Bridging

https://campus.barracuda.com/doc/72516590/

A Layer 2 bridge checks the destination MAC address of each incoming frame. If the MAC address is assigned to the bridge computer, the frame is processed by it as the destination. If the MAC address is not assigned to the bridge computer, the network bridge notes the source address of the frame and the port on which the frame was received and either creates or refreshes an entry in a Layer 2 bridge table. The port is a number that identifies the network adapter and its corresponding LAN segment. Each entry in the Layer 2 bridge table consists of a MAC address, the port number corresponding to the LAN segment on which a frame from the MAC address was received, and a timeout value. Entries in the Layer 2 bridge table persist for 5 minutes before being removed.

- How to Configure Layer 2 Bridging

Comparison of Bridging Features

To help you decide which method to use, the following table compares the features that are available for each bridging method:

Features	Transparent Layer 2 Bridging
Supported by Web Interface	Yes
MAC Transparent	Yes
Routing-Bridging-Forwarding	No
Local Firewall Traffic (Gateway)	No
Auto Learning of Network Nodes	Yes
Active Learning of Network Nodes	No
Next Hop Bridging	Yes
Broad-Multicast Propagation	Yes
High Availability	Yes
VLAN Capable	Yes
IP and ARP Forwarding	Yes
Non-IP Protocols Forwarding	No
IPv6	No
IPS	Yes
Application Control (Application Detection)	Yes
SSL Interception	No
URL Filter	Yes - default route required

Virus Scanning	**No**
ATP	**No**
SafeSearch	**No**
YouTube for Schools	**No**
Google Accounts	**No**
File Content Filtering	**Yes**
User Agent Filtering	**Yes**
Custom Block Pages	**No**

Security Weaknesses and Solutions

Since bridging heavily depends on broadcasts for establishing connectivity, there are a few weak points that you must carefully consider. Try to implement bridging in a trusted environment. Broadcasts in huge environments also consume a lot of bandwidth. The firewall offers different methods to help prevent the following common attacks:

Preventing IP or ARP Spoofing over Layer 2 Bridges

Network nodes may use the IP addresses of fake ARP responses in order to fake network traffic with arbitrary IP addresses. Since firewall security is enforced on Layer 3, the security policy is bypassed. These issues can be solved by taking the following measures:

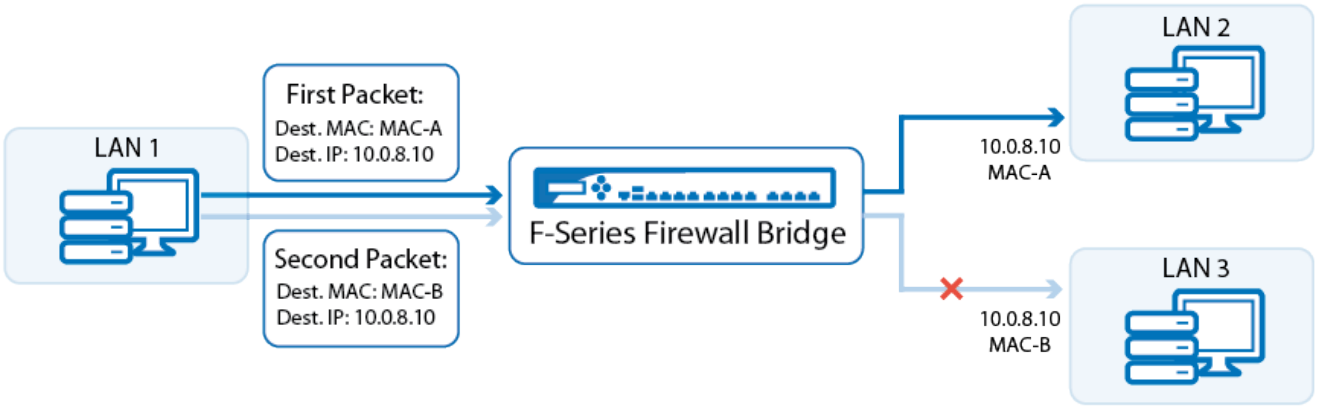
- **Segment Access Control Lists (Bridging Interface ACLs)** – Specify which IP addresses are allowed on a segment.
- **Static Bridge ARP Entries** – Statically specify IP addresses, MAC addresses, and segments to avoid learning via ARP.
- **MAC-based Access Rules** – Define source MAC conditions for network objects.
- **ARP Change Reporting** – Specify which types of the IP-MAC-Segment relationship changes must be reported in the access cache and log.

Prevent Destination MAC Spoofing

In bridged environments, there is also the possible exploitation of security enforcement on Layer 3 and traffic delivery on Layer 2. You can prevent these issues by enforcing Layer 2 when a Layer 3 session is granted. MAC addresses for a session are fixed when the session is created and remain enforced until the session ends.

In the figure below, a client from LAN 1 tries to force a connection grant to a client in LAN 3. To do so, it sends a packet to the client in LAN 2 using MAC-A as a destination MAC address and 10.0.8.10 as the destination IP address. After the session has been granted through the bridge and communication has been allowed, it sends a second packet, exchanging the MAC address for the client in LAN2 with

the MAC address for the client in LAN3, leaving the IP address the same. If MAC enforcement is configured, the connection with the spoofed MAC address will not be allowed.



Figures

1. bridge_mac_spoofing.png