How The RX Firewall Works

John M - 2019-12-23 - 5/10RX Routers

Firewall Overview

The RX Firewall is designed to block unauthorized access while permitting authorized communications. It is a device or set of devices which is configured to permit or deny computer applications based upon a set of rules and other criteria. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially internal secure networks or intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

There are five types of firewalls that have played significant roles as the firewall category has evolved:

- Packet filtering firewalls. ...
- Circuit-level gateways. ...
- Stateful inspection firewalls. ...
- Application-level gateways. ...
- Next-gen firewalls.

The RX firewall is a Stateful Inspection Firewall implementation. Stateful Inspection is a firewall technique used to control network access by tracking the state and type of traffic traversing the interface. Allowing packets to pass or be denied based on the source, destination Internet Protocol (IP) addresses, protocols, ports or session status.

Network layer firewalls define filtering rule sets, which provide highly efficient security mechanisms.

Firewall Packet Flow

The default state of the INOS Firewall is that Stateful inspection is disabled for each IP interface. An IP interface is defined as an Ethernet Port, a WAN IP/DLCI or a PPP connection.

The firewall is enabled or disabled globally for the RX. It is disabled by default. The user must classify each of the configured IP interfaces by assigning a security level. These security levels are assigned numerically, 0 is fully trusted, 100 is fully not trusted and 50 is DMZ trusted or not based on the interface that traffic from the interface is bound for. After the firewall is enabled on an INOS device, the default behavior of the firewall with NO rules defined:

- REJECT all Inbound IP packets on untrusted interfaces
- PERMIT all Outbound IP packets on untrusted interfaces tracking the session information to setup a temporary rule to allow inbound packets that match the session
- REJECT all Inbound IP packets on DMZ interfaces that would be routed to trusted interfaces
- PERMIT all Inbound IP packets on DMZ interfaces that would be routed to untrusted interfaces
- PERMIT all Outbound IP packets on DMZ interfaces that would be routed from trusted interfaces
- REJECT all Outbound IP packets on DMZ interfaces that would be routed from untrusted interfaces
- PERMIT all Inbound IP packets on trusted interfaces that would be routed to any interfaces
- PERMIT all Outbound IP packets on trusted interfaces that would be routed to untrusted interfaces

To restate this, when an interface has packet filtering enabled all packets originating externally to the RX/INOS system are considered inbound packets and are rejected by default. Any packets that originate within the RX/INOS system or pass through the RX/INOS system intended to exit via that interface are considered outbound packets and are allowed to leave the interface by default.

So the default actions for packet filtering is for Inbound packets to be rejected by the default deny all rule and Outbound packet are permitted as there are NO default rules for outbound.

Firewall Configuration

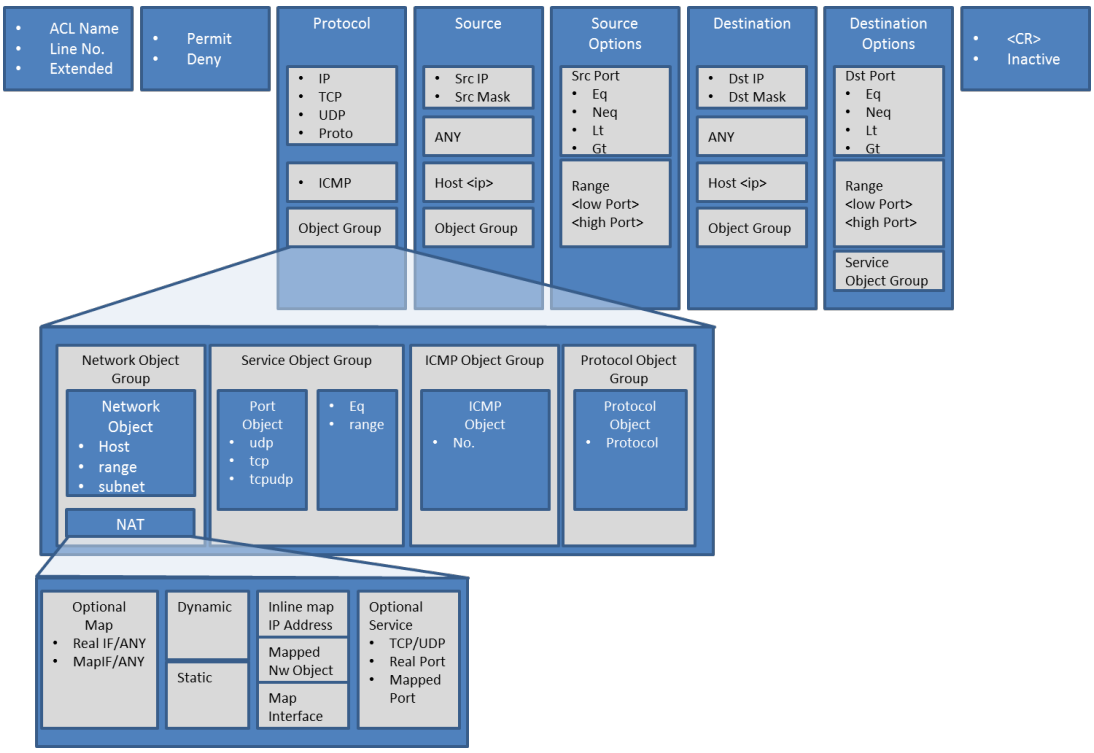
The INOS RX firewall works in 3 modes:

