AĞ YÖNETİMİNDE SD-WAN İLE DOMAİNLER ARASI WAN PAYLAŞIMININ ETKİN YÖNETİMİ

Kubilay AKDAĞ
231402103

YÜKSEK LİSANS TEZİ
Bilgisayar Mühendisliği Anabilim Dalı
Bilgisayar Mühendisliği Tezli Yüksek Lisans Programı
Danışman: Dr. Öğr. Üyesi Önder ŞAHİNASLAN

İstanbul
T.C. Maltepe Üniversitesi
Lisansüstü Eğitim Enstitüsü
Mayıs, 2025

AĞ YÖNETİMİNDE SD-WAN İLE DOMAİNLER ARASI WAN PAYLAŞIMININ ETKİN YÖNETİMİ

Kubilay AKDAĞ
231402103
ORCID: 0009-0006-8364-3272

YÜKSEK LİSANS TEZİ
Bilgisayar Mühendisliği Anabilim Dalı
Bilgisayar Mühendisliği Tezli Yüksek Lisans Programı
Danışman: Dr. Öğr. Üyesi Önder ŞAHİNASLAN

İstanbul
T.C. Maltepe Üniversitesi
Lisansüstü Eğitim Enstitüsü
Mayıs, 2025



JÜRİ VE ENSTİTÜ ONAYI

KUBİLAY AKDAĞ'ın "Ağ Yönetiminde SD-WAN ile Domainler Arası WAN Paylaşımının Etkin Yönetimi" başlıklı tezi 28.05.2025 tarihinde aşağıdaki jüri tarafından değerlendirilerek "Maltepe Üniversitesi Lisansüstü Eğitim ve Öğretim Yönetmeliği" nin ilgili maddeleri uyarınca Bilgisayar Mühendisliği Anabilim Dalı Yüksek Lisans/Doktora/Sanatta Yeterlik tezi oy birliğiyle/oy çokluğuyla, başarılı/başarısız olarak kabul edilmiştir.

	Unvanı. Adı ve Soyadı	İmza
Üye (Tez Danışmanı)	Dr. Öğr. Üyesi Önder ŞAHİNASLAN Maltepe Üniversitesi	.....
Üye	Dr. Öğr. Üyesi Sinan TATLIGİL İstanbul Sağlık ve Teknoloji Üniversitesi	.....
Üye	Dr. Öğr. Üyesi Engin OĞUZAY Maltepe Üniversitesi	.....

Prof. Dr. Selva ERSÖZ KARAKULAKOĞLU
Enstitü Müdürü

ETİK İLKE VE KURALLARA UYUM BEYANI

Bu belge, Yükseköğretim Kurulu tarafından 19.01.2021 tarihli "Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge" ile bildirilen 6698 Sayılı Kişisel Verilerin Korunması Kanunu kapsamında gizlenmiştir.

TEŞEKKÜR

Bu tezin hazırlanmasında bilgi ve deneyimleriyle yol gösteren, değerli katkıları ve yönlendirmeleriyle çalışmamın her aşamasında yanımda olan tez danışmanım Sayın Dr. Önder Şahinaslan'a; yapıcı geri bildirimleriyle çalışmama katkı sağlayan değerli jüri üyelerine; süreç boyunca destekleyici tutumları ve anlayışlarıyla bana destek olan sevgili eşime ve aileme; akademik gelişimime verdikleri katkılarla ilerlememe olanak sağlayan Migros Ticaret A.Ş. ailesine, değerli iş arkadaşlarıma ve kıymetli yöneticilerime gönülden teşekkür ederim.

Kubilay Akdağ

Mayıs, 2025

ÖZET

AĞ YÖNETİMİNDE SD-WAN İLE DOMAİNLER ARASI WAN PAYLAŞIMININ ETKİN YÖNETİMİ

Kubilay Akdağ
Yüksek Lisans Tezi
Bilgisayar Mühendisliği Anabilim Dalı
Bilgisayar Mühendisliği Tezli Yüksek Lisans Programı
Danışman: Dr. Öğr. Üyesi Önder Şahinaslan
Maltepe Üniversitesi Lisansüstü Eğitim Enstitüsü, 2025

Bu tez, Software-Defined Wide Area Network (SD-WAN) teknolojisinin domainler arası WAN paylaşımı üzerindeki etkilerini incelemektedir. SD-WAN, geleneksel WAN mimarilerinin sınırlamalarını aşmak amacıyla geliştirilmiş; esnek, merkezi olarak yönetilebilen ve maliyet açısından verimli bir ağ altyapısı sunmaktadır. Çalışmada, SD-WAN'ın temel bileşenleri, mimari yapısı ve sunduğu avantajlar kapsamlı şekilde ele alınmıştır. Tezin ilk bölümünde SD-WAN teknolojisi tanımlanmış; geleneksel WAN çözümleriyle karşılaştırmalı olarak değerlendirilmiştir. Bu kapsamda, trafik yönlendirme, ağ izolasyonu, uygulama performansı ve merkezi yönetim gibi önemli işlevler analiz edilmiştir. Özellikle domainler arası WAN paylaşımı kapsamında, SD-WAN'ın sunduğu dinamik yönlendirme, bant genişliği optimizasyonu ve SLA (Hizmet Düzeyi Anlaşması) temelli kontrol mekanizmaları, kurumsal ve IOT ağlarının aynı altyapı üzerinde verimli ve güvenli biçimde yönetilmesine olan katkılarıyla öne çıkmaktadır. Araştırma kapsamında, IOT ve kurumsal trafiğin farklı domainler üzerinden ortak bir LTE hattı aracılığıyla yönlendirildiği bir mimari senaryo LAB ortamında yapılandırılmış ve çeşitli testlerle değerlendirilmiştir. Trafik izolasyonu, SLA takibi, uygulama performansı ve yedeklilik senaryoları üzerinden yapılan sistematik analizlerle, paylaşımlı trafik yönetiminin performansa ve güvenliğe etkileri incelenmiştir. Sonuç olarak, SD-WAN teknolojisinin domainler arası WAN paylaşımında sunduğu esneklik, merkezi denetim, güvenlik ve maliyet avantajları ortaya konmuştur. Bu mimarinin, dağıtık yapılara sahip büyük ölçekli işletmeler için güçlü bir çözüm sunduğu, geleneksel WAN yapılarına kıyasla daha etkin kaynak kullanımı ve yönetilebilirlik sağladığı değerlendirilmiştir. Tez, ayrıca SD-WAN'ın benimsenmesiyle elde edilebilecek potansiyel faydaları ve karşılaşılabilecek teknik zorluklar ile beraber teknolojinin kurumsal ağlarda etkin kullanılabilmesine yönelik öneriler sunmaktadır.

Anahtar Sözcükler: SD-WAN, Dinamik Trafik Yönlendirme, SLA, IOT Ağları, Kurumsal Ağlar, LTE Hat Paylaşımı

ABSTRACT

EFFECTIVE MANAGEMENT OF INTER-DOMAIN WAN SHARING WITH SD-WAN IN NETWORK MANAGEMENT

Kubilay Akdağ
Master Thesis
Department of Computer Engineering
Computer Engineering Master Program with Thesis
Thesis Advisor: Asist. Prof. Dr. Önder Şahinaslan
Maltepe University Graduate School, 2025

This thesis investigates the impact of Software-Defined Wide Area Network (SD-WAN) technology on inter-domain WAN sharing. SD-WAN has been developed to overcome the limitations of traditional WAN architectures and offers a flexible, centrally manageable, and cost-effective network infrastructure. The study thoroughly examines the core components of SD-WAN, its architectural structure, and the benefits it provides. In the initial section, SD-WAN is defined and compared with conventional WAN solutions. Key features such as traffic steering, network segmentation, application performance, and centralized control are analyzed. Specifically, in the context of inter-domain WAN sharing, the study highlights how SD-WAN's dynamic routing, bandwidth optimization, and SLA (Service Level Agreement)-based control mechanisms contribute to the efficient and secure management of corporate and IOT networks over a shared infrastructure. As part of the research, a lab-based test scenario was designed where corporate and IOT traffic were routed through separate SD-WAN domains over a shared LTE link. Various performance tests were conducted to evaluate shared traffic management, focusing on traffic isolation, SLA monitoring, application-level performance, and redundancy scenarios. In conclusion, the thesis demonstrates that SD-WAN provides significant flexibility, centralized control, security, and cost-efficiency in inter-domain WAN sharing. This architecture is evaluated as a powerful solution for large-scale, distributed enterprises, offering more effective resource utilization and improved manageability compared to traditional WAN models. The thesis also discusses the potential benefits and technical challenges associated with SD-WAN adoption and provides practical recommendations for its effective deployment in enterprise network environments.

Keywords: SD-WAN, Dynamic Traffic Steering, SLA, IOT Networks, Enterprise Networks, LTE Link Sharing

İÇİNDEKİLER

JÜRİ VE ENSTİTÜ ONAYI ii

ETİK İLKE VE KURALLARA UYUM BEYANI iii

TEŞEKKÜR iv

ÖZET v

ABSTRACT vi

İÇİNDEKİLER vii

TABLOLAR LİSTESİ xii

ŞEKİLLER LİSTESİ xiii

KISALTMALAR xvii

1. GİRİŞ 1

1.1 Problem 1

1.2 Amaç 2

1.3 Önem 3

1.4 Varsayımlar 3

1.5 Sınırlıklar 4

1.6 Tanımlar 4

2. LİTERATÜR ARAŞTIRMASI 8

2.1 Temel Ağ Kavramları 8

2.1.1 Geleneksel ağ 8

2.1.2 Ağ türleri 9
2.1.2.1 Yerel alan ağı 9
2.1.2.2 Geniş alan ağı 9
2.1.2.3 Metropol alan ağı 9
2.1.2.4 Yazılım tabanlı geniş alan ağı 10
2.1.3 Ağ bileşenleri 10
2.1.3.1 Ağ cihazları 10
2.1.3.2 Protokoller ve standartlar 11
2.1.3.3 Adresleme 12
2.2 Veri İletimi ve Katmanlar 12
2.2.1 OSI modeli ve katmanları 12
2.2.2 TCP/IP modeli ve işleyişi 13
2.2.3 Yönlendirme ve anahtarlama 14
2.3 Ağ Güvenliği 15
2.3.1 Güvenlik duvarları 15
2.3.2 Sanal özel ağlar ve internet güvenlik protokolü 15
2.4 Ağ Yönetimi ve Optimizasyonu 16
2.4.1 Hizmet düzeyi anlaşmaları ve hizmet kalitesi 16
2.4.2 Ağ izleme ve yönetim protokolleri 16
2.4.3 Yazılım tabanlı ağ yönetimi 17
2.5 SD-WAN mimarisi 17

2.6 Domainler Arası WAN Paylaşımı 20
2.7 Domainler Arası WAN Paylaşımının Önemi 20
2.8 Geleneksel WAN ile SD-WAN Karşılaştırması 20
2.9 SD-WAN ile Domainler Arası WAN Paylaşımı 21
2.9.1 Teknik inceleme 21
2.9.2 SD-WAN'ın domainler arası wan paylaşımına getirdiği yenilikler 21
2.9.3 Kullanım senaryoları 22
3. YÖNTEM 23
3.1 Ağ Topolojisinin Oluşturulması 24
3.2 Lab Ortamın Hazırlanması 26
3.2.1 Fiziksel bağlantıların yapılandırılması 26
3.2.2 VDOM özelliğinin aktif edilmesi 26
3.2.3 WAN bağlantılarının aktif edilmesi 28
3.2.4 Erişim testlerinin yapılması 30
3.3 Konfigürasyon Adımları 32
3.3.1 Forti manager entegrasyonu 32
3.4 IPsec ve SD-WAN yapılandırmaları 33
3.4.1 IPsec tünel yapılandırmaları 34
3.5 SD-WAN Politikalarının Oluşturulması 36
3.5.1 SLA kontrolleri 36
3.5.2 Trafik yönlendirme kuralları 38

3.6 Güvenlik Politikalarının Oluşturulması 39
3.6.1 IPsec tünel trafik politikaları 39
3.6.2 Uygulama tabanlı güvenlik politikaları 40
3.6.3 Tehdit yönetimi ve koruma 41
3.6.4 Loglama ve izleme 42
3.7 Sistem Ayarlarının Oluşturulması 42
3.7.1 DNS ayarlarının yapılandırılması 42
3.7.2 NTP ayarlarının yapılandırılması 43
3.7.3 SNMP ayarlarının yapılandırılması 44
3.8 Test ve Doğrulama 45
3.8.1 Ağ bağlantısının doğrulanması 45
3.8.1.1 Vdomlar arası trafik testi 45
3.8.1.2 WAN bağlantısı doğrulama 46
3.8.1.3 IPSEC tünel bağlantı testi 47
3.8.1.4 Tünel üzerinden trafik testi 50
3.8.2 SD-WAN trafik yönlendirme testleri 52
3.8.3 Güvenlik politikalarının doğrulanması 55
3.8.4 Performans analizi 58
3.8.5 Bağlantı testi sonuçları 61
4. BULGULAR VE TARTIŞMA 63
4.1 Bulgular 63

4.1.1 Üç hatlı LTE paylaşımlı yedeklilik modeli 66

4.1.2 İki hatlı çapraz yedeklilik modeli 72

4.2 Tartışma 76

5. SONUÇ ve ÖNERİLER 78

KAYNAKÇA 80

ÖZ GEÇMİŞ 83

TABLOLAR LİSTESİ

Tablo 1. Test Ortamında Temel Alınan Şube Bileşenleri 4

Tablo 2. Ağ Topolojisi Bileşenleri 18

Tablo 3. IP Tablosu 25

Tablo 4. Performans Testleri Özet Sonuçları 60

Tablo 5. 3 Hatlı Topoloji Maliyet Analizi 70

Tablo 6. 2 Hatlı Topoloji Maliyet Analizi 75

ŞEKİLLER LİSTESİ

Şekil 1. OSI Modeli 13

Şekil 2. OSI Model ve TCP IP Model Karşılaştırması 14

Şekil 3. Basit Ağ Örneği 18

Şekil 4. Yedeklilik Algoritması 23

Şekil 5. SD-WAN Domainler Arası WAN Paylaşımı Kurulum Diyagramı 24

Şekil 6. Tek Hat Kullanılarak Oluşturulan Ağ Topolojisi 25

Şekil 7. Bağımsız VDOM'lar 26

Şekil 8. Root ve IOT VDOM'ların Oluşturulması 27

Şekil 9. Fiziksel Portların ve NPU Link'lerin VDOM'lara Atanması 27

Şekil 10. Root VDOM WAN1 Fiziksel Bağlantısının Yapılandırılması 28

Şekil 11. NPU Link'lerin Root ve IOT VDOM'lara Atanması 29

Şekil 12. IOT VDOM'dan Root VDOM'a Trafik Yönlendirme 29

Şekil 13. Root VDOM'dan Merkeze Trafik Yönlendirme (IPsec için) 30

Şekil 14. Root VDOM'dan Merkeze Trafik Yönlendirme 30

Şekil 15. IOT VDOM NPU Link IP'den IOT HUB IPsec Peer IP Adresine Ping Testi 31

Şekil 16. Root VDOM WAN IP'den Merkez HUB Loopback IP Adresine Ping Testi . 31

Şekil 17. Forti Manager Konfigürasyonu 33

Şekil 18. Analyzer Konfigürasyonu 33

Şekil 19. Root Vdom Phase 1 Konfigürasyonu 34

Şekil 20. Root Vdom Phase 2 Konfigürasyonu 35

Şekil 21. IOT Vdom Phase 1 Konfigürasyonu 35

Şekil 22. IOT Vdom Phase 2 Konfigürasyonu 36

Şekil 23. SLA Konfigürasyonu 37

Şekil 24. Trafik Yönlendirme Kuralları 38

Şekil 25. Firewall Policy Yapılandırma Örneği 40

Şekil 26. Uygulama Tabanlı Firewall Policy Örneği 40

Şekil 27. Tehdit Yönetimi ve Koruma Yapılandırma Örneği 41

Şekil 28. Loglama ve İzleme Konfigürasyonu 42

Şekil 29. DNS Konfigürasyonu 43

Şekil 30. NTP Konfigürasyonu 43

Şekil 31. SNMP Konfigürasyonu 44

Şekil 32. IOT VDOM'dan Root VDOM'a Ping Testi 45

Şekil 33. IOT VDOM'dan Merkez HUB'a Ping Testi 46

Şekil 34. Root VDOM'dan Merkez HUB'a Ping Testi 46

Şekil 35. Tünel Durumunun Kontrolü 47

Şekil 36. Root VDOM'dan Merkez HUB'a IPsec Tünel Üzerinden Ping Testi 48

Şekil 37. IOT VDOM'dan IOT HUB'a IPsec Tünel Üzerinden Ping Testi 49

Şekil 38. Tünel Durumunun Gösterilmesi 50

Şekil 39. DNS Trafiği İzleme 51

Şekil 40. Gerçek Zamanlı Trafik Yönlendirme ve Doğrulama 51

Şekil 41. Root VDOM için SLA Konfigürasyonu 52

Şekil 42. IOT VDOM için SLA Konfigürasyonu..... 53

Şekil 43. Root VDOM SLA Kontrolü Testi 54

Şekil 44. IOT VDOM SLA Kontrolü Testi 54

Şekil 45. Güvenlik Politikalarının Görüntülenmesi 56

Şekil 46. İzin Verilen Trafik Testi..... 57

Şekil 47. Engellenen Trafik Testi 57

Şekil 48. Günlük Kayıtları ile Doğrulama..... 58

Şekil 49. Latency, Jitter ve Packet Loss Analizi 59

Şekil 50. Bant Genişliği Testi..... 60

Şekil 52. Enerji Tasarruf Analizi..... 64

Şekil 53. Cihaz ve Lisans Maliyet Tasarruf Analizi..... 65

Şekil 54. 3 Hatlı LTE Paylaşımlı Yedeklilik Modeli 66

Şekil 55. LTE Yedeklilik Modeli Yük Analizi..... 68

Şekil 56. LTE Hattı SLA Performans Grafiği 69

Şekil 57. LTE Paylaşımlı Model Sızma Testi Sonuçları 70

Şekil 58. 3 Hatlı Topoloji Maliyet Grafiği 71

Şekil 59. 2 Hatlı Çapraz Yedekli Topoloji Modeli..... 72

Şekil 60. Çapraz Yedeklilik Modeli Yük Analizi..... 73

Şekil 61. ME Hattı SLA Performans Grafiği 74

Şekil 62. Çapraz Yedeklilik Sızma Testi Sonuçları 75

Şekil 63. 2 Hatlı Topoloji Maliyet Grafiği 76

KISALTMALAR

ADSL : Asymmetric Digital Subscriber Line

API : Application Programming Interface

ARP : Address Resolution Protocol

CPU : Central Processing Unit

DDoS : Distributed Denial of Service

DIA : Dedicated Internet Access

DSL : Digital Subscriber Line

GRE : Generic Routing Encapsulation

GSM : Global System for Mobile Communications

HTTP : Hyper Text Transfer Protocol

HTTPS : Hyper Text Transfer Protocol Secure

IANA : Internet Assigned Numbers Authority

ICMP : Internet Control Message Protocol

ISP : Internet Service Provider

IP : Internet Protocol

IPv4 : Internet Protocol Version 4

IPsec : Internet Protocol Security

LAN : Local Area Network

LTE : Long Term Evolution

MAC : Media Access Control

MPLS : Multiprotocol Label Switching

OSI : Open Systems Interconnection

QoS : Quality of Service

PoE : Power Over Ethernet

SDN : Software Defined Network

SD-WAN : Software Defined Wide Area Network

SFP : Small Form-factor Pluggable

SSH : Secure Shell Protocol

SLA : Service Level Agreement

SSL : Secure Socket Layer

STP : Spanning Tree Protocol

TCP : Transmission Control Protocol

TLS : Transport Layer Security

TTL : Time to Live

UDP : User Datagram Protocol

VDSL : Very high-speed Digital Subscriber Line

VLAN : Virtual Local Area Network

VoIP : Voice over Internet Protocol

VPN : Virtual Private Network

WAN : Wide Area Network

1. GİRİŞ

Bu çalışmada, SD-WAN teknolojisinin temel kavramlarını ve bu teknolojinin domainler arası WAN paylaşımı üzerindeki etkisini incelenmiştir. Domainler arası WAN paylaşımı, farklı ağ alanlarının sorunsuz bir şekilde entegrasyonunu sağlayarak veri akışının kesintisiz ve güvenli olmasını temin eder. Bu entegrasyon, özellikle IOT sistemlerinin yaygınlaştığı ve şube ağlarının daha karmaşık hale geldiği günümüzde büyük önem taşımaktadır. SD-WAN'ın, ağ yönetiminde sunduğu merkezi kontrol, otomasyon ve akıllı yönlendirme gibi özellikler, işletmelerin ağ performansını maksimize ederken, operasyonel verimliliği de artırır. Bu tez, SD-WAN'ın domainler arası WAN paylaşımı konusundaki katkılarını detaylı bir şekilde ele alarak, bu alandaki yenilikçi çözümleri ve gelecekteki potansiyel gelişmeler tartışılmıştır.

1.1 Problem

Teknolojinin gelişmesiyle birlikte, operasyonel verimliliği artırmak ve müşterilere daha iyi çözümler sunmak amacıyla IOT (Nesnelerin İnterneti) sistemleri yaygınlaşmaya başlamıştır. Dağıtık yapılarda bu sistemlerin otomasyonu ve anlık ihtiyaçlara göre daha etkili kullanılabilmesi için uzaktan erişim ihtiyacı doğmuştur. Bu nedenle, IOT sistemleri şube ağına bağlanmıştır (Li, 2024).

Şubede ağa bağlı ekipman sayısındaki artış, beraberinde çeşitli sorunlar getirmiştir:

- Merkezi Yönetim Zorlukları: Artan cihaz sayısı, merkezi yönetimi zorlaştırmıştır.

- Görünürlük Eksikliği: Ağa bağlı cihazların durumunu ve performansını izlemek güçleşmiştir.

- Bant Genişliği Sorunları: Artan veri trafiği, bant genişliği yetersizliklerine yol açmıştır.

- Hat Yedeklilik Sorunları: Bağlantı kesintileri ve yedek hatların eksikliği, ağın güvenilirliğini azaltmıştır.

- Ağ Topolojisi Uyumsuzlukları: Farklı ağ segmentleri arasında uyumsuzluklar ortaya çıkmıştır.

- QoS (Hizmet Kalitesi) Uyumsuzlukları: Farklı QoS politikalarının uygulanması, performans tutarsızlıklarına neden olmuştur.

- Gecikme ve Jitter: Yüksek gecikme süreleri ve jitter, özellikle gerçek zamanlı uygulamalarda ciddi performans sorunları yaratmıştır.

- Ağ Güvenliği : Ağa katılan IOT cihazlarına farklı firmaların erişim ve yönetim ihtiyacından dolayı ağda güvenlik zafiyeti yaratmıştır (Sahinaslan, 2019).

Ayrıca, yerel ağdaki cihazların birbirinden izole çalışması gerekliliği ve bazı sistemlerin internet erişimine açık olması ihtiyacı, güvenlik zaafiyetlerine yol açmıştır. IOT ve mağaza sistemlerinin aynı erişim altyapısını kullanması, şube hatlarında zaman zaman kritik faaliyetleri etkileyecek seviyede doygunluğa (satürasyon) neden olmuştur.

Zeybek ve Yılmaz (2019) yaptığı bir çalışmaya göre, IOT cihazlarının artan kullanımıyla birlikte ortaya çıkan güvenlik risklerini ve bu cihazların ağlarda oluşturabileceği potansiyel tehditleri ele almaktadır. Özellikle, IOT cihazlarının savunmasız yapıları nedeniyle siber saldırılara açık olduğu ve bu durumun ağ güvenliği açısından ciddi riskler oluşturduğu vurgulanmaktadır (Zeybek, 2019). IOT sistemlerinin şube ağlarına entegrasyonu, merkezi yönetim, ağ görünürlüğü ve bant genişliği yönetimi gibi çeşitli zorlukları beraberinde getirmiştir.

1.2 Amaç

Bu çalışmanın amacı, SD-WAN teknolojisini kullanarak şube ağlarında IOT sistemlerinin performansını ve güvenliğini artırmak, pasif hat maliyetlerini azaltmak, şubelerde internet altyapısı erişimi sağlamak için operasyon süreçlerini hızlandırmak, merkezi yönetim zorluklarını aşmak ve ağ kaynaklarının etkin kullanımını sağlamaktır. Bu kapsamda, SD-WAN'ın sunduğu çözümler ile yukarıda belirtilen sorunların nasıl giderilebileceği detaylı olarak incelenmiş ve uygulama örnekleri ile desteklenmiştir.

SD-WAN teknolojisi, özellikle dağıtık ağ yapılarında veri trafiğini daha etkin yönetmek ve güvenliği artırmak için çeşitli avantajlar sunar. VDOM (Virtual Domain) teknolojisinin avantajlarını kullanarak, farklı ağ segmentleri arasında izole edilmiş sanal ortamlar oluşturmak mümkündür. Bu, hem güvenliği artırır hem de ağ yönetimini kolaylaştırır. Ayrıca, VDOM sayesinde merkezi yönetim ve görünürlük sağlanarak, ağdaki her bir cihazın durumu ve performansı daha etkin bir şekilde izlenebilir (Troia, 2021).

Abergos ve Medjek (2024) çalışmasında, SD-WAN teknolojisinin IOT sistemleri üzerindeki etkilerini ve bu teknolojinin nasıl daha güvenli ve performanslı bir ağ yapısı sağlayabileceğini detaylandırmaktadır. Çalışmada, VDOM teknolojisinin farklı ağ segmentleri arasındaki izolasyonu nasıl sağlayarak güvenlik açıklarını minimize ettiği ve merkezi yönetim zorluklarını nasıl aştığı örneklerle açıklanmıştır (Abergos, 2024). Bu bilgiler, çalışmamızın temel hedeflerini desteklemekte ve SD-WAN teknolojisinin avantajlarını ortaya koymaktadır.

