



COMMON CRITERIA
EAL 4+



TRtest

Antikor v2 Tümleşik Siber Güvenlik Sistemi EPA-CLM-20K Serisi Yeni Nesil Güvenlik Duvarı (NGFW) Merkezi Loglama Sistemi (CLM), gelişmiş fonksiyonları ile merkezi loglamayı sağlayan %100 yerli ve milli bir üründür. Esnek yapılandırma, canlı gösterge paneli ve istatistik yetenekleri ile tüm güvenlik duvarlarınızı merkezi olarak loglarını tek merkezde toplayarak bu loglar üzerinde arama yapılmasını sağlar.

Loglama Desteği

Merkezi Loglama Sistemi, birden fazla uç NGFW'nin loglarını tek merkeze toplar ve birleştirir. Toplanan Loglardan üretilen grafiklerde ilgili loga tıklandığında "Loglarda Ara" seçeneği ile loglarda geçmişe dönük arama yapılabilir.

İstatistik Yetenekleri

Antikor Merkezi Loglama ürünü, Uç NGFW'lerden gelen Logların istatistiklerinde oturum sayılarının (geçen/drop olanların) grafiklerini çizer. En yüksek Kaynak IP, Hedef IP, Servislere ve Protokol'lere göre sınıflandırır ve grafiklerini çizer.

Performans



Merkezi Loglama Ürününde gösterilen tüm istatistiklerin geçmişe dönük saatlik/günlük/aylık ve yıllık verileri tutulur. Grafikler saniyeler içerisinde yeni veriler eklenerek yenisi ile değiştirilir.

Yetkilendirme



Antikor® Merkezi Loglama kendine bağlı Antikor NGFW lerden gelen verilerde yetkilendirme hizmeti verir. Yetki verilen kullanıcılar, yetkilendirmesine bağlı olarak kendi loglarında arama yapabilir.



Ürün Özellikleri

Merkezi Loglama Özellikleri

- Loglanan Antikor NGFW Sistemleri için;
- Loglama Yönetimi
- Loglama Şablon Yönetimi
- Anlık Log Monitörü
- Günlük Oturum (Session) sayısı istatistikleri
- Saatlik Oturum (Session) sayısı istatistikleri
- Top 10 Hedef IP'lerin İstatistikleri
- Top 10 Kaynak IP'lerin İstatistikleri
- Top 10 Servislerin İstatistikleri
- IPsec Tünel ile Şifreli İletişim
- Uyarı ve Bildirimlerini Takip Etme
- Protokollerin Dağılım İstatistikleri
- Loglama Şablon Yönetimi
- Uyarı ve Bildirimleri Takip Etme
- SSH Tünel ile Kriptolu Transfer

Detaylı Denetim Kayıtları

- Trafik Analizi
- Kural Logları
- VPN Raporları
- Uygulama Logları
- Tehdit Analizi
- Website Logları
- DNS Analizi

IPsec VPN

- Kriptolama:
 - AES, CAMELIA, CHACHA20-POLY1305, NULL
- Anahtar Değişimi (Key Exchange):
 - DH, Elliptic Curve, Post Quantum: ML-KEM
- Wildcard ID Desteği, NAT Traversal Desteği
- IKE v1/v2 Desteği
- PKI - Public Key Infrastructure Desteği
- PSK - Pre Shred Key Desteği

Servisler

- Canlı Gösterge Paneli
- Otomatik Güncelleme Servisi
- Çevrimdışı (Offline) Güncelleme
- Otomatik Konfigürasyon Yedekleme
- Antikor® Paylaşımlı Yönetim - Sanal Sistem
- SNMP v2/v3 Servisi
- 5651 Loglama
- Dahili Kamu SM - Zaman Uygulaması
- Loglarda Arama
- Uyarıları Gösterme
- LLDP Servisi

Lisanslama

- Bağımsız (Out of Band) Management Plane Var
- Adreslenebilen CPU Thread Sayısı 28
- Loglayabileceği Antikor NGFW Sayısı 100
- IPsec VPN Tünel Sayısı 100
- Maksimum Loglama Performansı (Log/Sn) 20K

Yönetim Arayüzü Özellikleri

- Özelleştirilebilir Canlı Gösterge Paneli (Dashboard)
- HTML5 Responsive Web Arayüzü (Servis Portunu özelleştirme)
- SSL Sertifika bazlı kimlik ve 2FA İki Faktörü doğrulama
- Management Plane için Kaynak Rezervasyonu
- SS Konsolu
- Fiziksel Konsol (Monitör, Klavye) ve Seri Konsol (Donanımsal varsa)
- Log - Rapor Yönetimi
- Olay Bildirim Servisi
 - SMS, E-posta, Tarayıcı Bildirimleri

Kimlik Doğrulama Yöntemleri

- Yerel Kullanıcı, SMS
- HTTP(API), POP3/IMAP
- SSO:Negotiate Kerberos – Active Directory
- LDAP, TACACS+, RADIUS, RADIUS Challenge

Entegrasyonlar

- API/TAXII/STIX Entegrasyonu
- ICAP, harici Sandbox Entegrasyonu
- SIEM & SOAR Entegrasyonları

Ürün Sertifikasyonları

- Common Criteria EAL4+
- TRtest Ürün Uygunluk Belgesi
- %100 Yerli Malı Belgesi

Yönlendirme

- IPv4 / IPv6 (Dual Stack)
- Statik Yönlendirme
- Sanal Yönlendirme ve İletme (VRF)

Fiziksel Platformlar için Minimum Gereksinimler

- En az 28 Core İşlemci
- En az 96 GB Bellek
- En az 10 TB Solid State Disk (SSD)
- En az 2 adet Ethernet Kartı (Management ve Dataplane için)

Sanal Platformlar için Minimum Gereksinimler

- VMware ESXi, Hyper-V, Proxmox Hipervizör
- En az 28 Core AESNI destekli İşlemci
- En az 96 GB Rezerve RAM
- En az 10 TB 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: 05.05.2025

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

