

— AĞ ERİŞİM DENETİMİ / FORTİGATE ENTEGRASYONU

Rosa FPortal – FortiGate İnternet Erişim Portalı

Kayıt, doğrulama ve onayla kontrollü internet erişimi

Rosa FPortal, kurum ağındaki kullanıcıların internet erişimini kayıt, SMS/e-posta doğrulaması ve IT onayına bağlar. Onaylanan cihaz FortiGate REST API ile anında izinli gruba eklenir; süreli izinler kendiliğinden kapanır, her işlem değiştirilemez bir denetim zincirine yazılır.

ÖNE ÇIKANLAR

01

FortiGate ile doğrudan entegrasyon

Adres nesnesi, grup, politika ve DHCP işlemleri REST API ile yapılır; ayrı captive portal lisansı gerekmez.

02

Doğrulanmış kimlik, onaylı erişim

6 haneli SMS/e-posta OTP, KVKK onayı ve isteğe bağlı IT onayı; süreli veya süresiz erişim.

03

Kayıtsız cihaz portala düşer

Yerleşik koşullu DNS, onaysız istemcinin sorgularını portala yönlendirir; işletim sistemi 'ağa giriş yap' uyarısı verir.

04

İz bırakan denetim kaydı

Her işlem SHA-256 zincirli kayda yazılır; kayıt silinse bile kişi ve cihaz geçmişi aranabilir kalır.

KİMLER İÇİN

Belediye ve kamu kurumlarında MPLS ile bağlı birimlerin internet erişimini kimliğe bağlamak

Kişisel telefon ve dizüstü bilgisayarların kurum ağına kayıt ve onayla alınması

Ortak kullanılan bilgisayarlarda her kullanıcının kendi adına internete çıkması

Misafir ve geçici personele süreli internet erişimi verilmesi

Yazıcı, kamera ve IoT cihazlarının envanterle birlikte kontrollü açılması

Özellikler 89 ÖZELLİK

Aşağıdaki liste ürünün mevcut sürümünde çalışan özellikleri modül modül gösterir.

Kullanıcı Kayıt Portalı 12

- Kayıt formu: ad soyad, T.C. kimlik no (algoritmik kontrol), birim, cep telefonu, kurumsal e-posta, cihaz türü, not
- Kullanıcının IP adresi otomatik alınır; MAC adresi FortiGate cihaz envanterinden ve DHCP kiralardan bulunur
- Ağ bazında doğrulama modu: Form + OTP, SMS ile hızlı giriş veya OTP'siz form (doğrudan IT onayına düşer)
- 6 haneli tek kullanımlık kod SMS veya e-postayla gönderilir; varsayılan 5 dk geçerli, en fazla 5 deneme
- OTP kanalı ağ bazında seçilir: yalnız SMS, yalnız e-posta veya kullanıcının tercihi
- KVKK aydınlatma metni onayı zorunlu; KVKK ve gizlilik metinleri herkese açık sayfalarda yayınlanır
- Doğrulanmış cihaza 180 gün geçerli imzalı çerez yazılır; rastgele MAC'li telefonlar tek tıkla yeniden bağlanır
- Cihaz başka ağa geçtiğinde 'Bu benim' ile kayıt yeni ağa taşınır, IT onayından sonra erişim sürer
- Kayıtlı kullanıcı hızlı girişi: telefon numarası + SMS doğrulamasıyla form yeniden doldurulmadan erişim
- Geçici kullanıcı girişi: yöneticinin verdiği kullanıcı adı: şifre ile 1 günlük erişim
- Oturum penceresi ve 'Oturumu Kapat' düğmesi; ortak cihazda erişim anında kesilir, sıradaki kişiye form gelir
- Kurum logosu, kurum adı ve metinlerle markalanabilen arayüz; açık ve koyu tema

