

VOIP VE SIP GÜVENLİK DUVARI

Rosa SIP Firewall

Santralinizin önünde SIP saldırılarını tespit eden ve engelleyen güvenlik katmanı

Rosa SIP Firewall, IP santral ile internet arasına konumlanan ve tüm SIP trafiğini üzerinden geçiren bir güvenlik duvarıdır. SIP tarama araçlarını, şifre deneme ve kullanıcı adı taramalarını, sel saldırılarını ve bozuk mesajları tespit eder; saldırganı tehdit puanına göre otomatik ve kademeli olarak yasaklar. Riskli numaralara yönelik tele-dolandırıcılık girişimleri, ülke bazlı kısıtlama, tehdit istihbaratı beslemeleri, isteğe bağlı Suricata IDS, L3/L4 güvenlik duvarı ve SIEM entegrasyonu Türkçe web arayüzünden yönetilir.

ÖNE ÇIKANLAR

01

SIP'e özgü saldırı tespiti

SIPVicious gibi tarama araçları, REGISTER ve INVITE şifre denemeleri, dahili taraması, sel saldırıları, bozuk mesajlar ve SIP başlığında SQL enjeksiyonu her istekte denetlenir.

02

Otomatik ve kademeli yasaklama

Her kaynak IP için zamanla azalan bir tehdit puanı tutulur; eşik aşıldığında IP yasaklanır, tekrar eden saldırganların yasak süresi uzar. Trunk, ofis ve izin listesindeki adresler hiçbir zaman yasaklanmaz.

03

Tele-dolandırıcılık ve coğrafi kısıtlama

Premium ve IRSF numara örneklerini arayan ya da kısa sürede çok sayıda uluslararası arama yapan kaynak yasaklanır; SIP trafiği kaynak ülkeye göre izin veya engelleme listesiyle kısıtlanır.

04

Santral önünde tek giriş noktası

Telefonlar ve operatör hatları santrale yalnızca firewall üzerinden ulaşır; alan adı başına santral yönlendirmesi, sağlık kontrolü ve yedek santrale geçiş, NAT geçişi ve medya aktarımı birlikte gelir.

KİMLER İÇİN

Uzaktan çalışan ve şube telefonları için santralini internete açmak zorunda olan kurumlar

SIP tarama ve şifre deneme saldırılarından santralini korumak isteyen BT ekipleri

Ele geçirilmiş dahiliiler üzerinden yapılan pahalı uluslararası aramaların riskini azaltmak isteyen işletmeler

Birden çok müşteri santralini farklı SIP alan adlarıyla barındıran hizmet sağlayıcılar

VoIP güvenlik olaylarını mevcut SIEM'e aktarmak isteyen güvenlik ekipleri

Özellikler 67 ÖZELLİK

Aşağıdaki liste ürünün mevcut sürümünde çalışan özellikleri modül modül gösterir.

SIP saldırı tespiti 10

- SIPVicious, sipcli, sipsak gibi tarama araçlarının User-Agent ile tanınması ve ilk mesajda yasaklanması
- REGISTER ve INVITE şifre deneme (kaba kuvvet) tespiti
- Tek IP'den çok sayıda farklı kullanıcı adıyla deneme tespiti
- Santralden dönen 404/604 yanıtlarıyla dahili ve numara taraması tespiti
- IP başına istek yoğunluğu sınırı ile sel (flood) koruması
- Bozuk, RFC'ye aykırı ve 8 KB'ı aşan mesajların reddi
- SIP başlıklarında SQL enjeksiyonu kalıplarının engellenmesi
- Hizmet verilmeyen alan adlarına gelen isteklerin reddi
- Oturum dışı BYE/CANCEL gibi diyalog içi enjeksiyon denemelerinin tespiti
- İzin verilmeyen SIP yöntemlerinin reddi

