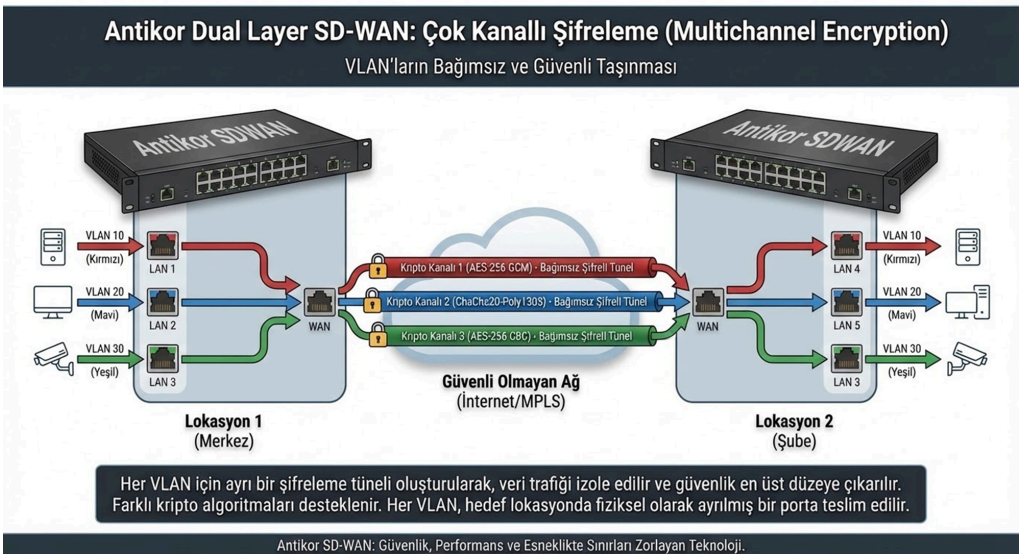
# İÇİNDEKİLER

**Antikor SDWAN Ürününe Genel Bakış....2**
1. Antikor SDWAN ne işe yarar?....3
1.1. Şubeleri ve Uzak Ofisleri Bağlama....3
1.2. Merkezi Yönetim Sistemi (Antikor CTNM)....4
2. Antikor SDWAN - Layer 2 ve LAN Genişletme Yetenekleri....4
2.1 WAN Üzerinden Layer 2 Haberleşme....4
2.2. Layer2 & Layer3 Haberleşme ve Multicast Trafik Aktarım Farkları....5
Multicast Trafik Nedir ve Neden Önemlidir?....5
Layer 3 Tabanlı Çözümlerde Multicast Zorlukları....5
Layer 2 Haberleşmenin Multicast İçin Sağladığı Avantajlar....6
Multicast Trafik Kullanım Senaryoları....6
Performans ve Güvenlik Dengesi....7
Sonuç....7
2.3 Virtual Switching Instance (VSI) ve Ağ İzolasyonu....7
2.4 VLAN Taşıma ve Yönetimi....9
2.5 Switching Özellikleri ve Protokol Desteği....9
**3. Antikor SDWAN - Layer 3 Özellikleri....10**
3.1 Routing ve Switching Birlikte: MultiLayer Switching....10
3.2 BGP Teknolojisi ve MPLS Muadili Kapalı Ağ....10
3.3 Layer 2-4 Paket Filtreleme ve Güvenlik Duvarı....11
3.4 Layer 2-4 QoS (Ağ trafiğini önceliklendirme ve Bant genişliği kontrol)....12
3.5 NAT Arkasından Çalışabilme ve Bağlantı Esnekliği....12
3.6 Çoklu Toplama Noktası Desteği ve FKM Senaryoları....13
4. Antikor SDWAN - Kripto (Şifreleme) Özellikleri....13
4.1. Dual Layer SDWAN Kripto Özellikleri....13
4.2 Çok Kanallı Şifreleme ve VLAN Bazlı İzolasyon....13
4.3 NIST Onaylı Şifreleme Algoritmaları....14
4.4 Peryodik Session Anahtarı Yenileme (Rekey)....15
4.5 Counter Mod Blok Şifreleme ve Gelişmiş Güvenlik....15
4.6 Kaynak Doğrulama ve Bütünlük Kontrolü....16
4.7 Yüksek Performans Şifreleme Altyapısı....16
5. Güvenlik Özellikleri Analizi....17
5.1 Homojen Güvenlik Mimarisi....17
5.2 Şifreleme ve Kapalı Ağ Oluşturma....17
5.3 Yasal Uyumluluk ve Loglama....18
6. Kripto ve Layer 3 Birlikte Kullanım Senaryoları....18
6.1 Entegrasyon Avantajları....18
6.2 Güvenlik ve Performans Dengesi....18
7. Maliyet Avantajları....19
7.1 Merkezi Güvenlik Yönetimi ile Maliyet Optimizasyonu....19
7.2 Bonding Özelliği ile Bant Genişliği Maliyetleri....20

7.3 Altyapı Bağımsızlığı ve Operatör Esnekliği..... 20
7.4 Bakım ve İşletme Maliyetleri.....20
8. Kolay Erişilebilirlik ve Kullanım Kolaylığı.....21
8.1 Kurulum ve Yapılandırma Basitliği.....21
8.2 Modern Yönetim Arayüzü.....21
8.3 Hızlı Entegrasyon ve Kullanım Senaryoları.....21
8.4 Ölçeklenebilirlik ve Genişleme Kolaylığı.....22
9. Antikor Dual Layer SDWAN Öne Çıkan Özellikler..... 22
10. Antikor Dual Layer SDWAN Teknik Özellikleri.....23
11. Antikor Dual Layer SDWAN Kullanım Senaryoları..... 24
12. Genel Değerlendirme ve Sonuç..... 25

# Antikor SDWAN Ürününe Genel Bakış

Kripto Dual Layer SDWAN, ePati Siber Güvenlik tarafından geliştirilen %100 yerli ve milli bir Türk siber güvenlik ürünüdür. Bu çözüm, şubeler arasında kriptolu güvenli Layer2 bağlantı kurulmasını, yerel ağın WAN üzerinden genişletilmesini ve WAN üzerinden VLAN taşınabilmesini sağlamaktadır. Geleneksel SDWAN çözümlerinden farklı olarak bu ürün, hem Layer 2 hem de Layer 3 katmanlarında çalışabilme yeteneğine sahiptir, bu da onu özellikle LAN genişletme ihtiyaçları için ideal kılmaktadır.

Ürünün temel değer önerisi, operatör bağımsız çalışabilirliği ve farklı internet türlerini birleştirebilme kapasitesidir. Metro ethernet, asenkron fiber, xDSL, 4.5G gibi çeşitli bağlantı teknolojileri ile uyumlu çalışabilmesi, kurumların mevcut alt yapılarını koruyarak SDWAN avantajlarından yararlanmalarına olanak tanımaktadır. Bu esneklik, özellikle çok lokasyonlu ve farklı operatörlerden hizmet alan kurumlar için kritik bir avantaj oluşturmaktadır.

- Detaylar ve Datasheetler: https://www.epati.com.tr/sdwan
- Sunum: Antikor SDWAN Tanıtım Sunumu

## 1. Antikor SDWAN ne işe yarar?

SDWAN (Software-Defined Wide Area Network), kurumların şube ve uzak lokasyonlarını merkezi bir şekilde yönetmelerini, ağ trafiğini optimize etmelerini ve güvenli bağlantılar kurmalarını sağlayan bir ağ teknolojisidir. Antikor SDWAN ürünlerinin temel işlevlerini aşağıda detaylı olarak belirtilmiştir.

### 1.1. Şubeleri ve Uzak Ofisleri Bağlama

SDWAN'ın en temel görevi, merkez ofis ile şubeler veya uzak ofisler arasında güvenilir iletişim kurmaktır. Bu bağlantı farklı internet türleri kullanılarak sağlanabilir:

- MPLS: Yüksek kaliteli, düşük gecikmeli kurumsal bağlantı türü
- Fiber: Yüksek hızlı sabit internet bağlantısı
- ADSL/VDSL: Ev ve ofis tipi standart internet bağlantısı
- LTE/4.5G: Mobil veya yedek bağlantı olarak kullanılan kablosuz internet

Bu farklı bağlantı türleri SDWAN tarafından birlikte kullanılabilir veya yedekli olarak çalıştırılabilir. Örneğin, bir şubede hem fiber hem de 4.5G bağlantısı varsa, SDWAN her iki hattı da aynı anda kullanarak toplam bant genişliğini artırabilir veya bir hat arızasında diğer hatta otomatik geçiş yaparak kesintisiz iletişimi sağlayabilir.

### 1.2. Merkezi Yönetim Sistemi (Antikor CTNM)

Antikor SDWAN Merkezi Yönetim Sistemi (CTNM), gelişmiş yönetim fonksiyonları ile merkezi yönetim imkanı sunan bir üründür. Esnek yapılandırma, canlı gösterge paneli ve gelişmiş profil yönetimi özellikleri ile tüm Dual Layer SDWAN cihazlarını merkezi olarak izler ve yönetir.

Antikor SDWAN ürünlerimiz, Konfigürasyon Yönetimi, Toplu Güncelleme Yönetimi, Güncelleme Sunucusu Hizmeti, Güvenlik Politikası ve Obje Yönetimi, Periyodik Konfigürasyon Yedekleme ve Gelişmiş Profil Yönetimi gibi yetenekler sunmaktadır. Bu özellikler sayesinde, tüm SDWAN uç noktaları merkezi olarak izlenebilir ve yönetilebilir.

Bu merkezi yaklaşım, özellikle yüzlerce şubesi olan bankalar, perakende zincirleri ve kamu kurumları için büyük operasyonel kolaylık sağlar.