1.3 Önem

SD-WAN teknolojisinin önemi, bu teknolojinin sağladığı maliyet düşüşleri ve operasyonel verimlilik artışlarının yanı sıra, güvenlik ve performans iyileştirmeleri ile de ilişkilidir. Literatürde, SD-WAN'ın ağ yönetimi ve güvenlik üzerindeki olumlu etkileri geniş bir şekilde tartışılmaktadır. Örneğin, VDOM (Virtual Domain) teknolojisi ile ağların izole edilmesi, güvenlik açıklarının minimize edilmesine yardımcı olur ve merkezi yönetim ile görünürlüğü artırır (George, 2023). Bu bağlamda, SD-WAN'ın sunduğu çözümler, hem pratik hem de teorik açıdan değerlidir ve bu çalışmada bu çözümlerin uygulanabilirliği detaylı olarak incelenmiştir.

1.4 Varsayımlar

Bu varsayım, 1000 şubeli bir yapıda farklı cihazların olduğu bir ortamı temel alarak oluşturulmuştur. Her şube, farklı türde ağ cihazlarına ve hat tiplerine sahip olup, merkez ofis ile bağlantılıdır. Testler lab ortamında bir şube özelinde yapılarak genele oranı hesaplanmıştır.

Tablo 1. Test Ortamında Temel Alınan Şube Bileşenleri

Kategori	**Detay**
Network Ekipmanları	Firewall, Switch, LTE Modem
IOT Cihazları	Akıllı Sensörler, RFID, IP Kamera
Kurumsal Ekipmanlar	Tablet, El Terminalleri, Bilgisayar, Printer
Hat Tipleri	ME, LTE

Tablo 1, test ortamında kullanılan network hat ve ekipmanları ile beraber dağıtık yapılarda kullanılan bazı cihaz tiplerini örnek olarak ele almıştır.

1.5 Sınırlıklar

Bu tezde SD-WAN yapabilmek için ihtiyaç duyulan temel donanım öğeleri,

Firewall (Fortigate): Ağ güvenliğini sağlamak ve SD-WAN özelliklerini yönetmek için FortiGate firewall cihazları gereklidir. Bu cihazlar, trafiği yönlendirme, güvenlik duvarı koruması ve VPN tünelleme gibi işlevleri yerine getirir.

Forti Manager: Ağın merkezi yönetimini sağlamak için FortiManager kullanılmalıdır. Bu cihaz, SD-WAN politikalarının ve konfigürasyonlarının merkezi olarak yönetilmesini ve izlenmesini sağlar.

Forti Extender: Yedek bağlantı ve mobil internet erişimi sağlamak için Forti Extender cihazları kullanılabilir. Bu cihazlar, LTE/4G bağlantılarını yedek hat olarak kullanarak ağın sürekliliğini ve erişilebilirliğini artırır.

Bu temel donanım öğeleri ve uygulama ürünleri (application), Fortinet ile SD-WAN uygulamalarında gerekli olan altyapıyı sağlamak için gerekli olan bileşenlerdir.

1.6 Tanımlar

SD- WAN: SD-WAN (Software-Defined Wide Area Network), ağ trafiğini merkezi olarak yönetmek ve optimize etmek amacıyla kullanılan, geleneksel WAN mimarilerinin sınırlamalarını aşarak esneklik, yönetilebilirlik ve maliyet etkinliği sağlayan yazılım

tabanlı geniş alan ağı teknolojisidir (Yang, 2019). SD-WAN, geleneksel WAN çözümlerine göre daha esnek ve yönetilebilir bir yapı sunar. ISP (Internet Service Provider) bağımlılığının azalmasına yardımcı olur.

WAN: WAN (Wide Area Network), geniş bir coğrafi alana yayılmış ve genellikle şirketler veya organizasyonlar tarafından uzak ofisleri birbirine bağlamak için kullanılan bir ağ türüdür. IOT (Internet of Things), fiziksel nesnelerin internete bağlanarak veri toplaması ve paylaşması konseptidir ve bu cihazlar sensörler, yazılımlar ve diğer teknolojiler aracılığıyla birbirleriyle ve merkezi sistemlerle iletişim kurar (Ercan, 2016).

Merkezi yönetim, bir ağın veya sistemin tüm bileşenlerinin tek bir merkezden yönetilmesi ve kontrol edilmesi sürecini ifade eder ve bu yöntem ağ verimliliğini artırarak sorunların hızlı bir şekilde tespit edilip giderilmesini sağlar. Bant genişliği, bir ağ bağlantısının veri iletim kapasitesini belirtir ve yüksek bant genişliği, daha fazla verinin daha hızlı bir şekilde iletilmesini sağlar. Yedeklilik ise bir sistemin veya ağın kesinti durumlarında çalışmaya devam edebilmesi için alınan ek önlemleri içerir ve bu sayede sistem güvenilirliği artırılarak veri kaybı önlenir.

QoS: QoS (Quality of Services), ağ hizmetlerinin performansını ve güvenilirliğini belirleyen çeşitli kriterler ve politikalar anlamına gelir ve özellikle ses ve video gibi gerçek zamanlı uygulamalar için büyük önem taşır. Latency (Gecikme), bir veri paketinin kaynağından hedefine ulaşması için geçen süreyi ifade eder ve düşük gecikme süreleri ağ performansını artırarak kullanıcı deneyimini iyileştirir. Jitter (Tutarsızlık) ise veri paketlerinin hedefe ulaşma sürelerindeki değişkenliktir ve düşük jitter, ses ve video gibi uygulamaların düzgün çalışmasını sağlar (Numan, 2019). Ağ topolojisi, bir ağın fiziksel veya mantıksal yapısını tanımlar ve bu yapı ağın performansını ve yönetimini etkileyen önemli bir faktördür. Tünelleme protokolleri, ağ verilerini güvenli bir şekilde iletmek için kullanılan yöntemler olup, verilerin bir ağ üzerinden şifreli bir şekilde aktarılmasını sağlar.

IPSEC: IPSEC (Internet Protocol Security), ağ üzerinden iletilen IP paketlerini şifreleyerek güvenli veri iletimi sağlayan bir protokoller bütünüdür. IPsec, özellikle uzak noktalar arasında güvenli bir iletişim sağlamak amacıyla VPN (Virtual Private Network)

yapılarında yaygın olarak kullanılmaktadır. Protokol, verinin bütünlüğünü, kimlik doğrulamasını ve gizliliğini sağlamak için çeşitli güvenlik mekanizmaları kullanır.

IPsec, Transport modu ve Tunnel modu olmak üzere iki farklı çalışma moduna sahiptir. Transport modunda, yalnızca IP paketinin içeriği şifrelenirken, tunnel modunda hem paket başlık bilgileri hem de içeriği kapsayan tam bir şifreleme gerçekleştirilir. Bu nedenle, tunnel modu özellikle iki farklı ağ arasında güvenli bağlantılar oluşturmak için tercih edilmektedir.

IPsec, AH (Authentication Header) ve ESP (Encapsulating Security Payload) olmak üzere iki temel protokol ile çalışır. AH, verinin kaynağını doğrulamak ve bütünlüğünü sağlamak için kullanılırken, ESP verinin gizliliğini sağlamak amacıyla şifreleme mekanizmasını içermektedir. Ayrıca, IKE (Internet Key Exchange) protokolü, IPsec bağlantılarında oturumların güvenli bir şekilde başlatılmasını ve anahtar değişimlerinin gerçekleştirilmesini sağlar.

IPsec'in sağladığı şifreleme, kimlik doğrulama ve bütünlük kontrolü mekanizmaları, özellikle geniş alan ağlarında kullanılan SD-WAN yapılarında güvenliği artırmak için önemli bir bileşen olarak değerlendirilmektedir (Frankel, 2005). SD-WAN mimarisinde, farklı şubeler arasında güvenli veri iletimini sağlamak ve dinamik tünel yönetimini gerçekleştirmek için IPsec tünelleri yaygın olarak kullanılmaktadır. Bu sayede, geleneksel MPLS (Multi Protocol Label Switching) tabanlı çözümlere kıyasla daha güvenli ve esnek bir WAN yönetimi mümkün hale gelmektedir.

SLA: SLA (Service Level Agreement), bir hizmet sağlayıcısı ile müşteri arasında belirlenen hizmetin kalitesini, erişilebilirliğini ve performansını tanımlayan resmi bir sözleşmedir. SLA, özellikle ağ yönetimi, bulut bilişim, internet servis sağlayıcıları, veri merkezleri ve yönetilen BT hizmetleri gibi alanlarda kritik bir rol oynamaktadır.

SLA kapsamında, hizmetin beklenen çalışma süresi (uptime), gecikme süresi (latency), paket kaybı (packet loss), tepki süresi (response time) ve hata toleransları gibi performans kriterleri tanımlanır. Ayrıca, hizmet sağlayıcının taahhüt ettiği süre içinde meydana gelebilecek kesintilere nasıl yanıt vereceği, MTTR (Mean Time to Repair) olası

sorunların çözüm süreleri ve SA (Service Availability) hizmetin ne ölçüde kullanılabilir olacağı gibi unsurlar da SLA kapsamında belirlenir.

Ağ yönetimi ve özellikle SD-WAN (Software-Defined Wide Area Network) çözümlerinde SLA, dinamik trafik yönlendirme ve bağlantı optimizasyonunda önemli bir rol oynar. SD-WAN ortamlarında SLA, belirli bağlantılar üzerinden hangi trafiğin yönlendirileceğini ve önceliklendirileceğini belirlemek için kullanılır (Nicolazzo, 2024). Örneğin, IPsec tünelleri üzerinden geçen trafiğin gecikme, jitter ve paket kaybı kriterleri baz alınarak en uygun bağlantı yolunun seçilmesi SLA politikaları doğrultusunda gerçekleştirilir.

2. LİTERATÜR ARAŞTIRMASI

Bu çalışmada, SD-WAN teknolojisinin domainler arası WAN paylaşımı üzerindeki etkileri değerlendirilmiştir. Yang ve diğerleri (2021) tarafından SD-WAN'ın mevcut durumu ve gelecekteki gelişimi incelenmiştir (Yang, 2019). Frankel ve diğerleri (2005) tarafından, IPsec protokolünün ölçeklenebilirlik ve güvenlik açısından sağladığı faydalar analiz edilmiş, IPsec VPN'lerinin geniş ölçekli ağlarda nasıl uygulanabileceğine dair çözümler sunulmuştur (Frankel, 2005). Bunlara ek olarak, Stojanović ve Rakas (2022) tarafından, hizmet düzeyi anlaşmalarının (SLA) ağ hizmetleri üzerindeki etkileri değerlendirilmiştir (Stojanović, 2009). Bu çalışmalar, SD-WAN tabanlı ağ yönetiminin güvenlik, trafik yönlendirme ve hizmet kalitesi (QoS) ile ilişkisini detaylandırarak, bu tez çalışmasının teorik çerçevesinin oluşturulmasına katkıda bulunmuşlardır.

2.1 Temel Ağ Kavramları

Günümüzde ağ teknolojileri, iletişim altyapısının temel yapı taşlarından birini oluşturmaktadır. Bilgisayar ağları, cihazların birbirleriyle veri alışverişi yapmasını sağlayan sistemlerdir ve bu sistemlerin sağlıklı bir şekilde çalışabilmesi için belirli temel kavramlar çerçevesinde değerlendirilmesi gerekmektedir.

2.1.1 Geleneksel ağ

Birbirine bağlı bilgisayar sistemleri ve diğer cihazların (örneğin, yazıcılar, veri depolama birimleri) veri paylaşımı ve iletişimi sağlamak amacıyla oluşturduğu yapıya ağ denir (Ahlawat, 2014). Ağlar, genellikle iletişim protokolleri kullanılarak veri alışverişini düzenler ve yönetir. Ağların amacı, bilgi ve kaynakların verimli bir şekilde paylaşılmasını sağlamak, iletişimi kolaylaştırmak ve işlemleri hızlandırmaktır.

Paket anahtarlamalı ağ "ARPANET" ile başlayan internet serüveni daha sonra paket uydu ağları, yer tabanlı paket radyo ağları ve diğer ağlar ile devam etmiştir. Günümüzde İnternet, açık mimarili ağ adı verilen bir kavrama dayanır (Leiner, 2009). Buna göre herhangi bir ağ teknolojisinin seçimi, özel bir mimari ile sınırlandırılamaz, kullanıcı

tarafından serbestçe seçilebilir ve diğer teknolojilere de uygun hale getirilip dizayn edilebilir.

2.1.2 Ağ türleri

Ağ türleri, cihazlar arasındaki iletişim mesafesine, kullanım alanına ve mimari yapısına göre sınıflandırılan bağlantı modelleridir. LAN (Local Area Network) küçük ölçekli ortamlarda cihazları birbirine bağlarken, WAN (Wide Area Network) farklı coğrafi bölgelerdeki ağları birleştirir. MAN (Metropolitan Area Network) şehir çapında iletişimi desteklerken, SD-WAN (Software-Defined Wide Area Network) merkezi yönetim ve dinamik yönlendirme avantajları sunarak ağ trafiğini optimize eder.

2.1.2.1 Yerel alan ağı

LAN (Local Area Network), ev, okul, laboratuvar veya iş binaları gibi sınırlı coğrafi alanlarda bilgisayarları ve çevre birimlerini birbirine bağlayan bir bilgisayar ağıdır. LAN'lar, yüksek veri aktarım hızı ve düşük gecikme süreleriyle karakterize edilir, bu da dosya paylaşımı, yazıcı erişimi ve diğer ağ hizmetlerinin verimli bir şekilde kullanılmasını sağlar (Petekci, 2021). Ayrıca, LAN'lar genellikle Ethernet veya Wi-Fi gibi teknolojilerle kurulurlar ve ağ yönetimi ile güvenlik kontrollerini merkezi bir noktadan sağlarlar.

2.1.2.2 Geniş alan ağı

WAN (Wide Area Network), farklı coğrafi konumlarda bulunan ağları birbirine bağlayan ve veri iletimini geniş mesafeler boyunca sağlayan önemli bir iletişim altyapısıdır. WAN teknolojileri, işletmelerin, kurumların ve bireylerin küresel ölçekte güvenli, verimli ve kesintisiz bağlantı kurmasını mümkün kılar.

2.1.2.3 Metropol alan ağı

bir şehir veya büyük bir yerleşim alanı içerisindeki ağları birbirine bağlayan ve geniş bant veri iletimi sağlayan bir ağ türüdür. LAN (Local Area Network) ile WAN (Wide Area Network) arasında konumlanan MAN (Metropolitan Area Network), genellikle üniversite kampüsleri, belediye altyapıları ve büyük kuruluşların veri merkezleri arasında yüksek hızlı bağlantılar kurmak için kullanılır. Fiber optik, kablosuz bağlantılar ve özel kiralık

hatlar gibi çeşitli teknolojilerle desteklenen MAN, geniş ölçekli veri paylaşımı ve kesintisiz iletişim için optimize edilmiş bir ağ mimarisi sunar.

2.1.2.4 Yazılım tabanlı geniş alan ağı

Yazılım Tanımlı Geniş Alan Ağı (SD-WAN), geniş alan ağlarını (WAN) daha esnek, merkezi ve dinamik bir şekilde yönetmek için geliştirilen yazılım tabanlı bir ağ mimarisidir. Geleneksel WAN yapılarının aksine, SD-WAN, farklı bağlantı türleri (MPLS, LTE, DIA vb.) arasında akıllı trafik yönlendirme, uygulama önceliklendirme ve güvenlik politikaları sağlayarak ağ yönetimini optimize eder.

2.1.3 Ağ bileşenleri

Ağ bileşenleri, veri iletiminin sağlıklı ve güvenli bir şekilde gerçekleşmesini mümkün kılan donanım ve yazılım öğelerinden oluşan temel unsurlardır. Bu bileşenler arasında Router (Yönlendirici), switch (Anahtarlama), Firewall (Güvenlik Duvarı), Access Point (Erişim Noktaları) ve çeşitli ağ protokolleri yer alır.

2.1.3.1 Ağ cihazları

Bilgisayar ağlarının işleyişini sağlayan temel donanım bileşenleridir. Bu cihazlar, verinin iletilmesi, yönlendirilmesi, filtrelenmesi ve güvenliğinin sağlanması gibi işlevleri yerine getirerek, ağ altyapısının kesintisiz ve verimli çalışmasını destekler. Farklı ihtiyaçlara ve ağ yapılarına göre çeşitlenen ağ cihazları, küçük ölçekli yerel ağlardan geniş ölçekli kurumsal ve bulut tabanlı ağlara kadar birçok alanda kullanılmaktadır.

Ağ trafiğinin yönetilmesinde kilit bir rol oynayan router, veri paketlerinin hedeflerine en verimli şekilde ulaşmasını sağlamak için kullanılır. IP tabanlı iletişimi mümkün kılan bu cihazlar, özellikle geniş alan ağlarında farklı bağlantılar arasında dinamik yönlendirme yaparak ağ trafiğinin etkin şekilde yönetilmesini sağlar. Router, Statik Yönlendirme ve Dinamik Yönlendirme gibi protokolleri destekleyerek verinin en iyi yolu takip etmesini mümkün kılar. MPLS, BGP, OSPF ve RIP gibi protokollerle çalışan gelişmiş yönlendiriciler, büyük ölçekli ağlarda performansı artıran temel bileşenlerden biridir.

Veri iletiminin LAN ortamında daha verimli hale gelmesini sağlayan switch, bağlı cihazlar arasında veri paketlerinin doğrudan hedefe yönlendirilmesini mümkün kılar.

Layer 2 (Katman 2) switch, MAC adresleri üzerinden çerçeve yönlendirme yaparken, Layer 3 (Katman 3) switch, IP tabanlı yönlendirme işlemlerini gerçekleştirir. Modern switchler, VLAN desteği, QoS yönetimi ve trafik önceliklendirme gibi özelliklere sahiptir. Bu sayede, ağ içerisindeki gereksiz trafiğin azaltılması ve kritik uygulamalara öncelik verilmesi sağlanır.

Ağ güvenliğinin sağlanması, her ölçekteki organizasyon için kritik bir gerekliliktir. Firewall, ağ trafiğini denetleyerek zararlı veya yetkisiz erişim girişimlerini engelleyen önemli bir güvenlik katmanıdır. Geleneksel güvenlik duvarları statik ve dinamik paket filtreleme yaparak belirlenen kurallara göre trafiği yönetirken, gelişmiş Derin Paket İnceleme (DPI) ve Saldırı Tespit ve Önleme Sistemleri (IPS/IDS) ile güvenlik seviyesini artıran yeni nesil güvenlik çözümleri kullanılmaktadır. Özellikle SD-WAN altyapılarında, uç noktalardaki güvenlik politikalarının merkezi olarak uygulanması için entegre güvenlik duvarları büyük önem taşımaktadır.

Kablosuz ağ bağlantılarının artmasıyla birlikte, AP (Access Point), kablosuz cihazların bir ağa bağlanmasını sağlayan önemli bir bileşen haline gelmiştir. Wi-Fi teknolojisini destekleyen erişim noktaları, özellikle geniş alanlarda kablosuz bağlantıların optimize edilmesini sağlar. Günümüzde 802.11ac, 802.11ax (Wi-Fi 6) gibi yeni nesil kablosuz iletişim standartları sayesinde daha yüksek hızlar, düşük gecikme süreleri ve artırılmış güvenlik özellikleri sunulmaktadır.

Mobil bağlantı gereksinimleri ve uzak lokasyonlardaki internet erişim ihtiyacı, LTE modemler ve SD-WAN cihazlarının yaygınlaşmasını sağlamıştır. LTE modemler, hücresel ağlar üzerinden kesintisiz internet erişimi sağlarken, SD-WAN cihazları farklı bağlantılar arasında akıllı trafik yönlendirme, uygulama bazlı optimizasyon ve merkezi yönetim gibi avantajlar sunar (Çınar, 2020). Geleneksel WAN yapılarının yerini alan SD-WAN teknolojisi, MPLS, LTE, DIA gibi farklı bağlantı türlerini destekleyerek ağ performansını artırırken, işletmelere maliyet avantajı sağlar.

2.1.3.2 Protokoller ve standartlar

Protokoller ve standartlar, bilgisayar ağlarında veri iletimini düzenleyen kurallar ve yönergeler bütünüdür. Ağ cihazları ve sistemler arasındaki iletişimin uyumlu ve güvenilir

bir şekilde gerçekleşmesini sağlayarak, farklı üreticilere ait donanım ve yazılımların birbiriyle sorunsuz çalışmasını mümkün kılar (Kurose, 2010). TCP/IP, HTTP, FTP, SNMP, ICMP ve BGP gibi yaygın protokoller, ağ trafiğini yönetirken, IEEE 802.11, ISO/OSI ve ITU-T standartları ise ağ altyapısının belirli kriterlere uygun şekilde yapılandırılmasını sağlar.

2.1.3.3 Adresleme

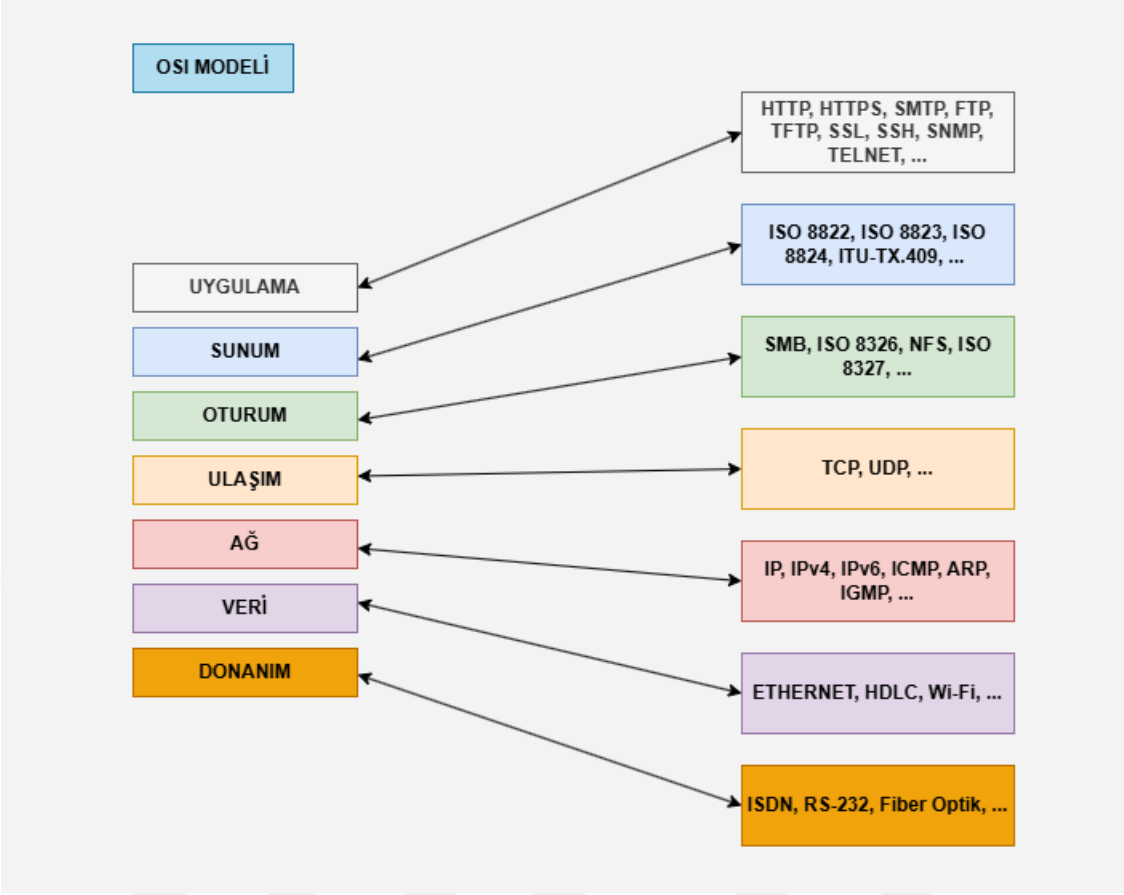
Adresleme (IPv4, IPv6), bilgisayar ağlarında cihazların birbirini tanımlaması ve veri iletimini yönlendirmesi için kullanılan temel bir mekanizmadır. IPv4 (Internet Protocol Version 4), 32 bitlik adresleme yapısıyla uzun yıllar internetin temel adresleme protokolü olarak kullanılmışken, artan cihaz sayısı ve adres yetersizliği nedeniyle IPv6 (Internet Protocol Version 6) geliştirilmiştir (Kurose, 2010). 128 bitlik adresleme kapasitesine sahip olan IPv6, daha fazla adres alanı, gelişmiş güvenlik özellikleri ve daha verimli yönlendirme mekanizmaları sunarak modern ağ altyapılarında giderek yaygınlaşmaktadır.

2.2 Veri İletimi ve Katmanlar

Veri iletimi ve katmanlar, bilgisayar ağlarında bilgilerin kaynak ile hedef arasında düzenli, güvenilir ve verimli bir şekilde aktarılmasını sağlayan yapılandırılmış bir sistemdir. OSI (Open Systems Interconnection) modeli ve TCP/IP modeli, veri iletim sürecini farklı katmanlara bölerek, her seviyede belirli görevlerin yerine getirilmesini sağlar. Fiziksel katmandan uygulama katmanına kadar uzanan bu yapılar, veri paketlerinin oluşturulması, yönlendirilmesi, hata kontrolü ve güvenliğini yöneterek ağ iletişiminin standartlara uygun ve uyumlu bir şekilde gerçekleşmesini sağlar.

2.2.1 OSI modeli ve katmanları

OSI (Open Systems Interconnection) modeli, bilgisayar ağlarında veri iletimini yedi katmana ayırarak standartlaştıran bir referans modelidir (Bora, 2014). Her katman, belirli bir iletişim işlevini yerine getirerek, farklı sistemler ve cihazlar arasında uyumlu ve verimli veri alışverişini sağlar. Fiziksel, Veri Bağı, Ağ, Taşıma, Oturum, Sunum ve Uygulama katmanlarından oluşan OSI modeli, ağ cihazları ve protokollerin birbiriyle sorunsuz çalışmasını sağlamak için geliştirilmiş evrensel bir çerçevedir.



Şekil 1. OSI Modeli

Şekil 1, OSI (Open Systems Interconnection) modelinin yedi katmanını ve her katmanda kullanılan bazı protokoller gösterilmiştir.

