Using Balabit's Privileged Session Management in a single-interface transparent mode

June 19, 2018

Abstract

Single-interface transparent mode Configuration Guide for Balabit's Privileged Session Management (PSM, formerly called SCB)

Table of Contents

1. Overview

This short document is about a special implementation of the Balabit's Privileged Session Management. This makes it possible to deploy the device without changing the network topology, but keeping all the advantages of the transparent mode of the PSM.

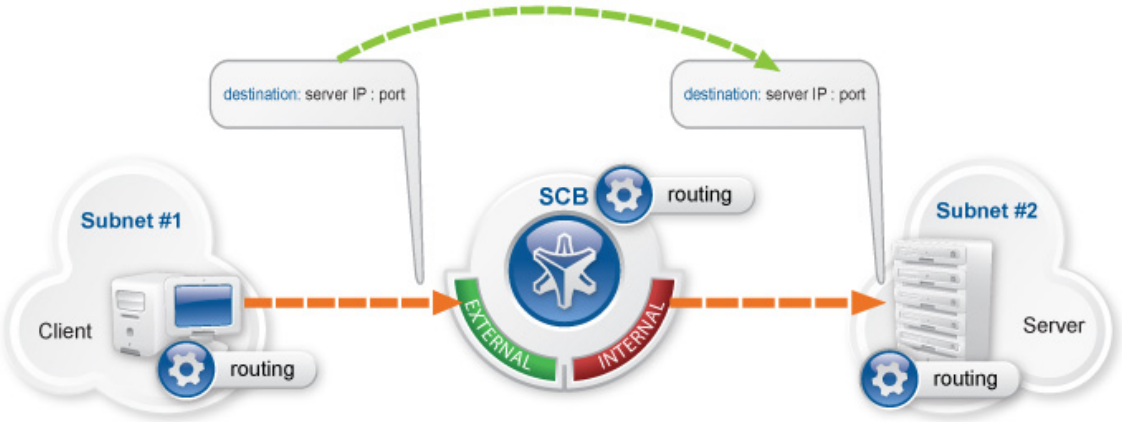
All questions, comments or inquiries should be directed to <info@balabit.com> or by post to the following address: One Identity LLC 1117 Budapest, Alíz Str. 2 Phone: +36 1 398 6700 Fax: +36 1 208 0875 Web: *https://www.balabit.com/*

2. Introduction

The Balabit's Privileged Session Management connection policies can work in different network models to make it easy to integrate it into an existing network. These two modes are transparent, and non-transparent modes (for details on modes of operation, see *Section 2.7, Modes of operation* in *The Balabit's Privileged Session Management 5 LTS Administrator Guide*). The aim is usually the transparent implementation. Although the non-transparent mode can provide some transparency, it is not the best to be used for that purpose.

For the easy-to-deploy and totally transparent solution the transparent mode would be the best. This mode requires integrating PSM in the network level, so all the administrative traffic could pass the box to make it controllable and auditable (for details and illustrations on transparent mode, see *Section 2.7.1, Transparent mode* in *The Balabit's Privileged Session Management 5 LTS Administrator Guide*).

Figure 1. PSM in transparent mode



In most cases it is not possible, or not optimal to integrate PSM into the network as in the abovementioned example, because it would require significant changes to the network topology, and PSM could act as a single point of failure. However, it is possible to use PSM in transparent mode transparently without changing the network layout, with a few additional configuration steps in some of the active network devices (firewalls or routers) and the PSM itself. The following sections will describe this in detail.

