ARP Spoof Inspector

ARP Spoof Inspector Overview

Type	Inspector (network)
Usage	Inspect
Instance Type	Singleton
Other Inspectors Required	None
Enabled	`true`

Address Resolution Protocol (ARP) is a stateless, communication protocol used within a single network for address resolution. When exchanging requests and responses, ARP does not provide authentication between hosts.

ARP spoof is a type of man-in-the-middle attack using ARP within a Local Area Network (LAN). An attacker alters the communication to a host by intercepting messages intended for a specific host media access control (MAC) address.

The `arp_spoof` inspector analyzes ARP packets and detects unicast ARP requests. To detect ARP cache overwrite attacks, the ARP Spoof inspector identifies inconsistent Ethernet-to-IP mapping.

If enabled, the `arp_spoof` inspector:

- Inspects Ethernet addresses and the addresses in the ARP packets. When an inconsistency occurs, the inspector uses rule 112:2 or rule 112:3 to generate alerts, and in an inline deployment, drop offending packets.
- Checks for unicast ARP requests. If a unicast ARP request is detected, the inspector uses rule 112:1 to generate alerts, and in an inline deployment, drop offending packets.

- If the `hosts[]` parameter is specified, the inspector uses that information to detect ARP cache overwrite attacks. If such an attack is detected, the inspector uses rule 112:4 to generate alerts, and in an inline deployment, drop offending packets.

ARP Spoof Inspector Parameters

The `arp_spoof` inspector does not provide default configuration parameter values in the Secure Firewall Management Center web interface.

ARP Spoof Inspector Rules

Enable the `arp_spoof` inspector rules to generate events and, in an inline deployment, drop offending packets.

Table 1: ARP Spoof Inspector Rules

GID:SID	Rule Message
112:1	unicast ARP request
112:2	ethernet/ARP mismatch request for source
112:3	ethernet/ARP mismatch request for destination
112:4	attempted ARP cache overwrite attack

ARP Spoof Inspector Intrusion Rule Options

The `arp_spoof` inspector does not have any intrusion rule options.