## 2. Antikor SDWAN - Layer 2 ve LAN Genişletme Yetenekleri

### 2.1 WAN Üzerinden Layer 2 Haberleşme

Kripto Dual Layer SDWAN'ın en güçlü yönlerinden biri, uzak ağlar arasında IP üzerinden Layer 2 düzeyinde güvenli köprüleme yapabilme kapasitesidir. Bu özellik, iki farklı lokasyondaki ağların sanki aynı fiziksel ağdaymış gibi davranmasını sağlar. Geleneksel SDWAN çözümleri genellikle Layer 3 seviyesinde çalışır ve routing tabanlı bir yaklaşım benimserken, bu ürün Layer 2 köprüleme yetenekleri sayesinde broadcast domainlerinin birleştirilmesine imkan tanımaktadır.

Bu yaklaşımın pratik sonuçları oldukça önemlidir. Örneğin, bir bankanın farklı şubelerindeki ATM ağları, merkez veri merkezi ile aynı Layer 2 ağ üzerinde olabilir. Bu sayede ATM cihazları, herhangi bir routing yapılandırması olmadan doğrudan merkezi sistemlerle iletişim kurabilir. Benzer şekilde, bir mağaza zincirinin tüm şubelerindeki satış terminal (POS) cihazları, merkezi ödeme sistemleriyle aynı ağ segmentinde çalışabilir. Bu durum, uygulama uyumluluğunu artırır ve migration süreçlerini basitleştirir.

Tüm ağlar arası iletişim şifreli olarak taşındığı için, bu genişletilmiş Layer 2 ağ güvenliği tehlikeye atmadan WAN üzerinden çalışabilmektedir. Şifreleme, IPSec tüneli içinde gerçekleştirilmekte olup, veri gizliliği ve bütünlüğü sağlanmaktadır. Bu kombinasyon, Layer 2 esnekliği ile güvenlik gereksinimleri arasında ideal bir denge sunmaktadır.

## 2.2. Layer2 & Layer3 Haberleşme ve Multicast Trafik Aktarım Farkları

Multicast (çoklu yayın) trafiği, ağ dünyasında özellikle belirli uygulamalar ve hizmetler için kritik öneme sahip bir iletişim yöntemidir. Layer 2 (Veri Bağlantı Katmanı) haberleşmenin multicast trafiklerinin temiz ve sorunsuz aktarımını sağlaması, Antikor Dual Layer SDWAN'ın en güçlü avantajlarından birini oluşturmaktadır. Bu konuyu teknik açıdan detaylı bir şekilde açıklamak gerekirse;

Multicast Trafik Nedir ve Neden Önemlidir?

Multicast, bir kaynaktan belirli bir alıcı grubuna aynı anda veri gönderilmesini sağlayan bir iletişim yöntemidir. Unicast (tekil yayın) modelinde kaynak her alıcıya ayrı ayrı paket gönderirken, multicast modelinde tek bir veri akışını anda birçok alıcıya ulaştırılmaktadır. Bu yaklaşım, bant genişliği kullanımını önemli ölçüde optimize etmekte ve ağ yükünü hafifletmektedir.

Günümüz ağlarında multicast trafiği birçok kritik uygulama tarafından kullanılmaktadır. Kurumsal video konferans sistemleri, canlı yayın eğitimler, IPTV ve dijital tabelalar, yazılım güncelleme dağıtımları, finansal veri akışları ve güvenlik kamera sistemleri bu uygulamaların başında gelmektedir. Özellikle merkezi bir kaynaktan çok sayıda uzak noktaya aynı içeriğin iletilmesi gereken senaryolarda multicast vazgeçilmez bir teknoloji haline gelmektedir.

Layer 3 Tabanlı Çözümlerde Multicast Zorlukları

Geleneksel Layer 3 (Ağ Katmanı) tabanlı SDWAN ve VPN çözümlerinde multicast trafik aktarımı önemli zorluklar içermektedir. Bunun temel nedeni, Layer 3 yönlendirme mantığının tekil ve çoklu yayın trafiğini farklı şekilde ele almasıdır. Routing protokolleri, paketleri hedef IP adresine göre yönlendirirken, multicast trafiğin doğası gereği birden fazla alıcıya aynı anda ulaşması gerekmektedir.

Layer 3 ortamlarında multicast trafiği genellikle unicast'e dönüştürülmek zorundadır. Kaynak cihaz, her alıcı için ayrı bir unicast akışı oluşturmak durumunda kalır. Bu yaklaşım, kaynak tarafında aşırı işlem yükü oluşturduğu gibi ağ bant genişliğini de verimsiz kullanmaktadır. On farklı şubeye multicast video yayını yapılması gerektiğinde, kaynak sunucu on ayrı video akışı oluşturmak zorundadır; bu da on katına çıkan bant genişliği tüketimi anlamına gelmektedir.

Ayrıca, Layer 3 multicast protokolleri (PIM, IGMP vb.) karmaşık yapılandırma gerektirmekte ve ağ ekipmanları tarafından desteklenmesi gerekmektedir. Farklı operatör ağları üzerinden geçişlerde bu protokollerin çalışması çoğu zaman sorunlu olmaktadır. Internet servis sağlayıcıları genellikle multicast trafiğini desteklememekte veya kısıtlamaktadır.

Layer 2 Haberleşmenin Multicast İçin Sağladığı Avantajlar

Layer 2 haberleşme, multicast trafik aktarımı için doğal ve verimli bir ortam sunmaktadır. Broadcast domain birleştirme özelliği sayesinde, farklı lokasyonlardaki ağlar sanki aynı fiziksel switch üzerindeymiş gibi davranmaktadır. Bu mimaride multicast trafiği, tıpkı yerel ağlarda olduğu gibi sorunsuz bir şekilde tüm ilgili alıcılara ulaştırılmaktadır.

Antikor Dual Layer SDWAN, Layer 2 köprüleme yetenekleri ile multicast paketlerinin WAN üzerinden temiz aktarımını sağlamaktadır. Bir şubedeki multicast kaynağı, herhangi bir özel protokol yapılandırması olmadan diğer tüm şubelerdeki ilgili alıcılara ulaşabilmektedir. Bu yaklaşım, uygulama düzeyinde herhangi bir değişiklik gerektirmeden mevcut multicast uygulamalarının çalışmasına olanak tanımaktadır.

Yerel ağ genişletme özelliği, broadcast domainlerin birleştirilmesini sağlayarak multicast trafiğin doğal yayılımını mümkün kılmaktadır. Şubeler arasında kurulan Layer 2 tüneli, yerel ağ ile WAN arasındaki sınırı ortadan kaldırmaktadır. Bu sayede IGMP (Internet Group Management Protocol) sorguları ve multicast paketleri, tıpkı tek bir LAN'da olduğu gibi sorunsuz çalışabilmektedir.

Multicast Trafik Kullanım Senaryoları

Antikor Dual Layer SDWAN'ın Layer 2 multicast aktarımı, birçok pratik senaryoda kritik avantajlar sunmaktadır. Kurumsal eğitim sistemlerinde merkezden tüm şubelere canlı eğitim yayını yapılması gerektiğinde, multicast teknolojisi tek bir video akışı ile tüm katılımcılara ulaşmayı sağlamaktadır. Bu yaklaşım, bant genişliği maliyetlerini önemli ölçüde düşürmekte ve sunucu yükünü hafifletmektedir.

Güvenlik kamera sistemlerinde merkezi izleme gereksinimleri Layer 2 avantajlarından faydalanmaktadır. Birden fazla şubedeki güvenlik kameralarının merkezde tek bir NVR (Network Video Recorder) üzerinde kaydedilmesi ve izlenmesi gerektiğinde, multicast akışlar sorunsuz çalışmaktadır. Her kamera için ayrı unicast bağlantı kurmak yerine, tek bir multicast grubu tüm kamera verilerini merkeze taşımaktadır.

IPTV ve dijital sistemler de bu teknolojiden büyük fayda sağlamaktadır. Otel zincirleri, alışveriş merkezleri ve hastaneler gibi çok lokasyonlu kurumlarda merkezi içerik dağıtımı multicast ile verimli şekilde gerçekleştirilebilmektedir. Bir kanal değişikliği veya içerik güncellemesi yapıldığında, tüm lokasyonlar anında güncel içeriği almaktadır.

Yazılım ve güvenlik güncellemeleri dağıtımında da multicast'in avantajları ortaya çıkmaktadır. Binlerce uç cihaza aynı anda güncelleme paketi gönderilmesi

gerektiğinde, unicast yerine multicast kullanımı ağ trafiğini dramatik şekilde azaltmaktadır. Kaynak sunucu tek bir akış oluştururken, ağ altyapısı bu akışı ilgili tüm alıcılara verimli şekilde dağıtmaktadır.

Performans ve Güvenlik Dengesi

Layer 2 multicast aktarımının bir diğer önemli avantajı, performans ile güvenlik arasındaki dengenin sağlanmasıdır. Antikor Dual Layer SDWAN, multicast trafiği şifreli tüneller üzerinden aktarırken, aynı zamanda Layer 2-4 paket filtreleme özellikleri ile istenmeyen multicast trafiğinin engellenmesini de sağlamaktadır. Bu kombinasyon, kurumların hem verimlilikten hem de güvenlikten taviz vermeden çalışmasına olanak tanımaktadır.

QoS (Kalite of Service) politikaları multicast trafiğe uygulanabilmektedir. Kritik multicast uygulamaları (örneğin VoIP veya video konferans) bant genişliği önceliği alırken, daha az kritik multicast trafiği (örneğin dijital içerikleri) düşük öncelikli olarak yapılandırılabilmektedir. Bu esneklik, ağ kaynaklarının optimum kullanımını sağlamaktadır.

