

Protecting Your System Against Address Resolution Protocol (ARP) Attacks

An Agnitum TechNote

This document describes how local area networks can be attacked from within and discusses how the new features in Outpost Firewall Pro v3.0 provide advanced protection against attacks that originate from inside the network.

What's the problem?

Information over the network is sent in data packets. Every packet has a sender and a recipient, and every packet needs to be sent to the specific hardware address, also known as the MAC (Medium Access Control) address. Network equipment defines the MAC address for every node on a network and directs traffic to devices based on these unique hardware addresses.

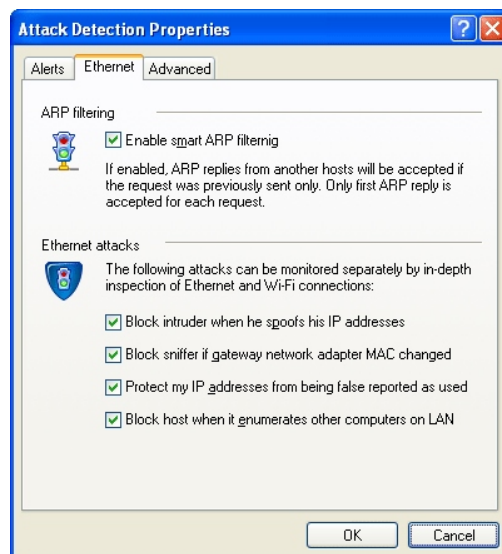
A process called Address Resolution Protocol (ARP) is used to convert the 32-bit IP address used to move data around a network to the 48-bit MAC address required by the network hardware. When data is sent from one computer to another over the network, the sending machine broadcasts an ARP request to determine the MAC address based on the IP address of the target machine and waits for it to send back its Ethernet address. During the time between the packet broadcast and the Ethernet address response, data is vulnerable to tampering, hijacking, and/or redirection to an unauthorized third party.

How Outpost overcomes the problem

In order to reliably defend against ARP-related attacks, a firewall must be able to deal with an attacker on the ARP-protocol level, by detecting and blocking not only port scanning but also network scanning with ARP requests. It should also be able to detect and prevent other Ethernet-specific attacks.

Outpost Firewall Pro 3.0's improved Attack Detection plug-in now detects and prevents specific Ethernet attacks such as IP spoofing, ARP scanning, and ARP flooding by examining Ethernet and Wi-Fi traffic on the ARP level. It also blocks ARP replies in cases where there has been no corresponding request from the system.

The Attack Detection plug-in provides the following capabilities:



Smart ARP Filtering

Smart ARP filtering is an effective mechanism to protect users from fake requests to initiate communications and shields wireless networks from illegitimate connections.

Imagine that a node on the network starts sending a huge number of ARP replies with varying MAC addresses in a short time span, trying to overload and confuse the network equipment as it tries to determine which MAC address actually belongs to the node.

ARP filtering ensures that ARP replies are dropped if no corresponding request was sent in the first place. With ARP filtering enabled, only the first ARP reply is accepted for each request.

Any system not protected by the ARP filtering is also susceptible to so-called ARP cache poisoning, which occurs when someone succeeds in intercepting Ethernet traffic using fake ARP replies in an effort to change the address of the network card to one that an attacker can monitor. Additionally, if ARP filtering is not enabled, ARP floods - where a huge number of bogus ARP replies are sent to the target machine - may cause a system to freeze.

IP Spoofing Prevention

IP spoofing is an attempt to overload the network with superfluous data and cause a denial of service attack on the recipient machine. Outpost's Attack Detection plug-in detects when networked computers are hit by an enormous number of IP packets coming from a single machine during a particular time period and blocks such communication to prevent network overload.

Sniffer Blocking

Hackers can substitute legitimate MAC addresses with ones of their own, rerouting legitimate traffic to the hacker-controlled machine, by spoofing the ARP replies. This enables them to be able to 'sniff' (read) packets and view any data in transit. This ARP spoofing also allows traffic to be directed to non-existent hardware, causing delays in data transmission or a denial of service on the affected equipment.

Specialized hackers' sniffing programs can also intercept traffic, including chat sessions and related private data such as password entries, names, addresses, and even encrypted files, by modifying MAC addresses at the Internet gateway.

To prevent this traffic interception and protect against sniffer attacks, Outpost's Attack Detection plug-in checks whether the MAC address correctly matches the source IP address in the ARP packet and thus ensures that no unauthorized modification of the gateway network adapter has taken place.

IP Address Conflict Prevention

An attacker can block a computer from accessing the network by generating false ARP replies, duplicating all the IP addresses on a network and causing IP address conflict. Outpost's Attack Detection plug-in blocks false ARP replies with the same IP address as that of the adapter but with a different MAC address. This ensures that IP address conflict is avoided and the computer can correctly start even if the IP address has been erroneously reported as used.



Network Scan Blocking

Some massively propagating viruses use mass host enumeration to hop from one computer to another, infecting them as they go. This technique is also used by scanners and vulnerability analyzers. Outpost's Attack Detection plug-in shields the user's local network by limiting the number of ARP requests enumerating IP addresses from one MAC address during a specified time interval and preventing the ARP network scan.

Summary

Protection against data theft and internally-generated attacks is of increasing importance to users of home and small business networks, wired or wireless. When computers are interconnected and exchanging data, there is considerable risk that information may be intercepted or sabotaged while in transit, resulting in compromised confidential data or disruption of network services.

Outpost Firewall Pro 3.0's advanced attack detection and anti-spoofing technology prevents your computer from being hijacked and used against its own network. Your computers are proactively defended against zero-day attacks and protected against vulnerabilities in Windows operating systems until such time as Microsoft issues a patch.

With Outpost protection in place on your system, you no longer need to be afraid that someone will steal your information over the network or the Internet. Next time you plan to visit a Wi-Fi Internet café, make sure you take Outpost along, too!