1. **Firewall Disabled**
    1. In this case, all inbound, outbound and control (including 10RX management)

traffic is allowed.
    2. ACLs can be configured at this instant but will not take into effect till firewall is enabled.
2. **Firewall enabled with default rules**
    1. In this case the **security level** configured on an interface decides which traffic is allowed and which is denied.
        - Security value is assigned to an interface.
        - It has a range from 0 to 100.
        - Default value of security level is 50 can also be called DMZ.
        - A security value indicates the trust level of an interface. Lower the value, lower is the trust level.
        - Examples:
            1. Interface towards internal (or protected) network is given a higher value, say 90. Ex. Gig 3/1
            2. Interface towards public (or internet) network is given a lower value, say 10. Ex. Fr-pvc 1
    2. Traffic is always allowed to pass from a higher security interface to a lower security interface.
        1. In the above example, traffic coming from gig3/1 and going to fr-pvc1 would by default be allowed to go out.
        2. Traffic coming from Fr-pvc 1 and going to gig3/1 would by default be denied.
        3. Security level is always relative with respect to the two interfaces that are exchanging traffic.
3. **Firewall enabled with user specified rules**
    1. RX provides option to create different firewall profiles under the name **Firewall-NAT-Group**.
        - ***At any instance user can create multiple Firewall-NAT-Groups, but only one group can be activated at a time.***
4. RX provides option to attach multiple **Access-Groups** to each Firewall-NAT-Group
    - Access-group uniquely applies ACL rules to traffic for a specific direction (inbound/outbound) on a specific interface (if name).
    - Unique Access-group is also required to specify ACL rules for control plane traffic. (ie. the traffic meant for the 10RX itself).
    - ***RX does not allow specifying multiple access-groups for the same combination of direction and interface.***
    - ***RX allows specifying multiple access-groups for the same direction but different interfaces.***
5. RX provides option to create multiple **rules** within an **ACL** and use it as an access-group.
    - Rules can be added in an ACL to permit or deny specific type (s)

(ip/tcp/udp/icmp/<protocol>) of traffic coming from a source (any/ip/port) and going for a specific destination (any/ip/port).
    - Rules can be arranged in the order of their priority within an ACL by specifying the line number for each rule.
    - Permit/deny property or the combination of source-destination can be modified for any rule by specifying the line number of the rule within that ACL.
    - ***RX does not allow modifications to the ACL or any of its rules while it is being used in a firewall-nat-group.*** In order to do that, user needs to:
        1. Deactivate the fw-nat-group
        2. Remove the ACL from fw-nat-group
        3. Modify the ACL
        4. Reattach the ACL to fw-nat-group
        5. Re-activate the fw-nat-group
6. RX provides option to create and associate object groups with an **ACL rule**.
    - Network Object Groups include:
        1. IP address (host)
        2. Network
        3. Network Range
    - Service Object Groups include:
        - TCP/UDP Port number
        - Range of ports
    - Protocol Object Groups include:
        - Protocol Number (ex. IP/tcp/udp/etc)

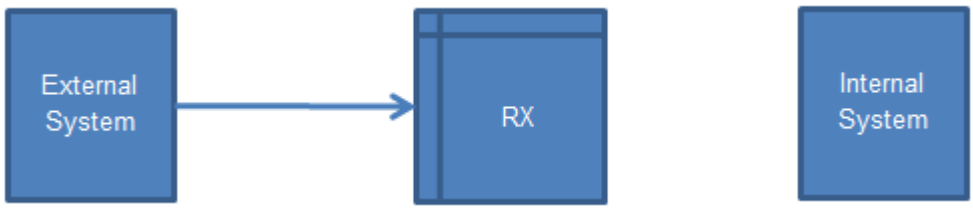
(Attached is the diagram that depicts various object groups and their position with in an ACL rule))