Sonuç

Layer 2 haberleşmenin multicast trafik aktarımı için sağladığı avantajlar, Antikor Dual Layer SDWAN'ı pazardaki diğer çözümlerden ayıran önemli farklardan birini oluşturmaktadır. Broadcast domain birleştirme, yerel ağ genişletme ve şifreli tünel yeteneklerinin kombinasyonu, karmaşık multicast senaryolarının basit ve güvenli bir şekilde hayata geçirilmesini sağlamaktadır. Bu özellik, özellikle çok lokasyonlu kurumlar, eğitim kurumları, güvenlik sistemleri ve İHA/Dron gibi kamera görüntüleri aktaran yerler için “multicast” stratejik bir değer taşımaktadır.

## 2.3 Virtual Switching Instance (VSI) ve Ağ İzolasyonu

Virtual Switching Instance özelliği, fiziksel olarak farklı ağların izole olarak lokasyonlar arasında taşınabilmesini sağlar. Bu yetenek, güvenlik ve ağ yönetimi açısından kritik öneme sahiptir. Pratik bir örnek olarak, bir kurumun kamera güvenlik sistemi ağı ile internet erişim ağı ayrı ayrı yönetilmek istenebilir. Kripto Dual Layer SDWAN, bu iki farklı ağı tek bir fiziksel hat üzerinden taşıyabilir ve her birini ayrı uplink olarak teslim edebilir.

Network Segmentasyon İhtiyaçlarına Yanıt

Modern kurumsal ağlarda network segmentasyonu, güvenlik, uyumluluk ve performans açısından kritik bir gereklilik haline gelmiştir. Antikor Dual Layer SDWAN'ın VSI özelliği, bu segmentasyon ihtiyaçlarına kapsamlı yanıtlar sunmaktadır. Her bir VSI, bağımsız bir sanal switch gibi davranarak farklı ağ

segmentlerinin birbirinden izole edilmesini sağlamaktadır. Bu izolasyon, güvenlik açıklarının yayılmasını engellemekte ve saldırı yüzeyini minimize etmektedir.

Farklı Güvenlik Seviyeleri İçin İzolasyon: Farklı güvenlik seviyelerine sahip ağ segmentlerinin yönetimi VSI ile son derece basitleşmektedir. Bir hastanede hasta verileri için kullanılan ağ segmenti, ziyaretçi internet erişimi için kullanılan segmentten tamamen izole edilebilmektedir. Tıbbi cihazların bağlı olduğu IoT ağı, ofis ağından ayrı bir VSI üzerinde çalışabilmektedir. Bu segmentasyon, hem düzenleyici gereksinimlerin karşılanması hem de güvenlik açıklarının kontrol altında tutulması açısından büyük önem taşımaktadır.

Yasal Uyumluluk: PCI-DSS, HIPAA, KVKK gibi düzenlemeler, farklı veri türlerinin ayrı ağ segmentlerinde tutulmasını gerektirmektedir. VSI özelliği, bu tür yasal gereksinimlerin WAN ortamında da uygulanabilmesini sağlamaktadır. Kredi kartı bilgileri işleyen sistemler, sağlık verileri içeren sistemler ve kişisel bilgi işleyen sistemler, her biri ayrı VSI üzerinde izole edilebilmektedir. Bu yaklaşım, denetim süreçlerini de kolaylaştırmakta ve uyumluluk kanıtlarının sunulmasını sağlamaktadır.

Departmanlar Arası İzolasyon: Büyük kurumsal ağlarda departmanlar arası izolasyon da VSI ile kolayca sağlanabilmektedir. İnsan kaynakları departmanı, finans departmanı, Ar-Ge departmanı gibi farklı birimlerin ağ trafiği birbirinden bağımsız olarak yönetilebilmektedir. Bu yaklaşım, iç tehditlere karşı koruma sağlarken, her departmanın kendi ağ politikalarını uygulamasına olanak tanımaktadır. Ayrıca, bir departmanda oluşan ağ sorunu diğer departmanları etkilememektedir.

Çok Kiracılı (Multi-Tenant) Ortamlar: Çok kiracılı ortamlarda VSI özelliği kritik bir değer sunmaktadır. Bir hosting sağlayıcısı veya bulut hizmeti vereni, farklı müşterilerinin ağlarını tamamen izole edilmiş VSI'lar üzerinde çalıştırabilmektedir. Her müşteri, kendi VLAN yapılandırmasını ve ağ politikalarını bağımsız olarak yönetebilmektedir. Bu izolasyon, müşteri verilerinin birbirine karışmasını engellemekte ve hizmet seviyesi anlaşmalarının (SLA) güvenli bir şekilde sunulmasını sağlamaktadır.

OT ve IT Ağ İzolasyonu: Bu özellik özellikle OT (Operational Technology) ve IT ağ izolasyonu gerektiren endüstriyel ortamlarda değerlidir. Enerji santralleri, maden ocakları, fabrikalar gibi lokasyonlarda IT ağları ile operasyonel teknoloji ağlarının birbirinden izole edilmesi zorunludur. Ürün, bu izolasyonu WAN bağlantısı üzerinden sürdürme yeteneği sunmaktadır. Bir enerji santralinde, SCADA sistemleri için kullanılan OT ağı ile ofis IT ağı ayrı VLAN'lar üzerinden taşınabilir ve merkeze güvenli bir şekilde ulaştırılabilir. Üstelik bu iki ağ segmenti, fiziksel olarak farklı port gruplarından çıkış yapabilir ve tam izolasyon sağlanabilir.

## 2.4 VLAN Taşıma ve Yönetimi

Ürün, kapsamlı VLAN yetenekleri sunmaktadır. IEEE 802.1Q VLAN standardı hem sanal portlar hem de fiziksel portlar için desteklenmektedir. Untagged, tagged ve hybrid port atamaları yapılabilmekte olup, bu esneklik farklı ağ altyapılarına uyum sağlamayı kolaylaştırmaktadır. Fiziksel portların VLAN üyeliği tanımlanabilir ve Layer2 tünel bağlantıları sanal port olarak üye edilebilir.

Operatör bağımsız olarak VLAN etiketlerini uçlar arasında taşıyabilme özelliği, çok operatörlü ortamlarda büyük kolaylık sağlar. Farklı şubelerde farklı telekomünikasyon operatörleri ile çalışan kurumlar, VLAN yapılandırmalarını merkezden yönetebilir ve tüm lokasyonlarda tutarlı bir ağ politikası uygulayabilir. Bu durum, özellikle belediyeler, bankalar ve perakende zincirleri gibi çok lokasyonlu organizasyonlar için kritik bir yönetim kolaylığı oluşturmaktadır.

Kenar şubelerdeki VLAN'ların merkeze taşınması senaryosu da desteklenmektedir. Bir mağaza zincirinde, her şubede farklı VLAN'lar (örneğin POS VLAN, stok yönetimi VLAN, misafir ağı VLAN) tanımlanmış olabilir. Bu VLAN'lar, merkeze taşınarak merkezi yönetim altında birleştirilebilir veya izole edilmiş olarak tutulabilir. Merkeze trunk (etiketli/tagged) olarak aktarım yapılabilmesi, VLAN kimliklerinin korunmasını sağlar.

VLAN taşıma esnasında MTU (Maximum Transmission Unit), bir ağ arayüzünün tek bir pakette iletebileceği maksimum veri boyutunu (byte cinsinden) 1500 byte lık parçalara böler. Normalde QinQ ile MTU 1500 den 1512 byte yükseldiğinde VLAN taşıma switchler arasında 1512 byte ayarlanarak olur ancak operatörler arası 1500 byte değişmeyeceğinden bu yöntem işe yaramaz. Bazı Firewallar 2 lokasyonu VXLAN (Layer-2 ağları Layer-3 (IP) altyapı üzerinden taşımanıza olanak sağlayan bir overlay (örtü) tünelleme) ile yapar ama burada 3.lokasyon devreye girerse VXLAN da devre dışı kalır.

Antikor Kriptolu Dual Layer SD-WAN ürünü, VXLAN/IPsec benzeri encapsulation kaynaklı MTU düşüşü veya QinQ daki MTU artışı problemini fragmente/defragmente mekanizması ile çözerek, overlay trafiği 1500 byte efektif MTU üzerinden çalıştırabilir. Bu sayede binlerce lokasyon arası yüzlerce VLAN taşıma işini aynı anda yapar.

## 2.5 Switching Özellikleri ve Protokol Desteği

Ürün, profesyonel ağ anahtarlama özelliklerini bünyesinde barındırmaktadır. Rapid Spanning Tree Protocol (RSTP) desteği, döngü önleme ve yedeklilik sağlarken, IEEE 802.3ad LACP (Link Aggregation Control Protocol) ile birden fazla

fiziksel bağlantının tek bir mantıksal bağlantıya birleştirilmesi mümkündür. Bu özellikler, enterprise sınıfı ağ altyapısı gereksinimlerini karşılamaktadır.

LLDP (Link Layer Discovery Protocol) desteği, ağ topolojisinin otomatik olarak keşfedilmesini sağlar. Bu özellik, merkezi yönetim sistemi ile entegre edildiğinde, ağ haritasının otomatik olarak oluşturulmasına ve değişikliklerin takip edilmesine olanak tanır. NetFlow Export servisi ise ağ trafiği analizi için gerekli verilerin toplanmasını sağlar, bu da kapasite planlaması ve performans optimizasyonu için kritik öneme sahiptir.

# 3. Antikor SDWAN - Layer 3 Özellikleri

## 3.1 Routing ve Switching Birlikte: MultiLayer Switching

Kripto Dual Layer SDWAN, hem routing hem de switching yeteneklerini tek bir cihazda birleştiren MultiLayer Switching yaklaşımını benimsemektedir. Bu özellik, ağ yönetimini önemli ölçüde basitleştirmekte ve karmaşıklığı azaltmaktadır. Geleneksel ağ mimarilerinde, routing ve switching için genellikle ayrı cihazlar kullanılmakta ve bu durum hem maliyet hem de yönetim açısından yük oluşturmaktadır. Bu ürün, her iki fonksiyonu tek bir platformda birleştirerek bu sorunu çözmektedir.

