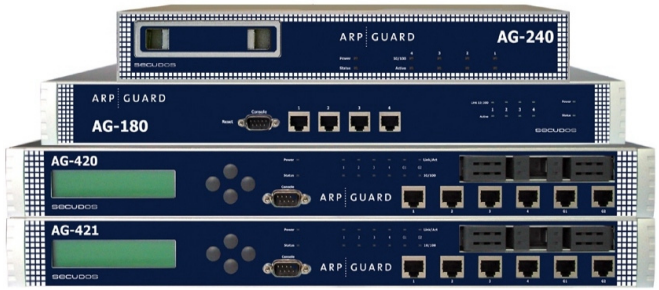
ARP GUARD

ARP GUARD

Die ARP-Guard Box

ARP-Guard ist selbstverständlich auch als „Plug and Play“ Lösung erhältlich. Gemeinsam mit unserem Appliance-Partner, der SECUDOS GmbH, haben wir die ARP-Guard Box entwickelt. Die **ARP-Guard Box** wird mit vorinstallierter Software ausgeliefert und macht Installationsarbeiten überflüssig.
Die Hardware und das von SECUDOS entwickelte DOMOS-Betriebssystem sind speziell auf die ARP-Guard Software abgestimmt. Die gesamte Konfiguration erfolgt über eine grafische Oberfläche und ermöglicht die Inbetriebnahme innerhalb von 10-15 Minuten.
Für die **ARP-Guard Box** kann ein Wartungsvertrag abgeschlossen werden, damit im Falle eines Defekts kurzfristig ein Ersatzgerät bereitgestellt werden kann.



ARP-Guard ist alternativ auch als reines Software-Produkt für die Betriebssysteme Linux (Red Hat und SUSE) und Windows (nur Sensor) verfügbar.

Weitere Informationen

Weitere Informationen erhalten Sie von 3MFuture
http://www.3mfuture.com/network_security/arp-guard-arp-spoofing.htm

3M FUTURE

Professor Dr. Wolfram Reiners

info@3mfuture.com
Phone +49 7531 9166 00
www.3mfuture.com
http://www.3mfuture.com/contact/contact-3mfuture.htm

	AG-180	AG-240	AG-240-e	AG-420	AG-421
CPU	VIA Samuel C3	VIA 1 GHZ	VIA 1 GHZ	Intel Pentium 4	Intel Pentium 4
Memory	256 MB	512 MB	512 MB	512 MB	1024 MB
HDD	40 GB	40 GB	40 GB	40 GB	40 GB
Ports	4x 10/100	4x 10/100	4x 10/100	4x 10/100	4x 10/100
Gigabit Ports	-	-	1x 10/100/1000	2x 10/100/1000	2x 10/100/1000
Gehäuse	Tisch / Rack	Tisch / Rack	Tisch / Rack	Rack	Rack
Zertifikate	CE, FCC Class A	CE, FCC Class B	CE, FCC Class B	CE, FCC Class A	CE, FCC Class A
LAN-Sensor	Max. 100 Geräte	Max. 100 Geräte	Max. 200 Geräte	Max. 350 Geräte	Max. 500 Geräte
SNMP-Sensor	Max. 1000 Geräte	Max. 2000 Geräte	Max. 2000 Geräte	Max. 5000 Geräte	Max. 10 000 Geräte

SCHUTZ VOR INTERNEN ANGRIFFEN UND FREMDEN GERÄTEN

ARP GUARD

Die Bedrohung

Laut Statistik kommen 70-80% aller Sicherheitsverletzungen von innen! Trotzdem sind die internen Bereiche der meisten IT-Netzwerke häufig ungeschützt. Dabei bieten interne Angriffe aufgrund des direkten Zugriffs auf das LAN ein weitaus höheres Bedrohungspotential als Attacken von außen.

Jeder, der Zugang zu Ihrem Netzwerk hat, kann z.B. ARP-Angriffe ausführen, ohne zu riskieren, dass dies bekannt wird!

Selbst bei wirksamer Absicherung aller Dienste und Applikationen sind meist die tieferliegenden Kommunikationsschichten angreifbar, beispielsweise über ARP-Angriffe. Im Internet frei verfügbare Hackertools versetzten einen Angreifer in die Lage, als man-in-the-middle in jegliche Kommunikation einzudringen, um Daten abzuhören, Passworte zu sammeln und Daten zu manipulieren. Auch verschlüsselte Verbindungen sind vor solchen Angriffen nicht sicher.

Jeder, der Zugang zu Ihrem Firmengelände hat, kann unbemerkt ein unautorisiertes Gerät in das Netzwerk einbringen!

Wie verhindern Sie, dass Besucher oder Mitarbeiter gegen die Sicherheitspolicy eigene Notebooks, PDAs oder drahtlose Netzwerkhardware an das LAN anschließen?