Tehdit puanı ve yasaklama 7

- Her kaynak IP için zamanla azalan tehdit puanı; eşikte otomatik yasak
- Tekrar eden saldırganlara artan süreli yasak (5 dakika, 1 saat, 24 saat)
- Çok yüksek tehdit puanında kalıcı yasak
- Yasakların yeniden başlatmalarda korunması ve düzenli yeniden eşitlenmesi
- İzin listesi, trunk ve ofis kaynakları hiçbir zaman yasaklanmaz
- IP adresini elle engelleme veya izin verme; süreli ya da kalıcı
- IP detay sayfası: tehdit puanı, eşleşen beslemeler, son olaylar, tek tıkla engelle/kaldır

Tele-dolandırıcılık ve coğrafi kısıtlama 6

- Riskli hedef örnek tablosu: premium, IRSF, yüksek risk, uluslararası
- Hazır gelen örnek riskli örnekler; ekleme, düzenleme ve kapatma
- Premium veya IRSF numarayı arayan kaynağın anında yasaklanması
- Dakikada eşik üzeri uluslararası arama yapan kaynağın yasaklanması
- Kaynak ülkeye göre izin veya engelleme listesi

- Olayların ülke ve ASN bilgisiyle zenginleştirilmesi

Tehdit istihbaratı 5

- Spamhaus DROP/EDROP, FireHOL Level 1, blocklist.de ve VolPBL beslemeleri hazır gelir
- Besleme adreslerinin ağ katmanında (nftables) düşürülmesi
- Yönetim ağları, özel IP aralıkları ve izin listesi beslemelerden korunur
- 6 saatte bir otomatik güncelleme, elle güncelleme ve besleme bazında açma/kapama
- Saldırı geçmişinden öğrenen IP itibar puanı (ülke, ASN, ihlal sayısı)

Saldırı tespit sistemi (IDS) 5

- İsteğe bağlı Suricata ile WAN arayüzünde trafik izleme
- ET Open kuralları ve Rosa VoIP imzaları
- Özel kural ekleme ve kesintisiz yeniden yükleme
- Seçilen önem seviyesindeki uyarılarda kaynağın otomatik yasaklanması
- IDS uyarı listesi ve itibar puanına katkı

SIP proxy ve santral koruması 9

- Telefonlar ve operatör hatları santrale yalnızca firewall üzerinden ulaşır
- Birden çok SIP alan adı ve takma ad; her alan adı kendi santrale yönlendirilir
- Alan adı başına birden çok santral, öncelik sırası ve hata durumunda sıradaki santrale geçiş
- Santrallerin OPTIONS ile 10 saniyede bir sağlık kontrolü
- Operatör hatları için güvenilir kaynak tanımı ve ayrı santral portu
- Uzak telefonlar için NAT geçişi; santral kayıt sunucusu olarak kalır
- rtpengine ile medya aktarımı; destekleyen çekirdekte çekirdek içi aktarım
- Santral kimliğini gizleme: Server/User-Agent maskelenir, iç başlıklar dışarıdan kabul edilmez
- Güvenlik servisi veya veritabanı dursa da SIP trafiği son bilinen güvenlik durumuyla sürer

Ağ ve güvenlik duvarı 8

- Arayüz rolleri: WAN, LAN, DMZ, yönetim
- VLAN (802.1Q) ve PPPoE; statik veya DHCP adresleme, statik rota ve DNS
- Canlı arayüz durumu: bağlantı, hız, MAC adresi, trafik
- Sıralı L3/L4 kuralları: izin ver, düşür, reddet; arayüz, protokol, port ve günlükleme
- Nesne grupları: host, ağ, port, port aralığı
- NAT: port yönlendirme (DNAT), SNAT, masquerade
- Ağ ve kural değişikliklerinde onayla ya da geri al; onaylanmayan değişiklik otomatik geri alınır
- SSH ve yönetim arayüzüne yalnızca tanımlı yönetim ağlarından erişim

İzleme, anomali ve raporlama 5

- Gösterge paneli: son 24 saatte engellenen saldırı, aktif yasak, olay sayısı ve saldırı türü dağılımı
- Güvenlik olayları: saldırı türü ve kaynak IP'ye göre filtreleme
- Saat-hafta taban çizgisine göre olay hacmi anomalisi, genel ve alan adı bazında
- Anomaliyi onaylama, çözüldü veya yanlış alarm olarak işaretleme
- Olaylar, IDS uyarıları ve engelleme listesinin CSV dışa aktarımı (24 saat, 7 gün, 30 gün)

