Dynamic Arp Inspection

The ARP message has no IP header, only broadcast in local network, both sender and receiver add an entry each in their ARP table, some devices automatically send gratuitous ARP messages when an interface is enabled, IP address or MAC address is changed,.. etc.

DAI only filters ARP messages, all ports are untrusted by default, all ports connected to other network devices should be trusted while those connected to endhosts should be untrusted (downlink ports can/'t be untrusted).

ARP Poisoning: an attacker manipulates target's ARP table so traffic is sent to attacker by sending gratuitous ARP messages or ARP replies to legitimate ARP requests using another device's IP address (the original device with that IP doesn't update its ARP table). (Man in the Middle attack).

DAI inspects the sender MAC and IP fields of ARP messages received on untrusted ports and checks if there is a matching entry in DHCP snooping binding table or discard the message, ARP ACLS can be manually configured to map IP to MAC, useful for hosts not using DHCP, DAI can perform more optional in depth checks, DAI supports ARP rate limiting.

DHCP snooping , DAI require work from switch's CPU so even if the attacker's messages are blocked, they can still overload the switch CPU with messages.

Command: ip arp inspection vlan <vlan number>. Command: ip arp inspection trust.

Command: show ip arp inspection interfaces.

DAI rate limiting is enabled on untrusted ports by defaults with a rate 15 packets per second, can be configured as X packets per Y seconds and disabled on trusted ports,faster rates cause interfaces to be error disabled, only received not sent.

DHCP snooping rate limiting is disabled on all interfaces by default.

Command: ip arp inspection limit rate <rate> optional of default 1 second **burst interval <seconds>.**

Command: errdisable recovery cause arp-inspection.

Command: ip arp inspection validate dst-mac ip src-mac. (all validation checks should be in the same command else overridden).

Dest-mac: the dest mac in Ethernet header against target MAC in ARP body for ARP responses.

IP: validates ARP body for invalid IP addresses as 0.0.0.0, 255.255.255.255, multicast addresses, sender IPS are checked in ARP requests, the target IP in ARP response.

Src-mac: validates source mac address against sender MAC in ARP body for requests and response.

Command: arp access-list <ACL name>

Command: permit ip host <ip> mac host <mac>.

Command: ip arp inspection filter <ACL name> vlan <vlan number>.

Command: show ip arp inspection.

If static ACL is enabled, implicit deny at the end of arp ACL is enabled so only ACL is checked without DHCP snooping binding table.