

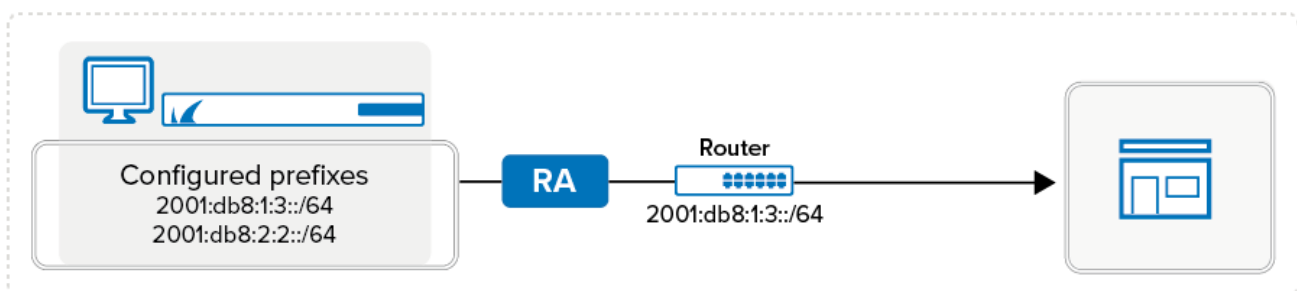
The IPv6 Router Advertisement Guard

<https://campus.barracuda.com/doc/75696529/>

The Barracuda Network Access Client helps you deal with different aspects of the IPv6 Router Advertisement functionality. The IPv6 Router Advertisement Guard keeps track of IPv6 Router Advertisement (RA) messages by inspecting the RA packets and puts you in control of them while conforming to IETF RFC 6105.

IPv6 Router Advertisement

Router Advertisement (RA) is a feature of the IPv6 Neighbor Discovery Protocol (NDP), which replaces the IPv4 Address Resolution protocol (ARP). RA helps network nodes determine information about their LAN, such as the network prefix list, the default routers list, the default gateway, and other information that can help them communicate. It can, for example, lead a node to utilize the emitting router as its default gateway. RA is sent out by routers periodically using ICMPv6 type-134 messages. Part of any RA message is an expiration time value. Entries created by RA messages within network nodes are deleted after expiration, so only routers persist in the lists that are actively broadcasting their presence by sending RA messages. An RA emission can also be forced by sending a Router Solicitation Message to the network's router multicast address to avoid waiting for an entry's expiry, which can, for example, help to quickly activate new interfaces.



Structural Parameters for RA Prefix Information

Refer to the following list for the structure of an RA prefix data set:

- **Hop Limit** – The hop limit is an 8-bit value containing the maximum hop count proposed by the router.
- **M bit** – If set, the receiving node may also use Stateful Auto Configuration, in addition to normal Auto Configuration, for the IP address.

- **O bit** – If set, the node may also use Stateful Auto Configuration, in addition to normal Auto Configuration, for all remaining values that are not the IP address.
- **Router Lifetime** – 16-bit integer that defines the expiration time for the information contained in this RA message. The maximum value is 18.2 hours. A value of 0 (zero) means that the router is not a default router and therefore should not be stored in the default router list.
- **Reachability Timeout** – 32-bit integer that defines the duration in milliseconds for which an entry in the Neighbor Cache should be indicated as being reachable after the last data was received.
- **Resolution Timeout** – 32-bit integer that defines the duration in milliseconds to wait until another Neighbor Solicitation message is to be sent.

Valid RA options are the sender's link layer address, the router's MTU, and all valid prefixes. All unknown options are ignored according to the RFC.

Potential Vulnerabilities in Conjunction with RA Messages

Given the purpose and capabilities of RA, harmful RA messages can become a security threat to a network node, to a LAN, or at least to performance and bandwidth. Barracuda Network Access Client offers various configuration options to effectively prevent such threats as:

- **Denial of Service (DoS) Attacks** – RA messages can be used for DoS attacks. Therefore, the forwarding of RA messages should be disabled on specific interfaces if they are not needed to prevent the generation of DoS messages.
- **Stateless Address Auto Configuration Attacks** – IPv6 nodes are capable of having a stateless address autoconfiguration mode, in which they listen to RA messages to automatically configure themselves. A local attacker can send malicious RA messages to divert traffic to a non-existing address, thus blackholing the victim's traffic. The attacker can also insert himself in the traffic flow in order to perform a man-in-the-middle attack.
- **Various Other Network Discovery Protocol Attacks** – IPv6 depends on the Neighbor Discovery Protocol to discover the mapping between an IPv6 address and an Ethernet MAC address. The protocol exhibits the same vulnerabilities as IPv4's ARP and is therefore not secure when the attacker is in the same LAN as the victim.

Note that there is a broad range of threats besides these given above.

IPv6 Router Advertisement Guard Functionalities

The IPv6 Router Advertisement Guard tracks all RA messages by reading the following data from an RA packet:

- Option 1: Source Link Layer Address
- Option 3: Prefix Information (including lifetimes)

The RA Guard starts to act as soon as a specific network prefix is detected for the second time. The first time a prefix is detected, it is always allowed to pass. It is thereby ensured that, also with a fully configured RA Guard with company prefixes, it is possible to establish a connection to an available network, e.g., in a hotel.

