

SAHAB

SANAL HAVA BOŞLUĞU



Aselsan Sanal Hava Boşluğu (SAHAB), "Görev Kritik" işlemlerin gerçekleştirilmesi amacıyla farklı güvenlik seviyesine sahip ağların birbirleriyle güvenli bilgi alışverişini sağlayan Ortak Kriterler EAL4+ güvenlik seviyesinde onaylı bir sistem çözümdür.

SAHAB, gerçek zamanlı hizmet alan/veren kuruluşlar için gündemde olan siber güvenlik tehditlerine karşı durmak ve onları ortadan kaldırmak amacıyla tasarlanmıştır.



SAHAB

SANAL HAVA BOŞLUĞU

ASELSAN SAHAB sistemi Linux sistemi üzerine kurulu iç ve dış sunucularla çalışır ve bilgi akışını harici güvenlik aygıtlarıyla yönetir.

ASELSAN SAHAB sistemi dış ağ ile gizli ağ arasına yerleştirilir ve iç bağlantı için IP tabanlı haberleşmeyi kullanmaz. Bu sayede isminden de anlaşılabilir gibi "sanal hava boşluğu" yüksek güvenlikle oluşturulur. Düzenli çalışması için SAHAB birçok çevresel bileşenler korunur. Her bir sunucuda bulunan bu bileşenler firewall (FW), network tabanlı sızıntı algılama sistemi (NIDS), protokol filtreleme ve sunucu tabanlı sızıntı algılama sistemi (HDIS) içerirler.

SAHAB üzerindeki veri akışı iki yönlüdür; dış ağdan iç ağa vb. Dış ağdaki istek/cevaplar dış sunucu tarafından alınır. Bu istek/cevaplar, dış sunucunun kontrolü altında uygulama tabanına geçer. Filtrelenen ve kontrol edilen istek/cevaplar şifreleme ve dijital imzalamaya sonucunda paylaşılan disklere iletilir. İç sunucu bu istek/cevapları paylaşılan diskten şifre çözümü ve imza doğrulama sonunda alır. Eğer herhangi bir sorun görülmezse istek/cevaplar kayıt edilir ve iç sunucudaki kendi uygulamasına iletilir. Aynı bilgi akışı iç ağdan dış ağa doğru olan bağlantılar için de geçerlidir.

SAHAB sunucuları arasındaki haberleşme şifreli ve imzalıdır.

Sanal Hava Boşluğu Sistemi

- İç ve dış ağ sunucuları üzerinde çalışır
- Sunucular arasında "Sanal Hava Boşluğu" sınırı oluşturur.
- İki yönlü veri akışı 40Mbit/s bant genişliğinde sağlanır.
- Paralel iletişim sırasındaki gecikme 4.5ms.
- İstekler/Yanıtlar iç ve dış sunucularda filtrelenir.
- Paylaşılan disk ünitesi üzerinden şifreli ve imzalı haberleşme yapılır.

Yazılım ve Güvenlik Bileşenleri

- Özelleştirilmiş Linux işletim sistemi
- Dahili Güvenlik Duvarı
- Dahili Saldırı Önleme Sistemi
- Sistem Bütünlük Kontrolü:
- İmzalı kodlar
- Şaşırtma
- Mesaj Şifreleme Algoritmaları
- Özelleştirilmiş Disk Biçimleme Yöntemi
- Audit/Log Yazılımı
- Harici Uygulama Seviyesi Güvenlik Duvarı
- Harici Ağ Güvenlik Duvarı ve Saldırı Önleme Sistemi

Donanım Özellikleri

SAHAB, Fault Tolerant Sunucu, Rack Tipi Sunucu ve Rack Tipi İş İstasyonu olmak üzere üç farklı donanım seçeneği üzerinde çalışmaktadır.