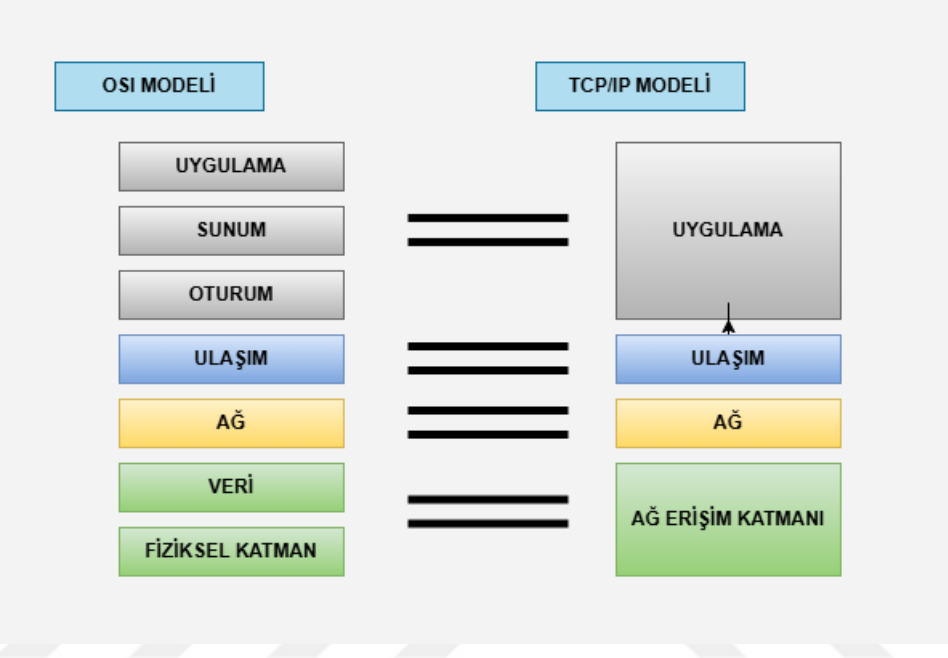
2.2.2 TCP/IP modeli ve işleyişi

TCP/IP (Transmission Control Protocol/Internet Protocol) modeli, internet ve benzeri bilgisayar ağlarında iletişim protokollerinin düzenlenmesi için kullanılan bir çerçevedir. Bu model, verilerin nasıl paketleneceğini, adresleneceğini, iletileceğini, yönlendirileceğini ve alınacağını belirleyen dört soyutlama katmanından oluşur (Wright, 1994).

- Bağlantı Katmanı (Link Layer), Tek bir ağ segmenti içinde kalan veriler için iletişim yöntemlerini içerir.
- İnternet Katmanı (Internet Layer), Bağımsız ağlar arasında internetworking sağlar.
- Taşıma Katmanı (Transport Layer), Ana bilgisayarlar arası iletişimi yönetir.

- Uygulama Katmanı (Application Layer), Uygulamalar için süreçten sürece veri alışverişi sağlar.

Bu katmanlar, verilerin kaynak ile hedef arasında güvenilir ve düzenli bir şekilde iletilmesini sağlar.



Şekil 2. OSI Model ve TCP IP Model Karşılaştırması

Şekil 2, OSI (Open Systems Interconnection) modeli ile TCP/IP (Transmission Control Protocol/Internet Protocol) modeli arasındaki katmanları karşılaştırmaktadır. OSI modeli yedi katmandan oluşurken, TCP/IP modeli dört katmana sahiptir. Uygulama, taşıma ve internet katmanları her iki modelde doğrudan karşılık bulurken, veri bağı ve fiziksel katmanları, TCP/IP modelinde ağ erişim katmanı altında birleştirilmiştir. Görsel, iki model arasındaki hiyerarşik yapının nasıl eşleştiğini göstermektedir.

2.2.3 Yönlendirme ve anahtarlama

Routing (Yönlendirme) ve switching (Anahtarlama), bilgisayar ağlarında veri paketlerinin hedef noktaya en verimli şekilde ulaşmasını sağlayan iki temel mekanizmadır. Routing, farklı ağlar arasındaki veri trafiğini yöneterek, paketlerin en uygun yolu takip etmesini sağlayan işlemdir ve genellikle router cihazları tarafından gerçekleştirilir. Switching ise, aynı ağ içindeki cihazlar arasında veri iletimini düzenleyen

bir süreçtir ve switch cihazları tarafından gerçekleştirilir (Lammle, 2013). Routing, ağ katmanında çalışırken, Switching veri bağı katmanında işlev görür ve her ikisi de ağ performansını ve iletişim verimliliğini artıran süreçlerdir.

2.3 Ağ Güvenliği

Ağ güvenliği, bilgisayar ağlarını yetkisiz erişim, veri ihlalleri, kötü amaçlı yazılımlar ve diğer siber tehditlerden korumayı amaçlayan bir dizi teknoloji, politika ve uygulamadan oluşur. Güvenlik duvarları (firewall), saldırı tespit ve önleme sistemleri (IDS/IPS), sanal özel ağlar (VPN), şifreleme ve kimlik doğrulama mekanizmaları, ağ güvenliğini sağlamak için yaygın olarak kullanılan yöntemler arasındadır (Şahinaslan & Şahinaslan, 2019). Kurumsal ve bireysel düzeyde siber güvenliği artırmak için sürekli izleme, güvenlik politikalarının uygulanması ve güvenlik tehditlerine karşı proaktif önlemler alınması için önemlidir.

2.3.1 Güvenlik duvarları

Güvenlik duvarı, SD-WAN mimarilerinde ağ trafiğini izleyen ve belirlenen güvenlik kurallarına göre filtreleyerek yetkisiz erişimleri engelleyen önemli güvenlik bileşenlerindendir. SD-WAN çözümleri içerisinde paket filtreleme, durum bilgisi tabanlı denetim (stateful inspection), derin paket inceleme (DPI) ve UTM (Unified Threat Management) gibi gelişmiş güvenlik teknikleri entegre edilerek, hem gelen hem de giden trafik merkezi olarak kontrol edilir. Donanım veya yazılım tabanlı olarak konumlandırılabilen bu güvenlik duvarları, SD-WAN altyapısında uç noktalar ile merkez arasında güvenli iletişim sağlayarak, ağın iç ve dış tehditlere karşı korunmasını ve genel sistem güvenliğinin artırılmasını destekler.

2.3.2 Sanal özel ağlar ve internet güvenlik protokolü

Sanal Özel Ağlar (VPN - Virtual Private Network) ve IPsec (Internet Protocol Security), ağ üzerindeki veri iletimini şifreleyerek güvenli ve özel bir iletişim sağlayan teknolojilerdir. VPN, uzak kullanıcıların veya şubelerin güvenli bir şekilde merkezi ağa bağlanmasını sağlarken, IPsec protokolü, veri paketlerini şifreleyerek ve kimlik doğrulama mekanizmaları kullanarak ağ trafiğinin bütünlüğünü ve gizliliğini korur (Mao,

2012). Kurumsal ve bireysel kullanımlarda yaygın olarak tercih edilen bu çözümler, güvenli uzaktan erişim, şube bağlantıları ve hassas verilerin korunması için önemlidir.

2.4 Ağ Yönetimi ve Optimizasyonu

Ağ yönetimi ve optimizasyonu, bir ağın performans, güvenlik ve verimlilik açısından sürekli izlenmesini, yönetilmesini ve iyileştirilmesini sağlayan süreçler bütünüdür. SNMP (Simple Network Management Protocol), NetFlow, SDN (Software-Defined Networking) ve yapay zeka destekli analiz sistemleri, ağ trafiğini izleyerek olası sorunları önceden tespit eder ve ağ kaynaklarının en verimli şekilde kullanılmasını sağlar. Bant genişliği yönetimi, yük dengeleme, QoS (Quality of Service) uygulamaları ve SLA (Service Level Agreement) kontrolleri, ağın optimize edilerek hızlı, güvenilir ve kesintisiz hizmet sunmasını sağlayan önemli unsurlardır.

2.4.1 Hizmet düzeyi anlaşmaları ve hizmet kalitesi

SLA (Service Level Agreement) ve QoS (Quality of Service), ağ hizmetlerinin performansını, güvenilirliğini ve kullanılabilirliğini belirleyen önemli bileşenlerdir (Numan, 2019). SLA, bir hizmet sağlayıcı ile müşteri arasında yapılan ve hizmetin sunulma süresi, gecikme, bant genişliği ve kesinti süreleri gibi performans kriterlerini tanımlayan bir anlaşmadır (Nicolazzo, 2024). QoS ise, ağ üzerindeki veri trafiğini önceliklendirerek gecikme, paket kaybı ve bant genişliği tahsisini optimize eden bir mekanizmadır.

2.4.2 Ağ izleme ve yönetim protokolleri

Ağ İzleme ve Yönetim Protokolleri, ağ altyapısının performansını ve güvenliğini sağlamak için kullanılan veri toplama ve analiz mekanizmalarıdır.

SNMP (Simple Network Management Protocol), yönlendiriciler, anahtarlar ve sunucular gibi ağ cihazlarından performans verileri toplayarak merkezi bir yönetim sistemine ileten bir protokoldür. Ağ trafiği, cihaz durumu ve hata tespiti gibi bilgileri yöneticilere sunarak, ağın sürekli izlenmesini ve yönetilmesini sağlar.

NetFlow, Cisco tarafından geliştirilen bir trafik analiz protokolü olup, ağ trafiğinin detaylı izlenmesine ve analiz edilmesine olanak tanır. Kaynak ve hedef IP adresleri, protokol

türü, port numaraları ve trafik hacmi gibi bilgileri toplayarak, ağ yöneticilerinin bant genişliği yönetimi, anormallik tespiti ve güvenlik tehditlerinin analizi gibi önemli süreçleri optimize etmelerine yardımcı olur.

2.4.3 Yazılım tabanlı ağ yönetimi

SDN (Software-Defined Networking) Yönetimi, ağ altyapısını daha esnek, merkezi ve otomatik yönetilebilir hale getiren modern bir ağ mimarisidir. Geleneksel ağ yapılarından farklı olarak, SDN yönetimi, kontrol düzlemi (control plane) ile veri düzlemini (data plane) birbirinden ayırarak, ağ cihazlarının merkezi bir yazılım tarafından yönetilmesini sağlar.

SDN teknolojileri, ağ yönetimindeki karmaşıklığı azaltmak, dinamik ve ölçeklenebilir ağ çözümleri sağlamak, yönetim ve otomasyon süreçlerini iyileştirmek, maliyetleri düşürmek ve güvenliği artırmak amacıyla ortaya çıkmıştır (Paillisse, 2021). Modern iş ortamlarının değişen ihtiyaçlarını karşılamak için SDN, geleneksel ağ yönetim yöntemlerine kıyasla daha esnek ve etkili çözümler sunar. Bu avantajlar, SDN'nin giderek daha fazla benimsenmesine ve yaygınlaşmasına neden olmaktadır.

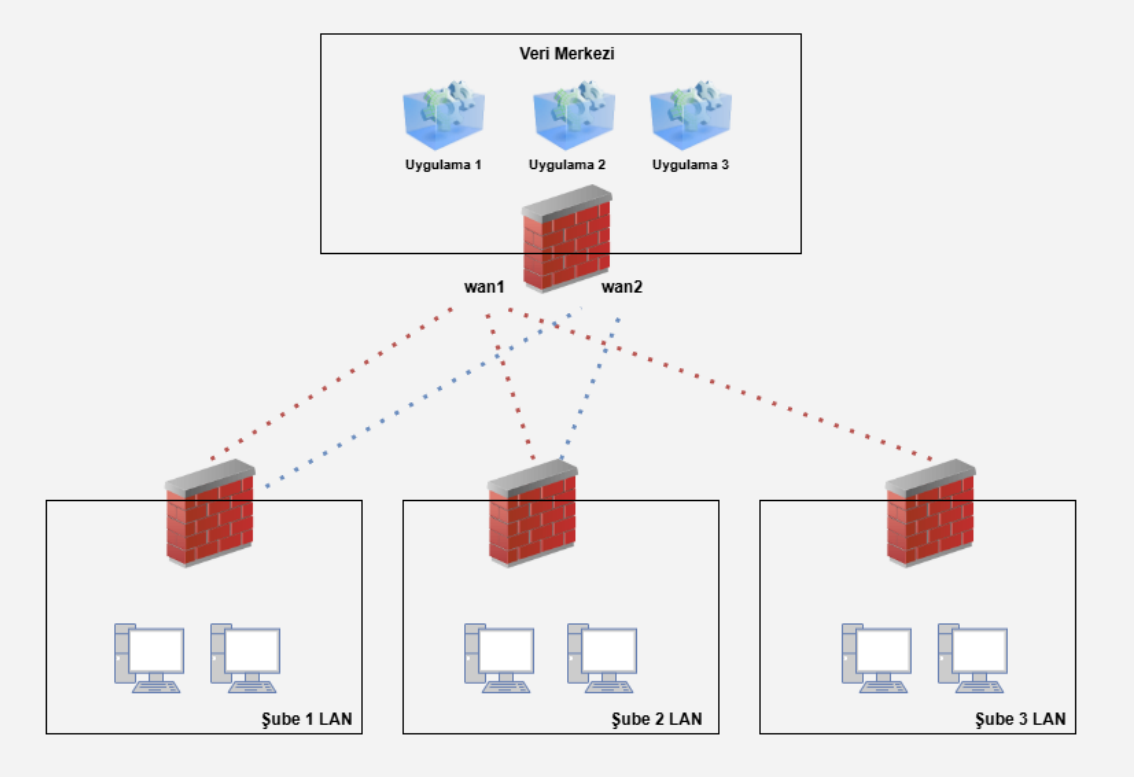
2.5 SD-WAN mimarisi

SD-WAN mimarisi, geleneksel geniş alan ağlarından farklı olarak yazılım tabanlı merkezi yönetim, dinamik yönlendirme ve uygulama farkındalıklı trafik optimizasyonu sağlayan modern bir ağ çözümüdür. Bu mimari, MPLS, LTE, DIA gibi farklı bağlantı türlerini destekleyerek, bant genişliği kullanımını iyileştirme, güvenlik politikalarını merkezi olarak uygulama ve hizmet kalitesini (QoS) artırma gibi kritik avantajlar sunmaktadır (Tahenni, 2023). Şube ağları, bulut entegrasyonu ve IOT sistemleri gibi geniş ölçekli yapılarda ağ yönetimini kolaylaştıran SD-WAN, hizmet seviyesi anlaşmalarını (SLA) etkin şekilde denetleyerek kesintisiz ve güvenli bir iletişim altyapısı sağlamaktadır.

Tablo 2. Ağ Topolojisi Bileşenleri

Element	**Açıklama**
Wan1	Ana Hat
Wan 2	Yedek Hat
Application1-3	Şirket İş Uygulamaları
Data Center	Veri Merkezi

Tablo 2, farklı ağ elemanlarını ve bu elemanların açıklamalarını göstermektedir. Örneğin: Bir şirketin ağı, Wan1 üzerinden internete bağlanır. Wan2 arıza durumunda devreye girer, şirketin kritik uygulamaları Application1-3 üzerinde çalışır ve tüm veriler Veri Merkezi'nde saklanır.



Şekil 3. Basit Ağ Örneği

Şekil 3, bir veri merkezine bağlı olan şubelerden oluşan basit bir ağ yapısını göstermektedir. Örneğin: Bir şirketin merkezi veri merkezinde kritik uygulamalar

barındırılırken, farklı şubeler bu uygulamalara WAN1 ve WAN2 hatları üzerinden erişim sağlar. Bu yapı, ağın kesintisiz ve güvenilir çalışmasını sağlar.

Şekil 3'de basit yapıda görülen elementler geleneksel ağ ve SD-WAN' da ortak bileşenlerdir. Ağ altyapısı tasarlanırken, olası hat kesintilerinde hizmet kesintisini önlemek ve maksimum performans sağlamak mühendisin temel amaçlarındandır. SD-WAN'a neden ihtiyaç duyulduğunu anlamadan önce geleneksel yapıdan kısaca bahsedelim.

Şube sayısı fazla olan şirketlerde uç noktanın (şube, mağaza, depo, operasyon merkezleri vb.) performanslı bir şekilde hizmet kesintisi olmadan çalıştığından emin olmak önemlidir. Uç nokta tasarlanırken bazı büyük yapılarda hem router hem de hat yedekliliği sağlanır. Bazı yapılarda iki hat aynı cihazda sonlandırılır. Hatlardan biri kesildiğinde şube trafiğinin diğer hattan devam etmesi garantilenmiş olur.

Yedeklilik sağlandığında sıra güvenliğe gelir. Uç noktanın merkezi uygulamalara yaptığı trafik, tesis edilen hat üzerinden internet servis sağlayıcı omurgasından geçerek veri merkezindeki uygulama sunucularına ulaşır. Trafik bu yolu takip ederken, internet servis sağlayıcı omurgasından geçtiği için güvenliği sağlamak adına MPLS hattı kullanılır. MPLS, şirkete tahsis edilen etiketlerle trafiği etiketleyip noktadan noktaya taşırken veri içeriğine bakılmamasını sağlar. Ancak, MPLS yüksek maliyetli bir hizmet olduğundan SD-WAN teknolojisinin doğuşunu hızlandırmıştır.

Şube İhtiyaçları:

- Performans
- Önceliklendirme
- Kesintisiz hizmet

Şubelerde kullanılan bazı uygulamalar, şirketin yaşam döngüsünün temel yapı taşlarıdır. Örneğin, bir banka şubesinde müşteriye kredi verirken merkeze gidip gelen trafiğin hızı ve hatasız oluşu ya da markette kasiyerin müşteriden ödeme alırken POS cihazının tepki süresi işin kalitesini ve verimliliğini etkileyen faktörlerdir. Bu yapılar kurulduğunda, sıradan bir işlem ile elzem bir uygulama trafiğini birbirinden ayıran bazı düzenlemeler

yapılmalıdır. Burada QoS (Quality of Service) devreye girer. Hangi uygulamanın bant genişliğini ne kadar kullanacağını ayarlayarak performansı optimize eder.

2.6 Domainler Arası WAN Paylaşımı

Domainler arası WAN paylaşımı, farklı ağ domainlerinin arasında veri ve kaynakların paylaşılmasını sağlayan bir ağ yönetim tekniğidir. Bu paylaşım, ağın farklı segmentlerinin birbirleriyle etkin ve güvenli bir şekilde iletişim kurmasını mümkün kılar (Segeč, 2020). SD-WAN teknolojisi, yazılım tanımlı ağ yönetimi sayesinde, bu tür paylaşımları daha esnek ve dinamik bir şekilde yapar. Geleneksel ağlarda, domainler arası iletişim genellikle karmaşık ve maliyetli olabilen fiziksel bağlantılar veya statik yönlendirme tabloları üzerinden gerçekleştirilirken, SD-WAN, sanal ağ katmanları oluşturarak bu süreci basitleştirir ve optimize eder.

2.7 Domainler Arası WAN Paylaşımının Önemi

Domainler arası WAN paylaşımı, özellikle büyük ölçekli ve coğrafi olarak dağılmış ağlarda büyük önem taşır (Fu, 2024). Bu paylaşımın sağladığı başlıca avantajlar şunlardır:

- Verimlilik Artışı: Farklı ağ domainleri arasında veri ve kaynakların sorunsuz paylaşımı, işletmelerin operasyonel verimliliğini artırır.
- Esneklik ve Ölçeklenebilirlik: SD-WAN sayesinde ağ yöneticileri, ağ yapılandırmalarını hızla değiştirebilir ve yeni kaynakları ağlarına entegre edebilirler.
- Maliyet Tasarrufu: Fiziksel bağlantılara olan bağımlılığı azaltarak ve ağ yönetimini otomatikleştirerek maliyetleri düşürür.
- Güvenlik: Domainler arası iletişimde güvenlik politikalarını merkezi olarak yönetme ve uygulama imkanı sunar.

2.8 Geleneksel WAN ile SD-WAN Karşılaştırması

Geleneksel WAN yapılarda;

- Statik ve Hantal Yapı: Geleneksel WAN sistemleri, sabit ve statik yönlendirme kuralları ile çalışır, bu da ağ trafiğini verimli yönetmeyi zorlaştırır.
- Yüksek Maliyet: Fiziksel bağlantıların kurulumu ve bakımı, yüksek maliyetlere neden olur.

- Kısıtlı Esneklik: Ağ yapılandırmalarını değiştirmek zordur ve yeni şubeler eklemek zaman alıcıdır.
- Güvenlik: Güvenlik politikaları çoğunlukla fiziksel cihazlar üzerinden yönetilir, bu da esneklikten ödün vermek anlamına gelir.

SD-WAN yapısında;

- Dinamik ve Esnek Yapı: SD-WAN, yazılım tabanlı yönetim ile ağ trafiğini dinamik olarak yönlendirir ve optimize eder.
- Maliyet Etkinliği: Sanal bağlantılar kullanarak maliyetleri düşürür ve mevcut geniş bant bağlantılarından daha fazla yararlanır (Patel, 2022).
- Yüksek Esneklik: Ağ yapılandırmaları hızla değiştirilebilir ve yeni şubeler kolayca eklenebilir.
- Gelişmiş Güvenlik: Güvenlik politikaları merkezi olarak yönetilir ve uygulama seviyesinde güvenlik sağlar.

2.9 SD-WAN ile Domainler Arası WAN Paylaşımı

2.9.1 Teknik inceleme

SD-WAN teknolojisi, geleneksel WAN altyapılarından farklı olarak yazılım tanımlı bir yaklaşımla çalışır ve ağ trafiğini merkezi bir kontrol mekanizması üzerinden yönetir. Bu teknoloji, fiziksel donanım bağımlılığını azaltır ve ağ yönetimini sanallaştırır. SD-WAN'ın teknik olarak en belirgin özelliklerinden biri, ağın uç noktalarına (şubeler, veri merkezleri vb.) yerleştirilen SD-WAN cihazları aracılığıyla trafiği yönlendirmesidir. Bu cihazlar, ağ trafiğini analiz eder ve en verimli rotayı belirler. Ayrıca, SD-WAN, MPLS (Multi-Protocol Label Switching), geniş bant internet ve LTE gibi çeşitli bağlantı türlerini entegre ederek çoklu bağlantı seçenekleri sunar. Böylece ağ performansını ve kullanılabilirliğini artırır. Güvenlik açısından ise, SD-WAN cihazları uçtan uca şifreleme, güvenlik duvarları ve tehdit tespit sistemleri gibi özelliklerle donatılmıştır.

2.9.2 SD-WAN'ın domainler arası wan paylaşımına getirdiği yenilikler

SD-WAN teknolojisi, sunduğu merkezi yönetim ve kontrol, ağ yöneticilerinin tüm ağ yapılandırmalarını tek bir platform üzerinden yönetmesine olanak tanır. Bu, özellikle

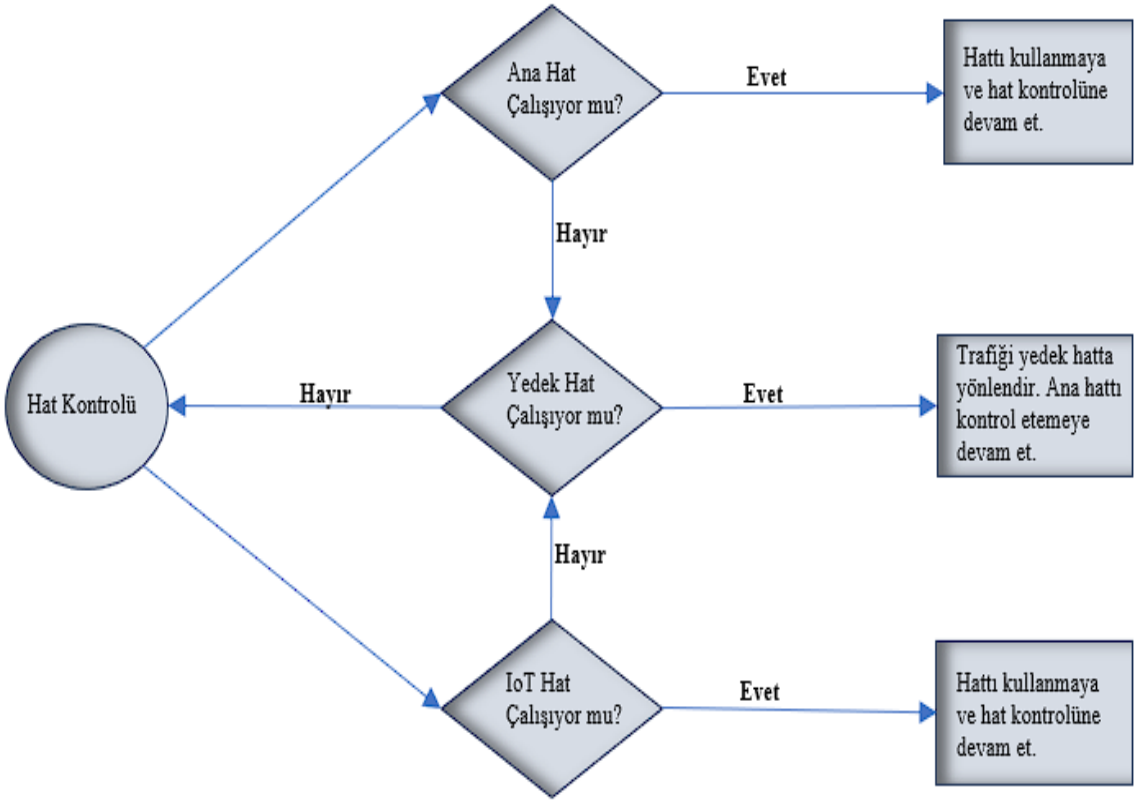
büyük ve dağıtık ağ yapılarında önemli bir avantaj sağlar. Ayrıca, SD-WAN, akıllı yönlendirme algoritmaları sayesinde, ağ trafiğini gerçek zamanlı olarak optimize eder ve en verimli rotaları kullanarak gecikmeleri minimize eder (Ouamri, 2024). Bu, yüksek bant genişliği gerektiren uygulamalar ve hizmetler için önemlidir. SD-WAN, sunduğu otomatik yapılandırma ve yönetim özellikleri ile yeni bir şube veya cihaz ağa eklendiğinde, SD-WAN otomatik olarak yapılandırma ayarlarını uygular ve entegrasyon sürecini hızlandırır. Güvenlik açısından, SD-WAN uçtan uca şifreleme ve tehdit tespiti gibi gelişmiş güvenlik protokolleri ile donatılmıştır, bu da domainler arası veri paylaşımının güvenliğini arttırılmasına katkı sağlar.