For a configured prefix **2001:db8:1:3::/64**, this means:

Example 1:

2001:db8:1:3::/64 is received > RA Guard allows connection

2001:db8:2:2::/64 is received > RA Guard instantly blocks **2001:db8:2:2::/64** (including RA)

Example 2:

2001:db8:2:2::/64 is received > RA Guard allows connection

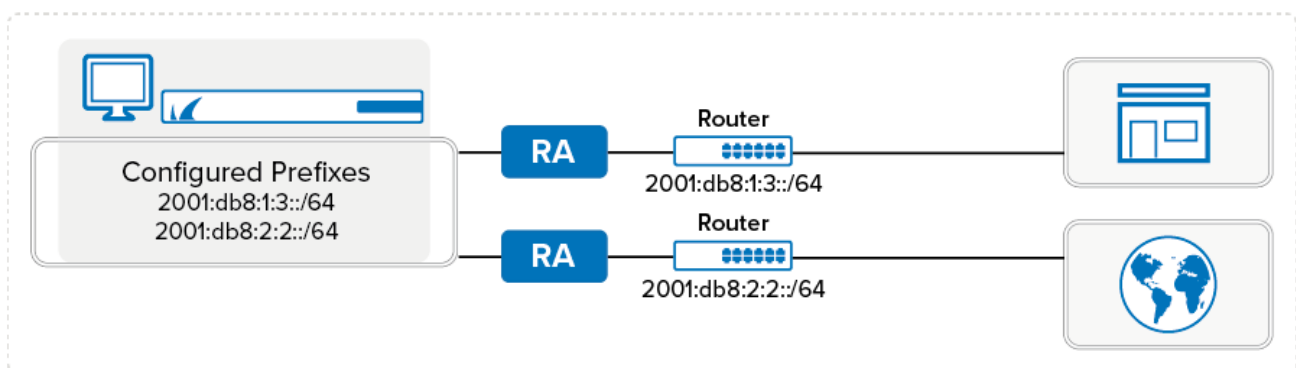
2001:db8:1:3::/64 is received > RA Guard instantly blocks **2001:db8:2:2::/64**

Example 3:

2001:db8:2:2::/64 is received > RA Guard allows connection

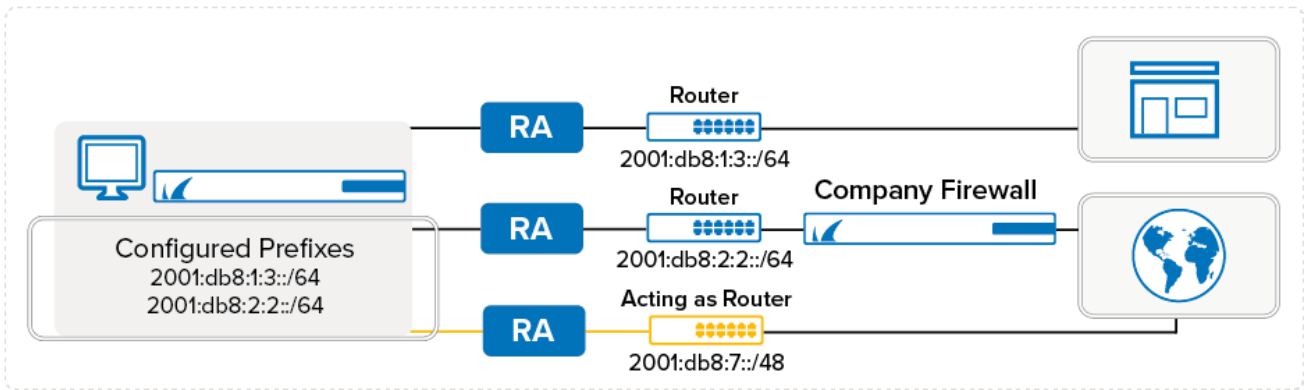
2001:db8:1:7::/64 is received > RA Guard instantly blocks **2001:db8:1:7::/64** and **2001:db8:2:2::/64**

The detected RA data is stored in a list and compared to prefixes configured in the Firewall ruleset. Known router prefixes will be ignored, as illustrated in the figure below.