Bildirim ve SIEM entegrasyonu 4

- Syslog (RFC 5424) veya CEF biçiminde UDP/TCP üzerinden SIEM'e iletim
- E-posta (SMTP), Telegram ve webhook bildirim kanalları
- Hedef ve kanal başına asgari önem seviyesi
- Test mesajı gönderme ve kanal durum göstergesi

Yönetim ve kurulum 8

- HTTPS üzerinden Türkçe web arayüzü
- Yönetici, operatör ve izleyici rolleri
- argon2id ile parola saklama; 5 hatalı girişte 15 dakika hesap kilidi; oturum zaman aşımı
- İsteğe bağlı Let's Encrypt sertifikası
- Debian 12/13 için kurulum betiği
- Güncellemede otomatik veritabanı yedeği; sağlıklısız sürümde önceki sürüme dönüş
- Yapılandırma ve veritabanı yedekleme/geri yükleme betiği
- Yönetici parolası sıfırlama komutu

Teknik özellikler

Konumlandırma	Santral ile internet arasında SIP proxy; tek bacaklı (tek arayüz) veya iki bacaklı (ayrı santral arayüzü) kurulum; 1:1 NAT arkasında genel IP tanımı
SIP taşıma	SIP over UDP ve TCP (varsayılan 5060)
Santral uyumluluğu	Standart SIP santraller; arayüzde FreeSWITCH, Asterisk, Yeastar, Cisco CUCM ve genel tür seçimi. Santral kayıt sunucusu olarak kalır; trunk trafiği ayrı santral portuna yönlendirilebilir
Medya	Tüm çağrılarda rtpengine ile RTP aktarımı; varsayılan port aralığı 20000-39999; destekleyen çekirdekte çekirdek içi aktarım
Tehdit istihbaratı	Spamhaus DROP/EDROP, FireHOL Level 1, blocklist.de, VoIPBL; 6 saatte bir güncelleme; DB-IP Lite ülke ve ASN veritabanı
Saldırı tespit sistemi	İsteğe bağlı Suricata (izleme modu, WAN arayüzü); ET Open kuralları, Rosa VoIP imzaları ve özel kurallar; seçilen önem seviyesinde otomatik yasak
Entegrasyonlar	SIEM: syslog RFC 5424 veya CEF, UDP/TCP; bildirim: e-posta (SMTP), Telegram, webhook; CSV raporlar
Kimlik doğrulama ve yetki	Kullanıcı adı/şifre (argon2id), 5 hatalı girişte 15 dakika kilit, oturum zaman aşımı; yönetici, operatör ve izleyici rolleri
Gereksinimler	Debian 12 veya 13 (amd64/arm64); fiziksel, sanal veya bulut sunucu; asgari 2 vCPU / 4 GB RAM, üretimde 4 vCPU / 8 GB önerilir
Arayüz	HTTPS üzerinden Türkçe web arayüzü; yalnızca tanımlı yönetim ağlarından erişim; isteğe bağlı Let's Encrypt sertifikası

KURULUM VE TESLİM

Debian 12 veya 13 sunucuya (fiziksel, sanal makine veya bulut sunucu) kurulum betiğiyle kurulur; SIP proxy, medya aktarımı, güvenlik motoru ve web arayüzü aynı sunucuda çalışır. Telefonlar ve operatör hatları firewall'a yönlendirilir, santral yalnızca firewall'dan SIP ve RTP kabul edecek şekilde kısıtlanır. Güncelleme betiği öncesinde veritabanı yedeği alır ve yeni sürüm sağlıklı açılmazsa önceki sürüme döner.

Demo ve fiyat teklifi için

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

TELEFON +90 850 441 3 441
+90 324 350 03 50

E-POSTA bilgi@martateknoloji.com.tr

WEB martateknoloji.com.tr

ADRES Mersin Teknopark 35C/B5, Çiftlikköy,
33343 Yenişehir / Mersin
Mersin · İzmir · Londra

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