisayarlarına veri sıkıştırabilme yeteneğine sahip hızlı modemler yerleştirip, ofisteki sunuculara bağlanabilmelerini sağlayabilmekteydiler. Çalışanların ve yöneticilerin yapması gereken sadece bulundukları ortamda RJ-11 telefon konnektörünü modemlerine takmak ve uzak erişim sunucularına şifreleri yetkisinde bağlanabilmekti.

1990 sonlarında kurumlar, uzak erişimin şirketlerine sağladığı avantajları daha çok farkına varmaya başladılar ve bazı büyük şirketler, ülke içinde ücretsiz aranabilecek telefon numaraları ile çalışanlarına bu hizmeti sundular. Uluslararası ticaret yapan kurumlarda ise, milletlerarası telefon görüşmelerinin ücretleri söz konusu olduğu için uzak erişim servisleri şirketlere ciddi bir maliyet getirmekteydi.

Sanal özel ağ teknolojisinin cazip hale gelmesinin sebebi, kurum/şirket çalışanlarının yerel ağ sunucularında ve kurumsal ağlarda uzak noktalardan çalışmaya başlamış olmalarıdır. Bu, çalışanların işlerini uygun bir şekilde yürütebilmeleri için kurumsal yerel ağlara, web uygulamalarına ve diğer sunuculara uzaktan erişim sağlamalarında büyük önem taşımaktadır.

Günümüzde sadece büyük kuruluşlar değil küçük ve orta ölçekli firmalar da ofislerini, bayilerini, iş ortaklıklarını kolayca ve ekonomik yoldan birbirine bağlayarak veri, hatta ses veya video iletişimi sağlama ihtiyacı duyuyor. Bu ağ yapısını firmaların kendi başına kurmaları son derece yüksek maliyetli ve zahmetli olduğundan, bağlantı ihtiyaçlarını sanal özel ağlar sayesinde daha düşük maliyetler karşılığında, ülke geneline dağılmış erişim noktalarına ve yüksek performanslı bir ulusal omurgaya sahip internet servis sağlayıcılar aracılığı ile karşılamayı tercih ediyorlar.

Sanal özel ağ teknolojisi, firmaların şubeleri ve iş ortaklıkları ile aralarında veri iletişimini güvenilir, kolay ve ekonomik biçimde sağlamasına olanak veren bir tünelleme teknolojisidir. Kurumların yerel ağlarını internet ortamı üzerine taşınmasını sağlar. Sanal özel ağ teknolojisinde, noktalar arası ekonomik ve güvenilir bağlantılar kurulurken iletişim maliyetini minimum seviyede tutabilmek için internet ortamı "iletişim omurgası" olarak kullanılır. Sanal özel ağlarda kullanılan ağ kamuya açık bir ağdır. Ancak ileti bir noktadan diğer bir noktaya kadar özel bir tünel aracılığı ile şifrelenerek ulaşır. Böylece personel ve yöneticiler dünyanın neresinde olursa olsunlar, yerel ağlarına sanki ofislerindeymiş gibi erişebilme imkânına sahip olurlar. Bu teknoloji sayesinde belirli lokasyonlarda uzak ofisleri bulunan kurumlar, ofislerinin kendi aralarında haberleşmelerini, doküman transferlerini, stok bilgilerini, satış bilgileri gibi çeşitli uygulamalarını bu sanal ağ üzerinden güvenli bir şekilde gerçekleştirebilirler.

Gerek intranet, extranet sanal özel ağlarda gerekse uzaktan erişim/çevirmeli sanal özel ağ çözümlerinde güvenlik, tünelleme teknolojisi ile garanti edilmektedir. Temel olarak, sanal özel ağ trafiği servis sağlayıcının internet omurgasında güvenli ve sarmalanmış, kapalı bir tüneli içinde dolanır. Bu tünele giriş veya tünelden çıkış noktası sadece kurum tarafındaki güvenli yönlendirici veya ağ güvenlik sunucusudur.

Geniş alan ağ (WAN) oluşturma yollarından biri olan sanal özel ağ, altyapı olarak interneti kullandığından maliyeti en düşük bir WAN çözümüdür. “sanal özel ağlar kiralık özel veri hatlarının güvenilirliğine erişebilir mi? ” sorusu akıllara gelmektedir. Pratik olarak sanal özel ağ çözümlerinde güvenlik sorun olmaktan çıkmıştır. Tüm

sanal özel ağ çözümlerinde internet erişimi üzerinden kurulan güvenli tüneller söz konusudur.

Güvenli tüneller, kriptolama teknikleri ile sağlanır. Sanal özel ağlar bir kuruma, bir servis sağlayıcının herkese açık ağının veya internetin ölçeğini kullanarak, servis sağlayıcı yerel (bulunma noktası) POP noktaları üzerinden kurum ağına uzaktan bağlanabilme olanağı sağlar. Bu durum, kurumlara merkez ofiste yer alan uzaktan erişim sunucuları (RAS, Remote Access Server) sunucuya doğru yapılan uzak mesafeli telefon çağrı ücretlerinden tasarruf sağladığı gibi aynı zamanda kurum içinde uzaktan erişim sunucu (RAS) tabanlı uzaktan erişim çözümleri barındırmanın getirdiği harcamalar ve yönetim masraflarında da azalmalar sağlar. Sanal özel ağlar aynı zamanda, işletmeden işletmeye e-ticaret bağlantılarına yönelik yeni extranet uygulamalarına da olanak tanır. Çerçeve anahtarlama (Frame Relay), özel kiralık hatların bulunmadığı veya çok pahalı olduğu birbirine uzak ofisler için kurumlar, internetin her tarafta bulunma ve ekonomik olma özelliğinden yararlanabilir. İnternet üzerinden kritik bilgilerin transfer için gerekli olan gizlilik ve güvenlik konuları sanal özel ağ teknolojileri yardımıyla çözülmüştür.

Sanal özel ağ sanaldır: Her bir sanal özel ağ bağlantıda ağın fiziksel yapısı şeffaf özelliktedir. Yani sanal özel ağ kullanıcısı bağlı olduğu esnada bağlantı yaptığı ağı sahiplenmez, bu ağ aynı anda birçok sanal özel ağ kullanıcısı tarafından paylaşılır.

Sanal özel ağ özeldir: Özel olması sanal özel ağ üzerinden akan trafiğin özel olması anlamındadır. Sanal özel ağ trafiği internet üzerinden geçer. Sanal özel ağ trafiğinin internet üzerinden güvenli geçişini sağlamak için özel ağ önlemlerine ihtiyaç vardır. Örneğin veri şifreleme, veri doğrulaması (data authentication), yetkilendirme (authorization) ve adres yanıltmanın önlenmesi gibi.

Sanal özel ağ bir ağdır: Fiziksel bir varlığı olmayıp sanal olsa da sanal özel ağ bir ağ özelliğindedir. Sanal özel ağ, iki uç arasında güvenilir tünel bağlantısı sağlayan bir ağdır.

Sanal özel ağ'ları kimler kullanır?

- Yurtdışında ofisleri bulunan,

- Yüksek seviyede bilgi güvenliğine ihtiyacı olan,

- Yurtiçi veya yurtdışında mobil personeli bünyesinde barındıran kurumlar için VPN en ideal çözümdür [1].

Chen X., De Leenheer M., Wang R., S.K. Vadrevu C., Shi L., Zhang J., Mukherjee B.'nin yaptığı çalışmada birinci katman sanal özel ağ'ları (Fiziksel ağ, Optik omurga ağ, vs.) kullanarak, bulut bilişim ve diğer kurumsal ağları için basit yapıları oluşturan çoklu sanal ağları destekleyebilmesinden bahsedilmiştir. Layer1 Sanal Özel Ağ hortum modeli tüketicilerin bant genişliği ihtiyaçlarını son nokta için toplam gelen ve giden bant genişliği ihtiyacını ortaya koyan uygun ve esnek olan bir yol olduğu belirtilmiştir. Bunun yanında çoklu alan fiziksel yapılar, küresel ölçekle uygulandığı için çok yaygındırlar. Bu yüzden yüksek performanslı çok alanlı özel sanal ağ hazırlığı için yönlendirme (RMVP, Routing for Multi-domain VPN Provisioning) hortum modeli için küresel sanal yapısını etkin bir şekilde destekleyen çok önemli bir problem olduğu ifade edilmiştir. RMVP problemini doğrusal birleşik karışım programı (MILP, Mixed Integrated Linear Program) olarak formüle edilmiştir. Sonuçlar TDR (Yukarından-Aşağı Yönlendirme) yaklaşımının Tek Domain Yönlendime (SDR) ile kıyaslandığı zaman minimum yönlendirme maliyetine sahip olduğunu göstermiştir [2].

Wang M., Pan J., Zheng Z.'in olduğu çalışmada internet ve multimedya bilgisayar teknolojisinin gelişmesi ile birlikte sanal sınıflar yeterli teknik desteğe ihtiyaç duymaları ele alınmıştır. Sanal sınıf uygulamasının geleneksel eğitimi, öğrenme ve öğretmede ana değişikliğe sebep olmasından bahsedilmiştir. İnternet üzerinden bilim adamı yetiştiren sanal sınıf içerisinde sanal özel ağ teknolojisi ve kampüste sanal sınıf öğrenmesi tartışılmıştır [3].

Matsuhashi Y., Shinagawa T., Ishii Y., Hirooka N., Kato K.'nun yaptığı çalışmada bulut bilişim yaygın olarak kullanım alanlarının yaygınlaşması ile birlikte sanal özel ağ'larda da kullanılmaya başlandığı belirtilmiştir. Bu kullanımla beraber kullanıcı ile bulut arasındaki iletişimin önem kazanmaya başladığı ifade edilmiştir. Bulut

hizmetinin Sanal Özel Ağ hatasından kaynaklı akmaları ortadan kaldırmak, en aza indirmek için bir şema hazırlanmıştır [4].

Yüksel E., Örencik B.'in yaptığı çalışmada Microsoft Windows Platformunda, WinPCap adlı açık kaynak kodlu bir kütüphane kullanılarak geliştirilmiştir. Çalışmanın amacı Sanal Özel Ağ'ı oluşturan şifreleme, asıllama ve kapsülleme gibi ana unsurları başarmaktır [5].

Guadong G,'ın yaptığı çalışmada geleneksel Sanal Özel Ağ yapısı ile halen çözülememiş olan kurumsal ağ yapılarında mevcut olan problemlerin Çok Noktalı Sanal Özel Ağ yapısında analizinin yapılmasıdır. Bu yapının hızlı, uygun, ekonomik bir yatırım olduğu önerilmiştir [6].

Soğukpınar İ.'ın yaptığı çalışmada açık anahtarlı kripto sistemleri ve sayısal imza oluşturulmasında kullanımı anlatılmıştır [7].

Yerlikaya T., Buluş E., Buluş N.'un yaptığı çalışmada kripto algoritmalarının gelişimi ve önemi açıklanmış, şifreleme algoritmalarının yapıları incelenmiş, simetrik şifreleme algoritmalarından DES şifreleme algoritmasının yapısı ve özellikleri incelenmiştir [8].

Akçam N,'ın yaptığı çalışmada bir çok alanda kullanılan cihazların yaygınlaşması nedeniyle kötü niyetli şahıslardan uzak tutularak gizlilik, güven içinde sürdürülmesi için şifreleme algoritmaları incelenmiş ve bunlardan en güvenlisi olarak bulunan RSA algoritması kullanılarak protokol hazırlanması için bir yazılım gerçekleştirilmiştir [9].

Demirkol S. A., Çağlayan U. M.'ın yaptığı çalışmada doğrulama, yetkilendirme, aktivite izlenmesi (AAA) ve Mobil IP v4 iletişimleri paralel gerçekleştirilerek yeni bir çözüm önerilmiştir. Bu öneride AAA ve Mobil IPv4 standartlarını bozmadan yeni bir oturum açmak için gereken zaman kısaltılmıştır [10].

Bu çalışmada siteden siteye sanal özel ağ ile dinamik çok noktalı sanal özel ağ karşılaştırmalı incelenmesi yapılmıştır. Tezin ikinci bölümünde sanal özel ağ hakkında bilgiler verilmiştir. Tezin üçüncü bölümünde siteden siteye sanal özel ağ ve dinamik çok noktalı sanal özel ağ kurulumu yapılmıştır, her iki sanal özel ağ'da eşit büyüklükte paketler gönderilmiştir. Bu paket ölçüt alınarak iki sanal özel arasında karşılaştırma ve incelemeler yapılmıştır. Tezin dördüncü bölümünde yapılan karşılaştırmalı incelemeler neticesinde ulaşılan sonuçlar verilmiştir. Bu sonuçlara ölçüt alınarak öneriler yapılmıştır.

2. MATERYAL VE YÖNTEMLER

Araştırma, ihtiyaçlar neticesinde ortaya çıkan ve birçok firma tarafından kullanılmaya başlanan siteden siteye sanal özel ağ ve dinamik çok noktalı sanal özel ağ karşılaştırmalı incelenmesidir.

Araştırma kapsamını sanal özel ağın ne olduğu, hangi cihazların kullanıldığı, güvenliğinin nasıl sağlandığı, sanal özel ağ içerisinde kullanılan şifreleme protokollerinin neler olduğu, siteden siteye sanal özel ağ oluşturması ve yapılandırması, dinamik sanal özel ağ topolojisinin çıkarılması ve yapılandırması oluşturmaktadır.

Materyaller
Araştırma kapsamında kullanılan materyaller:

1. Sanal özel ağ topolojisini oluşturulması ve gözlemlerin yapılması için GNS3 isimli benzetim uygulaması kullanılmıştır.

2. İlgili yerleşkelerin haberleşmesinin sanal bilgisayarlar üzerinde testlerinin yapılması için Vmware isimli sanallaştırma uygulaması kullanılmıştır.

Yöntemler
Araştırma kapsamında kullanılan yöntemler:

1. Siteden siteye sanal özel ağ yapılandırması

2. Dinamik çok noktalı sanal özel ağ yapılandırması

3. EIGRP yönlendirme protokolü

4. İlgili şifreleme algoritmaları (AES, DES, 3DES, MD5, Deffie-Helman, RSA)

2.1. Genel Ağlara Bakış

İnternet bir açık ağ olarak nitelendirilir. Fakat başka açık ağlarda mevcuttur. Açık ağların listesi aşağıda görülmektedir.

1. Düz Eski Telefon Hizmeti (POTS, Plain Old Telephone Service): POTS günlük yaşantımızda kullandığımız sabit telefon servislerini sağlayan ağdır. POTS ve POTS olmayan servisler arasındaki temel fark iletim hızıdır. POTS ağlarda en yüksek iletim hızı 56 Kbps'dir.

2. Genel Aktarmalı Telefon Şebekesi (PSTN, Public Switched Telephone Network): PSTN bakır kablo altyapısı üzerinden telefon servislerini sağlayan bir analog teknoloji olup son zamanlarda ADSL, DSL, ISDN, FDDI, Frame Relay ve ATM gibi dijital teknolojilerde de kullanılmaya başlanmıştır.

3. İnternet: İnternet ağı POTS ve PSTN altyapısını kullanır. Bu iki ağdan farkı tüm haberleşmeleri kontrol etmek ve yönetmek için TCP/IP protokolünü kullanmasıdır. Genel ağlar hızlı iletimler için farklı teknolojiler kullanır. Bu teknolojiler aşağıda görülmektedir:

- Asimetrik Sayısal Abone Hattı (ADSL, Asymmetric Digital Subscriber Line): ADSL, PSTN altyapısını kullanarak yüksek hızda dijital veri iletimi sağlar. ADSL, 64 Kbps ve 8 Mbps arasındaki bant genişliklerini destekler.

- Fiber Dağıtık Veri Bağdaştırıcı (FDDI, Fiber Distributed Data Interface): FDDI, dijital sinyalleri fiber optik altyapı üzerinden ileten bir LAN teknolojisidir. Veri iletiminde jeton yapısını kullanır. Genelde WAN omurgasında kullanılır. FDDI'in son versiyonu olan FDDI-2'de ses ve video sinyallerinin iletimi daha başarılı olmaktadır.

- Tümleşik Hizmetler Sayısal Şebekesi (ISDN, Integrated Services Digital Network): Bakır altyapı üzerinden ses, video ve veri iletimini fiber altyapı kadar başarılı bir şekilde yapabilen teknolojidir. ISDN, modem yerine uçlarda ISDN adaptör (CSU/DSU) kullanır. ISDN'de temel oran ISDN (BRI, Basic Rate ISDN) ve

birincil oran ISDN (PRI, Primary Rate ISDN) olmak üzere 2 tip servis vardır. BRI ev kullanıcıları için uygun bir servistir, PRI ise daha çok kurumsal amaçlı kullanılan bir servistir. ISDN'de 2 tip kanal vardır. B kanalı, veri, ses ve diğer sinyalleri taşırken D kanalı kontrol ve sinyalleşme bilgisini taşır. Günümüzde geniş bant bir ISDN teknolojisi olan B-ISDN yaygın olarak kullanılmaktadır. Aynı kanal üzerinden farklı tipte sinyal gönderme yeteneğine sahiptir ve 1.5 Mbps hızı destekleyebilmektedir. ISDN BRI, 2 adet 64 Kbps B kanalına ve bir adet 16 Kbps D kanalına sahiptir. Bundan dolayı 144'Kbps'lik bir kapasiteye sahiptir. PRI ise 30 adet B kanalı ve 1 adet D kanalına sahiptir ve yaklaşık 2 Mbps kapasiteye sahiptir.

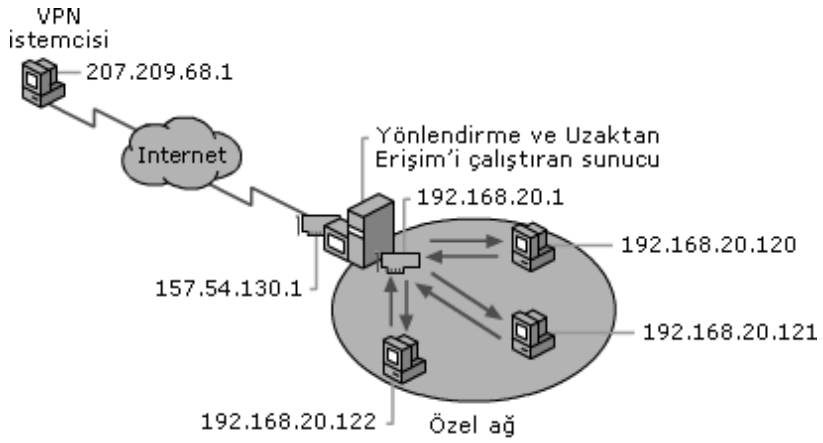
- Çerçeve Anahtarlama (Frame Relay): X25 paket anahtarlama teknolojisine dayanır. LAN ağından WAN ağına veri trafiğini taşıyan düşük maliyetli bir çözümdür. Veri transferi için farklı boyutlarda çerçeveler kullanılır. Ayrıca kendi içinde hata kontrol mekanizması da mevcuttur. FR veri iletiminde sürekli olarak kurulan sanal devre (PVC, Permanent Virtual Circuit) ve geçici kurulan sanal devre (SVC, Switched Virtual Circuit) olmak üzere iki tip devre kullanır. Bu devreler uç kullanıcıya düşük maliyetli adanmış bağlantı imkânları sağlar.

- Eş zamansız Aktarım Modu (ATM, Asynchronous Transfer Mode): ATM, ses, video ve veri sinyallerini dijital iletim ortamından ileten PVC tabanlı bir anahtarlama teknolojisidir. 155 Mbps ve 10 Gbps arasındaki bant genişliklerini destekler. Veriyi 53 byte uzunluğundaki hücre formunda karşı tarafa iletir. ATM'de sabit hızda veri aktarımı (CBR, Constant Bit Rate), uygun veri aktarımı (ABR, Available Bit Rate) değişken veri aktarımı (VBR, Variable Bit Rate) ve belirsiz veri aktarımı (UBR, Unspesified Bit Rate) olmak üzere 4 çeşit servis vardır. CBR, kullanıcıya bant genişliğini garanti eder, ABR trafiğe bağımlı olarak bant genişliğini belli zamanlarda garanti eder, VBR video konferans uygulamalarında kullanılır. UBR servisinde bant genişliği garanti edilmez [11].

2.2. Sanal Özel Ağ Kullanım Alanları

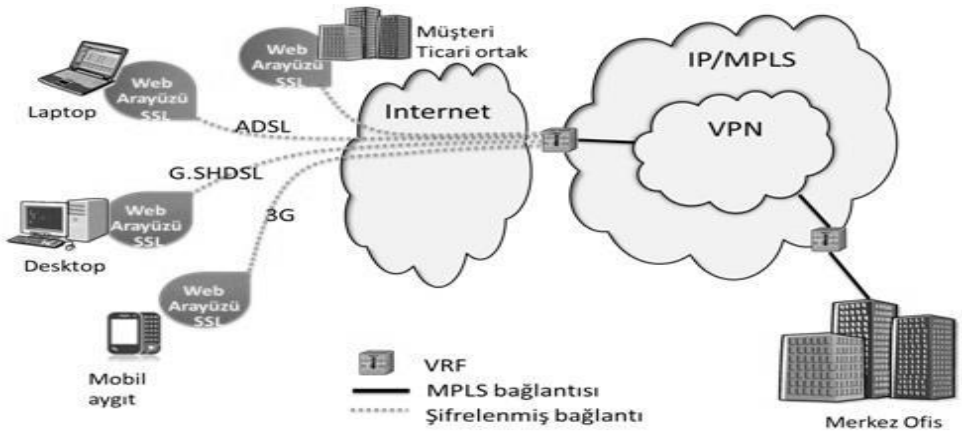
2.2.1. Sanal Özel Ağ (Uzaktan Erişimli)

Mobil kullanıcılar, küçük ofisleri, ev uzak ofisleri merkeze uzaktan erişimli sanal özel ağ ile güvenli bir şekilde bağlanabilirler. Uzaktan erişimli sanal özel ağ istenilen zamanda ağ kaynaklarına uzaktan mobil olarak erişim imkânı sağlar. Birçok firma mobil olarak çalışan personeli veya şirketin uzaktaki bir ofisinden, bu şirketin intranetine istenilen an erişim yetkisine sahiptir. Kullanıcılar uzaktan erişim yapmak istedikleri zaman uzaktan erişim sunucusuna istek gönderirler ve bu sunucu kullanıcının kimlik doğrulamasını ve yetkilendirilmesini gerçekleştirir. Bu sanal özel ağ tipinde intranete çevirmeli bağlantı ile erişilir.



Şekil 2.1. Sanal özel ağ olmadığı durumda tipik bir uzaktan erişim yapısı

Sanal özel ağ ile uzaktaki kullanıcılar internet servis sağlayıcı veya internet servis sağlayıcının (bulunma noktası) POP noktasına çevirmeli yerel bağlantı yaparak internet üzerinden karşı ağa bağlanırlar. Bu bağlantının yapısı Şekil 2.1.'de görülmektedir.



Şekil 2.2. Sanal özel ağ (Uzaktan Erişimli Yapısı)

Sanal özel ağ ile erişimin diğer erişimlere göre avantajları aşağıda belirtilmektedir:

- Uzaktan erişim sunucusuna ihtiyaç olmaz ve uzaktan erişim sunucusunun modem havuzunu da kullanmaya gerek kalmaz.

- Uzun mesafe çevirmeli bağlantılar yapılmaz. Bu işlemin yerine yerel çevirmeli bağlantılar yapılır.

- Uzak mesafe kullanıcıları için ekonomik bir çevirmeli yerel bağlantı servisi sağlar.

- Lokal ağa eş zamanlı erişmek isteyen kullanıcılar olursa, bu kullanıcıların sayısı ne kadar artsa da sanal özel ağ bağlantılarda problem olmaz.

- Çevirmeli bağlantılar yerel olduğu için, modemlerin uzak mesafe erişimlerde de performansı iyidir.

Sanal özel ağ bu kadar avantajlı olmasına rağmen, olumsuz yönleri de vardır. Dezavantajları aşağıda belirtilmiştir:

- Veri kaybı ve paketlerin iletimi esnasında bu verilerin yapısının bozulma ihtimali vardır.

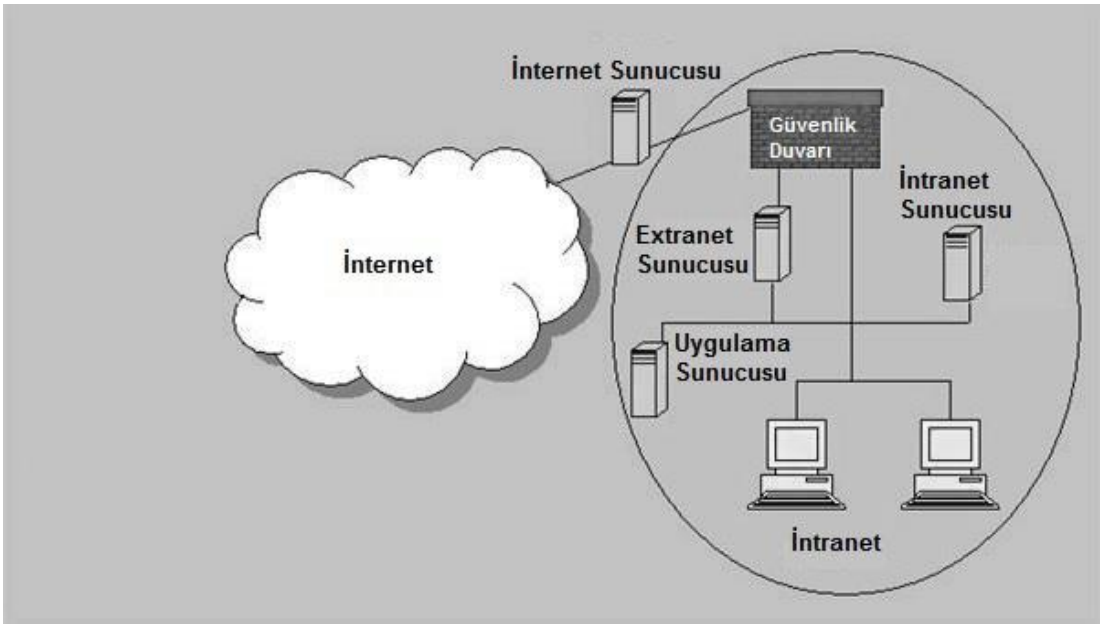
- Gelişmiş şifreleme algoritmalarından dolayı, protokol yoğunluğu söz konusu olduğundan bir yük meydana gelmektedir. Bu durum kimlik doğrulama sürecinde gecikmelere yol açmaktadır.

Ayrıca sanal özel ağdaki IP ve noktadan noktaya protokol tabanlı veri sıkıştırması uzun bir sürede gerçekleşmektedir.

- İletim ortamı olarak interneti kullandığı için, çoklu medya içerikli veriler uzaktan erişimli sanal özel ağ tüneller içinden iletilirken, iletimde gecikmeler söz konusu olabilmektedir [11].

2.2.2. Sanal Özel Ağ (Intranet)

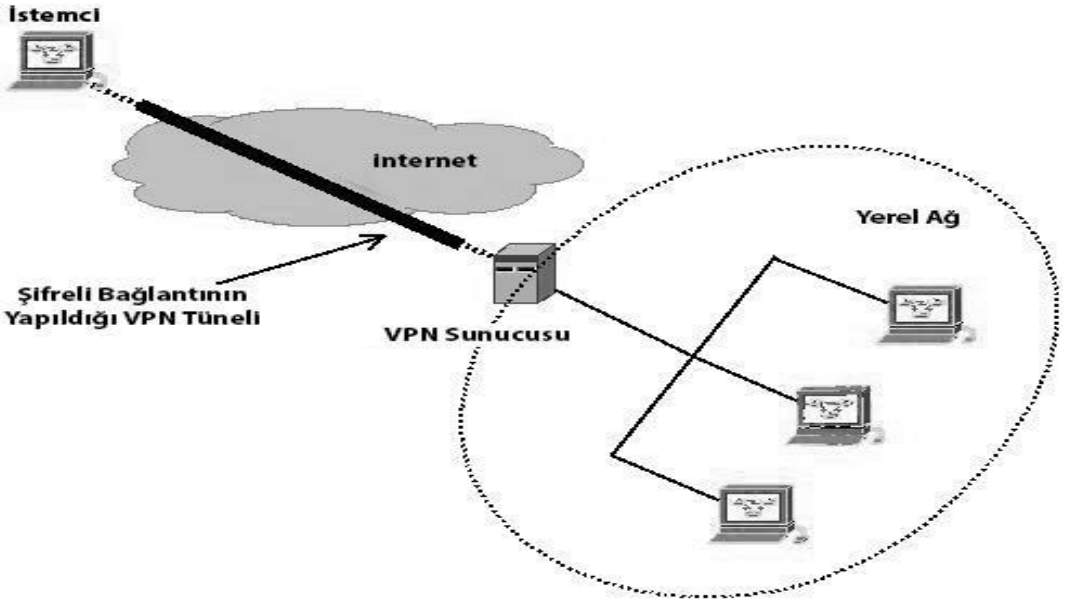
Intranet sanal özel ağ, bir organizasyonun uzaktaki ofislerinin, organizasyonun ortak intranetine erişip işlem yapabilmesi için kullanılır. Sanal özel ağ olmadan intranet bağlantılarında her bir kullanıcı merkezdeki yönlendiriciye erişmek durumundadır. Intranet sanal özel ağ ile merkez ofis, bölge veya şubelerin dâhil olduğu ağlar güvenli bir şekilde birbirine bağlanabilmektedir.



Şekil 2.3. Sanal özel ağ olmayan geniş alan ağ

Şekil 2.3.'te görülen bağlantı yapısının donanım maliyeti yüksektir. Çünkü organizasyonun intranetine uzaktan bağlantı için en az dört yönlendiriciye ihtiyaç vardır. Ayrıca tüm lokasyonlardan akan trafiğin intranet omurgasında tanımlanmasının ve yönetimini de maliyeti yüksek ve çözümü karmaşık olmaktadır. Intranet ne kadar geniş olursa maliyet o kadar çok artmaktadır.

Sanal özel ağ çözümleri ile intranetler için pahalı WAN omurga bağlantıları, düşük maliyetli internet bağlantısı ile ortadan kalkmıştır.



Şekil 2.4. Sanal özel ağ ile intranet bağlantısı

Sanal özel ağ çözümlü intranet bağlantılarının sağladığı avantajlar aşağıda belirtilmiştir:

- Özel bir WAN omurgasına ihtiyacı olmayıp, interneti kullandığı için donanım maliyeti düşüktür.

- Çok fazla donanıma ihtiyaç duymadığı için bu konuda destek sağlayan personel sayısı da az olacaktır, yani daha az işgücü gerektirecektir. Bu durum da daha az maliyet demektir.

- İletim ortamı olarak interneti kullandığı için uçtan uca bağlantılarda yeni bir uç bağlantı eklenmesi kolaylaşmaktadır.

- Sanal özel ağ tünellemede anahtarlama işlemi hızlı olduğundan sanal özel ağ bağlantılarda yedek alma özelliği vardır.

- İnternet servis sağlayıcıya yerel çevirmeli ağ bağlantı yapıldığı için erişim hızı yüksektir.

İntranet sanal özel ağ çözümlerindeki dezavantajlar aşağıda belirtilmiştir:

- İletim esnasında paket kaybı ihtimali söz konusudur.

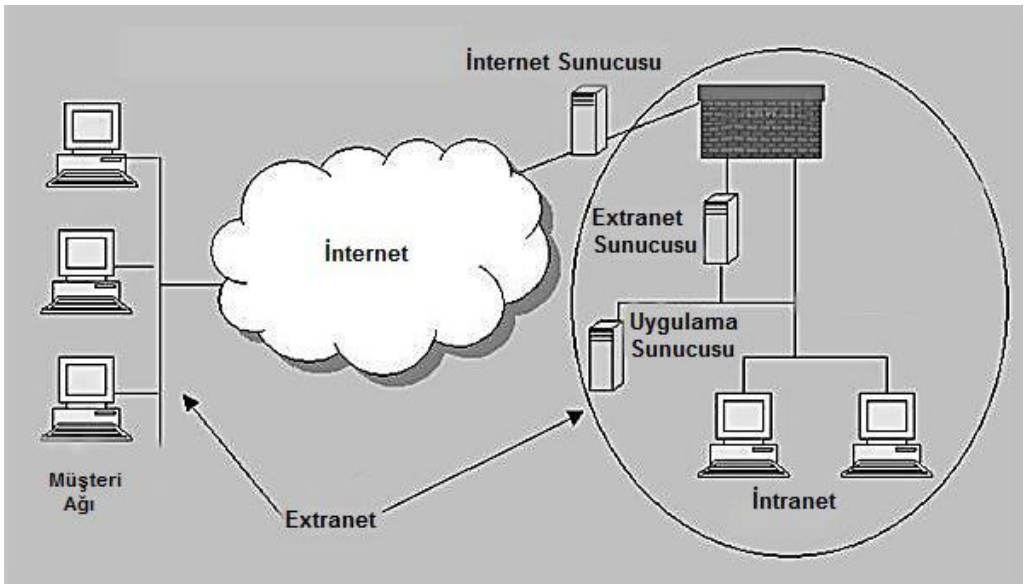
- Veriler ortak bir ağ içindeki tünellerden iletildiği için bazı internet atakları söz konusu olabilmektedir.

- Çoklu ortam içerikli verilerin iletiminde gecikmeler olabilmektedir

- İnternet ortamından dolayı zaman zaman performans düşüklüğü olabilir ve bu anlarda servis kalitesi (QOS) garanti edilemez [11].

2.2.3. Sanal Özel Ağ (Extranet)

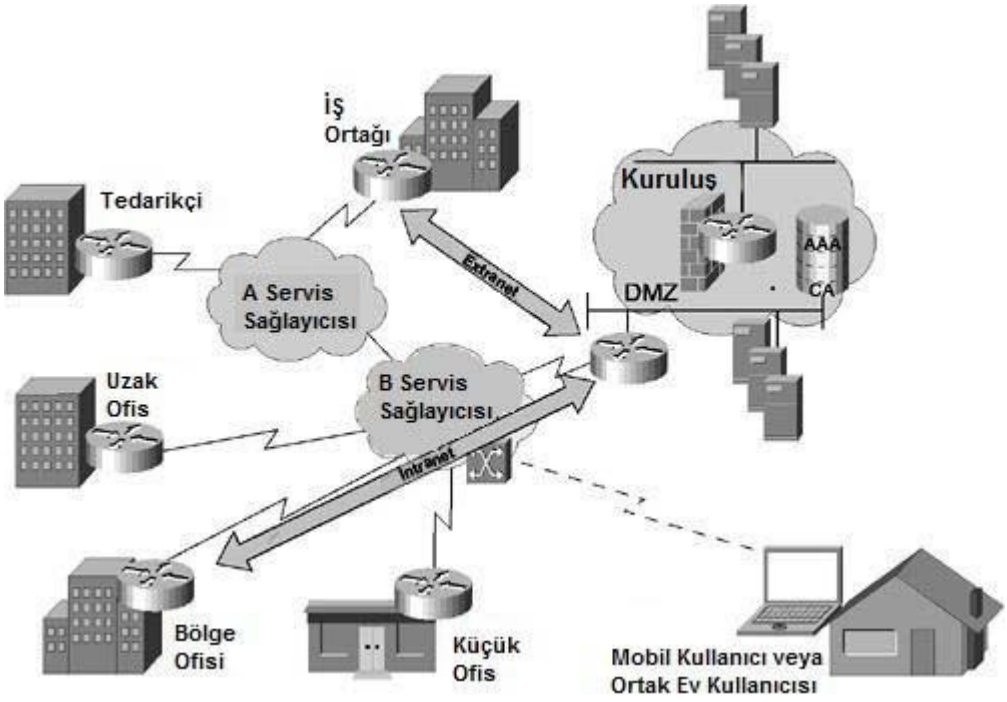
Extranet sanal özel ağ çözümlerinden bir diğeridir. Firma yakın ilişkilerde bulunduğu bayi, çözüm ortağı, üretici ya da müşteri ile extranet sanal özel ağ kullanarak tüm bu firmaların paylaşılmış bir ortamda çalışmalarını sağlar. Burada istenilen firmaya istenilen erişim yetkisi tanımlanabilmektedir.



Şekil 2.5. Sanal özel ağ kullanılmayan extranet yapısı

Şekil 2.5.'de görüldüğü gibi intranette yer alan her bir ağın bağlı bulunduğu ağa göre yapılandırılması gerektiğinden bu yapı pahalı, karmaşık ve yönetimi zor bir yapıdır. Bu yapıyı yönetecek olan personel sayısı da fazla olacaktır dolayısıyla ekstradan bir işgücü gerektirecektir. Bu durumda extranet artı maliyet demektir.

Ayrıca bu yapıyı genişletmek de kolay değildir. Bu güçlüklerden dolayı bir ağ üzerinden bir intranete bağlanılırken problemler yaşanabilir. Extranet sanal özel ağ çözümü, yukarıda bahsedilen problemlerin yaşanmaması için extranet ağlarda ideal bir çözümdür. Şekil 2.6.'da extranet sanal özel ağ yapısı görülmektedir.



Şekil 2.6. Extranet sanal özel ağ yapısı

Extranet sanal özel ağı'nın sağladığı avantajlar aşağıda belirtilmiştir:

- Sanal özel ağ'sız extranet bağlantılara göre maliyeti çok düşüktür.

- Yönetimi, tanımlaması ve tanımlamada değişiklik yapılması kolaydır.

- İletim ortamı internet olduğundan sanal özel ağ çözümünde organizasyonun ihtiyacına göre çözüm sağlayabilecek birçok servis sağlayıcı seçeneği vardır.

- İnternet üzerinden bağlantı servis sağlayıcı (service provider) tarafından sağlandığı için ilave bir işgücü gerektirmez dolayısıyla operasyon maliyeti de çok düşüktür.