Now, if the IPv6 Router Advertisement Guard detects an RA message with a still unknown network prefix, it will become active on those firewall rules having the IPv6 Company Prefix Match check box

activated. The advertised router with the unknown prefix will be blocked. The following figure illustrates this:



Default Access Rules for the IPv6 Router Advertisement Guard

There are two rules for the IPv6 Router Advertisement Guard within the Personal Firewall's default ruleset. One of them is an outbound rule named **Core Network - Router Advertisement Guard**. It lets outbound RA messages pass by default:

Outbound			
Inbound			
Nr.	Name	Adapter	Source
+ Network Discovery (3)			
- Core Network (14)			
3	Core Network - Dynamic Host Configuration		0.0.0.0/0
4	Core Network - Dynamic Host Configuration for IPv6		Any
5	Core Network - Router Advertisement Guard		Any
6	Core Network - Neighbor Discovery		Any

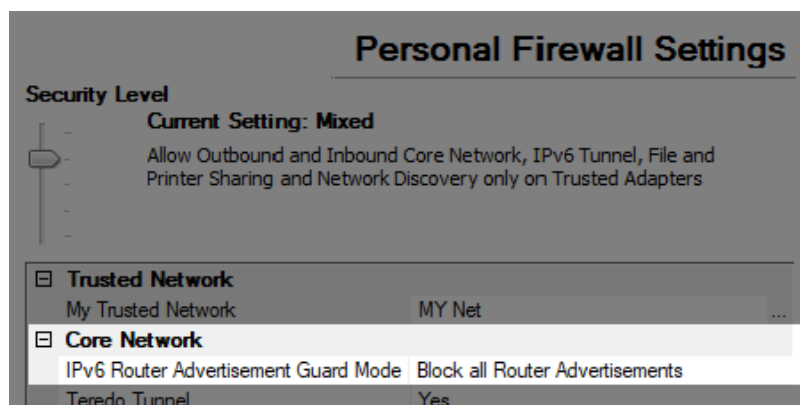
The other one is an inbound rule also named **Core Network - Router Advertisement Guard**. It blocks all inbound RA messages by default:

Outbound		Inbound	
Nr.	Name	Adapter	Source
⊕ Network Discovery (3)			
⊖ Core Network (7)			
➡ 3	Core Network - Dynamic Host Configuration		0.0.0.0/0
➡ 4	Core Network - Dynamic Host Configuration for IPv6		Any
⊘ 5	Core Network - Router Advertisement Guard		Any
⊘			
➡ 6	Core Network - Neighbor Discovery		Any

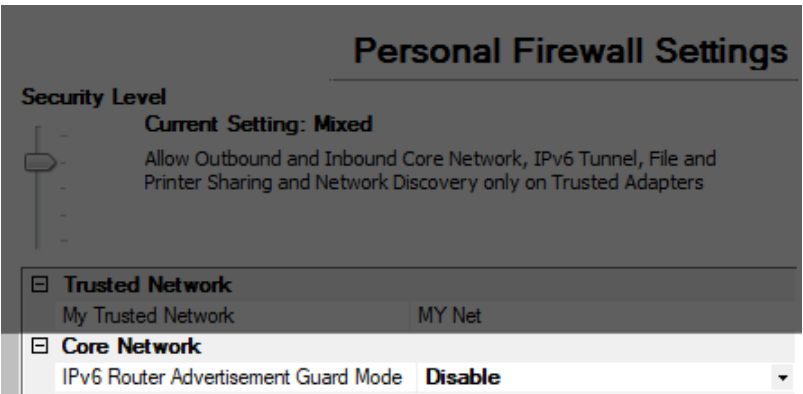
Configuring the IPv6 Router Advertisement Guard

There are different possible configuration modes for the IPv6 Router Advertisement Guard.

The first configuration mode sets **Personal Firewall Settings > Core Network > IPv6 Router Advertisement Guard Mode** to **Block all Router Advertisements**. This blocks all incoming RA messages. The inbound rule **Core Network - Router Advertisement Guard** is set to **Block All** and a log entry is generated to the **Firewall History** for every blocked RA message.



The second configuration mode sets **Personal Firewall Settings > Core Network > IPv6 Router Advertisement Guard Mode** to **Disable**. This allows all incoming RA messages. The inbound rule **Core Network - Router Advertisement Guard** is set to **Pass**. Incoming RA messages are still logged in the **Firewall History**.





Switching to a ruleset, e.g., by activating quarantine, while the Router Advertisement Guard is set to **Disable** or **Block all**, triggers clearance of the list of known routers and prefixes. Thus, when loading a new ruleset with configured Router Advertisement Guard, the system must re-learn the routers and their advertised prefixes.

The next step is to activate the IPv6 Router Advertisement Guard for each access rule it is needed in by selecting the **Router Advertisement Guard** check box.

Monitoring the IPv6 Router Advertisement Guard

Rules that the IPv6 Router Advertisement Guard is active in are marked with a corresponding symbol within the ruleset overview, as can be seen in the **ALL** rule in the following illustration:

LOCAL (2)			
	24 Internet	localIP	Any
	25 ALL	localIP	Any

As soon as the IPv6 Router Advertisement Guard is active, a corresponding text is displayed within the firewall's **Summary** overview, either displaying that the guard is only active or in **Block all** mode. Furthermore, by clicking **Alt key > View > Route Advertise List**, information about all received routes and a list of the allowed MAC addresses can be displayed.

Connections blocked by the IPv6 Router Advertisement Guard are logged by generating a corresponding entry within the Info column in the **Firewall History**.

Figures

1. ra_01.png
2. ra_02.png
3. ra_03.png
4. ra_rule_01.png
5. ra_rule_02.png
6. ra_settings_01.png
7. ra_settings_02.png
8. ra_rule_03.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.