2.9.3 Kullanım senaryoları

SD-WAN'ın domainler arası WAN paylaşımında kullanımı çeşitli senaryolarda önemli avantajlar sağlamaktadır. Örneğin, küresel bir şirketin farklı kıtalardaki ofislerini düşünelim. Bu ofisler arasında veri paylaşımı ve iletişimin önemi yüksektir. SD-WAN, bu ofislerin birbirleriyle yüksek hızda ve güvenli bir şekilde iletişim kurmasını sağlar. Bir diğer kullanım senaryosu, IOT (Nesnelerin İnterneti) cihazlarının yoğun olduğu bir fabrikadır. Fabrikadaki tüm IOT cihazlarının verileri, SD-WAN sayesinde merkezi bir veri merkezine etkin bir şekilde yönlendirilir ve işlenir. Ayrıca, bir perakende zincirinin farklı şehirlerdeki mağazaları arasında envanter ve satış verilerinin paylaşılması gerektiğinde, SD-WAN, bu verilerin hızlı ve güvenli bir şekilde aktarılmasını sağlar.

3. YÖNTEM

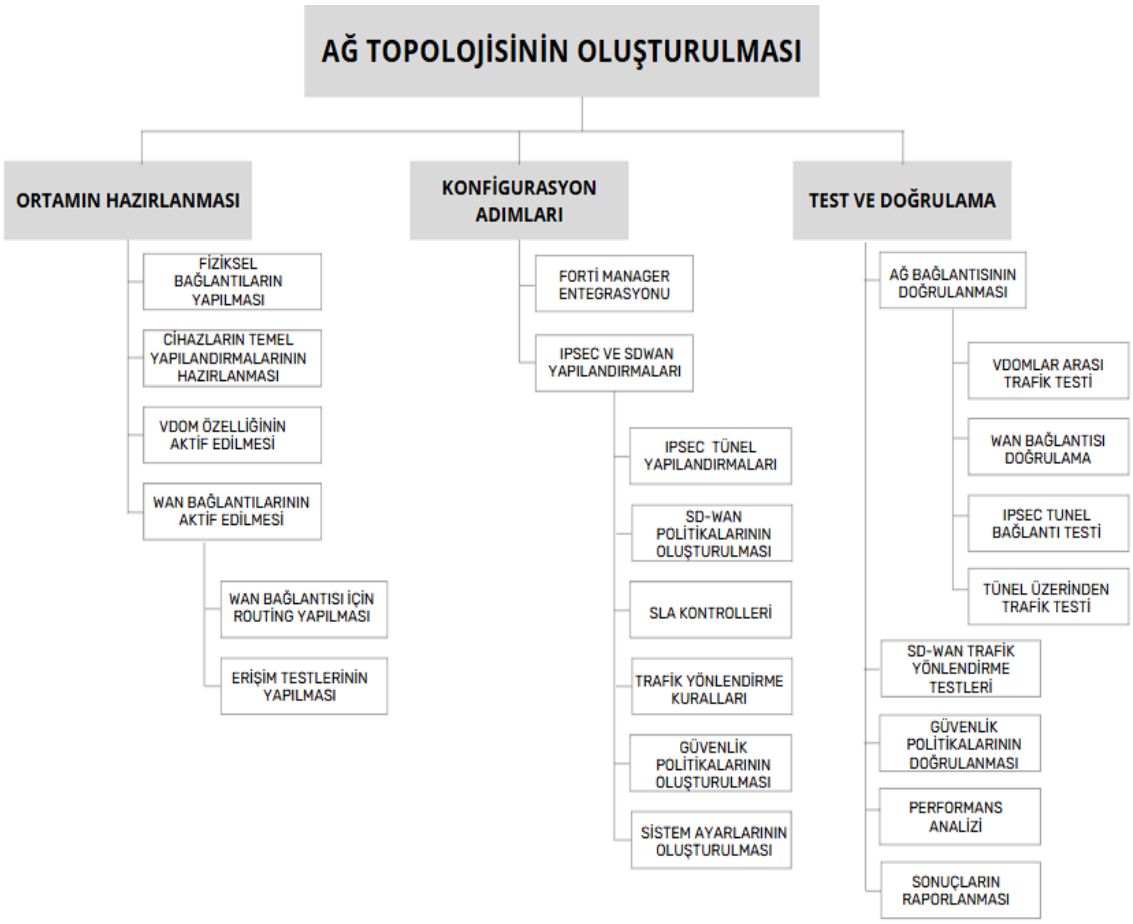
Bu bölümde, SD-WAN teknolojisi kullanılarak iki farklı domain arasında WAN paylaşımının sağlanması hedeflenmiştir. Çalışmanın yöntemi üç temel başlık altında ele alınmıştır. İlk olarak, ağ topolojisinin oluşturulması ve fiziksel/mantıksal altyapının hazırlanmasına odaklanılmıştır. İkinci aşamada, konfigürasyon adımları detaylandırılarak VDOM yapılandırması, NPU Link üzerinden WAN paylaşımı, IPsec tünellerin kurulumu ve SD-WAN politikalarının oluşturulması açıklanmıştır. Son aşamada ise, yapılandırmaların doğruluğunu ve sistem performansını değerlendirmek amacıyla test adımları gerçekleştirilmiş ve sonuçlar analiz edilmiştir. Bu sistematik yaklaşım, yapılandırmanın güvenilir ve optimize bir şekilde tamamlanmasını amaçlamaktadır.



Şekil 4. Yedeklilik Algoritması

Şekil 4'te hazırlanan yedeklilik algoritması ile SD-WAN'ın paylaşımlı hat senaryosunda karar mekanizması gösterilmiştir.

3.1 Ağ Topolojisinin Oluşturulması



Şekil 5. SD-WAN Domainler Arası WAN Paylaşımı Kurulum Diyagramı

Şekil 5'de bulunan akış diyagramı, SD-WAN teknolojisi kullanılarak iki farklı domain arasında WAN paylaşımını gerçekleştirmek için izlenen yöntemin genel sürecini özetlemektedir.

Diyagram, yöntemin sistematik bir şekilde ilerleyişini göstermek ve süreç boyunca takip edilecek adımları netleştirmek amacıyla hazırlanmıştır.

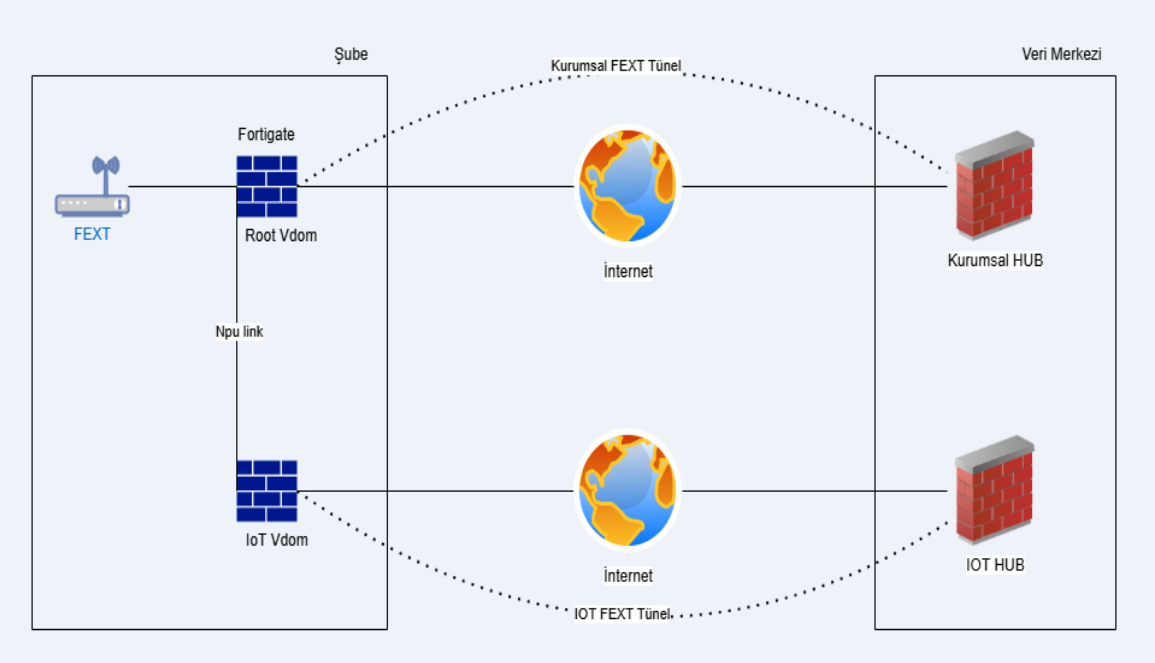
,

Tablo 3. IP Tablosu

Bölge	Ağ Bileşeni	IP/Subnet	Açıklama
Root VDOM	WAN	192.168.1.1/29	Root VDOM WAN IP
	Tünel IP (Interface)	192.168.2.1/29	Root VDOM IPsec Tünel IP
	LAN Subnet	10.10.10.0/24	Root VDOM Local Subnet
	NPU Link 1	192.168.50.1/30	Root VDOM NPU Link IP
	Management IP	192.168.0.99/24	FortiGate Yönetim Arayüzü IP
IoT VDOM	WAN	NPU Link (192.168.50.2)	IoT VDOM WAN (NPU Link üzerinden)
	Tünel IP (Interface)	192.168.20.1/29	IoT VDOM IPsec Tünel IP
	LAN Subnet	10.10.20.0/24	IoT VDOM Local Subnet
Merkez HUB	LTE IPsec Peer	172.16.1.1/32	Root VDOM için Merkez HUB LTE Peer
	SLA Loopback	172.16.2.2/32	Root VDOM için SLA Test IP
IoT HUB	LTE IPsec Peer	172.16.10.10/32	IoT VDOM için IoT HUB LTE Peer
	SLA Loopback	172.16.20.20/32	IoT VDOM için SLA Test IP

Tablo 3'de test süreci boyunca kullanılacak tüm ağ bileşenlerini, subnetleri ve bağlantı ilişkilerini detaylı bir şekilde sunmaktadır.

Tablo, Root ve IOT VDOM'lar ile Merkez ve IOT HUB cihazları arasındaki WAN, LAN ve tünel yapılandırmalarında kullanılacak ip adreslerini göstermektedir. Bu plan, tüm yapılandırmalar ve trafik yönlendirme işlemleri için referans niteliği taşımaktadır.



Şekil 6. Tek Hat Kullanılarak Oluşturulan Ağ Topolojisi

Şekil 6, tek hat kullanılarak domainler arası wan paylaşımının kullanımı için çizilmiş bir topolojidir.

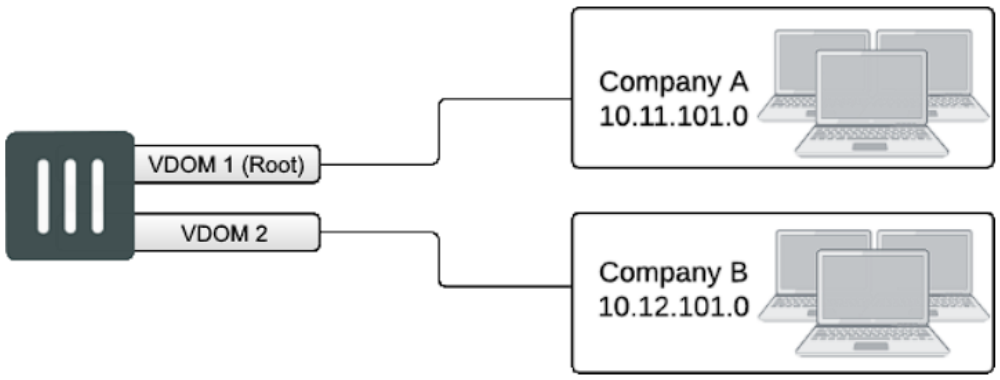
3.2 Lab Ortamın Hazırlanması

Test sürecinin başarılı bir şekilde yürütülebilmesi için önemlidir. Bu aşamada, fiziksel bağlantıların düzenlenmesi, temel cihaz yapılandırmalarının yapılması ve IP adresleme planına uygun ağ altyapısının oluşturulması hedeflenir.

3.2.1 Fiziksel bağlantıların yapılandırılması

Ağ ekipmanlarının ve bileşenlerinin fiziksel olarak doğru şekilde yerleştirilmesi ve bağlantılarının sağlanması, ağın sağlıklı çalışması için temel bir adımdır. Bu kapsamda, WAN portu internet bağlantısı için, LAN portları ise yerel ağ bağlantıları için kullanılır. Root VDOM'un WAN bağlantısı, router'ın wan1 portu üzerinden gerçekleştirilmiş olup, bu porta 192.168.1.1/29 IP adresi atanarak internet sağlayıcısına bağlantı sağlanmıştır. Yerel ağ tarafında ise Root VDOM'a 10.10.10.0/24 IP bloğu atanarak LAN bağlantısı yapılandırılmıştır.

3.2.2 VDOM özelliğinin aktif edilmesi



Şekil 7. Bağımsız VDOM'lar

Şekil 7'de VDOM yapısının mantıksal gösterimi ele alınmıştır.

VDOM (Virtual Domain), FortiGate cihazlarında birden fazla bağımsız ağ domaini oluşturmayı sağlayan sanallaştırma teknolojisidir. Bu özellik, tek bir fiziksel cihaz üzerinde birden fazla mantıksal ağ yapılandırması yapılmasına olanak tanır. Her VDOM,

kendi güvenlik politikalarını, rotalarını ve konfigürasyonlarını bağımsız olarak yönetebilir. IOT ve Root VDOM'ları birbirleriyle haberleştirmek için npu link interface kullanılmıştır. NPU Link , Root VDOM'da kalacak. NPU Link 2, IOT VDOM'a atanacak. Bu atamalarla birlikte npu link interfacelerine aynı subnet içerisinden 2 farklı ip adresi kullanılarak 2 vdom arasında haberleşmeyi sağlayacağız. Bu haberleşme ile beraber tek wan interface üzerinden ipsec trafiğini farklı noktalara götürebileceğiz.

```
config vdom
    edit "Root"
    next
    edit "IoT"
    next
end
```

Şekil 8. Root ve IOT VDOM'ların Oluşturulması

Şekil 8'de "Root" ve "IOT" isimleriyle iki bağımsız VDOM'un nasıl oluşturulacağı gösterilmiştir. Her bir VDOM, kendi trafik yönlendirme kurallarına ve güvenlik politikalarına sahip olacak şekilde izole edilmiştir.

```
config system interface
    edit "wan1"
        set vdom "Root"
    next
    edit "npu-link1"
        set vdom "Root"
    next
    edit "npu-link2"
        set vdom "IoT"
    next
end
```

Şekil 9. Fiziksel Portların ve NPU Link'lerin VDOM'lara Atanması

Şekil 9'da fiziksel portların ve npu linklerin vdomlara ataması gösterilmiştir.

3.2.3 WAN bağlantılarının aktif edilmesi

Root ve IOT VDOM'lar için WAN bağlantılarının yapılandırılması ele alınır. IOT VDOM, NPU Link üzerinden root VDOM'a trafik yönlendirecek şekilde yapılandırılır. Root VDOM ise WAN1 portu üzerinden merkezdeki IPsec tünel cihazına bağlanır. Her iki VDOM için gerekli IP adresleri atanır ve rotalar yazılarak trafik yönlendirilir.

Root VDOM, fiziksel WAN bağlantısı olarak WAN1 portunu kullanacak şekilde yapılandırılmıştır. Root ile IOT VDOM arasında iletişim sağlamak amacıyla, NPU Link 1 arayüzü devreye alınmış ve bu bağlantıya, NPU Link 2 ile aynı subnet içinde bir IP adresi atanmıştır. Root VDOM üzerinden merkezdeki IPsec cihazına (172.16.1.1/32) ulaşım sağlamak üzere bir statik rota tanımlanmıştır.

IOT VDOM tarafında ise WAN bağlantısı olarak NPU Link 2 yapılandırılmış ve bu arayüz, root VDOM ile iletişimi mümkün kılacak biçimde atanmıştır. Ayrıca, IOT VDOM'dan merkezdeki IOT HUB cihazının loopback adresi olan 172.16.10.10/32'ye trafik yönlendirebilmek için bir statik yönlendirme kuralı uygulanmıştır.

```
config system interface
    edit "wan1"
        set vdom "root"
        set ip 192.168.1.1 255.255.255.248
        set allowaccess ping https ssh
    next
end
```

Şekil 10. Root VDOM WAN1 Fiziksel Bağlantısının Yapılandırılması

Şekil 10'da root VDOM'un fiziksel WAN bağlantısı için gerekli IP adresi ataması örneği gösterilmiştir.

```
config system interface
    edit "npu-link1"
        set vdom "root"
        set ip 192.168.50.1 255.255.255.252
    next
    edit "npu-link2"
        set vdom "IoT"
        set ip 192.168.50.2 255.255.255.252
    next
end
```

Şekil 11. NPU Link'lerin Root ve IOT VDOM'lara Atanması

Şekil 11'de NPU linklerin ip yapılandırması ve vdom atamaları gösterilmiştir.

```
config router static
    edit 1
        set dst 172.16.10.10 255.255.255.255
        set gateway 192.168.50.1
        set device "npu-link2"
    next
end
```

Şekil 12. IOT VDOM'dan Root VDOM'a Trafik Yönlendirme

Şekil 12'de IOT VDOM'daki trafik, NPU Link 2 üzerinden root VDOM'a yönlendirilir. Merkezdeki IOT HUB'ın loopback adresine (172.16.10.10/32) ulaşmak için yazılan rota gösterilmiştir.

```
config router static
    edit 1
        set dst 172.16.1.1 255.255.255.255
        set gateway 192.168.1.2
        set device "wan1"
    next
end
```

Şekil 13. Root VDOM'dan Merkeze Trafik Yönlendirme (IPsec için)

Şekil 13'de root VDOM'daki trafiğin, merkez HUB'ın IPsec loopback adresine (172.16.1.1/32) ulaşmak için WAN1 bağlantısını kullanacak şekilde yönlendirilmesi için gerekli routing çıktısını göstermektedir.

```
config router static
    edit 1
        set dst 172.16.10.10 255.255.255.255
        set gateway 192.168.10.1
        set device "npu-link"
    next
end
```

Şekil 14. Root VDOM'dan Merkeze Trafik Yönlendirme

Şekil 14'de IOT VDOM'undan root VDOM'una taşıdığımız trafiğin, merkezdeki IOT HUB IPsec tünel adresine (172.16.10.10/32) WAN1 fiziksel bağlantısından trafiği taşıması için yapılan rota gösterilmiştir.

3.2.4 Erişim testlerinin yapılması

Erişim testlerinin yapılması, IOT VDOM ile root VDOM arasındaki haberleşmenin ve root VDOM üzerinden merkeze olan trafiğin düzgün bir şekilde yönlendirilip yönlendirilmediğini doğrulamak açısından kritik öneme sahiptir. Bu testler, yapılandırmanın doğru çalıştığını teyit ederek olası bağlantı veya rotalama hatalarını erken tespit etmemizi sağlar ve ilerleyen aşamalarda yapılacak IPsec tünel

konfigürasyonu, SD-WAN politikalarının oluşturulması ve trafik yönetimi gibi işlemlerde karşılaşılabilecek sorunları minimize ederek sürecin daha hızlı ve sorunsuz ilerlemesini sağlar.

```
exec ping 172.16.10.10
PING 172.16.10.10 (172.16.10.10): 56 data bytes
64 bytes from 172.16.10.10: icmp_seq=1 ttl=64 time=10.2 ms
64 bytes from 172.16.10.10: icmp_seq=2 ttl=64 time=10.1 ms
64 bytes from 172.16.10.10: icmp_seq=3 ttl=64 time=10.0 ms
64 bytes from 172.16.10.10: icmp_seq=4 ttl=64 time=10.3 ms
64 bytes from 172.16.10.10: icmp_seq=5 ttl=64 time=10.1 ms

--- 172.16.10.10 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 10.0/10.1/10.3 ms
```

Şekil 15. IOT VDOM NPU Link IP'den IOT HUB IPsec Peer IP Adresine Ping Testi

Şekil 15'de yapılan ping testi IOT VDOM'un NPU Link IP (192.168.50.2) üzerinden IOT HUB'ın IPsec Peer IP (172.16.10.10) adresine 5 ping ile başarılı bir şekilde erişebildiğini doğrular.

```
exec ping 172.16.1.1
PING 172.16.1.1 (172.16.1.1): 56 data bytes
64 bytes from 172.16.1.1: icmp_seq=1 ttl=64 time=15.5 ms
64 bytes from 172.16.1.1: icmp_seq=2 ttl=64 time=15.4 ms
64 bytes from 172.16.1.1: icmp_seq=3 ttl=64 time=15.3 ms
64 bytes from 172.16.1.1: icmp_seq=4 ttl=64 time=15.6 ms
64 bytes from 172.16.1.1: icmp_seq=5 ttl=64 time=15.5 ms

--- 172.16.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 15.3/15.4/15.6 ms
```

Şekil 16. Root VDOM WAN IP'den Merkez HUB Loopback IP Adresine Ping Testi

Şekil 16’da yapılan ping testi root VDOM’un WAN IP (192.168.1.1) adresinden merkez HUB’ın loopback IP (172.16.1.1) adresine başarılı bir şekilde erişebildiğini gösterir.

3.3 Konfigürasyon Adımları

Bu aşamada, IOT ve Root VDOM'lar arasında trafik yönlendirme, IPsec tünel yapılandırması, SD-WAN politikalarının oluşturulması ve güvenlik kurallarının tanımlanması gibi temel işlemler gerçekleştirilecek.

Yapacağımız bu konfigürasyonlar ile bir yandan domainler arası WAN paylaşımını sağlarken diğer yandan ağın sürdürülebilir bir performans ve güvenlik düzeyine ulaşması sağlanacaktır. Konfigürasyon sürecinin doğru şekilde tamamlanması, ilerleyen aşamalarda testlerin başarılı olabilmesi ve ağın işlevselliğinin kesintisiz sürdürülebilmesi açısından önemlidir.

Konfigürasyon adımları, tez çalışmasında belirlenen ağ topolojisi ve IP planlamasına sadık kalınarak hazırlanmıştır.

3.3.1 Forti manager entegrasyonu

FortiManager, FortiGate cihazlarının merkezi olarak yönetilmesi, yapılandırmaların hızlı ve tutarlı bir şekilde dağıtılması ve sistemlerin izlenmesi için kullanılan bir ağ yönetim platformudur. FortiGate cihazlarının FortiManager’a eklenmesi, ADOM ve VDOM bazlı ayrımların yapılması ve merkezi yönetim ayarlarının etkinleştirilmesi hedeflenir. Bu adım, ağdaki tüm güvenlik politikalarının ve yapılandırmaların tek bir merkezden kontrol edilmesini sağlayacaktır.

```
config system central-management
    set mode normal
    set type fortimanager
    set fmg <FortiManager_IP>
    set fmg-source-ip <FortiGate_Management_IP>
end
```

Şekil 17. Forti Manager Konfigürasyonu

Şekil 17'de bulunan CLI komutu FortiGate cihazını FortiManager'a bağlar. "FortiManager_IP" ve "FortiGate_Management_IP" değerleri gerçek ağ yapılandırmasına göre düzenlenir.

Merkezi Yönetim Ayarlarının Yapılandırılması

FortiManager üzerinden merkezi politika ve yapılandırmaların dağıtılabilmesi amacıyla uygun şablonlar oluşturulmuştur. Bu sayede ağ cihazlarının yönetimi merkezi bir noktadan etkin şekilde gerçekleştirilmektedir. Ayrıca, loglama, raporlama ve yedekleme ayarları yapılandırılarak yönetim süreçlerinin takibi kolaylaştırılmış ve sistemin sürdürülebilirliği artırılmıştır.

```
config log fortianalyzer setting
    set status enable
    set server <FortiAnalyzer_IP>
    set upload-option realtime
end
```

Şekil 18. Analyzer Konfigürasyonu

Şekil 18'de bulunan CLI Komutu FortiManager üzerinde loglama işlevini etkinleştirir ve FortiAnalyzer'a log verilerinin gerçek zamanlı olarak gönderilmesini sağlar.

3.4 IPsec ve SD-WAN yapılandırmaları

IPsec (Internet Protocol Security) ve SD-WAN (Software-Defined Wide Area Network), ağ altyapılarının güvenli ve verimli bir şekilde çalışmasını sağlayan iki temel teknolojidir.

IPsec, iki farklı ağ arasında güvenli iletişim sağlamak için kullanılan bir tünelleme protokolüdür. SD-WAN ise farklı WAN bağlantılarını merkezi bir yönetimle optimize ederek trafik yönlendirme ve performans artırımı sağlar.

Bu başlık altında, IPsec tünellerin yapılandırılması, SD-WAN politikalarının oluşturulması, SLA kontrollerinin tanımlanması ve trafik yönlendirme kurallarının belirlenmesi adımları ele alınmıştır. Tüm yapılandırmalar, IOT ve Root VDOM'lar arasında güvenli ve performanslı iletişim sağlamak için tasarlanmıştır.

Bu bölüm, iki domain için IPsec tünellerinin oluşturulmasına odaklanır.

3.4.1 IPsec tünel yapılandırmaları

Root VDOM IPsec tüneli

Amaç, Root VDOM ile Merkez HUB arasında güvenli bir tünel oluşturmak.

Yapılandırma adımları

```
config vpn ipsec phase1-interface
    edit "Root-IPsec"
        set interface "wan1"
        set ike-version 2
        set peertype any
        set net-device enable
        set proposal aes256-sha256
        set dhgrp 14
        set remote-gw 172.16.1.1
        set psksecret "<PSK>"
    next
end
```

Şekil 19. Root Vdom Phase 1 Konfigürasyonu

Şekil 19, root VDOM'un WAN1 arayüzü üzerinden merkez HUB'ın 172.16.1.1 IP adresi ile IPsec tünel kurmasını sağlayan konfigürasyon çıktısını vermiştir. Phase 1'de kullanılan şifreleme algoritmaları ve ön paylaşımlı anahtar (PSK) güvenli iletişim için önemlidir.

```
config vpn ipsec phase2-interface
    edit "Root-IPsec-P2"
        set phase1name "Root-IPsec"
        set proposal aes256-sha256
        set src-subnet 10.10.10.0 255.255.255.0
        set dst-subnet 172.16.100.0 255.255.255.0
    next
end
```

Şekil 20. Root Vdom Phase 2 Konfigürasyonu

Şekil 20'de phase 2'de, Root VDOM'un yerel LAN subneti (10.10.10.0/24) ile merkez HUB'ın subneti (172.16.100.0/24) arasında güvenli trafik akışı için kullanılacak subnetlerin anonsu yapılmıştır.

