Bridging Configuration Settings

This article describes the implementation of logical entities in context with the Barracuda NextGen Firewall F-Series bridging. It also explains how various bridging elements interact with each other during the bridging process.

Bridging Groups

A bridged interface group defines a set of network interfaces for which network traffic is forwarded with bridging.

Bridging Interfaces

A bridging interface is a network interface that is assigned to a bridged interface group.

A bridging interface can only be a member of one bridged interface group.

Bridging ARP Entries

A bridging ARP entry (BARP) stores the information that specifies on which bridge interface that a certain MAC address resides. Additionally, associated IP addresses are stored along with the BARP entry.

The IP address is only used for visualization purposes.

Dynamic BARPs

Dynamic BARPs are built up during run time by analyzing network traffic. Whenever a packet is received on an interface, dynamic BARPs are generated or updated. This way, the firewall "learns" which MAC address resides on which bridging interface. When ARP packets are analyzed, the Layer 3 IP information is added to the BARP entry by adding the IP address.

With dynamic BARPs, relationships are learned as follows:

- MAC-Interface relationship learned by any IP traffic.
- MAC-Interface-IP relationship learned by ARP traffic.

Static BARPs

Static BARPs are part of the configuration and define a MAC-Interface-IP relationship that is present at all times and is not overwritten by "learning" from traffic.

Bridging Interface ACL

The bridging interface ACL specifies which IP addresses can be received on a bridging interface. ACLs can be used to enforce a Layer 3 topology when operating on the firewall. The most restrictive implementation of the ACL maintains a list of single IP addresses that are expected on a certain bridge interface.

Virtual Bridge Interface

A virtual bridge interface is an interface that acts as parent interface for all interfaces of a bridged interface group. The name of a virtual interface is always the name of the bridged interface group with a *phbr-* prefix. For example: *phbr- <group-name>*

Virtual Bridge Interface IP Address

Optionally, each virtual bridge interface may be configured with an IP address and a netmask. This way, the firewall itself can actively probe (learn) on which segments each MAC address resides. It can also route traffic from a routed network to a bridged network or between bridging groups. Through the introduction of a virtual bridge interface, Transparent Layer 2 is changed to Routed Layer 2 Bridging.

A virtual bridge interface has following main characteristics:

- Active ARP queuing.
- Forwarding between bridge groups.
- Forwarding between routed and bridged networks.
- Local firewall traffic (application gateways).
- Still MAC transparent (like).

Broadcast and Multicast

Broadcast and multicast traffic can be forwarded between segments and routed networks. You must create a specific firewall rule to allow broadcast or multicast propagation. Specify a list of network interfaces, IP addresses, and multicast addresses that define how traffic should be propagated. Broadcast to unicast or multicast translations are possible.

For example, if you create a rule that specifies the following:

- Rule from *10.0.8.0/24* to *10.0.0.255 (ALL-UDP)*
- Action: *Broad- Multicast*
- Propagate *10.0.1.45*, *eth1.123, eth2.234, eth4:10.0.4.244, phbr-test, eth3:224.1.2.3.*

Traffic is propagated as follows:

- Unicast to *10.0.1.45*
- Broadcast *10.0.8.255* on interface eth1.123
- Broadcast *10.0.8.255* on interface eth1.234
- Broadcast *10.0.4.255* on interface eth4
- Broadcast *10.0.8.255* on all bridge interfaces on bridge group phbr-test
- Multicast *224.1.2.3* on interface eth3

High Availability

Bridging ARPs and sessions are synchronized between high availability (HA) partners. Synchronized BARPs are inactive as long as no bridged interface group exists that indicates bridged forwarding. Upon activation (HA takeover), the bridging groups are introduced and all related BARP entries are activated. Along with the activation, a dummy ARP request is sent on all bridging interfaces except for the one that the BARP resides on. The MAC address is entered into the MAC-Port table of the switch.

HA bridging includes:

- Firewall session synchronization
- BARP HA synchronization
- Dummy ARP for switch MAC-Port update