

FAQ - OFT GESTELLTE FRAGEN

Frage 1: Was ist ARP?

ARP (Address Resolution Protocol, RFC 826) ist ein Protokoll, das eine Zuordnung zwischen physikalischen Adressen und Protokolladressen herstellt. Dadurch wird die Kommunikation in lokalen Netzen oft überhaupt erst ermöglicht.

In lokalen Netzen wird in der Regel anhand der (physikalischen) Hardware-Adresse der Netzwerkkarte (MAC-Adresse) adressiert. Diese Adresse ist weltweit einmalig und in der Netzwerkkarte verankert. In IP-Netzen wird jedoch die IP-Adresse zur Kommunikation verwendet. Sobald IP in lokalen Netzen eingesetzt wird, stellt ARP eine Zuordnung zwischen physikalischen Adressen und IP-Adressen her.

Frage 2: Wie funktioniert ARP?

Wenn ein Absender ein Paket an einen Empfänger im lokalen Netz schicken möchte, kennt er oft nur dessen IP-Adresse. Um die entsprechende MAC-Adresse, die er zur Kommunikation im lokalen Netz benötigt, festzustellen, kann er eine ARP-Anfrage mit seinen Adressdaten und der IP-Adresse des Empfängers an alle Stationen im lokalen Netz senden.

Der Empfänger antwortet auf diese Anfrage mit einem Paket, in dem er dem Sender seine Adressdaten mitteilt.

Um nicht bei jedem Paket solche Anfragen durchführen zu müssen, werden die Adressdaten in einem Zwischenspeicher (ARP-Cache, ARP-Tabelle) gespeichert.

Frage 3: Was ist ARP-Spoofing? Was ist ARP-Poisoning?

ARP-Spoofing ist das Versenden von gefälschten ARP-Paketen. Oft wird ARP-Spoofing eingesetzt, um gezielt die ARP-Tabellen anderer Systeme zu manipulieren. Dies wird als 'ARP-Poisoning' bezeichnet.

Frage 4: Was ist ein man-in-the-middle?

Im Internet frei verfügbare Software-Tools zum sogenannten **ARP-Poisoning** ermöglichen auch einem weniger versierten Angreifer von einem Rechner innerhalb eines Netzsegmentes das **ARP-Protokoll** so auszunutzen, dass mit diesem Rechner die gesamte Kommunikation eines anderen Rechners protokolliert und am Bildschirm dargestellt wird, man spricht auch vom **man-in-the-middle Angriff**.

Ein man-in-the-middle kann die folgenden Angriffe ausführen:

- Blockierung eines Rechners oder eines kompletten Netzsegments
- Abhören der Kommunikation eines Rechners
- Sammeln von Passwörtern
- Manipulation von Daten

Damit sind internen Angreifern alle Türen geöffnet zum Ausspähen von interessanten Informationen (Konstruktionspläne, Projektverlauf, Buchhaltung, Personal- und Finanzinformationen) bis hin zur Manipulation von sensiblen und wichtigen Unternehmensdaten.

Frage 5: Ist ARP-Poisoning in WLANs (Wireless LANs, Funknetzen) ebenfalls möglich?

ARP wird in WLANs genauso eingesetzt wie in 'normalen' LANs. Aus diesem Grund kann auch in WLANs ARP-Poisoning durchgeführt werden.

Frage 6: Was ist ARP-Guard?

ARP-Guard funktioniert als Frühwarnsystem und konzentriert sich auf die Erkennung von ARP-Angriffen. ARP-Guard besteht aus einem Management-System und einem oder mehreren Sensoren. Die ARP-Guard Sensoren registrieren Veränderungen an den ARP-Tabellen und leiten diese an das ARP-Guard Management-System weiter. Im **ARP-Guard** Management-System werden die Sensormeldungen ausgewertet und bearbeitet. Im Angriffsfall benachrichtigt das Management-System automatisch die autorisierten Sicherheitsbeauftragten oder Netzadministratoren.

Frage 7: Gibt es außer ARP-Guard noch andere Lösungen?

ARP-Guard ist die weltweit erste wirksame Lösung zum Schutz vor ARP-Angriffen. Folgende Lösungsansätze sind denkbar, haben sich jedoch alle als nicht praktikabel, unwirtschaftlich oder schlicht unwirksam erwiesen:

- Herunterladen oder Ausführen fremder Software muss wirksam unterbunden werden: Unmöglich
- Einschränkung von Verkehrsbeziehungen (Port Protection, Zugriffskontrolllisten von Layer-3/4/5/6/7-Switches): Hoher Managementaufwand, hohe Kosten, evtl. eingeschränkte Funktionalität
- Bildung kleinerer Subnetze: Hohe Kosten für Router, hoher Administrationsaufwand, beschränkter Schutz
- Statische ARP-Tabellen: Aufwendig, nicht administrierbar
- arpwatch: Lediglich bei statischen IP-Adressen und nur für kleine Netze anwendbar
- Intrusion Detection: Teuer, die meisten IDS erkennen keine ARP-Angriffe
- Schutzfunktionen im IP-Stack: Nur beschränkt wirksam, nur für Unix verfügbar, kann zu Fehlfunktionen führen.
- Kryptografische Lösungen: Teilweise nicht verfügbar, teilweise nicht zur Abwehr von ARP-Angriffen konzipiert

Frage 8: Wo liegt der Unterschied zwischen dem ASP- und dem Lizenz-Modell?

