epati

antikor v2

Tümleşik Siber Güvenlik Sistemi

EPA-CFWM-K3 Serisi
NGFW Merkezi Yönetim Sistemi

COMMON CRITERIA EAL 4+

TRtest

Antikor v2 Tümleşik Siber Güvenlik Sistemi EPA-CFWM-K3 Serisi Yeni Nesil Güvenlik Duvarı (NGFW) 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 güvenlik duvarlarınızı merkezi olarak izler ve yönetir.

Profil Desteği

Merkezi Yönetim Sistemi, birden fazla güvenlik politikasını "Profil" adı altında yönetir. Yönetilen Antikor NGFW'ler 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 Yeni Nesil Güvenlik Duvarı (NGFW) Merkezi Yönetim Sistemi, kurumsal güvenlik politikanızı, yönettiğiniz Antikor Yeni Nesil Güvenlik Duvarlarına 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 NGFW lere Güncelleme Sunucu Hizmeti verebilir, Konfigürasyon Şablon Yönetimi, Tekil olarak Yönetebilme ve Toplu Güncelleme Yönetimi 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 Yönetim Özellikleri

- Yönetilen Antikor NGFW Sistemleri için;
  - Konfigürasyon Yönetimi
  - Konfigürasyon Şablon Yönetimi
  - Güncelleme Sunucusu Hizmeti
  - Güvenlik Politikası ve Obje 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
- Lisans Sunucusu (Lisans kurulum durumunun görüntülenmesi)
- Lisans Portalı (Update ve Lisans Durumları Güncellemesi)
- SSH Tünel ile Kriptolu Transfer

Uç NGFW Senaryoları

- Merkezden Donanım kaynak kullanımı (CPU/RAM) takibi
- Merkezden Güncelleme ve Sürüm Durumunun İzlenmesi
- Merkezden Uç NGFW'lerin Erişim Tespiti ve Renkli Gösterimi
- Merkezden Uç NGFW'lere Tekil Yönetim
- Merkezden Uç NGFW'lere Kural ve Konfigürasyon Basabilme
- Merkezden Uç NGFW' lere Şablon(Template) Tabanlı Konfigürasyon
- Merkezden Uç NGFW'lerin Yedeklerini Alma ve Yeni Cihaza Göderme

IPsec VPN

- Kriptolama:
  - AES, CAMELIA, CHACHA20-POLY1305, NULL
- Anahtar Değişimi (Key Exchange):
  - DH, Elliptic Curve, Post Quantum: ML-KEM
- WildCard ID Destegi, 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 (Kendi Ayarları)
- 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	32
Yönetebileceği Antikor NGFW Sayısı	3000
IPsec VPN Tünel Sayısı	3000
Maksimum Profil Sayısı	300

Yönetim Arayüzü Özellikleri

- Özelleştirilebilir Canlı Gösterge Paneli (Dashboard)
- HTML5 Responsive Web Arayüzü (Servis Portunu özelleştirme)
  - SSL Sertifika bazlı kimlik ve 2FA İki Faktörlü 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

- Commom 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 32 GB Ram
- En az 2 TB Solid State Disk
- En az 2 adet Ethernet Portu (Managemet ve Dataplane için)

Sanal Platformlar için Minimum Gereksinimler

- VMware ESXi, Hyper-V, Proxmox Hipervisör
- En az 32 Core İşlemci
- En az 64 GB Rezerve Ram
- En az 2 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: 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