Nornia
Akıllı İletişim Platformu — Kurumsal Kullanım Kılavuzu

v3.10.11
23 Kasım 2026

Bölüm 50: Güvenlik Kalkanı (SIP Firewall, Fail2Ban, IP Yasaklama & Dolandırıcılık Koruması)

Santralinizi internetten gelebilecek SIP şifre kırma (brute-force), yetkisiz uluslararası arama (toll-fraud), SIP tarayıcı botlar (sipvicious/friendly-scanner) ve API saldırılarına karşı 7/24 koruyan; engellenen IP adreslerini yönetip beyaz liste (Whitelist) tanımladığınız kurumsal siber güvenlik merkezidir.

BÖLÜM 50 Yönetim & Sistem Ayarları

Fail2Ban • Brute-Force • IP Whitelist • Anti-Fraud ~9 dk okuma

Güvenlik Kalkanı (SIP Firewall, Fail2Ban, IP Yasaklama & Dolandırıcılık Koruması)

Santralinizi internetten gelebilecek SIP şifre kırma (brute-force), yetkisiz uluslararası arama (toll-fraud), SIP tarayıcı botlar (sipvicious/friendly-scanner) ve API saldırılarına karşı 7/24 koruyan; engellenen IP adreslerini yönetip beyaz liste (Whitelist) tanımladığınız kurumsal siber güvenlik merkezidir.

SANTRAL MENÜ YOLU & URL

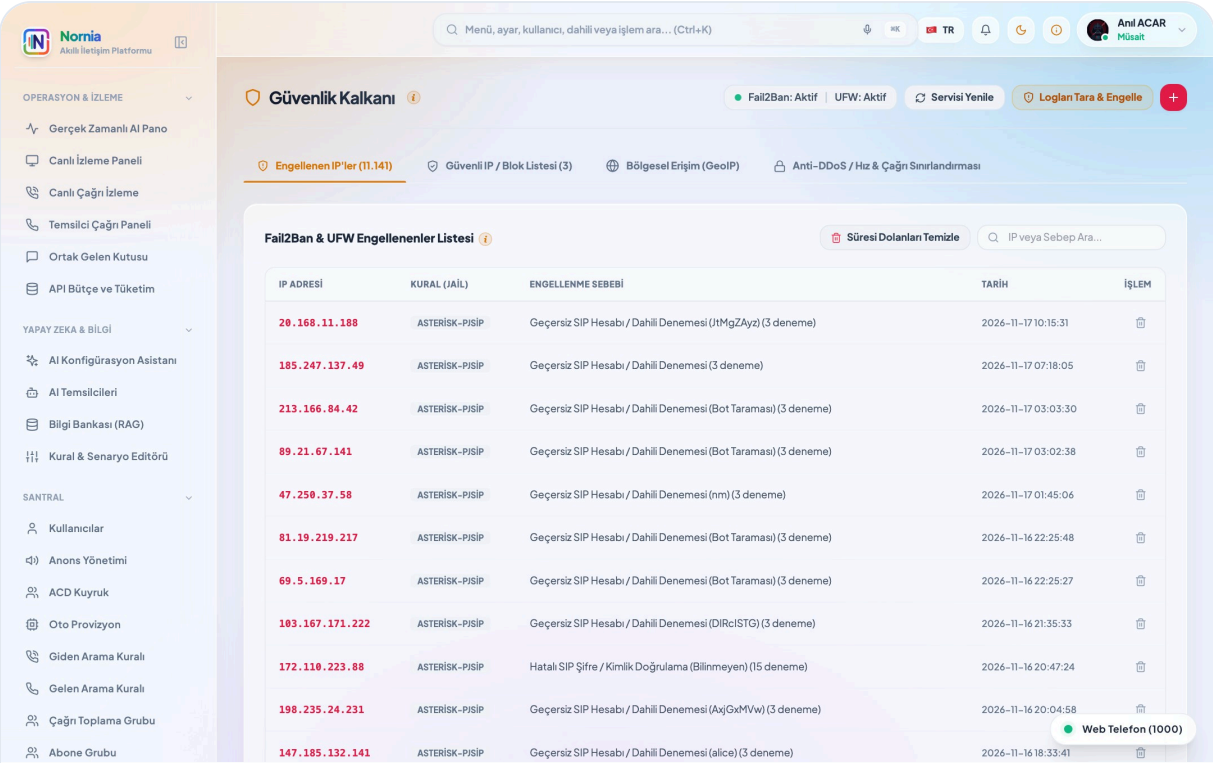
Yönetim & Ayarlar → Güvenlik Kalkanı

`/?tab=security`

GEREKLİ ROL YETKİ KODLARI (RBAC)

`security:read` `security:write` `security:delete`

CANLI SANTRAL ARAYÜZ EKRAN GÖRÜNTÜSÜ



Güvenlik Kalkanı — Engellenen saldırgan IP'ler, Beyaz Liste (Whitelist), SIP Brute-Force eşikleri ve canlı alarm akışı