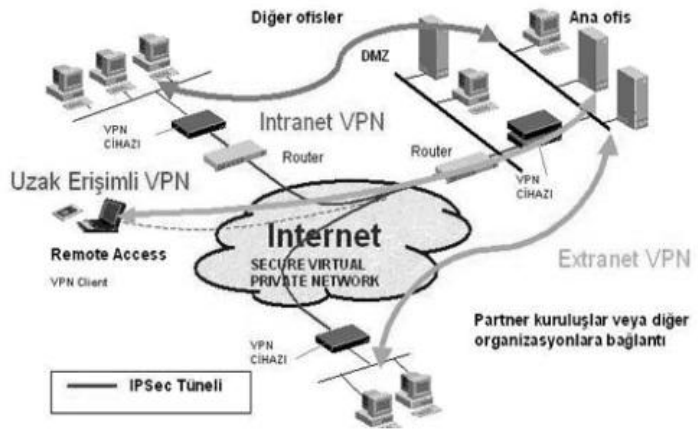
Extranet sanal özel ağın olumsuz yönleri de aşağıda belirtilmiştir:

- Dağıtık hizmet engelleme gibi güvenlik tehditleri söz konusu olabilmektedir.

- İntranete bilinmeyen kaynaklardan erişilme riski vardır.

- İnternet ortamından dolayı, çoklu ortam içerikli verilerin iletiminde zaman zaman gecikmeler meydana gelebilir.

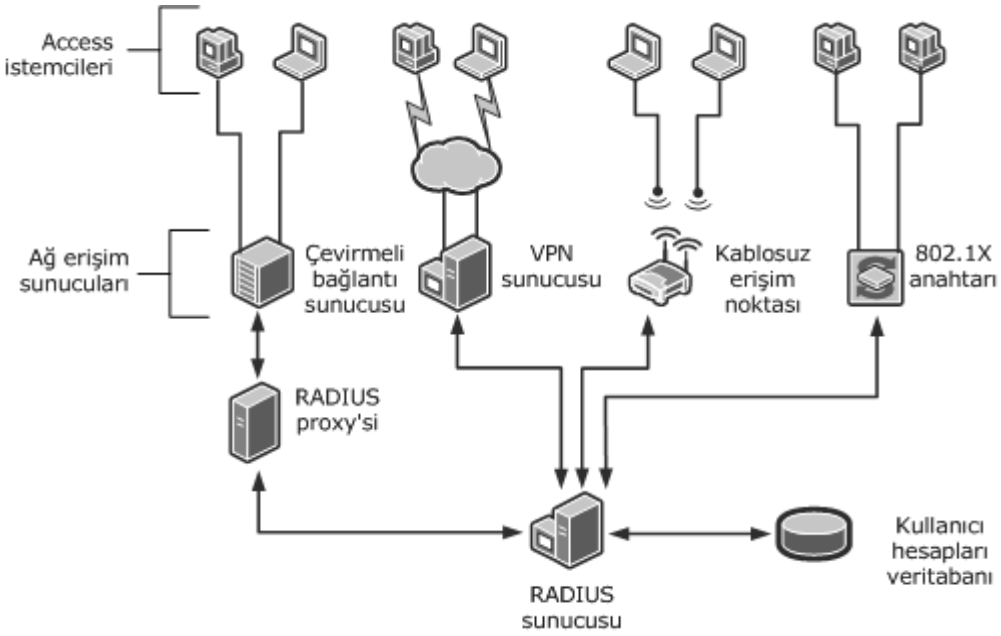
- İnternet ortamından dolayı performans değişkendir, zaman zaman servis kalitesi (Quality of Servis) garanti edilemeyebilir. Bazı dezavantajları olmasına rağmen sanal özel ağ tabanlı çözümün sağladığı avantajlar, dezavantajlarının önüne geçmektedir. Şekil 2.7.'de sanal özel ağ tipleri görülmektedir [11].



Şekil 2.7. Sanal özel ağ bağlantı tipleri

2.3. Sanal Özel Ağ Bileşenleri

Aşağıda bir sanal özel ağ çözümünün şekli görülmektedir:



Şekil 2.8. Sanal özel ağ çözümünde kullanılan bileşenler

- Sanal özel ağ donanım: Sanal özel ağ sunucular, istemci makineler, sanal özel ağ yönlendiriciler, ağ geçitleri ve sanal özel ağ yoğunlaştırıcılardan oluşur.

- Sanal özel ağ yazılımı: Sunucu ve istemci yazılımı ile sanal özel ağ yönetim araçlarından oluşur.

- Organizasyon tarafındaki güvenlik: Arayan kullanıcının uzaktan kimliğini doğrulama (RADIUS), terminal giriş kontrol ünitesi, kontrol sistemi (TACACS), ağ adres dönüştürme (NAT) ve doğrulama, yetkilendirme, aktivite izlenmesi (AAA) güvenlik servisleri bu gruptadır.

- Servis sağlayıcı tarafındaki sanal özel ağ bileşenleri: Servis sağlayıcının ağ erişimi için kullandığı anahtarlama omurgası ve internet omurgası bu gruptadır.

- Açık ağ: İnternet, PSTN ve POTS bu gruptadır.

- Tüneller: PPTP tabanlı, L2TP tabanlı ve IPSEC tabanlı tüneller bu gruptadır.

2.3.1. Sanal Özel Ağ Donanım Bileşenleri

Sanal Özel Ağ Sunucuları: Sanal özel ağ sunucular uzak bağlantı servislerini sağlar. Genel fonksiyonları aşağıdaki gibidir:

- İstemcilerden gelen sanal özel ağ bağlantı isteklerini dinler.

- Şifreleme ve kimlik doğrulama gibi bağlantı için gerekli olan işlemleri gerçekleştirir.

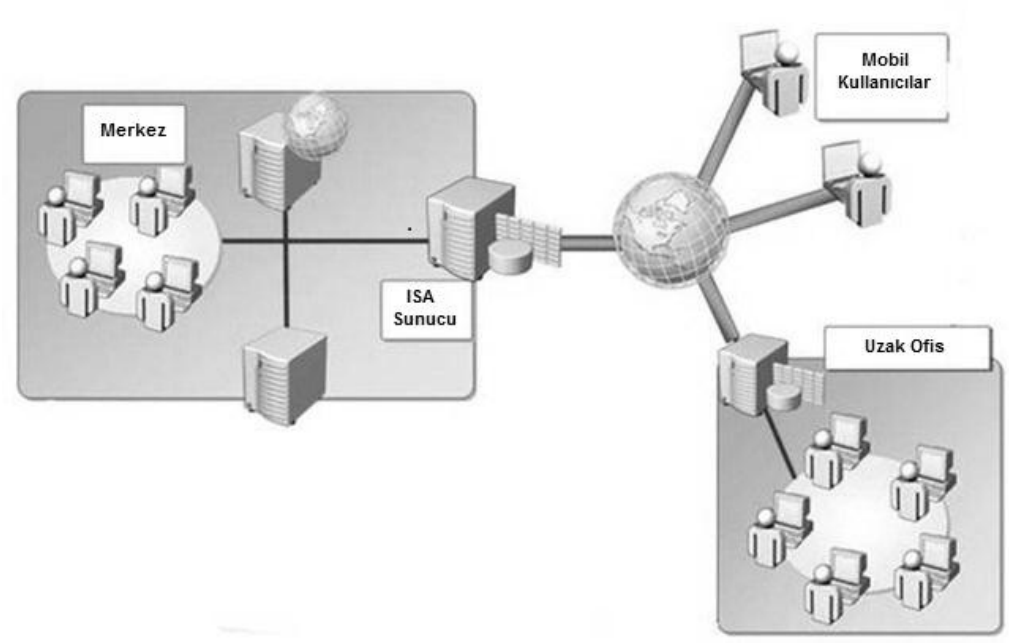
- Sanal özel ağ istemcilerinin kimlik doğrulamasını ve yetkilendirmesini gerçekleştirir.

- İstemciden iletilen verileri kabul eder, istemci tarafından beklenen verileri iletir.

- Sanal özel ağ bağlantı ve tünelin son noktasıdır.

Sanal özel ağ sunucularda iki veya daha fazla sayıda ağ adaptör kartı kullanılmalıdır. Bu kartlardan biri organizasyonunun intranetine bağlanılırken kullanılmakta olup diğer kart internet bağlantısını sağlar. Sanal özel ağ sunucular aynı zamanda sanal özel ağ ağ geçidi veya yönlendirici görevi de yapar. Ağ geçidi veya yönlendirici görevi olan bir sanal özel ağ sunucu, istemci sayısının az olduğu durumlarda kullanılır (Maximum 20). Sanal özel ağ sunucuların sadece sanal özel ağ isteklerine cevap vermesi amacıyla kullanılması tavsiye edilen bir durumdur [11].

Sanal Özel Ağ İstemcileri: Özel sanal ağ istemciler kimlik doğrulaması yapıldıktan sonra sanal özel ağ sunucuda sanal özel ağ bağlantıyı başlatarak uzaktaki bir ağa bağlanan uzak veya lokal makinelerdir. Sanal özel ağ sunucu ve istemci ancak başarılı bir oturum açma (log-in) işleminden sonra birbiriyle haberleşebilir. Genellikle istemci tarafında yazılım tabanlı bir istemci bileşeni kullanılır. Bununla birlikte istemci tarafında adanmış bir donanımda bulunabilir. Şekil 2.9.'da sanal özel ağ istemci profilleri gösterilmiştir:



Şekil 2.9. Sanal özel ağ istemci profilleri

- Evden organizasyonun kaynaklarına internet üzerinden erişebilen çalışanlar (Telecommuter),

- İnternet üzerinden organizasyonun intranet kaynaklarına erişebilen mobil çalışanlar,

- Yönetim, monitör, problem çözme, yapılandırma yapma amaçlı internet üzerinden intranete erişebilen ağ yöneticileri.

Sanal Özel Ağ Yönlendirici ve Yoğunlaştırıcılar: Küçük çaplı bir sanal özel ağ kurulumu durumunda sanal özel ağ sunucu yönlendirme görevi yapar. Fakat bu durum büyük ölçekli bir sanal özel ağ kurulumunda tavsiye edilmez. Büyük ölçekli sanal özel ağlarda yönlendirici görevi yapan ayrı bir donanıma ihtiyaç vardır. Genelde, ağ güvenlik duvarı arkasında olmadığı sürece yönlendirici o ağın son noktasıdır. Sanal özel ağ yönlendiriciler hedef ağa doğru yolları bulmakta olup en kısa yoldan istemcinin hedef ağa erişebilmesini sağlar.

Sanal özel ağ teknolojisinde ayrıca ek yönlendiricilerde yaygındır. Bu yönlendiriciler gerçekte bir yönlendirici değildir, normal bir yönlendiricinin LAN veya WAN ara yüzüne tanımlanır ve bu yönlendiriciye tünelleme veya Ipsec şifreleme ve kimlik doğrulama fonksiyonlarını ekler. Böylece bir organizasyon ek bir yönlendiriciye ihtiyaç duymadan, önceden mevcut olan yönlendiricisine ek özellikler kurarak donanım maliyetini azaltmış olur.

Sanal özel ağ yoğunlaştırıcılar uzaktan erişimli sanal özel ağ bağlantılarında kullanılır. Bu cihazlar yüksek performans ve gelişmiş şifreleme ile kimlik doğrulama yeteneğine sahiptir. Cisco'nun 3000 ve 5000 serisi sanal özel ağ yoğunlaştırıcıları yaygın olarak kullanılan cihazlardır.

IP ağ geçitler farklı protokolleri IP protokolüne dönüştüren cihazlardır. Bu nedenle ağ geçidi cihazları özel bir ağın IP protokolünü de desteklemesini sağlar. Bu cihazlar hem donanım hem de yazılım tabanlı olabilir. Donanım tabanlı bir ağ geçidi, genelde intranet tarafında kullanılır, yazılım tabanlı ağ geçitlerinin kurulumu herhangi bir sunucu üzerine yapılabilir ve bu ağ geçidi farklı protokollerin IP protokollerine dönüştürülmesi için kullanılır. Novell firmasının "Border Manager" IP ağ geçidi ürünü yaygın olarak kullanılan bir yazılım tabanlı ağ geçididir.

2.3.2. Sanal Özel Ağ Yazılım Bileşenleri

Özel sanal ağ yazılımları üç kategoride sınıflandırılabilir:

1. Sanal özel ağ sunucu yazılımı: Sanal özel ağ sunucularda, Windows Server 2003 ailesi üyesi, Windows XP, Windows 2000, Windows NT 4.0, Windows 95, Windows 98 veya Windows Millennium Edition, Windows Server 2003 Datacenter Edition; Windows Server 2003 Enterprise Edition; Windows Server 2003 Web Edition ve Windows Server 2003 Standard Edition, Novell-NetWare, ve Linux işletim sistemleri kullanılabilir.

2. Sanal özel ağ istemci yazılımı: Bir ağ içinde sanal özel ağ sunucuya istekte bulunan herhangi bir makine sanal özel ağ istemci olarak nitelendirilir.

3. Sanal özel ağ yönetim araçları: Bu tip yazılımlar sanal özel ağ yönetimi, monitör edilmesi ve problemlerin çözülmesi için kullanılır. Bu amaçla kullanılan en yaygın yazılım Novell firmasının "Border Manager" ve Cisco firmasının "Secure Policy Manager" yazılımıdır. Windows 2000'de "RRAS snapin for MMC" yazılımı da bu amaçla kullanılabilir. Yazılım tabanlı sanal özel ağ çözümlerinin maliyeti daha düşük ve yapılandırmaları daha kolaydır. Fakat ilk kurulumları ve yönetimi zordur. Donanım tabanlı sanal özel ağ çözümlerinin maliyeti yüksek fakat kurulumu ve yönetimi daha kolay olup, performansı daha iyidir. Tek bir donanımda tüm özel sanal ağ bileşenleri mevcuttur [12].

2.4. Sanal Özel Ağlarda Güvenlik

Sanal özel ağ teknolojisindeki güvenlik çözümleri aşağıda listelenmiştir:

- Güvenlik duvarı (Firewall)

- Ağ adres dönüştürme (NAT)

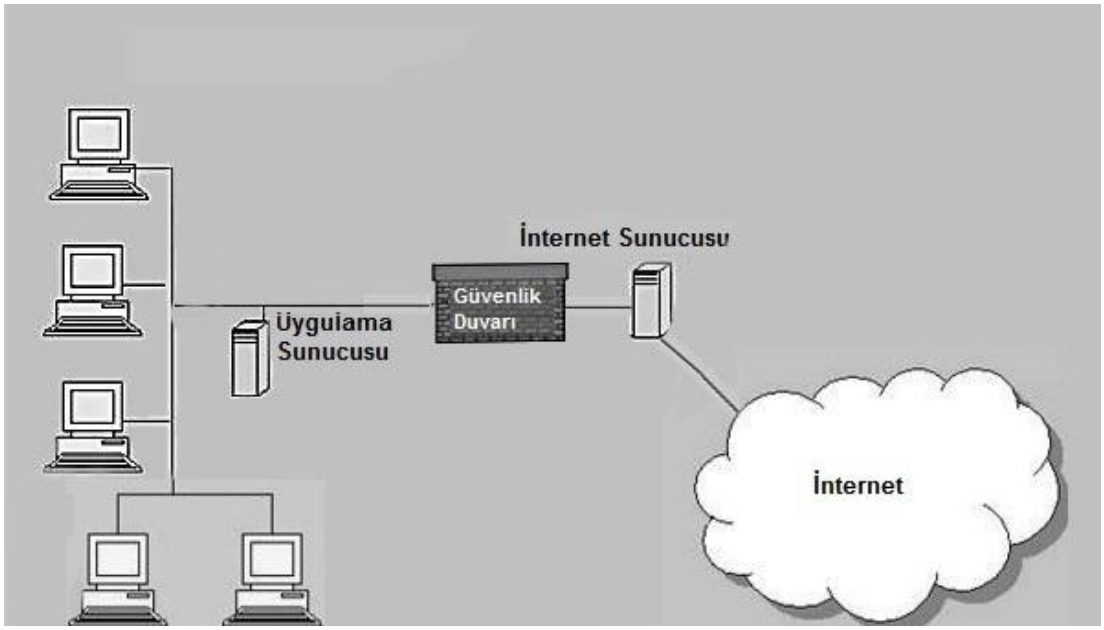
- Kimlik doğrulama sunucuları ve veri tabanları

- Doğrulama, Yetkilendirme, Aktivite izleme mimarisi

- İnternet güvenlik protokolü

2.4.1. Güvenlik Duvarı

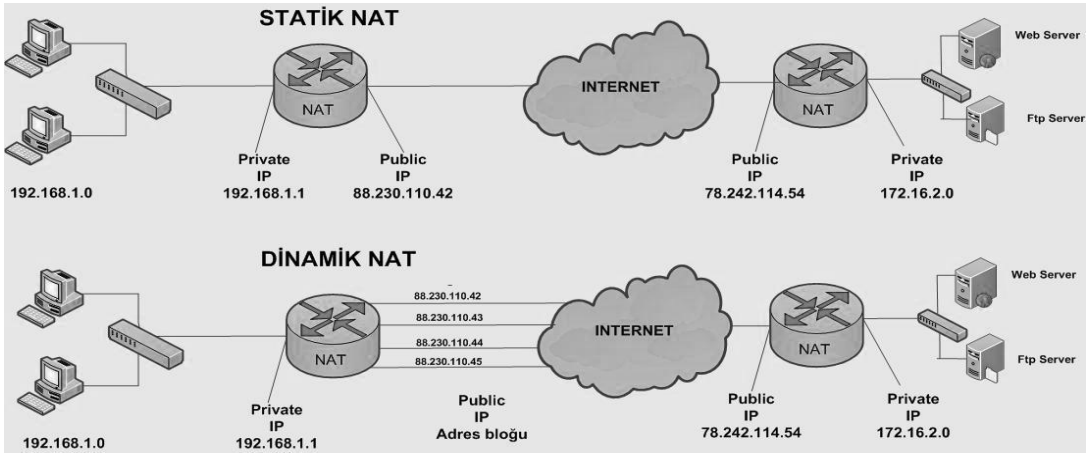
Güvenlik duvarı intranetteki kaynaklara, yetkilendirilmemiş kişilerin erişimini engelleyen bir set rolü oynar. IP adresleri, portların dinlenmesi, paket tipleri, uygulama tipleri ve veri içeriğine göre engelleme yapan güvenlik duvarları mevcuttur. Şekil 2.10.'da intranet içinde yer alan bir güvenlik duvarı görülmektedir [13].



Şekil 2.10. Intranet ve İnternet arasındaki güvenlik duvarı

2.4.2. Ağ Adresi Dönüştürme (NAT)

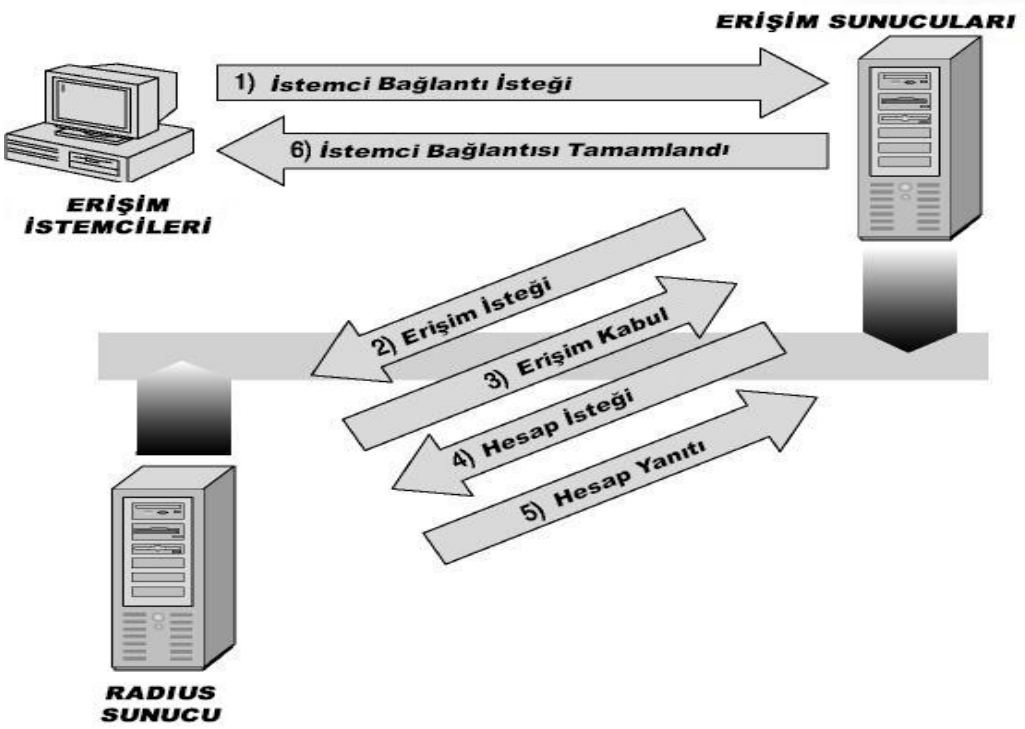
Ağ adres dönüştürme (NAT, Network Address Translation) tabanlı cihazlar, istemciye intranetin kaynaklarının lokalde sahip oldukları IP adreslerini açığa vurmadan intranet kaynaklarına güvenli erişimini sağlar. Temel güvenliği sağlamanın yanında IP adreslerinin de ekonomik olarak kullanılmasını sağlaması bir avantajdır [14].



Şekil 2.11. Ağ adresi dönüştürme yapısı

2.4.3. Kimlik Doğrulama

Arayan kullanıcının uzaktan kimliğini doğrulama hizmeti (RADIUS) ve terminal giriş kontrol ünitesi, kontrol sistemi (TACACS) kimlik doğrulama amaçlı kullanılan sunucu tipleridir. Bu donanımlar, intranet dışındaki bir istemcinin intranet kaynaklarına erişimini sağlamak için kimlik doğrulama ve yetkilendirme işlemlerini gerçekleştirir.



Şekil 2.12. Radius sunucu

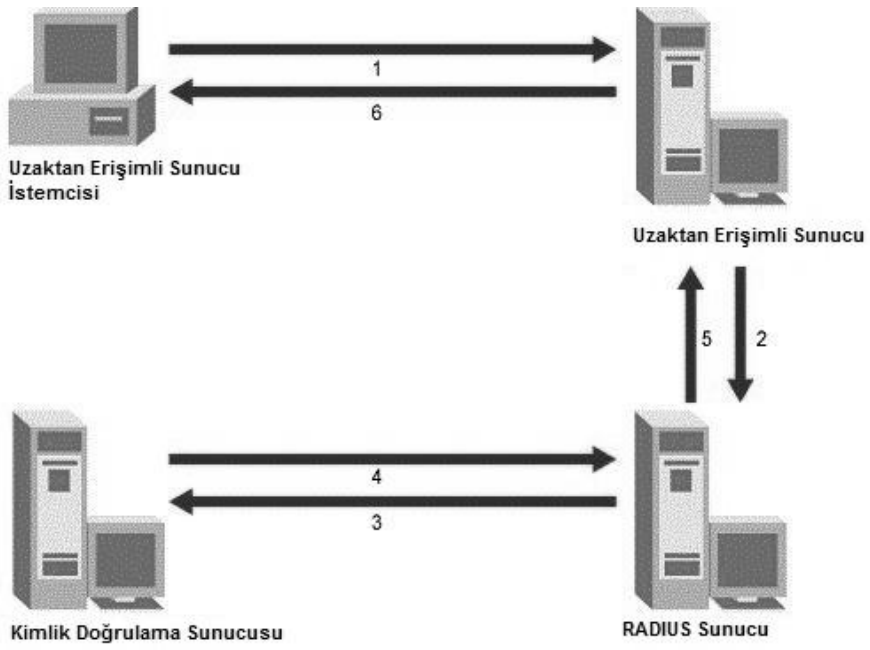
RADIUS uzaktan erişimli kullanıcılar ile var olan bilgisayar ağı arasında kullanıcı ID ve parola bilgilerinin güvenli olarak değiş tokuşunu sağlamakla görevlidir. RADIUS açık bir protokol standardıdır ve uzaktan erişimli kullanıcıların merkezi olarak uzaktan erişimini sağlar. RADIUS sunucu, uzak erişim sunucu (RAS) aygıtları ile birlikte çalışır. Bu birliktelikte RAS bir istemci ve RADIUS sunucu bir AAA sunucudur.

RADIUS, Lusent Technologies tarafından geliştirilmiştir ve 3COM, Assend, CISCO gibi ağ teknolojisi sağlayan firmalar tarafından kullanılmıştır. Pek çok uzak erişim aygıtı RADIUS ile birlikte çalışacak şekilde tasarlanmıştır.

RADIUS istemci/sunucu modeli, karşılıklı el sıkışma kimlik doğrulama protokolü (CHAP)'ne benzer yapıda girişim,yanıt protokolünün kullanımını destekler. RADIUS'un kullanılma gereksinimi derhal ortaya çıkan bir görünüm çizmemiştir. Bunun da nedeni; RAS güvenli bir kullanıcı kimlik ve parola değiş tokuşunu sağlayan özelliğe (CHAP gibi) sahip bulunmaktaydı. RAS yalnız başına, çok az

kullanıcı bilgisayar ağına ulaşma ve ağ içinde güvenli noktalara bağlanma isteğinde bulunuyorsa yeterli olabilir.

Buna karşılık pek çok kullanıcı uzaktan erişim gereksinimi gösteriyorsa ve bunların pek çoğu da kişilik belirleme mekanizmasının çalışmasını gerektiriyorsa, RADIUS bu gereksinimleri çok basit bir uygulama ile çözer; kişilik belirleme geçit kapısı olarak düşünülebilir ve kapı stratejik olarak uzaktan erişim kullanıcısı ile bilgisayar ağı arasına yerleştirilir. RADIUS'un devreye giriş aşamasında ID ve parolaya sahip kullanıcıların yeniden veya ek olarak parola almalarına gerek yoktur. Zira RADIUS, direkt olarak bilgisayar ağına veya ağa uzak erişimli olarak bağlanma aşamasında parolanın kullanılmasına olanak sağlar. Bu durum özellikle parolaları düzeltmekten sorumlu ağ yöneticisi için büyük bir destektir. Bu sunucular bir kimlik doğrulama isteği aldıklarında, istemcinin lokaldeki veri tabanında kayıtlı olup olmadığına bakar ve kayıtlı ise istemcinin intranete erişimine izin verir, istemci kayıtlı değilse merkezdeki veri tabanına bakılır. İstemcinin kimlik doğrulaması yapıldıktan sonra RADIUS sunucu internet servis sağlayıcı tarafındaki ağ erişim sunucusu (NAS, Network Access Server) ile haberleşir, sanal özel ağ bağlantısı kurulur veya reddedilir [15].



Şekil 2.13. RAS sunucu

2.4.4. Doğrulama Yetkilendirme Aktivite İzlenmesi (AAA)

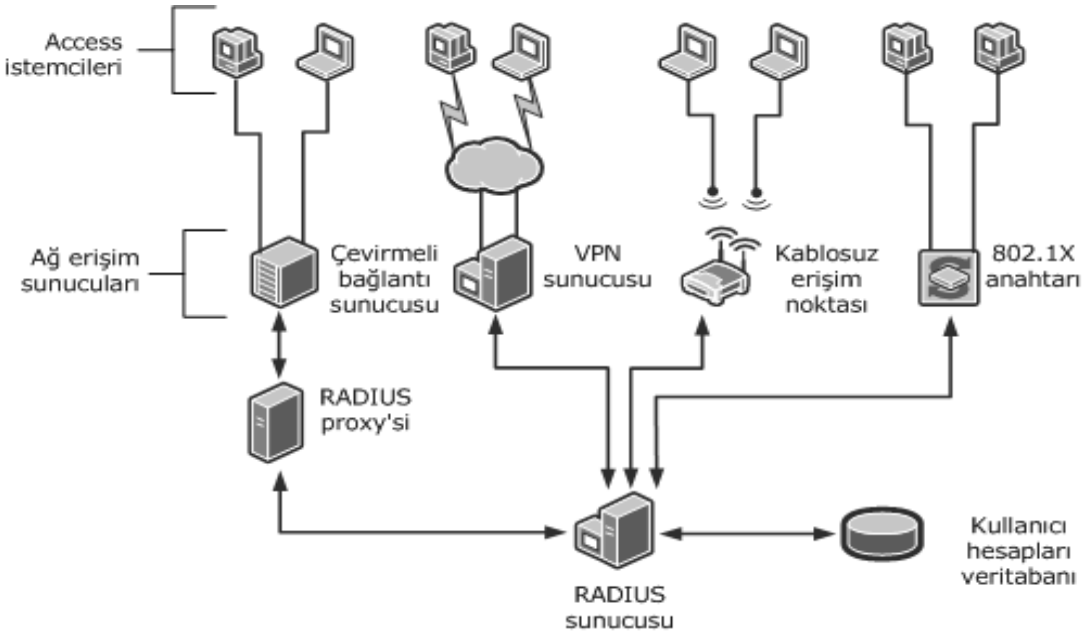
Doğrulama, yetkilendirme, aktivite izlenmesi (AAA, Authentication Authorization Accounting) lokal kaynaklara erişim için kullanılan bir diğer kimlik doğrulama ve yetkilendirme mekanizmasıdır. Arayan kullanıcının uzaktan kimliğini doğrulama hizmeti (RADIUS), terminal giriş kontrol ünitesi, kontrol sistemi (TACACS) sunucular ile birlikte kullanılan bir tamamlayıcı yapıdır. AAA uzaktan erişim ile ilgili aşağıdaki sorgulamaları yapar:

- Ağa kim erişmek istiyor?

- İstemci ağa eriştiğinde hangi yetkilere sahip olacak?

- Kullanıcı ağ içinde hangi işlemleri yapmış ve bu işlemleri ne zaman gerçekleştirmiş?

Ağ erişim sunucusu internet servis sağlayıcı tarafında bulunduğu durumda, uzaktan bağlantı isteğini alır, bu isteği organizasyon tarafında bulunan AAA sunucuya iletir. Bu sunucu istemcinin kimlik doğrulamasını gerçekleştirir veya reddeder, kimlik doğrulanmışsa istemcinin ağda hangi yetkilere sahip olduğunu belirler. Eğer istemci ağda yetkisi dâhilinde olmayan bir işlem yapmak isterse bu istek reddedilir ve istemciye uyarı mesajı verilir.



Şekil 2.14. Sanal özel ağ doğrulama, yetkilendirme, aktivite izlenme yapısı

AAA; kimlik doğrulama, yetkilendirme ve muhasebe işlemlerinin birleşimidir. Aşağıda bu işlemler anlatılmaktadır. Şimdi uygulamayı adım adım izleyelim:

Adım–1: Kullanıcı RAS ‘a bağlantı kurar

Adım–2: AAA, RAS ile ilişki kurar

Adım–3: AAA, RAS ‘a yanıt verir

Adım–4: Hedef kaynağa ulaşım onaylanır.

Doğrulama: Kimlik doğrulama, uzaktan erişim söz konusu olduğunda en önemli fonksiyondur. Güçlü bir kişilik belirleme olmaksızın ağa erişimin kontrol altına alınması olanaksızdır ve bunun sonucu olarak kurumsal bilgilerin yetkilendirilmemiş kişilerin eline geçmesi çok kolay olacaktır. En yaygın kullanılan kimlik doğrulama yöntemi tek uygulamalı parola (OTP, One Time Password) dır. Kimlik doğrulama kullanıcı ağın RAS veya yönlendiricisine ulaştığında çalışmaya başlar. Bazı durumda kullanıcı aynı anda bir diğer kısıtlı alana ulaşmak ister, bu durumda ek bir kişilik

belirleme uygulaması gerekmektedir. Sanal özel ağ'da kişilik belirlemede kullanılan en etkin yöntem iki faktörlü kişilik belirlemedir. Bu yöntemde kimlik/parola kontrolüne ek olarak kişiyi belirlemek için ikinci bir eleman devreye alınır. Bu uygulama ATM işlemlerine benzetilebilir. Birinci kontrol makinaya okuttuğunuz kart üzerinden yapılır. İkinci kontrol için kişisel kimlik numarası kontrolü devreye girer.

Yetkilendirme: Kimlik doğrulama ile yetkilendirmenin sınırı her zaman kesin çizgilerle belli değildir. Yetkilendirme genellikle kimlik doğrulama işlemini izleyerek uygulanır, ancak kimlik doğrulama gerekli değilse birinci uygulama olarak devreye girer. Örneğin, web sayfasında herkesin kullanımına açık bilgiler gibi verilere ulaşma durumunda yani kimlik doğrulamaya gereksinim duyulmayan durumlarda ve kullanılan ağ servisi gerekli desteği sağladığı durumlarda yetkilendirme işlemi yeterli olacaktır.

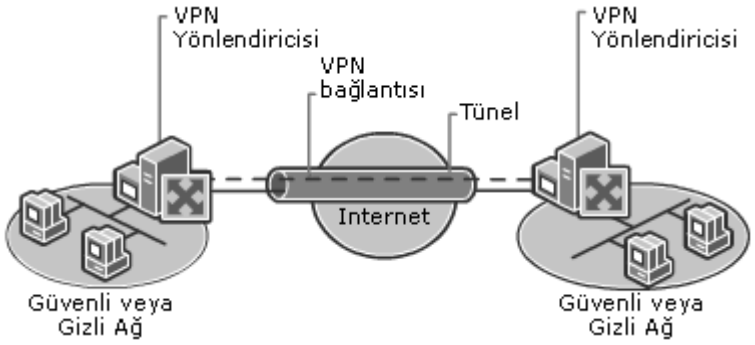
Aktivite İzlenmesi: İş hayatında muhasebe kurumun finansal kayıtlarını yürütmek ve denetlemek amacı ile kurulmuş olan teori ve sistemlerdir. Sanal özel ağ dünyasında iş hayatında olduğu gibi muhasebenin işlevi aynıdır. Sanal özel ağ istemcilere ait kayıtları ve sistemle ilgili hareketleri, faturalama ve güvenlikle ilgili raporların üretilmesi amacı ile tutulmaktadır. Muhasebe, kullanıcıların ağın hangi noktasından, ne sıklıkla ve ne kadar süre ile işlem yaptığını belirler. Muhasebe işlemi genellikle kimlik doğrulama ve yetkilendirme işleminden sonra gerçekleştirilir ancak bu iki işlemle herhangi bir bağı yoktur.

2.5. Sanal Özel Ağ Güvenliği

İnternet üzerinde veri iletiminin güvenli olmadığı birçok uygulama da görülmüştür. Sanal özel ağlarda kullanılan tünelleme tekniği internet ortamını daha güvenli bir hale getirebilmektedir.

2.5.1. Kimlik Doğrulama ve Erişim

Güvenlik açıklarını engellemek için en temel işlem kimlik doğrulama ve yetkilendirmedir. Şekil 2.15.'te bir sanal özel ağ senaryosunda kimlik doğrulama işlemi gösterilmektedir.



Şekil 2.15. Sanal özel ağ senaryosunda kimlik doğrulama

2.5.2. Erişim Kontrolü

Kullanıcıların ağ kaynaklarına erişimi aşağıdaki kontrollerle sağlanır:

- Giriş Kimliği (Login ID) ve Şifre (Password): Sanal özel ağ erişiminde kullanıcı tanımlanması için işletim sistemi tabanlı giriş kimliği ve şifre sorgulaması yapılır.

- S/Key şifresi: Kullanıcı şifreyi girdiğinde kullanıcıya S/KEY ve bir parametre atanır. Bu parametre, şifre için tanımlanan ileti özeti MD4 (güvenli hash fonksiyonu) sayısını belirtir ve sunucuda kaydedilir. İstemci sisteme giriş yapmayı denediğinde istemci tarafındaki yazılım şifreye hash fonksiyonunun n-l iterasyonunu uygulayıp sonucu sunucuya gönderir. Sunucu bu cevaba hash fonksiyonunu uygular. Eğer sonuç daha önceden sunucuya kaydedilen sonuç ile eşleşirse istemcinin kimlik doğrulaması başarılı bir şekilde gerçekleşmiş olur ve sunucu daha önceden kayıtlı olan parametreyi istemcinin cevabı ile değiştirir ve şifre sayıcı sistemin değerini bir azaltır.

- Arayan kullanıcının uzaktan kimliğini doğrulama (RADIUS, Remote Access Dial-In User Service): RADIUS, istemci/sunucu modeline dayanan bir internet güvenlik protokolüdür. Genelde RADIUS sunucu istemciyi kullanıcı adı ve şifre ile yetkilendirir. Veri güvenliği için istemci ve RADIUS sunucu arasındaki işlem, kimlik doğrulama mekanizması (PAP, CHAP) kullanılarak şifrelenebilir.

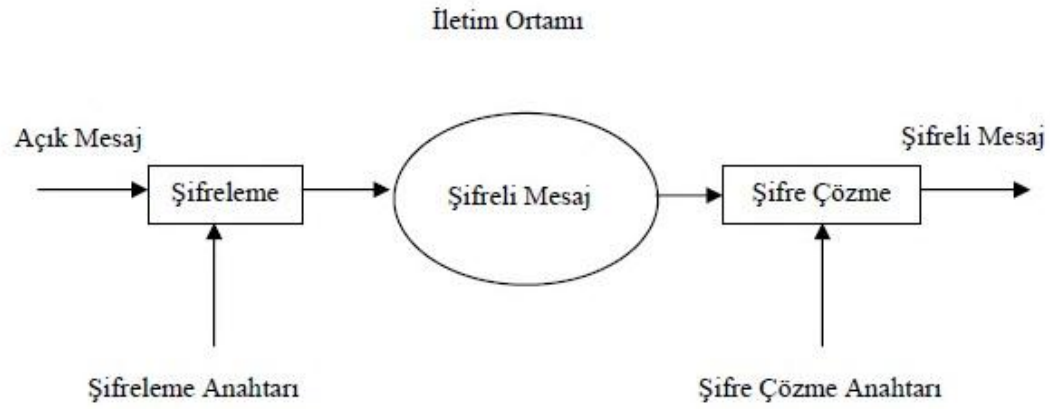
- İki faktörlü jeton tabanlı teknik: Kullanıcı bilgilerinin doğrulanması için iki tane kimlik doğrulama aşaması vardır. Kimlik sorgulanması esnasında cihazlar bir jeton ve şifre rolü oynar. Bu tekniği ATM cihazlarından para çekme işlemine benzetebiliriz. ATM kartımızla kimliğimizi sisteme tanıtır ve şifre sorgulamasında doğru şifreyi girersek ATM sisteminden başarı ile para çekebiliriz. Sadece bu iki faktör sağlandığı zaman sistemden kendi hesabımıza ulaşabiliriz.