3. Inline routing scenario in PSM

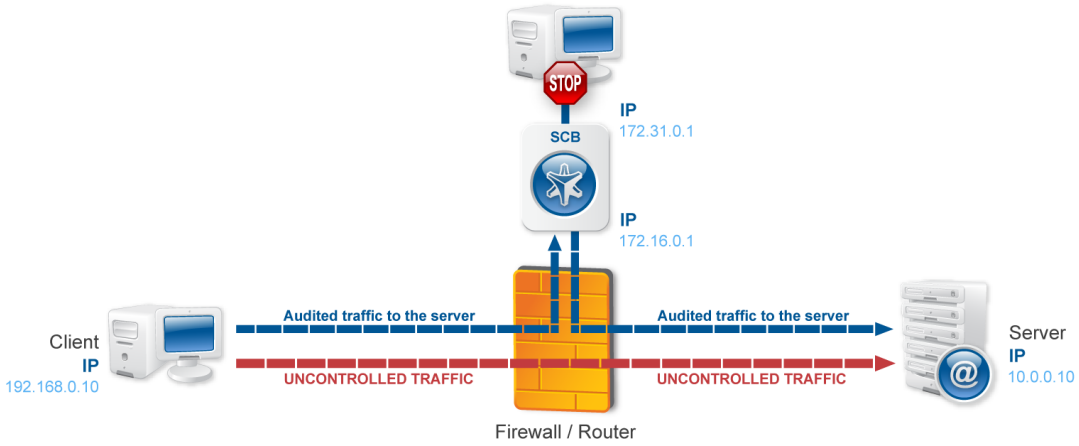
PSM has two physical network interfaces that are normally used for production (monitored) traffic: “External” and “Internal”. The function of these interfaces is interchangeable, the names are only used in this document for easier identification. PSM is implemented as it is visible on Figure *PSM in transparent mode*. In this case the connections are coming from the client's network (define it as 192.168.0.0/24) and heading towards the server's network (define it as 10.0.0.0/24). The routing on the client is configured so that it uses PSM as a gateway, when the server network is accessed. The servers are configured so that they send the answers into the client network through PSM. Also, all the networks and gateways are defined in the routing table of PSM, to send the traffic out on the appropriate interface.

PSM does not check whether the client is coming from the “External” interface or if the connections are going out on the “Internal” interface. Because of this, it is possible to create a topology, where both the clients and the servers are located on the “External” side.

4. Single-interface transparent mode

Single-interface transparent mode is similar to transparent mode, but both client-side and server-side traffic use the same interface. An external device — typically a firewall or a router (or a layer3 switch) — is required that actively redirects the audited traffic to PSM. To accomplish this, the external device must support advanced routing (also called policy-based routing or PBR). For details on configuring an external devices to work with PSM in single-interface transparent mode, see *Appendix A, Configuring external devices* in *The Balabit's Privileged Session Management 5 LTS Administrator Guide*.

Figure 2. PSM in single-interface transparent mode



Advantages:

The advantages of using the single-interface transparent mode are:

- Totally transparent for the clients, no need to modify their configuration
- The network topology is not changed
- Only the audited traffic is routed to PSM, production traffic is not

Disadvantages:

The disadvantages of using the single-interface transparent mode are:

- PSM acts as a man-in-the-middle regarding the connection between the client and the target server. Instead of a single client-server connection, there are two separate connections: the first between the client and PSM, and a second between PSM and the server. Depending on how you configure PSM, the source IP in the PSM-server connection can be the IP address of PSM, or the IP address of the client. In the latter case — when operating in transparent mode (including single-interface transparent mode) — PSM performs IP spoofing. Consult the security policy of your organization to see if it permits IP spoofing on your network.
- Traffic must be actively routed to PSM using an external device, consequently a network administrator can disable PSM by changing routing rules.
- When adding a new port or subnet to the list of audited connections, the configuration of the external device must be modified as well.

- A network administrator can (intentionally or unintentionally) easily disable monitoring of the servers, therefore additional measures have to be applied to detect such activities.

5. Advanced or Policy-based routing

Usually there is a central network device somewhere close to the location where PSM is planned to be implemented. This central network device (a router or firewall) can facilitate improving the previous layout into a real working scenario, as it is visible on Figure *PSM in single-interface transparent mode*.

There is a router (or firewall, or layer3 switch) between the zones, and PSM is installed into a new, separated network. Here, all the devices (including PSM) are configured to use the central router as their default gateway. So, if a client is trying to reach a server, the connection is going through the router. However, PSM is not able to audit the remote administration with this configuration.

Here comes the router into the play. For example if we have to audit RDP connections, the router can be configured to route all the connections to PSM (connections are coming from the client network, going to the server network, and the destination port is `3389`). With this configuration, all RDP connections are “redirected” to PSM. It sends the traffic back to the router, which then sends the connection to its original destination, to the server zone. PSM receives a connection on its “External” interface, and it routes it back on the same interface. It creates a “hook” in the network traffic, but it also makes the connection totally transparent: the client IP can be the same (optional), and the client does not have to know anything about PSM. Non-administrative traffic can also be unaffected, as we can selectively route the necessary traffic to PSM.