IOT VDOM IPsec tünel bağlantılarının yapılması :

IOT VDOM ile IOT HUB arasında güvenli bir tünel oluşturmak için gerekli konfigürasyon örneklerinin bazı aşamaları aşağıda gösterilmiştir.

```
config vpn ipsec phase1-interface
    edit "IoT-IPsec"
        set interface "npu-link2"
        set ike-version 2
        set peertype any
        set net-device enable
        set proposal aes256-sha256
        set dhgrp 14
        set remote-gw 172.16.10.10
        set psksecret "<PSK>"
    next
end
```

Şekil 21. IOT Vdom Phase 1 Konfigürasyonu

Şekil 21'de IOT VDOM'un NPU Link 2 üzerinden IOT HUB'ın 172.16.10.10 IP adresi ile güvenli bir tünel oluşturmasını sağlamak için yapılan konfigürasyon çıktısıdır.

```
config vpn ipsec phase2-interface
    edit "IoT-IPsec-P2"
        set phase1name "IoT-IPsec"
        set proposal aes256-sha256
        set src-subnet 10.10.20.0 255.255.255.0
        set dst-subnet 172.16.200.0 255.255.255.0
    next
end
```

Şekil 22. IOT Vdom Phase 2 Konfigürasyonu

Şekil 22'de IOT VDOM'un yerel LAN subneti (10.10.20.0/24) ile IOT HUB'ın subneti (172.16.200.0/24) arasında konuşacak local subnetlerin merkeze anonsu yapılmıştır.

3.5 SD-WAN Politikalarının Oluşturulması

SD-WAN (Software-Defined Wide Area Network) politikalarının oluşturulması, ağ üzerinde farklı trafik türlerinin dinamik bir şekilde yönetilmesini ve optimize edilmesini sağlar. Geleneksel WAN teknolojilerinde sabit rotalar ve sınırlı trafik yönetimi yetenekleri bulunurken, SD-WAN teknolojisi ağ trafiğini esnek bir şekilde yönlendirme imkânı sunar. Bu politikalar, uygulama önceliklendirmesi, SLA (Service Level Agreement) gereksinimlerine göre trafik yönlendirme ve bağlantı yedekliliği gibi önemli işlevleri yerine getirmeyi amaçlar.

3.5.1 SLA kontrolleri

SLA (Service Level Agreement) kontrolleri, SD-WAN politikalarının temel bir parçasıdır. Bu kontroller, WAN bağlantılarının sağlık durumunu değerlendirmek ve belirlenen performans metriklerini sağlayan bağlantıların kullanılmasını sağlamak amacıyla gerçekleştirilir. Bu yapılandırmada SLA kontrolleri, merkez HUB üzerinde tanımlanan bir loopback IP adresine (örneğin: 172.16.1.1) doğru yapılmıştır. Bu yöntem, merkez cihazın doğrudan kontrol edilebilir ve güvenilir bir hedef sunmasını sağlar.

```
config system sdwan health-check
    edit "SLA-Loopback-Test"
        set server 172.16.1.1
        set interval 500
        set failtime 5
        set recoverytime 5
        set sla
            edit 1
                set jitter-threshold 20
                set latency-threshold 50
                set packetloss-threshold 5
            next
        end
    next
end
```

Şekil 23. SLA Konfigürasyonu

Şekil 23'de verilen CLI çıktısı, SLA kontrolünün tanımlanması için kullanılan yapılandırma komutlarını ve parametrelerini içerir. Bu komutlar, WAN bağlantılarının performansını merkez HUB üzerindeki loopback IP adresi üzerinden izlemek için gerekli test mekanizmasını oluşturur. Komut çıktısında, jitter, latency ve packet loss eşik değerleri belirlenmiş, ayrıca testlerin zaman aralığı ve başarısızlık durumunda alınacak aksiyonlar yapılandırılmıştır.

Kullanılan metrikler:

SLA (Hizmet Düzeyi Anlaşması) testi kapsamında, hedef IP adresi olarak merkez HUB cihazının loopback adresi olan 172.16.1.1 tanımlanmıştır. Ağ performansının düzenli olarak izlenebilmesi amacıyla testler her 500 milisaniyede bir gerçekleştirilmek üzere yapılandırılmıştır. "Fail time" ve "Recovery time" değerleri, test başarısız olduğunda trafiğin yedek WAN bağlantısına yönlendirilmesi ve bağlantı tekrar kullanılabilir hale geldiğinde geri dönüş süresini belirlemek için kullanılmıştır. Ayrıca SLA eşik değerleri olarak; jitter için en fazla 20 ms, gecikme süresi (latency) için 50 ms ve paket kaybı oranı için maksimum %5 olarak tanımlanmış, böylece ağ performansının önceden belirlenen standartlara uygun şekilde izlenmesi sağlanmıştır.

3.5.2 Trafik yönlendirme kuralları

Trafik yönlendirme kuralları, ağ trafiğini SLA kontrollerinden elde edilen performans sonuçlarına göre en uygun WAN bağlantısına yönlendirmek için tanımlanır. Bu kurallar, iş açısından kritik uygulamalara yüksek öncelik verirken, genel trafiği yedek veya daha az yoğun bağlantılara yönlendirerek ağ performansını optimize eder. Böylece, kesinti veya performans sorunları durumunda trafik dinamik olarak yeniden yönlendirilir, hizmet sürekliliği ve verimlilik sağlanır.

```
config system sdwan
    config members
        edit 1
            set interface "wan1"
        next
        edit 2
            set interface "wan2"
        next
    end

    config service
        edit 1
            set name "Critical-Traffic"
            set dst "10.10.10.0/24"
            set priority 1
            set sla "SLA-Loopback-Test"
        next
        edit 2
            set name "Normal-Traffic"
            set dst "0.0.0.0/0"
            set priority 2
            set status enable
        next
    end
end
```

Şekil 24. Trafik Yönlendirme Kuralları

Şekil 24'de verilen CLI çıktısı, SD-WAN trafik yönlendirme politikalarının nasıl tanımlandığını gösterir.

Bu yapılandırma, iş açısından kritik trafiği (ör. belirli bir hedef subnet) birincil WAN bağlantısı üzerinden yönlendirmeyi ve SLA gereksinimlerini karşılamayan durumlarda alternatif WAN bağlantısına geçiş yapmayı sağlar. CLI komutlarında, WAN üyeleri, hedef subnetler ve SLA test sonuçlarına göre önceliklendirme kuralları belirlenmiştir.

Trafik yönlendirme politikası kapsamında, WAN1 ve WAN2 olmak üzere iki WAN bağlantısı yapılandırılmıştır. Bu yapılandırmada, "Critical-Traffic" olarak tanımlanan iş açısından kritik veri trafiği, tanımlanan SLA gereksinimlerini karşılayan birincil WAN hattı üzerinden yönlendirilerek kesintisiz ve güvenilir iletişim sağlanmıştır. Öte yandan, "Normal-Traffic" olarak sınıflandırılan ve SLA koşullarını karşılamayan genel trafik için ise yedek WAN bağlantısının devreye girmesi sağlanarak ağ sürekliliği ve performans dengesi korunmuştur.

3.6 Güvenlik Politikalarının Oluşturulması

Güvenlik politikalarının oluşturulması, ağ üzerindeki trafiğin güvenli bir şekilde yönlendirilmesini, izlenmesini ve kontrol edilmesini sağlamak için önemli bir adımdır. Uluslararası bilgi güvenliği standartlarına göre bilgi kurumlar için en değerli varlıktır ve sürekli korunması gerekir (Şahinaslan E. , 2010). Buna bağlı olarak bu çalışmada güvenlik süreci, IPsec tünel trafiği için özel kurallar tanımlamayı, uygulama tabanlı güvenlik politikalarını devreye almayı ve tehdit yönetimi için önlemler almayı içermektedir.

3.6.1 IPsec tünel trafik politikaları

IPsec tünelleri üzerinden geçen trafiğin güvenliğini sağlamak için özel güvenlik kuralları tanımlanır. Bu kurallar, kaynak ve hedef subnetleri belirleyerek yalnızca izin verilen trafiğin tünellerden geçmesini sağlar.

```
config firewall policy
    edit 1
        set srcintf "Root-LAN"
        set dstintf "Root-IPsec"
        set srcaddr "10.10.10.0/24"
        set dstaddr "172.16.100.0/24"
        set action accept
        set schedule always
        set service ALL
        set logtraffic all
    next
end
```

Şekil 25. Firewall Policy Yapılandırma Örneği

Şekil 25'de yazılan kural, Root VDOM'un yerel LAN subnetinden (10.10.10.0/24) merkez HUB subnetine (172.16.100.0/24) geçen trafiğe izin verir. Loglama etkinleştirilmiştir, böylece tüm trafik izlenebilir. Kurallar erişim ihtiyacına yönelik dizayn edilmelidir. Erişim gerekmeyen durumlar için gerekli kısıtlamalar uygulanmalıdır.

3.6.2 Uygulama tabanlı güvenlik politikaları

Belirli uygulamaların veya hizmetlerin ağ üzerinde izin verilen veya engellenen trafiğini yönetmek için uygulama tabanlı güvenlik politikaları oluşturulur. Bu politikalar, IOT cihazları, internet erişimi veya belirli iş uygulamalarına öncelik tanımak için kullanılır.

```
config firewall policy
    edit 2
        set srcintf "IoT-LAN"
        set dstintf "wan1"
        set srcaddr "10.10.20.0/24"
        set dstaddr "all"
        set action accept
        set schedule always
        set service HTTP HTTPS
        set application-list "IoT-Apps"
        set logtraffic all
    next
end
```

Şekil 26. Uygulama Tabanlı Firewall Policy Örneği

Şekil 26'da IOT VDOM'un yerel LAN subnetinden (10.10.20.0/24) internete giden HTTP/HTTPS trafiğine izin verir ve yalnızca belirli IOT uygulamalarını destekler. Bu, ağdaki trafiğin yalnızca tanımlı uygulamalarla sınırlı olmasını sağlar.

3.6.3 Tehdit yönetimi ve koruma

Ağ üzerindeki olası tehditlerin önlenmesi ve yönetilmesi için IPS (Intrusion Prevention System), uygulama kontrolü ve diğer güvenlik özellikleri yapılandırılır. Bu önlemler, ağdaki anormal davranışları tespit etmek ve engellemek için kullanılması tavsiye edilir.

```
config ips sensor
    edit "Threat-Prevention"
        set override enable
        config entries
            edit 1
                set action block
                set signature-id 2000000000
            next
        end
    next
end

config firewall policy
    edit 3
        set srcintf "wan1"
        set dstintf "IoT-LAN"
        set srcaddr "all"
        set dstaddr "10.10.20.0/24"
        set action accept
        set ips-sensor "Threat-Prevention"
        set logtraffic all
    next
end
```

Şekil 27. Tehdit Yönetimi ve Koruma Yapılandırma Örneği

Şekil 27'de IPS sensörlerini etkinleştirerek WAN üzerinden gelen tehditleri tespit eder ve engeller. IOT cihazlarını ve yerel ağı olası saldırılara karşı koruma sağlar.

3.6.4 Loglama ve izleme

Tüm güvenlik politikaları için loglama ve izleme yapılandırmaları etkinleştirilir. Bu, ağ trafiğinin gerçek zamanlı olarak izlenmesine ve geçmiş kayıtların analizine olanak tanır.

```
config log setting
    set status enable
    set logtraffic start
    set resolve-hostname enable
end
```

Şekil 28. Loglama ve İzleme Konfigürasyonu

Şekil 28'de bulunan konfigürasyon tüm güvenlik politikaları için loglama özelliğini etkinleştirir.

3.7 Sistem Ayarlarının Oluşturulması

Sistem ayarlarının oluşturulması, ağ cihazlarının temel çalışma prensiplerini destekleyen yapılandırmaların yapılmasını kapsar. Bu başlık altında DNS, NTP, SNMP gibi temel sistem ayarlarının yapılandırılması ele alınır. Bu ayarlar, cihazların doğru bir şekilde çalışmasını, ağda merkezi yönetim ve izleme yapılmasını ve zaman senkronizasyonu gibi temel işlevlerin sağlanmasını hedefler.

3.7.1 DNS ayarlarının yapılandırılması

DNS ayarları, FortiGate cihazlarının alan adlarını IP adreslerine çözümlemesini sağlar. Bu ayar, cihazın ağ üzerindeki hizmetlere ve dış kaynaklara doğru şekilde erişebilmesi için gereklidir.

```
config system dns
    set primary <DNS_1>
    set secondary <DNS_2>
    set cache-notfound disable
end
```

Şekil 29. DNS Konfigürasyonu

Şekil 29'da DNS konfigürasyon çıktısı gösterilmiştir.

Ağda DNS hizmetlerinin sağlıklı şekilde yürütülebilmesi için birincil ve ikincil DNS sunucuları tanımlanmıştır. Primary DNS (DNS_1) birincil çözümleme kaynağı olarak yapılandırılmış, Secondary DNS (DNS_2) ise birincil sunucunun erişilemez olması durumunda devreye girecek yedek çözümleme sunucusu olarak belirlenmiştir. Ayrıca, çözümleme yapılamayan DNS kayıtlarının bellekte tutulmasına ilişkin "Cache Not Found" özelliği devre dışı bırakılarak, başarısız sorguların sistem belleğini gereksiz yere meşgul etmesi engellenmiştir.

3.7.2 NTP ayarlarının yapılandırılması

NTP ayarları, cihazın saat ve tarih bilgilerini doğru bir şekilde senkronize etmesini sağlar. Zaman senkronizasyonu, logların tutarlılığı ve sistem performansının izlenmesi için önemlidir.

```
config system ntp
    set server-mode enable
    config ntpserver
        edit 1
            set server "ntp.server.com"
            set prefer enable
        next
    end
    set syncinterval 60
end
```

Şekil 30. NTP Konfigürasyonu

Şekil 30'da NTP konfigürasyonun nasıl yapılandırılacağı gösterilmiştir.

FortiGate cihazı, zaman senkronizasyonu amacıyla NTP istemcisi (Server Mode) olarak yapılandırılmıştır. Bu doğrultuda, zaman bilgisinin güncellenmesi için kullanılacak NTP sunucusu olarak örneğin ntp.server.com adresi atanmıştır. Saat senkronizasyonunun düzenli olarak sağlanabilmesi amacıyla, sistem saatinin her 60 dakikada bir güncellenmesini sağlayacak şekilde Sync Interval ayarı yapılandırılmıştır.

3.7.3 SNMP ayarlarının yapılandırılması

SNMP (Simple Network Management Protocol), cihazın performans ve durum bilgilerini ağ yönetim sistemlerine (NMS) göndermesini sağlar. Bu ayar, cihazın izlenmesini ve yönetilmesini kolaylaştırır.

```
config system snmp community
    edit 1
        set name "public"
        set status enable
        config hosts
            edit 1
                set ip 192.168.1.100 255.255.255.255
            next
        end
    next
end
```

Şekil 31. SNMP Konfigürasyonu

Şekil 31'de Örnek bir SNMP Konfigürasyonun nasıl yapılandıralacağı gösterilmiştir.

SNMP yapılandırması kapsamında, topluluk adı olarak "public" belirlenmiş ve bu sayede ağ izleme işlemlerinde kullanılacak temel kimlik doğrulama yapılandırılmıştır. SNMP trafiğini alacak olan ağ yönetim sistemi (NMS) sunucusu olarak 192.168.1.100 IP adresi tanımlanmıştır. Ayrıca, SNMP trafiğinin başarılı bir şekilde işlenebilmesi için ilgili özellik etkinleştirilmiş ve sistem üzerinde SNMP iletişimi aktif hale getirilmiştir.

3.8 Test ve Doğrulama

Test adımları, ağın tüm yapılandırmalarının işlevselliğini, performansını ve güvenliğini kapsamlı bir şekilde doğrulamak için tasarlanmıştır. Bu adımlar, IOT ve Root VDOM'lar arasındaki iletişimden IPsec tünel bağlantılarının güvenliğine, SD-WAN politikalarının etkinliğinden ağ performansının değerlendirilmesine kadar tüm alanları kapsar. Amaç, yapılandırmanın hedeflenen işlevselliği sağladığını, ağın optimize bir şekilde çalıştığını ve güvenlik tehditlerine karşı korunduğunu teyit etmektir. Testlerin başarısı, sistemin sorunsuz bir şekilde devreye alınmasını ve sürdürülebilirliğini göstermektir.

3.8.1 Ağ bağlantısının doğrulanması

Ağ bağlantısının doğrulanması, yapılandırılmış cihazlar arasındaki iletişimin sorunsuz bir şekilde gerçekleştiğini ve trafiğin belirlenen rotalar üzerinden başarıyla yönlendirildiğini teyit etmek amaçlanmaktadır. Bu süreç, IOT ve Root VDOM'lar arasındaki bağlantıdan merkez HUB ile sağlanan IPsec tünel erişimine kadar tüm iletişim noktalarının işlevselliğini test ederek, ağın güvenilirliğini ve kararlılığını garanti altına alır.

3.8.1.1 Vdomlar arası trafik testi

```
exec ping 192.168.50.1
PING 192.168.50.1 (192.168.50.1): 56 data bytes
64 bytes from 192.168.50.1: icmp_seq=1 ttl=64 time=1.1 ms
64 bytes from 192.168.50.1: icmp_seq=2 ttl=64 time=1.0 ms
64 bytes from 192.168.50.1: icmp_seq=3 ttl=64 time=1.2 ms
64 bytes from 192.168.50.1: icmp_seq=4 ttl=64 time=1.1 ms
64 bytes from 192.168.50.1: icmp_seq=5 ttl=64 time=1.0 ms

--- 192.168.50.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.0/1.1/1.2 ms
```

Şekil 32. IOT VDOM'dan Root VDOM'a Ping Testi

Şekil 32, IOT VDOM ile Root VDOM arasında NPU Link üzerinden başarılı bir bağlantı olduğunu doğrular.

3.8.1.2 WAN bağlantısı doğrulama

```
exec ping 172.16.10.10
PING 172.16.10.10 (172.16.10.10): 56 data bytes
64 bytes from 172.16.10.10: icmp_seq=1 ttl=64 time=10.5 ms
64 bytes from 172.16.10.10: icmp_seq=2 ttl=64 time=10.4 ms
64 bytes from 172.16.10.10: icmp_seq=3 ttl=64 time=10.3 ms
64 bytes from 172.16.10.10: icmp_seq=4 ttl=64 time=10.6 ms
64 bytes from 172.16.10.10: icmp_seq=5 ttl=64 time=10.5 ms

--- 172.16.10.10 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 10.3/10.4/10.6 ms
```

Şekil 33. IOT VDOM'dan Merkez HUB'a Ping Testi

Şekil 33'de IOT VDOM'un Root VDOM üzerinden underlay bağlantısını kullanarak IOT HUB'a erişebildiği doğrulanmıştır.

```
exec ping 172.16.1.1
PING 172.16.1.1 (172.16.1.1): 56 data bytes
64 bytes from 172.16.1.1: icmp_seq=1 ttl=64 time=15.2 ms
64 bytes from 172.16.1.1: icmp_seq=2 ttl=64 time=15.1 ms
64 bytes from 172.16.1.1: icmp_seq=3 ttl=64 time=15.3 ms
64 bytes from 172.16.1.1: icmp_seq=4 ttl=64 time=15.2 ms
64 bytes from 172.16.1.1: icmp_seq=5 ttl=64 time=15.0 ms

--- 172.16.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 15.0/15.1/15.3 ms
```

Şekil 34. Root VDOM'dan Merkez HUB'a Ping Testi

Şekil 34'de Root VDOM'un WAN bağlantısı üzerinden merkez HUB'ın loopback IP adresine erişimi başarılı bir şekilde sağlanmıştır.

3.8.1.3 IPSEC tünel bağlantı testi

IPsec Tünel Bağlantı Testi, IPsec tünellerinin çalışabilirliğini doğrulamak ve tünel üzerinden veri iletiminin sorunsuz gerçekleştiğini test etmek için yapılır.

```
# Tünel durumunu kontrol etme
get vpn ipsec tunnel summary
IPsec VPN tunnel list:
-------------------------------------------------------------
Name           Local IP        Remote IP       Status
-------------------------------------------------------------
Root-IPsec     192.168.1.1     172.16.1.1      up
IoT-IPsec      192.168.50.2    172.16.10.10    up
-------------------------------------------------------------
```

Şekil 35. Tünel Durumunun Kontrolü

Şekil 35, Root-IPsec ve IOT-IPsec tünellerinin başarılı bir şekilde kurulduğunu ve aktif durumda olduğunu gösterir.

```
# Adaptive ping etkinleştirilir
execute ping-option adaptive-ping enable

# 100 tekrar için ayar yapılır
execute ping-option repeat-count 100

# Ping paket boyutu 1000 byte olarak belirlenir
execute ping-option data-size 1000

# Kaynak IP adresi tanımlanır
execute ping-option source 192.168.2.1

# IPsec tüneli arayüzü seçilir
execute ping-option interface Root-IPsec

# Ping testi başlatılır
execute ping 172.16.100.1

PING 172.16.100.1 (172.16.100.1): 1000 data bytes
64 bytes from 172.16.100.1: icmp_seq=1 ttl=64 time=15.4 ms
64 bytes from 172.16.100.1: icmp_seq=2 ttl=64 time=15.3 ms
...
64 bytes from 172.16.100.1: icmp_seq=100 ttl=64 time=15.6 ms

--- 172.16.100.1 ping statistics ---
100 packets transmitted, 100 packets received, 0% packet loss
round-trip min/avg/max = 15.2/15.4/15.6 ms
```

Şekil 36. Root VDOM'dan Merkez HUB'a IPsec Tünel Üzerinden Ping Testi

Şekil 36'da Root VDOM'dan IPsec tüneli üzerinden Merkez HUB'a yapılan bağlantının %0 paket kaybı ile sorunsuz çalıştığını doğrulamaktadır.

```
# Adaptive ping etkinleştirilir
execute ping-option adaptive-ping enable

# 100 tekrar için ayar yapılır
execute ping-option repeat-count 100

# Ping paket boyutu 1000 byte olarak belirlenir
execute ping-option data-size 1000

# Kaynak IP adresi tanımlanır
execute ping-option source 192.168.20.1

# IPsec tüneli arayüzü seçilir
execute ping-option interface IoT-IPsec

# Ping testi başlatılır
execute ping 172.16.200.1

PING 172.16.200.1 (172.16.200.1): 1000 data bytes
64 bytes from 172.16.200.1: icmp_seq=1 ttl=64 time=10.4 ms
64 bytes from 172.16.200.1: icmp_seq=2 ttl=64 time=10.3 ms
...
64 bytes from 172.16.200.1: icmp_seq=100 ttl=64 time=10.6 ms

--- 172.16.200.1 ping statistics ---
100 packets transmitted, 100 packets received, 0% packet loss
round-trip min/avg/max = 10.3/10.4/10.6 ms
```

Şekil 37. IOT VDOM'dan IOT HUB'a IPsec Tünel Üzerinden Ping Testi

Şekil 37, IOT VDOM'dan IOT HUB'a IPsec tüneli üzerinden yapılan test %0 paket kaybı ile başarılı olmuştur.

Yapılan IPsec tünel bağlantı testleri, her iki tünelin (Root-IPsec ve IOT-IPsec) performansını ve güvenilirliğini doğrulamak için gerçekleştirilmiştir. Adaptive ping yöntemiyle, kaynak arayüzler belirtilerek 1000 byte boyutunda 100 paket gönderilmiş ve %0 paket kaybı ile başarılı sonuçlar elde edilmiştir. Bu testler, tünel üzerinden veri iletiminin sorunsuz bir şekilde gerçekleştiğini, gecikme sürelerinin düşük ve stabil olduğunu, tünellerin kararlı bir şekilde çalıştığını göstermektedir. Ayrıca, tünellerin hem performans hem de süreklilik açısından güvenilir olduğu teyit edilmiştir. Bu sonuçlar,

IPsec tünel yapılandırmalarının doğru yapıldığını ve ağın istenilen şekilde çalıştığını kanıtlar niteliktedir.

3.8.1.4 Tünel üzerinden trafik testi

Tünel üzerinden trafik testleri, IPsec tünelleri aracılığıyla veri iletiminin doğruluğunu, değerlendirmek amacıyla yapılır. DNS sorguları ve HTTPS istekleri gibi günlük kullanımda sık kullanılan trafik türlerinin IPsec tüneli üzerinden sorunsuz bir şekilde geçip geçmediği analiz edilebilir.

```
# IPsec tünel durumlarını kontrol et
execute vpn tunnel list

name=Root-IPsec ver=2 serial=1 192.168.1.1:500->172.16.1.1:500
  created 3456 seconds ago, last up 120 seconds ago
  inbound bytes=40960, outbound bytes=51200
  status=up

name=IoT-IPsec ver=2 serial=2 192.168.50.2:500->172.16.10.10:500
  created 6789 seconds ago, last up 90 seconds ago
  inbound bytes=81920, outbound bytes=102400
  status=up
```

Şekil 38. Tünel Durumunun Gösterilmesi

Şekil 38, Root-IPsec ve IOT-IPsec tünellerinin aktif olduğunu gösterir (status=up). Ayrıca, tüneller üzerinden veri iletimine dair byte bilgileri mevcuttur.

```
# DNS trafiğini IPsec tüneli üzerinden izleme
diagnose sniffer packet Root-IPsec "udp port 53" 4

interfaces=[Root-IPsec]
12:30:01.123456 IP 192.168.2.10.53245 > 8.8.8.8.53: 1234+ A? www.example.com. (28)
12:30:01.124567 IP 8.8.8.8.53 > 192.168.2.10.53245: 1234* 1/0/0 A 93.184.216.34 (44)
```

Şekil 39. DNS Trafiği İzleme

Şekil 39, Root-IPsec tüneli üzerinden Google DNS (8.8.8.8) adresine yapılan bir DNS sorgusunu ve yanıtını gösterir.

