IP Source Address Spoofing Protection

Overview

The MX Security Appliance implements several forms of traffic verification to detect and prevent forms of IP spoofing. These are similar in nature to unicast reverse path forwarding in loose mode.

Key Terms

To understand the anti-IP spoofing mechanisms implemented on the MX, it is important to understand several key concepts.

**IP Source Address Spoofing**

IP source address spoofing is the process of intentionally configuring an IP address to impersonate another host or device on the network. This type of action is typically performed by a malicious actor attempting to circumvent access control restrictions that it would normally be subject to.

**Unicast Reverse Path Forwarding**

Unicast Reverse Path Forwarding (Unicast RPF) is used to help limit the malicious traffic on an enterprise network. This security feature works by enabling a router to verify the reachability of the source address in packets being forwarded. This capability can limit the appearance of spoofed addresses on a network. If the source IP address is not valid, the packet is discarded.

Operating mode

All MXs can be configured in either NAT or passthrough mode. More detailed information on concentrator modes, click here.

**NAT Mode**

In NAT mode the MX is configured with one or more local subnets or VLANs. In this configuration, the MX appliance generally serves as the default gateway for devices on the LAN. Client traffic destined to the Internet will have its source IP rewritten to match the WAN IP of the appliance.

**Passthrough Mode**

In this mode, the MX device does not provide any address translation and operates as a passthrough device between the Internet and the LAN ports (sometimes referred to as a Layer 2 bridge).

Implementation

In order to mitigate IP spoofing, the MX Security Appliance implements a form of unicast reverse path forwarding.

**NAT mode**

When configured in NAT mode, the MX appliance performs several validation checks on each packet received on the LAN before routing them. The following
validations are performed:

- The source IP address is reachable through a configured static route or local VLAN
- If the source IP address is contained within a configured VLAN, the source VLAN must match the configured VLAN ID for the source IP's subnet
- If the source IP address is contained within a configured static route, the source VLAN must match the VLAN ID for the subnet that the next hop IP of the static route is accessible through

Special exceptions are made for DHCP discover messages and for traffic used to synchronize information between MXs in a NAT warm spare configuration.

If any traffic received on the LAN of the MX fails any of the validation checks and does not match one of the special exceptions, it will be dropped. It is important to keep this in mind when designing and configuring networks.

**VLANs Disabled**

When VLANs are disabled, the MX appliance performs one validation check on each packet received on the LAN before routing them. The following validation is performed:

- The source IP address is reachable through a configured static route or the configured local LAN

Special exceptions are made for DHCP discover messages and for traffic used to synchronize information between MXs in a NAT warm spare configuration.

If any traffic received on the LAN of the MX fails this validation check and does not match one of the special exceptions, it will be dropped. It is important to keep this in mind when designing and configuring networks.

Regardless of the IP spoofing prevention mechanisms of the MX Security Appliance, in order to properly process traffic received on the LAN, the source IP address must be contained within the local LAN's subnet or a configured static route.

**Correct Topologies**

The following example topologies demonstrate configurations that will not result in valid traffic being dropped by the ip spoofing prevention mechanisms.
In this topology:

- Client VLANs are only defined on a single layer 3 device.
- Client devices have a default gateway of the layer 3 device the VLAN has been defined on.
- A single transit VLAN is used to allow for communications between the MX and downstream subnets.
- For downstream infrastructure and client subnets, static routes are configured on the MX. The next hop IP address is that of the layer 3 switch's IP on the transit VLAN.
- The layer 3 switch is configured with a default route with a next hop IP address of the MX's IP on the transit VLAN.
- The ports used to connect the MS and MX are both properly defined as being on VLAN 50, the transit VLAN.
How is traffic routed given the above configuration?

In each scenario below, traffic is always sent from the downstream client - 192.168.22.3.

If traffic is destined to 192.168.22.22
The traffic is forwarded at layer 2 by the downstream switching infrastructure. This traffic is not processed by the layer 3 switch, or by the MX.

If traffic is destined to 192.168.32.14
The traffic is received by the layer 3 switch and routed directly to 192.168.32.14. This traffic is not processed by the MX.

If traffic is destined to 216.58.194.206
The traffic is received by the layer 3 switch and routed to the MX via the transit VLAN. This traffic is received by the MX on VLAN 50.

The MX compares the source VLAN (50) and the source IP (192.168.22.3) against the anti-IP spoofing validation checks. In this case, the source IP (192.168.22.3) is contained within a subnet configured on the MX (192.168.22.0/24) and was received on the expected VLAN (50), based on the next hop IP of the static route for 192.168.22.0/24. This traffic passes the anti-IP spoofing validation checks.

The MX will then compare the traffic against any other filtering rules (e.g. layer 3 firewall rules, layer 7 firewall rules, content filtering policies, etc...). If the traffic does not match another block rule configure on the MX, the traffic will be NATed and sent to the Internet.
In this topology:

- Client VLANs are only defined on the MX.
- Client devices have a default gateway of the MX.
- The ports used to connect the MS and MX are both properly configured to allow traffic from VLANs 1 and 2 and are using the same native VLAN.

How is traffic routed given the above configuration?
In each scenario below, traffic is always sent from the downstream client - 192.168.22.3.

If traffic is destined to 192.168.22.22
The traffic is forwarded at layer 2 by the layer 2 MS, or the MX, depending upon where 192.168.22.22 is located in the network.

