Dynamic ARP Inspection

Overview

Dynamic ARP Inspection (DAI) is a security feature in MS switches that protects networks against man-in-the-middle ARP spoofing attacks.

DAI inspects Address Resolution Protocol (ARP) packets on the LAN and uses the information in the DHCP snooping table on the switch to validate ARP packets. DAI performs validation by intercepting each ARP packet and comparing its MAC and IP address information against the MAC-IP bindings contained in the DHCP snooping table. Any ARP packets that are inconsistent with the information contained in the DHCP snooping table are dropped.

Supported Models for DAI: MS210, MS225, MS250, MS350, MS355, MS410, MS425, MS450

Understanding DAI

This section describes the useful concepts required to understand DAI.

ARP

In order to send packets on LAN, network devices need to know the IP and MAC address of the hosts they intend to communicate with. Address Resolution Protocol provides the mechanism to determine the MAC address associated with an IP address. These IP to MAC bindings are stored in each device’s ARP cache.

For example, Host A wants to communicate with Host B but it does not have the MAC address of Host B in its ARP cache. Host A generates a broadcast message (ARP request) for all hosts within the LAN segment to obtain the MAC address associated with the IP address of Host B. All hosts within the broadcast domain receive the ARP request and only Host B responds with its MAC address.

ARP Spoofing attacks

ARP spoofing is a form of man-in-the-middle attack which allows an attacker to intercept traffic intended for other hosts. This is accomplished by sending out crafted ARP packets which poison the ARP cache on the network devices. By poisoning the ARP caches of network devices such as end hosts, switches and firewalls on a LAN segment, traffic is redirected to the attacker’s machine. An example of an ARP spoofing attack is shown below.
Hosts A, B, and C are connected to the switch on ports 1, 2, and 3 respectively. When Host A needs to communicate to Host B, it broadcasts an ARP request to determine the MAC address associated with 10.10.10.20, the IP address of Host B. When Host B responds, the switch and Host A populate their ARP caches with a binding for a host with the IP address 10.10.10.20 and the MAC address bb:bb:bb:bb:bb:bb. The switch also learns the MAC address of Host B on port 2.

Host C can poison the ARP cache of the switch and Host A for Host B by broadcasting forged ARP responses. The ARP packets from Host C claim that the IP address 10.10.10.20 exists on cc:cc:cc:cc:cc:cc. Host A and the switch will now use the MAC address “cc:cc:..” as the destination MAC address for traffic intended for Host B. The switch will now forward all traffic towards 10.10.10.20 to port 3. This means that Host C intercepts that traffic. Host C has now successfully inserted itself into the traffic stream from Host A to Host B, which is a classic form of man-in-the-middle attack.

DAI

DAI associates a trust state with every port on the switch. Ports marked as trusted are excluded from DAI validation checks and all ARP traffic is permitted. Ports marked as untrusted are subject to DAI validation checks and the switch examines ARP requests and responses received on those ports.

The IP-to-MAC binding information in ARP packets are compared to the DHCP Snooping table on the switch. If no IP-to-MAC entry in the DHCP snooping table corresponds to the information in the ARP packet, DAI drops the ARP packet and the local ARP cache is not updated with the information in that packet.

It is recommended to configure only ports facing end-hosts as untrusted (Trusted: disabled). Ports connecting network devices such as switches should be configured as trusted to avoid connectivity issues.

Configuring DAI

1. Configure Trusted ports before enabling DAI. Go to Switch > Switch ports. By default all ports are configured marked untrusted (disabled).

DAI relies on DHCP snooping table information to perform validation. If a switch does not have a corresponding entry in its DHCP Snooping table, and an ARP packet arrives on an untrusted port, DAI validation will fail and the ARP packet will be dropped. It is therefore recommended to use DAI only for DHCP enabled subnets.
2. Navigate to **Switch > DHCP Servers and ARP**

3. DAI is disabled by default.
A warning is displayed in case DAI is enabled without configuring trusted ports.

**DAI Blocked Events**

If a client device is attempting to spoof an IP address, and traffic on a switchport fails validation, then DAI will take action. Events where DAI has found potentially malicious client traffic can be found both in the Network-wide > Event log, or on the switch related page under Switch > DHCP servers and ARP. The events will list the source MAC address, the VLAN this traffic was identified on, the likely IP address, timestamps of the events, and the total count of the events.
Whitelisting Blocked Entries

If a client has been flagged by DAI incorrectly, it is possible to whitelist the entry so the traffic does not get dropped. Whitelisting these entries will add them to the DHCP snooping table as valid snoop entries. This will tie the MAC address of the client to the IP address in the table so traffic will not be flagged as invalid or malicious. This action can be done under Switch > DHCP servers and ARP.

In the DAI Blocked Events, you can select the entry you wish to whitelist, and then use the Move to whitelist button.

You will now see the entry you selected under the Whitelisted snoop entries section. Traffic from this MAC address using this IP address will no longer be blocked by DAI on the switches.