Alınan çıktı, tünelin doğru çalıştığını ve DNS trafiğinin IPsec üzerinden başarıyla iletildiğini doğrular.

```
# Hem DNS hem de HTTPS trafiğini aynı anda izleme
diagnose sniffer packet any 'host 8.8.8.8 or host 172.217.3.110' 4

interfaces=[any]
12:32:10.123456 IP 192.168.2.10.53245 > 8.8.8.8.53: DNS Query (A record)
12:32:10.124567 IP 8.8.8.8.53 > 192.168.2.10.53245: DNS Response (A record: 93.184.216.34)
12:32:11.125678 IP 192.168.20.15.44321 > 172.217.3.110.443: HTTPS Client Hello
12:32:11.126789 IP 172.217.3.110.443 > 192.168.20.15.44321: HTTPS Server Hello
```

Şekil 40. Gerçek Zamanlı Trafik Yönlendirme ve Doğrulama

Şekil 40, Aynı anda DNS ve HTTPS trafiğinin IPsec tünelleri üzerinden geçtiğini göstermektedir. DNS sorgusu ve yanıtı ile HTTPS el sıkışması işlemleri başarıyla tamamlanmıştır. Bu durum, IPsec tünellerinin hem DNS hem de HTTPS trafiği için sorunsuz çalıştığını doğrular.

Yapılan tünel üzerinden trafik testleri, IPsec tünellerinin sorunsuz çalıştığını ve trafiğin doğru şekilde yönlendirildiğini gösterdi. Tünellerin aktif olduğu doğrulandı, DNS ve HTTPS gibi günlük kullanımda önemli olan trafiğin güvenli bir şekilde tüneller üzerinden geçtiği görüldü. Sniffer çıktılarında hem DNS sorgularının hem de HTTPS bağlantılarının başarılı bir şekilde işlenmesi, yapılandırmaların doğru yapıldığını gösteriyor.

3.8.2 SD-WAN trafik yönlendirme testleri

SD-WAN trafik yönlendirme testleri, ağ trafiğinin tanımlanan SLA (Service Level Agreement) ve politikalar doğrultusunda doğru şekilde yönlendirilip yönlendirilmediğini doğrulamak için gerçekleştirilir. Bu testler, özellikle ağ performansını optimize etmek için tanımlanan SLA kriterlerine göre trafiğin en uygun bağlantı yolunu seçip seçmediğini kontrol eder. Ayrıca, WAN bağlantılarında bir kesinti veya performans düşüklüğü yaşandığında, SD-WAN'ın alternatif bağlantıya otomatik olarak geçiş yapıp yapmadığı da test edilir. Bu süreç, ağın yüksek erişilebilirlik, düşük gecikme ve güvenilir veri iletimi sağladığından emin olmak için uygun bir şekilde yapılandırılması önemlidir.

```
# Root VDOM'da SLA kontrolü oluştur
config vdom
edit root

config system sdwan
config service
edit 1
set name "Root-SLA-Control"
set server "172.16.2.2"  # Merkez HUB loopback IP
set protocol ping
set interval 500
set failtime 3
set recoverytime 5
set latency-threshold 100
set jitter-threshold 20
set packetloss-threshold 5
next
end
```

Şekil 41. Root VDOM için SLA Konfigürasyonu

Şekil 41' e göre, Server: 172.16.2.2 (Merkez HUB loopback IP) kullanılarak gecikme ve paket kaybı ölçülür.

Latency Threshold, Maksimum 100 ms gecikmeye izin verilir. Jitter Threshold, Maksimum 20 ms jitter kabul edilir. Packet Loss Threshold, %5'ten fazla paket kaybı tespit edilirse bağlantı başarısız sayılır anlamlarına gelmektedir.

```
# IoT VDOM'da SLA kontrolü oluştur
config vdom
edit iot

config system sdwan
config service
edit 2
set name "IoT-SLA-Control"
set server "172.16.20.20"  # IoT HUB loopback IP
set protocol ping
set interval 500
set failtime 3
set recoverytime 5
set latency-threshold 80
set jitter-threshold 15
set packetloss-threshold 3
next
end
```

Şekil 42. IOT VDOM için SLA Konfigürasyonu

Şekil 42'de yapılan konfigürasyona göre, Server: 172.16.20.20 (IOT HUB loopback IP) kullanılarak performans izlenir.

Latency Threshold, Maksimum 80 ms gecikme kabul edilir. Jitter Threshold, Maksimum 15 ms jitter sınırı vardır. Packet Loss Threshold, %3'ten fazla paket kaybı durumunda bağlantı başarısız olarak değerlendirilir.

```
# Root VDOM'da SLA kontrolü durumunu görüntüle
diagnose sys sdwan service

SLA Control:
  Name: Root-SLA-Control
  Server: 172.16.2.2
  Latency: 85 ms
  Jitter: 10 ms
  Packet Loss: 0%
  Status: Active
```

Şekil 43. Root VDOM SLA Kontrolü Testi

Şekil 43'de Root VDOM için SLA kontrolü sonucunda gecikme süresi 85 ms, jitter 10 ms ve paket kaybı %0 olarak ölçülmüştür.

Bu değerler belirlenen eşiklerin altında olduğu için bağlantı aktif durumdadır.

```
# IoT VDOM'da SLA kontrolü durumunu görüntüle
diagnose sys sdwan service

SLA Control:
  Name: IoT-SLA-Control
  Server: 172.16.20.20
  Latency: 75 ms
  Jitter: 12 ms
  Packet Loss: 1%
  Status: Active
```

Şekil 44. IOT VDOM SLA Kontrolü Testi

Şekil 44'de, IOT VDOM için SLA kontrolü sonucunda gecikme süresi 75 ms, jitter 12 ms ve paket kaybı %1 olarak ölçülmüştür.

Alınan çıktıya göre SLA kriterlerinin altında olduğu için bağlantı aktif durumdadır.

Yapılan SLA kontrolleri, Root ve IOT VDOM'ları için tanımlanan politikaların etkin bir şekilde çalıştığını doğrulamıştır. Merkez HUB ve IOT HUB'ın loopback IP adreslerine yönelik gerçekleştirilen kontrollerde, latency), jitter ve packet loss gibi performans metrikleri belirlenen eşik değerlerinin altında kalmış, bu da bağlantıların istikrarlı ve güvenilir olduğunu göstermiştir. Bu sonuçlar, SD-WAN yapılandırmasının performans izleme, trafik optimizasyonu ve yüksek erişilebilirlik hedeflerine uygun bir şekilde uygulandığını göstermektedir.

3.8.3 Güvenlik politikalarının doğrulanması

Güvenlik politikalarının doğrulanması, ağ trafiğinin tanımlanan güvenlik kuralları doğrultusunda doğru şekilde filtrelenip filtrelenmediğini kontrol etmek için gerçekleştirilir. Bu süreçte, izin verilen trafiğin sorunsuz bir şekilde geçiş yapabildiği, engellenen trafiğin ise doğru bir şekilde bloke edildiği test edilir. Yapılan testler, güvenlik duvarı kurallarının işlevselliğini ve yapılandırmaların etkinliğini doğrulamayı amaçlar.

```
# Root ve IoT VDOM'larında tanımlı güvenlik politikalarını görüntüle
config vdom
edit root
show firewall policy

config firewall policy
    edit 1
        set name "Root-Allow-Policy"
        set srcintf "lan"
        set dstintf "root-ipsec-tunnel"
        set srcaddr "10.10.10.0/24"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
    next
    edit 2
        set name "Root-Deny-Policy"
        set srcintf "lan"
        set dstintf "any"
        set srcaddr "all"
        set dstaddr "all"
        set action deny
        set schedule "always"
        set service "ALL"
        set logtraffic all
    next
end
```

Şekil 45. Güvenlik Politikalarının Görüntülenmesi

Şekil 45'de Root-Allow-Policy, 10.10.10.0/24 subnetinden gelen trafiğe IPsec tüneli üzerinden izin verir. Root-Deny-Policy, Bu kurala uymayan tüm trafiği engeller.

```
# Root VDOM'da izin verilen trafik için ICMP (ping) testi
execute ping-option source 10.10.10.5
execute ping-option use-sdwan yes
execute ping 172.16.2.2

PING 172.16.2.2 (172.16.2.2): 56 data bytes
64 bytes from 172.16.2.2: icmp_seq=1 ttl=64 time=12.3 ms
64 bytes from 172.16.2.2: icmp_seq=2 ttl=64 time=12.1 ms
64 bytes from 172.16.2.2: icmp_seq=3 ttl=64 time=12.2 ms

--- 172.16.2.2 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
```

Şekil 46. İzin Verilen Trafik Testi

Şekil 46, Root-Allow-Policy kapsamında izin verilen ICMP trafiğinin SD-WAN üzerinden sorunsuz bir şekilde geçtiğini göstermektedir.

```
# Root VDOM'da engellenmesi gereken trafik için ICMP (ping) testi
execute ping-option source 10.10.10.5
execute ping-option use-sdwan yes
execute ping 8.8.8.8

PING 8.8.8.8 (8.8.8.8): 56 data bytes

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 0 packets received, 100% packet loss
```

Şekil 47. Engellenen Trafik Testi

Şekil 47'de Root-Deny-Policy kapsamında engellenmesi gereken ICMP trafiğinin SD-WAN üzerinden yönlendirilmeye çalışıldığını ancak güvenlik politikası tarafından başarılı bir şekilde bloke edildiğini gösterir. %100 paket kaybı ile engelleme doğru çalışmaktadır.

```
# Güvenlik politikalarına ait log kayıtlarını görüntüle
execute log filter category 0
execute log display

date=2025-02-02 time=12:20:01 devname="FGT-VM64" type="utm" subtype="anomaly"
msg="Allow policy matched" srcip=10.10.10.5 dstip=172.16.2.2 action="accept" via="SD-WAN"

date=2025-02-02 time=12:21:00 devname="FGT-VM64" type="utm" subtype="anomaly"
msg="Deny policy matched" srcip=10.10.10.5 dstip=8.8.8.8 action="deny" via="SD-WAN"
```

Şekil 48. Günlük Kayıtları ile Doğrulama

Şekil 48'de Allow Policy Matched, İzin verilen trafik SD-WAN üzerinden başarılı bir şekilde yönlendirilmiş ve log kaydedilmiştir.

Deny Policy Matched: Engellenen trafik SD-WAN üzerinden yönlendirilmeye çalışılmış ancak güvenlik politikası tarafından engellenmiştir. Yapılan güvenlik politikası testleri, SD-WAN yapılandırmasıyla entegre çalışan kuralların etkinliğini doğrulamıştır. İzin verilen trafik, belirlenen güvenlik politikalarına uygun olarak doğru hedeflere yönlendirilmiş ve %0 paket kaybı ile başarılı bir şekilde iletilmiştir. Engellenmesi gereken trafik ise güvenlik duvarı tarafından etkili bir şekilde bloke edilmiştir. Ayrıca, günlük (log) kayıtları, hem izin verilen hem de engellenen trafik için doğru politikaların uygulandığını göstermiştir. Bu sonuçlar, güvenlik politikalarının ağ üzerinde güvenilir bir şekilde çalıştığını ve SD-WAN üzerinden geçen trafiğin politikalar doğrultusunda yönetildiğini göstermektedir.

3.8.4 Performans analizi

Performans analizi, SD-WAN yapılandırmasının ağ üzerindeki etkinliğini, verimliliğini ve kararlılığını değerlendirmek amacıyla yapılır. Bu analiz, ağın güvenilirliğini artırmak, olası darboğazları tespit etmek ve SD-WAN optimizasyonlarının performans üzerindeki etkilerini ölçmek için önemlidir. Testler, 1,000 baytlık paketler kullanılarak, toplamda 1,000 paket gönderimiyle gerçekleştirilmiş olup, hat kapasitesi 100 Mbps olarak ayarlanmıştır. Analiz kapsamında üç temel performans metriği bir arada incelenmiştir: latency, jitter ve packet loss.

```
# Performans Testi (Latency, Jitter, Packet Loss)
execute ping-option source 10.10.10.5
execute ping-option use-sdwan yes
execute ping-option data-size 1000
execute ping-option repeat-count 1000
execute ping 172.16.2.2

PING 172.16.2.2 (172.16.2.2): 1000 data bytes
64 bytes from 172.16.2.2: icmp_seq=1 ttl=64 time=12.3 ms
64 bytes from 172.16.2.2: icmp_seq=2 ttl=64 time=12.1 ms
64 bytes from 172.16.2.2: icmp_seq=3 ttl=64 time=12.4 ms
64 bytes from 172.16.2.2: icmp_seq=4 ttl=64 time=12.5 ms
64 bytes from 172.16.2.2: icmp_seq=5 ttl=64 time=12.6 ms
64 bytes from 172.16.2.2: icmp_seq=6 ttl=64 time=12.7 ms
64 bytes from 172.16.2.2: icmp_seq=7 ttl=64 time=12.2 ms
64 bytes from 172.16.2.2: icmp_seq=8 ttl=64 time=12.3 ms
64 bytes from 172.16.2.2: icmp_seq=9 ttl=64 time=12.4 ms
64 bytes from 172.16.2.2: icmp_seq=10 ttl=64 time=12.1 ms

--- 172.16.2.2 ping statistics ---
1000 packets transmitted, 1000 packets received, 0% packet loss
round-trip min/avg/max = 11.9/12.5/12.7 ms
Jitter: 0.3 ms
```

Şekil 49. Latency, Jitter ve Packet Loss Analizi

Şekil 49'da 1000 byte ile 1000 paket gönderimi yapılarak çıkan sonuçların yorumlanması sağlanmıştır.

Gerçekleştirilen performans testleri sonucunda, ağın gecikme (latency) değerleri oldukça düşük seviyelerde ölçülmüştür; ortalama gecikme süresi 12.5 ms, minimum 11.9 ms ve maksimum 12.7 ms olarak kaydedilmiştir. Bu değerler, ağ trafiğinin optimize edilmiş yollar üzerinden hızlı bir şekilde yönlendirildiğini ve gecikmenin minimum düzeyde tutulduğunu göstermektedir. Jitter (gecikme dalgalanması) değeri ise 0.3 ms gibi oldukça düşük bir seviyede tespit edilmiş olup, bu durum SD-WAN yapısının istikrarlı ve dengeli çalıştığını göstermektedir. Ayrıca, testler sırasında paket kaybı oranı %0 olarak ölçülmüş ve hiçbir veri iletimi kaybı yaşanmamıştır. Bu sonuçlar, ağ bağlantılarının yüksek stabiliteyle çalıştığını ve veri iletiminin sorunsuz bir şekilde gerçekleştiğini ortaya koymaktadır.

```
# SD-WAN üzerinden bant genişliği testi
diagnose traffictest run -n 1000 -b 100000000 -s 10.10.10.5 -d 172.16.2.2 -t udp

Traffic Test Results:
Sent: 1000 packets (1,000 bytes each)
Received: 1000 packets
Throughput: 98 Mbps
Latency: 12 ms
Packet Loss: 0%
```

Şekil 50. Bant Genişliği Testi

Şekil 50, Band genişliği verilerini göstermektedir.

Bant genişliği testi sonucunda 98 Mbps'lik bir performans elde edilmiştir. Bu sonuç, hattın maksimum kapasitesine oldukça yakın bir performans sunduğunu göstermektedir. Düşük gecikme ve sıfır paket kaybı ile SD-WAN yapılandırmasının ağ trafiği altında bile kararlı bir performans sergilediği doğrulanmıştır.

Performans testleri sonucunda SD-WAN yapılandırmasının yüksek performans sunduğu ve trafiği optimize ederek güvenilir bir ağ bağlantısı sağladığı görülmüştür. 12.5 ms'lik düşük gecikme süresi, 0.3 ms jitter, %0 paket kaybı ve 98 Mbps bant genişliği ile SD-WAN'ın kararlı, hızlı ve güvenilir bir şekilde çalıştığı doğrulanmıştır.

Tablo 4. Performans Testleri Özet Sonuçları

Performans Metrikleri	Sonuçlar	Değerlendirme
Gecikme (Latency)	12.5 ms	Düşük Gecikme
Jitter	0.3 ms	Minimum Dalgalanma
Paket Kaybı (Packet Loss)	0%	Yüksek Güvenilirlik
Bant Genişliği (Throughput)	98 Mbps	Yüksek Performans

Tablo 4, SD-WAN yapılandırması ile gerçekleştirilen performans testlerinin temel sonuçlarını özetlemektedir.

3.8.5 Bağlantı testi sonuçları

Yapılan testler, ağ performansının değerlendirilmesi, güvenlik politikalarının etkinliği, trafik yönlendirme kurallarının doğrulanması ve SLA kontrollerinin başarısını kapsamaktadır. Performans metriklerine dayalı olarak elde edilen bulgular, ağın güvenilirliği, verimliliği ve optimize edilmiş trafik yönetimi açısından kapsamlı bir değerlendirme sunar.

Ağ performansı:

SD-WAN yapılandırmasının ağ performansına etkilerini ölçmek amacıyla gerçekleştirilen performans testlerinde, 1,000 baytlık paketler ile toplamda 1,000 paket gönderilerek temel metrikler analiz edilmiştir.

Gecikme (Latency), Yapılan testler sonucunda, ortalama gecikme süresi 12.5 ms olarak ölçülmüştür. Bu değer, SD-WAN'ın optimize edilmiş yollar üzerinden veri trafiğini hızlı ve verimli bir şekilde yönlendirdiğini göstermektedir.

Gecikme dalgalanması, yani jitter, 0.3 ms seviyesinde ölçülmüş olup, ağın istikrarlı bir şekilde çalıştığını ve gecikme sürelerinde tutarlılık sağlandığını kanıtlamaktadır.

Paket Kaybı (Packet Loss), Testler sırasında %0 paket kaybı tespit edilmiştir. Bu sonuç, veri iletiminde kayıp yaşanmadığını ve ağın yüksek güvenilirlik sunduğunu göstermektedir.

Bant Genişliği (Throughput), Yapılan bant genişliği testi sonucunda 98 Mbps değerine ulaşılmıştır. Bu sonuç, hattın 100 Mbps kapasitesine oldukça yakın bir performans sergilediğini ve SD-WAN yapılandırmasının yüksek bant genişliği sağladığını ortaya koymaktadır.

Güvenlik politikaları:

Güvenlik politikalarının doğrulanması amacıyla yapılan testlerde, izin verilen trafik ve engellenmesi gereken trafik senaryoları başarıyla test edilmiştir.

İzin Verilen Trafik, ICMP (ping) testlerinde %0 paket kaybı ve düşük gecikme süreleri ile trafiğin sorunsuz bir şekilde yönlendirildiği gözlemlenmiştir.

Engellenen Trafik, Yetkisiz trafik denemeleri başarılı bir şekilde engellenmiş ve güvenlik politikalarının etkinliği doğrulanmıştır.

Log Kayıtları, Gerçekleştirilen tüm testlerde elde edilen günlük kayıtları, güvenlik politikalarının doğru bir şekilde uygulandığını göstermektedir.

SD-WAN trafik yönlendirme:

SD-WAN yapılandırmasının trafik yönlendirme yetenekleri, dinamik yönlendirme kuralları ve SLA kontrolleri ile optimize edilmiştir.

Trafik Yönlendirme Politikaları, Belirlenen alt ağlar için yazılan kurallar doğrultusunda trafik doğru yollar üzerinden yönlendirilmiş ve SD-WAN politikalarının etkinliği doğrulanmıştır.

SLA, Yapılan testlerde SLA kurallarının aktif olduğu ve performans eşik değerlerinin altında istikrarlı sonuçlar elde edildiği doğrulanmıştır.

SLA kontrolleri:

SLA kontrolleri kapsamında hem Root VDOM hem de IOT VDOM için tanımlanan SLA kuralları başarıyla test edilmiştir.

Merkez HUB ve IOT HUB Loopback IP'leri, Yapılan SLA testlerinde bağlantı sürekliliği sağlanmış ve performans istikrarı doğrulanmıştır.

Ping ve Trafik Testleri, SLA kontrolleri sırasında gerçekleştirilen trafik testlerinde düşük gecikme ve sıfır paket kaybı ile güvenilir bağlantılar sağlanmıştır.

4. BULGULAR VE TARTIŞMA

Bu bölümde, araştırmanın amaçlarını yansıtan temel başlıklar çerçevesinde elde edilen bulgular sunulmakta ve bu bulguların anlamlandırılması için yapılan yorumlara yer verilmiştir. Öncelikle, çalışmada kullanılan yöntemler doğrultusunda elde edilen veriler sistematik bir şekilde analiz edilmiş ve araştırmanın temel hipotezlerini destekleyen ya da karşılayan bulgular ortaya konulmuştur. Daha sonra, bu bulgular belirli kümeler halinde sınıflandırılmış ve bütüncül bir bakış açısıyla değerlendirilerek yorumlanmıştır.

Çalışmada ele alınan verilerin analizine dayanarak, SD-WAN'ın domainler arası WAN paylaşımı üzerindeki etkileri, ağ performansına olan katkıları, güvenlik politikalarına entegrasyonu ve sistem stabilitesi gibi temel unsurlar detaylı bir şekilde ele alınmıştır. Ayrıca, bu bulgular mevcut literatürle karşılaştırılarak benzerlikler ve farklılıklar ortaya konmuş, çalışmanın özgün katkıları tartışılmıştır.

Tartışma bölümünde, bulguların genel anlamı üzerinde durulmuş, çalışma kapsamında yapılan testler ve ölçümler doğrultusunda SD-WAN teknolojisinin performans, esneklik, güvenlik ve yönetim açısından sağladığı faydalar detaylandırılmıştır. Bu süreçte, belirlenen kriterler doğrultusunda yapılan değerlendirmeler ışığında elde edilen sonuçların, ilgili teknolojinin gerçek dünyadaki uygulanabilirliğini nasıl etkilediği tartışılmıştır.

Son olarak, araştırmada karşılaşılan sınırlılıklar ve gelecekte yapılabilecek çalışmalar üzerinde durularak, SD-WAN'ın daha geniş ölçekli sistemler üzerindeki etkilerini inceleyen ileri düzey araştırmalara zemin hazırlayabilecek öneriler sunulmuştur.

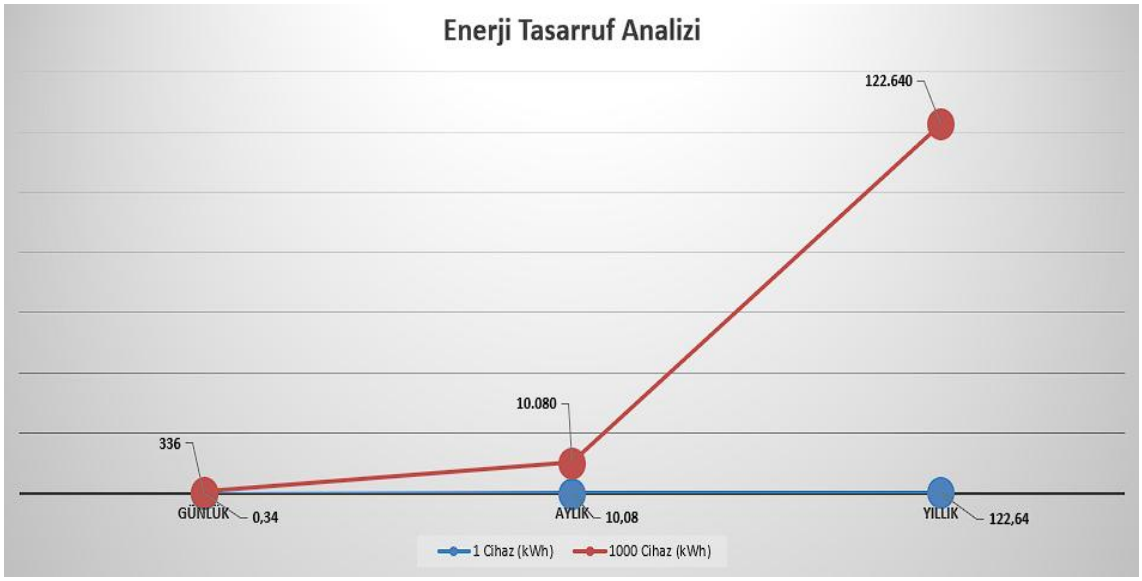
4.1 Bulgular

Bu çalışmada, IOT teknolojilerinin yaygınlaşmasıyla birlikte çok şubeli kurumsal ağlarda oluşan yeni gereksinimler ve bu gereksinimlerin SD-WAN ile nasıl optimize edilebileceği ele alınmıştır. IOT cihazlarının genellikle basit, düşük maliyetli ve işletim sistemine sahip olmayan sensörler veya kameralar gibi veri toplama odaklı cihazlardan oluşması ve firmalarla yapılan işbirliklerinde ağa dahil edilen cihazların yönetiminin firma tarafından

yapılması, bu cihazların doğrudan kurumsal ağa bağlanmasının güvenlik açıklarına yol açabileceğini göstermektedir. Bu nedenle, IOT cihazlarının kurumsal ağdan izole edilerek farklı bir altyapı üzerinden yönetilmesi gerekliliği ortaya çıkmıştır.

Bununla birlikte, uç noktalarda hem kurumsal ağ hem de IOT altyapısı için ana hat ve yedek hat gereksinimi, şirketler için ciddi bir maliyet yükü oluşturmaktadır. Bu çalışmada, SD-WAN teknolojisinin sunduğu dinamik trafik yönlendirme ve IPsec tünelleme yöntemlerinin, kurumsal ve IOT ağlarının yedeklilik ihtiyacını optimize ederek hem güvenlik hem de maliyet açısından sağladığı avantajlar analiz edilmiştir.