Layer 3 routing yetenekleri, IP seviyesinde trafiğin yönlendirilmesini sağlamaktadır. Farklı alt ağlar arasındaki iletişim, routing kurallarına göre gerçekleştirilmektedir. Static routing ve dinamik routing protokolleri desteklenmektedir. Dinamik routing, ağ topolojisindeki değişikliklere otomatik olarak uyum sağlamakta ve manuel müdahale gerektirmeden en uygun yolları belirlemektedir. Bu özellik, büyük ve dinamik ağlarda kritik öneme sahiptir.

Layer 2 switching yetenekleri ise aynı alt ağdaki cihazlar arasındaki iletişimi verimli bir şekilde yönetmektedir. MAC adresi tabanlı anahtarlama, düşük gecikme süreleri sağlamaktadır. VLAN desteği ile ağ segmentasyonu uygulanabilmektedir. Bu kombinasyon, karmaşık ağ gereksinimlerinin tek bir cihazla karşılanmasını mümkün kılmaktadır. Kurumlar, ayrı router ve switch yatırımı yapmak yerine bu entegre çözümü tercih edebilmektedir.

## 3.2 BGP Teknolojisi ve MPLS Muadili Kapalı Ağ

Border Gateway Protocol (BGP), internetin temel routing protokolü olarak kabul görmektedir ve büyük ölçekli ağlarda güvenilir yönlendirme sağlamaktadır. Kripto Dual Layer SDWAN, hem iBGP (internal BGP) hem de eBGP (external BGP) desteği sunmaktadır. Bu yetenek, kurumların kendi özel ağlarında BGP'nin güçlü

yönlendirme kapasitesinden yararlanmalarına olanak tanımaktadır. Özellikle çok lokasyonlu ve karmaşık ağ topolojilerine sahip kurumlar için bu özellik büyük değer taşımaktadır.

BGP teknolojisi kullanılarak oluşturulan ağ, MPLS (Multiprotocol Label Switching) ağlarına benzer özellikler sunmaktadır. MPLS, büyük kurumlar tarafından şube bağlantıları için yaygın olarak kullanılmakta ancak yüksek maliyetleri nedeniyle alternatif çözümler aranmaktadır. Kripto Dual Layer SDWAN, BGP tabanlı kapalı ağ ile MPLS benzeri deneyimi daha uygun maliyetle sunmaktadır. Bu yaklaşım, MPLS'e kıyasla önemli mal tasarrufu sağlamaktadır.

Kapalı ağ oluşturma özelliği, internet üzerinden güvenli ve izole edilmiş ağ bağlantıları sağlamaktadır. Şubeler arası iletişim, genel internetten bağımsız olarak gerçekleşmektedir. Her tünel, şifreli ve izole edilmiş bir kanal üzerinden çalışmaktadır. Bu yapı, internet bağlantısının kesintiye uğraması durumunda bile şubeler arası iletişimin devam etmesini sağlamaktadır. Ayrıca, bu yaklaşım dış tehditlere karşı ek bir koruma katmanı oluşturmaktadır.

## 3.3 Layer 2-4 Paket Filtreleme ve Güvenlik Duvarı

Ürün, Layer 2 seviyesinden Layer 4 seviyesine kadar kapsamlı paket filtreleme yetenekleri sunmaktadır. Bu çok katmanlı güvenlik yaklaşımı, farklı ağ seviyelerinde tehditlerin engellenmesini sağlamaktadır. Layer 2 seviyesinde MAC adresi filtreleme, yetkisiz cihazların ağa erişimini kontrol etmektedir. Layer 3 seviyesinde IP adresi ve protokol filtreleme, ağlar arası erişim kurallarını uygulamaktadır. Layer 4 seviyesinde ise port ve servis bazlı kontrol, uygulama seviyesi erişimini düzenlemektedir.

Stateful packet inspection (durumlu paket denetimi) yeteneği, gelen ve giden paketlerin ilişkisini takip ederek daha akıllı filtreleme kararları vermektedir. Örneğin, içeriden başlatılan bir HTTP oturumuna izin verildiğinde, bu oturuma ait dönen paketler de otomatik olarak kabul edilmektedir. Bu yaklaşım, güvenlik ve kullanılabilirlik arasında iyi bir denge sağlamaktadır. Yetkisiz dış bağlantı girişimleri ise engellenmektedir.

Merkezi güvenlik duvarı politikaları, tüm lokasyonlar için tutarlı şekilde uygulanabilmektedir. Bir politika değişikliği merkezde yapıldığında, anında tüm şubelere dağıtılmaktadır. Bu merkezi yaklaşım, dağıtık güvenlik modellerine kıyasla yönetim kolaylığı sağlamakta ve tutarsızlık riskini ortadan kaldırmaktadır. Özellikle yüzlerce lokasyonu olan kurumlar için bu özellik kritik operasyonel avantajlar sunmaktadır.

## 3.4 Layer 2-4 QoS (Ağ trafiğini önceliklendirme ve Bant genişliği kontrol)

Quality of Service (QoS) yetenekleri, ağ trafiğinin önceliklendirilmesini ve bant genişliğinin verimli yini sağlamönetilmesaktadır. Kripto Dual Layer SDWAN, Layer 2-4 seviyesinde QoS uygulanabilmektedir. Bu kapsamlı yaklaşım, farklı uygulama ve hizmetlerin ağ kaynaklarına erişim önceliklerinin belirlenmesine olanak tanımaktadır. Kritik iş uygulamaları (voip, video konferans) düşük öncelikli trafiğe göre önceliklendirilebilmektedir.

DSCP (Differentiated Services Code Point) işaretleme ve önceliklendirme, ağ üzerinde end-to-end QoS uygulanmasını sağlamaktadır. Trafik sınıflandırma kuralları, kaynak IP, hedef IP, port numarası, protokol ve hatta uygulama türüne göre tanımlanabilmektedir. Bu esneklik, kurumların kendi QoS politikalarını oluşturmalarına ve uygulamalarına olanak tanımaktadır. Bant genişliği garantileri ve limitleri, her trafik sınıfı için ayrı ayrı yapılandırılabilmektedir.

Bant genişliği yönetimi, özellikle birden fazla internet bağlantısının birleştirildiği (bonding) senaryolarda kritik önem kazanmaktadır. Farklı hatlardan gelen trafik, QoS kurallarına göre dağıtılmakta ve öncelikli trafiklerin en uygun hat üzerinden iletilmesi sağlanmaktadır. Bu yaklaşım, yük dengeleme ve yedeklilik ile birlikte değerlendirildiğinde, yüksek erişilebilirlik ve performans sağlamaktadır. VoIP gibi hassas uygulamalar için jitter ve gecikme minimizasyonu sağlanmaktadır.

## 3.5 NAT Arkasından Çalışabilme ve Bağlantı Esnekliği

Network Address Translation (NAT), birçok kurumsal ağda yaygın olarak kullanılmaktadır. Geleneksel VPN çözümleri, genellikle genel IP adresleri veya özel NAT yapılandırmaları gerektirmektedir. Kripto Dual Layer SDWAN, NAT arkasından sorunsuz çalışabilme yeteneği ile bu engeli aşmaktadır. Özel IP adresleri kullanan ağlarda bile tünel kurulabilmekte ve şubeler arası bağlantı sağlanabilmektedir.

NAT traversal (NAT geçişi) mekanizması, UDP hole punching ve diğer teknikler kullanarak NAT cihazları üzerinden bağlantı kurmaktadır. Bu özellik, özellikle port yönlendirme yapılamayan veya ISP tarafından kısıtlanan ortamlarda büyük kolaylık sağlamaktadır. Statik IP gerektirmemesi, dinamik IP'li internet hizmetlerinde bile çalışabilmesi anlamına gelmektedir. Bu esneklik, kurumların mevcut altyapılarını değiştirmeden SDWAN çözümüne geçiş yapmalarına olanak tanımaktadır.

Port yönlendirme gerektirmemesi, güvenlik açısından da avantajlar sağlamaktadır. NAT cihazlarında açık port bulunmadığından, dış saldırılara maruz kalma riski azalmaktadır. Tünel kurulumu, cihazın NAT cihazından çıkış yapan ilk

paketle tetiklenmektedir. Bu yaklaşım, güvenlik ve kullanım kolaylığı arasında iyi bir denge oluşturmaktadır. Özellikle paylaşımlı internet bağlantıları kullanan lokasyonlarda (OTG, cafe, AVM) bu özellik kritik önem taşımaktadır.

### 3.6 Çoklu Toplama Noktası Desteği ve FKM Senaryoları

FKM (Felaket Kurtarma Merkezi) senaryoları, kurumların iş sürekliliği planlarının kritik bir bileşenidir. Birincil veri merkezi kullanılamaz hale geldiğinde, yedek merkez devreye alınabilmelidir. Kripto Dual Layer SDWAN, çoklu toplama noktası (aggregation point) desteği ile bu gereksinimi karşılamaktadır. Birden fazla merkezi lokasyon tanımlanabilir ve yedekleme senaryoları yapılandırılabilmektedir.

Çoklu merkez desteği, coğrafi olarak dağıtık ağlarda da değerli avantajlar sunmaktadır. Farklı şehirlerdeki veri merkezleri, farklı operatör bağlantıları ve farklı alt ağ yapıları ile çalışabilmektedir. Bu esneklik, kurumların mevcut altyapılarını korumalarına ve kademeli geçiş yapmalarına olanak tanımaktadır. Ayrıca, çoklu merkez yapılandırması yük dengeleme senaryolarında da kullanılabilmektedir.

Yüksek Erişilebilirlik (HA) - Cluster Desteği için aktif-pasif merkez yapılandırmaları desteklenmektedir. Aktif-pasif modelde, yedek merkez normalde pasif durumdadır ve birincil merkez arızasında devreye girmektedir. Bu seçenek, kurumların kendi iş sürekliliği gereksinimlerine uygun mimari seçmelerine olanak tanımaktadır.