Bir istemcinin kimlik doğrulaması başarıyla yapıldıktan sonra istemci ağ dâhilindeki tüm kaynaklara erişim yetkisi kazanmış olur, bu da güvenlik açısından bir tehdittir. Çünkü istemci bilinçli olarak ya da olmayarak sistemlerdeki verilerde değişiklik yapabilir. Bu güvenlik açığı da istemcilere limitli yetkiler verilerek kapatılabilir. Örneğin sadece yönetici olanlar sistemlerde yazma yetkisine sahip olup diğer istemciler sadece okuma yetkisiyle sistemlere erişebilirler.

Erişim kontrolü kullanıcının tanımlanması ile yapılır, bunun yanında kaynak ve hedef IP adresi ve port adresleri, tarih, servis, uygulama ve Tekdüzen Kaynak Bulucu (URL, Uniform Resorce Locator) gibi parametrelerle erişim kontrolleri de vardır.

2.5.3. Veri Şifrelenmesi

Veri şifreleme, veriyi anlaşılamayacak bir formata dönüştürme mekanizmasıdır. Böylece iletim esnasında veriler yetkisiz erişimlere karşı korunmuş olur. Veri şifrelenmesi ile iletim kayıplarının ve verinin değişikliğe uğramasının önüne geçilmiş olur. Şekil 2.16.'da şifreleme modeli görülmektedir:

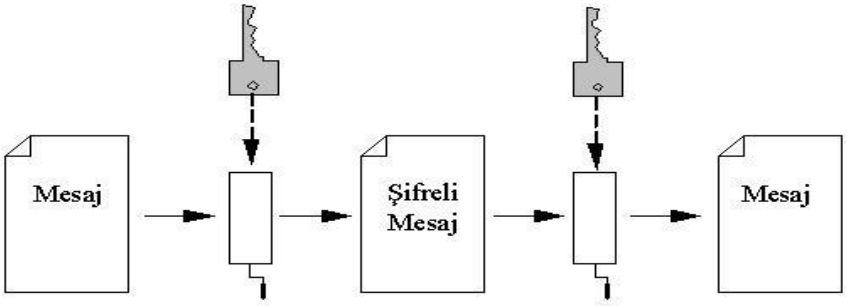


Şekil 2.16. Şifreleme mekanizması

Gönderen ve alan tarafta simetrik veya asimetrik şifreleme tekniği kullanılır. Şifreleme tekniği kullandıkları anahtarlara göre kategorize edilebilir. Bu anahtar, şifreleme ve çözümleme amaçlı kullanılır, bir sayı veya kelime formatında olabilir.

2.5.4. Simetrik Kripto Algoritmaları

Sabit uzunlukta bit dizisinden oluşan tek bir anahtar kullanılır. Bundan dolayı bu sisteme "tek anahtarlı şifreleme" de denir. Anahtar gizlidir ve şifreleme ile çözümleme işleminde görev alır. Her iki tarafta da veri iletilmeden önce, anahtar iki taraf arasında paylaşılır. Gönderen taraf bu özel anahtarı kullanarak orijinal veriyi şifreler ve karşı tarafa gönderir. Veri karşı tarafta şifreli formatta alındığında, aynı anahtar kullanılarak verinin şifresi çözümlenir. Şekil 2.17.'de simetrik şifreleme tekniği görülmektedir.



Şekil 2.17. Simetrik şifreleme tekniği

Anahtar değişim tekniklerinin tam anlamıyla güvenli olabilmesi için anahtarın mümkün olduğunca uzun bir formatta olması gerekmektedir. Daha uzun bir anahtarın şifrelenmesi, çözümlenmesi ve kırılması zorlaşır. Böylece yetkisiz istemciler anahtarı ele geçirdiklerinde kullanamazlar yani güvenlik sağlanmış olur. Anahtarın uzunluğuna bağlı olarak birçok simetrik şifreleme algoritması geliştirilmiştir. Aşağıda sanal özel ağ çözümlerinde yaygın olarak kullanılan simetrik şifreleme algoritmaları belirtilmiştir.

Gelişmiş Şifreleme Standardı (AES, Advanced Encryption Standard), elektronik verinin şifrelenmesi için sunulan bir standarttır. Amerikan hükümeti tarafından kabul edilen AES, uluslararası alanda da defacto şifreleme (kripto) standardı olarak kullanılmaktadır. Des'in (Data Encryption Standard, Veri şifreleme standardı) yerini almıştır. AES ile tanımlanan şifreleme algoritması, hem şifreleme hem de şifreli metini çözmede kullanılan anahtarların birbiriyle ilişkili olduğu, simetrik anahtarlı bir algoritmadır. AES için şifreleme ve şifre çözme anahtarları aynıdır.

AES, Amerikan Ulusal Standart ve Teknoloji Enstitüsü (NIST, National Institute of Standarts and Technology) tarafından 26 Kasım 2001 tarihinde US FIPS PUB 197 kodlu dokümanla duyurulmuştur. Standartlaştırma 5 yıl süren bir zaman zarfında tamamlanmıştır. Bu süreçte AES adayı olarak 15 tasarım sunulmuş, tasarımlar güvenlik ve performans açısından değerlendirildikten sonra en uygun tasarım standart şifreleme algoritması olarak seçilmiştir. Federal hükümetin ticaret müsteşarının onayının ardından 26 Mayıs 2002 tarihinde resmi olarak etkin hale

gelmiştir. Hâlihazırda birçok şifreleme paketinde yer alan algoritma Amerikan Ulusal Güvenlik Teşkilatı (NSA, National Security Agency) tarafından çok gizli bilginin şifrelenmesinde kullanımı onaylanan kamuya açık ilk şifreleme algoritmasıdır [16].

Veri şifreleme standardı (DES, Data Encryption Standard) tekniği 128 bit'e kadar anahtar uzunluğunu destekler. Fakat bu sayı algoritmanın daha hızlı olabilmesi için 56 bite düşürülmüştür. Bu sayının azaltılmasıyla bu teknik kaba kuvvet (Brute Force) ataklarına karşı açık hale gelmiştir. Bu tip ataklarda rastgele bir anahtar üretilir ve doğru anahtar belirlenene kadar orijinal veriye uygulanır. Anahtar ne kadar kısa olursa bu anahtarı tespit etmek ve şifreleme sistemini kırmak o kadar kolaylaşır [17].

Üç katlı veri şifreleme standardı (3DES, Triple Data Encryption Standard) 56 bit'lik anahtarlar kullanılır. DES tekniğine göre daha güvenlidir çünkü veriyi şifrelemek için 3 farklı anahtar kullanır. Birinci anahtar veriyi şifreler, ikinci anahtar bu şifreyi de şifreler, üçüncü anahtarda bu veriyi ikinci bir defa şifreler. Bu teknik DES tekniğine göre daha güvenli fakat üç kat daha yavaştır [18].

2.5.5. Asimetrik Kripto Sistemler

Asimetrik sistemlerde anahtar çiftleri kullanılır. Bu anahtarlardan biri sadece istemcinin bildiği özel bir anahtar, diğeri ise genel bir anahtardır. Açık anahtar şifreleme amaçlı kullanılır, özel anahtarlar ise şifreli mesajları çözümlemek için kullanılır. Asimetrik şifreleme sistemleri genelde açık anahtar şifreleme sistemler olarak bilinir. Sanal özel ağ çözümlerinde daha çok Diffie-Hellman (DH) ve Rivest Shamir Adleman (RSA) asimetrik şifreleme algoritmaları kullanılır.

Diffie-Hellman Algoritması: Her bir bağlantı, bir tanesi genel diğeri özel olmak üzere bir anahtar çifti alır. Aşağıda bu algoritmanın çalışma mantığı anlatılmıştır:

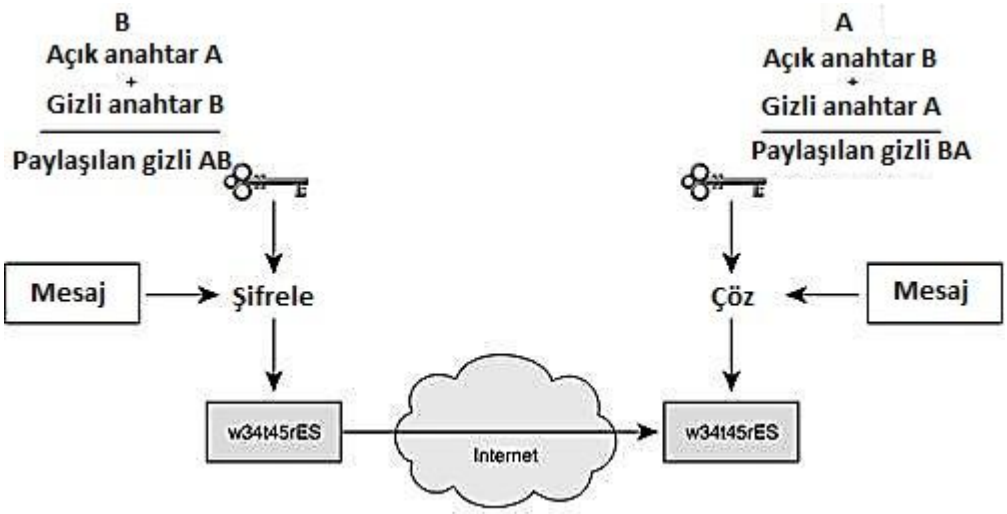
1. Gönderen taraf istemcinin tüm bağlantılarında kullanacağı açık anahtarını öğrenir.

2. Gönderen taraf özel anahtar ve istemcinin açık anahtarını birleştirerek bir hesaplama yapar ve bu hesabın sonucu ortak gizli bir anahtarda saklanır.

3. Mesaj bu ortak gizli şifre kullanılarak şifrelenir.

4. Şifrelenmiş mesaj istemciye gönderilir.

5. Şifreli mesaj alındığında, istemci kendi özel anahtarı ve gönderen tarafın açık anahtarı ile bir hesaplama yapar gizli anahtarı üretir. Bu algoritmanın temel mantığı, yetkisiz bir istemci şifreli mesajı ele geçirse bile özel anahtar saklı olduğu için orijinal bilgiye ulaşamayacak olmasıdır [19]. Şekil 2.18.'de bu algoritma gösterilmektedir:



Şekil 2.18. Diffie-Hellman algoritması

RSA (Rivest, Shamir, Adleman) Algoritması: Diğer teknikten farklı olarak istemcinin açık anahtarı kullanılarak şifreleme yapılır. İstemci gönderen tarafın açık anahtarını kullanarak orijinal mesajı elde eder [20].

Dijital imza kullanarak kimlik doğrulaması yapan RSA algoritmasının çalışma mantığı aşağıdaki gibidir:

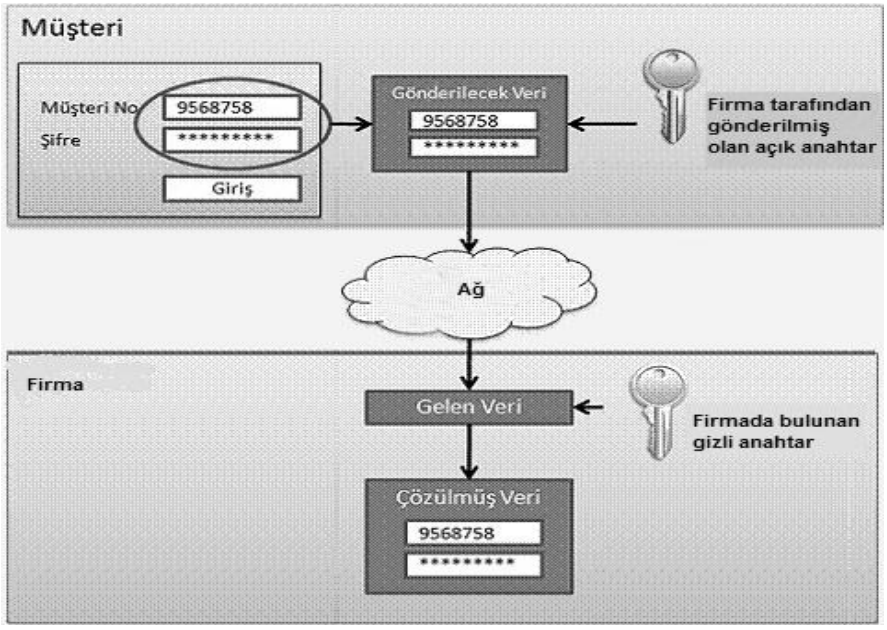
- İstemci taraf, bilgi gönderecek olan taraftan açık anahtarını öğrenir.

- Gönderen taraf orijinal mesajın boyutunu azaltmak için bir hash fonksiyonu kullanır. Elde edilen sonuç ileti özeti (MD, Message digest) olarak bilinir.

- Gönderen taraf özel anahtarla ileti özeti (MD, Message digest) mesajı şifreler ve dijital bir imza üretilmiş olur.

- Dijital imza ile mesaj istemci tarafına iletilir.

- Şifreli mesaj istemciye iletildiğinde, istemci MD (Message digest, İleti özeti) mesaja hash fonksiyonunu uygular. Daha sonra istemci, gönderen tarafın açık anahtarını kullanarak dijital imzayı çözümler. Bu iki sonucu karşılaştırır ve eşleşme sağlanırsa veri iletilmeye devam eder, sağlanmadığı durumda ise bağlantı sona erer. Şekil 2.19.'da RSA mantığı kullanan bir yapı gösterilmiştir.



Şekil 2.19. RSA algoritma mantığı

İstemci taraf verinin doğruluğunu üç aşamada kontrol ettiğinden RSA daha güvenli bir veri iletimi sağlar. Ayrıca bu teknikte anahtar yönetimi daha kolaydır.

2.5.6. Açık Anahtar Yapısı

Açık anahtar yapısı (PKI, Public Key Infrastructure) veri iletiminde güvenli bir bağlantı kurma ve anahtar yönetimi politikalarını belirler. Dağıtık sistemlerde açık anahtarlar ve X.509 dijital sertifikaların kullanımını sağlayan güvenlik hizmetleri kümesidir. Açık anahtar altyapısı kişilerin sahip olduğu açık ve özel anahtarları kullanarak oluşturulan bir bilgi altyapısıdır. Açık anahtar altyapısının temel görevi, internet/intranet üzerinde haberleşen, çalışan kişiler veya kurumlar arasında güvenilir dijital birimler oluşturmaktır.

Açık anahtarlı şifreleme sisteminde açık anahtar ve özel anahtar bulunmaktadır. Bu anahtarlar tek yönlü çalışmaktadırlar fakat birbirlerini tamamlarlar. Açık anahtar şifrelemek için, özel anahtar da açık anahtarın şifrelediğini deşifre etmek için kullanılır. Özel anahtar sadece ait olduğu kişide bulunmakta ancak açık anahtar çeşitli şekillerde insanlara iletilebilmektedir yani açık olarak dağıtılır. Bu altyapıda anahtarların oluşturulması, yetkili bir kurum tarafından onaylanması, sertifikaların saklanması ve dağıtılması, gerektiği durumlarda onayın geri alınması, sonlandırılması gibi işlemler vardır.

PKI tekniği organizasyon çapında, ülke çapında veya alan çapında kullanılabilir. PKI fonksiyonları aşağıda anlatılmaktadır:

- PKI istemciler için özel ve açık anahtar üretir.

- Dijital imzaları üretir ve bu imzaların doğrulanmasını sağlar.

- Yeni kullanıcıların kaydını ve kimlik doğrulamasını yapar.

- Her bir anahtarın geçmiş değerlerini kaydeder ve tutar.

- Geçersiz olan ve süresi dolan kullanıcıların sertifikalarını iptal eder.

Açık anahtar yapısı bileşenleri dört başlıktan oluşur:

- PKI istemci

- Sertifikasyon Makamı (CA, Certification Authority): CA, PKI istemcilerin dijital kimlikleri olan sertifikalarını sağlar, günümüzde yaygın olarak kullanılan CA Verisign'dır.

- Kayıt Makamı (RA, Registration Authority): CA'daki dijital sertifika istekleri yoğun sayıda olduğunda, CA bazı istekleri RA'ya yönlendirir. Bu durumda RA istekleri alır ve sertifikaları geçerli hale getirir. RA kullanıcıların sertifikalarını tanımladıktan sonra istekleri CA'ya gönderir ve CA kullanıcıların sertifikalarını RA'ya iletir. Bu durumda RA, PKI istemciler ve CA arasında görev yapar.

- Dijital sertifikalar: Sertifikalar temel olarak açık anahtar için bir taşıyıcı görevi görürler. Ancak açık anahtardan daha fazla belirleyici bilgiye sahip oldukları için çok daha işlevseldirler. Dijital sertifikalar, sahibinin anonim anahtarını, adını, son kullanma tarihini, dijital sertifikayı hazırlayan sertifika merciinin adını, seri numarasını e-posta adresini ve diğer bazı bilgileri içerir. Dijital sertifikalar kimlik kartların elektronik ortamdaki eşleniğidir. Aynı zamanda dijital kimlik, dijital pasaport, X.509 sertifikası ve açık anahtar sertifikası olarak da isimlendirilirler.

Dijital sertifika aşağıdaki bilgileri içerir:

- Sertifikanın seri numarası

- Sertifikanın süresi

- CA dijital imzası

- PKI istemcinin açık anahtarı

Gönderici taraf kendi kimliğini belirtmek için karşı tarafa şifreli mesajla birlikte dijital sertifikasını gönderir. İstemci taraf aldığı mesajın içinde mevcut olan göndericinin açık anahtarının geçerliliğini CA'nın açık anahtarını kullanarak tespit eder. İstemci taraf gönderici tarafın kimlik doğrulamasını yaptıktan sonra, istemci taraf mesajı çözümlemek için gönderen tarafın açık anahtarını kullanır.

- Sertifika Dağıtım Sistemi (CDS, The Certificate Distribution System): CDS açık anahtarların geçerliğini sağlar, anahtarları üretir, anahtarların kaydını tutar ve süresi dolmuş anahtarları iptal eder.

PKI istemci CA veya RA sisteminde tanımlı olan bir dijital sertifikaya sahip olur. PKI istemci CA veya RA'dan sertifika alır ve bu sertifikayı dijital bir kimlik olarak kullanır.

Açık anahtar yapısı tabanlı kimlik doğrulama:

1. Anahtar çiftinin tanımlanması: Gönderen taraf istemciye veri iletirken her iki taraf içinde bir özel ve birde açık anahtar tanımlanır. İlk önce özel anahtar tanımlandıktan sonra bu anahtara hash fonksiyonu uygulanarak açık anahtar üretilir. RSA tabanlı iletimlerde olduğu gibi PKI iletimlerde de özel anahtar mesaja eklenir, açık anahtar ise bu imzanın doğruluğunu tespit eder.

2. Dijital imza tanımlanması: Anahtar çifti tanımlandıktan sonra, dijital imza tanımlanır. Bu imza gönderen tarafın kimliğini tanımlar, dijital imza tanımlanması için orijinal mesaja hash fonksiyonu uygulanır. Bu işlemin sonucunda ileti özeti (MD) mesaj üretilmiş olur ve bu mesaj gönderen tarafın özel anahtarı ile şifrelenir ve bu şifreli mesaj dijital imza olarak isimlendirilir.

3. Mesaj şifreleme ve dijital imza uygulaması: Dijital imza türetildikten sonra orijinal mesaj gönderen tarafın açık anahtarı ile şifrelenir.

4. Şifrelenmiş mesaj ve gönderen tarafın açık anahtarı: Şifrelenmiş mesaj gönderen tarafın açık anahtarı ile birlikte istemciye iletilir. Açık anahtar istemciye gönderilmeden önce istemcinin açık anahtarı ile şifrelenir ve karşı tarafta bu şifrenin

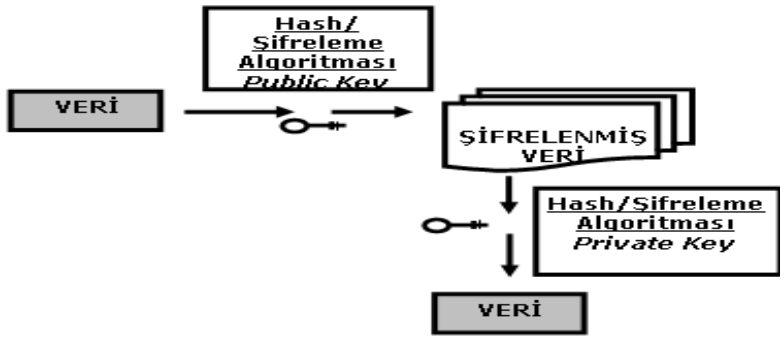
çözümlenebilmesi için istemci kendi özel anahtarını kullanır. Gönderen tarafın anahtarı aynı zamanda oturum anahtarı olarak da bilinir.

5. Gönderen tarafın kimlik doğrulaması: Şifrelenmiş mesaj ve açık anahtar iletildiğinde, istemci göndericinin kimlik doğrulamasını yapmak için CA parametresine bakar. Dijital imza başarı ile doğrulanırsa, istemci mesajı çözümler, kimlik doğrulaması yapılamazsa alınan mesaj reddedilir ve sanal özel ağ bağlantısı sonlandırılır.

6. Mesaj çözümlemesi: Gönderen tarafın kimlik doğrulaması yapıldıktan sonra istemci özel anahtarını kullanarak gönderen tarafın açık anahtarını elde eder ve ardından mesajı çözümler.

7. Mesaj içeriği doğrulaması: Son olarak istemci alınan mesajın içeriğine bakar, gönderen tarafın açık anahtarını kullanarak dijital imza çözümlenir ve ileti özeti (MD) mesajı elde edilir. Çözümlenmiş olan mesaja hash fonksiyonu uygulanır ve yeni bir MD mesaj türetilir. İletilen MD ve yeni türetilmiş olan MD karşılaştırılır [21].

Şekil 2.20.'de açık anahtar yapısı kullanılarak verinin şifrelenmesi ve şifrelenmiş verinin orijinal haline çevrilmesi gösterilmiştir.



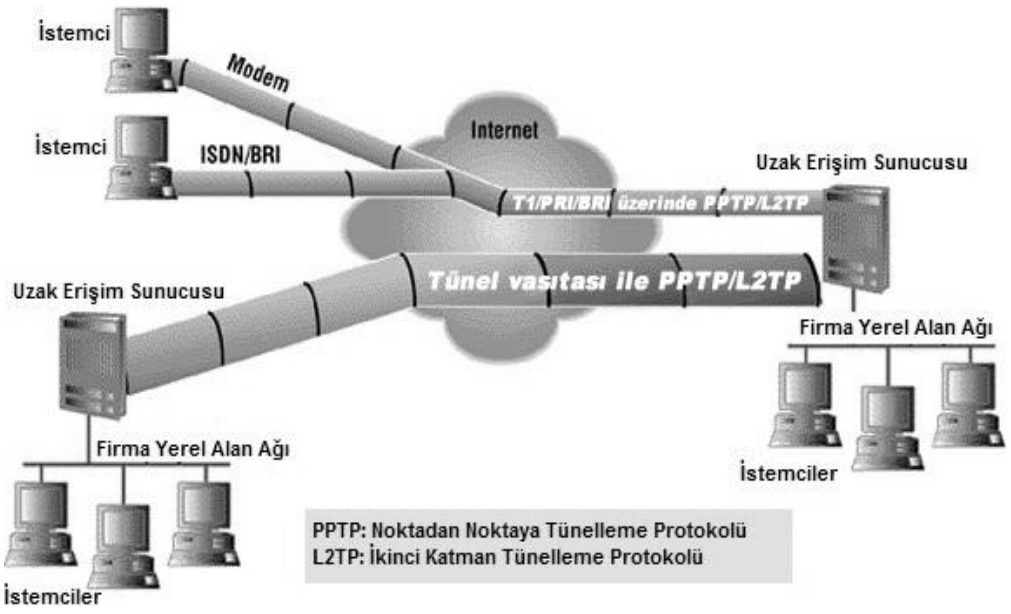
Şekil 2.20. Açık anahtar yapısı tabanlı iletim

2.6. Sanal Özel Ağlarda Tünelleme

Sanal özel ağlarda bir bağlantıyı yapabilmek bir port açıp bunun üzerinden bağlantıyı sağlamaya denir. Genellikle şifreleme ile yapılır yani özel bir ağ üzerinde akan veri ve genel ağdaki protokol bilgileri birlikte sarılır böylece genel ağda, özel ağımızdaki protokol bilgileri görünür olur.

2.6.1. Tünellemenin Fonksiyonu

Sanal özel ağlar da en önemli işlem tünelleme olarak değerlendirilmiştir. Tünelleme ile konu geçen ağa internet üzerinden kendi sanal ağını oluşturma imkânı bulur. İç ağ dışında izni olmayan kullanıcıların bu ağa girmesine izin verilmez.



Şekil 2.21. Sanal özel ağ tüneli

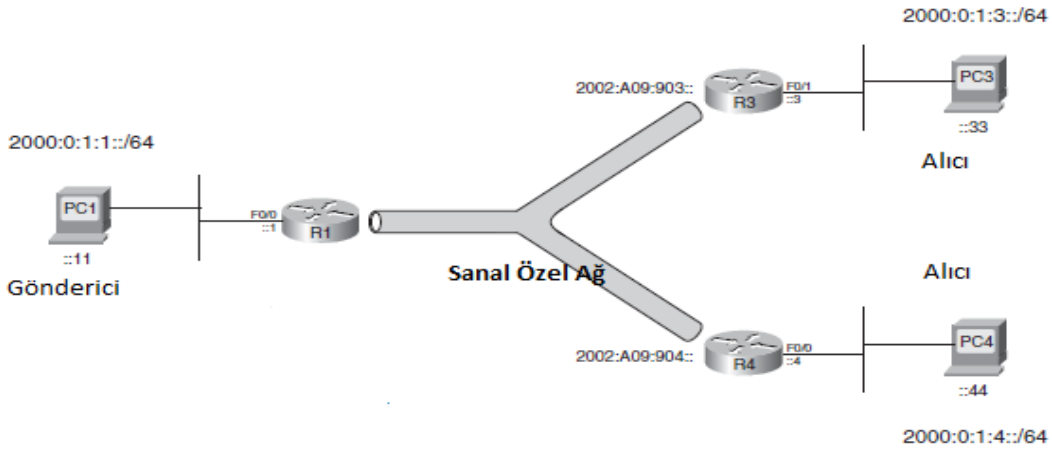
Tünelleme tekniğini mektup gönderme işlemine benzetilebilir. Şekil 2.21.'de görülen sanal özel ağ yoğunlaştırılarında mesaj şifrelenir, sonra gönderilmek üzere kapsüllenir. Bu kapsülleme sırasında, mesaj bir "zarf" içine yerleştirilir ve Ankara

sanal özel ağ yoğunlaştırıcısına doğru adreslenir. Ankara sanal özel ağ yoğunlaştırıcısı mesajı aldığında en dıştaki zarfı yok eder ve verinin şifresini çözer ve mesajı hedef sunucuya aktarır. Tünelleme tekniğinde de veri yükü mesajı mektuba benzetilebilir ve zarf da veri yükü mesajı sarmalayan protokoldür. Zarfın üzerindeki adres bilgisi de pakete eklenen yönlendirme bilgisidir. Tünellemede paket hedef ağa iletilmeden önce bu pakete tünelleme protokolünün başlık bilgisi eklenir. Yük olarak da isimlendirilen orijinal paket internetin desteklemediği bir protokolü kullanıyor olabilir, bu durumda tünelleme protokolü tünel içindeki pakete başlık bilgisini ekler. Bu başlık yönlendirme bilgilerini içerir ve paket artık internet üzerinden iletilebilecek hale gelir. Tünelleme protokolleri, tünelin en ucundaki kullanıcı için, oturum yönetimi olarak bilinen işlemleri gerçekleştirmek üzere, tünelleri kurar ve yönetir. Tünelleme protokolleri IP kadar diğer protokollerin kapsülleşmesi işini de yapar ve tünel aygıtları için yetkilendirme yöntemlerini gerçekleştirir. Bu protokoller genel olarak verileri şifreler ve tünel içine gönderir.

Sanal özel ağ tünelleri tarafından hedeflenen güvenlik seviyesinin gerçekleşmesi için, tüneller çok dikkatli oluşturulmalıdır. Tüneller iki grup altında toplanabilir. Bazıları sabit olarak kurulurken, bazıları ihtiyaç durumunda oluşturulabilir. C sınıfı IP adres alanı için en fazla 256 tünele izin verilmektedir. Tünel kurulduğunda, tünel aygıtları alışverişini başlatır.

Paket hedef noda yönlendirildiğinde, internet üzerinde mantıksal bir yoldan iletilir. Bu mantıksal yol tünel olarak isimlendirilir. Alıcı taraf tünellenmiş paketi aldığında tekrar paketi orijinal formatına dönüştürür.

Şekil 2.22.'de tünelleme işlemi görülmektedir:



Şekil 2.22. Tünelleme tekniği

2.6.2. Tünellemenin Avantajları

- IP adresi ekonomisi: Tünelleme, IP desteği olmayan paketlerin, IP adresi kullanan paketlere eklenerek internet üzerinden iletilmesini sağlayabilir. Böylece ağ dâhilindeki her bir noda IP adresi atanmasına gerek kalmaz, küçük bir IP bloğu ile sanal özel ağı kurulabilir.

- Güvenlik: Bir tünel yetkisiz kişilerin erişimine kapalıdır, bundan dolayı tünel içinden iletilen veri, her ne kadar internet gibi güvensiz bir ortamdan iletilse de güvendedir.

- Düşük maliyet: Tünelleme iletim ortamı olarak interneti kullandığı için özel ağlar ya da kiralık devrelere kıyasla düşük maliyetli bir çözümdür.

- Protokolden bağımsızdır: temel ağ girdi/çıktı sistemi (NetBIOS) ve Netbios kullanıcı arayüzü (NetBEUI, Netbios Extended User Interface) gibi yönlendirme özelliği olmayan protokoller TCP/IP ile uyumlu değildir. Bu nedenle bu tip paketler internet üzerinde yönlendirilemezler. Fakat tünelleme ile IP olmayan paketlerde internet üzerinden iletilebilir.

- Kolay tanımlanması: Tünelleme yapılandırması diğer yapılandırmalara göre daha kolaydır.

2.6.3. Tünelleme Tekniğinin Bileşenleri

Temel olarak 4 adet bileşenle bir tünel kurabiliriz:

1. Hedef ağ: İstemcinin erişmek istediği kaynakları bulunduran ağdır.

2. İstemci nod: Sanal özel ağ bağlantısını başlatan istemci veya sunucudur. Lokal ağın bir parçası veya mobil bir çalışan olabilir.

3. Ev temsilcisi (HA, Home Agent): Sanal özel ağ isteklerini alır ve bu isteklerin kimlik doğrulamasını gerçekleştirir. Kullanıcıyı yetkilendirdikten sonra tünel kurulmasına izin verir.

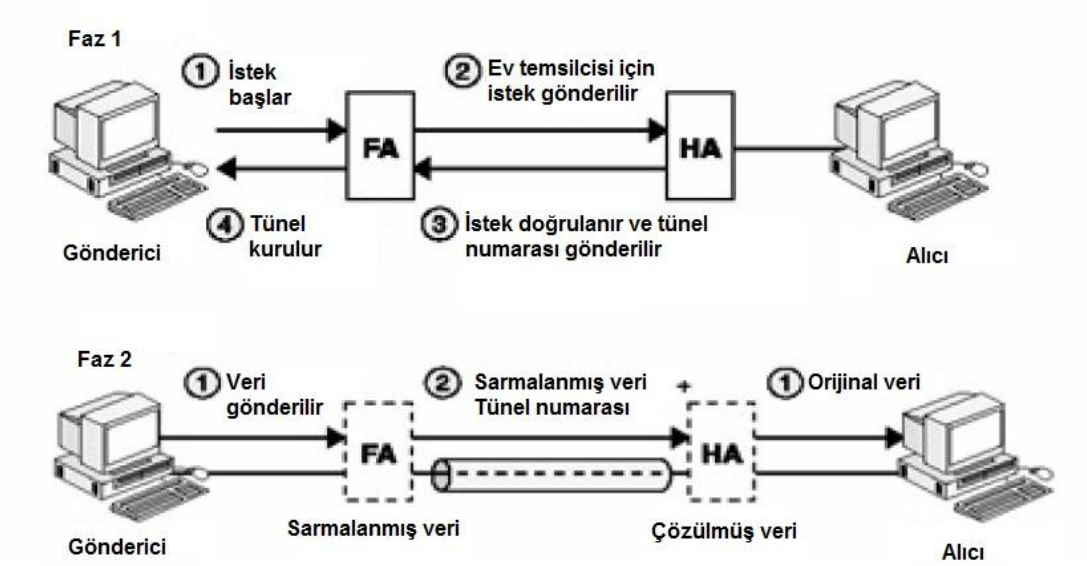
4. Yabancı temsilcisi (FA, Foreign Agent): Hedef ağ tarafındadır, HA sisteminden sanal özel ağ isteklerini alır. Tünel tekniğini iki fazda anlatabiliriz:

Faz1: İstemci sanal özel ağ isteğini gönderir ve HA sistemi bu istemcinin kimlik sorgulamasını yapar.

Faz2: Tünel içinden veri transferi başlatılır.

Faz1 de bir istek başlatılır, bu istek kabul edildiğinde iki uç arasında tünel kurulur ve FA sistemine bağlantı isteği gönderilir. FA (genelde RADIUS sunucudur) istemciyi kullanıcı adı ve şifresi ile doğrular. Eğer kullanıcının kullanıcı adı ve şifresi yanlış ise sanal özel ağ isteği reddedilir. Kimlik doğrulaması yapılabilirse bu sanal özel ağ isteği hedef ağdaki HA sistemine iletilir. İstek HA tarafından alındığında, FA sistemi HA sistemine şifrelenmiş giriş kimliği ve şifrelenmiş kullanıcı şifresini gönderir. HA bu mesajların doğrulamasını yapar ve FA sistemine bir tünel numarası gönderir ve FA mesajı aldığında bir tünel kurulmuş olur.

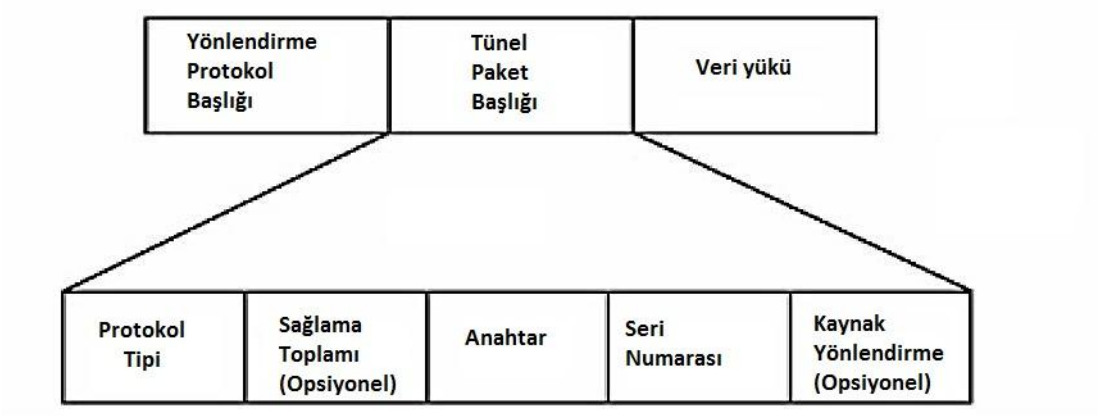
Tünelin kurulmasından sonra veri iletim aşaması olan faz2'ye geçilir. Faz2'de veri paketleri FA sistemine iletilmeye başlanır. FA bir tünel başlığı türeterek her bir veri paketine bu başlığı ekler. FA tünel numarasını kullanarak şifrelenmiş verileri HA sistemine gönderir. HA bu verileri aldığında, paketi orijinal formatına dönüştürür. Orijinal veri ağdaki hedef noda gönderilir. Şekil 2.23.'te tünelleme işleminin 1. ve 2. faz görülmektedir:



Şekil 2.23. Tüneller içinden iki fazda veri iletimi

2.6.4. Tünellenen Paket Formatı

Daha önceden de bahsedildiği gibi paket hedef ağa iletilmeden önce orijinal paket FA tarafından şifrelenir. Bu formattaki paket tünellenmiş paket olarak isimlendirilir. Şekil 2.24.'te tünelleme işlemi geçirmiş bir paket görülmektedir:



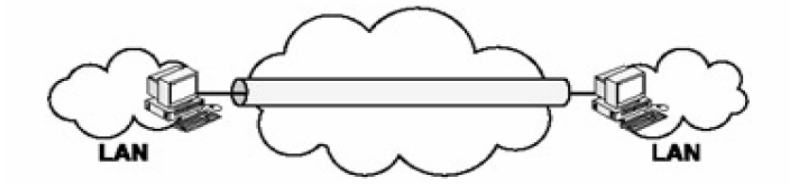
Şekil 2.24. Tünellenmiş paketin yapısı

Yönlendirilebilir protokol başlık bilgisi: Hedef HA ve kaynak FA sistemlerin IP adres bilgisini içeren başlıktır. Tünel paket başlığı aşağıdaki alanları içerir:

- Protokol Tipi: Veri yükü (Pay-load) protokol tipidir.
- Anahtar: İstemcinin tanımlamasını ve kimlik doğrulamasını gerçekleştirir.
- Seri Numarası: İletilen paketlerin seri numarasıdır.
- Kaynak Yönlendirme: İlave yönlendirme bilgisi içerir, seçmeli bir alandır.
- Veri yükü (Pay-load): İstemci tarafından FA sistemine gönderilen orijinal pakettir.