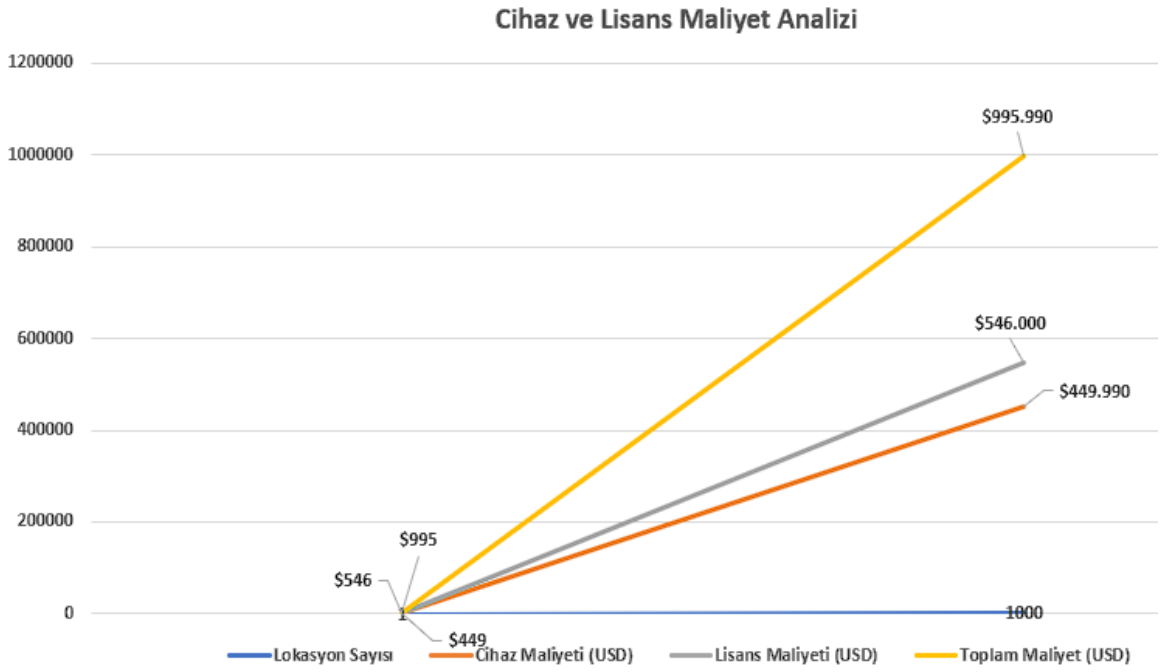
SD-WAN ve IPsec teknolojilerinin, uç noktalarda gereksiz hat maliyetlerini düşürerek ve ağ kaynaklarını daha etkin kullanarak, kurumsal ve IOT altyapıları arasında daha güvenli ve ölçeklenebilir bir çözüm sunduğunu göstermektedir. Ayrıca, SD-WAN'ın merkezi yönetim yetenekleri, trafik optimizasyonu ve politika tabanlı yönlendirme mekanizmaları sayesinde, kurumsal ve IOT ağlarının bağımsız ancak entegre bir şekilde yönetilmesi mümkün hale gelmiştir. Çalışma kapsamında gerçekleştirilen testler ve analizler doğrultusunda, SD-WAN'ın sağladığı operasyonel esneklik, güvenlik ve maliyet avantajlarının, geleneksel WAN çözümlerine kıyasla daha etkili olduğu ortaya konulmuştur.



Şekil 51. Enerji Tasarruf Analizi

Şekil 52'de lokasyonlarda hat yedekliliği ve domain ayrımı için ikincil bir cihaz kullanılmadığında yıllık elde edilen enerji tasarruf analizi gösterilmektedir.

Bir lokasyonda elde edilen enerji tasarrufu günlük yaklaşık 0,34 kWh, aylık yaklaşık 10,22 kWh ve yıllık olarak 122,64 kWh düzeyindedir. Bu değerler, FortiGate 60E model cihazın maksimum 14W güç tüketimi baz alınarak hesaplanmıştır. Hesaplama formülüne göre; 14 W × 24 saat × 365 gün ÷ 1000 = 122,64 kWh/yıl şeklinde yıllık tüketim belirlenmiştir. Bu tasarruf tezin varsayımı olan dağıtık yapılı bir kuruluşun 1000 lokasyon ölçeğinde değerlendirildiğinde yıllık toplam 122.640 kWh enerji kazancı elde edilmekte, bu durum hem çevresel sürdürülebilirlik açısından önemli bir katkı sağlamakta hem de enerji maliyetlerinin düşürülmesinde ciddi bir avantaj sunmaktadır (Fortinet, Forti 60E series data sheet, 2016).



Şekil 52. Cihaz ve Lisans Maliyet Tasarruf Analizi

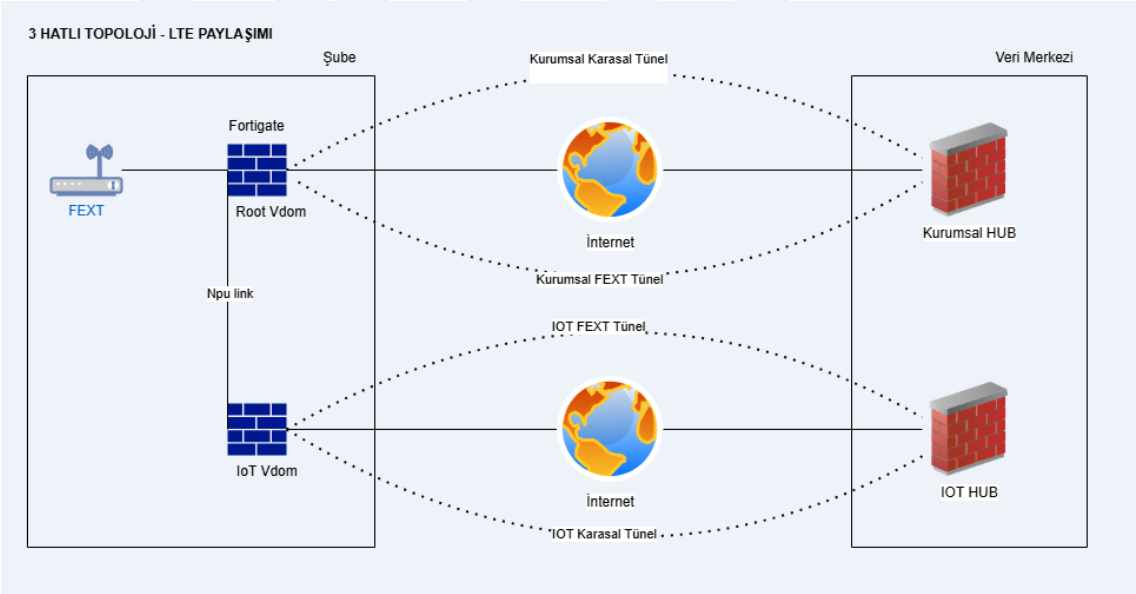
Şekil 53'de 1000 lokasyon için her lokasyonda bir cihaz kullanıldığında toplam maliyet analizi gösterilmiştir.

Tabloya göre, VDOM teknolojisi kullanılarak önerilen modelde her lokasyonda yalnızca tek bir FortiGate 60E cihazı ve lisansı kullanıldığında ortaya çıkan toplam maliyet gösterilmektedir. Geleneksel yöntemde IOT ve kurumsal ağlar ayrı ayrı fiziksel cihazlarla

yönetileceği için, her lokasyona ikinci bir cihaz ve lisans daha eklenmesi gerekecektir. Bu durumda işletmenin toplam cihaz ve lisans maliyeti, önerilen modelin 2 katı kadar olacak ve bütçede ciddi bir yük oluşturacaktır. 1000 lokasyonlu bir yapıda, VDOM tabanlı bu çözüm sayesinde yaklaşık 996.000 USD'lik bir maliyetin önüne geçilmiş olmaktadır (Fortinet, Fortigate 60E datasheet, 2016). Bu da sadece donanım ve lisans açısından bile yüksek ölçekli yatırım tasarrufu anlamına gelmektedir.

Bu doğrultuda, IOT ve kurumsal ağları birlikte yöneten, maliyet etkin ve güvenli bir SD-WAN mimarisi oluşturabilmek için iki temel topoloji önerilebilir. Bu topolojiler, ağ yapısının gereksinimlerine, yedeklilik seviyelerine ve operasyonel önceliklere göre şekillendirilmelidir. Aşağıda, önerilen iki topoloji modeli oluşturulmuştur.

4.1.1 Üç hatlı LTE paylaşımlı yedeklilik modeli



Şekil 53. 3 Hatlı LTE Paylaşımlı Yedeklilik Modeli

Şekil 54'de LTE hattının 2 vdom arasında nasıl kullanılması gerektiğiyle ilgili 3 hatlı olarak tasarlanmış topoloji modeli bulunmaktadır.

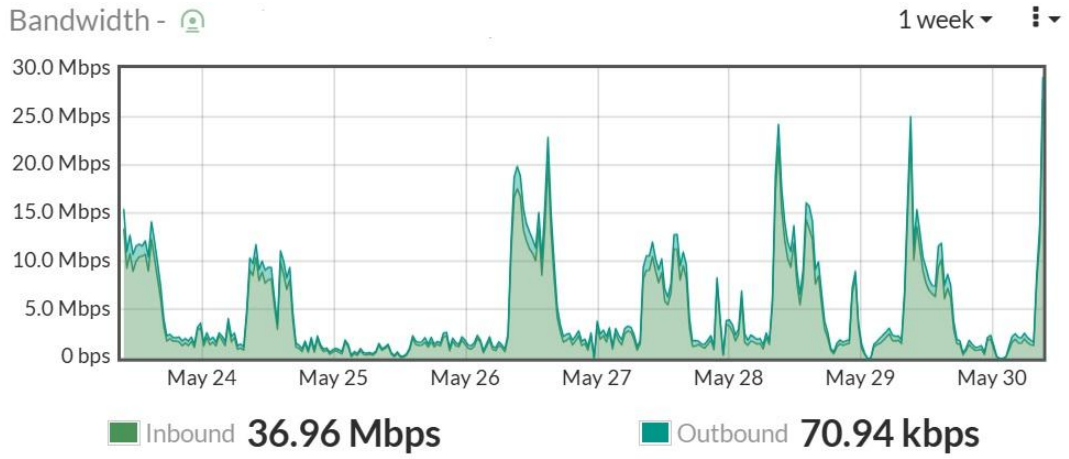
Üç Hatlı Topoloji, yani Tam Yedeklilik Modeli, kurumsal ağ, IoT ağı ve yedek bağlantıların birbirinden ayrılarak yönetildiği güvenli ve esnek bir mimari sunmaktadır. Bu yapıda, kurumsal trafik yalnızca kurumsal hat üzerinden yönlendirilirken, IoT cihazları için özel olarak izole edilmiş ayrı bir ağ bağlantısı tahsis edilmiştir. Böylece,

IoT sistemlerinin kurumsal altyapıdan bağımsız çalışması sağlanarak güvenlik ve performans artırılmıştır. Ayrıca, hem kurumsal hem de IoT ağları için ortak olarak tanımlanan yedek hat, ana bağlantılarda yaşanabilecek olası kesintilerde devreye girerek sürekliliği sağlamaktadır. SD-WAN teknolojisi sayesinde, bu üç bağlantı arasında dinamik trafik yönlendirmesi yapılabilmekte ve ağ kaynakları en verimli şekilde kullanılabilmektedir.

Üç Hatlı Tam Yedeklilik Modeli, ağ güvenliği ve sürekliliği açısından önemli avantajlar sunmaktadır. Bu modelde, IoT ve kurumsal ağlar tamamen izole edilerek birbirinden bağımsız çalışmaları sağlanmakta, böylece güvenlik riskleri en aza indirilmektedir. Olası bir kesinti durumunda ise, iş açısından kritik servisler önceliklendirilerek ilgili trafik yedek hat üzerinden yönlendirilmekte ve hizmet sürekliliği korunmaktadır. Ayrıca, hem IoT hem de kurumsal ağlar için ayrı yedekleme hatlarının bulunması, her iki ağ türü için de güvenilir ve kararlı bir yedekleme mekanizması oluşturulmasına olanak tanımaktadır. Bu yapı, yüksek erişilebilirlik ve ağ dayanıklılığı açısından ideal bir çözüm sunar.

3 Hatlı Topoloji için Önerilen Temel Bileşenler,

- 3 ayrı WAN bağlantısı, (Kurumsal, IOT, Yedek Hat)
- SD-WAN'ın dinamik yönlendirme yetenekleriyle trafik yönetimi
- IOT ve kurumsal ağlar için ayrı güvenlik politikaları ve IPsec tünelleri

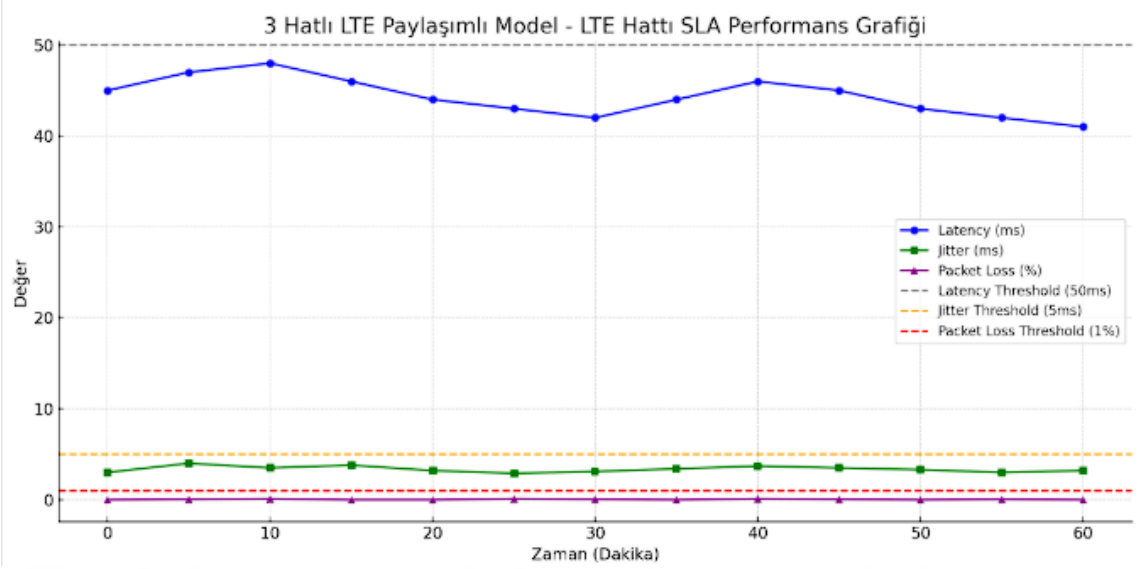


Şekil 54. LTE Yedeklilik Modeli Yük Analizi

Şekil 55'de görülen MRTG tablosu, önerilen 3 hatlı SD-WAN topolojisinde, iki ayrı domain (Kurumsal ve IOT) için LTE bağlantısının yedek hat olarak çalıştığı bir senaryoda, 1 haftalık bant genişliği kullanımını göstermektedir.

Senaryo kapsamında, her iki domainin ana bağlantılarında kesinti yaşanmış ve tüm trafik, ortak LTE hattı üzerinden yönlendirilmiştir.

50 Mbps kapasiteli LTE hattı üzerinde gerçekleşen bu yük aktarımı süresince, özellikle inbound (gelen) trafik değerleri ortalama 36.96 Mbps seviyelerinde seyretmiş; bu da hattın yaklaşık %74'lük bir kapasitesinin kullanıldığını göstermiştir. Outbound (giden) trafik ise yalnızca 70.94 kbps seviyelerinde kalmış, bu da ağın büyük oranda veri indirme yönünde çalıştığını ve veri çıkışının oldukça sınırlı kaldığını ortaya koymuştur. Tüm bu yükün LTE hattı üzerinden sorunsuz bir şekilde taşınabilmiş olması, önerilen topolojide LTE'nin paylaşımlı yedek hat olarak başarılı bir şekilde kullanılabileceğini göstermektedir.



Şekil 55. LTE Hattı SLA Performans Grafiği

Şekil 56, LTE hattının SLA metriklerini göstermektedir.

LTE hattına ait performans analizine göre, gecikme (latency) değerleri 41–48 ms aralığında ölçülmüş olup, 50 ms'lik SLA eşiğinin altında kalmıştır. Bu durum, LTE hattının kritik uygulamalar için dahi yeterli hızda veri iletimi sağlayabildiğini göstermektedir. Gecikme dalgalanması (jitter) ise tüm ölçüm süresince 3–4 ms aralığında seyretmiş ve 5 ms'lik eşik değeri aşılmamıştır. Bu da ses ve video gibi gerçek zamanlı uygulamalar açısından ağın kararlı ve tutarlı bir performans sunduğunu göstermektedir. Paket kaybı ise %0 ile %0.1 arasında ölçülmüş ve %1'lik SLA sınırının oldukça altında kalmıştır; bu da veri iletiminin güvenli, sağlam ve kesintisiz biçimde gerçekleştiğini ortaya koymaktadır. Tüm bu pozitif göstergeler, LTE hattının SD-WAN ortamında yalnızca yedek bağlantı olarak değil, aynı zamanda yüksek öncelikli servisler için de güvenle kullanılabileceğini göstermekte; bağlantının güvenilirliği, kararlılığı ve iş sürekliliği açısından güçlü bir çözüm sunduğunu kanıtlamaktadır.

```
Starting Nmap 7.94 ( https://nmap.org ) at 2025-05-30 14:12 +0300
Nmap scan report for 10.10.20.1
Host is up (0.0040s latency).
All 65535 scanned ports on 10.10.20.1 are filtered

Nmap scan report for 10.10.20.2
Host is up (0.0038s latency).
All 65535 scanned ports on 10.10.20.2 are filtered

Nmap scan report for 10.10.20.3
Host is up (0.0041s latency).
All 65535 scanned ports on 10.10.20.3 are filtered

Nmap done: 256 IP addresses (3 hosts up) scanned in 48.31 seconds
```

Şekil 56. LTE Paylaşımlı Model Sızma Testi Sonuçları

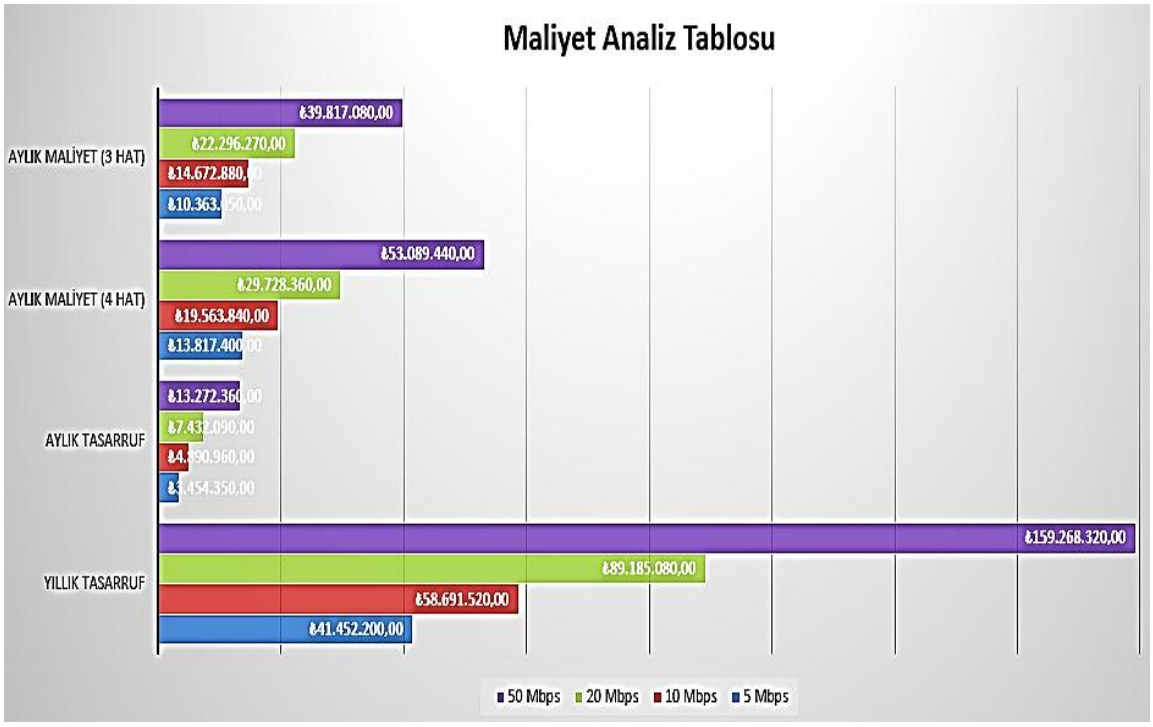
Şekil 57, Kurumsal Domain'e ait bir istemci üzerinden IoT Domain'ine ait 10.10.20.0/24 subnet'ine yönelik tüm TCP portlarını kapsayan bir sızma testidir.

Tüm portların "filtered" durumda olması, iki domain arasında doğrudan erişim olmadığını ve yönlendirme ya da firewall kuralları aracılığıyla başarılı ağ izolasyonu sağlandığını göstermektedir. Bu bulgu, önerilen SD-WAN topolojisinde domainler arası güvenliğin sürdürülebilir olduğunu kanıtlamaktadır.

Tablo 5. 3 Hatlı Topoloji Maliyet Analizi

Band Genişliği	**5 MBPS**	**10 MBPS**	**20 MBPS**	**50 MBPS**
MPLS Aylık Maliyet	₺₺3.454,35	₺4.890,96	₺7.432,09	₺13.272,36
Lokasyon Sayısı	1000	1000	1000	1000
Aylık Maliyet (3 Hat)	₺10.363.050	₺14.672.880	₺22.296.270	₺39.817.080
Aylık Maliyet (4 Hat)	₺13.817.400	₺19.563.840	₺29.728.360	₺53.089.440
Aylık Tasarruf	₺3.454.350	₺4.890.960	₺7.432.090	₺13.272.360
Yıllık Tasarruf	**₺41.452.200**	**₺58.691.520**	**₺89.185.080**	**₺159.268.320**

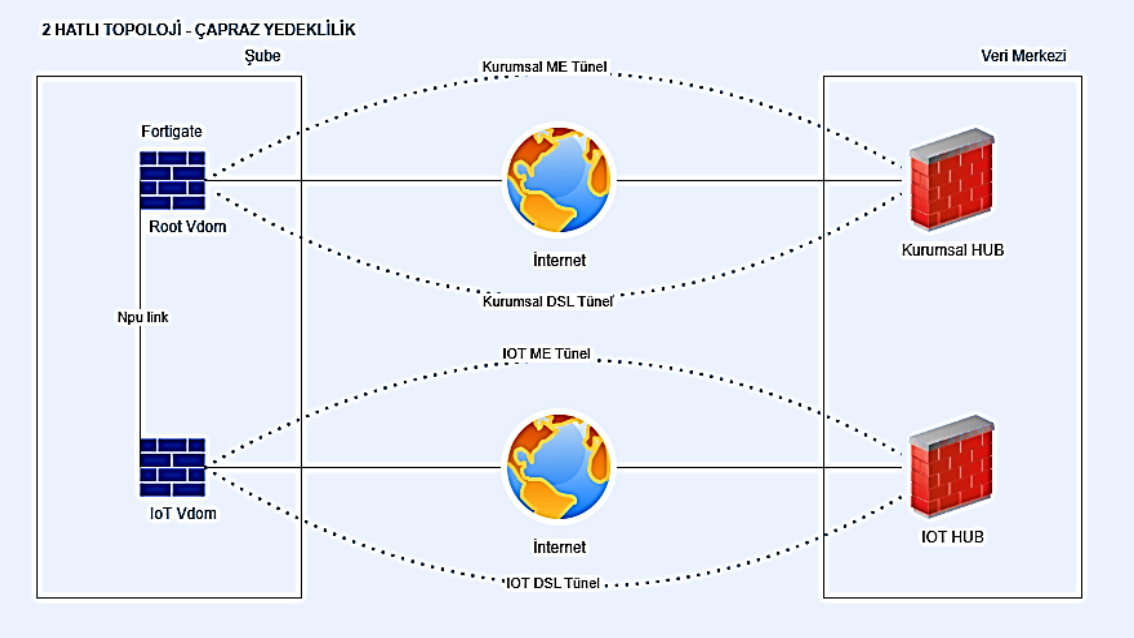
Tablo 5’te 3 hatlı topolojinin 4 hatlı topolojiye oranla sadece MPLS hat fiyatları baz alınarak aylık ve yıllık oranda tasarruf oranları hesaplanmıştır (Turkcell, 2025). Bu hesaplamalara göre domainler arası wan paylaşımının dağıtık yapılı ve çok lokasyonu olan kuruluşlarda maliyet etkisinin önemi gösterilmiştir.



Şekil 57. 3 Hatlı Topoloji Maliyet Grafiği

Şekil 58’de, 1000 lokasyon baz alınarak 3 Hatlı topolojinin maliyet tasarruf analiz hesaplaması yapılarak grafiksel gösterimi verilmiştir.

4.1.2 İki hatlı çapraz yedeklilik modeli



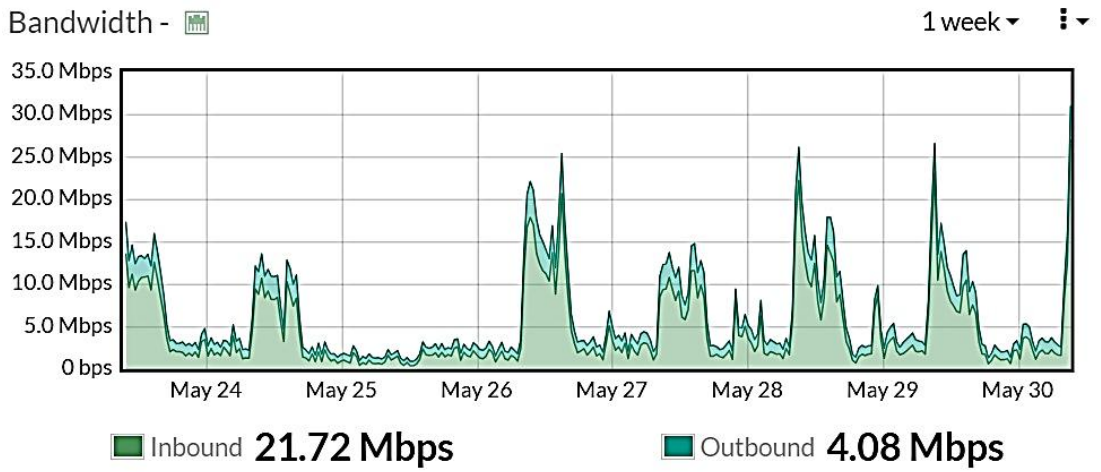
Şekil 58. 2 Hatlı Çapraz Yedekli Topoloji Modeli

Şekil 59'da 2 VDOM arasında hattın çapraz olarak yedeklenmesi için oluşturulmuş topoloji modelidir.