Im **ASP-Modell** wird die Software für die ARP-Guard Sensoren von ISL zur Verfügung gestellt und der Betrieb des ARP-Guard Management-Systems von ISL übernommen. Wartungsmaßnahmen und Software-Updates sind in diesem Service eingeschlossen. Die Datenauswertung bindet in diesem Modell keine internen Ressourcen und verlangt kein eigenes Know-How.

Im **Lizenz-Modell** werden neben den Sensoren auch das ARP-Guard Management-System im Unternehmen installiert und betrieben.

Frage 9: Welches Service-Modell ist für mein Unternehmen das richtige?

Mit dem Lizenzmodell können Sie **ARP-Guard** vollständig im eigenen Netz betreiben. Möchten Sie keine weiteren internen Ressourcen an IT-Security-Aufgaben binden, so ist das ASP-Modell empfehlenswert. Wir helfen Ihnen gern in einem Beratungsgespräch, die für Sie passende Lösung zu finden.

Frage 10: Was kostet ARP-Guard?

Das ist davon abhängig welches Modell (ASP oder Lizenz) Sie wählen. In jedem Fall bleiben die Investitionen für Sie transparent und kalkulierbar. Wir erstellen Ihnen gern ein individuelles Angebot.

Frage 11: In welcher Netzwerkumgebung kann ARP-Guard eingesetzt werden?

ARP-Guard kann in jeder Netzwerkumgebung eingesetzt werden, die TCP/IP auf Ethernet-Netzen verwendet. **ARP-Guard** lässt sich problemlos in weitere IT-Sicherheitsumgebungen (Firewalls, Virens Scanner, Intrusion Detection) einbinden.

Frage 12: Welche Systemvoraussetzungen müssen für die Installation der ARP-Guard LAN-Sensoren gegeben sein?

Je nach Anzahl und Geschwindigkeit der Netzsegmente sind adäquate Rechner für die Sensor-Software einzusetzen. Als Minimalkonfiguration für 10/100 Base-T-Netze setzen wir voraus:

- IP-Netzsegmente mit Ethernet-Switches inklusive Spiegelport
- Pentium III mit 1000 MHz
- 128 MB RAM und 128 MB freier Plattenplatz
- SuSE Linux (8.2 oder 9.0) oder Redhat Linux (8.0 oder 9.0)
- Eine Ethernet-Schnittstelle pro überwachtem Switch und ein zusätzliches Interface für die Kommunikation mit dem Management-System

Frage 13: Welche Systemvoraussetzungen müssen für die Installation des ARP-Guard Management-Systems gegeben sein?

Je nach Anzahl der ARP-Guard Sensoren und überwachten Adressen ist ein adäquater Rechner für die Management-Software einzusetzen. Als Minimalkonfiguration setzen wir voraus:

- Pentium III mit 1800 MHz
- 256 MB RAM und 1 GB freier Plattenplatz
- SuSE Linux (8.2 oder 9.0) oder Redhat Linux (8.0 oder 9.0)
- RAID empfohlen
- Ethernet-Schnittstelle

Frage 14: Wieviele LAN-Sensoren benötige ich für mein Netzwerk?

Jeder **ARP-Guard LAN-Sensor** kann bis zu bis zu 8 LAN-Switches überwachen. Damit kann bereits ein Sensor zwischen 150 bis 200 Rechner/Stationen abdecken.

Frage 15: Mit welchen Betriebssystemen ist ARP-Guard getestet?

ARP-Guard ist mit SuSE Linux (8.2 und 9.0) und Redhat Linux (8.0 und 9.0) getestet, sollte jedoch auch mit neueren Distribution arbeiten. Bei älteren Distributionen können Probleme auftreten, insbesondere SuSE Linux 7.3 und Redhat Linux 7.0 können nicht empfohlen werden.

Frage 16: Wir erhalten falsche Angriffsmeldungen (false positives). Was können wir tun?