Erişim Talepleri ve Onay 10

- Ayrı listeler: Onay Bekleyen, Onaylı, Hotspot Cihazları, Geçici Cihazlar, OTP Aşamasında, Reddedilen, Süresi Dolan, Tümü
- Tek tıkla onay: 4 saat, 8 saat, 1 gün, 1 hafta, 30 gün veya süresiz erişim
- Onay sonrası erişim süresi değiştirilebilir; süresi dolan izin otomatik kapatılır
- Ağ bazında otomatik onay: doğrulama tamamlanınca erişim IT beklemeden açılır
- Talebi reddetme, erişimi kesip yeniden onaya alma, kalıcı silme ve listeyi topluca temizleme
- Onaylı kaydı kara listeye alma: erişim kesilir, cihaz yasak grubuna eklenir
- Cihaza elle IP atama, IP modu (DHCP / rezervasyon / statik) ve cihaz türü değiştirme

- Cihazı hotspot (ortak kullanım) olarak işaretleme; hotspot cihazda çerez yazılmaz, herkes kendi adına girer
- Kayda erişim profili atama veya profil değiştirme; cihaz yeni profilin izin grubuna taşınır
- Arama ve filtreler: ağ, profil, IP modu, cihaz türü; sütun sıralama ve sayfalama

Kişiler, Cihazlar ve Envanter 14

- Kişi kartı: iletişim bilgileri, kayıtlı cihazlar, envanter cihazları ve Active Directory eşleşmesi
- Kişiyi AD kullanıcısına atama, birimi AD organizasyon birimi (OU) listesinden güncelleme
- Aynı kişiye ait iki kaydı birleştirme; cihazı kişiden düşürüp 'sahipsiz' işaretleme
- Kişiyi yeniden başvuruya gönderme: kayıtlar arşivlenir, kullanıcı formu baştan doldurur; arşivden geri alma
- Eşleşmeyenler ekranı: ağda görülen sahipsiz cihazlar ve portal kaydı olmayan domain kullanıcıları
- Sahipsiz cihazı tek adımda kişiye bağlama veya jenerik cihaz olarak onaylama
- Envanter: hostname, MAC, IP, tür, birim, kullanıcı, domain ve uç nokta ajanı durumu
- Envanter satırından internete açma, erişimi kesme, yasaklama ve erişim profili değiştirme
- FortiGate cihaz envanteriyle tarama: IP'ler ve cihaz geçmişi güncellenir
- Envanter kayıtlarını AD kullanıcılarıyla toplu eşleştirme; önce önizleme, sonra uygulama
- Uç nokta güvenlik ajanı kurulu mu, port taramasıyla otomatik tespit edilir
- Cihaz geçmişi: cihazın ağ ve IP değişimleri tarihli olarak tutulur
- Yazıcı, kamera, IP telefon, IoT gibi form dolduramayan cihazlar için yönetici kaydı (bypass)
- Envanter CSV dışı aktarımı (UTF-8, Excel uyumlu)

Kara Liste ve Geçici Kullanıcılar 3

- MAC veya IP ile cihaz yasaklama; etiket ve gerekçe girilir, yasaklayan kayda geçer
- Yasağı kaldırma: cihaz önceden onaylıysa aynı adımda izinli gruba geri eklenir
- Geçici kullanıcı hesapları: oluşturma, açma/kapatma, şifre değiştirme, silme

Ağlar, DHCP ve IP Denetimi 12

- FortiGate'ten arayüz/VLAN ve statik rota (MPLS) ağlarının canlı keşfi, tek tıkla ağ kaydı
- L2 (VLAN, MAC görülür) ve L3 (route ile gelen, yalnız IP) ağ tipleri
- 4 adımlı ağ sihirbazı: ağ tanımı, DHCP sunucusu, portal davranışı, kural seti ve özet
- Ağa özel izin/yasak grupları ve sıralı kural seti: yasak DENY, portal erişimi, izinli ACCEPT, genel DENY
- Ağ bazında portal aç/kapat, doğrulama modu, OTP kanalı, otomatik onay ve DHCP rezervasyonu ayarı
- DHCP scope listesi: kayıtlı ağa bağlı, diğer ve scope'u olmayan ağlar; IP almış istemci sayıları
- Scope ayarlarını düzenleme: aralık, gateway, netmask, DNS, kira süresi, aç/kapat
- Scope ayrıntısında DHCP kiralari, ARP tablosu, kablosuz istemciler (SSID/AP, sinyal) ve MAC-IP rezervasyonları
- Rezervasyon zorunlu ağlarda eksik rezervasyonlar tek tıkla ve periyodik olarak tamamlanır
- IP Denetimi: bayat ve aralık dışı rezervasyonlar, korumasız adresler, klon MAC şüphesi
- Çakışmalar tek tek veya toplu düzeltilir; aktif kaydı olmayan nesne ve rezervasyon artıkları temizlenir
- Onaylı cihazın IP'si başka cihaza kiralanırsa erişim otomatik kesilir