If traffic is destined to 192.168.32.14
The traffic is received by the MX with a tagged VLAN ID of 2 and processed by the MX. The MX compares the source VLAN (2) and the source IP (192.168.22.3) against the anti-IP spoofing validation checks. In this case, the source IP (192.168.22.3) is contained within a subnet configured on the MX (192.168.22.0/24) and was received on the expected VLAN (2). This traffic passes the anti-IP spoofing validation checks. The MX will then compare the traffic against any other filtering rules (e.g. layer 3 firewall rules, layer 7 firewall rules, content filtering policies, etc...). If the traffic does not match another block rule configured on the MX, the traffic will be routed directly to 192.168.32.14 on the LAN.

If traffic is destined to 216.58.194.206
The traffic is received by the MX with a tagged VLAN ID of 2 and processed by the MX. The MX compares the source VLAN (2) and the source IP (192.168.22.3) against the anti-IP spoofing validation checks. In this case, the source IP (192.168.22.3) is contained within a subnet configured on the MX (192.168.22.0/24) and was received on the expected VLAN (2). This traffic passes the anti-IP spoofing validation checks. The MX will then compare the traffic against any other filtering rules (e.g. layer 3 firewall rules, layer 7 firewall rules, content filtering policies, etc...). If the traffic does not match another block rule configured on the MX, the traffic will be NATed and sent to the Internet.

Incorrect Topologies
The following example topologies demonstrate configurations that will result in traffic being dropped by the ip spoofing prevention mechanisms.
In this topology:

- Client VLANs are only defined on both layer 3 devices.
- Client devices have a default gateway of the layer 3 switch.
- A transit VLAN is not used.
- For downstream infrastructure and client subnets, static routes are not configured on the MX.
- Asymmetric routing exists.
- The layer 3 switch is configured with a default route with a next hop IP address of the MX's IP on one of the client VLANs.
The ports used to connect the MS and MX are both properly configured to allow traffic from VLANs 1 and 2 and are using the same native VLAN.

**How is traffic routed given the above configuration?**

In each scenario below, traffic is always sent from the downstream client - 192.168.22.3.

**If traffic is destined to 192.168.22.22**
The traffic is forwarded at layer 2 by the downstream switching infrastructure. This traffic is not processed by the layer 3 switch, or by the MX.

**If traffic is destined to 192.168.32.14**
The traffic is received by the layer 3 switch and routed directly to 192.168.32.14. This traffic is not processed by the MX.

**If traffic is destined to 216.58.194.206**
The traffic is received by the layer 3 switch and routed to the MX via its default route. The MS's default route has a next hop IP address of the MX's IP address on VLAN 1.

The MX compares the source VLAN of the packet sent from the layer 3 switch (1) and the source IP (192.168.22.3) against the anti-IP spoofing validation checks. In this case, the source IP (192.168.22.3) is contained within a subnet configured on the MX (192.168.22.0/24); however, the 192.168.22.0/24 subnet is configured as VLAN 2 on the MX.

Since the source VLAN (1) and the subnet the source IP is contained within (192.168.22.0/24) do **not** match the configuration of the MX (VLAN ID 2 is configured for 192.168.22.0/24 on the MX). This traffic **fails** the anti-IP spoofing validation checks and is **dropped**.
Layer 2 switch

In this topology:

- Client VLANs are only defined on the MX.
- Client devices have a default gateway of the MX.
- The ports used to connect the MS and MX are both properly configured to allow traffic from both VLAN 1 and 2 and are **not** using the same native VLAN.

How is traffic routed given the above configuration?
In each scenario below, traffic is always sent from the downstream client - 192.168.22.3.

**If traffic is destined to 192.168.22.22**

The traffic is forwarded at layer 2 by the layer 2 MS, or the MX, depending upon where 192.168.22.22 is located in the network.

**If traffic is destined to 192.168.32.14**

The traffic is received by the MX without a tagged VLAN ID and is processed by the MX. As the traffic is received at the MX untagged, it is interpreted as being on the port's native VLAN (1).

The MX compares the source VLAN (1) and the source IP (192.168.22.3) against the anti-IP spoofing validation checks. In this case, the source IP (192.168.22.3) is contained within a subnet configured on the MX (192.168.22.0/24) and was not received on the expected VLAN (2).

Since the source VLAN (1) and the subnet the source IP is contained within (192.168.22.0/24) do not match the configuration of the MX (VLAN ID 2 is configured for 192.168.22.0/24 on the MX). This traffic fails the anti-IP spoofing validation checks and is dropped.

**If traffic is destined to 216.58.194.206**

The traffic is received by the MX without a tagged VLAN ID and is processed by the MX. As the traffic is received at the MX untagged, it is interpreted as being on the port's native VLAN (1).

The MX compares the source VLAN (1) and the source IP (192.168.22.3) against the anti-IP spoofing validation checks. In this case, the source IP (192.168.22.3) is contained within a subnet configured on the MX (192.168.22.0/24) and was not received on the expected VLAN (2).

Since the source VLAN (1) and the subnet the source IP is contained within (192.168.22.0/24) do not match the configuration of the MX (VLAN ID 2 is configured for 192.168.22.0/24 on the MX). This traffic fails the anti-IP spoofing validation checks and is dropped.

**Passthrough Mode**

No IP spoofing validation checks are performed in a passthrough configuration.

**IP source address spoofing configuration**

To enable/disable IP source address spoofing, navigate to Security Appliance > Configure > Firewall > IP source address spoofing protection.

This option is set to "Block" by default on new Meraki networks starting 07/12/2018. As an example, the figure below shows that when this option is set to "Block", traffic that does not pass the VLAN validation checks will be dropped.
Any existing network created before 07/12/2018 will have this option set to "Log" as shown below:

For new networks, the following warning will appear if this option is changed from "Block" to 'Log':

Additional Reading

The functionality this feature implements is intended to bring networks in line with IETF Best Current Practice 38 - for more detailed information on why this is a feature Meraki recommends be enabled, please refer to that document.