



Antikor Tümleşik Siber Güvenlik Sistemi EPA-CTNM-500 Serisi SD-WAN Merkezi Yönetim Sistemi, gelişmiş yönetim fonksiyonları ile merkezi yönetim sağlayan %100 yerli ve milli bir üründür. Esnek yapılandırma, canlı gösterge paneli ve gelişmiş profil yetenekleri ile tüm Dual Layer SD-WAN ürünlerinizi merkezi olarak izler ve yönetir.

### Profil Desteği

Merkezi Yönetim Sistemi, birden fazla güvenlik politikasını "Profil" adı altında yönetir. Yönetilen SD-WAN ürünleri birden fazla profile üye edilebilir. Bu sayede genel güvenlik profiline tüm yönetilen sistemleri dahil edilebilir, özelleşmiş güvenlik profilleri ile bölgesel ayarlar uygulanabilir.

### Toplu Politika Yönetimi

Antikor Dual Layer SD-WAN Merkezi Yönetim Sistemi(CTNM), kurumsal güvenlik politikanızı, yönettiğiniz Antikor Dual Layer SD-WAN ürünlerine toplu olarak uygular. Yönettiğiniz uçların erişilebilirlik durumu ve bildirimlerini merkezi olarak harita üzerinde görüntüler.

### Performans



Güvenlik fonksiyonlarını yürütürken ağınızı maksimum performansla işletir. Güçlü network stack sayesinde kurumsal ağınızın güvenlik ve network ihtiyaçlarını kolaylıkla, yüksek verimle karşılar.

### Yönetim



Antikor® Merkezi Yönetimden kendine bağlı Antikor SD-WAN'lara Güncelleme Sunucu Hizmeti verebilir, Konfigürasyon Şablon Yönetimi, Tekil olarak Yönetebilme ve Toplu Güncelleme Yönetimi yapabilir.





# Ürün Özellikleri

## Merkezi Yönetim Özellikleri

Yönetilen Antikor Dual Layer SD-WAN Sistemleri için;

- Konfigürasyon Yönetimi
- Konfigürasyon Şablon Yönetimi
- Güncelleme Sunucusu Hizmeti
- Güvenlik Politikası ve Objeler Yönetimi
- Periyodik Konfigürasyon Yedekleme
- Harita Üzerinde Erişim Takibi
- Uyarı ve Bildirimlerini Takip Etme
- IPsec Tünel ile Şifreli İletişim
- Tekil Olarak Yönetebilme
- Profil / Global Konfigürasyon Yönetimi
- Toplu Güncelleme Yönetimi
- Detaylı Denetim Kayıtları
- Bildirim Yönetimi
- Yetki Yönetimi

## Network Arayüzü Özellikleri

- Loopback Arayüzü, IEEE 802.1Q VLAN Desteği
- Link Birleştirme:
  - LACP, Failover, Load Balance, Round Robin
- Köprüleme / STP / Ethernet Bypass
- Virtual Extensible LAN (VXLAN)
- IPv4 / IPv6 Statik Yönlendirme
- Statik ARP

## IPsec VPN

- Kriptolama:
  - AES, CAMELIA, NULL\_ENC, SERPENT, TWOFISH
- Kimlik Doğrulama:
  - MD5, SHA1, SHA256, SHA384, SHA512, AES
- Wildcard ID Desteği
- NAT Traversal Desteği
- PKI - Public Key Infrastructure Desteği
- PSK - Pre Shared Key Desteği

## Servisler

- Canlı Gösterge Paneli
- Otomatik Güncelleme Servisi
- Çevrimdışı (Offline) Güncelleme
- Otomatik Konfigürasyon Yedekleme
- Antikor® Paylaşımlı Yönetim
- SNMP v2/v3 Servisi
- Syslog - Desteklenen Formatlar;
  - RAW, CEF, EWMM, GELF, JSON, WELF, CIM
- LLDP Servisi

## Lisanslama

Bağımsız (Out of Band) Cluster (HA) Desteği	Aktif-Pasif
Adreslenebilir CPU Thread Sayısı	24
Yönetilebileceği Antikor SD-WAN Sayısı	500
IPsec VPN Tünel Sayısı	500
Maksimum Profil Sayısı	100

## Yönetim Arayüzü Özellikleri

- HTML5 Responsive Web Arayüzü
- SSL Sertifika bazlı kimlik doğrulama
- 2FA - İki Faktörlü Doğrulama
- Servis Portunu özelleştirme
- SSH Konsolu
- Fiziksel Konsol (Monitör, Klavye)
- Seri Konsol (Donanımda mevcutsa)
- Olay Bildirim Servisi
  - SMS, E-posta, Tarayıcı Bildirimi

## Sanal Switch Özellikleri

- Layer2 Tünel Bağlantısını Sanal Port olarak Üye Etme
- Layer2 Tünel için IPsec Şifreleme
- Fiziksel Port Üye Etme
- Hem Sanal Portlar Hem de Fiziksel Portlar için IEEE 802.1Q VLAN:
  - Untag Port Atama
  - Tagged Port Atama
  - Hibrit Port Atama
- VLAN Destekli MAC Tablosu
- IEEE 802.3ad Link Aggregation Control Protocol (LACP)
- Spanning Tree Protocol
- Rapid Spanning Tree Protocol
- Link Layer Discovery Protocol
- NetFlow Export Servisi
- MAC Learning

## Fiziksel Platformlar için Minimum Gereksinimler

- En az 24 Core İşlemci
- En az 32 GB Ram
- 960 GB Solid State Disk
- MultiQueue Server Ethernet Kartı

## Sanal Platformlar için Minimum Gereksinimler

- VMware ESXi 6.7 ve üstü Hipervizör
- En az 24 Core AESNI destekli İşlemci
- En az 32 GB Rezerve Ram
- 960 GB Depolama Alanı (4 KB ile En az 10000 IOPS destekli)
- Ethernet Kartları, PassThrough olarak konfigüre edilmelidir

\* Minimum gereksinimler sistem yapılandırmasına ve donanıma göre değişiklik gösterebilir.

eP-FR-79 Rev.02 / Yayın Tarihi: 01.04.2019 / Rev.Tarihi: 02.05.2021

ePati Siber Güvenlik Teknolojileri A.Ş.

Mersin Üniversitesi Çiftlikköy Kampüsü  
Teknopark İdari Binası Kat: 4 No: 411  
Posta Kodu: 33343 Yenışehir / MERSİN

www.epati.com.tr

bilgi@epati.com.tr

+90 324 361 02 33

+90 324 361 02 39