FortiGate Politika ve Profil Yönetimi 6

- Politika listesi; aksiyon, durum ve gruba göre filtre, yalnız portal kurallarını gösterme
- Yeni politika: kaynak/hedef arayüz ve adres, servis, ACCEPT/DENY, NAT ve log seçenekleri
- Politika sıralama (yukarı/aşağı), açma/kapatma ve silme
- Erişim profilleri: FortiGate web filtresi ve uygulama kontrolü profillerine bağlı ayrı izin grupları
- Eksik izin/yasak adres gruplarını FortiGate'te tek tıkla oluşturma
- Elle Yapılacaklar: API yazma yetkisi yoksa işlem hazır CLI komutu olarak kuyruğa düşer, kopyalanır, sonra doğrulanır

Koşullu DNS ve DNS İzleme 8

- Onaysız istemcinin sorguları portal IP'sine yanıtlanır; tarayıcıya ne yazılırsa kayıt formu açılır (HTTP)
- Windows, Android ve Apple bağlantı kontrolleri yakalanır, cihazda 'ağa giriş yap' uyarısı çıkar
- Split-horizon: kurum içi alan adları ve özel ağ ters sorguları DC'ye, diğerleri genel DNS'e

- Yakalama istisnası tanımlanan alan adları onaysız istemcide de normal çözülür
- UDP ve TCP 53; yanıt önbelleği, üst DNS kesintisinde son bilinen yanıt
- DNS ayarlarının DHCP scope'larına birincil (portal) + ikincil DNS olarak tek tıkla dağıtımı
- DNS raporları: son 24 saat saatlik yoğunluk, en çok sorgulanan ve en çok engellenen 50 alan adı, en çok sorgulayan istemci
- WPAD/PAC isteklerine 'DIRECT' yanıtı: sahte vekil (WPAD kaçırma) saldırılarını önler

Güvenlik, Denetim ve Yedekleme 9

- Yönetici girişinde zorunlu iki adımlı doğrulama (TOTP, Google/Microsoft Authenticator uyumlu)
- 8 hatalı girişte IP 15 dk kilitletlenir; başarısız girişler denetime yazılır
- Parolalar PBKDF2-SHA256 (200.000 tur) ile saklanır; yönetici oturumu 8 saat
- Denetim kaydı: her işlem kişi ve zamanla SHA-256 zincirine yazılır; zincir doğrulanır, ana yönetici onarabilir
- Erişim geçmişi: başvurudan silmeye tüm olaylar; kayıt silinse bile ad, sicil, telefon, MAC, IP ile aranır
- Kişi zaman çizelgesi: kullandığı cihazlar, aldığı IP'ler, ilk/son görülme
- FortiGate yapılandırması periyodik ve elle yedeklenir; değişmeyen sürüm tekrar yazılmaz, 30 gün saklanır
- Yedekler SHA-256 özetleriyle listelenir, indirilir, önceki sürümle farkı gösterilir; şifreli alanlar maskelenir
- İstemci IP'si yalnız vekilin yazdığı başlıktan okunur; sahte IP başlıkları dikkate alınmaz