Bereits ein einziges unautorisiertes Gerät kann in einem Unternehmensnetz Tür und Tor für fatale Sicherheitsrisiken öffnen:

- Verbreitung von Viren, Würmern und Trojanern
- Wirtschaftsspionage
- Sabotage und Schädigung des Unternehmens

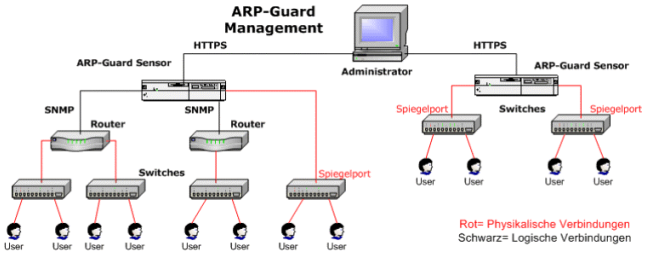
Die ARP-Guard Lösung

ARP-Guard ist die innovative Lösung zum Schutz vor internen Angriffen und fremden Geräten. Damit kann erstmals eine Sicherheitslücke geschlossen werden, die konventionelle Sicherheitssysteme wie Firewalls oder Intrusion Detection / Intrusion Prevention Systeme nicht abdecken. Der Einsatz von **ARP-Guard** sorgt für Sicherheit in Ihrem Netzwerk und bietet darüber hinaus ein leistungsstarkes Werkzeug zur Qualitätssicherung. ARP-Guard fungiert als Beobachter und greift nicht in interne Applikationen ein, sondern reagiert nur im konkreten Angriffsfall.

ARP GUARD

Vorteile

- ARP-Guard lässt sich problemlos in bestehende IT-Sicherheitsumgebungen (Firewalls, Virenscanner, Intrusion Detection Systeme) einbinden.
- ARP-Guard arbeitet hersteller- und plattformunabhängig mit allen gängigen Routern und programmierbaren Switches (Cisco Systems, Hewlett-Packard, 3Com, Nortel Networks, Lucent Technologies, Extreme Networks etc.).
- Bereits vorhandene Infrastruktur kann genutzt werden, Investitionen in neue Endgeräte sind nicht erforderlich.
- ARP-Guard ist beliebig skalierbar und zeichnet sich durch einen geringen Konfigurationsaufwand aus.
- ARP-Guard beeinträchtigt weder die Netzwerkperformance noch interne Applikationen.
- Die Alarmierung erfolgt flexibel per Email, SNMP Trap, SMS, Syslog oder benutzerdefiniertem Skript.



Module

Jedes Unternehmen hat individuelle Sicherheitsanforderungen. Das ARP-Guard System ist in verschieden Modulen erhältlich und damit optimal an die unterschiedlichen Bedürfnisse anzupassen. Die Lizenzierung erfolgt abhängig von der Anzahl der zu schützenden Geräte (MAC-Adressen).

ARP-Guard Access

Erkennung, Lokalisierung und Abwehr fremder Geräte und Zugriffskontrolle im LAN

- Das ARP-Guard System meldet unverzüglich unautorisierte Notebooks, WLAN Devices etc., die an das Netzwerk angeschlossen werden, und leitet bei entsprechender Konfiguration automatisch Gegenmaßnahmen ein.

ARP GUARD

- Mit ARP-Guard Access lässt sich eine zuverlässige Zugriffskontrolle im LAN durch eine komfortable, zentral administrierbare Port-Security einfach realisieren.
- Das integrierte Adressmanagement bietet eine umfassende Übersicht über das Netzwerk.
- Alle verwendeten Adressen und Zuordnungen werden vollständig dargestellt.
- Änderungen werden protokolliert und lassen sich zurückverfolgen.
- Mit der Lokalisierung von MAC-Adressen steht ein elegantes Tool zum Auffinden von Endgeräten selbst in größeren Umgebungen zur Verfügung.
- Bestandlisten können leicht auf dem neuesten Stand gehalten werden.

ARP-Guard Defend

Erkennung, Lokalisierung und Abwehr interner Angriffe

- Die Erkennung, Lokalisierung und Abwehr von ARP-Spoofing und MAC-Flooding verhindert Denial of Service-Angriffe sowie das Abhören und/oder Manipulieren von Daten.
- Geheime Produktentwicklungen und firmeninterne Passworte sind vor unerwünschtem Zugriff gesichert.
- Die Erkennung, Lokalisierung und Abwehr von IP-Spoofing verhindert die Erschleichung besonderer Rechte im Netzwerk.
- Durch die zuverlässige Erkennung, Lokalisierung und Abwehr von Adresskonflikten leistet ARP-Guard einen wesentlichen Beitrag zur Qualitätssicherung in Ihrem Netzwerk.
- Adressänderungen werden protokolliert und lassen sich zurückverfolgen.
- Auch präventiver Schutz gegen interne Angriffe lässt sich mit ARP-Guard Defend leicht verwirklichen.

ARP-Guard Premium

Erkennung, Lokalisierung und Abwehr interner Angriffe und fremder Geräte

ARP-Guard Premium vereint die Funktionen von ARP-Guard Access und ARP-Guard Defend und bietet einen kompletten Schutz vor internen Angriffen und dem Anschluss unerwünschter Geräte.