The configuration of the router can vary depending on the type of the router. The following two procedures describe configuration scenarios for a Linux and a Cisco router.

6. Example scenarios

On the PSM side, no special configuration is required. PSM has to be in transparent mode. The “External” interface has to be configured correctly, and has to be connected to the router. On the “Internal” interface any IP address can be configured that is not used on the network, as we will not use this interface at all. The default gateway should be the router.

6.1. Procedure – Configuring advanced routing on Linux

Purpose:

To configure a Linux-based router to redirect selected traffic to PSM instead of its original destination, complete the following steps. This procedure should work on most modern Linux-based routers, including Check Point® firewalls.

Prerequisites:

The router must have the *iptables* and *ip* tools installed.

Steps:

Step 1. Create the packet filter rules that will mark the connections to be sent to PSM using the CONNMARK feature of iptables. Mark only those connections that must be redirected to PSM.

```
# iptables -t mangle -I PREROUTING -i <interface-facing-the-clients> -p tcp
 -d <network-of-the-servers> --dport <port-to-access> -j CONNMARK --set-mark
 1
```

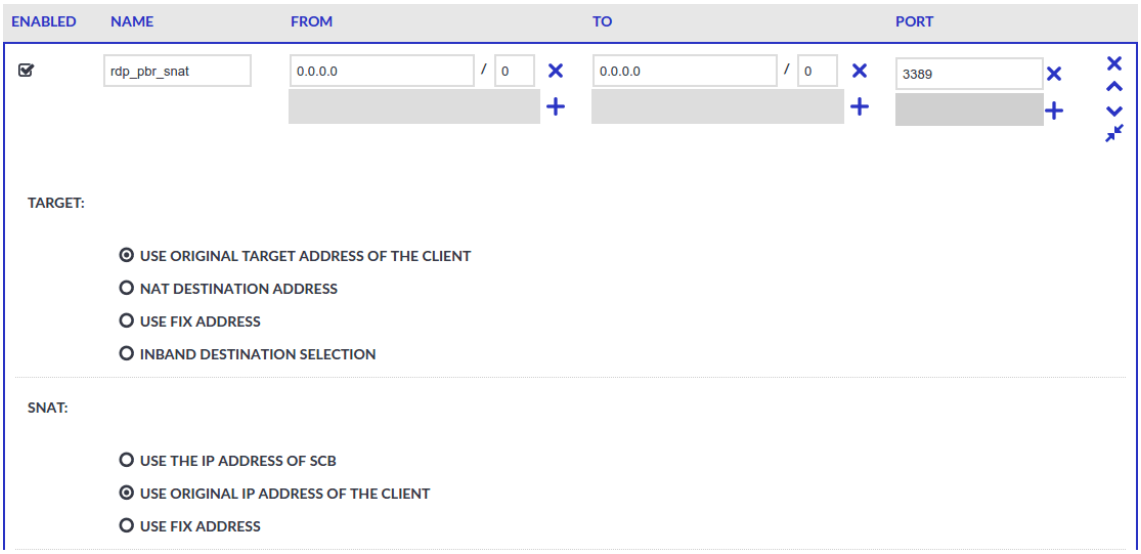
Example 1. Setting up a connection mark for Linux policy routing
For example, if the network interface of the router that faces the clients is called *eth0*, the servers are located in the *10.0.0.0/24* subnet, and the clients access the servers using port *3389* (the default port of the RDP protocol), then this command looks like:

```
# iptables -t mangle -I PREROUTING -i eth0 -p tcp -d 10.0.0.0/24 --dport 3389 -j
 CONNMARK --set-mark 1
```

Step 2. Create a rule that redirects the answers of the servers to PSM. That way both the client-to-server and the server-to-client traffic is routed to PSM.

Note
This step is only required if you want to use Source NAT (IP Spoofing) instead of PSM’s address towards the monitored servers.