Yönetim Paneli, Ayarlar ve Entegrasyonlar 10

- Genel bakış: talep ve izin sayıları, son işlemler, CPU/RAM/disk/ağ (3 sn'de bir güncellenir)
- Uç nokta sıkılaştırma özeti: domain üyesi / domain dışı PC'ler ve ajan durumu
- Çoklu yönetici: ekleme, açma/kapatma, parola değiştirme, MFA sıfırlama, silme; son giriş zamanı
- FortiGate bağlantısı: yönetim IP'si, API token, VDOM, izin/yasak grupları; bağlantı testi
- SMS sağlayıcıları: Teknomart, Netgsm, İletim Merkezi, Sanal Santral veya özel URL şablonu; gönderici başlığı
- SMTP ile e-posta doğrulaması; SMS ve e-posta için test mesajı gönderme

- Active Directory (WinRM: NTLM, Kerberos, Basic): bilgisayar, kullanıcı, OU ve DNS kayıtları eşitlenir; varsayılan 10 dk
- Panelden SSL sertifikası yükleme (PEM/DER, anahtar eşleşmesi kontrolü); 60 sn içinde devreye girer
- Kurum adı, kısa ad, logo (PNG/JPG), KVKK ve gizlilik metinleri, OTP süresi panelden düzenlenir
- İlk kurulum ekranı: hızlı ayarlar, FortiGate bağlantı denemesi, adres gruplarını oluşturma

Kurulum ve İşletim 5

- Kurum içi Linux sunucuda Docker Compose ile çalışır; uygulama, veritabanı ve ters vekil konteynerleri
- HTTPS 443 (TLS 1.2/1.3, HTTP/2) ve HTTP 80; yerel bakım için 8088 portu; portlar ayarlanabilir
- Ayrı FortiGate captive portal kurulumu gerekmez; kullanıcılar portal adresine doğrudan girer
- Sunucu içi zamanlanmış görev: süre dolumu, hotspot oturumları, rezervasyonlar, yedek, AD eşitlemesi, ajan taraması
- En dar yetkiyle çalışabilir: yalnız adres/grup yetkisi yeterli, politika yönetimi için policy yazma yetkisi

Teknik özellikler

Ölçeklenme	Çok süreçli çalışma; web ve DNS servisi tüm işlemci çekirdeklerine dağılır
Kurulum	Docker Compose: uygulama, veritabanı ve ters vekil konteynerleri
Web / TLS	HTTPS 443, TLS 1.2/1.3, HTTP/2; SSL sertifikası panelden yüklenir
FortiGate bağlantısı	FortiOS REST API (token), VDOM desteği
OTP	6 hane, kriptografik rastgele; varsayılan 5 dk geçerlilik, en fazla 5 deneme
SMS / E-posta	Teknomart, Netgsm, İleti Merkezi, Sanal Santral veya özel URL şablonu; SMTP
Yönetici güvenliği	PBKDF2-SHA256 (200.000 tur), zorunlu TOTP, 8 hatalı denemede 15 dk kilit, 8 saatlik oturum
Koşullu DNS	UDP/TCP 53, yanıt önbellegi, kesintide son bilinen yanıt, upstream sağlık takibi
Active Directory	WinRM (5985/5986), NTLM

KURULUM VE TESLİM Kurum içinde bir Linux sunucuda Docker Compose ile çalışır. FortiGate tarafında REST API yöneticisi ve izin/yasak adres grupları tanımlanır; politika seti portal sihirbazından kurulabilir. Tüm ayarlar web panelinden yönetilir, test butonlarıyla doğrulanır.

Demo ve fiyat teklifi için

Ürünü kendi ortamınızda görmek, kapsamı ve fiyatı konuşmak için bize ulaşın.

TELEFON +90 850 441 3 441
E-POSTA bilgi@martateknoloji.com.tr
WEB martateknoloji.com.tr
ADRES Mersin Üniversitesi Teknopark İdari
Binası 35C/B5, Yenişehir, Mersin
Mersin · İzmir · Londra

© 2026 Marta Teknoloji A.Ş. — Bu broşürdeki bilgiler bilgilendirme amaçlıdır; özellik kapsamı sürüme ve kurulumu göre değişebilir.