`Yönetim & Ayarlar → Güvenlik Kalkanı`

Tüm Alanlar, Parametreler & Teknik Etkileri

5 parametre

ALAN / SEKME ADI	TİP / SEÇENEKLER	VARSAYILAN	DETAYLI AÇIKLAMA & SA ETKİSİ
Engellenen IP Listesi (Banned IPs)	`IPv4 + Neden + Süre + Kaldır`	`Otomatik Fail2Ban`	Kısa sürede hatalı SIP RE(API/Web girişi yapan sald anında engeller; yanlışlıkl engellenen ofis IP'si tek t açılabilir.
Güvenilir IP Beyaz Listesi (Whitelist)	`IPv4 / CIDR`	`127.0.0.1 + Yerel LAN`	Merkez ofis, şubeler ve o IP'lerini buraya ekleyerek koşulda otomatik engelle sağlarsınız.
Brute-Force & API Koruma Eşiği	`Hatalı Deneme / Dakika`	`SIP: 5 deneme | API: 25 deneme/dk`	Eşik aşıldığında IP geçici bloklanır ve Olay Günlükl SECURITY kaydı düşer.
Uluslararası Arama & Toll-Fraud Kalkanı	`Otomatik Engel`	`Aktif`	Yetkisiz yüksek tarifeli (p ülke aramalarını anında bl

ALAN / SEKME ADI	TİP / SEÇENEKLER	VARSAYILAN	DETAYLI AÇIKLAMA & SA ETKİSİ
Ülke (GeoIP) & User-Agent Filtresi	`Politika`	`sipvicious / friendly-scanner engelli`	Bilinen SIP saldırı araçları imzalarını paket seviyesin

Ekle / Düzenle & Alt Sekme Ayarları (Detaylı Referans)

Bu modülün içindeki her sekme, form alanı, anahtar (toggle) ve gizli davranışın tam teknik dökümü (1 alt bölüm).

1

Engellenen IP Yönetimi, Beyaz Liste (Whitelist) & Saldırı Koruma Politikaları

SIP & API Firewall (3 ayar)

Brute-force engelleme, güvenilir IP tanımlama ve toll-fraud kalkanı ayarları.

AYAR / ALAN	SEÇENEKLER / TİP	VARSAYILAN	NE İŞE YARAR & TEKNİK DA
Engellenen IP'ler (Banned IPs) & Engel Kaldırma	`IPv4 + Neden + Tarih + Kaldır`	`Otomatik Fail2Ban`	Yanlışlıkla engellenen bir şul IP'sini tek tıkla açabilir veya IP'yi kalıcı engelleyebilirsiniz
Güvenilir IP Beyaz Listesi (Whitelist) ZORUNLU	`IPv4 / CIDR`	`Ofis + Operatör SBC`	Beyaz listedeki IP'ler hiçbir l denemede otomatik engelle
Brute-Force Eşikleri, Toll-Fraud & Scanner Kalkanı	`SIP/API Eşik + GeoIP + User-Agent`	`Aktif`	sipvicious/friendly-scanner ve yetkisiz yüksek tarifeli ülk aramalarını otomatik bloklar

1. Üretim Santrali Güvenlik Kontrol Listesi

Santralinizi canlıya alırken şu 5 güvenlik adımını mutlaka tamamlayın:

1. Ofisinizin statik dış IP'sini ve SIP Trunk operatör SBC IP'lerini Güvenlik Kalkanı → Beyaz Liste'ye ekleyin.
2. Dışarıya port açmak yerine Nornia Connect (Sıfır-Port Bulut Köprüsü) kullanarak 5060/8000 portlarını internete tamamen kapatın.
3. Yönetici hesaplarında Sistem Ayarları / Kullanıcı Kartı üzerinden 2FA (Google Authenticator / E-Posta / WhatsApp OTP) zorunlu yapın.
4. Abone Gruplarında 'Uluslararası Arama' yetkisini yalnızca gerekli yöneticilere tanımlayın ve PIN koruması ekleyin.
5. Dış API anahtarlarında mutlaka IP Beyaz Liste (Whitelist) ve sadece gerekli en dar Scope yetkilerini kullanın.

Sık Karşılaşılan Hatalar & Sorun Giderme

Belirti: Ofisteki tüm IP telefonlar bir anda bağlantıyı kaybetti

Kök Neden: Ofis içinde şifresi yanlış girilmiş tek bir telefon arka arkaya 401 alarak ortak ofis NAT IP'sini Fail2Ban'a düşürmüş olabilir.

Çözüm: Güvenlik Kalkanı → Engellenen IP'ler listesinden ofis IP'nizin engelini kaldırın, ofis IP'nizi Beyaz Liste'ye ekleyin ve hatalı şifreli cihazı düzeltin.