## 4. Antikor SDWAN - Kripto (Şifreleme) Özellikleri

### 4.1. Dual Layer SDWAN Kripto Özellikleri

- NIST Onaylı Güçlü Simetrik Şifreleme Algoritmaları
- Peryodik Session Anahtarı Yenileme (rekey)
- NIST Onaylı KEX (Key Exchange) Algoritmaları
- Entegre Kimlik Doğrulama ve Bütünlük Kontrolü
- Yüksek Performans (AES-NI, QAT)
- AEAD (Authenticated Encryption-Authenticated Decryption)
- 256 bit Anahtar
- 128 bit Başlangıç Vektörü (Initalization Vector)
- Dahili Counter Mod ile Benzersiz Kriptolama
- Tümleşik Kaynak Doğrulama ve Bütünlük Kontrolü

### 4.2 Çok Kanallı Şifreleme ve VLAN Bazlı İzolasyon

Kripto Dual Layer SDWAN'ın en güçlü yönlerinden biri, her VLAN için ayrı bir şifreleme tüneli oluşturabilme kapasitesidir. Bu özellik, veri trafiğinin izole edilmesini ve güvenliğin en üst düzeye çıkarılmasını sağlamaktadır. Geleneksel VPN

çözümlerinde genellikle tek bir tünel üzerinden tüm trafik şifrelenirken, bu üründe farklı VLAN'lar için ayrı şifreleme kanalları oluşturulabilmektedir. Bu yaklaşım, farklı güvenlik seviyelerine sahip ağ segmentlerinin birbirinden bağımsız olarak korunmasına olanak tanımaktadır.

Her VLAN için ayrı kripto algoritması kullanılabilme özelliği, esneklik ve güvenlik açısından önemli avantajlar sunmaktadır. Örneğin, hassas finans verileri için daha güçlü şifreleme algoritmaları kullanılırken, daha düşük güvenlik gereksinimleri olan ağlar için optimize edilmiş algoritmalar tercih edilebilir. Bu seçimlik yaklaşım, performans ve güvenlik arasında optimal denge kurulmasını sağlamaktadır. Her VLAN, hedef lokasyonda fiziksel olarak ayrılmış bir porta teslim edildiğinden, ağ segmentasyonu fiziksel düzeyde de korunmaktadır.

Şifreleme tüneli yapısının detaylı incelenmesi, ürünün güvenlik mimarisinin daha iyi anlaşılmasını sağlamaktadır. Her bir şifreleme tüneli, bağımsız anahtar yönetimi ile çalışmakta ve bir tüneldeki güvenlik açığı diğerlerini etkilememektedir. Bu izolasyon yaklaşımı, sıfır güvenlik mimarisinin (Zero Trust Architecture) temel prensiplerine uygun olarak tasarlanmıştır. Kurumlar, farklı iş birimleri, departmanlar veya müşteri grupları için izole edilmiş güvenli ağlar oluşturabilir.

## 4.3 NIST Onaylı Şifreleme Algoritmaları

Ürün, NIST (National Institute of Standards and Technology) tarafından onaylanmış güçlü simetrik şifreleme algoritmaları kullanmaktadır. NIST onayı, şifreleme algoritmalarının uluslararası standartlara uygunluğunu ve güvenilirliğini temsil etmektedir. Bu algoritmalar, dünya çapında kamu ve özel sektör tarafından en hassas verilerin korunmasında kullanılmaktadır. Federal standartlara uyum gerektiren ABD kamu projelerinde ve düzenlemeye tabi sektörlerde bu onay kritik bir gereklilik olarak karşılanmaktadır.

Kullanılan simetrik şifreleme algoritmaları, AES (Advanced Encryption Standard) ailesinden güçlü varyantları içermektedir. AES-256 gibi yüksek anahtar uzunlukları, brute-force saldırılarının pratik olarak imkansız olmasını sağlamaktadır. Şifreleme blok boyutları ve modları, veri bütünlüğünü koruyacak şekilde tasarlanmıştır. Donanım hızlandırma desteği (AES-NI, QAT), yüksek bant genişlikli ortamlarda bile performans kaybı yaşanmadan şifreleme işlemlerinin gerçekleştirilmesine olanak tanımaktadır.

Anahtar değişim (Key Exchange - KEX) algoritmaları da NIST onaylı olup, taraflar arasında güvenli anahtar paylaşımını sağlamaktadır. Diffie-Hellman gibi klasik algoritmaların yanı sıra, modern elliptic curve varyantları da desteklenmektedir. Bu esneklik, farklı performans ve güvenlik gereksinimlerine

uygun konfigürasyon seçenekleri sunmaktadır. Anahtar değişim süreçleri, man-in-the-middle saldırılarına karşı koruma sağlayacak şekilde tasarlanmıştır.

## 4.4 Peryodik Session Anahtarı Yenileme (Rekey)

Siber güvenlik dünyasında, uzun süreli şifreleme oturumları potansiyel bir risk oluşturmaktadır. Aynı anahtarın uzun süre kullanılması, kriptografik analiz saldırılarına karşı savunmasızlık yaratabilmektedir. Kripto Dual Layer SDWAN, periyodik session anahtarı yenileme özelliği ile bu riski ortadan kaldırmaktadır. Belirlenen süre aralıklarında veya belirli veri miktarı aktarıldıktan sonra otomatik olarak yeni anahtar üretilmekte ve kullanılmaktadır.

Rekey mekanizması, mevcut bağlantıyı kesintiye uğratmadan arka planda çalışmaktadır. Veri akışı devam ederken anahtar yenileme işlemi gerçekleştirilmekte ve kullanıcılar herhangi bir kesinti yaşamamaktadır. Bu özellik, kritik uygulamalarda sürekli bağlantı gereksinimlerini karşılamaktadır. Özellikle finansal işlemler, sağlık veri aktarımları ve telekomünikasyon gibi kesintisiz hizmet gerektiren sektörler için bu yetenek hayati öneme sahiptir.

Anahtar yenileme politikaları, merkezi yönetim konsolundan yapılandırılabilmektedir. Zaman tabanlı yenileme (örneğin her saat başı), veri miktarı tabanlı yenileme (örneğin her 1 GB aktarım sonrası) veya hibrit yaklaşımlar uygulanabilir. Denetim amaçlı olarak tüm anahtar yenileme olayları loglanmakta ve merkezi log sunucusuna gönderilmektedir. Bu sayede, güvenlik denetimlerinde kapsamlı izlenebilirlik sağlanmaktadır.

## 4.5 Counter Mod Blok Şifreleme ve Gelişmiş Güvenlik

Klasik blok şifreleme yöntemlerinde, aynı plaintext bloğu aynı ciphertext'e dönüştürülmektedir. Bu durum, tekrarlayan veri örüntüleri içeren trafik için önemli bir güvenlik açığı oluşturmaktadır. Örneğin, düzenli aralıklarla gönderilen benzer paketler, şifrelenmiş olmalarına rağmen tahmin edilebilir kalıplar oluşturabilmektedir. Bu kalıpların analizi, saldırganlara değerli bilgiler sağlayabilmektedir.

Counter Mod (CTR) blok şifreleme, bu sorunu her blok için benzersiz bir sayaç (nonce) değeri kullanarak çözmektedir. Aynı veri bloğu farklı zamanlarda şifrelendiğinde, farklı sayaç değerleri nedeniyle tamamen farklı ciphertext üretilmektedir. Bu yaklaşım, şifrelenmiş verinin tahmin edilmesini dramatik olarak zorlaştırmaktadır. Görsel karşılaştırmalarda, klasik blok şifreleme ile counter mod şifreleme arasındaki fark açıkça görülebilmektedir; counter modda her şifreleme işlemi tamamen benzersiz çıktı üretmektedir.

Ürünün counter mod şifreleme kullanması, yüksek güvenlik gereksinimleri olan kurumlar için kritik bir avantaj oluşturmaktadır. Bankalar, sağlık kuruluşları, devlet kurumları ve düzenlemeye tabi sektörler, bu gelişmiş şifreleme yönteminden

faydalanabilmektedir. Ayrıca, counter mod şifreleme paralel işleme yetenekleri sayesinde yüksek performans sunmakta ve çok çekirdekli işlemcilerde verimli çalışmaktadır. Bu kombinasyon, güvenlik ve performans arasında optimal denge sağlamaktadır.

## 4.6 Kaynak Doğrulama ve Bütünlük Kontrolü

Şifreleme, verilerin gizliliğini korurken, bütünlük kontrolü verilerin değiştirilmediğini garanti etmektedir. Kripto Dual Layer SDWAN, tümleşik kaynak doğrulama ve bütünlük kontrolü mekanizmalarını içermektedir. Her paket, şifrelenmeden önce bütünlük kontrol değeri (MAC - Message Authentication Code) ile işlenmektedir. Alıcı taraf, paketi deşifre etmeden önce bu değeri kontrol ederek, paketin yolda değiştirilip değiştirilmediğini doğrulayabilmektedir.

Bütünlük kontrolü için HMAC (Hash-based Message Authentication Code) algoritmaları kullanılmaktadır. SHA-256 gibi güçlü hash fonksiyonları ile anahtar kombinasyonu, sahte paket ekleme veya manipülasyon saldırılarını etkili bir şekilde engellemektedir. Bu mekanizma, hem veri gizliliği hem de veri bütünlüğü için kapsamlı koruma sağlamaktadır. Saldırganlar, doğru anahtar olmadan geçerli bütünlük etiketi oluşturamadıklarından, ağa yetkisiz erişim girişimleri engellenmektedir.

Tümleşik yaklaşım, şifreleme ve bütünlük kontrolünün ayrı işlemler olarak değil, tek bir bütünleşik süreç olarak gerçekleştirilmesini sağlamaktadır. Bu tasarım, performans optimizasyonu sağlarken, uygulama hatalarından kaynaklanabilecek güvenlik açıklarını da minimize etmektedir. Ayrıca, bu bütünleşik yapı, uyumluluk denetimlerinde daha kolay doğrulama yapılabilmesini sağlamaktadır.

