WoraLOG 5651 Log Toplama

Kurulum ve Entegrasyon Kılavuzu

Sürüm 0.1.0-preview (pilot) · Worasoft · worasoft.com

Bu bir pilot (önizleme) sürümdür

Şu an saha doğrulaması tamamlanmış tek firewall **Sophos SFOS 22.x**'tir. pfSense, OPNsense, FortiGate, Palo Alto gibi diğer markalar doğrulama aşamasındadır; bunlardan birini kullanıyorsanız kurulumdan önce Worasoft ile görüşün. Mevzuat uygunluk belgesi ya da zaman damgası hizmeti bu sürümün kapsamında değildir.

1. WoraLOG nedir?

WoraLOG, firewall'unuzun loglarını toplayıp **sizin kendi sunucunuzda** (Hyper-V, VMware veya Proxmox üzerinde çalışan bir sanal makinede) saklı ve şifreli tutan bir log toplama cihazıdır. Firewall logları bu cihaza TLS ile gelir; **log içeriği Worasoft sunucularına gitmez**. Worasoft yalnızca cihazın ayakta olup olmadığını ve sağlık durumunu uzaktan izler (log içeriğini değil).

- Ham log, ayrıştırılmadan AES-256-GCM ile şifrelenir; her kayıt bir SHA-256 zincirine bağlanır ve cihazın kendi anahtarıyla imzalanır.
- **Yerel mod:** kayıtlar yalnızca sizde kalır (ilk sürümde varsayılan budur).
- **Hibrit mod:** aynı şifreli kayıtlar merkeze de kopyalanır — ilk sürümde kapalıdır, çözme anahtarı merkezde tutulmaz.

2. Gereksinimler

Sanallaştırma	Hyper-V, VMware (ESXi/Workstation) veya Proxmox VE
Kaynak (öneri)	2 vCPU, 4 GB RAM, 40 GB+ disk (log hacmine göre artırın)
Ağ	Cihaza sabit bir IP önerilir; firewall ile aynı ağda erişilebilir olmalı
Firewall erişimi	Firewall → WoraLOG cihazı: TCP 6514 (TLS) açık olmalı
Firewall CA	Firewall'un açık CA sertifikası (istemci sertifikası doğrulaması için; özel anahtar istenmez)
SSH anahtarı	Uzaktan yönetim için kendi açık SSH anahtarınız

Platform notu: Hyper-V / VMware / Proxmox gerçek platform kabul testleri pilot sürümde sürmektedir. Kurulum öncesi güncel durum için Worasoft ile görüşün.

3. Kurulum adımları (konsol sihirbazı)

1. **İmajı indirin.** WoraLOG imaj paketini platformunuza göre indirin (Hyper-V ZIP, VMware OVA veya Proxmox ZIP) ve SHA-256 özetini doğrulayın.
2. **Sanal makineye aktarın.** Hyper-V'de Generation 2 / UEFI, VMware'de OVA (EFI), Proxmox'ta QCOW2. **VM adını "WoraLOG"** verin. Ağ kartını firewall ve yönetim bilgisayarınızın eriştiği ağa bağlayın (varsayılan DHCP; ev modemini değiştirmeniz gerekmez).

3. **İlk açılış — konsol.** VM'i başlatın; konsoldaki ilk kurulum ekranında **cihaz adı (hostname)** ve **bu cihaza özel bir yönetici parolası** belirleyin. Paylaşılan/ortak parola yoktur; parola yalnız konsol ve sudo içindir (SSH parola girişi kapalı).
4. **SSH anahtarınız.** Uzaktan yönetim için kendi **açık SSH anahtarınızı** girin. Özel anahtarı cihaza koymayın.
5. **Firewall bilgileri.** İzin verilen **firewall IP** adreslerini ve firewall'un **açık CA sertifikasını** girin. Cihaz yalnız bu kaynaklardan ve TLS istemci sertifikasıyla log kabul eder; rastgele kaynaklar reddedilir.
6. **Mod ve IP. "local"** modu seçin (kayıtlar yalnız sizde kalır; merkezi aktarım/hybrid ilk sürümde kapalıdır). DHCP rezervasyonu ya da sabit IP tanımlayın. Konsol, alıcı TLS sertifikasının SHA-256 parmak izini gösterir.

