

# Intrusion Prevention System

**Autoren:** Morris Tichy, Lukas Freundesprung

## Inhaltsverzeichnis

1. Theorie .....	2
2. Konfiguration .....	2
3. Test .....	2

## 1. Theorie

Ein Intrusion Prevention System (IPS) ist eine Technologie, die den unautorisierten Zugriff auf ein Netzwerk verhindert. IPS-Systeme überwachen den Datenverkehr und blockieren oder alarmieren, wenn sie verdächtige Aktivitäten erkennen. IPS-Systeme können auf verschiedenen Ebenen des OSI-Modells arbeiten, um Daten zu schützen. IPS-Systeme können auf der Anwendungsschicht arbeiten, um Daten in E-Mails oder Webseiten zu schützen.

## 2. Konfiguration

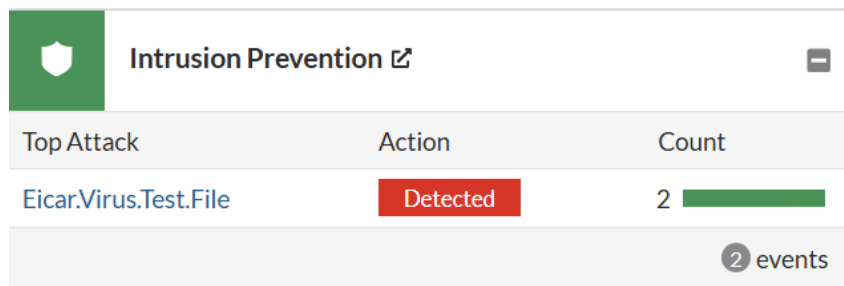
In der FortiGate GUI wird unter **Security Profiles > Intrusion Prevention** ein neues IPS-Profil erstellt. In diesem Profil werden Regeln definiert, die den Datenverkehr überwachen und blockieren oder alarmieren, wenn verdächtige Aktivitäten erkannt werden. Es wird dabei eine Signatur erstellt.

Dieses Profil wird dann anschließend der Firewall Policy zugewiesen, um den Datenverkehr zu überwachen.

## 3. Test

Um die Funktionalität des IPS zu testen, kann ein Angriff simuliert werden. Dazu kann eine Angriffssignatur in das Profil eingefügt werden.

Unter **Logs & Reports > System Events** werden die Events von IPS angezeigt.



Intrusion Prevention		
Top Attack	Action	Count
Eicar.Virus.Test.File	Detected	2

2 events

Abbildung 1: System Events