*Figure 3. **Control > Connections** — Using SNAT*




```
# iptables -t mangle -I PREROUTING -i <interface-facing-the-servers> -p tcp
 -s <network-of-the-servers> --sport <port-to-access> -j CONNMARK --set-mark
 1
```

Step 3. Convert the CONNMARK marks to MARK:

```
# iptables -t mangle -A PREROUTING ! -i <interface-facing-the-scb> -m connmark
 --mark 1 -j MARK --set-mark 1
```

Warning
This rule must be placed after the CONNMARK rules.

Step 4. Add the table name to the `/etc/iproute2/rt_tables` of the router. Use the following format (for details on routing tables, see for example the *Guide to IP Layer Network Administration with Linux*):

```
103 scb
```

Step 5. Create a routing table that has a single entry with a default route to PSM:

```
# /sbin/ip route add default via <ip-address-of-PSM> table scb
```

Step 6. Create a routing rule that selects the routing table called *scb*, if the connection is marked.

```
# /sbin/ip rule add from all fwmark 1 table scb
```

Step 7. If PSM is configured to spoof the IP address of the clients on the server side (that is, the **SNAT > Use original IP address of the client** option of the connection policies is selected), enable spoofing on the router for the interface connected to PSM.

```
# echo 0 > /proc/sys/net/ipv4/conf/<interface-facing-PSM>/rp_filter
# echo 0 > /proc/sys/net/ipv4/conf/all/rp_filter
```

Expected result:

The traffic from the clients targeting the specified port of the servers is redirected to PSM. Therefore, PSM can be configured to control and audit this traffic.

6.2. Procedure – Configuring advanced routing on Cisco routers

Purpose:

To configure a Cisco router to redirect selected traffic to PSM instead of its original destination, complete the following steps. This procedure should work on most modern Cisco IOS releases but was specifically tested on IOS version 12.3.

Steps:

Step 1. Create an ACL (Access Control List) entry that matches the client and server subnets and the to-be-audited port. Keep in mind that whatever is permitted by this ACL is what will be matched, so make sure that the scope of the ACL entry is narrowed down as much as possible.

```
#(config) ip access-list extended ssh-inbound
#(config-ext-nacl) permit tcp <src net> <src mask> <dst net> <dst mask> eq
<dst port>
```

Example 2. Configuring an ACL entry for Cisco policy routing
For example, if the clients are in the *192.168.0.0/24* subnet, the servers are located in the *10.0.0.0/24* subnet, and the clients access the servers using port *22* (the default port of the SSH protocol), then the permit clause should be:

```
#(config-ext-nacl) permit tcp 192.168.0.0 0.0.0.255 10.0.0.0 0.0.0.255 eq 22
```

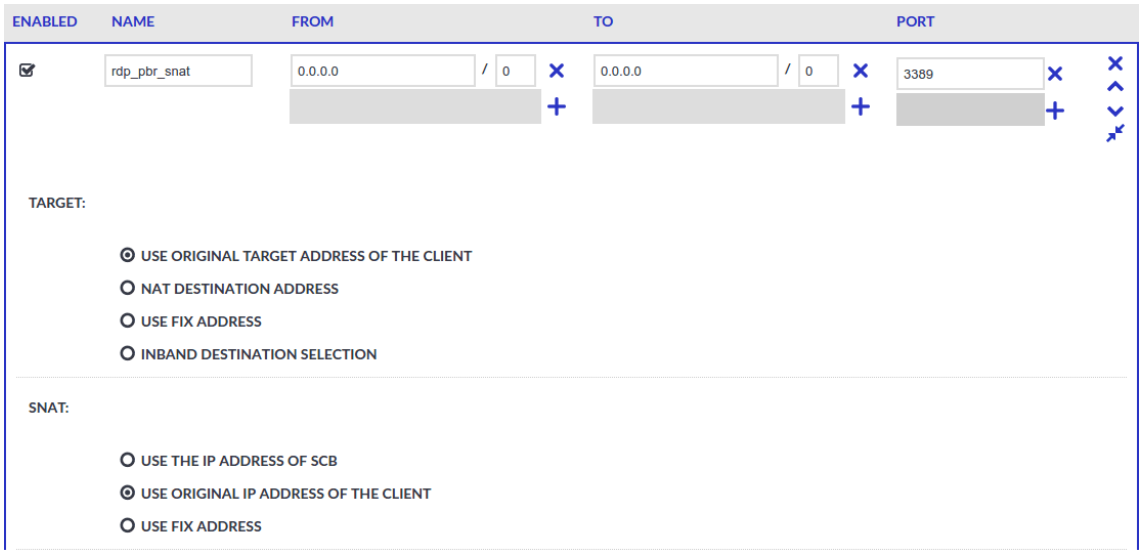
Tip
Cisco ACLs use inverse netmasks for defining network addresses. To calculate an inverse mask given a subnet mask, simply subtract each octet value from 255.

