Policy Based Routing (PBR) Settings on ISA500 Series Integrated Security Appliances

Objective

Policy-Based Routing (PBR) directs traffic to different WAN connections based on sources, destinations, services, source VLAN, and Differentiated Services Code Point (DSCP). PBR can be used to send more critical data such as voice and video to a faster WAN connection and direct less critical data such as email to a slower WAN connection. This setup makes the overall network more efficient.

This article explains how to configure PBR settings on the ISA500 Series Integrated Security Appliance.

Applicable Devices

- ISA500 Series Integrated Security Appliances

Software Version

- v1.1.14

Policy-Based Routing Settings

Primary Configuration

This procedure explains how to configure the primary settings for PBR.

Step 1. Use the ISA500 Series Configuration Utility to choose Networking > Routing > Policy Based Routing from the left side navigation menu.

Step 2. In the Policy Based Routing field, click a radio button.

- On — This option enables PBR.
• Off — This option disables PBR.

Step 3. In the Policy Based Routing Rules table, click Add. The Policy Based Routing Rule - Add/Edit window appears:

Step 4. From the From drop-down list, choose a VLAN from which the traffic to be directed comes, or choose Any to direct traffic from any VLAN.

Step 5. From the Service drop-down list, choose an option.

• All Traffic — This option directs traffic regardless of service that the traffic performs.

• Create a new service — This option allows you to create a new service on which traffic filters are based. For configuration of this option, refer to the Create a New Service subsection.

• Service Objects — This option lists pre-configured services that you can choose.

Step 6. From the Source IP drop-down list, choose an option.

• Any — This option directs traffic regardless of the source IP address of the traffic.

• Create a new address — This option allows you to create a new source IP address on which traffic filters are based. For configuration of this option, refer to the Create a New IP Address Object subsection.

• IP Address Objects — This option lists pre-configured IP addresses and ranges that you can choose.

Step 7. From the Destination IP drop-down list, choose an option.

• Any — This option directs traffic regardless of the destination IP address of the traffic.

• Create a new address — This option allows you to create a new destination IP address on which traffic filters are based. For configuration of this option, refer to the Create a New IP Address Object subsection.

• IP Address Objects — This option lists pre-configured IP addresses and ranges that you can choose.
Step 8. From the DSCP drop-down list, choose a level of priority for which the traffic is filtered. Choose Any to filter traffic regardless of DSCP value.

Step 9. From the Route to drop-down list, choose a WAN connection to which the filtered traffic is directed.

Step 10. In the Failover field, click a radio button.
  • On — This option directs all traffic to the WAN connection that functions when the other WAN connection fails.
  • Off — This option does not direct traffic to the WAN connection that functions when the other WAN connection fails.

Step 11. Click OK. The Policy Based Routing window reappears.

Step 12. Click Save.

To know the current routing table used by the device refer to this article, View the Routing Table on ISA500 Series Integrated Security Appliances.

Create a New Service

This procedure explains how to create a new service from the Policy Based Routing Rule - Add/Edit window.

Step 1. From the Service drop-down list in the Policy Based Routing Rule - Add/Edit window, choose Create a new service. The Service/Add window appears:

Service / Add

- Name: EmailService
- Protocol: UDP
- Port Range Start: 20 (Range: 1-65535)
- Port Range End: 21 (Range: 1-65535)

Step 2. In the Name field, enter a name for the service.

Step 3. From the Protocol drop-down list, choose a protocol for the service to perform.
• TCP — Transmission Control Protocol (TCP) is a transport protocol that sends traffic and also checks to make sure the traffic arrived completely in the correct order. TCP, though, is slower than UDP because of the check process. TCP should be used to send data that requires reliable transport.

• UDP — User Datagram Protocol (UDP) is a transport protocol that sends traffic but does not check to make sure the traffic arrived completely in the correct order. The advantage of UDP is that it is faster than TCP since it does not double check the messages. UDP should be used when messages do not require reliable transport.

• both(TCP/UDP) — This option sets the service to perform both UDP and TCP.

• ICMP — Internet Control Message Protocol (ICMP) is a protocol that sends error and control messages. A ping is an example of ICMP.

Service / Add

- Name: EmailService
- Protocol: UDP

- Port Range Start: 20 (Range: 1-65535)
- Port Range End: 21 (Range: 1-65535)

Step 4. If you choose both(TCP/UDP), TCP, or UDP in Step 3, enter the first port in the range of ports to which the service applies in the Port Range Start field, and enter the last port in the range of ports in the Port Range End field. For a single port, enter the same number in both fields.
Step 5. If you choose ICMP in Step 3, enter the service ICMP type value in the ICMP Type field. The ICMP type value is the first eight bits of ICMP header and indicates what type of message the ICMP packet is.


Create a New IP Address Object

This procedure explains how to create a new IP address object from the Policy Based Routing Rule - Add/Edit window.

Step 1. If you are directed from Step 6 of the Primary Configuration subsection, choose Create a new address from the Source IP drop-down list. If you are directed from Step 7 of the Primary Configuration subsection, choose Create a new address from the Destination IP drop-down list. In either case, the Address/Add window appears:
Step 2. In the Name field, enter a name for the IP address or addresses.

Step 3. From the Type drop-down list, choose what type of address the IP address is.

- Host — This option sets the IP address to the address of a single host.
- Network — This option sets the IP address to the address of an entire network.
- Range — This option sets the IP address to a range of addresses.
Step 4. (Optional) If you chose Host from the Type drop-down list, enter the host IP address in the IP address field.

Step 5. (Optional) If you chose Network from the Type drop-down list, enter the network IP address in the IP address field, and enter the network subnet mask in the netmask field.
Step 6. (Optional) If you chose Range from the Type drop-down list, enter the first address in the IP address range in the Starting IP Address field, and enter the last address in the IP address range in the Ending IP Address field.