2.6.5. Tünel Tipleri

İstemci tarafından başlatılan tüneller: Uçtan uca tünel olarak bilinir. İstemcinin bağlantı isteği üzerine oluşturulur. İstemci nod tünelin son noktasıdır. Bundan dolayı, her bir uç için farklı tüneller oluşturulur ve iki uç arasındaki iletişim sona erdiğinde tünelde sonlandırılır.



Şekil 2.25. İsteğe bağlı olarak oluşturulan tünel yapısı

Sunucu tarafından başlatılan tüneller: İstemci tarafındaki istekle oluşturulan tünelden farklı olarak, bu tüneller ağa bağlı depolama (NAS, Network Attached Storage) veya çevirmeli sunucular tarafından oluşturulur. Uzaktaki istemci ilk olarak bu sistemlerle bağlantı kurar (bu sistemler genelde internet servis sağlayıcı tarafında bulunur) ve tünel oluşturulur.

Şekil 2.26. Sunucular tarafından oluşturulan tüneller

İstemci tarafından oluşturulan tünel sunucu tarafından oluşturulan tünel istemci tünelin son noktasıdır. NAS veya dial-up sunucular tünelin son noktasıdır. Her bir bağlantı için farklı tüneller kurulur. Çoklu bağlantılar aynı tüneli kullanırlar. Veri iletimi daha hızlıdır. Aynı anda birden fazla bağlantı durumunda bağlantılar aynı tüneli paylaştığı için veri iletimi daha yavaştır. Tünellerin süresi kısadır. Tünellerin süresi diğer tekniğe göre daha uzundur.

2.7. Tünelleme Protokolleri

Tünelleme protokollerini üç şekilde sınıflandırabiliriz:

1. Taşıyıcı protokoller: Tünellenmiş paketlerin internet üzerinden iletimini sağlamak için bu paketleri yönlendirir. Tünellenmiş paketler bu protokolün paketleri içine sarmalanır.

2. Sarmalama protokolleri: Veri yükü (Pay-load) paketin sarmalanmasını sağlar. Bu protokol ile tünel kurulur ve sonlandırılır. Günümüzde en yaygın olan sarmalama protokolleri PPTP, L2TP, ve IPSEC'tir.

3. İletim protokolleri: Tünel içinden iletilmesi amacıyla sarmalanması gereken orijinal veriler için bu protokol devreye girer. En yaygın olan iletim protokolleri PPP ve seri hat internet protokolü (SLIP, Serial Line Internet Protocol) protokolleridir.

Şekil 2.27. Tünelleme protokolünü kullanan tünellenmiş paketler

2.7.1. Noktadan Noktaya Protokol (PPP)

Noktadan noktaya protokol (Point to Point Protocol): Seri ve uçtan uca bağlantılarda kullanılan sarmalama protokolüdür. PPP, EIA/TIA-232-C ve ITU-T V.35 'e sahip olan herhangi bir veri bağlantı ekipmanları (DTE, Data Terminal Equipment) veya veri iletişim ekipmanları (DCE, Data Communications Equipment) sistemde kullanılabilir. IP ve IP olmayan verilerin sarmalanması ve iletilmesi aşağıdaki gibi gerçekleştirilir.

- IP olmayan datagramlara IP adreslerinin atanması,

- Kurulan bağlantının konfigürasyonu ve test edilmesi,

- Datagramların senkron ve asenkron sarmalanması,

- İletim esnasında hata algılama.

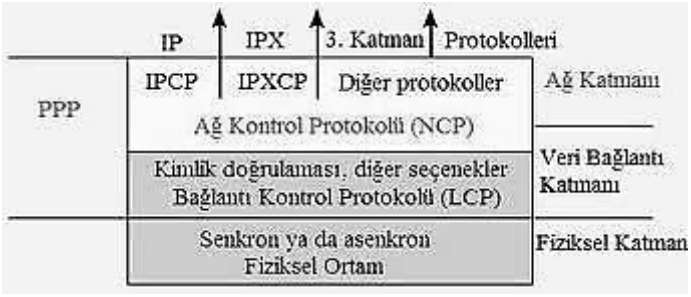
Noktadan noktaya protokol yukarda bahsedilen işlemleri gerçekleştirmek için üç standart kullanır.

1. Uçtan uca bağlantılarda veri paketlerini sarmalamak için kullandığı standart. Genelde bu standart yüksek seviyeli veri bağlantı kontrol protokolü (HDLC, High Level Data Link Control Protocol) olarak bilinir ve bu protokol veri paketlerini çerçevelere bölerken, PPP paket formatını değiştirmez.

2. Uçtan uca bağlantıların kurulması ve test edilmesi için standart olarak bağlantı kontrol protokolü (LCP, Link Control Protocol) kullanır.

3. İletim esnasında hataları yakalamak için standart olarak ağ kontrol protokolü (NCP, Network Control Protocol) kullanır.

Noktadan Noktaya Protokol Tekniği
Veri paketleri sarmalandıktan sonra istemci, karşı tarafa uçtan uca bağlantı üzerinden LCP çerçeveleri gönderir. Karşı taraf bağlantı isteğini aldığında, bağlantı kurulmuş olur, kaynak nod uygun ağ katmanı protokollerinin seçimi için NCP çerçeveleri gönderir ve iki uç arasında veri iletimi başlar.



Şekil 2.28. Noktadan noktaya protokol bağlantının kurulması

PPP bağlantılar kurulduğunda, bu bağlantılar LCP ve NCP çerçeveler bağlantıyı sonlandırana dek devam eder. Bağlantıda bir problem olduğu durumda da bu bağlantı sonlandırılabilir.

Noktadan Noktaya Protokol Paket Formatı
Bir PPP çerçeve altı bölümden oluşur:

Flag: 1 byte uzunluğundadır, çerçevenin başlangıç ve bitimini belirtir.

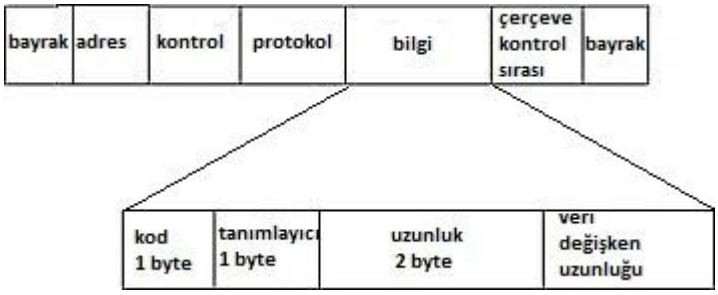
Adres: PPP uçtan uca bağlantıları kullandığından, yayın (broadcast) adres kullanır, bu alanın uzunluğu 1 byte'tır.

Kontrol: Bu bilginin uzunluğu 1 byte'tır ve 00000011 serisini kullanır. Çerçevenin istemci bilgisini taşıdığını belirtir.

Protokol: Çerçevenin veri alanında sarmalanmış olan verinin protokolünü belirtir. Uzunluğu 2 byte'tır.

Data: Kaynak ve hedef nodlar arasındaki bilgiyi içerir. Maksimum uzunluğu 1500 byte'tır.

Çerçeve Kontrol Sırası (FCS, Frame Check Sequence): Uzunluğu 2-4 byte'tır.



Şekil 2.29. Noktadan noktaya çerçeve formatı

Noktadan Noktaya Protokol Bağlantı Kontrolü

PPP, iki nod arasındaki veri iletiminin yanında iki uç arasındaki bağlantının kontrolünü yapma işleminden de sorumludur. Bu amaçla LCP standardını kullanır. LCP aşağıdaki işlemleri yapar:

- PPP bağlantısının kurulumunda görev alır.

- Kurulu olan bağlantının konfigürasyonunu yapar.

- Kurulu olan bir PPP bağlantının düzenli kontrollerini sağlar.

- İki uç arasındaki veri iletimi tamamlandığında bu bağlantıyı sonlandırır.

LCP tabanlı link kontrolü 4 fazda çalışır: Link kurulumu, link kalitesi, uygun ağ katman protokolünü belirleme, link sonlandırma fazları. Bu fazların açıklamaları aşağıdadır:

- Link kurulumu: İki uç arasındaki bağlantı LCP tarafından kurulur, LCP bu işlem için bağlantı kurulum çerçevelerini kullanır. Her bir uç cevap olarak kendi çerçevelerini gönderdiğinde bu faz tamamlanmış olur.

- Link kalitesi: Kurulan bağlantının tam olarak hazır olup olmadığını kontrol eder.

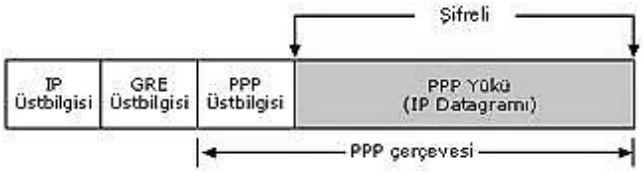
- Ağ katman protokolünü belirleme: Bu fazda PPP çerçevelerinin protokol alanına sarmalanmış olan verinin ağ katmanı protokolü belirlenir.

- Link sonlandırma: LCP'nin son fazıdır ve iki uç arasındaki mevcut PPP bağlantıyı sonlandırır.

2.7.2. Noktadan Noktaya Tünelleme Protokolü (PPTP)

Noktadan noktaya tünelleme protokolü (Point to Point Tunnel Protcol): Bir ikinci katman protokolüdür ve PPP çerçeveleri IP ağı üzerinden (internet) iletilmesi için IP

datagramlar içine sarmalanır. PPTP daha çok uzaktan erişimli sanal özel ağ bağlantılarda kullanılır. RFC 2637'de tanımlı bir protokoldür. PPTP, tünel işlemleri için TCP bağlantı, PPP çerçevelerin sarmalanması için genel yönlendirme sarmalaması (GRE) kullanır. Şekil 2.30.'da bir PPTP paketin yapısı gösterilmektedir:



Şekil 2.30. Noktadan noktaya tünelleme protokol paketin yapısı

PPTP, IP ağ üzerinden sanal özel ağ bağlantısı sağlayarak, istemci ve sunucu arasında güvenli veri transferi yapar. Talep edildiğinde sanal özel ağ bağlantıları kurmayı sağlar. PPTP protokolünün avantajları aşağıdaki gibidir.

1. Genel Aktarmalı Telefon Şebekesi (PSTN, Public Switched Telephone Networks) ağı kullanır: Sanal özel ağ bağlantılarda PSTN ağının kullanılmasına imkân sağlar ve böylece sanal özel ağ konfigürasyonları daha kolay bir hale gelir. Bu kolaylığından ve düşük maliyetinden dolayı günümüzde yavaş yavaş kiralık devre ağlarının yerini almaktadır.

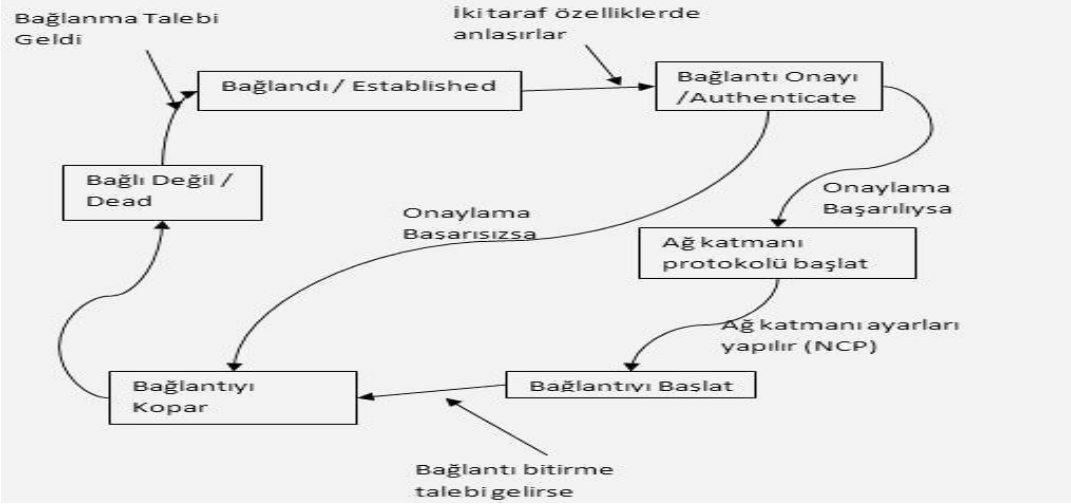
2. IP tabanlı olmayan protokolleri de destekler: IP protokolünün yanında TCP/IP, IPX, NetBEUI ve NetBIOS standartlarını da desteklemektedir. Bundan dolayı sadece internet üzerinden değil, özel ağlar üzerinden de sanal özel ağ bağlantıları kurulabilir.

Noktadan Noktaya Tünelleme Protokolünde Noktadan Noktaya Protokolünün Rolü:
PPTP, PPP protokolünün gelişmiş bir sürümüdür. Temel olarak PPP protokolünün tekniklerini kullanır. Farkı ise sadece PPP trafiğini genel ağlar üzerinden farklı bir yöntemle geçirmesidir. PPTP protokolü de PPP gibi çoklu bağlantıları desteklememektedir. PPTP kullanan tüm bağlantılar uçtan-uca bağlantılardır. PPP protokolü PPTP tabanlı iletimlerde aşağıdaki fonksiyonları destekler.

- Uç noktalar arasında fiziksel bağlantının kurulması ve sonlandırılması

- PPTP istemcilerin kimlik doğrulamasının gerçekleştirilmesi

- PPP datagramlarının oluşturulabilmesi için IPX, NetBEUI, NetBIOS ve TCP/IP datagramlarının şifrelenmesi



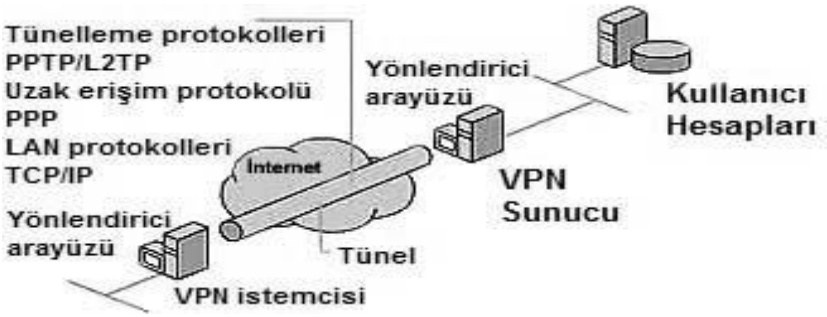
Şekil 2.31. Noktadan noktaya protokol işlemleri

Noktadan Noktaya Tünelleme Protokolü Bileşenleri
PPTP üç temel bileşenden oluşmaktadır.

- PPTP istemci

- Network Access Server (NAS)

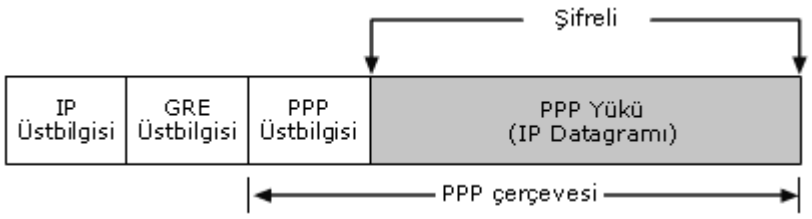
- PPTP sunucu



Şekil 2.32. Noktadan noktaya tünel protokolü ve bileşenleri

Noktadan Noktaya Tünelleme Protokolü İstemcileri:

PPTP istemci uzak bir sunucuya bağlantı isteği gönderdiğinde internet servis sağlayıcı tarafındaki NAS sisteminin servislerini kullanır. İstemci ilk olarak internet servis sağlayıcı tarafına dial-up PPP bağlantı kurabilmek için bir modeme ve bir tünel oluşturulması için sanal özel ağ cihazına bağlanır. Sanal özel ağ cihazları internet üzerinden tünel oluşturmak için internet servis sağlayıcı tarafındaki NAS sistemine dial-up olarak bağlanırlar. Şekil 2.33.'te noktadan noktaya tünelleme protokolü paket yapısı gösterilnmiştir.



Şekil 2.33. Noktadan noktaya tünel protokolü paketi

Noktadan Noktaya Tünelleme Protokolü Sunucuları: Uzakta veya lokalde bulunan bir noddan diğer bir noda sanal özel ağ isteklerini iletme yeteneğine sahip sunuculardır. Uzak isteklere cevap verebilen PPTP sunucuların yönlendirme özelliğine sahip olması gerekmektedir. RAS (Remote Access Server) sunucular yaygın olarak kullanılan PPTP sunuculardır.

Noktadan Noktaya Tünelleme Protokolü Ağ Erişim Sunucuları (NAS): İstemcilerin PPP veya arama (dial-in) olarak internet bağlantısını sağlayan ve internet servis sağlayıcı tarafında bulunan sunuculardır.

Noktadan Noktaya Tünelleme Protokolü Güvenliği
PPTP güvenli bir iletişim için aşağıdaki özelliklere sahiptir:

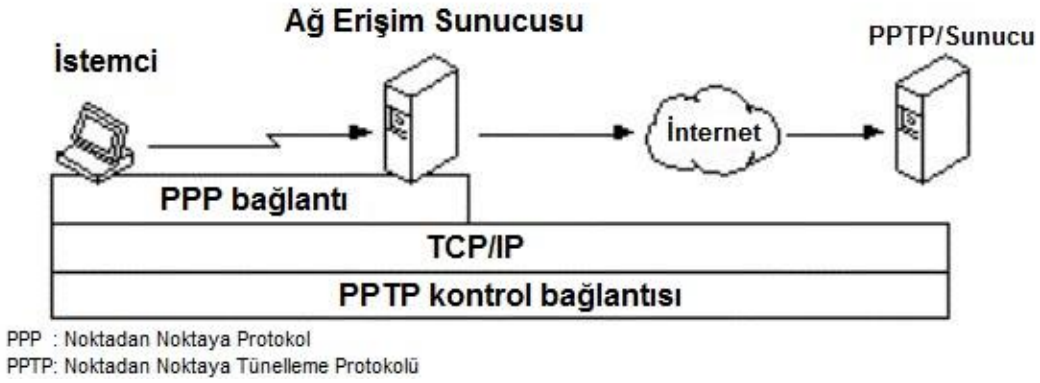
- PPP tabanlı bağlantı kurma

- Bağlantı kontrolü

- PPTP tünelleme ve PPTP veri transferi

- PPTP bağlantı kontrolü

PPTP sunucu ve istemci arasında PPP tabanlı bir fiziksel bağlantı kurulduktan sonra PPTP bağlantı kontrolü yapılır. Bu kontrol tipi Şekil 2.34.'te görülmektedir:



Şekil 2.34. PPP bağlantı üzerinden PPTP kontrolünün yapılması

PPTP kontrol mesajları TCP datagramlara sarmalanır. Bundan dolayı, uzak sunucu veya istemciyle PPP bağlantısı kurulduktan sonra bir TCP bağlantı başlatılır. PPTP kontrol mesajları bu bağlantı üzerinden iletilir.

Noktadan Noktaya Tünelleme Protokolü Tünelleme
Bir PPTP veri paketi aşağıdaki sarmalama işlemlerinden geçirilir.

- Verinin Sarmalanması: Veri yükü şifrelenir ve bir PPP çerçeve içine sarmalanıp bu çerçeveye bir PPP başlık eklenir.

- PPP çerçevelerin sarmalanması: Başlık bilgisi eklenmiş olan PPP çerçeve, GRE içine sarmalanır.

- GRE paketi sarmalanması: GRE paketin içine sarmalanmış olan PPP çerçeveye bir IP başlık eklenir ve bu başlıkta PPTP istemci ve hedef ağdaki sunucunun IP adresleri taşınır.

- Veri bağlantı katmanı sarmalanması: PPTP bir Layer 2 tünelleme protokolüdür. Bundan dolayı veri bağlantı katmanı başlığı tünellemede büyük öneme sahiptir. Bu katman datagramlara kendi başlık bilgisini ekler. Eğer bu datagram lokal PPTP tünelinden geçecekse, bir LAN teknolojisi başlığı ile sarmalanır. Eğer bir WAN tünelini kullanacaksa bu datagramda değişiklik yapılmaz.

Şekil 2.35. Noktadan noktaya tünel prtokolü ile veri tünelleme işlemi

PPTP veri transferi istemciye başarıyla yapıldığında istemci tünellenmiş paketleri orijinal paketlere dönüştürmeyi isteyecektir. PPTP tünellenmiş paketin geri dönüşümü, PPTP tünelleme işleminin tam tersidir. Orijinal paketlerin elde edilebilmesi için aşağıdaki işlemler takip edilir:

- İstemci pakete gönderen tarafından eklenmiş olan veri bağlantı (data link) başlığını kaldırır

- GRE başlık kaldırılır

- IP başlık kaldırılır

- PPP başlık kaldırılır

- Son olarak şifre çözümleme yapılır.

PPTP bağlantıların kontrolü TCP 1723 portu üzerinden PPTP istemcinin ve sunucunun IP adresi ile yapılır. Kontrol mesajları ile PPTP tünellerin devamlılığı ve sonlandırılması sağlanır, PPTP sunucu ve istemci arasındaki bağlantıda bir problem olup olmadığı kontrol edilir.

PPTP protokolündeki güvenlik işlemleri aşağıda görülmektedir:

- Veri şifrelemesi

- Kimlik doğrulama

- Erişim kontrolü

- Paket filtrelemesi

- PPTP veri şifrelemesi

PPTP, PPP tarafından desteklenen MPPE (Microsoft Point-to-Point Encryption) şifreleme servislerini kullanır. Anahtar üreten algoritma RSA-RC4 hash algoritmasıdır. Bu anahtar tünel içinden iletilen verilerin şifrelenmesi için kullanılır.

Noktadan Noktaya Tünelleme Protokolü Kimlik Doğrulaması
PPTP aşağıda anlatılan kimlik doğrulama mekanizmalarını kullanır.

- Karşılıklı El Sıkışma Kimlik Doğrulama Protokolü (MS-CHAP, Microsoft Challenge Handshake Authentication Protocol): PPP tabanlı kimlik doğrulamalar için kullanılır. CHAP tekniğine benzemektedir. Tek farkı, MS-CHAP tekniği RSA RC4 algoritmasını, CHAP tekniği ise RSA MD5 algoritmasını kullanır.

- Şifreli Kimlik Doğrulama Protokolü (PAP, Password Authentication Protocol): En yaygın arama (dial-in) kimlik doğrulama protokolüdür. Ayrıca PPP tabanlı bağlantılarda da kimlik doğrulamada kullanılır.
PPTP protokolünün temel avantajları aşağıdaki gibidir.

- PPTP yaygın olarak kullanılan bir built-in (dahili) Microsoft çözümüdür.

- IP tabanlı olmayan protokolleri de destekler.

- Unix, Linux, Apple’s Macintosh desteği vardır.

PPTP Protokolünün dezavantajları ise aşağıdaki gibidir.

- L2TP ve IPSEC protokolüne göre güvenliği daha azdır.

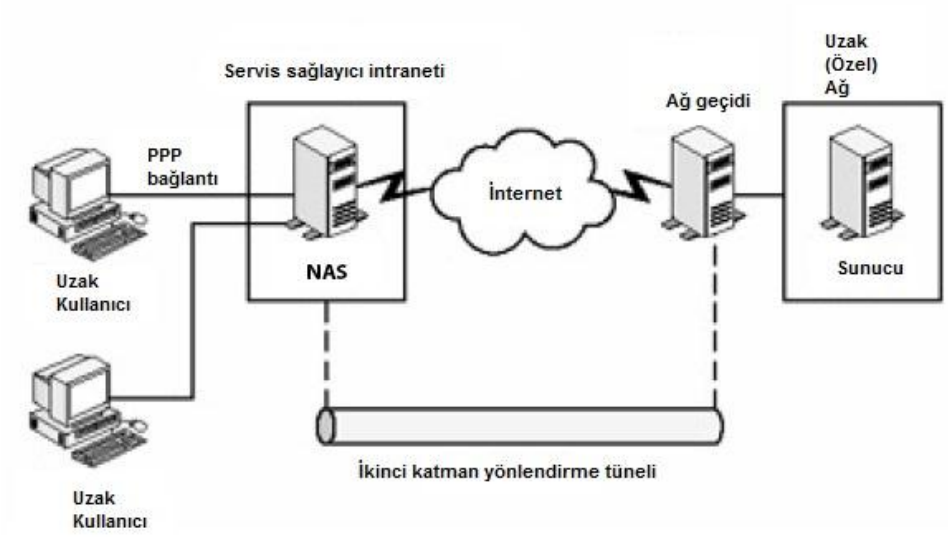
- PPTP platform bağımlı bir protokoldür.

- PPTP sunucudaki tanımlamaları zordur.

- PPTP protokolünün en büyük dezavantajı güvenlik mekanizmasının çok sağlam olmamasıdır. Çünkü anahtarın kullanıcı şifresinden elde edildiği simetrik şifreleme tekniğini kullanır.

2.7.3. İkinci Katman Yönlendirme Protokolü (L2FP)

İkinci katman yönlendirme protokolü (L2TP, Layer 2 forwarding protocol): Uzak bağlantılarda birçok avantajlara sahiptir. Bir tünel içinde birden fazla oturum açabilir. Yani tek bir çevirmeli bağlantı ile birden fazla kullanıcı intranete erişebilir. Bu nedenle L2F ile sanal özel ağ çözümlerinin maliyeti daha düşük olacaktır, çünkü uzak lokasyon ile internet servis sağlayıcı arasında ve internet servis sağlayıcı (bulunma noktası) POP noktası ile intranet arasındaki bağlantıların sayısı azalacaktır. Şekil 2.36.'da L2F tünelleme yapısı görülmektedir.



Şekil 2.36. Servis sağlayıcı intraneti ile ağ geçidi arasındaki ikinci katman yönlendirme tünel

İkinci Katman Yönlendirme Tekniği: Bir istemci intranetteki bir kaynağa çevirmeli bağlantı ile eriştiğinde aşağıda bahsedilen olaylar gerçekleşir:

- İstemci servis sağlayıcı ile ISDN veya PSTN ağı üzerinden PPP bağlantı başlatır.

- İnternet servis sağlayıcı (bulunma noktası) POP noktasındaki NAS sistemi istemcinin bağlantısını kabul ederse, NAS sistemi ile istemci arasında bir PPP bağlantı başlatılmış olur.

- İstemcinin servis sağlayıcıda CHAP veya PAP teknikleri ile kimlik doğrulaması yapılır.

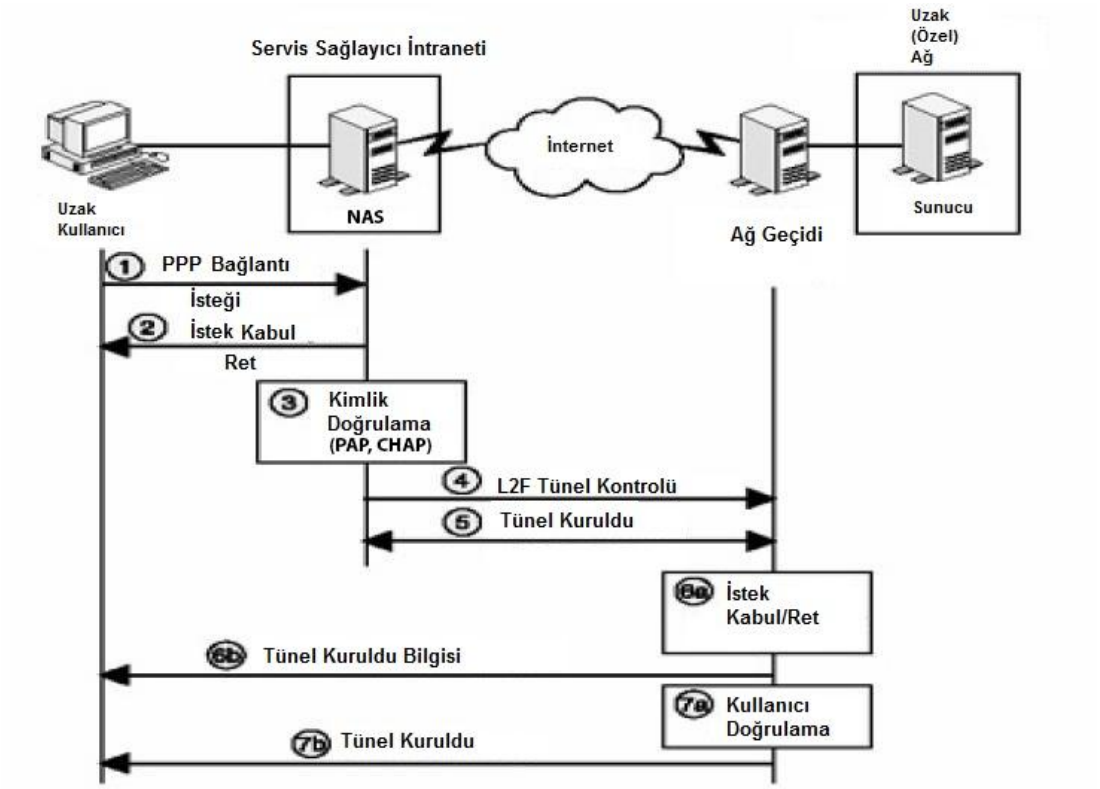
- Eğer hedef ağın ağ geçidine mevcut bir tünel yoksa bir tünel kurulur.

- Tünel kurulumu gerçekleştikten sonra bağlantıya bir MID atanır ve ağ geçidine uzak bir kullanıcının bağlantı isteği olduğu mesajı gönderilir.

- Ağ geçidi bağlantı isteğini ya kabul eder ya da reddeder. İstek reddedilirse dial-up bağlantı sonlandırılır, kabul edilirse ağ geçidi kullanıcıya bağlantıyı başlatacağına dair mesaj gönderir.

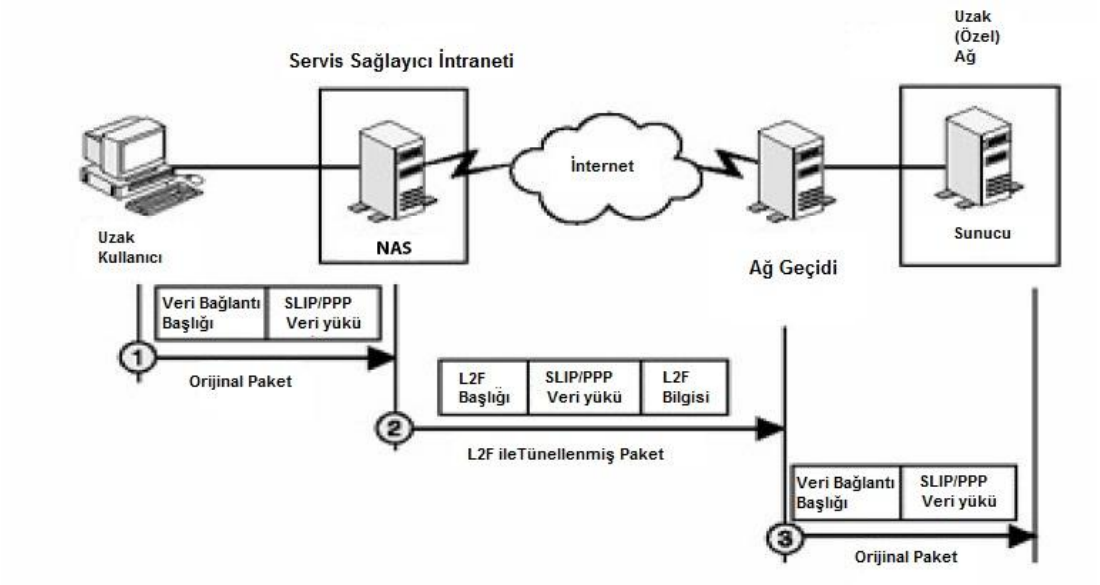
- Kullanıcının ağ geçidi tarafından kimlik doğrulaması yapıldıktan sonra kullanıcı ile ağ geçidi arasında sanal bir ara yüz kurulur.

Şekil 2.37.'de iki uç arasında L2F tünelin kurulması işlemleri gösterilmektedir:



Şekil 2.37. İstemci ve sunucu arasında ikinci katman yönlendirme tünelin kurulması

İkinci Katman Yönlendirme Tünelleme: İstemcinin kimlik doğrulaması yapılıp bağlantı isteği kabul edildikten sonra, Servis Sağlayıcı-NAS sistemi ile hedef ağın ağ geçidi arasında Şekil 2.38.'de görüldüğü gibi bir tünel kurulur.



Şekil 2.38. İkinci katman yönlendirme tünelleme işlemi

L2F tüneller aynı zamanda "sanal ara yüz" olarak ta isimlendirilirler. Tünel kurulduktan sonra çerçeveler tünel üzerinden aşağıda anlatıldığı gibi iletilir:

- İstemci çerçeveleri Servis Sağlayıcı-NAS sistemine gönderir.

- NAS sisteminde çerçeveye bir L2F başlık eklenir, çerçeve sarmalanır ve tünel üzerinden hedef ağa gönderilir.

- Ağ geçidi tünellenmiş paketleri kabul eder, L2F başlığına bakar ve paketi intranet içinden hedef kaynağa iletir.

- Hedef kaynak aldığı tünellenmiş paketleri orijinal haline dönüştürür.

Şekil 2.39. İkinci katman yönlendirme paket formatı

Hedef ağdan istemciye cevap gönderilmesi de aynı şekilde gerçekleşir, çerçeveler ilk olarak ağ geçidine gönderilir ve L2F paketlerin içinde sarmalanır, Servis Sağlayıcı-NAS sistemine iletilir. NAS sistemi çerçevenin L2F bilgisine göre çerçeveyi istemciye iletir.

İkinci Katman Yönlendirme Veri Şifrelenmesi: L2F şifreleme işlemi için MPPE (Microsoft Point-to-Point Encryption) tekniğini kullanır. Fakat bu teknik günümüzde güvenlik açısından yetersiz kaldığı için verinin iletiminde ek olarak IPSEC tekniğini de kullanır. IPSEC, şifreleme amaçlı olarak ESP (Encapsulating Security Payload) AH (Authentication Header) ve IKE (Internet Key Exchange) protokollerini kullanır.

İkinci Katman Yönlendirme Kimlik Doğrulama: L2F kimlik doğrulaması iki aşamada gerçekleştirilir: ilk olarak istemci ISP (bulunma noktası) POP noktasına dial-in bağlantı yapar, kimlik doğrulama geçekleşir ve bir tünel kurulur. İkinci aşamada ise ağ geçidi ile NAS sistemi arasında istemcinin kimlik doğrulaması yapılır ve tünel kurulur. L2F, PPTP tekniğinde olduğu gibi, kimlik doğrulama işlemlerinde PPP servislerinden yararlanır. L2F ağ geçidi bir bağlantı isteği aldığında istemcinin kimlik doğrulama işlemi yapılırken PAP tekniği kullanılır. L2F veri güvenliğini sağlamak için ayrıca CHAP, EAP, Arayan kullanıcının uzaktan kimliğini doğrulama (RADIUS) ve terminal giriş kontrol ünitesi, kontrol sistemi (TACACS) tekniklerinden de yararlanır.

L2F çözümlerinin sağladığı avantajlar aşağıdaki gibidir:

- Gelişmiş güvenlik özelliği

- Platform bağımsız olması

- İnternet servis sağlayıcı tarafında çok fazla tanımlama yapılmaması

- ATM, FDDI, IPX, NETBEUI ve Frame Relay desteğinin de olması.

L2F çözümlerinde aşağıdaki gibi bazı dezavantajlarda söz konusu olmaktadır. Bunlar aşağıdaki gibidir:

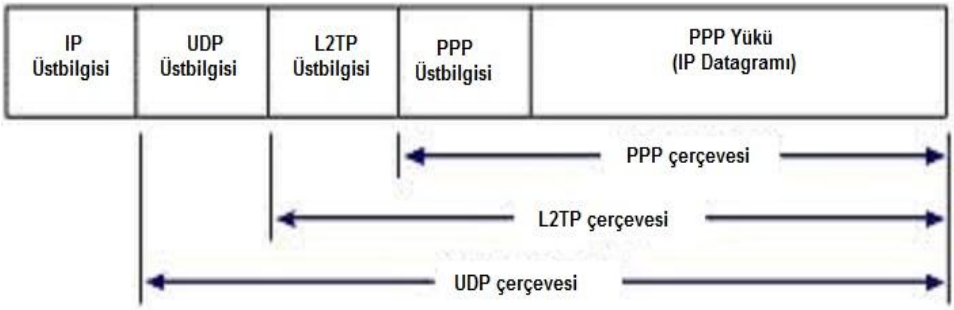
- Konfigürasyonları kolay olmamaktadır

- İnternet servis sağlayıcı tarafında da L2F desteği olması gerekmektedir

- PPTP ile kıyaslayınca L2F tünellerde iletim hızı daha yavaştır

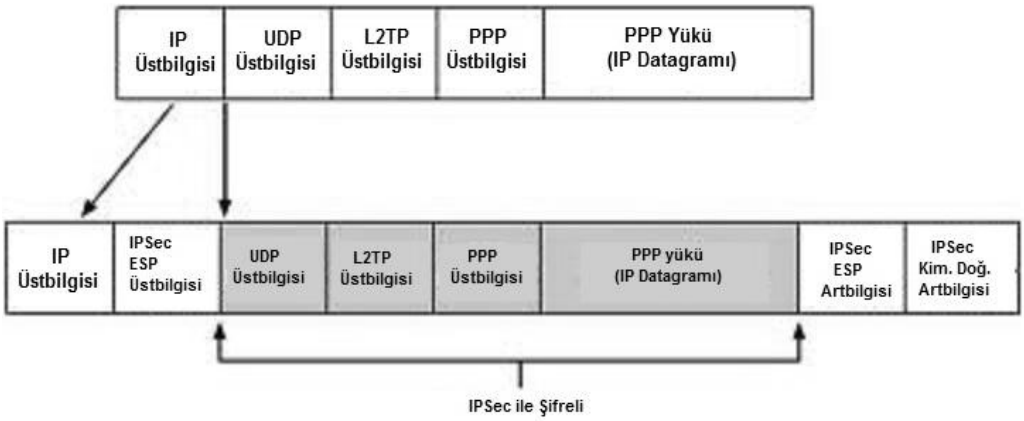
2.7.4. İkinci Katman Yönlendirme Tünelleme Protokolü (L2TP)

İkinci katman yönlendirme tünelleme protokolü, noktadan noktaya tünelleme protokolü ve ikinci katman yönlendirme protokollerinin birleşimidir. Noktadan noktaya tünelleme protokolü ve ikinci katman yönlendirme protokollerinin en iyi özelliklerine sahiptir. PPP çerçeveleri; IP, X25, Frame Relay ve ATM ağları üzerinden iletilebilmesi için sarmalar. Datagram olarak IP kullanacak şekilde tanımlama yapılırsa internet üzerinden bir tünelleme protokolü olarak kullanılabilir. RFC 2661'de tanımlıdır. İnternet üzerinden, sarmalanmış PPP çerçevelerin tünellenmiş veri olarak iletilebilmesi için UDP protokolünü kullanır.