> **Önemli: kod yok, her cihaz kendi anahtarını üretir**
>
> WoraLOG genel imajında ortak parola, ortak anahtar ya da girilecek bir "kurulum kodu" **yoktur**. Her kurulum kendi cihaz UUID'sini, SSH host, TLS, AES ve Ed25519 anahtarlarını **kendisi üretir**. Yönetim paneli yalnız loopback'tedir; SSH tüneliyle erişilir. (Dilerseniz Worasoft, ağ/firewall bilgilerini gömülü bir kurulum ISO'su ile hazır da verebilir.)

4. Sophos Firewall entegrasyonu (doğrulanmış)

Sophos Firewall (SFOS 22.x) yönetim arayüzünde:

1. **System → System services → Log settings → Syslog servers → Add** yolunu açın.
2. **Name:** WoraLOG (ya da dilediğiniz bir ad).
3. **IP Address / Port:** WoraLOG cihazının IP'si, port **6514**.
4. **Transport / Secure connection:** TLS ile güvenli bağlantı seçin ve firewall'un istemci sertifikasını (CA) kullanın. Şifresiz UDP/TCP önerilmez.
5. **Log kategorileri:** ihtiyacınıza göre seçin (Firewall, Content Filtering, System Health, Event vb.).
6. WoraLOG tarafında **izinli kaynak IP** olarak Sophos'un IP'sini ekleyin (allowlist). Yalnızca izinli kaynaklardan log kabul edilir.

Doğrulama: kısa bir süre sonra panelinizde cihaz durumu **"Çalışıyor / Log alınıyor"** olmalıdır. Sophos resmi yardım: docs.sophos.com → Sophos Firewall 22.0 → Syslog server add.

5. Diğer firewall'lar

pfSense, OPNsense, FortiGate, Palo Alto, SonicWall, WatchGuard gibi cihazlar **şu an doğrulama aşamasındadır** ve bu pilot sürümde desteklendiği beyan edilmez. Bu markalardan birini kullanıyorsanız, syslog hedefini (TLS 6514) ve sertifika yapılandırmasını birlikte kurmak için kurulum öncesi Worasoft ile iletişime geçin.

6. Lisans ve yenileme

Cihazınız, satın aldığınız lisans süresi (ay veya yıl) boyunca çalışır. Lisans bitiminde bir **ek süre** tanınır; bu sürede cihaz çalışmaya devam eder ve uyarı verir. Ek süre de dolunca **yeni log alımı durur** — ancak eski kayıtlarınıza erişim her zaman açık kalır. Kalan sürenizi ve kaynak limitinizi müşteri panelinizde **"Aboneliğim"** ekranında görürsünüz. Yenileme için Worasoft'a başvurun; yenilemede süre otomatik uzar.

7. Doğrulama ve destek

- Cihaz panelde yeşil / “Çalışıyor” görünüyor mu?
- Firewall tarafında syslog hedefi doğru IP ve 6514/TLS ile tanımlı mı?
- WoraLOG izinli kaynak listesinde firewall IP'si var mı?
- “Cihaz çalışıyor” ile “log akıyor” ayrı bilgilerdir; panelde ikisini de kontrol edin.

Kurulum desteği: panelinizdeki iletişim kanalları ya da Worasoft üzerinden.

Kapsam ve doğrulama notları

Bu kılavuz pilot (0.1.0-preview) sürüm içindir. “5651 uyumlu” ifadesi ve zaman damgası (Kamu SM) doğrulaması bu sürümde beyan edilmez (zaman damgası durumu “bekliyor”dur). Saha doğrulaması tamamlanan tek firewall Sophos SFOS 22.x'tir. Kapsam genişledikçe bu kılavuz güncellenecektir.