Zunächst müssen Sie den Grund für die false positives feststellen:

1. Es liegt ein Cluster (Hochverfügbarkeit oder Lastverteilung) vor:
Bitte fixieren Sie die entsprechenden Zuordnungen, dann wird die Meldung nicht wieder auftreten.
2. Die ARP-Cache Live-Time ist zu hoch eingestellt (nur SNMP-Sensor):
Konfigurieren Sie die ARP-Cache Live-Time auf einen Wert von z.B. 5 Minuten. Hersteller wie z.B. Cisco verwenden hier in der Standardkonfiguration eine sehr hohe Live-Time von 4 Stunden, bei der falsche Angriffsmeldungen (false positives) auftreten können.
3. Ein Router in Ihrem Netz arbeitet mit Proxy-ARP (nur LAN-Sensor):
Manche Router antworten auf ARP-Anfragen, die ausserhalb des gültigen Subnetzes liegen. Dies kann zu Adresskonflikten und daher zu Meldungen im ARP-Guard-System führen. Bitte deaktivieren Sie dieses Feature auf Ihren Routern bzw. setzen Sie es nur da ein, wo Sie es wirklich benötigen.
4. Ein ARP-Cache Eintrag auf einem SNMP-Server ist ungültig (nur SNMP-Sensor):
Manche Router tragen '00-00-00-00-00-00' als MAC-Adresse ein, falls eine IP-Adresse nicht aufgelöst werden kann. Diese Meldung tritt zum Glück nur sehr selten auf.

Ein Router versendet merkwürdige ARP-Pakete für die Broadcast-MAC-Adresse (nur LAN-Sensor):
Manche Router versenden für ihre eigenen IP-Adressen ARP-Pakete, die eine Zuordnung zur Broadcast-MAC-Adresse enthalten. Da Angriffe oder Konflikte von der Broadcast-MAC-Adresse unwahrscheinlich sind, können diese ARP-Pakete durch das Setzen der Option 'LansIgnoreBroadcastMac' unter Unternehmen / Einstellungen / Sensor für alle Sensoren ignoriert werden.

Frage 17: Der Sensor kommuniziert nicht mit dem Management-System.

Folgende Ursachen können zugrunde liegen:

- Die Lizenz ist noch nicht eingespielt:
Bitte installieren Sie Ihre Lizenz und vergessen Sie bitte nicht, das Management-System danach neu zu starten, damit die neue Lizenz wirksam wird.
- Der Sensor kennt die IP-Adresse Ihres Management-Systems nicht (in der Standardkonfiguration versucht er, eine Verbindung mit dem Management-System sensor.arp-guard.com herzustellen):
Bitte konfigurieren Sie die korrekte IP-Adresse des Management-Systems und vergessen Sie bitte nicht, den Sensor danach neu zu starten, damit die Änderung wirksam wird.

Die IP-Adressen in der Sensorkonfiguration und in der Lizenz stimmen nicht überein:

Bitte stellen Sie sicher, dass bei der Konfiguration des Sensors genau die IP-Adresse verwendet wird, die in der Lizenz eingetragen ist. Bitte vergessen Sie nicht, den Sensor neu zu starten, wenn Sie die Konfiguration ändern, damit die Änderungen wirksam werden.

Frage 18: Welche zusätzliche Netzlast wird durch ARP-Guard erzeugt?

Es existieren vier Stellen, an denen ARP-Guard zusätzliche Last erzeugt:

- Switch zum LAN-Sensor: Auf den Verbindungen vom Switch zum LAN-Sensor liegt hohe Last vor, da die Switchports als Spiegelports konfiguriert sein sollten, aber dies beeinflusst den Rest des Netzverkehrs nicht.
- SNMP-Server zum SNMP-Sensor: Eine Anfrage zum SNMP-Server enthält etwa 100 Bytes pro IP-Adresse. Bei einer Anfrage pro Minute wird dadurch eine durchschnittliche Last von 13 kBit/s für 1000 IP-Adressen erzeugt. Falls dies zuviel für Ihre WAN-Verbindungen ist, denken Sie bitte darüber nach, an Ihren größeren externen Standorten eigene Sensoren aufzustellen.
- Sensor zum Management-System: Daten von einem Sensor zum Management-System werden nur bei der Initialisierung und bei Adressänderungen übertragen. Solange keine Adressänderungen auftreten wird zweimal pro Minute eine Anfrage versandt, bei der ein paar hundert Byte pro Minute übertragen werden.

Management zum Administrator: Durch das Management des Systems über das Webinterface sowie durch die Emails, die bei Angriffen verschickt werden, wird zusätzlicher Verkehr verursacht. Dadurch wird die Netzlast aber nicht wirklich erhöht.

Frage 19: Weitere Fragen?

Haben Sie weitere Fragen, die hier nicht beantwortet sind?

Bitte senden Sie eine E-mail an info@arp-guard.com.