Şekil 2.40. İkinci katman yönlendirme tünelleme mesajın yapısı

Windows 2000 sisteminde L2TP paketlerin şifrelenmesi için IPSec, ESP (Encapsulating Security Payload) kullanılır. L2TP paketlerinin ESP ile şifrelenmiş formatı aşağıda görülmektedir:



Şekil 2.41. ESP ile şifrelenmiş bir ikinci katman yönlendirme tünelleme paketin yapısı

2.7.5. Protokollerin Karşılaştırılması

L2TP ve PPTP, OSI modeline göre 2. katmanda çalışan protokollerdir. Kullanıcı yetkilendirmesi esasına dayanarak çalışırlar. Örneğin bir PPTP istemcisi, PPTP sunucusuna kullanıcı adı ve şifresini göndererek bağlantı talebinde bulunur. Şayet istemcinin gönderdiği kullanıcı adı ve şifre doğruysa oturum açılır. Artık istemci ile sunucu arasındaki bilgi şifreli olarak taşınır. Şifreleme için kullanılan anahtar, kullanıcı şifresinden türetilir. Hem L2TP hem de PPTP verinin aktarımını datagram (UDP) paketleri ile yapar. Ancak PPTP, L2TP'den farklı olarak tünelin kurulumu ve yönetimi ile ilgili kontrol işlemlerini, sunucu ile istemci arasında TCP bağlantısı kurarak yapar. Bu PPTP protokolünün, paket geçirme süresinin yüksek olduğu ağlarda L2TP protokolüne göre performansın düşmesine sebep olur. Diğer yandan L2TP'nin bir özelliği de aynı anda iki nokta arasında birden fazla tünel açabilmesidir.

Uygulama, güvenlik ve performans açısından tünelleme protokolleri aşağıdaki gibi birbirinden ayrılırlar:

1. IPSEC, en güvenilir olan tünelleme protokolüdür.

2. PTP protokolü güvenlik açısından L2TP'den daha iyi ancak performans yönünden daha kötüdür. IPSEC daha karmaşık güvenlik algoritmaları kullandığından, donanım kapasitesi yetersiz olan IPSEC istemci ve sunucular paketlerin gecikmesine neden olabilir.

3. PPTP ve IPSEC protokolü, aralarında mevcut bir IP bağlantısı olan hostlar arasında yapılır. Diğer yandan L2TP, aralarında ISDN, TDM, FR, ATM gibi devreler üzerinde direkt tünel kurup içinden IP, IPX, NETBEUI gibi her türlü trafiği taşıyabilir.

4. PPTP ve IPSEC protokolleri, istemci ile sunucu arasında aynı anda sadece bir tünel kurarlar. Diğer yandan L2TP, birden fazla oturum açabilir. Bu yönüyle, bazı ağ uygulamaları için L2TP oldukça uygun bir tünelleme protokolüdür.

Yukarıdaki maddelerden de anlaşılacağı gibi, L2TP daha çok özel uygulamalar için kullanılan bir protokoldür. Diğer yandan PPTP ve IPSEC protokolleri daha genel uygulamalar için kullanılan protokollerdir.

3. ARAŞTIRMA BULGULARI

GNS3 Cisco yönlendiricileri ve anahtarlama cihazları için tasarlanmış bir benzetim programıdır. Bu benzetim programı gerçek bir Cisco yönlendiricisini gerçekte çalışmış olduğu işletim sistemi (IOS) ile çalışacak şekilde kullanılan bir programdır. Buda gerçek bir Cisco cihazı ile çalışılıyor gibi olmaktadır.

Vmware gerçek bir bilgisayar üzerinde sanal bilgisayarlar oluşturmak ve sanal bilgisayar ağları oluşturmak için kullanılan bir programdır.

GNS3 ve Vmware programlarının her ikisi de yüksek bellek kullanımına neden olmaktadırlar. Bir bilgisayarda bu programların kullanılabilmesi için en az aşağıda belirtilen özelliklere sahip olması tercih edilmektedir;

- Intel Core 2 Duo 1.86 Ghz
- 2 GB RAM
- 80 GB HDD

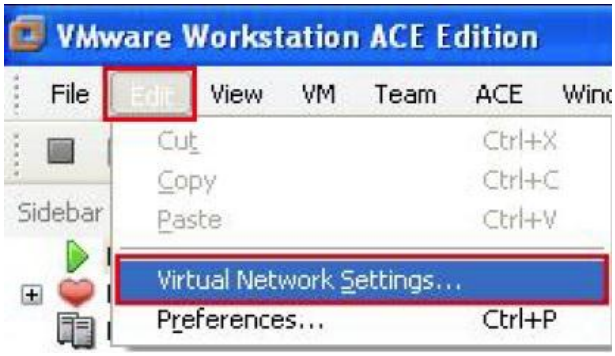
GNS3 benzetim programına http://www.gns3.net adresinden ulaşılabilmektedir. Program üzerinden çalışacak olan Cisco yönlendirici seçimi doğrultusunda bu yönlendiriciye uygun IOS'un bulunması gerekmektedir. Aksi takdirde yönlendirici çalışmayacaktır. Vmware üzerinde çalışılacak sanal bilgisayar seçimi tamamlandıktan sonra gerekli işletim sisteminin kurulup yüklenmesi gerekmektedir.

Konfigürasyonlar bitiminden sonra sanal bilgisayarların test işlemi ping komutu ile denenmiştir. Ayrıca paket detaylarını incelemek için ise WireShark programı kullanılmıştır. Bu programa ise http://www.wireshark.org adresinden ulaşılabilmektedir.

Tez içerisinde yapılacak çalışmalarda kullanılmak üzere 6 adet Windows XP işletim sistemine sahip sanal bilgisayar hazırlanmıştır. Hazırlanan sanal bilgisayarların dış

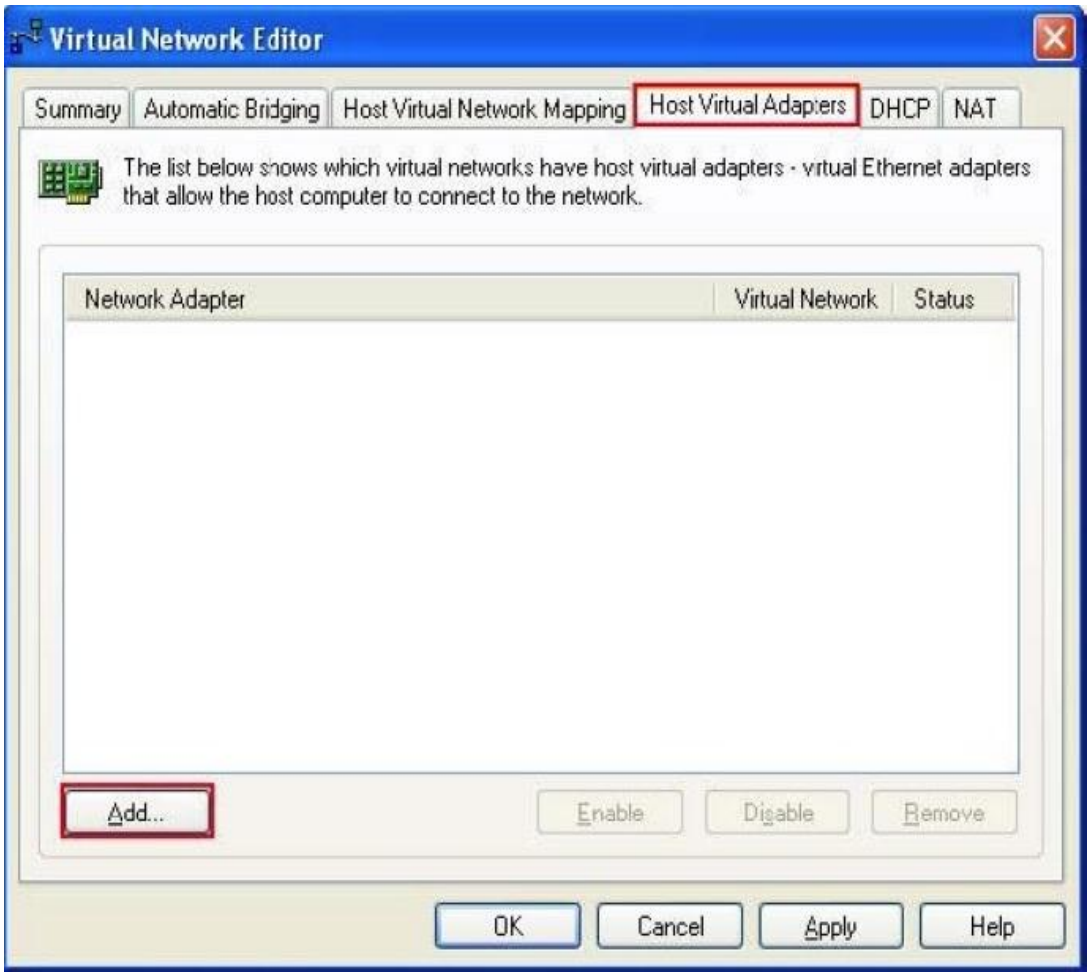
dünya (tez içerisinde yapılan çalışmada Cisco yönlendiriciler) ile iletişimi için sanal ağ ethernet kartları oluşturulması gerekmektedir. Bunun için sırası ile gerekli işlemler anlatılmıştır.

VMware yazılımı çalıştırılır ve Şekil 3.1.'de gösterilen **Edit** sekmesinde yer alan **Virtual Network Settings** seçeneği seçilir.



Şekil 3.1. Sanal ağ ayarları

Şekil 3.2.'de ekrana gösterilen ekrana gelen pencerede **Host Virtual Adapters** sekmesine tıklanır ve sisteme sanal ethernet kartları eklemek için **Add…** tuşuna tıklanır.

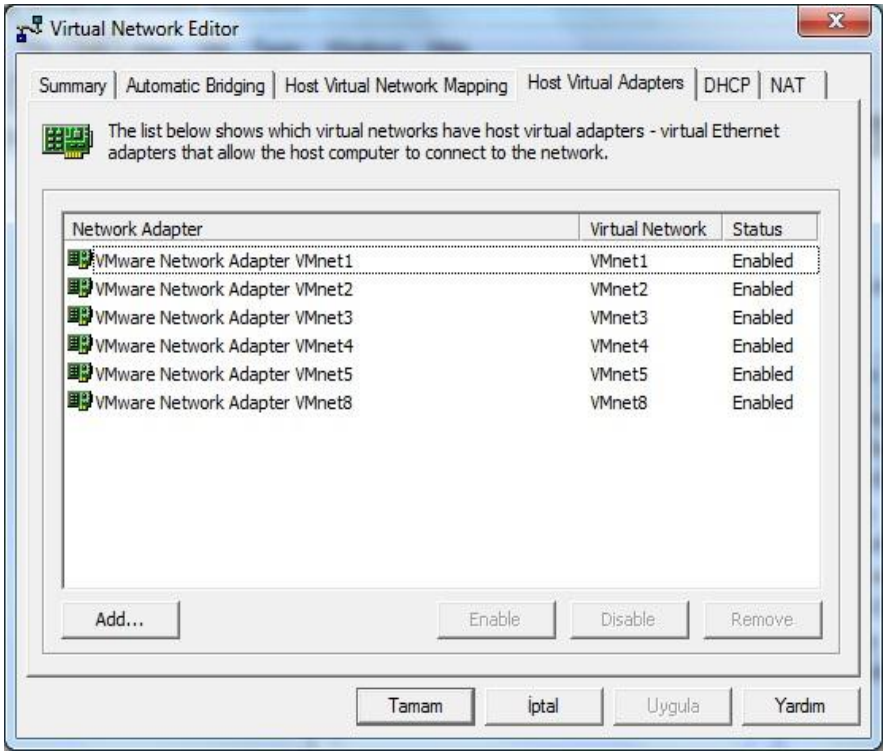


Şekil 3.2. Sanal ağ ayarları sanal ethernet kartı ekleme

Çıkan pencerede eklenmek istenen sanal ethernet kartı listeden seçilip **OK** tuşuna tıklanır. **VMnet1** ve **VMnet8** haricindeki ihtiyaç duyulan tüm sanal ethernet kartları eklenebilir.

Şekil 3.3. Sanal ağ ayarları sanal ethernet kartı seçimi

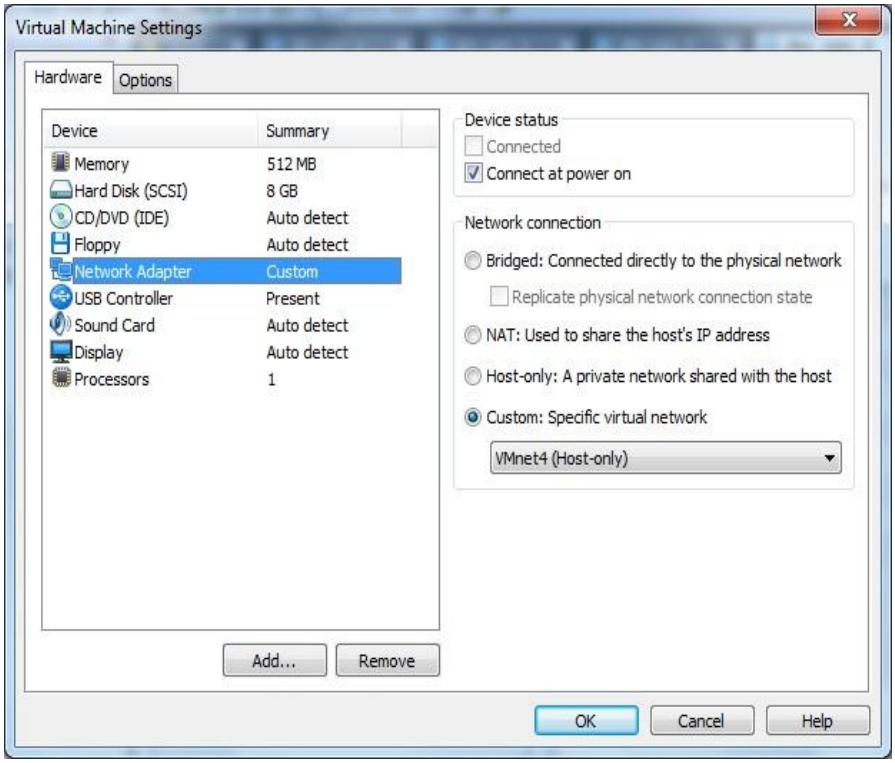
Adımlar eklenmek istenen her bir sanal Ethernet kartı için tekrarlanmalıdır. Tez içerisinde yapılan çalışmalarda kullanılmak üzere 5 adet sanal ethernet kartı eklenmiştir.



Şekil 3.4. Sanal ağ ayarları eklenen ethernet kartları

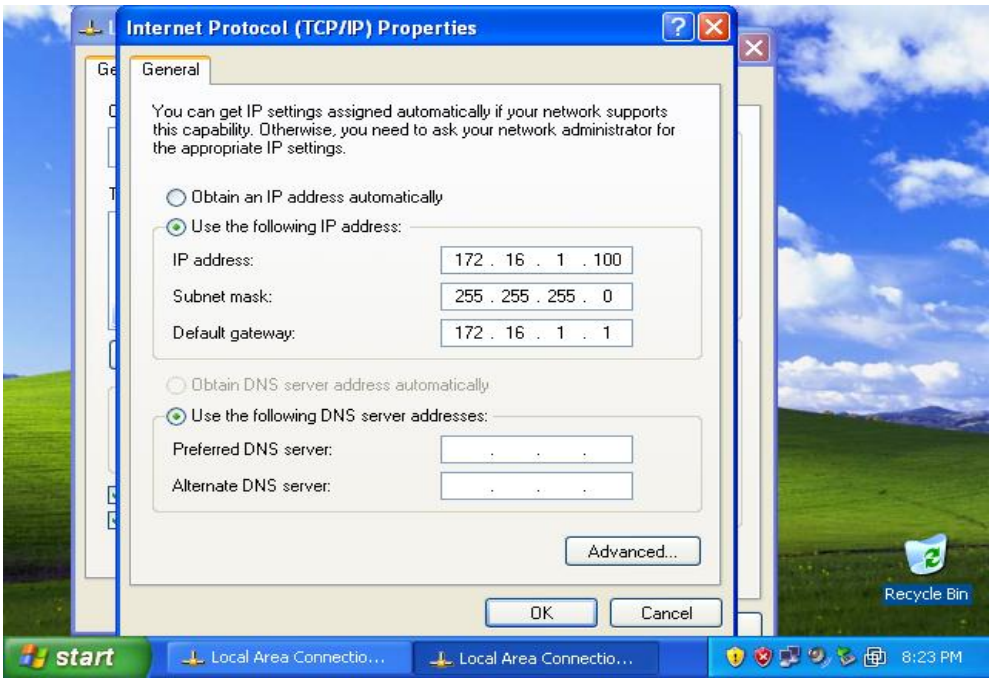
VMware yazılımının ana penceresinde **Edit virtual machine settings** üzerine tıklanır (Şekil 3.5.) ve ekrana gelen pencerenin sol kısmından **Ethernet** ayarları seçilir (Şekil 3.6.). Daha sonra pencerenin sağ tarafındaki **Network connection** seçeneklerinden **Custom: Specific virtual network** seçilir ve bu ayar altında kullanılmak istenen sanal Ethernet ara yüzü belirlenir.

Şekil 3.5. Sanal bilgisayar ayarı



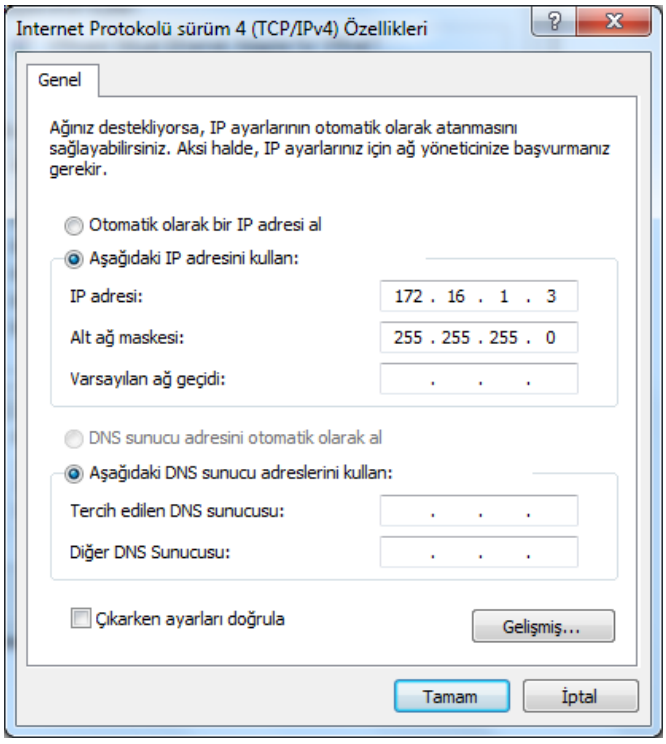
Şekil 3.6. Sanal bilgisayar ethernet seçimi

Her bir sanal makine çalıştırılır ve IP ayarları topoloji doğrultusunda yapılır. Bu amaçla her bir sanal makinenin **IP adresi**, **ağ maskesi** ve **varsayılan ağ geçidi** ayarlanır.



Şekil 3.7. Sanal bilgisayar ip adresi

VMware yazılımının kurulu olduğu makinede sanal ethernet kartları gerçek ara yüzler olarak görüntülenecektir. Bu Ethernet ara yüzlerine, bu ara yüzlere karşılık gelen sanal makinelerin bulunduğu network ağından olmak üzere **IP adresi** ve **ağ maskesi** vermek yeterli olacaktır. Bu işlem, sonraki adımlarda sanal ethernet kartlarının birbirlerinden ayırt edilmesini sağlayacaktır.



Şekil 3.8. Sanal bilgisayar ethernet adresi

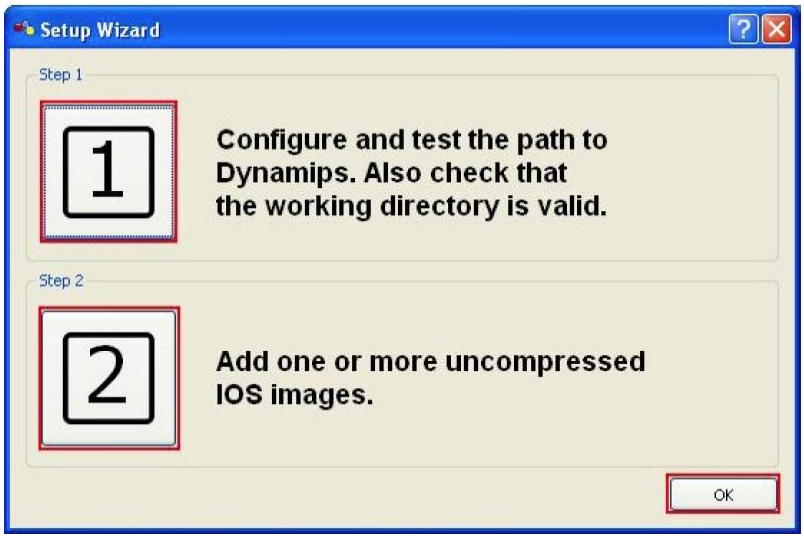
Bu adımlar sonucunda sanal VMware makineleri için gereken tüm ayarlar yapılmış hale gelecektir.

GNS3 yazılımı gerçek Cisco donanımını simüle edebilen, bu sanal donanım üzerinde gerçek Cisco IOS'larini çalıştırabilen ve bu yönüyle diğer benzeri simülatörlerden ayrılan oldukça güçlü bir benzetim yazılımıdır. Şimdi bu yazılımın adım adım nasıl kurulup ayarlanacağına geçelim:

GNS3 yazılımını çalıştırın. İlk çalışmada ekrana Şekil 3.9.'da gösterilen pencere gelir. Bu pencerede GNS3 yazılımının, dynamips yazılımını çalıştırması için gerekli yol (path) bilgisinin ayarlanıp kontrol edilmesi ve çalışılmak istenen Cisco IOS'lerinin sisteme eklenmesi amaçlanmaktadır.

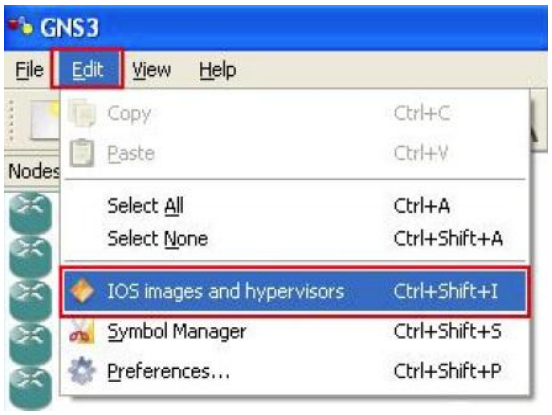
GNS3 yazılımı çalıştığı zaman arka planda dynamips yazılımını da çalıştırır. Böylece dynamips yazılımını ayrıca çalıştırmaya gerek kalmaz. Cisco IOS dosyalarının

kullanılabilmesi için yazılıma eklenmesi gerekmektedir. Bu amaçla yazılımın ana penceresinde **Edit IOS images and hypervisors** seçeneğine tıklanır.



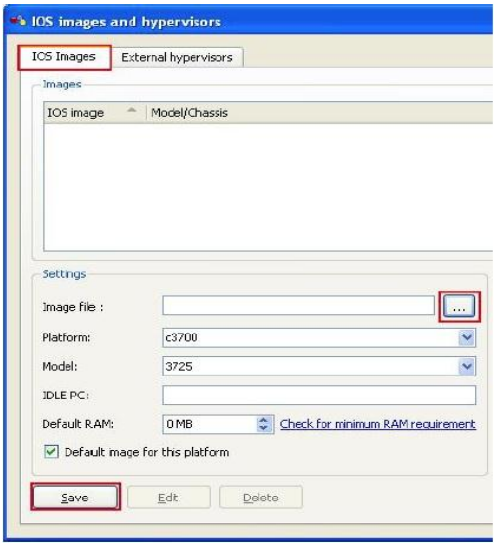
Şekil 3.9. GNS3 açılış ekranı

Ekrana gelen pencerede **IOS Images** sekmesine gelinir ve sisteme IOS eklemek için **Settings** altındaki **Image file** kutusunun yanındaki üç noktalı tuşa tıklanır.



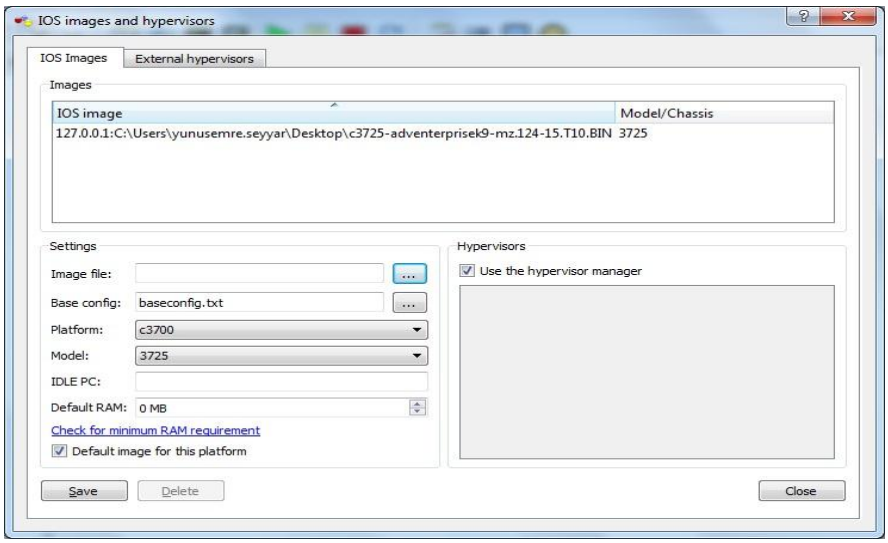
Şekil 3.10. GNS3 Cisco yönlendirici IOS seçimi

Açılan diyalog penceresinde sisteme eklenmek istenen IOS dosyası seçilir ve **Open** tuşuna tıklanır.



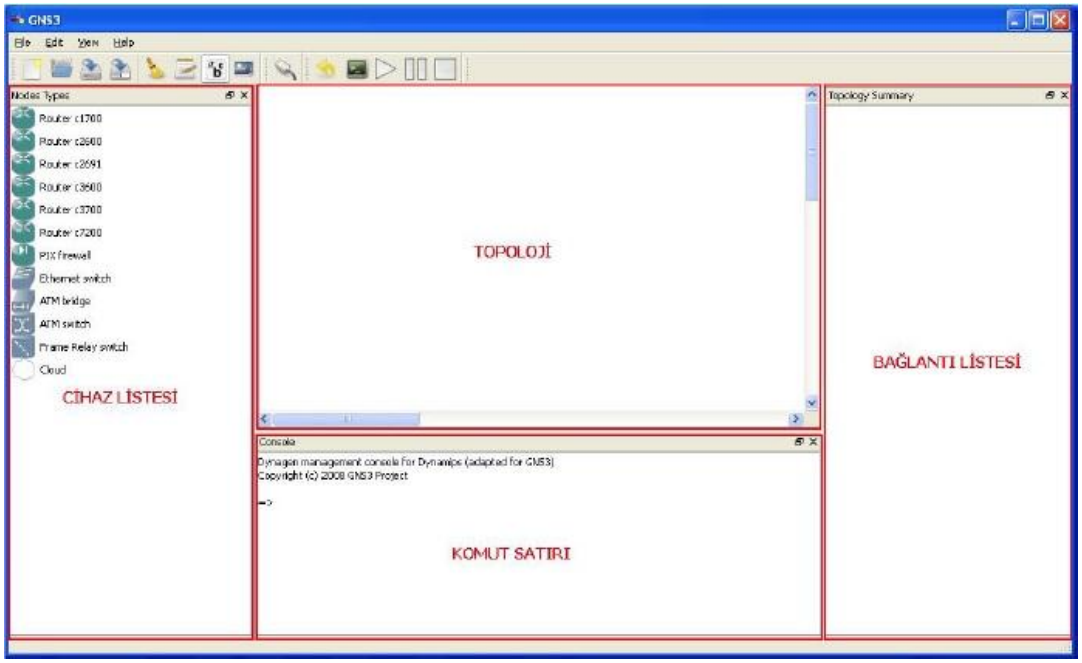
Şekil 3.11. GNS3 IOS yüklenmesi

Ekleme işlemi bittikten sonra Şekil 3.12'de gösterilen pencerede **Save** tuşuna tıklanıp yapılan ayarlar kaydedilir. Daha sonra bu pencere kapatılır.



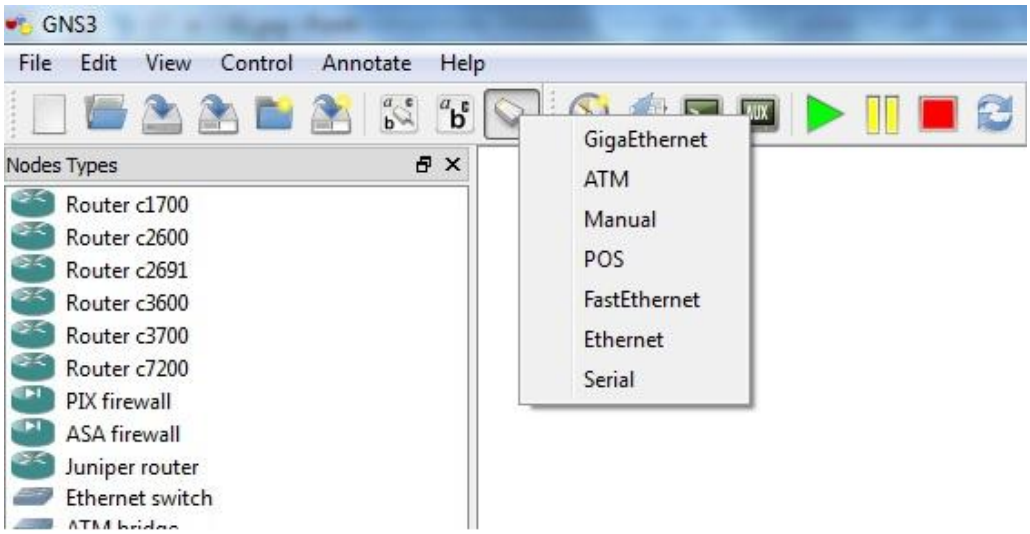
Şekil 3.12. Cisco IOS kaydedilmesi

GNS3 dört bölümden oluşmaktadır. Pencerenin sol tarafında topoloji için kullanılabilen cihazların listesi ve pencerenin sağ tarafında cihazlar arasındaki bağlantıların listesi bulunmaktadır. Ortadaki boş alan topoloji çizimi için kullanılmaktadır. Alt orta kısımdaki komut satırı ise cihazları listelemek, başlatmak, durdurmak gibi temel bir takım işlevlerin yerine getirilmesi için kullanılmaktadır.



Şekil 3.13. GNS bölümleri

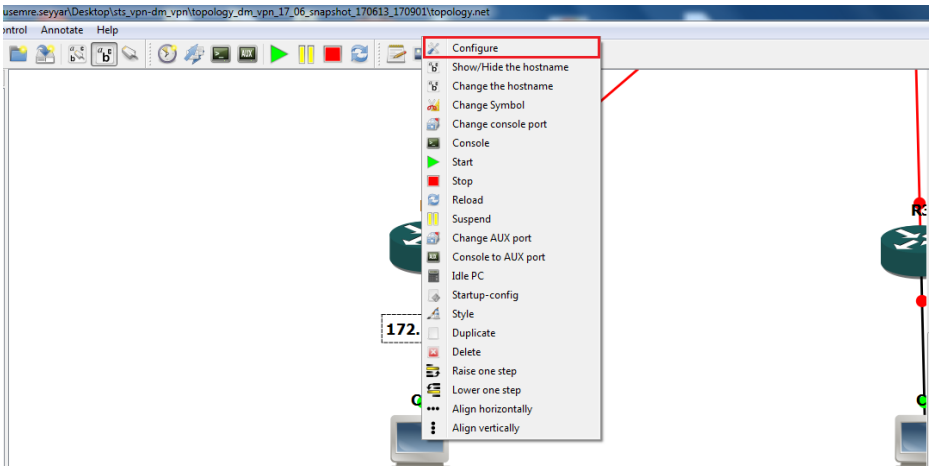
Yönlendiriciler arasındaki kablo bağlantıları Şekil 3.14'te gösterilen sekme altındaki seçenekler arasından yapılır. Burada topoloji gereksinimi doğrultusunda kablolar seçilir.



Şekil 3.14. Sanal yönlendiriciler arasında yapılacak bağlantı için kablolama çeşitleri

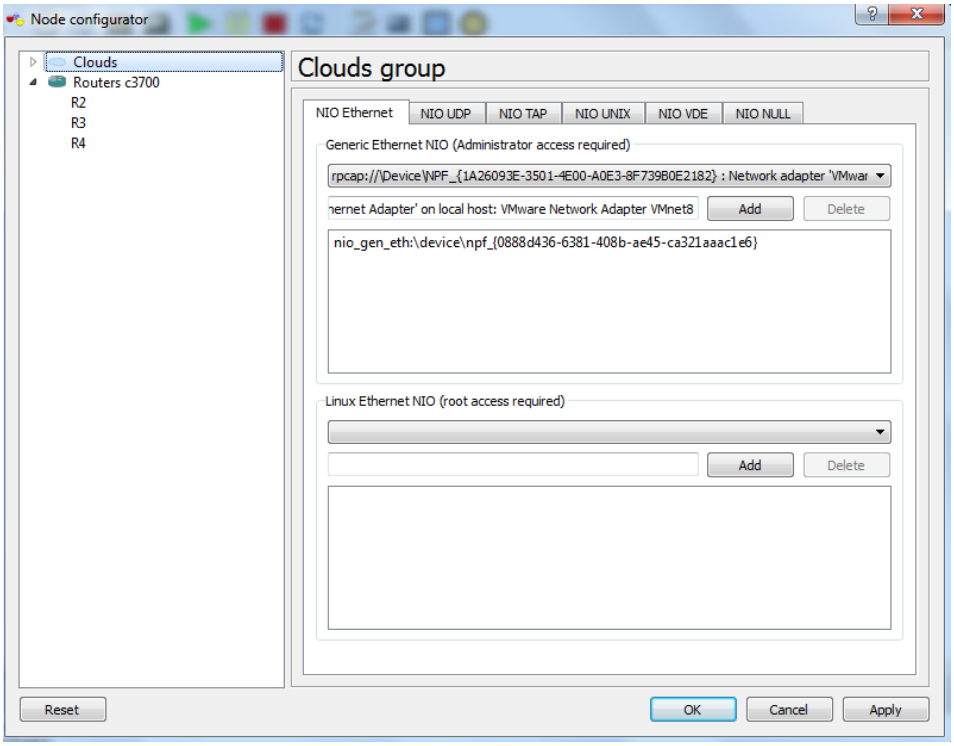
Idlepc değerleri, yönlendiricilerin minimum sistem kaynakları kullanılarak çalıştırılmasını sağlar. Bu değerler her sistemde farklılık gösterebilir. Tavsiye edilen **idlepc** değerinin başında * işareti bulunmaktadır. Bu değerin seçilmesi faydalı olacaktır. Eğer tavsiye edilen birden fazla değer varsa bunların arasından istenilen biri seçilebilir. Bazı durumlarda tavsiye edilen bir **idlepc** değeri olmayabilir. Bu gibi durumlarda ise yine istenilen bir değerin seçilmesinde sakınca olmayacaktır. Seçilen **idlepc** değerinin indeks numarası en aşağıdaki metin kutusuna girilip **OK** tuşuna tıklanır. Bu işlem her bir yönlendirici için ayrı ayrı tekrarlanmalıdır. Bir kere yapıldıktan sonra aynı topoloji için bir daha bu işlemin yapılmasına gerek yoktur.

Her iki programında kurulumunun bitmesinin ardından Vmware programında oluşturlan sanal bilgisayarların GNS3 programı ile eş zamanlı çalışabilmesi işlemini tamamlamak gerekmektedir. GNS3 programı ile oluşturulan topolojide yer alan bilgisayarın üzerine gelinip sağ tıklanır. Şekil 3.15.'te gösterilen **Configure** sekmesi seçilir.