Firewall Operation Summary

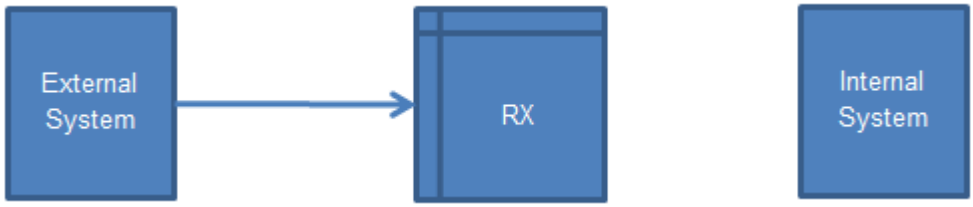
In summary all IP communications are bidirectional in nature so a request for Information followed by an answer in return. A Stateful Inspection firewall with the default configuration of no user defined rules such as the RX and at least two IP Interfaces (Ethernet, PPP or WAN IP), one configured as LAN/Trusted and a second configured as External/Untrusted. When the firewall is enabled globally on an RX/INOS system the firewall will allow all packets to leave from the safe LAN side of the External/Untrusted Interface (OUTGOING) and block packets that are arriving at that External/Untrusted Interface (INCOMING). There is an exception to the deny all packets rule for packets arriving at the External/Untrusted Interface (INCONING). If the packet arriving at the External/Untrusted Interface is a reply to a packet that originated from the RX (a session request considered as OUTGOING) the RX will have created a temporary rule to allow replies for this session so the packets are passed back to the originating application on the LAN/Trusted side of the Interface allowing for the conversation to continue. So for packets that wholly originate from the External/Untrusted side of the Interface half of the bidirectional conversation is closed off, thus NO conversation takes place.

Example One:



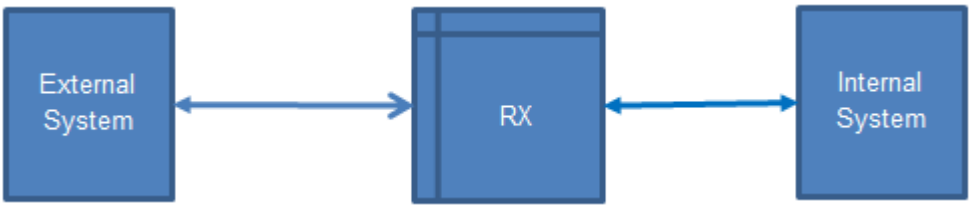
- The User has enabled the firewall globally on the RX the external system connects to.
- The External System tries to start an HTTP/HTTPS connection to the Internal System
- The Firewall rejects the first packet received to start the connection and communication ends

Example Two:



- The User has enabled the firewall globally on the RX the external system connects to.
- The External System tries to start an HTTP/HTTPS connection to the DX Web Server
- The Firewall rejects the first packet received to start the connection and communication ends

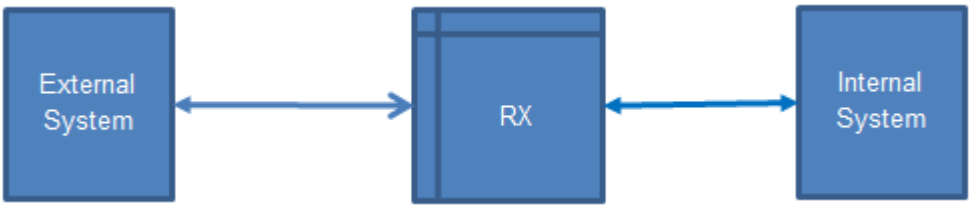
Example Three:



- The User has enabled the firewall globally on the RX the external system connects to.
- The Internal System tries to start an HTTP/HTTPS connection to the External System
- The Firewall passes the first packet received from the Internal System to start the communication and sends it to the External System
- The RX creates a temporary rule to allow replies for this HTTP/HTTPS session only
- The External System receives the first packet and replies

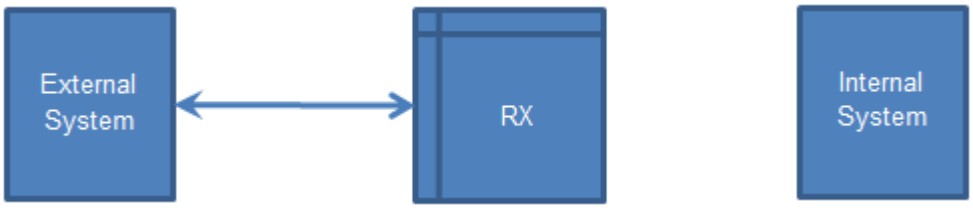
- The RX allows the reply packet and the communication continues.
- Once the HTTP/HTTPS session ends the temporary rule is disabled and no further traffic is allowed from the External System

Example Four:



- The RX has enabled the firewall on the Interface the external system connects to.
- An INBOUND firewall rule is created for HTTP/HTTPS protocol and IP addresses of both the External System as source address and Internal System as destination address
- The External System tries to start an HTTP/HTTPS connection to the Internal System
- The Firewall accepts the first packet received to start the connection, the Internal System also receives the packet and replies
- An HTTP/HTTPS connection is established and the External System has access to the Web Server of the Internal System

Example Five:



- The RX has enabled the firewall on the Interface the external system connects to.
- An INBOUND firewall rule is created for HTTP/HTTPS protocol and IP addresses of both the External System as source address and RX management IP as destination address
- The External System tries to start an HTTP/HTTPS connection to the DX Web Server
- The Firewall accepts the first packet received to start the connection and the DX web server also receives this packet and replies
- An HTTP/HTTPS connection is established and the External System has access to the Web Server of the DX

NOTE: For all of these examples OUTBOUND rules are NOT required do to the default action of all packets allowed.