## 4.7 Yüksek Performans Şifreleme Altyapısı

Şifreleme işlemleri, özellikle yüksek bant genişlikli ağlarda önemli hesaplama kaynakları gerektirmektedir. Geleneksel yazılım tabanlı şifreleme, yüksek veri akışlarında darboğaz oluşturabilmektedir. Kripto Dual Layer SDWAN, donanım hızlandırma teknolojileri ile bu performans sınırlamalarını aşmaktadır. AES-NI (Advanced Encryption Standard New Instructions) ve QAT (QuickAssist Technology) desteği, şifreleme işlemlerinin işlemci yerine özel donanım üzerinde gerçekleştirilmesini sağlamaktadır.

AES-NI, Intel ve AMD işlemcilerde bulunan ve AES şifreleme algoritmalarını donanım düzeyinde hızlandıran komut setidir. Bu teknoloji, şifreleme işlemlerini onlarca kat hızlandırabilmekte ve CPU yükünü önemli ölçüde azaltmaktadır. QAT ise Intel'in sunucu işlemcilerinde bulunan ve karmaşık kriptografik işlemleri özel donanım

üzerinde gerçekleştiren bir teknolojidir. Bu iki teknolojinin kombinasyonu, 10 Gbps ve üzeri veri aktarım hızlarında bile kesintisiz şifreleme sağlamaktadır.

Performans optimizasyonu sadece şifreleme hızıyla sınırlı değildir. Anahtar yönetimi, oturum kurulumu ve bütünlük kontrolü işlemleri de optimize edilmiştir. Özellikle çok sayıda eşzamanlı tünel gerektiren senaryolarda (binlerce şube), bu optimizasyonlar kritik önem kazanmaktadır. Performans testlerinde, ürünün yüksek yük altında bile tutarlı throughput sağladığı gösterilmektedir. Bu performans özellikleri, kurumların mevcut altyapılarını tam kapasite kullanmalarına olanak tanımaktadır.

# 5. Güvenlik Özellikleri Analizi

## 5.1 Homojen Güvenlik Mimarisi

Kripto Dual Layer SDWAN'ın güvenlik mimarisinin temelinde homojen güvenlik yaklaşımı yatmaktadır. Merkezi güvenlik duvarı politikaları, tüm lokasyonlar için geçerli olmaktadır. Bu yaklaşım, dağıtık güvenlik modellerine kıyasla önemli avantajlar sunar. Geleneksel yaklaşımda her lokasyonda ayrı güvenlik duvarı cihazları konuşlandırılması ve her birinin ayrı yapılandırılması gerekmekteydi. Bu durum, yönetim karmaşıklığına ve potansiyel güvenlik açıklarına yol açabilmektedir.

Merkezi politika yönetimi ile tüm şubelerde tutarlı güvenlik kuralları uygulanabilir. Bir güvenlik politika değişikliği merkezde yapıldığında, anında tüm lokasyonlara yayılır. Bu durum, özellikle büyük ölçekli kurumsal ağlarda güvenlik güncellemelerinin hızlı ve tutarlı bir şekilde dağıtılmasını sağlar. Bir bankanın onlarca veya yüzlerce şubesinde aynı güvenlik politikasının uygulanması gerektiğinde, bu merkezi yaklaşım büyük operasyonel kolaylık sağlamaktadır.

## 5.2 Şifreleme ve Kapalı Ağ Oluşturma

Ağlar arası iletişim şifreli olarak taşınmakta olup, bu durum WAN üzerinden aktarılan verilerin gizliliğini ve bütünlüğünü garanti etmektedir. IPSec tünel şifrelemesi kullanılmakta olup, end-to-end güvenlik sağlanmaktadır. Şifreleme anahtarları merkezi olarak yönetilebilir ve düzenli olarak rotasyonu yapılabilir.

Kapalı ağ oluşturma özelliği, WAN üzerinden güvenli sanal anahtarlama ile izole edilmiş ağ segmentleri oluşturulmasını sağlar. Bu yaklaşım, farklı iş birimleri veya farklı müşteriler için ayrı ağlar oluşturulmasına olanak tanır. Bir hosting şirketi, farklı müşterilerinin ağlarını izole edilmiş sanal anahtarlama ile taşıyabilir. Bir belediye, farklı departmanlarının (fen işleri, sosyal hizmetler, imar) ağlarını ayrı güvenlik alanlarında tutabilir.

### 5.3 Yasal Uyumluluk ve Loglama

5651 sayılı kanun, Türkiye'de internet servis sağlayıcılarının ve kurumsal ağ yöneticilerinin uyması gereken önemli düzenlemeler içermektedir. Kripto Dual Layer SDWAN, 5651 uyumluluğu kapsamında IP dağıtım loglarının tutulabilmesi için MAC adreslerinin merkeze aktarılmasını sağlamaktadır. Bu özellik, özellikle kamu kurumları ve düzenlemeye tabi sektörler için kritik öneme sahiptir.

Merkezi loglama özelliği, tüm SIEM (Security Information and Event Management) çözümlerine uyumlu log gönderimi yapmaktadır. RAW, CEF, EWMM, GELF, JSON ve WELF formatlarında log aktarımı desteklenmektedir. Bu geniş format desteği, kurumların mevcut güvenlik altyapılarına kolayca entegre olmalarını sağlar. Merkezi loglama, güvenlik olaylarının korelasyonu ve forensic analiz için kritik öneme sahiptir.

## 6. Kripto ve Layer 3 Birlikte Kullanım Senaryoları

### 6.1 Entegrasyon Avantajları

Kripto Dual Layer SDWAN'ın güçlü yanı, kripto ve Layer 3 özelliklerinin entegre bir şekilde çalışmasıdır. Her iki yetenek seti, tek bir yönetim arayüzünden yapılandırılabilmekte ve izlenebilmektedir. Bu bütünleşik yaklaşım, ağ yönetim karmaşıklığını azaltmakta ve operasyonel verimliliği artırmaktadır. Kurumlar, ayrı güvenlik ve routing çözümleri yerine bu entegre platformu tercih edebilmektedir.

Performans optimizasyonları, hem şifreleme hem de routing işlemlerini kapsamaktadır. Donanım hızlandırma, şifreleme yükünü hafifletirken, optimize edilmiş routing tabloları hızlı paket yönlendirme sağlamaktadır. Bu kombinasyon, yüksek bant genişlikli ortamlarda bile düşük gecikme süreleri sunmaktadır. Özellikle VoIP ve video uygulamaları için bu performans karakteristikleri kritik öneme sahiptir.

Yönetim ve izleme araçları, her iki özellik setini de kapsamaktadır. Merkezi yönetim konsolu, şifreleme tünel durumlarını, routing tablolarını, güvenlik duvarı kurallarını ve QoS istatistiklerini tek bir ekranda göstermektedir. Bu görünürlük, ağ performansının optimizasyonu ve sorun gidermesi için değerli içgörüler sağlamaktadır. Sorunlar hızlıca tespit edilebilir ve müdahale edilebilmektedir.

### 6.2 Güvenlik ve Performans Dengesi

Kripto Dual Layer SDWAN, güvenlik ve performans arasında optimal denge kurmak için tasarlanmıştır. Güçlü şifreleme algoritmaları kullanılırken, donanım

hızlandırma sayesinde performans kaybı minimize edilmektedir. Kurumlar, güvenlik gereksinimlerine göre şifreleme seviyesini ayarlayabilmektedir. Düşük güvenlik gereksinimli senaryolarda daha hafif algoritmalar, yüksek güvenlik gereksinimli senaryolarda daha güçlü algoritmalar kullanılabilmektedir.

Routing optimizasyonları, şifreleme ek yükünü telafi etmeye yardımcı olmaktadır. En kısa yol hesaplamaları, yük dengeleme kararları ve failover mekanizmaları, ağ verimliliğini artırmaktadır. QoS politikaları, kritik uygulamaların şifreleme işlemlerinden öncelikli olarak geçmesini sağlamaktadır. Bu önceliklendirme, ses ve video gibi hassas uygulamaların performansını korumaktadır.

Yerli ve milli ürün olması, güvenlik açısından ek avantajlar sağlamaktadır. Tüm geliştirme, üretim ve destek süreçleri Türkiye'de gerçekleşmektedir. Bu durum, tedarik zinciri risklerini azaltmakta ve düzenleyici gereksinimlere uyumu kolaylaştırmaktadır. 5651 sayılı kanun, CBDDO rehberi ve diğer Türkiye spesifik düzenlemeleri ile uyum sağlanmaktadır.

# 7. Maliyet Avantajları

## 7.1 Merkezi Güvenlik Yönetimi ile Maliyet Optimizasyonu

Kripto Dual Layer SDWAN'ın maliyet avantajlarının temelinde merkezi güvenlik yönetimi mimarisi yatmaktadır. Geleneksel yaklaşımda, her şube lokasyonunda ayrı bir güvenlik duvarı cihazı konuşlandırılması gerekmektedir. Bu durum, hem donanım maliyetleri hem de lisans maliyetleri açısından önemli bir yük oluşturmaktadır. Ürünün merkezi güvenlik modelinde ise güvenlik duvarı sadece merkezde bulunmaktadır.

Bu yaklaşımın maliyet etkisi boyutludur. Yüz lokasyonlu bir kurum düşünüldüğünde, geleneksel modelde yüz adet güvenlik duvarı lisansı ve donanımı gerekirken, bu çözümde sadece merkezi bir güvenlik altyapısı yeterlidir. Ayrıca, WAN üzerinden tüm trafiğin merkeze yönlendirilmesi sayesinde, her lokasyonda ayrı internet çıkışı ve güvenlik abonelikleri için ödeme yapılması gerekmemektedir. Merkezi internet çıkışı, toplu alım avantajlarından yararlanmayı da mümkün kılmaktadır.