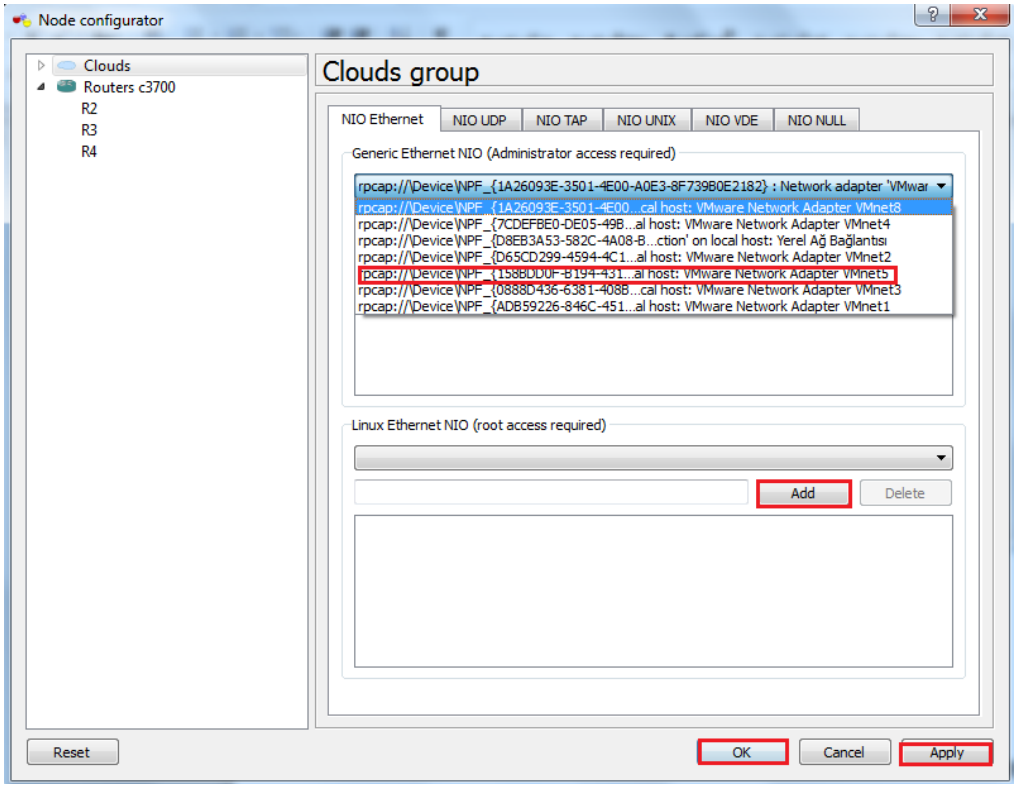
Şekil 3.15. Sanal Ethernet kart eklenmesi

Karşımıza Şekil 3.16.'te gösterilen ekran gelir. Burada **NIO Ethernet** Sekmesine gelinir.



Şekil 3.16. Sanal ethernet kart seçimi

Şekil 3.17.'te gösterilen sanal ethernet kart seçimi yapılıp, adda karasından ok basılarak sanal bilgisayar ile bağlantı kurulmuş olur. Bu adımdan sonra ilgi paket gönderme işlemlerini ping, tracert, sunuya erişim vb. sanal bilgisayar üzerinden yapılabilecektir.



Şekil 3.17. Sanal ethenert kartının yüklenmesi

3.1. Yönlendirme Protokolleri

Yönlendirme Protokolleri iki türlüdür:

1) Mesafe Vektörü (Distance Vector)
2) Bağlantı Durum (Link State)

Mesafe vektörü protokolünde yönlendirici, kendisine doğrudan bağlı diğer yönlendiricilerle bilgi alışverişinde bulunur ve bu yolla ağdaki yolların bilgisini

edinir. Yönlendirme Bilgi Protokolü (RIP), İç Ağ Geçidi Yönlendirme Protokolü (IGRP), Apple yönlendirme (AURP, AppleTalk Routing) mesafe vektörü protokolleridir.

Bağlantı durum protokolünde ise yönlendiricilerin birer veri tabanı bulunur. Bu veri tabanı yolu ile tüm ağ hakkında bilgi sahibi olur. Dezavantajlar: Veri tabanı büyük bir yer kaplayabilir. İkincisi bir yol çöktüğü zaman yeni yolların ayarlanması gerekir ki bu da fazla hesap demektir. Güvenilirliği yüzünden büyük ağlarda bağlantı durum protokolü kullanılır. Veri tabanını küçültmek için de yol özeti, değişken büyüklükteki alt ağ maskeleri gibi yöntemler geliştirilmiştir.
İlk Açık Yöne Öncelik (OSPF), Artırılmış İç Ağ Geçidi Yönlendirme (EIGRP), Sınır Ağ geçidi Yönlendirme (BGP, Border Gateway Protocol), Integrated ISIS ve NLSP bağlantı durum protokolleridir.

Yönlendirme Bilgi Protokolü (RIP): Xerox Parc tarafından yaratılmıştır. Yol bilgisi 30 saniyede bir anons edilir. Yol bilgisi anons edilirken alt ağ maskesi bilgisi gönderilmez. Bu sayede her bir anonstaki trafik düşürülmüş olur ama değişken büyüklükteki alt ağ maskeleri kullanılamaz. Hop sayısı 15 ile sınırlıdır.

İç Ağ Geçidi Yönlendirme Protokolü (IGRP, Interior Gateway Routing Protocol): Cisco'nun protokolü. Orta büyüklükteki ağlarda kullanılır (50 ila 75 yönlendiricinin bulunduğu). Hop sayısı max 100. Bir yolun diğerinden iyi olduğu geçilecek hop sayısı ile belirlenmez. Bunun yerine bant genişliği, bağlantı güvenilirliği, maksimumum paket büyüklüğü bağlantı kullanımı ve toplam gecikmeden oluşan bir metrik kullanır. Yol bilgisi 90 saniyede bir anons edilir. Ama ağdaki değişikliklerin anons edilmesi hemen gerçekleşir. Bir yol göçtüğünde sistemin yeni bir yol bulması 280 saniye sürebilir. RIP gibi IGRP'de alt ağ bilgisini yollamaz.

IGRP'nin performansını arttırmak için Cisco otonom sistem adını verdiği bir teknik kullanır. Bu teknikte yönlendiriciler gruplandırılır ve bir yönlendirici yalnızca kendi grubundaki yönlendiricilerle konuşur. Her grup için de bir sınır yönlendiricisi tayin edilir. Sınırdakiler birbirleri ile konuşarak yol bilgilerinin paylaşılması sağlanır.

İlk Açık Yöne Öncelik (OSPF, Open Shortest Path First): Büyük ağlarda kullanılır. En iyi yolu saptamak için yalnızca bant genişliğini kullanır. Bir bağlantının değeri 100 Megabit bölü o bağlantının bant genişliği şeklinde hesaplanır. Örneğin, 10 Megabit'lik bir ethernet bağlantısının değeri 10'dur. OSPF yönlendiricileri de IGRP'de olduğu gibi alanlara ayrılmışlardır. Ondan farklı olarak sıfır numaralı bir alan vardır ve bütün alanlar "Alan 0"a bağlı olmak zorundadırlar. OSPF yönlendiricileri birbirleri ile doğrudan konuşmazlar; onun yerine çoklu yayın (multicast) yaparlar. Yol bilgisi her 30 dakikada bir gönderilir. Çok daha sık olarak da küçük test paketleri gönderilir. Bir yol göçtüğünde ne olur ne olmaz denilerek 10 saniye beklenir, halen yol çökük durumda ise duyurusu yapılır. Yol bilgisi gönderilirken alt ağ bilgisi de gönderilir.

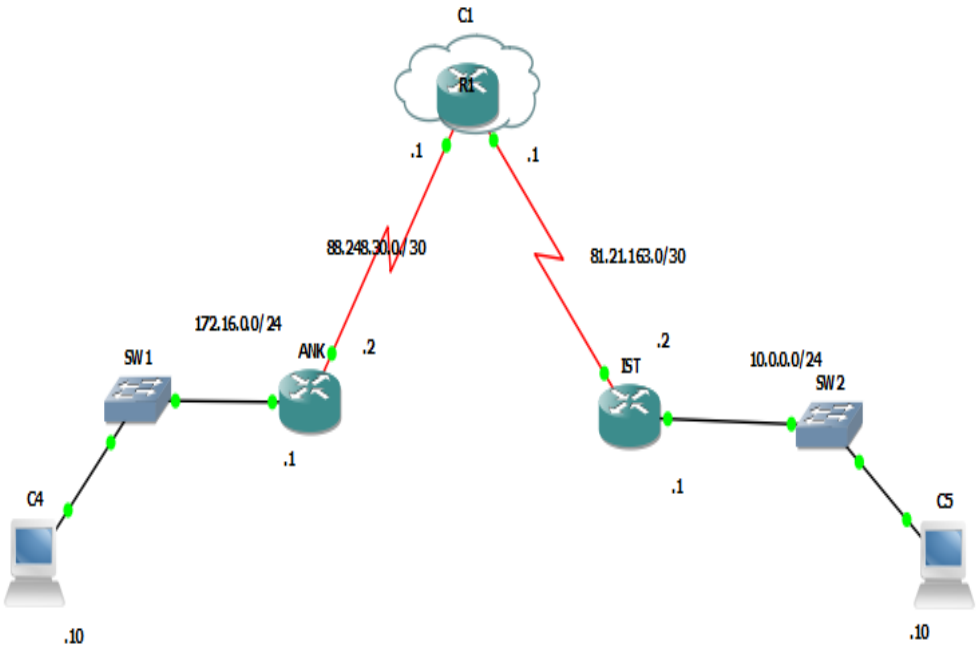
Artırılmış İç Ağ Geçidi Yönlendirme Protokolü (EIGRP, Enhanced Interior Gateway Routing Protocol): IGRP'nin hem bağlantı durum hem de uzaklık vektörü özelliklerinin ey iyilerini almış bir karışım protokolüdür.

Farkları: Yönlendirme tablosunda bir en iyi yol bir de ikinci en iyi yol bilgisi bulunur. Böylelikle bir yola bir şey olduğunda yeni bir yol arayışı için uzun zaman harcamak gerekmez. Yol bilgisi özetlenir. Alt ağ mask bilgisi gönderilir.

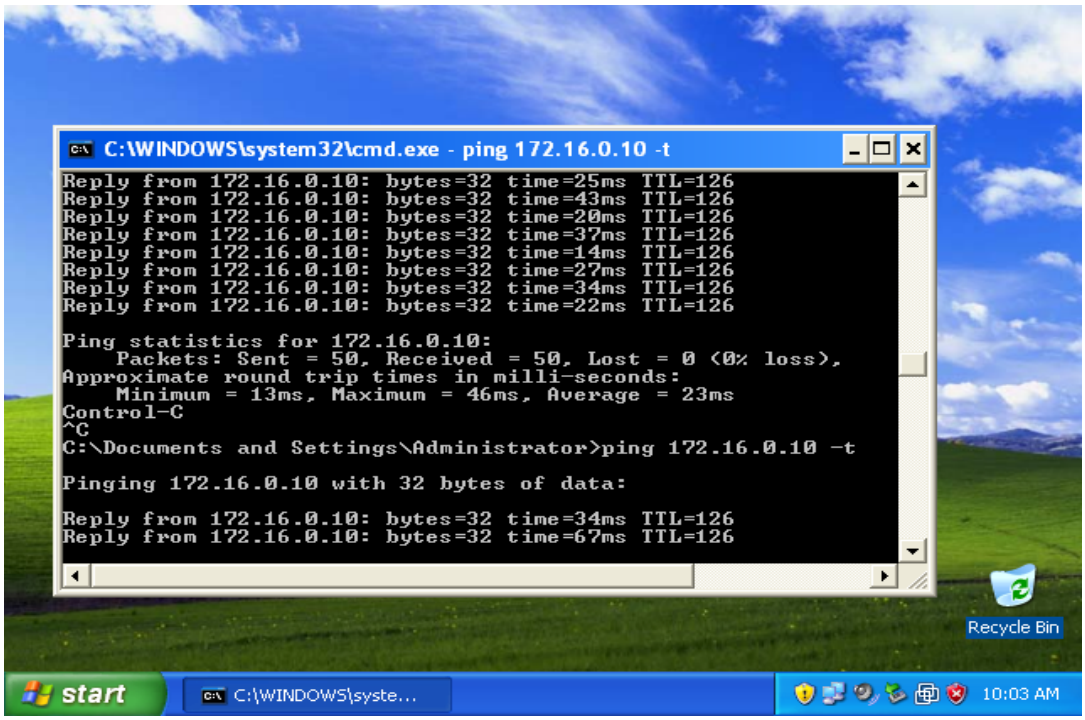
3.2. Siteden Siteye Sanal Özel Ağ

Siteden siteye sanal özel ağ için hazırlanan senaryo Şekil 3.18.'te gösterilmiştir. Bu arada bir firmanın Ankara ve İstanbul lokasyonları temel alınarak bu iki noktanın TT (Türk Telekom) üzerinden haberleştikleri gösterilmiştir. İlgili konfigürasyonlar ekler kısımda bulanabilir. Başlangıç olarak ilgili yönlendiricilerin ilgili bacaklarına gerekli ip adres atamaları yapılmıştır. Cihazların haberleşmesi için yönlendirme protokollerinden olan EIGRP protokolü kullanılmıştır. IPSEC protokolü kullanılarak tünel oluşturulmuştur. İki ağın haberleşmesi için TT'den geçen verinin şifrelenmesi için her iki ağa Isakamp profili uygulanmıştır. Isakamp için gerekli kurallar oluşturulmuştur. Verilerin şifrelemesi için 128 byte'lık AES (Gelişmiş Şifreleme Standardı) kullanılarak gerekli anahtarlar oluşturulmuştur. Tünel için gerekli olan hash algoritması olarak güvenli hash algoritması (SHA, Secure Hash Algorithm)

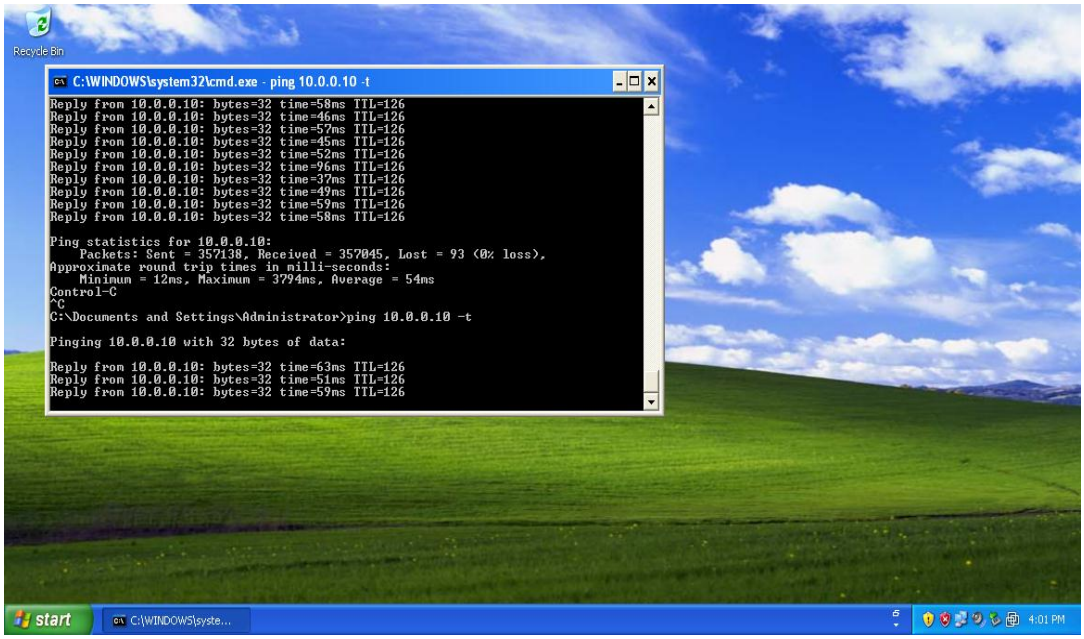
kullanılmıştır. Tünel kurulumu tamamlandıktan sonra oluşturulan sanal bilgisayarların birbirleri ile iletişimi Şekil 3.19., Şekil 3.20., ve Şekil 3.21.'te gösterilmiştir. Yönlendiriciler arasında oluşan sanal özel ağ kurulduğunu gösteren İnternet Güvenlik Anlaşması Anahtar Yönetimi Güvenlik Antlaşması (ISAKAMP SA)'nın aktifliği Şekil 3.22., Şekil 3.23.'da gösterilmiştir.



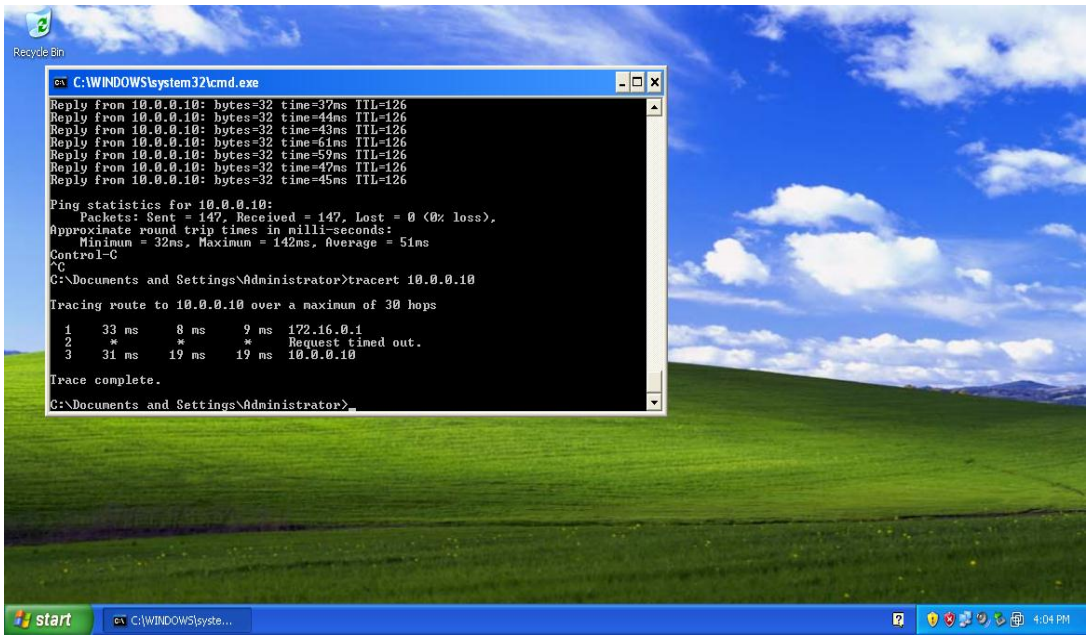
Şekil 3.18. Siteden siteye sanal özel ağ



Şekil 3.19. Sanal bilgisayarlardan atılan ping ve alınan cevaplar



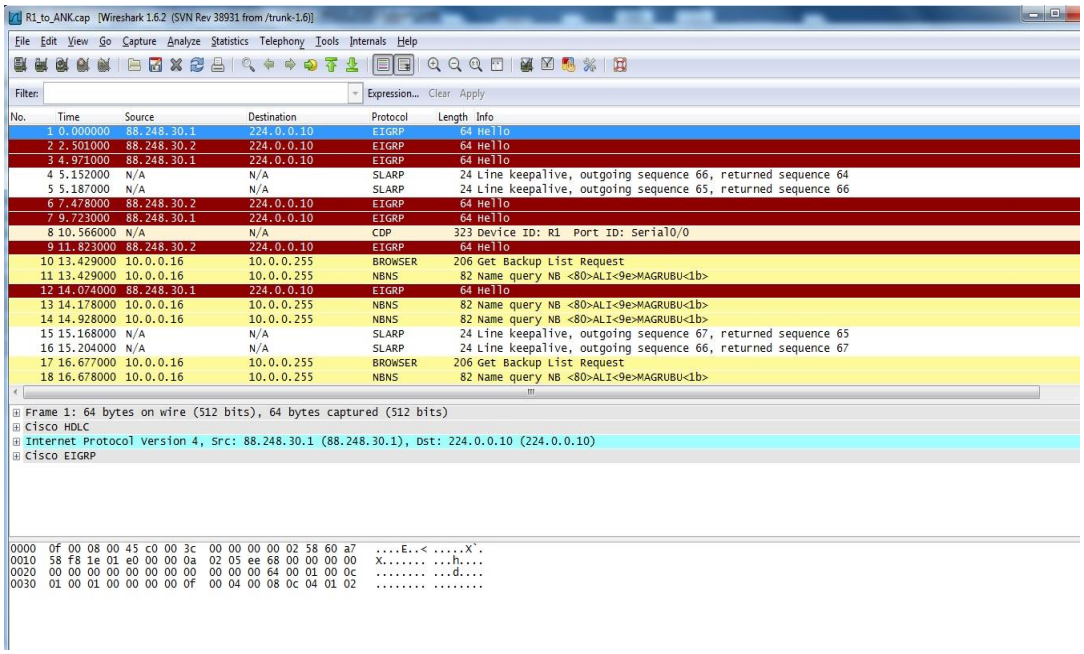
Şekil 3.20. Sanal bilgisayarlardan atılan ping ve alınan cevaplar



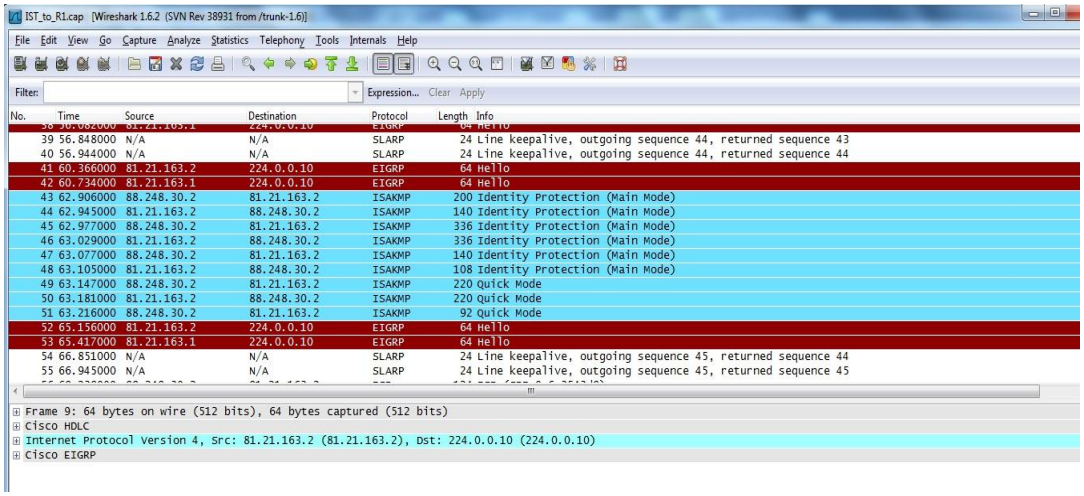
Şekil 3.21. Sanal bilgisayarlardan atılan tracert ve alınan cevap

Şekil 3.22. ANK yönlendiricisinde isakmp doğrulanması

Şekil 3.23. IST yönlendiricisinde isakmp tablosu



Şekil 3.24. ANK yönlendiricisinde eigrp komşuluğu ve hello paketleri



Şekil 3.25. ANK yönlendiricisinde tünelin başlaması

Şekil 3.21.'de kullanılan tracert komutu iletişim esnasında hangi rotayı kullanarak gidileceği için kullanılan bir komuttur. Şekil 3.21'de ilgili bilgisayar kendi ağ geçidi olan yönlendiriciye gittikten sonra adres görünmemektedir. Bunun nedeni ise kullanılan tünel ve şifreleme işlemidir. Tünel başladıktan sonra wireshark programı

ile dinlenen ağlarda gönderimi başlanan merhaba (hello) paketleri Şekil 3.24.'de gösterilmiştir. Kurulumu tamamlanan tünellerde başlayan ISAKAMP trafiği ise Şekil 3.25.'de gösterilmiştir. Siteden siteye sanal özel ağların kimlik doğrulaması için üç seçenek mevcuttur. Bunlar;

- Ön tanımlı anahtar (Pre-share)

- Rsa şifreli anahtar (Rsa-encryption)

- Rsa İmzalı anahtar (Rsa-signature)

Bu proje içerisinde siteden siteye sanal özel ağlarda kullanımı yaygın olan ön tanımlı anahtar (Pre-Share) seçeneği kullanılmıştır. Anahtar değişimi (Key-Exchange) olarak belirtilen anahtar değişimi sırasında kullanılması için Diffie-Helman için grup seçimi gerçekleştirilmiştir. Bu süreç için lifetime olarak 86400 sn belirlenmiştir. Karşı taraf olarak adlandırılan İstanbul (diğer sanal özel ağ eşi) yönlendiricisine Ankara yönlendiricisini sanal özel ağ eşlenmesi sırasından kendini tanıtması için kimliği (identity) tanımlanmıştır. Bu tanıtımı adres olarak yapılması belirlenerek ve Ankara yönlendiricisinin dış IP'si verilmiştir.

Isakamp esnasında kullanılacak olan anahtar (key) seçimi yapıldı. Anahtar seçimi sırasından karşımıza iki seçenek sunulmaktadır: 0 ve 6 numaralı olmak üzere iki seçenek sunulmaktadır. Bu seçeneklerden 0; girilen anahtarı şifrelemeden, 6 ise bu anahtarı şifreleyerek karşı çifte göndermektedir. Burada güvenlik göz önüne alınarak 6 seçilerek. Anahtar seçimi tamamlanmıştır.

IPSEC konfigürasyonu için gerekli transfer-set'lerin oluşturulması için bir adlandırma yapılması gerekmektedir. Daha sonra bu transfer-set setlerinin gönderilmesi için bir şifreleme algoritması seçilmesi gerekmektedir. Bu algoritmalar ise 128b ESP-AES olarak seçilmiştir. Bunun arkasından ESP-SHA-HMAC hash algoritmaları olarak belirlenmiştir.

Bu konfigürasyonlardan sonra yönlendiricilerin arkasında yer alan ağların hangilerinin İstanbul lokasyonuna ulaşması için bir erişim listesi yazılması

gerekmektedir. Bunun için ilgili erişim listesi yazılmıştır. Bu yazılması gereken erişim listesi "Extended Access-list" olması gerekmektedir. Son olarak bu ilgili erişim listesi ilgili projede yer alan seri bacağa uygulanması gerektiğinden ilgili bacağa erişim listesi uygulandı. Erişim listesinin doğru çalışıp çalışmadığının belirlenmesi için eşleme (match) işlemi kontrol edilmiştir.

Sanal özel ağ yapısının düzgün bir şekilde çalışabilmesi için yukarıda bahsedilen işlemleri İstanbul yönlendiricisine da uygulamak gerektiğinde, aynı işlemleri yalnızca anahtar değişimi (Key-exchange) sırasında kullanılan kimlik için gerekli olan adres, İstanbul yönlendiricisinin dış IP'si veriler konfigürasyonu İstanbul yönlendiricisine de uygulanır.

3.2.1. İnternet Güvenlik Protokolü (IPSEC)

İnternet güvenlik protokolü (IPSEC, Internet Protocol Security), ağ katmanında IP güvenliği sağlamak için İnternet Mühendisliği Görev Gücü (IETF, Internet Engineering Task Force) tarafından tanımlanmış protokol takımıdır. IPSEC temelli sanal özel ağ iki kısımdan oluşmaktadır:

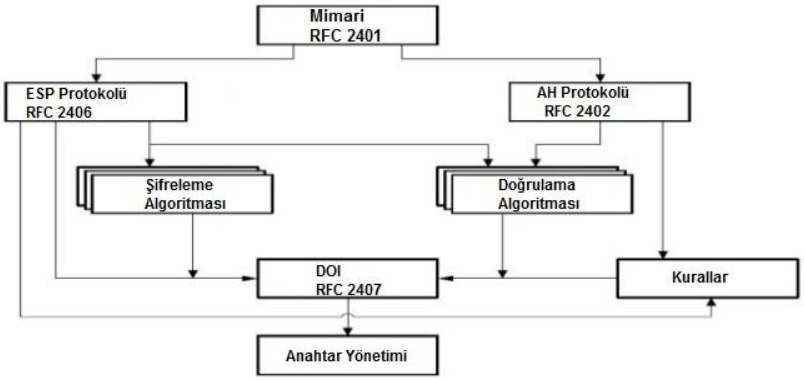
1. İnternet Anahtar Değişim Protokolü (IKE, Internet Key Exchange Protocol)

2. İnternet Güvenlik Protokolü (AH, ESP, tümü)

Birinci kısım, IKE ilk görüşme (negotiation) fazıdır. Bu fazda iki sanal özel ağ uç noktası IP trafiğini hangi metotlar ile güvenlik altına alacağı konusunda anlaşır. Buna ek olarak IKE, Güvenlik ilişkileri (Security Associations-SAs) kurarak bağlantıları yönetir. SA'lar tek yönlüdür ve böylece her IPSEC bağlantısı için iki adet SA bulunur. Diğer kısım ise transfer edilen gerçek IP verisidir. Bu transfer IKE görüşmesinde karar verilen şifreleme ve doğrulama metotları (ESP, AH veya her ikisi) ile yapılır.

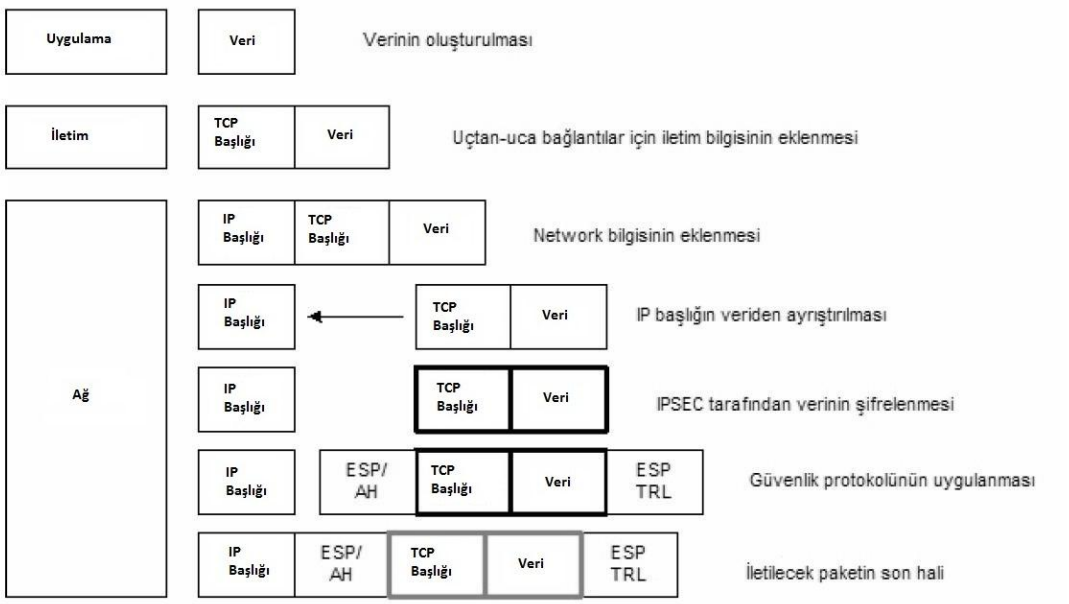
IPSEC Servisleri

	AH	ESP (sadece şifreleme)	ESP (Şifreleme ve kim doğrulama)
Erişim Kontrolü	✓	✓	✓
Connectionless	✓		✓
Veri kimlik doğrulam	✓		✓
Tekrarlanan aynı paketlerin iptali	✓	✓	✓
Güvenilirlik		✓	✓
Trafik akışının limitlenebilmesi		✓	✓



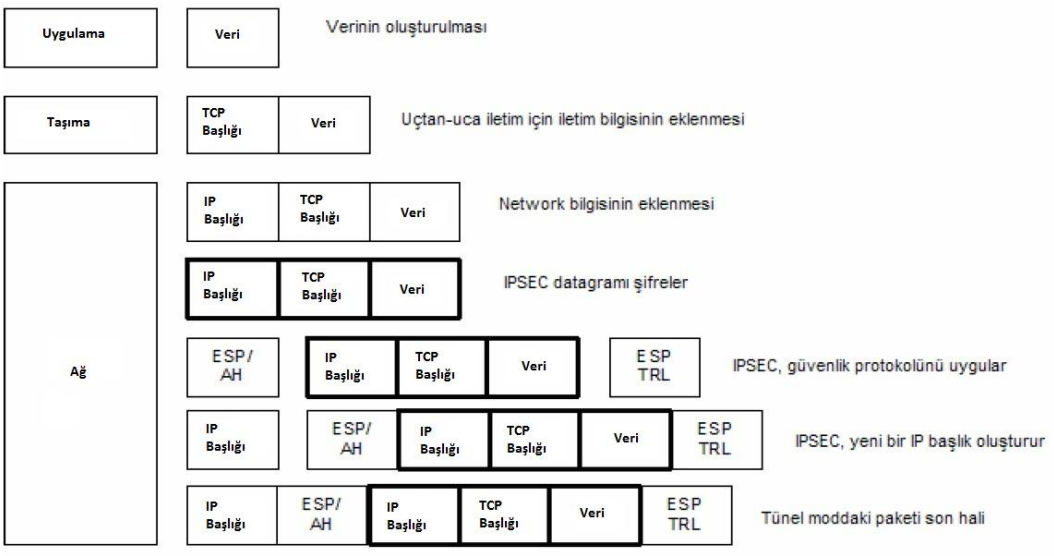
Şekil 3.26. İnternet güvenlik protokolü mimarisi

IPSEC yapısında iki mod söz konusudur; tünel ve iletim modu. Şekil 3.27.'te iletim modu görülmektedir:



Şekil 3.27. İnternet güvenlik protokolü iletim modu

Bu mod da en üst katmandan en alt katmana kadar paketin yönlendirilebilmesi için IP başlık kullanılır.



Şekil 3.28. İnternet güvenlik protokolü tünel modu

Tünel modun da internet güvenlik protokolü paketin son haline gerçek IP adresi eklenir [22].

İnternet Anahtar Değişimi (IKE)

İnternet anahtar değişimi (IKE, Internet Key Exchange): Veriyi şifrelemek ve doğrulamak için gerekli işlemler şifreleme ve doğrulama algoritmaları ve bunlar için gerekli anahtarladır. IKE protokolü bu oturum anahtarlarının (session keys) dağıtımını yapmak ve sanal özel ağ uç noktalarının hangi güvenlik politikalarında anlaşacaklarını kararlaştırmak için kullanılan bir metottur. IKE üç ana göreve sahiptir:

- Uç noktalara karşılıklı doğrulama için yöntem sağlar,
- Yeni IPSEC bağlantıları oluşturur (SA oluşturur),
- Mevcut bağlantıları yönetir.

IKE her bağlantıya SA tahsis ederek bağlantıların izini tutar. SA bir bağlantı için atanmış ESP, AH, oturum anahtarları gibi tüm parametreleri tanımlar. SA tabiatı gereği tek yönlüdür.

IKE ve IPSEC bağlantılarının limitli ömürleri vardır. Bu ömürler zaman (saniye) veya veri miktarı olarak tanımlanır. Bu ömürler bağlantıların çok uzun süreler boyunca kullanılmamasını sağlamak için tanımlanırlar. IPSEC bağlantı ömrü genellikle IKE bağlantı ömründen kısadır ve IPSEC bağlantısı kolaylıkla yenilenebilir.

IPSEC bağlantısı başlatan sanal özel ağ ağ geçidi karşı tarafa bir öneri listesi gönderir. Bu listede bağlantının güvenlik altına alınabilmesi için kullanılabilecek şifreleme, doğrulama metotları bulunur. Üzerinde görüşülen bağlantı veri güvenliğini sağlayan IPSEC bağlantısı olabilir veya IKE bağlantısı güvenliğini sağlayan IKE bağlantısının kendisi olabilir.

Listeyi alan karşı taraf mevcut politikalarına bağlı olarak kendisine en uygun metodu seçer ve bu seçimini karşı tarafa iletir [23].

IKE protokolü güvenli iletişimin en ünlü sorunun çözer: eşlerin kimlik kanıtlama yapması ve simetrik anahtarların değişimi. Bu sayede güvenlik anlaşmaları yapılır ve SAD oluşturulur. IKE protokolü genellikle kullanıcı tarafı sürecine ihtiyaç duyar, işletim sisteminde bir gerçekleştirmesi yoktur. İletişim 500/UDP portunuz kullanır.

IKE protokol fonksiyonları iki safhalıdır. İlk safhada İnternet Güvenlik Anlaşması Anahtar Yönetimi Güvenlik Antlaşması (ISAKMP SA) tesis edilir. İkinci safhada ISAKMP SA kullanılarak IPSEC SA'ları kurulur.

İlk safhada eşlerin kimlik kanıtlaması RSA anahtarları veya X.509 sertifikaları (hatta Kerberos desteğindeki racoon) gibi daha önceden paylaşılan anahtarlara dayanarak yapılır.

İlk safha genellikle iki farklı modu destekler: temel mod ve saldırgan mod. İki mod da eşlerin kimlik kanıtlaması yapar ve bir ISAKMP SA oluşturur ama saldırgan mod bu işi yapmak için temel modun yarısı kadar mesaj kullanır. Bunun sakıncası saldırgan modun kimlik korumasını desteklemediğinden eğer önceden paylaşılmış anahtarla birlikte kullanılırsa aradaki adam saldırılarına karşı korumasız oluşudur. Diğer yandan bu saldırgan modun tek amacıdır. Temel mod, iç işleyişleri yüzünden bilinmeyen eşler için önceden paylaşılmış farklı anahtarların kullanımını desteklemez. Saldırgan mod kimlik korumasını desteklemez ve istemcinin kimliğini açık olarak gönderir. Bu nedenle eşler birbirini kimlik kanıtlaması gerçekleşmeden bilirler ve farklı eşler için önceden paylaşılmış farklı anahtar kullanılabilir.

İkinci safhada IKE protokolü güvenlik anlaşma tekliflerinin karşılıklı değiştirir ve ISAKMP SA sayesinde sonuca bağlar. ISAKMP SA'nın sunduğu kimlik denetimi aradaki adam ataklarına karşı koruma sağlar. İkinci safha hızlı modu kullanır.

Genellikle iki eş sadece bir ISAKMP SA üzerinde anlaşırlar ve bu kullanılarak birçok (en azından iki adet) tek yönlü IPSEC SA'ları kurulur [24].

İnternet Anahtar Değişim Parametreleri: Sanal özel ağ oluşturabilmek için IKE görüşmesi esnasında kullanılabilecek birçok parametre mevcuttur. Sanal özel ağ bağlantısını oluştururken bu parametrelerin iyice anlaşılması ve bu parametrelere dikkat edilmesi gerekmektedir.

