ARP GUARD by ISL

ADD-ON

ARP-GUARD Layer 2 IPS

SecurITy made in Germany

Trust Seal www.teletrust.de/itsmig

Schutz vor internen Angriffen

Die unsichtbare Gefahr

Die meisten IT-Sicherheitskonzepte sind darauf ausgelegt, die Unternehmen vor externen Bedrohungen zu schützen. Dementsprechend gibt es ein breites Spektrum an verschiedenen Sicherheitslösungen gegen Viren und Hackerangriffe.

Oft werden dabei die internen Kommunikationswege vernachlässigt. Doch gerade interne Netzwerkangriffe besitzen ein hohes Gefährdungspotential, weil diese oft unentdeckt bleiben. Durch Manipulationen der IP-basierten Kommunikation können Adressen von Netzwerkkomponenten verändert, Adresseinträge manipuliert und damit Systeme lahmgelegt oder Datenströme abgegriffen werden.

Sichere Kommunikation gewährleisten

Das ARP-GUARD Layer 2 Intrusion Prevention System (IPS) schützt Ihr Netzwerk vor internen Angriffen und verbessert die Sicherheit Ihrer internen Kommunikation signifikant.

Dank der Echtzeitüberwachungsfunktion wird der Datenverkehr in Ihrem Netzwerk kontinuierlich kontrolliert und verdächtige Aktivitäten sofort erkannt.

Unsere Lösung bietet dabei nicht nur die Erkennung von Angriffen, sondern auch die automatisierte Abwehr. Ein individuell definierbares Regelwerk ermöglicht es, verdächtigen Datenverkehr oder infizierte Geräte sofort zu blockieren. Diese Sicherheitsrichtlinien sind jederzeit anpassbar, um den jeweiligen Sicherheitsanforderungen Ihres Netzwerkes gerecht zu werden.

Mit den integrierten Reporting-Funktionen erhalten Sie detaillierte Berichte über erkannte Angriffe und Sicherheitsvorfälle. Sie haben die Möglichkeit, Statistiken zur Netzwerkauslastung und -sicherheit zu generieren und diese für weitere Analysen zu exportieren.

Das ARP-GUARD Layer 2 IPS lässt sich nahtlos in Ihre bestehende Netzwerkinfrastruktur integrieren. Es ist kompatibel mit allen gängigen Layer 2 Switches & Routern und schützt Ihre Geräte in LAN- als auch WLAN-Umgebungen. Die Konfiguration erfolgt über eine benutzerfreundliche Web-Oberfläche oder CLI.

Ein kosteneffizienter Ansatz
Die Verwendung des Simple Network Management Protokolls (SNMP) ermöglicht eine kostengünstige Umsetzung, da SNMP in fast allen Netzwerken und nahezu allen Infrastrukturkomponenten (Switches, Router) verfügbar ist. Das ARP-GUARD Layer 2 IPS kann somit flächendeckend zur Überwachung der Netzwerkports genutzt werden. Adressmanipulationen werden erkannt und Angreifer vom Netzwerk isoliert.

Ein Redesign des Unternehmensnetzwerks oder die Anschaffung neuer Hardware ist nicht erforderlich. Der Implementierungsaufwand und der Wartungsaufwand sind gering, so dass die Kosten unseres Lösungsansatzes deutlich unterhalb der herkömmlicher Lösungsstrategien für interne Netzwerksicherheit angesetzt werden können.

ARP-GUARD unterstützt Netzwerke jeder Größe und kann bei Bedarf beliebig skaliert werden. Schützen Sie Ihr Netzwerk vor Layer 2 Angriffen und sorgen Sie für eine sichere und zuverlässige Kommunikation.

LAYER 2 IPS AUF EINEN BLICK

Schutz vor Layer 2 Angriffen durch

- ✓ ARP-Spoofing
- ✓ DoS- und DDoS-Attacken
- ✓ MAC-Flooding
- ✓ IP-Spoofing, IP- und MAC-Adresskonflikten

Echtzeitüberwachung des Netzwerkverkehrs:

- ✓ Kontinuierliche Überwachung des Datenverkehrs auf Layer 2
- ✓ Erkennung und Meldung vedächtiger Aktivitäten und potenzieller Angriffe in Echtzeit

Automatische Reaktion auf Angriffe:

- ✓ Automatische Isolierung verdächtiger Geräte und Unterbindung von verdächtigem Datenverkehr
- ✓ Flexible Anpassung der Netzwerkkonfiguration zur Abwehr von Angriffen

Integrierte Reporting-Funktionen:

- ✓ Generierung detaillierter Berichte über erkannte Angriffe und Sicherheitsvorfälle
- ✓ Statistiken zur Netzwerkauslastung und -sicherheit
- ✓ Exportmöglichkeit der Berichte für weitere Analysen

Integration in bestehende Netzwerkinfrastrukturen:

- ✓ Kompatibel mit gängigen Layer 2 Switches und Routern