Lisans maliyetleri açısından da önemli avantajlar bulunmaktadır. WAN lisansı veya her lokasyona ayrı lisans alınmasına gerek yoktur. Lisans sayısı, toplam lokasyon sayısına göre değil, merkezi cihaz kapasitesine göre belirlenir. Bu model, özellikle büyüme potansiyeli olan kurumlar için ölçeklenebilir ve öngörülebilir maliyetler sunmaktadır.

## 7.2 Bonding Özelliği ile Bant Genişliği Maliyetleri

Bonding özelliği, farklı internet türlerini aynı anda LACP yöntemiyle merkeze aktarabilme kapasitesi sunmaktadır. xDSL, 4.5G, metro, asimetrik fiber gibi farklı bağlantı türleri birleştirilebilir ve yük dengelemesi yapılabilir. Bu özellik, birden fazla düşük maliyetli internet hizmetinin tek bir yüksek kapasiteli bağlantı gibi kullanılmasını sağlar.

Pratik bir örnek olarak, bir şube için iki ayrı xDSL hattı alınabilir ve bu hatlar bonding ile birleştirilebilir. Tek bir pahalı metro ethernet hattı yerine, iki adet uygun fiyatlı xDSL hattı toplamda daha yüksek bant genişliği sağlayabilir ve aynı zamanda yedeklilik oluşturabilir. Bir hat kesildiğinde, diğer hat üzerinden iletişim devam eder. Bu yaklaşım, hem maliyet optimizasyonu hem de yüksek erişilebilirlik sağlamaktadır.

## 7.3 Altyapı Bağımsızlığı ve Operatör Esnekliği

Operatör bağımsız çalışma özelliği, kurumların en uygun fiyatlı operatörleri seçmelerine olanak tanımaktadır. Geleneksel MPLS çözümlerinde, genellikle tek bir operatör ile sözleşme yapılması ve yüksek MPLS maliyetleri ödenmesi gerekmektedir. Kripto Dual Layer SDWAN, IP ile çalışan herhangi bir internet bağlantısı ile çalışabildiği için, en rekabetçi fiyatları sunan operatörlerle çalışılabilir.

Statik IP gerektirmemesi ve dinamik IP ile çalışabilmesi, operatör seçimini daha da esnekleştirmektedir. Dinamik IP'li internet hizmetleri genellikle statik IP'li hizmetlerden daha uygun fiyatlıdır. NAT ve port yönlendirme gerektirmemesi, modemlerde herhangi bir özel ayar yapılmasına gerek bırakmadan çalışma imkanı sunmaktadır. Bu durum, kurumların mevcut internet hizmetlerini kullanmaya devam etmelerini ve ek maliyetlerden kaçınmalarını sağlamaktadır.

## 7.4 Bakım ve İşletme Maliyetleri

Merkezi yönetim ve izleme yetenekleri, operasyonel maliyetleri önemli ölçüde düşürmektedir. Antikor Merkezi Yönetim ve Monitoring (CTNM) ürünü ile binlerce lokasyonun konfigürasyon yönetimi ve izlemesi tek merkezden yapılabilir. Bu durum, ağ yönetim personeli ihtiyacını azaltır ve insan kaynağı maliyetlerini optimize eder.

Yüksek erişilebilirlik özellikleri (High Availability Cluster ve hat yedekliliği), arıza durumlarında oluşabilecek iş kayıplarını minimize eder. Geleneksel çözümlerde bir hat arızası veya cihaz arızası, lokasyonun tamamen bağlantısının kesilmesine yol

açabilirken, bu üründe otomatik failover ile kesintisiz hizmet sağlanmaktadır. Bu durum, hem doğrudan iş kaybı hem de destek maliyetleri açısından tasarruf sağlamaktadır.

# 8. Kolay Erişilebilirlik ve Kullanım Kolaylığı

## 8.1 Kurulum ve Yapılandırma Basitliği

Ürünün kurulum ve yapılandırma süreçleri, geleneksel ağ çözümlerine kıyasla önemli ölçüde basitleştirilmiştir. NAT veya port yönlendirme gerektirmemesi, mevcut ağ altyapısında herhangi bir değişiklik yapılmasına gerek bırakmadan devreye alınabilmesini sağlamaktadır. Modemlerde özel ayar yapılması gerekmemekte, cihaz doğrudan mevcut internet hattına bağlanarak çalışabilmektedir.

Merkezi yönetim arayüzü, lokasyon ekleme, konfigürasyon dağıtımı ve politika yönetimi işlemlerini basitleştirmektedir. Yeni bir şube eklendiğinde, şablon tabanlı konfigürasyon ile hızlıca devreye alınabilir. Standart yapılandırma şablonları, manuel hata olasılığını azaltır ve tutarlılığı sağlar. Bu yaklaşım, özellikle çok sayıda lokasyonu yöneten ekipler için değerlidir.

## 8.2 Modern Yönetim Arayüzü

HTML5 ve Bootstrap tabanlı responsive arayüz, modern ve kullanıcı dostu bir deneyim sunmaktadır. Herhangi bir ek yazılım veya eklenti gerektirmeden web tarayıcısı üzerinden erişilebilir olması, farklı işletim sistemlerinde çalışma esnekliği sağlamaktadır. Mobil cihazlardan da erişilebilir olması, acil durum yönetimi ve uzaktan müdahale için kolaylık sağlamaktadır.

Arayüzün göz yormayan tasarımı, uzun süreli kullanımda konfor sağlamaktadır. Dashboard yaklaşımı, ağ sağlığı, bağlantı durumu, bant genişliği kullanımı gibi kritik metrikleri tek ekranda göstermektedir. Anlaşılır görselleştirmeler, teknik olmayan yöneticilerin de ağ durumunu takip edebilmesini kolaylaştırmaktadır. Merkezi loglama ve alarm özellikleri, sorunların erken tespit edilmesini ve müdahale edilmesini sağlamaktadır.

## 8.3 Hızlı Entegrasyon ve Kullanım Senaryoları

Ürün, çeşitli kullanım senaryoları için hızlı entegrasyon imkanı sunmaktadır. Banka ATM'leri için intranet güvenliği sağlanması, mobil araçlarda (ambulans, itfaiye) Voice VLAN ve Data VLAN taşınması, toplu taşıma araçlarında 5651'e uygun internet paylaşımı gibi özel senaryolar desteklenmektedir.

Farklı operatörlerden hizmet alan çok lokasyonlu kurumlar için operatör bağımsız çalışma özelliği büyük kolaylık sağlamaktadır. Herhangi bir operatör değişikliğinde veya yeni operatör eklenmesinde, mevcut altyapı korunabilir. Telekomünikasyon altyapısı yetersiz lokasyonlarda bonding ile geniş bant sağlanması, kırsal bölgelerde veya geçici lokasyonlarda hızlı network kurulumu mümkün kılmaktadır.

Belediyeler için merkezi yazıcı VLAN, Voice VLAN ve kamera VLAN taşıma gibi özel ihtiyaçlar karşılanabilir. Enerji santralleri ve maden ocakları gibi kritik altyapılarda IT ve OT ağ izolasyonu ile güvenli bağlantı sağlanabilir. Mağaza ve market zincirlerinde şubeler arası güvenli iletişim, merkezi sistem erişimi ve izleme altyapısı kurulabilir.

### 8.4 Ölçeklenebilirlik ve Genişleme Kolaylığı

Geniş ürün yelpazesi, farklı boyut ve ihtiyaçlara uygun çözümler sunmaktadır. KOBI sınıfından (EPA-TN-4-TR, EPA-TN-8-TR, EPA-TN-16-TR) Data Center sınıfına (EPA-TN-M1-TR, EPA-TN-K500-TR) kadar geniş bir model yelpazesi mevcuttur. Bu durum, kurumların mevcut ihtiyaçlarına uygun boyutlandırma yapmasına ve büyümeye paralel ölçeklendirme planlaması yapmasına olanak tanımaktadır.

Yüksek erişilebilirlik için High Availability Cluster (Aktif-Pasif Cluster) desteği bulunmaktadır. Kritik uygulamalarda, yedeklilik gereksinimleri karşılanabilir. Hat yedekliliği (fail-over) özelliği, birincil bağlantı kesildiğinde ikincil bağlantıya otomatik geçiş sağlar. Bu özellikler, kurumların iş sürekliliği gereksinimlerini karşılamaktadır.

## 9. Antikor Dual Layer SDWAN Öne Çıkan Özellikler

- Operatör bağımsız çalışma: IP üzerinden haberleşebilen (İnternet ve intranet) tüm lokasyonlarınızı bağlayabilirsiniz. Telekomünikasyon operatöründen bağımsız olarak yurtiçi / yurtdışı tüm noktalardan Layer2 SDWAN kurabilir.
- Bağlantı türü özgürlüğü: Metro ethernet, Asenkron (ev tipi) Fiber, xDSL (ADSL, VDSL, G.SHDSL vb.), 4.5G vb. IP ile çalışan tüm bağlantı teknolojileri ile çalışır.
- Bonding özelliği sayesinde farklı internet türlerini (xDSL, 4.5G arkasından, metro, asimetrik fiber vb.) aynı anda LACP yöntemiyle merkeze aktarır.
- Statik IP gerektirmez: Lokasyonlarınızda statik IP ye ihtiyaç yoktur. Dinamik IP ile çalışabilir.
- Port Yönlendirme, NAT ayarı gerektirmez: Lokasyonlardaki modemlerde herhangi bir ayar gerektirmez, NAT arkasından çalışabilir, port yönlendirme gerektirmez. Paylaşımlı internetlerden dahi Layer2 SDWAN kurabilirsiniz.
- Taşınan Layer2 Trafikte Paket Filtreleme (Layer2-4 Firewall) özelliği vardır.