Uç Nokta Tanımlamaları:

- Tünel/transport modu

- Main/agresif modu

- IKE şifreleme

- IKE DH grup

- PFS açık/kapalı/kimlik

- IPSEC şifreleme

- IPSEC ömrü

Yerel ve Uzak Ağlar/Bilgisayarlar:

- Uzak ağ geçidi

- IPSEC protokolü (ESP/AH/tümü)

- IKE doğrulama

- IKE ömür

- IPSEC DH grup

- IPSEC doğrulama

İnternet Anahtar Değişimi Kimlik Doğrulama

A. Elle anahtar girişi: Sanal özel ağ konfigürasyonunun en basit yolu elle anahtar girişinden geçer. Bu metot da IKE hiç kullanılmaz ve karşılıklı iki sanal özel ağ uç noktasına şifreleme, doğrulama anahtarları ve diğer parametreler elle girilir.

Avantajları: Düz bir mantığa sahip olduğu için kısmen birlikte çalışabilir (interoperable) bir yapıya sahiptir. Birlikte çalışabilirlik problemleri çoğunlukla IKE'de yaşanır. Elle anahtar girişi IKE'yi tamamıyla baypas eder. SA'lar bizzat tanımlanır.

Dezavantajları: IKE kullanımından önce geliştirilmiştir ve ilkel bir metottur. Böylelikle IKE'nin fonksiyonelliklerinden uzaktır. Bu yüzden bazı limitlemeleri vardır, örneğin her zaman aynı anahtarlar kullanılır ve inkâr edememe özelliği eksiktir. Bu tip bağlantı yeniden gönderme saldırısı (reply attacks) olarak adlandırılan saldırılara karşı açıktır, Üçüncü bir şahıs belirli bir zamanda gönderilen şifreli paketleri kaydeder ve bir müddet sonra tekrar gönderir. Sanal özel ağ uç noktası paketin sonradan gönderildiğini algılayamaz ve gerekli tedbiri alamaz. IKE bu güvenlik açığını kapatmaktadır.

B. Ön tanımlı anahtarlama (PSK, Pre-Shared Keying): Sanal özel ağ uç noktaları gizli bir anahtarı paylaşır. Bu servis IKE tarafından sağlanır ve bu servis PSK metodunu elle anahtar girişi metoduna kıyasla esnek kılar.

Avantajları: Elle anahtar girişi metoduna kıyasla birçok avantajı vardır. Örneğin; uç nokta doğrulaması sağlar, tünel ömürleri tanımlanabilir, yeni anahtar tanımlanabilir.

Dezavantajları: Ön tanımlı anahtarlama metodunda en ciddi dezavantaj anahtar dağıtımı sorunudur. Gizli anahtarlar uç nokta sanal özel ağ geçitlerine veya istemcilerine güvenli bir şekilde nasıl dağıtılacaktır.

C. Sertifika: Her sanal özel ağ geçidi kendisine ait özel sertifikaya ve bir veya birden çok kök sertifikasına sahiptir. Her uç nokta, sertifikasında bulunan bir açık

anahtara denk gelen bir özel anahtara sahiptir ve bu özel anahtar sadece kendisinde bulunur.

Avantajları: Birçok sanal özel ağ istemcisi ön tanımlı anahtar olmadan yönetilebilir, bir istemcinin sertifikası başkası tarafından ele geçirilmişse, sadece o istemcinin sertifikası iptal edilir veya yenilenir, diğer sanal özel ağ geçitleri/istemcileri için yeniden sertifikalandırma çalışmasına gerek yoktur.

Dezavantajları: İyi bir yönetim yazılımı olmadan yönetilmesi güçtür.

İnternet Güvenlik Protokolleri (ESP, AH)
IPSEC protokolleri (AH ve ESP) sanal özel ağ geçitleri arasındaki gerçek veri trafiğini korumak amacı ile kullanılır.

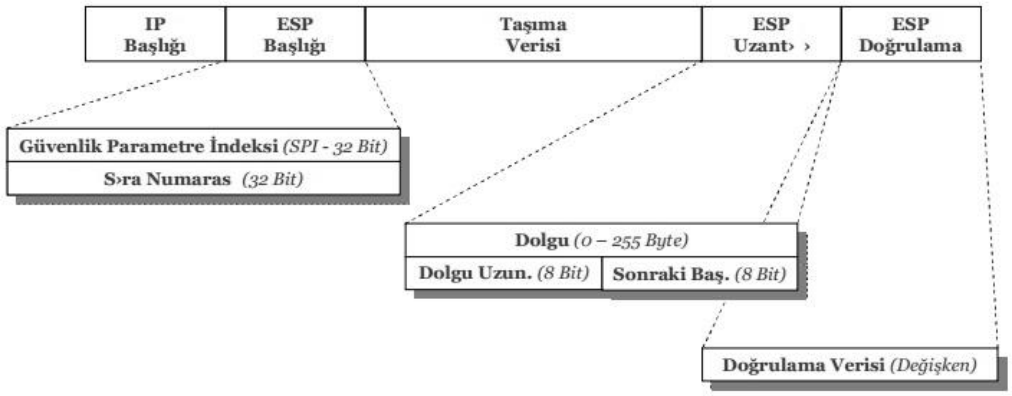
Doğrulama Başlığı (AH)
Doğrulama başlığı (AH, Authentication Header): Veri akışını doğrulamak için kullanılan bir protokoldür. IP paketinde bulunan veriden MAC oluşturmak için hash fonksiyonu kullanır. Elde edilen MAC, karşı tarafa mesajın bütünlüğünün korunduğunun anlaşılması için orijinal paketle birlikte iletilir [25].

Şekil 3.29. Pakete doğrulama başlığı uygulanması

AH protokolü IP paket verisinin yanı sıra IP başlığının parçalarını da doğrular. AH protokolü IP başlığından sonra pakete AH başlığı yerleştirir. Bu protokol ile adres yanıltma ve yeniden yönlendirme atakları (spoofing ve replay) önlenir. Bu tip atakları bir yetkilendirme fonksiyonu olan ve simetrik anahtar yapısına sahip olan MAC tekniği ile önler. AH, şifreleme işlemi için MD5 hesaplama metodu kullanır. AH protokolünün şifreleme için HMAC-MD5-96 ve HMAC-SHA-1-96 MD5 standartlarını kullanır.

3.2.2. Kapsülleyen Güvenlik Veri Yükü (ESP)

IPSEC, ESP protokolü IP paketleri için, doğrulama, şifreleme ile veri gizliliği ve seçime bağlı olarak tekrarlama saldırılarına karşı koruma sağlar [26].



Şekil 3.30. Pakete kapsülleyen güvenlik veri yükü uygulanması

ESP protokolü IP başlığından sonra pakete ESP başlığı yerleştirir. ESP başlığından sonraki tüm veri şifrelenmektedir ve/veya doğrulanmaktadır. AH protokolünden farkı ESP protokolü IP paketinin şifrelenmesini de sağlamaktadır. ESP kimlik doğrulama işlemleri için aşağıdaki teknikleri kullanmaktadır:

- DES/CBC

- 3DES

- RC5

- IDEA

- 3 IDEA

- CAST

- BLOWFISH

3.3. Dinamik Çok Noktalı Sanal Özel Ağ (DM VPN)

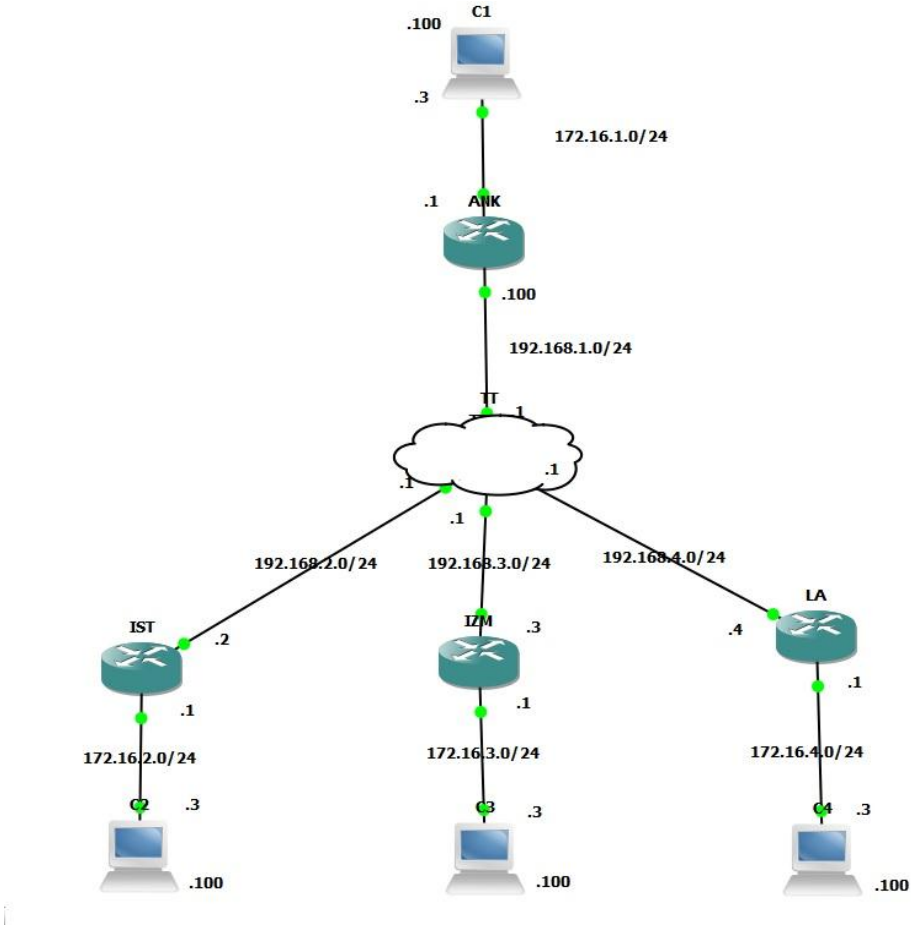
Dinamik çok noktalı sanal özel ağ (Dmvpn, Dynamic Multipoint Virtual Private Network) için hazırlanan senaryo Şekil 3.31.'de gösterilmiştir. Yapılandırmaya başlarken ilk olarak ilgili lokasyonlara ait yönlendiricilere ait bacakların IP adresleri verilmiştir. Burada siteden siteye sanal özel ağ örneğinde olduğu gibi hem dış-gerçek yani Türk Telekom ya da hangi servis sağlayıcıdan internet hizmeti alınıyor ise ilgili sağlayıcının vermiş olduğu IP'ler ve iç ağda kullanılan iç IP'ler mevcuttur.

Temel konfigürasyon ilgili yönlendiricilere IP adresini atamaktan oluşmaktadır. Bu aşamadan sonra yapılacak TT tarafından internete çıkılması için hizmet veren ilgili yönlendiricilere herhangi bir işlem yapılmaması gerekmektedir. İlgili IP adresleri atamaları gerçekleştirdikten sonra ikinci aşama olan ve bölüm 10.1. NHRP ve bölüm 10.2 MGRE konularında bahsedilen MGRE ile tünel oluşturma işlemleri yer almaktadır. İlk olarak 0 numarasına sahip bir tünel oluşturulmuştur (TT için bu işlem gerçekleştirilmemektedir). Her bir yönlendirici için ilgili tünele ait IP adresleri tanımlanmıştır. Bu işlem sonrasında NHRP için gerekli olan haritayı oluşturmak için burada merkez/şube topolojisi kullanıldığından sonraki durak olarak ANK isimli yönlendiriciye ait tünel adresi verilmiştir. Ve bu haritanın çoklu yayın (multicast) olarak hizmet vereceği belirlenmiştir. NHRP için gerekli ağ 1 olarak belirlenmiştir.

İlgili iç ağdan çıkıldıktan sonraki düğüm sunucusu belirtilmiştir, bu sunucunun ANK lokasyonuna ait tünel IP'si olması gerekmektedir. Bu ayarlamayı tamamladıktan sonra tünel için bir kaynak adresi verilmesi gerekmektedir. Bu kaynak adresi ise ilgili lokasyona ait servis sağlayıcı (TT) tarafından verilen ilgili dış IP tanımlanmak zorundadır. Ayrıca tünel modunun belirlenmesi gerekmektedir. Bunu ise trasport olarak belirlenmiştir. Bu takip eden aşmada ise bir maksimum iletim birimi (mtu, maximum transmission unit) değeri verilmesi gerekmektedir. Bu değeri ise 1416 olarak belirlenmiştir.

İkinci konfigürasyon kısmı tamamlandıktan sonra bölüm 10.3 IPSEC'te bahsedilen konfigürasyonlara gelinmiştir. Burada ise Isakamp şifrelenmesi için gerekli 10 (istediğiniz sayı verilebilir ancak hepsinde bu kural isminin aynı olması gerekmektedir) isimli bir kural oluşturulmuştur. Burada kullanılması zorunlu olan hash algoritması MD5 olarak belirlenmiştir. Sonrasında şifreleme için 3DES kullanması tercih edildi. Kimlik denetleme (Authontication) için ön tanımlı (pre-share) seçimi gerçekleştirilmiştir. Takip eden aşamada kimlik denetleme işlemini gerçekleştirmek için anahtar tanımlaması yapılmıştır. Siteden siteye sanal özel ağ konfigürasyonunda da belirtilen anahtar seçimi iki şekilde belirlenmektedir. Bunlar 0 ve 6 seçimi yapılarak gerçekleştirilebilmektedir. Burada 0 seçilirse şifresiz bir şekilde görülmektedir, 6 seçilirse şifrelenerek görülmesini gizlenebilmektedir. Burada seçim 6'dan yana kullanılarak ilgili şifre girilmiştir. Bu aşama sonrasında ise bir transform-set oluşturulmuştur. Sonrasında ilgili tünel korunması için bir IPSEC profili oluşturulmuştur ve ilgili oluşturulan transform-set'i bu protection un altına uygulanmıştır. Sonrasında ilgili tünele bu profil uygulanmıştır.

Son olarak farklı lokasyonlar da mevcut olan lokasyonların her birinin haberleşmesi için ilgili EIGRP yönlendirme protokolü ilgili lokasyonlara uygulanmıştır (TT bu konfigürasyonlardan muaf tutulmuştur).

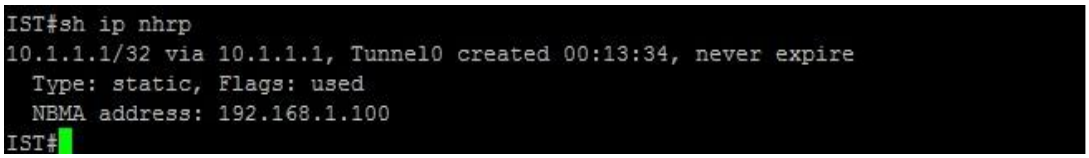


Şekil 3.31. Dinamik Çok Noktalı Sanal Özel Ağ

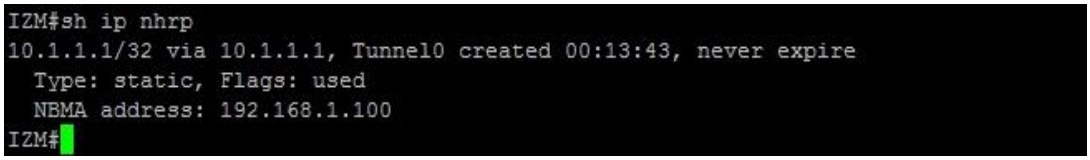
Dinamik çok noktalı sanal özel ağ mimarisinin temellerinden olan gelecek durak karar tabloları HUB, IST, IZM ve LA yönlendiriciler için sırası ile Şekil 3.32., Şekil 3.33., Şekil 3.34. ve Şekil 3.35.'de gösterilmiştir.

```
HUB#sh ip nhrp
10.1.1.2/32 via 10.1.1.2, Tunnel0 created 00:13:08, expire 01:46:51
  Type: dynamic, Flags: unique registered
  NBMA address: 192.168.2.2
10.1.1.3/32 via 10.1.1.3, Tunnel0 created 00:13:08, expire 01:46:52
  Type: dynamic, Flags: unique registered
  NBMA address: 192.168.3.3
10.1.1.4/32 via 10.1.1.4, Tunnel0 created 00:13:08, expire 01:46:51
  Type: dynamic, Flags: unique registered
  NBMA address: 192.168.4.4
HUB#
```

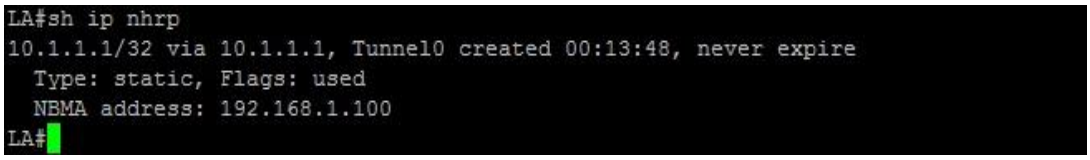
Şekil 3.32. HUB yönlendiricisine ait nhrp tablosu



Şekil 3.33. IST yönlendiricisine ait nhrp tablosu



Şekil 3.34. IZM yönlendiricisine ait nhrp tablosu



Şekil 3.35. LA yönlendiricisine ait nhrp tablosu

Dinamik çok noktalı sanal özel ağ topolojisinde lokasyonlarda bulunan yönlendiricilerin eş olarak hangi lokasyonları gördükleri dmvpn tablosundan anlaşılmaktadır. Bu tablolar HUB, IST, IZM ve LA yönlendiriciler için sırası ile Şekil 3.36., Şekil 3.37., Şekil 3.38. ve Şekil 3.39.'da gösterilmiştir.

```
HUB#sh dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incompletea
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer

Tunnel0, Type:Hub, NHRP Peers:3,
 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1     192.168.2.2        10.1.1.2    UP    never D
     1     192.168.3.3        10.1.1.3    UP    never D
     1     192.168.4.4        10.1.1.4    UP    never D

HUB#
```

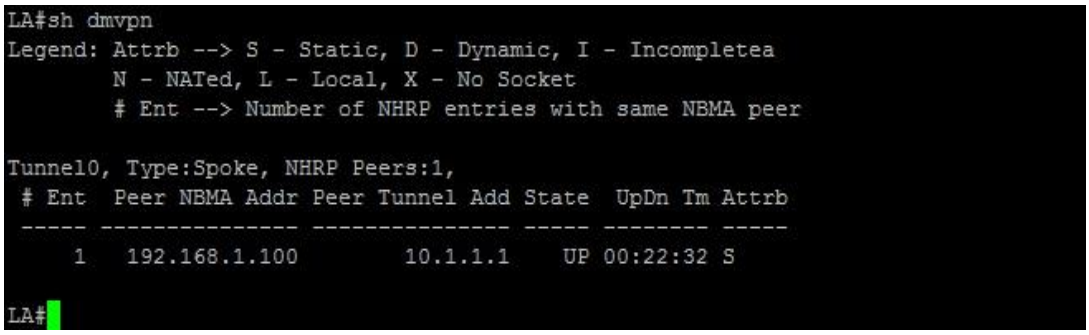
Şekil 3.36. HUB yönlendiricisine ait dmvpn tablosu

```
IST#sh dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incompletea
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer

Tunnel0, Type:Spoke, NHRP Peers:1,
 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1   192.168.1.100        10.1.1.1    UP 00:22:17 S

IST#
```

Şekil 3.37. IST yönlendiricisine ait dmvpn tablosu

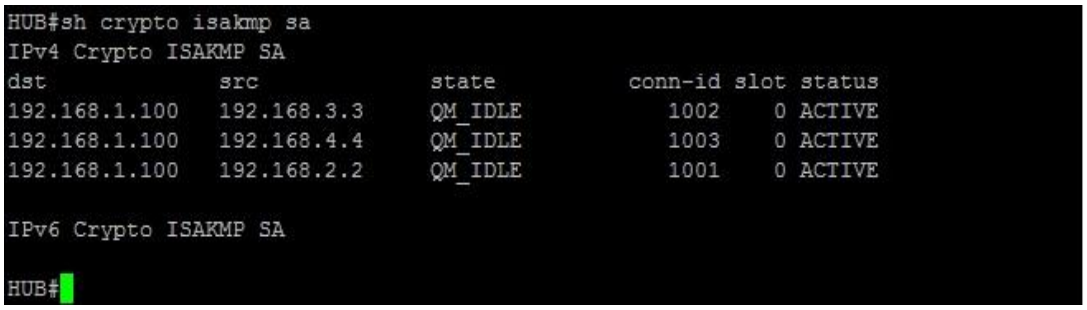
```
IZM#sh dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incompletea
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer

Tunnel0, Type:Spoke, NHRP Peers:1,
 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1   192.168.1.100        10.1.1.1    UP 00:22:25 S

IZM#
```

Şekil 3.38. IZM yönlendiricisine ait dmvpn tablosu

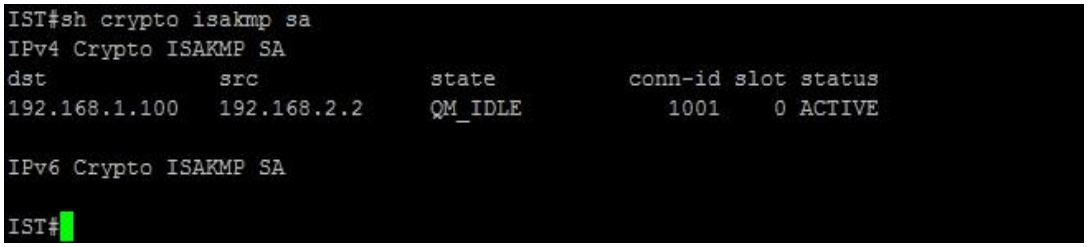


Şekil 3.39. LA yönlendiricisine ait dmvpn tablosu

Sanal özel ağ'larda tünelin sağlıklı bir şekilde kurulduğunu gösteren ISAKAMP SA' leri ise HUB, IST, IZM ve LA yönlendiriciler için sırası ile Şekil 3.40., Şekil 3.41., Şekil 3.42. ve Şekil 3.43.'da gösterilmiştir.



Şekil 3.40. HUB yönlendiricisine ait isakamp tablosu



Şekil 3.41. IST yönlendiricisine ait isakamp tablosu

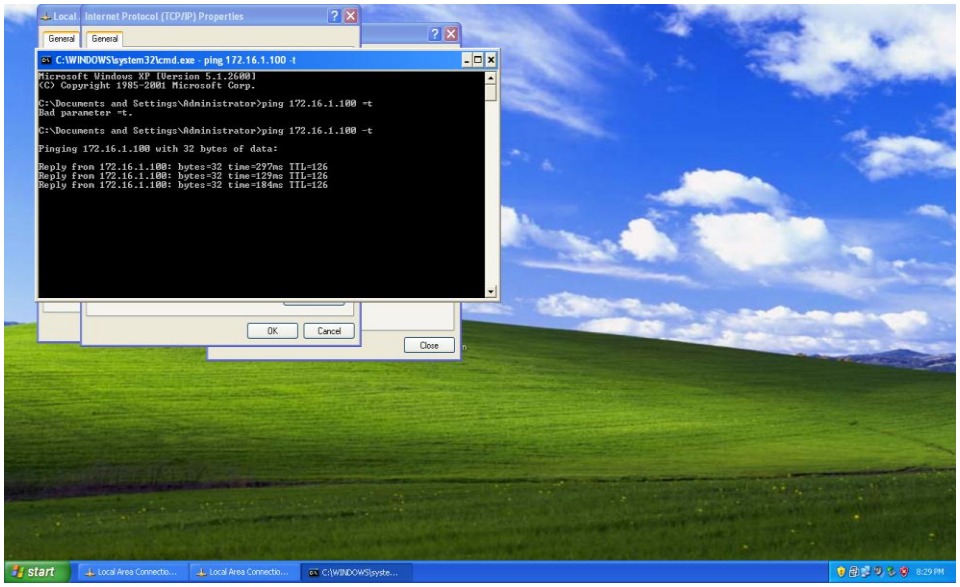
```
IZM#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
192.168.1.100   192.168.3.3     QM_IDLE           1001    0 ACTIVE

IPv6 Crypto ISAKMP SA

IZM#
```

Şekil 3.42. IZM yönlendiricisine ait isakamp tablosu

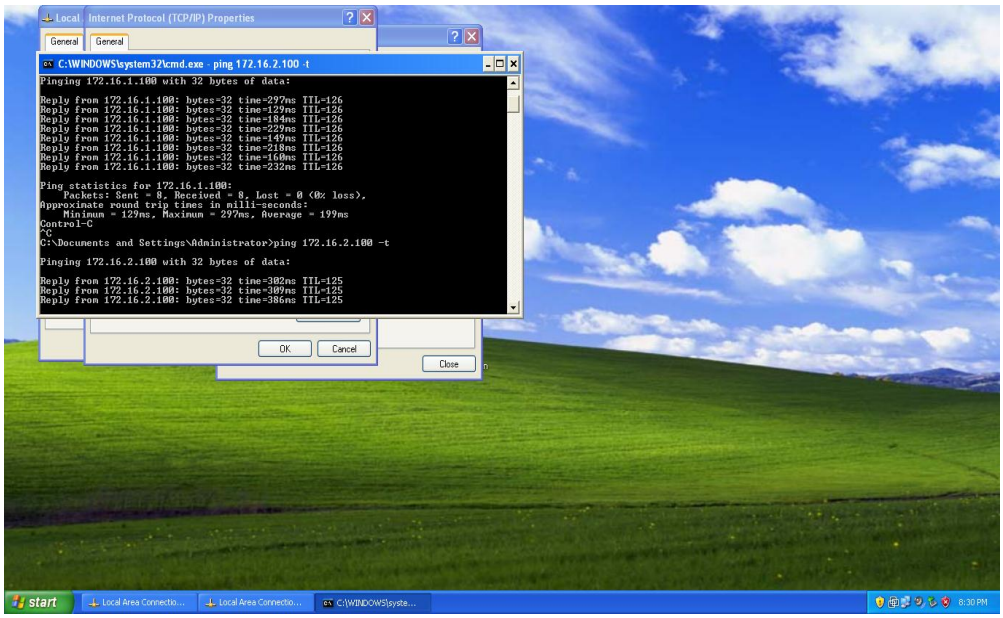
```
LA#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
192.168.1.100   192.168.4.4     QM_IDLE           1001    0 ACTIVE

IPv6 Crypto ISAKMP SA
```

Şekil 3.43. LA yönlendiricisine ait isakamp tablosu

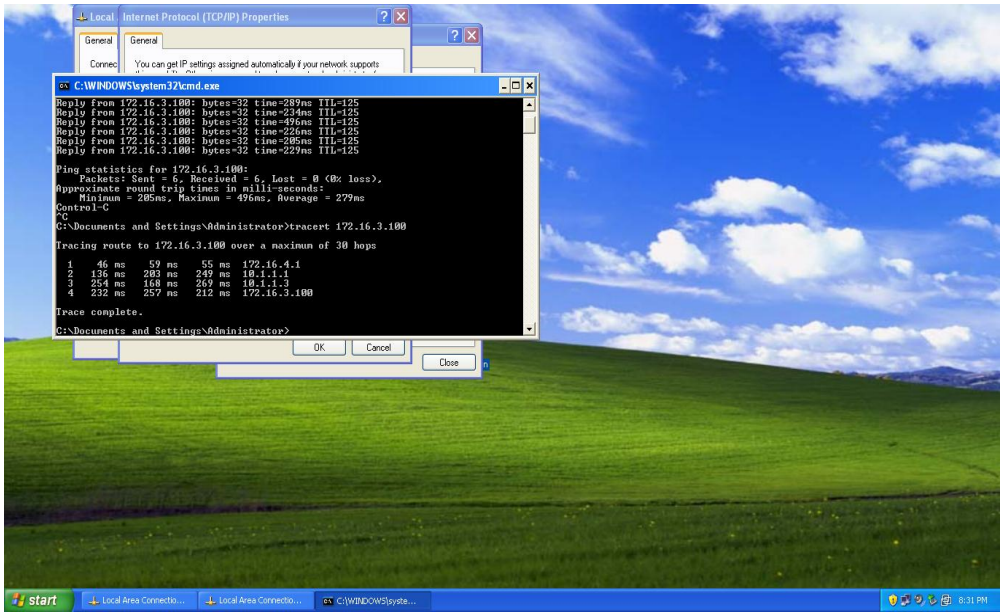
Lokasyonlarda yer alan sanal bilgisayarlardan diğer lokasyonlarda bulunan sanal bilgisayarlarla iletişiminin testi için ping komutunun uygulandığı ve alınan sonuçların başarılı olduğu Şekil 3.44., Şekil 3.45. ve Şekil 3.46.'te gösterilmiştir.



Şekil 3.44. İlgili sanal bilgisayardan diğer bilgisayar ping işlemi



Şekil 3.45. İlgili sanal bilgisayardan diğer bilgisayar "ping" işlemi



Şekil 3.46. İlgili sanal bilgisayardan diğer bilgisayar "tracert" işlemi

3.3.1. Gelecek Durak Karar Protokolü (NHRP)

Bu özellik sayesinde her bir şube, merkeze tünelle bağlı olan diğer şubelerin fiziksel ve tünel adreslerini öğrenerek bu bilgileri hafızasına alır. Bu işlemler sırasında merkez NHS (Next Hop Server), şubeler ise NHC (Next Hop Client) görevi görürler [27].

3.3.2. Çok Noktalı Genel Yönlendirme Kapsülü (MGre)

Normal GRE tünelinin her bir şube için yeni bir tünel ara yüzü oluşturması özelliğini ortadan kaldırarak bir tünel ara yüzünde birden fazla tünel desteklemesini sağlar. NHRP konfigürasyonuyla aktif hale gelir [28].

3.3.3. İnternet Güvenlik Protokolü (IPSEC)

IP paketlerinin güvenli olarak hedefe ulaşmasını sağlayan protokoldür. Detay Bkz. Bölüm 3.2.1.

3.4. Siteden Siteye Sanal Özel Ağ Ve Dinamik Çok Noktalı Sanal Özel Ağ Karşılaştırmalı İncelenmesi

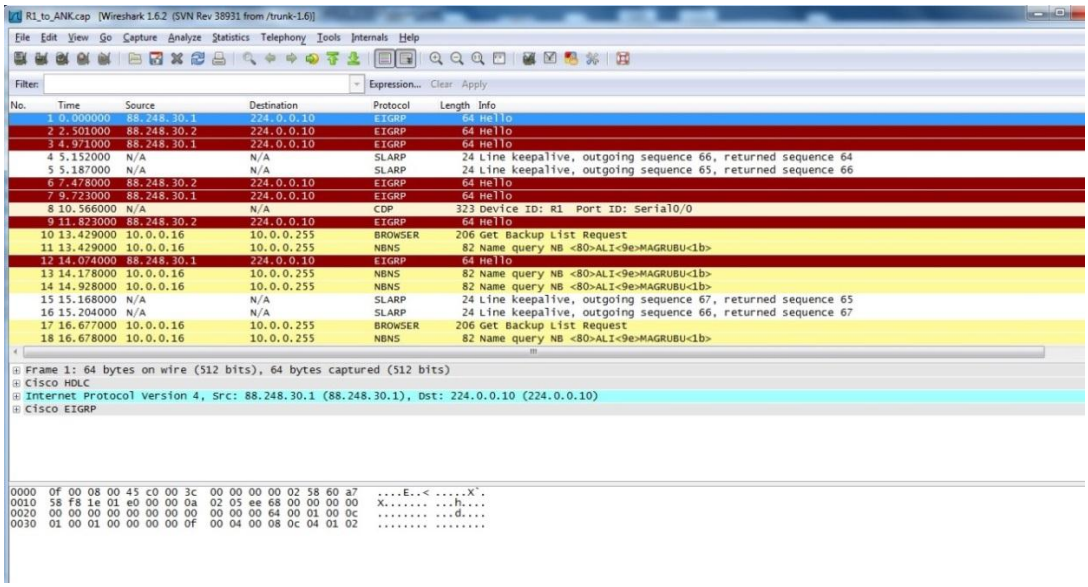
Her iki uygulamada da benzer yönlendiricisineler ve bilgisayarlar kullanılmıştır. Mevcut lokasyonların fazla olması nedeni ile gerçek cihaz kullanımı yerine sanal cihaz kullanımı tercih edilmiştir. Gerçeği ile en yakın sonucu veren benzetim/sanallaştırma uygulamaları araştırılıp, en uygun olan uygulamalar belirlenmiştir.

Yönlendiriciler için GNS3 benzerim uygulaması, sanal bilgisayarlar için Vmware sanallaştırma uygulaması kullanılmıştır. Yönlendirici seçimi Cisco marka 3700 serisinden yapılmıştır. Sanal bilgisayarlara kullanım kolaylığı açısından Win98 işletim sistemi yüklenip, ilgili IP adresleri verilmiştir.

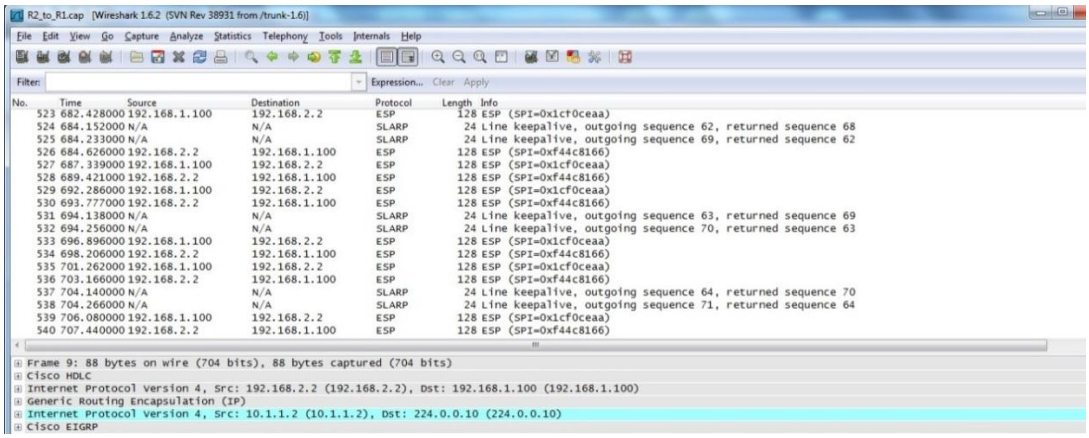
Siteden siteye sanal özel ağ uygulamasından EIGRP yönlendirme protokolü, tünel haberleşmesi için internet güvenlik anlaşması protokolü (ISAKMP) ve internet güvenlik protokolü (IPSEC) kullanılmıştır.

Dinamik çok noktalı sanal özel ağ uygulamasında EIGRP yönlendirme protokolü, tünel haberleşmesi için internet güvenlik anlaşması protokolü (ISAKMP), internet güvenlik protokolü (IPSEC), gelecek karar protokolü (NHRP), çok noktalı genel yönlendirme kapsülü (MGRE) kullanılmıştır.

Oluşturulan sanal bilgisayarlar GNS3 uygulaması ile ethernet bağdaştırıcıları vasıtasıyla eşleştirilerek her lokasyondan sanal makinalar üzerin veri gönderme işlemleri gerçekleştirilmiştir. Siteden siteye sanal özel ağ yapılandırılması ve dinamik çok noktalı sanal özel ağ uygulamalarının yapılandırmaları tamamlandıktan sonra iki uygulamaya da eş değer paket verileri gönderilmiştir. İlgili paketler şifreli olduklarından aralarında fark gözlemlenmemiştir. Bunlar dışında yapılan konfigürasyonalar da siteden siteye sanal özel ağ uygulamalarında ağa katılan her lokasyon için ekte belirtilen ayarların hepsi hem ana yönlendirici için hem de eklenen yeni lokasyona ait yönlendirici için uygulanması gerektiği tespit edilmiştir. Dinamik çok noktalı sanal özel ağ için ise başlangıçta yapılan konfigürasyonlara ek bir konfigürasyon gerekmemekte olup yalnızca yeni ağın eklenmesi ve yeni eklenen lokasyona ilgili konfigürasyonların eklenmesi ile sanal özel ağımızın eklenmiş olduğu sonucuna ulaşılmıştır. Bu yapılan konfigürasyonlar dinamik çok noktalı sanal ağı konfigürasyon açısından dolaylı olarak performans ve maliyet açısından daha avantajlı olduğu görülmüştür. Gönderilen paket sonuçları Şekil 3.47.'da ve Şekil 3.48.'de gösterilmiştir.