İki Hatlı Çapraz Yedeklilik Modeli, hem kurumsal hem de IOT trafiğinin aynı hatlar üzerinden yönlendirildiği, yedekleme mekanizmasının ise çapraz yedeklilik prensibine dayandığı esnek bir ağ mimarisi sunmaktadır. Bu yapıda birinci hat, öncelikli olarak kurumsal trafik için kullanılmakta olup, gerektiğinde IOT ağı için yedek bağlantı olarak da hizmet verebilmektedir. Benzer şekilde, ikinci hat öncelikli olarak IOT trafiğine tahsis edilmiştir ancak aynı zamanda kurumsal ağın yedek bağlantısı görevini de üstlenmektedir. Bu sayede her iki ağ türü için karşılıklı yedeklilik sağlanmakta, bağlantı sürekliliği ve sistem dayanıklılığı artırılmaktadır. En önemli avantajlarından biri, üçüncü bir bağlantıya ihtiyaç duyulmaması sayesinde maliyetlerin düşürülmesidir. Bu model, ekstra bir hat yatırımı gerektirmeden hem kurumsal hem de IoT trafiği için yüksek erişilebilirlik sağlar. Ayrıca, SD-WAN teknolojisi sayesinde trafik anlık ağ koşullarına göre analiz edilerek en uygun hatta yönlendirilir; bu da ağ trafiğinde esneklik ve performans optimizasyonu sağlar. Çapraz yedekleme prensibi sayesinde, her iki ağ türü için de kesintisiz iletişim sürdürülebilir hale getirilmiş olur, bu da iş sürekliliğini önemli ölçüde destekler.

2 Hatlı Topoloji için Önerilen Temel Bileşenler,

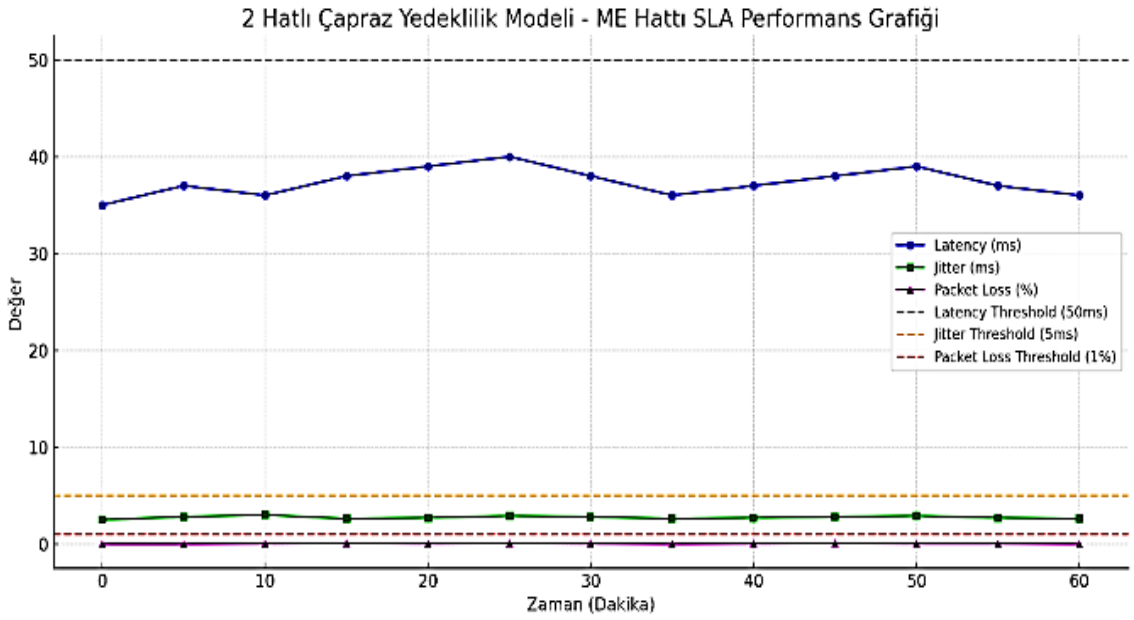
- 2 WAN bağlantısı (Kurumsal ve IOT)
- SD-WAN SLA politikaları ile dinamik yönlendirme
- IOT ve kurumsal ağlar için ayrı güvenlik politikaları ve IPsec tünelleri



Şekil 59. Çapraz Yedeklilik Modeli Yük Analizi

Şekil 60'da yer alan MRTG grafiği, önerilen 2 hatlı çapraz yedeklilik modeline ait bir haftalık bant genişliği kullanımını göstermektedir

Bu senaryoda, IoT domain'ine ait birincil bağlantı hattının devre dışı kalması üzerine, IoT trafiği geçici olarak Kurumsal domain'in ME (Metro Ethernet) hattı üzerinden yönlendirilmiştir. 50 Mbps hat kapasitesine sahip bu altyapı ile hem kurumsal hem de IOT trafiği, aynı fiziksel hat üzerinden birlikte taşınmıştır. Bu bulgu, SD-WAN mimarisiyle yapılandırılmış 2 hatlı çapraz yedeklilik modelinin, yalnızca anlık felaket senaryolarında değil, uzun süreli geçici erişim durumlarında da istikrarlı performans sağladığını ortaya koymaktadır.



Şekil 60. ME Hattı SLA Performans Grafiği

Şekil 61, ME hattının SLA metriklerini göstermektedir.

Grafik, 2 Hatlı Çapraz Yedeklilik Modeli kapsamında IOT hattının devre dışı kaldığı senaryoda, hem kurumsal hem de IOT trafiğinin ME hattı üzerinden taşındığı durumu yansıtmaktadır. Gecikme (latency) değerleri 35–40 ms aralığında seyretmiş ve 50 ms'lik SLA eşiğinin altında kalmıştır; bu da ME hattının iki farklı trafik türünü aynı anda taşımasına rağmen hızlı ve istikrarlı bir veri iletimi sağladığını göstermektedir. Gecikme dalgalanması (jitter) 2.5–3 ms seviyelerinde ölçülmüş olup, 5 ms'lik sınırın oldukça altında kalarak ağın gerçek zamanlı uygulamalar için güvenilir olduğunu ortaya koymuştur. Paket kaybı ise %0 ile %0.1 arasında ölçülerek %1'lik SLA eşik değerinin altında kalmış ve yoğun trafik yüküne rağmen veri iletiminin güvenli ve kesintisiz gerçekleştiğini kanıtlamıştır. Genel olarak değerlendirildiğinde, ME hattı bu senaryoda hem kurumsal hem de IOT trafiğini aynı anda taşımasına rağmen SLA kriterlerini karşılamakta ve çapraz yedeklilik prensibinin etkili şekilde çalıştığını göstermektedir. Bu da, geçici yük aktarımlarında performans kaybı yaşanmadan sistemin sürekliliğinin sağlandığını ortaya koymaktadır.

```
Starting Nmap 7.94 ( https://nmap.org ) at 2025-05-30 16:00 +0300
Nmap scan report for 10.10.10.1
Host is up (0.0031s latency).
All scanned ports on 10.10.10.1 are filtered

Nmap scan report for 10.10.10.2
Host is up (0.0028s latency).
All scanned ports on 10.10.10.2 are filtered

Nmap scan report for 10.10.10.3
Host is up (0.0035s latency).
All scanned ports on 10.10.10.3 are filtered

Nmap done: 256 IP addresses (3 hosts up) scanned in 65.41 seconds
```

Şekil 61. Çapraz Yedeklilik Sızma Testi Sonuçları

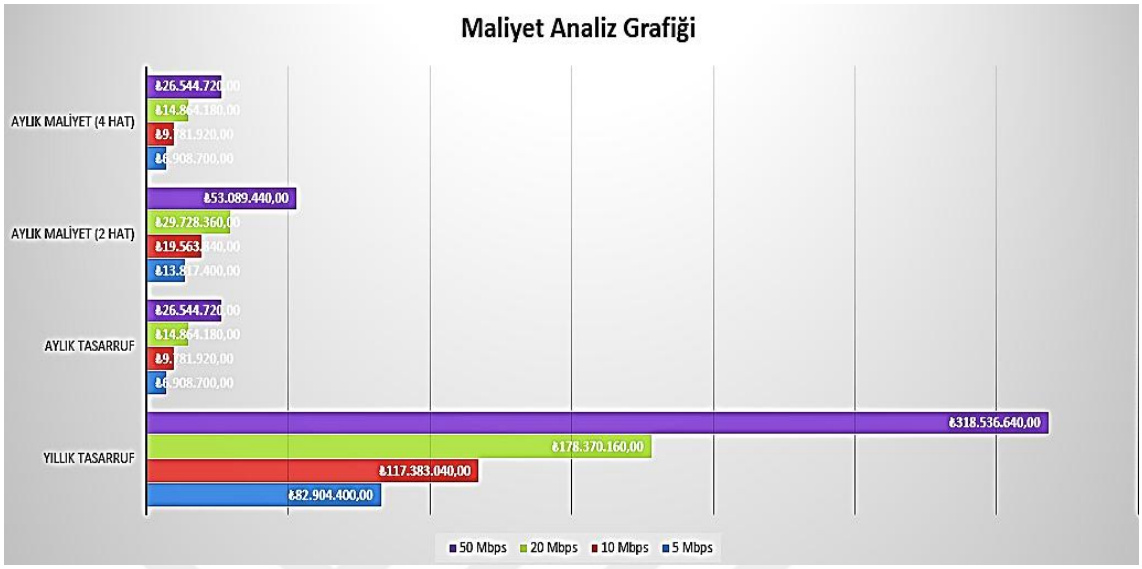
Şekil 62'de Çapraz yedeklilik modeli için domainler arasında sızma testi sonuçları gösterilmiştir.

IOT domain'ine ait bir cihazdan başlatılarak, kurumsal domain'e ait 10.10.10.0/24 subnet'inde bulunan cihazlara yönelik ilk 1000 port üzerinde zafiyet taraması gerçekleştirilmiştir. Tarama sonucunda tüm portların "filtered" statüsünde olduğu görülmüş, bu da IoT domain'inden Kurumsal domain'e doğrudan erişim veya zafiyet istismarı olasılığının engellendiğini göstermiştir.

Tablo 6. 2 Hatlı Topoloji Maliyet Analizi

Band Genişliği	**5 MBPS**	**10 MBPS**	**20 MBPS**	**50 MBPS**
MPLS Aylık Maliyet	₺3.454,35	₺4.890,96	₺7.432,09	₺13.272,36
Lokasyon Sayısı	1000	1000	1000	1000
Aylık Maliyet (2 Hat)	₺6.908.700	₺9.781.920	₺14.864.180	₺26.544.720
Aylık Maliyet (4 Hat)	₺13.817.400	₺19.563.840	₺29.728.360	₺53.089.440
Aylık Tasarruf	₺6.908.700	₺9.781.920	₺14.864.180	₺26.544.720
Yıllık Tasarruf	**₺82.904.400**	**₺117.383.040**	**₺178.370.160**	**₺318.536.640**

Tablo 6’da 2 hatlı topolojinin 4 hatlı topolojiye oranla MPLS hat fiyatları baz alınarak aylık ve yıllık oranda tasarruf oranları hesaplanmıştır (Turkcell, 2025).



Şekil 62. 2 Hatlı Topoloji Maliyet Grafiği

Şekil 63’de, 1000 lokasyon baz alınarak 2 Hatlı topolojinin yarattığı tasarruf maliyet analiz hesaplaması yapılarak grafiksel gösterimi verilmiştir.

Elde edilen bulgulara göre, SD-WAN ile paylaşımlı hat kullanımı, geleneksel WAN mimarilerine kıyasla daha esnek ve maliyet etkin bir çözüm sunarken; aynı zamanda kurumların ağ yapılarına önemli siber dayanıklılık katkıları sağlar. Segmentasyon, şifreleme, uygulama tabanlı yönlendirme ve merkezi yönetim gibi özellikler sayesinde veri bütünlüğü korunur, tehdit yüzeyi daraltılır ve farklı trafik türleri güvenli şekilde aynı fiziksel altyapı üzerinde çalışabilir hale gelir. Özellikle IoT sistemleriyle entegre kurumsal ağlarda bu yapı, güvenliğin sürdürülebilirliği açısından kritik rol oynar.

4.2 Tartışma

Mendiola ve arkadaşları (2016) tarafından yapılan çalışmada, yazılım tanımlı ağ (SDN) teknolojisinin trafik mühendisliğine sunduğu esneklik ve merkezi kontrol avantajları vurgulanmıştır. Çalışmada, SDN'in farklı trafik türlerini etkin bir şekilde yönetebilmesi ve ağ kaynaklarının dinamik olarak tahsis edilmesi, özellikle geniş ölçekli ve karmaşık ağ ortamlarında performansı artıran bir unsur olarak gösterilmiştir. Bu bulgular, bizim SD-WAN tabanlı domainler arası WAN paylaşımı modelimizin, trafik türlerine göre

akıllı yönlendirme ve merkezi yönetim yetenekleri ile ağ verimliliğini artırdığı yönündeki yaklaşımımızı desteklemektedir.

Ancak, Mendiola ve arkadaşlarının çalışması temel olarak veri merkezleri ve backbone ağlar gibi büyük ölçekli, merkezi SDN mimarileri üzerinde yoğunlaşmış olup, dağıtık şube yapıları ve IOT entegrasyonu gibi alanlardaki uygulamalara doğrudan odaklanmamaktadır. Bu açıdan, bizim çalışmamız, SD-WAN mimarisinin domainler arası WAN paylaşımı senaryolarında nasıl uygulanabileceğini ve özellikle IOT ve kurumsal trafiğin birlikte yönetilmesindeki katkılarını ele alarak literatürdeki mevcut çalışmaları tamamlayıcı bir perspektif sunmaktadır (Mendiola, 2016).

Araştırma bulguları, IOT ve kurumsal ağların ayrı yönetilmesi gerektiği fikrini desteklemektedir. Literatürde IOT ağlarının güvenlik riskleri oluşturabileceği ve yüksek bant genişliği kullanımı nedeniyle kurumsal trafiği olumsuz etkileyebileceği ifade edilmektedir. Bu çalışma, SD-WAN'ın sunduğu dinamik trafik yönlendirme mekanizmalarının, kurumsal ve IOT ağlarının aynı altyapı içerisinde yönetilmesini optimize ederek bu riskleri minimize ettiğini göstermektedir. Ancak, bu bulgular bazı çalışmalarla tamamen örtüşmemekte ve SD-WAN'ın yedeklilik yönetimi konusundaki farklı avantajları literatürde yeterince ele alınmamış görünmektedir.

Bununla birlikte, SD-WAN ile sağlanan çapraz yedeklilik ve LTE paylaşımlı model güvenli bağlantı mekanizmalarının, özellikle IOT cihazlarının artan kullanımı ile birlikte, ağ yönetimi için değerlendirilmesi gereken bir topoloji modelidir. Literatürde, geleneksel ağ yönetim modellerinin bu tür dinamik yük değişimlerine karşı esnek olmadığı ifade edilmekte olup, yapılan testler bu görüşü desteklemektedir. Ancak, IOT ve kurumsal trafik için önerilen farklı topoloji modelleri, SD-WAN'ın kullanım senaryolarına yönelik yeni açılımlar sağlamaktadır.

Bu araştırma, SD-WAN'ın domainler arası WAN paylaşımı üzerindeki etkilerini değerlendirerek, hem performans hem de maliyet optimizasyonu açısından avantajlarını ortaya koymaktadır. Bulgular, SD-WAN'ın IOT ve kurumsal ağları ortak bir yapıda yönetirken güvenlik ve yedeklilik sorunlarını çözdüğünü göstermektedir. Literatürdeki benzer çalışmalarla karşılaştırıldığında, bu çalışmanın katkısı çapraz yedeklilik modeli ve LTE paylaşımlı model SD-WAN üzerinden farklı topolojilerin değerlendirilmesiyle ortaya çıkmıştır.

5. SONUÇ ve ÖNERİLER

Bu araştırmada, SD-WAN teknolojisinin domainler arası WAN paylaşımı üzerindeki etkileri değerlendirilmiş ve özellikle IOT ile kurumsal ağların güvenli ve maliyet etkin bir şekilde yönetimi açısından sunduğu avantajlar incelenmiştir. Çalışma kapsamında gerçekleştirilen testler ve analizler, SD-WAN'ın geleneksel ağ yönetim çözümlerine kıyasla daha esnek, güvenli ve ölçeklenebilir bir yapı sunduğunu ortaya koymuştur. Elde edilen bulgular, IOT sistemlerinin yaygınlaşmasıyla birlikte, kurumsal ağlar ile IOT altyapılarının aynı bağlantı üzerinden yönetilmesinin hem güvenlik hem de ağ performansı açısından olumsuz sonuçlara yol açabileceğini göstermektedir. Bu bağlamda, IOT ve kurumsal ağların ayrılarak farklı altyapılar üzerinden yönetilmesi gerekliliği ön plana çıkmıştır.

Çalışmanın sonuçları, SD-WAN'ın sunduğu dinamik trafik yönlendirme ve akıllı yedeklilik mekanizmalarının, kurumsal ağlar ile IOT ağlarının aynı çatı altında daha güvenli ve etkin bir şekilde yönetilmesine olanak tanıdığını göstermektedir. Araştırmada, farklı topoloji senaryoları değerlendirilmiş ve hem tam yedeklilik sağlayan üç hatlı yapı hem de maliyet etkinliği gözeten iki hatlı çapraz yedeklilik modeli ele alınmıştır. Bu modellerin her biri, işletmelerin ihtiyaçlarına göre özelleştirilerek, güvenlik ve performans dengesinin sağlanmasına yardımcı olmaktadır. Çalışma kapsamında yapılan testler, SD-WAN'ın IPsec tünelleme ve trafik yönlendirme mekanizmaları ile kurumsal ve IOT altyapılarının güvenli bir şekilde yönetilebileceğini ve maliyetlerin optimize edilebileceğini ortaya koymaktadır.

Bu araştırmada ortaya konan bulgular, SD-WAN'ın güvenlik ve yönetilebilirlik açısından sağladığı avantajların yanında, belirli sınırlamaların da göz önünde bulundurulması gerektiğini göstermektedir. Çalışmada belirlenen senaryolar spesifik test ortamlarında uygulanmış olup, SD-WAN'ın farklı ölçeklerde ve trafik yoğunluklarında nasıl performans göstereceği konusunda daha geniş çaplı testlerin gerçekleştirilmesi gerekmektedir. Ayrıca, SD-WAN çözümlerinin farklı güvenlik protokolleri ve tehdit algılama sistemleri ile entegrasyonu üzerinde durulmalı ve sektöre özel optimizasyon yöntemleri geliştirilmelidir.

Araştırmanın sonuçları doğrultusunda, SD-WAN teknolojisinin geniş alan ağı yönetiminde sunduğu avantajların daha kapsamlı çalışmalarla desteklenmesi gerektiği sonucuna varılmıştır. Özellikle IOT ve kurumsal ağların birlikte yönetilmesi gereken yapılarda, SD-WAN'ın sunduğu merkezi yönetim, dinamik yönlendirme ve güvenlik politikalarının optimizasyonu, gelecekteki çalışmalar için önemli bir araştırma alanı oluşturmaktadır. Bu doğrultuda, Domainler arası WAN paylaşımının desteklenmesi için merkezden dinamik olarak LTE hat kapasitelerinin ölçülebilmesi, shaping yöntemine göre farklı domainler arasında hat paylaşımı yapılması gerektiği durumlarda hat kapasitesine göre istenilen oranda bant genişliği oranlarının ayarlanması hattın daha verimli kullanımına katkı sağlayacaktır.

KAYNAKÇA

Abergos, V. J. (2024). A Risk Assessment Analysis to Enhance the Security of OT WAN Infrastructures: A Software-Defined Wide Area Network Approach. *Cybersecurity and Privacy*, 4(4), 910-937.

Ahlawat, S. v. (2014). An Introduction to Computer Networking. *International Journal of Computer Science and Information Technology Research*, 2(2), 373-377.

Bora, G. B. (2014). OSI reference model: An overview. *International Journal of Computer Trends and Technology (IJCTT)*, 7(4), 214-218.

Çınar, S. M. (2020). Bir Kurumsal Geniş Alan Ağının Ağ Yönetim Sistemiyle Etkili Yönetimi. *Niğde Ömer Halisdemir Üniversitesi Mühendislik Bilimleri Dergisi*, 9(1), 9-22.

Ercan, T. v. (2016). Endüstride Nesnelerin İnterneti (IoT) Uygulamaları. *Afyon Kocatepe Üniversitesi Fen ve Mühendislik Bilimleri Dergisi*, 16(3), 599-607.

Fortinet. (2016). Forti 60E series data sheet. 05 19, 2025 tarihinde https://avfirewalls.com/datasheets/FortiGate/FortiGate_FortiWiFi_60E_Series.pdf adresinden alındı.

Fortinet. (2016). Fortigate 60E datasheet. 05 19, 2025 tarihinde https://avfirewalls.com/FortiGate-60E.asp?srsltid=AfmBOooXILfpwh3Vv48UBv9Xuis7OJkzNnsyxIghMyqqQpqI1jJqewIF&utm adresinden alındı.

Frankel, S. E. (2005). *Guide to IPsec VPNs.* Gaithersburg, MD, United States: National Institute of Standards and Technology.

Fu, C. W. (2024). Software-defined wide area networks (sd-wans): A survey. *Electronics*, 13(15), 3011.

George, A. S. (2023). SD-WAN Security Threats, Bandwidth Issues, SLA, and Flaws: An In-Depth Analysis of FTTH, 4G, 5G, and Broadband Technologies. *Partners Universal International Innovation Journal*, 1(3), 1-15.

Kurose, J. v. (2010). *Computer Networking: A Top-Down Approach* (Seventh Edition ed.). (A. University of Massachusetts, Ed.) Shanghai: Pearson. 05 19, 2025 tarihinde.https://www.ucg.ac.me/skladiste/blog_44233/objava_64433/fajlovi/Computer%20Networking%20_%20A%20Top%20Down%20Approach,%207th,%20converted.pdf adresinden alındı.

Lammle, T. (2013). *CCNA Routing and Switching Study Guide.* John Wiley & Sons.

Leiner, B. M. (2009). A Brief History of the Internet. *ACM SIGCOMM Computer Communication Review*, 39(5), 22-31.

Li, H. W. (2024). Driving Intelligent IoT Monitoring and Control through Cloud Computing and Machine Learning. *Applied and Computational Engineering*, 64, 75-80.

Mao, H. Z. (2012). *A comparative research on SSL VPN and IPSec VPN.* Shanghai, China: IEEE.

Mendiola, A. A. (2016). A survey on the contributions of software-defined networking to traffic engineering. *IEEE Communications Surveys & Tutorials*, 19(2), 918-953.

Nicolazzo, S. N. (2024). *Service Level Agreements and Security* SLA: A Comprehensive Survey. *arXiv*.

Numan, P. E. (2019). On the latency and jitter evaluation of software defined networks. *Bulletin of Electrical Engineering and Informatics*, 8(4), 1507–1516.

Ouamri, M. A. (2024). A comprehensive survey on software-defined wide area network (SD-WAN): principles, opportunities and future challenges. *The Journal of Supercomputing*, 81, 291–337.

Paillisse, J. P.-N. (2021). SD-Access: Practical Experiences in Designing and Deploying Software Defined Enterprise Networks. *arXiv preprint arXiv*.

Patel, U. v. (2022). SD-WAN Technology: Advantages and Use Cases. *International Journal of Science and Research (IJSR)*, 11(10), 1434-1448.

Petekci, A. R. (2021). Ağ Teknolojileri ile İlgili Makalelerin Bibliyografik Yöntemle İncelenmesi. *Açıköğretim Uygulamaları ve Araştırmaları Dergisi*, 7(3), 141-158.

Sahinaslan, O. (2019). Encryption protocols on wireless IoT tools. In AIP Conference Proceedings. *AIP Publishing*, Vol. 2086, No. 1.

Segeč, P. M. (2020). Architecture, Functions and Benefits. *2020 18th International Conference on Emerging eLearning Technologies and Applications (ICETA)*, 312–317.

Stojanović, M. v. (2009). Service Level Agreements İn Next Generation Networks. *Mihajlo Pupin Institute, Belgrade*.

Şahinaslan, E. (2010). *Standartlara Dayalı Bilgi Güvenliği Risk Analiz ve Ölçümleme Metodolojisinin Bankacılık Sektörüne Özgü Modellenmesi ve Uygulama Yazılımının Geliştirilmesi,.* (Yayın no: 269257). [Doktora Tezi, Trakya Üniversitesi Fen Bilimleri Enstitüsü. Edirne]. https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

Şahinaslan, Ö., ve Şahinaslan, E. (2019). Cross-object information security: A study on new generation encryption. *AIP Conf. Proc.*, 2086 (1): 030034.

Tahenni, A. v. (2023). SD-WAN over MPLS: A Comprehensive Performance Analysis and Security with Insights into the Future of SD-WAN. *arXiv preprint arXiv*.

Troia, S. Z. (2021). SD-WAN: How the Control of the Network Can Be Shifted from Core to Edge. *In 2021 International Conference on Optical Network Design and Modeling (ONDM)*, 1-5.

Turkcell. (2025, 03 01). Kurumsal MPLS VPN Erişim Fiyatları. 05 11, 2025 tarihinde https://superonline.net/hakkimizda/duyurular/mpls-vpn-erisim-hakkinda-bilgilendirme adresinden alındı.

Wright, G. R. (1994). TCP/IP illustrated, volume 2. In G. R. Wright, *The implementation.* Addison-Wesley Professional.

Yang, Z. C. (2019). Software-Defined Wide Area Network (SD-WAN): Architecture, Advances, and Challenges. *In 2019 28th International Conference on Computer Communication and Networks (ICCCN)*, 1-9.

Zeybek, M. v. (2019). Nesnelerin İnterneti: Risk Temelli Yaklaşım. *Denetişim*, (19), 73-88.

ÖZ GEÇMİŞ

Kubilay Akdağ

Eğitim

Yüksek Lisans	Maltepe Üniversitesi, Lisansüstü Eğitim Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı
Lisans	İstanbul Üniversitesi, AUZEF, Yönetim Bilişim Sistemleri
Lisans	Anadolu Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Kamu Yönetimi
Önlisans	Süleyman Demirel Üniversitesi, Bilgisayar Teknolojisi ve Programlama

İş/İstihdam

2020-devam	Migros Genel Müdürlük, Geniş Alan Ağı Teknolojileri Yönetimi
2019-2020	Securitas, B.T. Sistem Uzmanı
2013-2019	Migros Genel Müdürlük, Operasyon ve Servis Yönetimi
2011-2013	Turkcell, B.T. Sistem Uzmanı
2009-2009	ODE Yalıtım Sanayi A.Ş, Bilgi İşlem Stajyeri