- Taşınan Layer2 Trafikte QoS - Etkin Bant Genişliği Yönetimi yapabilir.
- Manager'a Otomatik Register ve NAT Arkasından Yönetim
- Merkezi Yönetim Desteği ile Erişilebilirlik Takibi, Konfigürasyon Yönetimi
- Manager, aynı zamanda Yerel Güncelleme Sunucusu olarak çalışır.
- Hem Yurtiçi Hem Yurtdışı Tüm Operatörlerle Sorunsuz Çalışma
- FKM Senaryoları için Çoklu Toplama Noktası Desteği
- Binlerce Lokasyonda Sorunsuz Çalışma (iBGP ve eBGP desteği)
- BGP ile Dinamik Routing; Full Mesh / Partial Route Paylaşımı
- 4,5G/LTE, MetroEthernet, xDSL vb. Tüm Bağlantıları Destekler
- Bağımsız Yönetim Bacağı (Out of Band Management)
- Bağımsız Cluster Bacağı (Out of Band Cluster Interface)
- Denetim Günlüğü ile Detaylı ve Geri Alınabilir Audit Loglar
- Çevrimiçi/Çevrim-Dışı Güncelleme Esnasında Trafik Kesintisi yaşanmaz
- Syslog – SIEM Entegrasyonu (CEF, JSON, EWMM, WELF, CIM)
- Save / Deploy aşamasında değişiklikler listelenir ve onaya sunulur
- Yönetim Paneli ve SSL VPN için Yerel, RADIUS, LDAP, AD, TACACS+, POP3, SOAP, HTTP API + 2FA desteği
- HTTP API Desteği

## 10. Antikor Dual Layer SDWAN Teknik Özellikleri

- Layer3 SDWAN özelliklerine ek olarak; Antikor Merkezi yönetim ve monitoring ürünü ile yönetilebilir. binlerce lokasyonun konfigürasyon yönetimi ve izlemesi sağlanabilir.
- Virtual Switching Instance özelliği ile fiziksel olarak birbirinden farklı ağları da izole olarak lokasyonlar arasında taşıyabilirsiniz. Ör: Kamera ağı ile İnternet ağından ayrı ayrı uplinkler alarak lokasyonlara 2 ayrı uplink kablosu olarak teslim edebilir. Trafikler karışmaz.
- Yerel ağınızı internet hatlarınız üzerinden uzatarak, Layer2 düzeyinde güvenli sanal anahtarlama (virtual switching) yaparak kapalı bir ağ oluşturur. Switchler arasında uplink gibi çalışır.
- Kenar şubelerdeki VLAN'ları merkeze taşır. Kenar şubede VLAN destekli switch bulunmaması halinde Antikor Layer2 SDWAN kendisi switch gibi VLAN tagging yapabilir.
- Yerel ağlarınızı genişleterek, bağladığı ağın broadcast domainlerini birleştirir, Wide area üzerinde Layer2 anahtarlama yapmanıza olanak tanır.
- Bonding özelliği sayesinde (Farklı internet türlerini -xDSL, 4.5G arkasından, metro, asimetrik fiber vb.-) yük dengeleme yapar.
- Tüm SIEM çözümlerine RAW, CEF, EWMM, GELF, JSON, WELF formatlarında log gönderimi yapar.
- High Availability Cluster (Aktif - Pasif Cluster) ve Hat Yedekliliği (fail-over) özelliği
- Spanning Tree Protocol, Rapid Spanning Tree Protocol özelliği vardır.
- Hem Sanal Portlar Hem de Fiziksel Portlar için IEEE 802.1Q VLAN (Untag Port Atama, Tagged Port Atama ve Hibrit Port Atama) özelliği vardır.
- Fiziksel Port Üye Etme, Layer2 Tünel Bağlantısını Sanal Port olarak Üye Etme özelliği vardır.

- IEEE 802.3ad Link Aggregation Control Protocol (LACP) desteği vardır.
- Link Layer Discovery Protocol(LLDP) desteği vardır.
- NetFlow Export Servisi vardır.

## 11. Antikor Dual Layer SDWAN Kullanım Senaryoları

- Banka ATM leri gibi intranet güvenliği için Dual Layer SDWAN kullanılabilir. Layer2 ulaşım imkanı sağlanması nedeniyle ATM Router'larında kurulan GRE tünellere ihtiyaç kalmayacaktır. ATM'lerde yer alan Kamera, ATM'nin bilgisayarı ve switch vb. cihazların Management interfacelerinin her biri izole VLAN'da olmak üzere trafiği Layer2 olarak VLAN tagged/trunk şekilde merkeze taşınması sağlar. Multi Channel encryption ile her bir VLAN farklı bir kriptoya dahil edilerek çok katmanlı güvenlik ve izolasyon sağlar.
- Mobil araçlarda Layer2 SDWAN kurularak, hem Voice VLAN hem Data VLAN taşınmasına olanak tanınması. Ambulans vb. uygulamalar olabilir.
- Toplu taşıma araçlarında, halka açık alanlarda 5651'e uygun kaydı tutulan internet paylaşımı için 4.5G üzerinden Layer2 SDWAN ile merkezdeki firewall'a trafiğin taşınması. Merkezdeki firewalldan Mernise Entegre Hotspot yapılması.
- Uluslararası lokasyonları olan kurum/kuruluşlarda güvenli intranet ağı kurulması
- Farklı operatörlerden hizmet alma ihtiyacı olan çok lokasyonlu kurum/kuruluşlarda güvenli intranet ağı kurulması
- Telekomünikasyon altyapılarının yetersiz olduğu lokasyonlarda geniş bant ihtiyacı halinde birden fazla internet hattı ile bonding yapılarak merkeze bağlanması
- Ek hizmet binası gibi yapılanmalarda, merkezdeki VLAN'ların kullanılması ihtiyaçlarının karşılanması
- Araştırma Geliştirme, Lab. gibi router kullanılmayan kapalı networklerin lokasyonlar arası genişletilmesi ihtiyaçlarının karşılanması
- Belediyeler gibi çok lokasyonlu yapılarda Merkezi Yazıcı VLAN'ı, Voice VLAN, Kamera VLAN gibi izole kalması gereken ağların tüm lokasyonlara ulaştırılabilmesi ihtiyaçlarının karşılanması
- Enerji santrali, maden ocağı gibi lokasyonların merkeze güvenli bağlanması. Ek olarak ihtiyaç halinde IT ve OT ağlarının izole olarak taşınması.
- Mağaza/market zincirlerinin şubeler arası güvenli bağlantısının sağlanması.

## 12. Genel Değerlendirme ve Sonuç

Kripto Dual Layer SDWAN, Layer 2 yetenekleri açısından pazardaki en kapsamlı çözümlerden birini sunmaktadır. VLAN taşıma, virtual switching, broadcast domain birleştirme ve kapsamlı VLAN yönetimi özellikleri, özellikle LAN genişletme ihtiyaçları için güçlü bir araç oluşturmaktadır. Bu özellikler, geleneksel SDWAN çözümlerinin sunmadığı yetenekler sunarak, farklı kullanım senaryolarına yanıt vermektedir.

Güvenlik açısından, merkezi yönetim mimarisi, Layer 2-4 firewall, şifreleme ve yasal uyumluluk özellikleri, kapsamlı bir güvenlik çözümü sunmaktadır. 5651 uyumluluğu ve merkezi loglama özellikleri, Homojen güvenlik yaklaşımı, kurumların tutarlı güvenlik politikaları uygulamasını kolaylaştırmaktadır.

Kripto Dual Layer SDWAN, kripto ve Layer 3 özellikleri açısından pazardaki en kapsamlı çözümlerden birini sunmaktadır. Şifreleme tarafında, NIST onaylı algoritmalar, periyodik anahtar yenileme, counter mod şifreleme ve donanım hızlandırma gibi gelişmiş özellikler, yüksek güvenlik gereksinimlerini karşılamaktadır. Layer 3 tarafında ise BGP desteği, MultiLayer switching, kapsamlı QoS ve NAT geçişi gibi yetenekler, enterprise sınıfı ağ gereksinimlerini karşılamaktadır.

Bu iki özellik setinin entegrasyonu, kurumlara tek bir platformda bütünleşik ağ ve güvenlik çözümü sunmaktadır. Maliyet optimizasyonu, yönetim kolaylığı ve performans avantajları, bu entegrasyonun somut faydalarıdır. Özellikle Türkiye'deki yerli ürün gereksinimleri ve düzenleyici uyum ihtiyaçları göz önüne alındığında, Kripto Dual Layer SDWAN stratejik bir seçenek oluşturmaktadır.

Maliyet avantajları, özellikle çok lokasyonlu kurumlar için oldukça çekicidir. Merkezi güvenlik yönetimi, bonding ile bant genişliği optimizasyonu, operatör esnekliği ve düşük işletme maliyetleri, toplam sahip olma maliyetini optimize etmektedir. Statik IP gerektirmemesi ve mevcut altyapı ile uyum, ek yatırım ihtiyacını minimize etmektedir.

Kolay erişilebilirlik ve kullanım kolaylığı, ürünün önemli güçlü yönlerindendir. Basit kurulum, modern yönetim arayüzü, hızlı entegrasyon senaryoları ve ölçeklenebilirlik, kurumların çözümü hızlıca benimsemesini ve verimli bir şekilde kullanılmasını sağlamaktadır. Bu özellikler, özellikle sınırlı IT kaynaklarına sahip kurumlar için kritik avantajlar oluşturmaktadır.

Sonuç olarak, Kripto Dual Layer SDWAN, Layer 2 tabanlı LAN genişletme ihtiyaçları olan, güvenlik, maliyet ve kullanım kolaylığı dengesini arayan kurumlar için güçlü bir seçenek sunmaktadır. Özellikle Türkiye'deki yerli ürün gereksinimleri, 5651 uyumluluğu ihtiyaçları ve operatör esnekliği arayan kurumlar için ideal bir çözüm niteliğindedir.