epati

antikor v2

Tümleşik Siber Güvenlik Sistemi

EPA-CLM-5 Serisi
NGFW Merkezi Loglama Sistemi

COMMON CRITERIA EAL 4+

TRtest

Antikor v2 Tümleşik Siber Güvenlik Sistemi EPA-CLM-5 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.

ePati Siber Güvenlik Teknolojileri A.Ş.
Mersin Üniversitesi Çiftlikköy Kampüsü
Teknopark İdari Binası Kat: 4 No: 411
Posta Kodu: 33343 Yenişehir / MERSİN

www.epati.com.tr
bilgi@epati.com.tr
+90 324 361 02 33
+90 324 361 02 39

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
- 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)
- NAT64, IPv6 6to4 Tünelleme
- Statik ARP

IPsec VPN

- Kriptolama:
  - AES, CAMELIA, NULL_ENC, SERPENT, TWOFISH
- Kimlik Dogrulama:
  - MD5, SHA1, SHA256, SHA384, SHA512, AES
- WildCard ID Destegi
- NAT Traversal 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 - Zamane Uygulaması
- Syslog - Desteklenen Formatlar;
  - RAW, CEF, EWMM, GELF, JSON, WELF, CIM
- LLDP Servisi

Lisanslama

Bağımsız (Out of Band) Cluster (HA) Desteği	Aktif-Pasif
Adreslenebilen CPU Thread Sayısı	4
Loglayabileceği Antikor NGFW Sayısı	5
IPsec VPN Tünel Sayısı	5
Maksimum Loglama Performansı (Log/Sn)	5K

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

Kimlik Doğrulama Yöntemleri

- Mernis
- SMS
- Yerel Kullanıcı
- HTTP(API)
- LDAP / Active Directory
- RADIUS
- POP3 / IMAP
- TACACS+

Ürün Sertifikasyonları

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

Yönlendirme

- IPv4 / IPv6 Statik Yönlendirme
- Yönlendirme Monitörü

Fiziksel Platformlar için Minimum Gereksinimler

- En az 4 Core Atom İşlemci
- En az 4 GB DDR4 2400 MHz RAM
- 240 GB Solid State Disk
- Intel MultiQueue Server Ethernet Kartı

Sanal Platformlar için Minimum Gereksinimler

- VMware ESXi 6.7 ve üstü Hipervizör
- En az 4 Core AESNI destekli İşlemci
- En az 4 GB Rezerve RAM
- 240 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 Yenişehir / MERSİN

www.epati.com.tr
bilgi@epati.com.tr
+90 324 361 02 33
+90 324 361 02 39