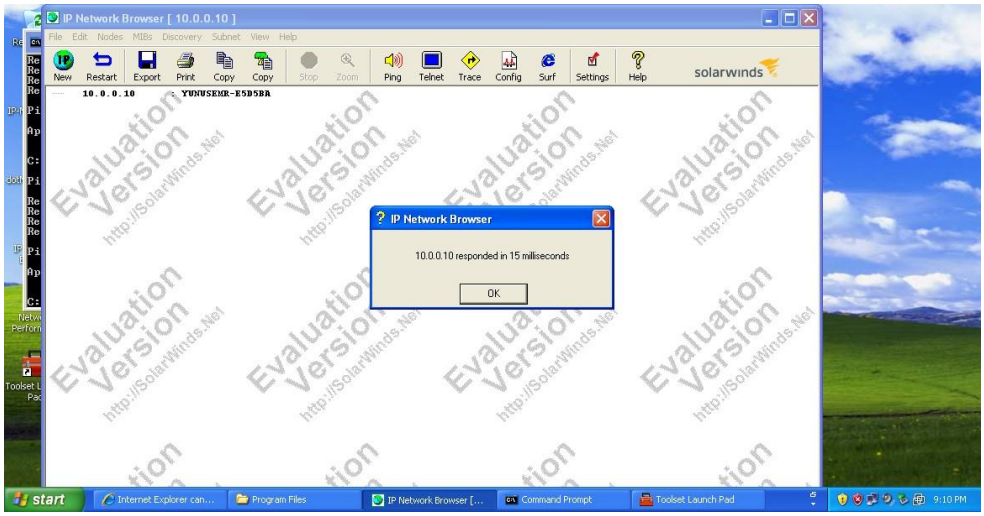
Şekil 3.47. Siteden siteye sanal özel uygulamasına gönderilen paket (ping)



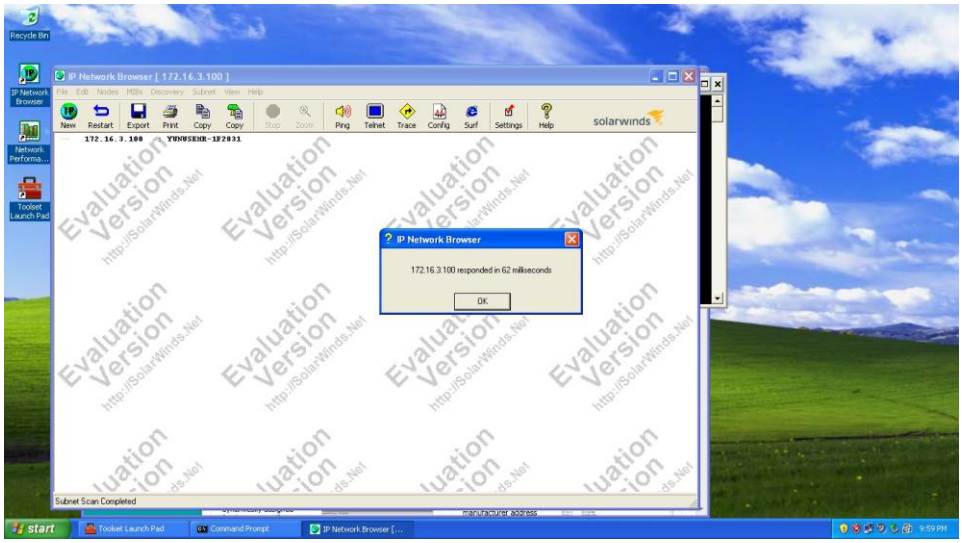
Şekil 3.48. Dinamik çok noktalı sanal özel uygulamasına gönderilen paket (ping)

Siteden siteye sanal özel ağ uygulaması ve Dinamik çok noktalı sanal özel ağ uygulaması için yapılan çalışmaların karşılaştırması yapılırken zaman açısından da değerlendirilmesi yapılmıştır. Bu süre işlemi için iki tarafın haberleşmesini gösteren ping işlemi uygulanmıştır. Lokasyonlar arasında mevcut sanal bilgisayarlar arasında yapılan işlem milisaniye cinsinden gösterilmiştir. Şekil 3.49. ‘da Siteden siteye sanal özel ağ uygulaması için hazırlanan topolojide yer alan iki farklı lokasyonda mevcut sanal bilgisayarlar arasından gerçekleşen ping işleminin 15 milisaniye olduğu

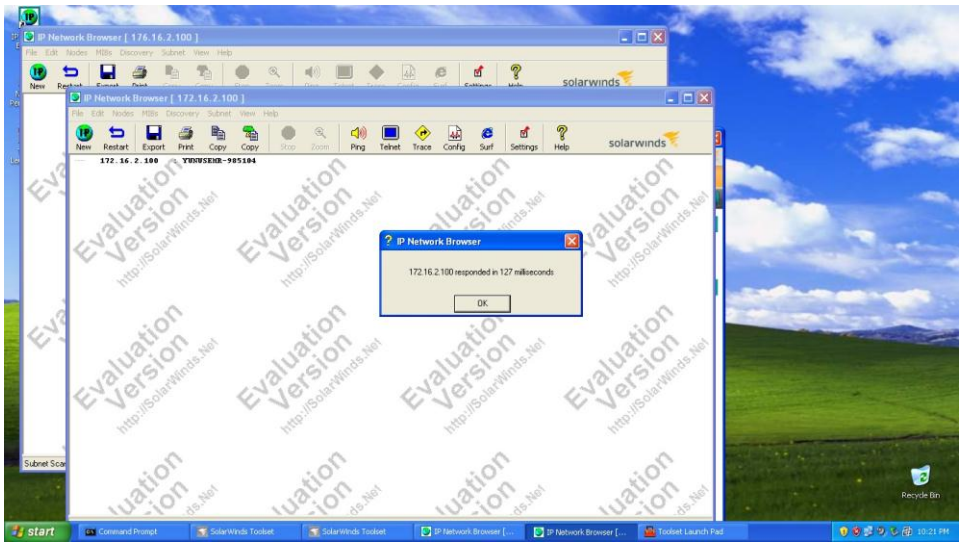
gösterilmiştir. Şekil 3.50., Şekil 3.51. ve Şekil 3.52.'da Dinamik çok noktalı sanal özel ağ uygulaması için hazırlanan topolojide yer alan sırasıyla merkez/şube, şube/şube ve Şube/merkez arasında gerçekleşen ping işlemlerinin 62 milisaniye,127 milisaniye,55 milisaniye olduğu gösterilmiştir.



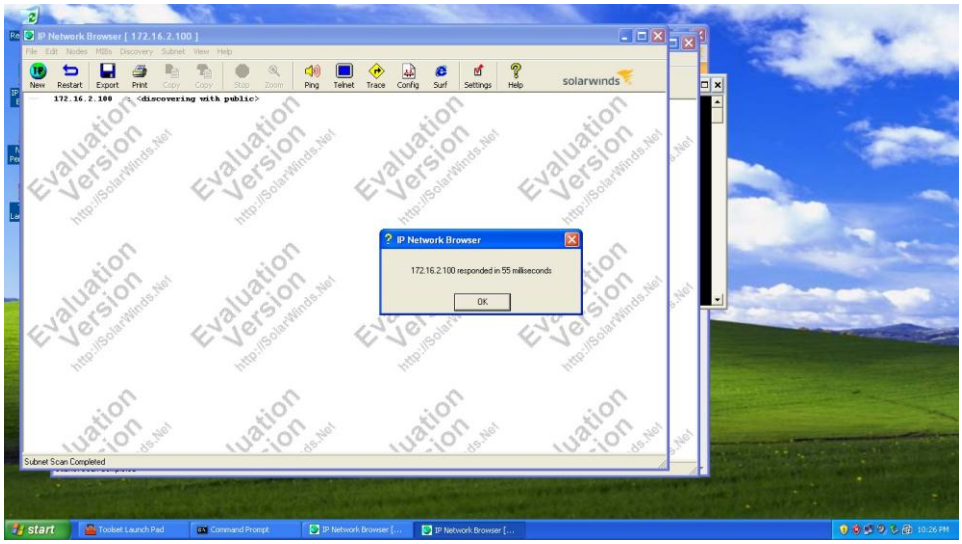
Şekil 3.49. Siteden siteye sanal özel ağ uygulamasında yer alan iki lokasyon arasında mevcut sanal bilgisayarlar arasındaki ping işleminin süresi



Şekil 3.50. Dinamik çok noktalı sanal özel uygulamasında yer alan merkez lokasyon ve şube lokasyon arasında mevcut sanal bilgisayarlar arasındaki ping işleminin süresi



Şekil 3.51. Dinamik çok noktalı sanal özel uygulamasında yer alan iki şube lokasyon arasında mevcut sanal bilgisayarlar arasındaki ping işleminin süresi



Şekil 3.52. Dinamik çok noktalı sanal özel uygulamasında yer alan şube ve merkez lokasyon arasında mevcut sanal bilgisayarlar arasındaki ping işleminin süresi

Avantajları/Dezavantajları:

- Siteden siteye sanal özel ağ iki site arasından şifreleme imkânı sağlar.

- Dinamik çok noktalı sanal özel ağ noktadan noktaya genel yönlendirme şifrelemesi sunar.

- Siteden siteye sanal özel ağ birden fazla tedarikçi (multivendor) desteği sunar.

- Dinamik çok noktalı sanal özel ağ yalnızca Cisco yönlendiricilerde çalışır. (Ancak Huawei dsvpn olarak kullanılmaktadır)

- Siteden siteye sanal özel ağ'da binlerce yönlendirici kullanılabilir.

- Dinamik çok noktalı sanal özel ağ'da binlerce merkez-şube yapısında kullanılabilir.

- Siteden siteye sanal özel ağ'da küçük ölçekli ve yönetilebilir mesh topolojisinde kullanılır ve tünel sürekli açıktır.

- Dinamik çok noktalı sanal özel ağ çok büyük ölçekli yapılarda tercih edilir ve tüneli trafik başladığında açar, trafik kesilince tüneli kapatır.

- Siteden siteye sanal özel ağ yönlendirme protokollerini desteklemez.

- Dinamik çok noktalı sanal özel ağ yönlendirme protokollerini destekler.

- Siteden siteye sanal özel ağ yedeksiz yapılarda devamlılık süresi fazladır.

- Dinamik çok noktalı sanal özel yönlendirme yapılarından devamlılık süresi fazladır.

- Siteden siteye sanal özel ağ uygulaması az noktalı olan ve trafiğin merkezde olmasında sorun teşkil etmeyecek yapılarda kullanılması tercih edilir.

- Dinamik çok noktalı sanal özel ağ yapısında yalnızca yeni eklenen lokasyon konfigürasyonu yapılır.

- Dinamik çok noktalı sanal özel ağ yapısında topolojiye göre istenirse tüm trafik merkez üzerinden geçirilir, istenmez ise merkez trafikten etkilenmez.

- Dinamik çok noktalı sanal özel ağ yapısında konfigürasyon siteden siteye sanal özel ağ yapısına nazaran daha azdır.

- Siteden siteye sanal özel ağ konfigürasyonları ağa dâhil olan her lokasyon ve merkez için tekrar tekrar girilmesi gerekmektedir.

- Siteden siteye sanal özel ağ yapısından trafik her zaman merkez üzerinden geçmek zorundadır.

4. SONUÇLAR

Bu çalışma içerisinde genel bilgisayar ağlarına bir giriş yapılıp, bu konu hakkında genel bilgiler verilmiştir. Genel bilgileri takiben sanal özel ağ mimarisine giriş yapılıp ve bu konu hakkında detaylı bilgiler verilmiştir. Siteden siteye sanal özel ağ topolojisi GNS3 benzetim uygulaması kullanılarak hazırlanmıştır. Hazırlanan topolojide ilgili yönlendiricilerin yapılandırması tamamlanmıştır. Topolojide yer alan yerleşkelerin birbirleri ile haberleşip haberleşmedikleri test edilip, ekran görüntüleri konulmuştur. Gerekli yapılandırmalar dinamik çok noktalı sanal özel ağ için de gerçekleştirilmiştir. İlgili yerleşkelerin birbirleri ile haberleşip haberleşmedikleri test edilip ekran görüntüleri konulmuştur. Hazırlanan topolojilere Vmware sanal uygulaması kullanılarak sanal bilgisayarlar ile çalışır hale getirilmiştir.

Bu çalışmada bilgisayarların haberleşmeleri ping komutu ile test edilmiştir. Bu nedenle gönderilen paket boyutları eş değer olarak görülmüştür. Aynı zamanda haberleşme hızları kıyaslandığında kayda değer farklar gözlemlenmemiştir. Her iki uygulamada da cihaz maliyetleri açısından da fark olmadığı görülmüştür. Ancak performansları detaylı incelendiğinde, dinamik çok noktalı sanal özel ağ yapılandırmasının sanal özel ağ yapılandırmasından daha kolay ve az olması nedeni ile genel ağ trafiğini rahatlattığı gözlenmiştir.

Sonuç olarak çok noktaya sahip kullanıcılar (yurt dışı ofisleri olan firmalar, bankalar, yurt içi birden çok noktaya sahip holdingler) için siteden siteye sanal özel ağ uygulamasından ziyade çok noktalı sanal özel ağ uygulamasının binlerce merkez/şube yapısını desteklemesi, tüneli trafik başladığında başlatması bittiğinde kesmesi, yönlendirme protokollerinde devamlılık süresinin fazla olması, yalnızca yeni eklenen lokasyona ilgili konfigürasyon kolaylığı sağlaması, daha az konfigürasyon dolayısıyla daha az kaynak tüketimi nedenlerinden dolayı faydalı olacağı sonucuna varılmıştır.

KAYNAKLAR

[1] Gupta, Meeta (2002) Building A Virtual Private Network, Cincinnati, OH: Premier Press Inc.

[2] Chen X., De Leenheer M., Wang R., S.K. Vadrevu C., Shi L., Zhang J., Mukherjee B., (2012), "High-performance routing for hose-based VPNs in multi-domain backbone networks", IEEE, Sayfa: 3013-3018

[3] Wang M., Pan J., Zheng Z., (2012), "The Application of VPN in the Remote Virtual Classroom", ScineDirect, Cilt No:2, Sayfa:828-833

[4] Matsuhashi Y., Shinagawa T., Ishii Y., Hirooka N., Kato K., (2012), "Transparent VPN failure recovery with virtualization", ScineDirect, Dergi Cilt No:28,1, Sayfa:78-84

[5] Yüksel E., Örencik B., (2005), Sanal Özel Ağ Tasarımı ve Gerçeklemesi, Ağ ve Bilgi Güvenliği Ulusal Semp. (ABG 2005) Bildiriler Kitabı, ISBN 975-395-885-4, s. 114-118.

[6] Guadong G, (2011), "Design and Implementation of Secure Enterprise Network Based on DMVPN", Sayfa: 506-511

[7] Soğukpınar İ., Açık Anahtarlı Kriptosistemler ve Sayısal İmzalar. G.Y.T.E.

[8] Yerlikaya T., Buluş E., Buluş N., "Kripto Algoritmalarının Gelişimi ve Önemi", Akademik Bilişim Konferansları 2006-AB2006, Denizli-TÜRKİYE,

[9] Akçam N, (2007), "RSA Algoritması Kullanılarak Hata Düzeltmeli ve Dijital İmzalı Protokol Geliştirme", Cilt:10, Sayı:1

[10] Demirkol S. A., Çağlayan U. M., Paralel AAA ve Mobil IPv4 İletişimiyle Hızlı Kablosuz Ağ Dolaşımı, Boğaziçi Üniversitesi, 2008.

[11] Building A Virtual Private Network by Meeta Gupta_2

[12] http://technet.microsoft.com/en-us/network/dd420463.aspx (26.09.2012)

[13] http://tr.docdat.com/docs/index-99198.html (03.10.2012)

[14] http://tr.wikipedia.org/wiki/NAT (17.10.2012)

[15] http://tr.wikipedia.org/wiki/RADIUS (03.11.2012)

[16] http://tr.wikipedia.org/wiki/AES (07.11.2012)

[17] ab.org.tr/ab08/bildiri/121.doc (13.12.2012)

[18] http://www.bidb.itu.edu.tr/?d=891 (23.12.2012)

[19] http://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange (01.01.2013)

[20] http://www.math.washington.edu/~morrow/336_09/papers/Yevgeny.pdf (13.01.2013)

[21] http://www.arx.com/resources/white-papers/pki-solution-for-electronic-signatures. htm (25.20.2013)

[22] Ip Security Protocol, Peter LINDGREN (03.03.2013)

[23] http://en.wikipedia.org/wiki/Internet_Key_Exchange (08.04.2013)

[24] http://docs.comu.edu.tr/howto/ipsec-howto-theory.html (15.04.2013)

[25] http://www.networksorcery.com/enp/protocol/ah.htm (20.05.2013)

[26] http://www.networksorcery.com/enp/protocol/esp.htm (18.06.2013)

[27] http://www.cisco.com/en/US/products/ps9422/products_configuration_example09186a0080ba1d0a.shtml (23.07.2013)

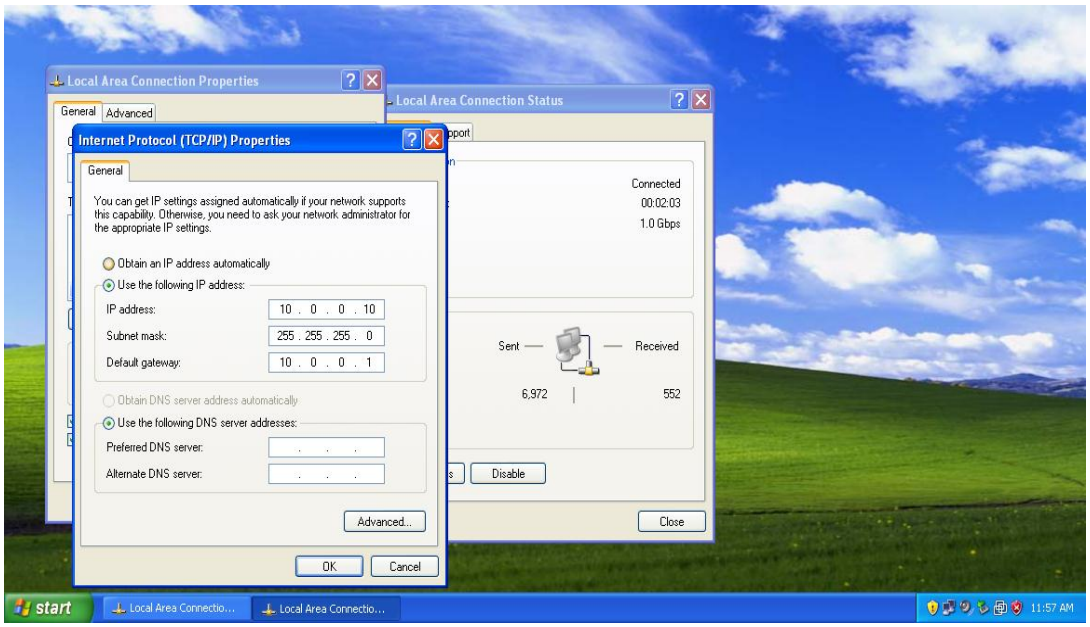
[28] http://en.wikipedia.org/wiki/Dynamic_Multipoint_Virtual_Private_Network (28.08.2013)

[29] http://www.trainsignal.com/blog/multipoint-gre-tunnel-introduction (01.09.2013)

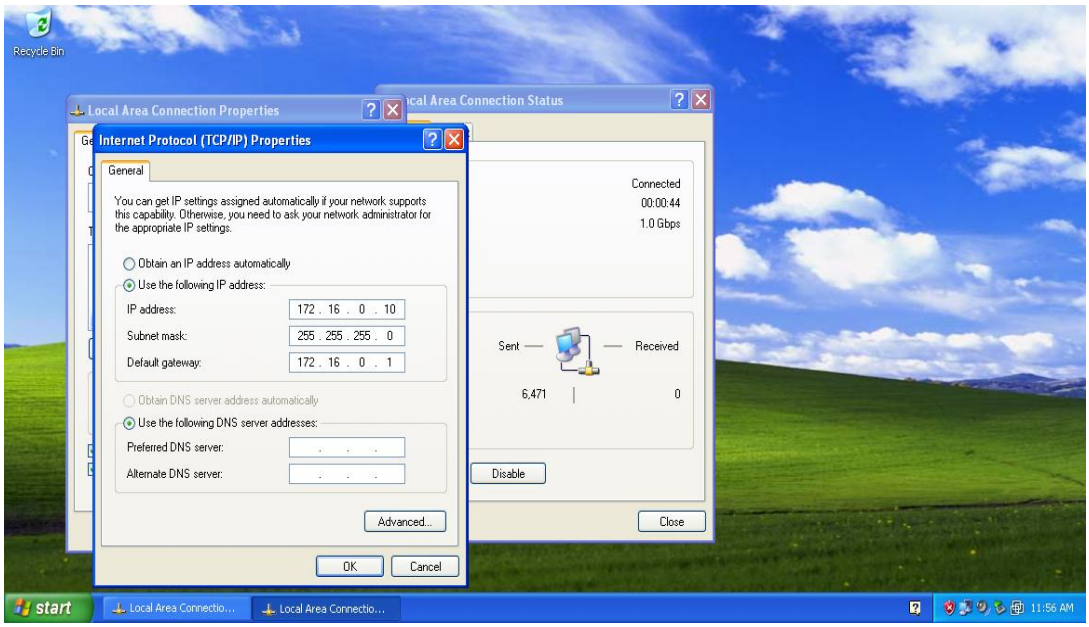
EKLER

1. Siteden siteye sanal özel ağ uygulaması yönlendirici konfigürasyonları ve sanal bilgisayar ağ ayarları:

Sanal bilgisayarlar:



Şekil 1. Siteden siteye sanal özel ağ uygulamasında kullanılan sanal bilgisayar ağ adresi



Şekil 2. Siteden siteye sanal özel ağ uygulamasında kullanılan sanal bilgisayar ağ adresi

“ANK” yönlendiricisine ait ilgili konfigürasyon:

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname ANK
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 5
ip cef
no ip domain lookup
multilink bundle-name authenticated
archive
log config
hidekeys
crypto isakmp policy 1

encr aes
authentication pre-share
group 2
crypto isakmp key cisco address 81.21.163.2
crypto ipsec transform-set ACD esp-aes esp-sha-hmac
crypto map ACD_MAP 1 ipsec-isakmp
set peer 81.21.163.2
set transform-set ACD
match address VPN
interface FastEthernet0/0
ip address 172.16.0.1 255.255.255.0
duplex auto
speed auto
interface Serial0/0
ip address 88.248.30.2 255.255.255.252
clock rate 2000000
crypto map ACD_MAP
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
interface Serial0/1
no ip address
shutdown
clock rate 2000000
interface Serial0/2
no ip address
shutdown
clock rate 2000000
interface Serial0/3
no ip address
shutdown
clock rate 2000000

router eigrp 100
network 88.0.0.0
no auto-summary
ip forward-protocol nd
ip route 10.0.0.0 255.255.255.0 88.248.30.1
no ip http server
no ip http secure-server
ip access-list extended VPN
permit ip 172.16.0.0 0.0.0.255 10.0.0.0 0.0.0.255
control-plane
line con 0
exec-timeout 0 0
logging synchronous
line aux 0
line vty 0 4
login
End

IST yönlendiricisine ait ilgili konfigürasyon:

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname IST
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 5
ip cef
no ip domain lookup
multilink bundle-name authenticated
archive
log config

hidekeys
crypto isakmp policy 1
encr aes
authentication pre-share
group 2
crypto isakmp key cisco address 88.248.30.2
crypto ipsec transform-set ACD esp-aes esp-sha-hmac
crypto map ACD_MAP 1 ipsec-isakmp
set peer 88.248.30.2
set transform-set ACD
match address VPN
interface FastEthernet0/0
ip address 10.0.0.1 255.255.255.0
duplex auto
speed auto
interface Serial0/0
ip address 81.21.163.2 255.255.255.252
clock rate 2000000
crypto map ACD_MAP
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
interface Serial0/1
no ip address
shutdown
clock rate 2000000
router eigrp 100
network 81.0.0.0
no auto-summary
ip forward-protocol nd
ip route 172.16.0.0 255.255.255.0 88.248.30.2
no ip http server

no ip http secure-server

ip access-list extended VPN

permit ip 10.0.0.0 0.0.0.255 172.16.0.0 0.0.0.255

control-plane

line con 0

exec-timeout 0 0

logging synchronous

line aux 0

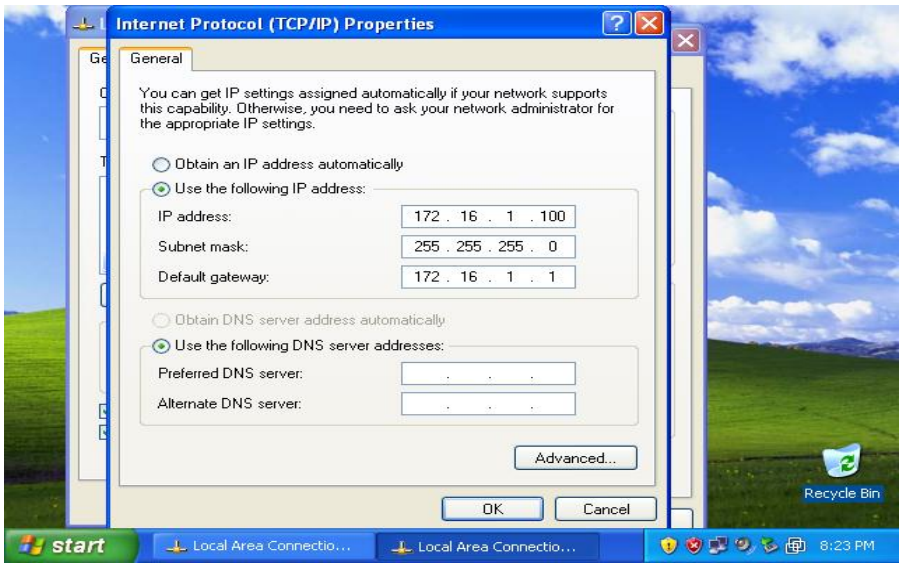
line vty 0 4

login

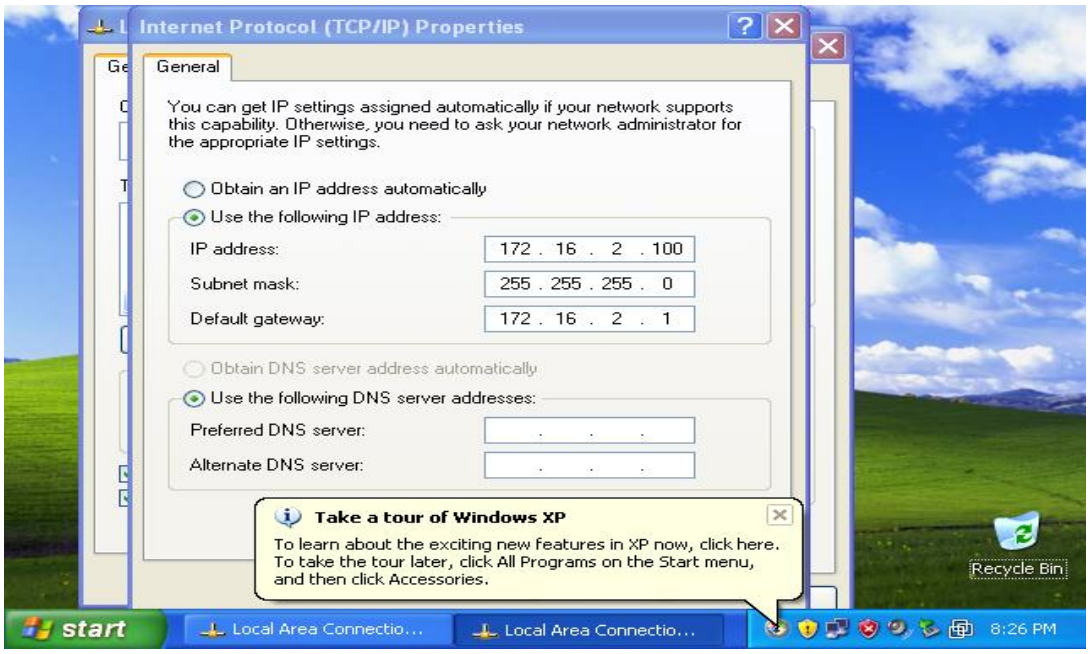
end

2. Dinamik çok noktalı sanal özel ağ uygulaması yönlendirici konfigürasyonları ve sanal bilgisayar ağ ayarları:

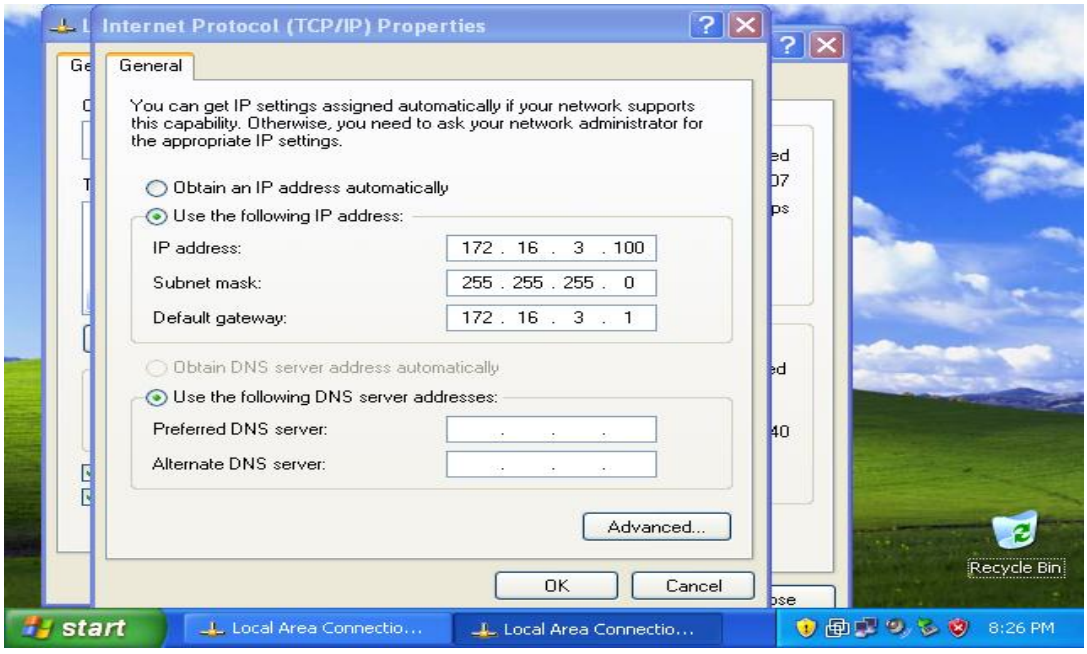
Sanal bilgisayarlar:



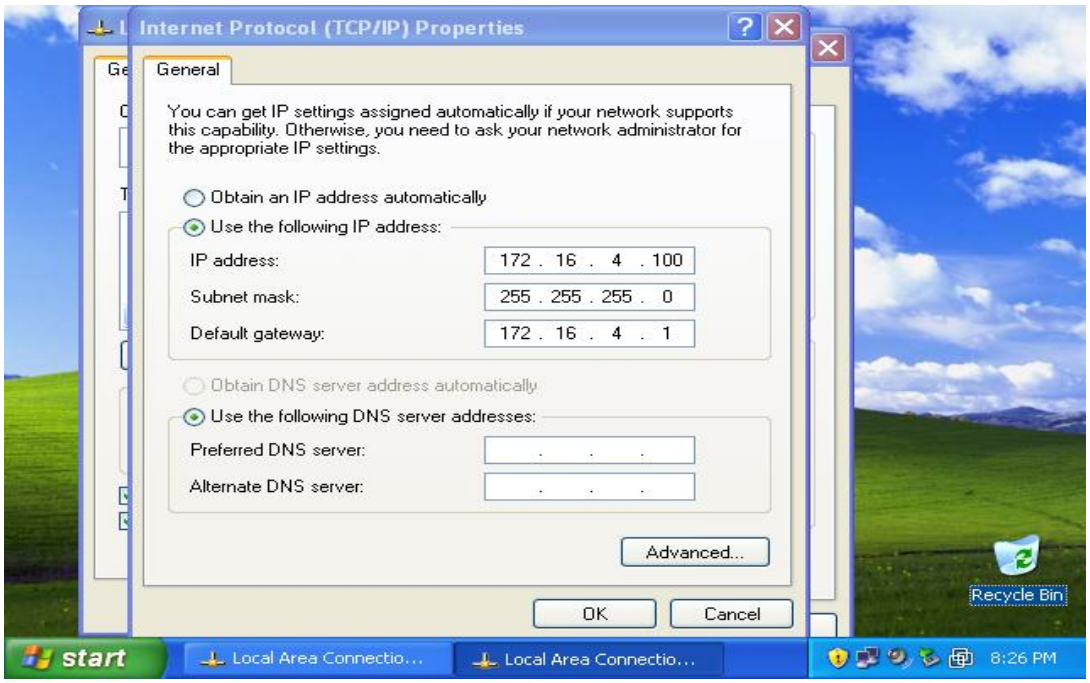
Şekil 3. Dinamik çok noktalı sanal özel ağ uygulamasında kullanılan sanal bilgisayar ağ adresi



Şekil 4. Dinamik çok noktalı sanal özel ağ uygulamasında kullanılan sanal bilgisayar ağ adresi



Şekil 5. Dinamik çok noktalı sanal özel ağ uygulamasında kullanılan sanal bilgisayar ağ adresi



Şekil 6. Dinamik çok noktalı sanal özel ağ uygulamasında kullanılan sanal bilgisayar ağ adresi

HUB yönlendiricisine ait ilgili konfigürasyon:

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname HUB
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 5
ip cef
no ip domain lookup
multilink bundle-name authenticated
archive
log config
hidekeys

```
crypto isakmp policy 10
encr 3des
hash md5
authentication pre-share
crypto isakmp key 6 cisco123 address 0.0.0.0 0.0.0.0
crypto ipsec transform-set MINE esp-3des
crypto ipsec profile DMVPN
set transform-set MINE
interface Tunnel0
ip address 10.1.1.1 255.255.255.0
no ip redirects
ip mtu 1416
ip hold-time eigrp 1 35
no ip next-hop-self eigrp 1
ip nhrp map multicast dynamic
ip nhrp network-id 1
no ip split-horizon eigrp 1
tunnel source 192.168.1.100
tunnel mode gre multipoint
tunnel protection ipsec profile DMVPN
interface FastEthernet0/0
ip address 192.168.1.100 255.255.255.0
duplex auto
speed auto
interface FastEthernet0/1
ip address 172.16.1.1 255.255.255.0
duplex auto
speed auto
router eigrp 1
network 10.0.0.0
network 172.16.0.0
network 192.168.0.0
no auto-summary
ip forward-protocol nd
```

ip route 192.168.2.0 255.255.255.0 192.168.1.1
ip route 192.168.3.0 255.255.255.0 192.168.1.1
ip route 192.168.4.0 255.255.255.0 192.168.1.1
no ip http server
no ip http secure-server
control-plane
line con 0
exec-timeout 0 0
logging synchronous
line aux 0
line vty 0 4
login
end

IST yönlendiricisine ait ilgili konfigürasyon:

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname IST
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 5
ip cef
multilink bundle-name authenticated
archive
log config
hidekeys
crypto isakmp policy 10
encr 3des
hash md5
authentication pre-share

```
crypto isakmp key 6 cisco123 address 0.0.0.0 0.0.0.0
crypto ipsec transform-set MINE esp-3des
crypto ipsec profile DMVPN
set transform-set MINE
interface Tunnel0
ip address 10.1.1.2 255.255.255.0
no ip redirects
ip mtu 1416
ip hold-time eigrp 1 35
no ip next-hop-self eigrp 1
ip nhrp map 10.1.1.1 192.168.1.100
ip nhrp map multicast 192.168.1.100
ip nhrp network-id 1
ip nhrp nhs 10.1.1.1
no ip split-horizon eigrp 1
tunnel source 192.168.2.2
tunnel mode gre multipoint
tunnel protection ipsec profile DMVPN
interface FastEthernet0/0
ip address 172.16.2.1 255.255.255.0
duplex auto
speed auto
interface Serial0/0
ip address 192.168.2.2 255.255.255.0
clock rate 2000000
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
interface Serial0/1
no ip address
shutdown
clock rate 2000000
```

router eigrp 1
network 10.0.0.0
network 172.16.0.0
network 192.168.0.0
no auto-summary
ip forward-protocol nd
ip route 192.168.1.100 255.255.255.255 192.168.2.1
ip http server
no ip http secure-server
control-plane
line con 0
line aux 0
line vty 0 4
login
End

IZM yönlendiricisine ait ilgili konfigürasyon:

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname IZM
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 5
ip cef
multilink bundle-name authenticated
archive
log config
hidekeys
crypto isakmp policy 10
encr 3des

```
hash md5
authentication pre-share
crypto isakmp key 6 cisco123 address 0.0.0.0 0.0.0.0
crypto ipsec transform-set MINE esp-3des
crypto ipsec profile DMVPN
set transform-set MINE
interface Tunnel0
ip address 10.1.1.3 255.255.255.0
no ip redirects
ip mtu 1416
ip hold-time eigrp 1 35
no ip next-hop-self eigrp 1
ip nhrp map 10.1.1.1 192.168.1.100
ip nhrp map multicast 192.168.1.100
ip nhrp network-id 1
ip nhrp nhs 10.1.1.1
no ip split-horizon eigrp 1
tunnel source 192.168.3.3
tunnel mode gre multipoint
tunnel protection ipsec profile DMVPN
interface FastEthernet0/0
ip address 172.16.3.1 255.255.255.0
duplex auto
speed auto
interface Serial0/0
ip address 192.168.3.3 255.255.255.0
no fair-queue
clock rate 2000000
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
interface Serial0/1
```

no ip address
shutdown
clock rate 2000000
router eigrp 1
network 10.0.0.0
network 172.16.0.0
network 192.168.0.0
no auto-summary
ip forward-protocol nd
ip route 192.168.1.100 255.255.255.255 192.168.3.1
ip http server
no ip http secure-server
control-plane
line con 0
line aux 0
line vty 0 4
login end

LA yönlendiricisine ait ilgili konfigürasyon:

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname LA
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 5
ip cef
multilink bundle-name authenticated
archive
log config

```
hidekeys
crypto isakmp policy 10
encr 3des
hash md5
authentication pre-share
crypto isakmp key 6 cisco123 address 0.0.0.0 0.0.0.0
crypto ipsec transform-set MINE esp-3des
crypto ipsec profile DMVPN
set transform-set MINE
interface Tunnel0
ip address 10.1.1.4 255.255.255.0
no ip redirects
ip mtu 1416
ip hold-time eigrp 1 35
no ip next-hop-self eigrp 1
ip nhrp map 10.1.1.1 192.168.1.100
ip nhrp map multicast 192.168.1.100
ip nhrp network-id 1
ip nhrp nhs 10.1.1.1
no ip split-horizon eigrp 1
tunnel source 192.168.4.4
tunnel mode gre multipoint
tunnel protection ipsec profile DMVPN
interface FastEthernet0/0
ip address 172.16.4.1 255.255.255.0
duplex auto
speed auto
interface Serial0/0
ip address 192.168.4.4 255.255.255.0
no fair-queue
clock rate 2000000
interface FastEthernet0/1
no ip address
shutdown
```

```
duplex auto
speed auto
interface Serial0/1
no ip address
shutdown
clock rate 2000000
router eigrp 1
network 10.0.0.0
network 172.16.0.0
network 192.168.0.0
no auto-summary
ip forward-protocol nd
ip route 192.168.1.100 255.255.255.255 192.168.4.1
ip http server
no ip http secure-server
control-plane
line con 0
line aux 0
line vty 0 4
login end
```