Step 2. Create an ACL entry that matches the reply packets coming from the server zone and targeted at the client zone to make sure that replies are reaching the PSM.

```
#(config) ip access-list extended ssh-outbound
#(config-ext-nacl) permit tcp <dst net> <dst mask> eq <dst port> <src net>
<src mask>
```

Note
This step is only required if you want to use Source NAT (IP Spoofing) instead of PSM's address towards the monitored servers.

*Figure 4. **Control > Connections** — Using SNAT*



Example 3. Configuring an ACL entry for reply packets with Cisco policy routing
In case of the example in step 1, the permit clause should be:

```
#(config-ext-nacl) permit tcp 10.0.0.0 0.0.0.255 eq 22 192.168.0.0 0.0.0.255
```

Step 3. Create a route-map entry. It controls which packets are affected by policy routing and where they should be forwarded to. The *match* commands specify the conditions under which policy routing occurs. The *set* commands specify the routing actions to perform if the criteria enforced by the *match* commands are met. A new route-map can be defined as follows:

```
#(config) route-map scb-inbound
```

Step a. Set your route-map to match the traffic in ACL *ssh-inbound*:

```
#(config-route-map) match ip address ssh-inbound
```

Step b. Set an action on the matching traffic. Define a next-hop entry to redirect the traffic to the PSM.

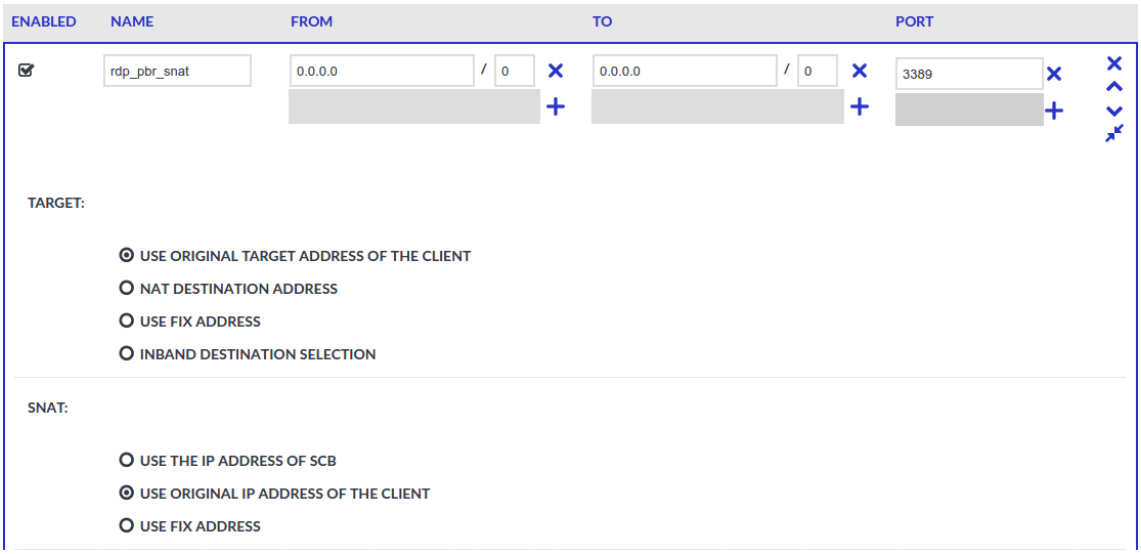
```
#(config-route-map) set ip next-hop <PSM IP address>
```

Step 4. Create another route-map that controls the reply packet flow.

```
#(config) route-map scb-outbound
#(config-route-map) match ip address ssh-outbound
#(config-route-map) set ip next-hop <PSM IP address>
```

Note
This step is only required if you want to use Source NAT (IP Spoofing) instead of PSM's address towards the monitored servers.

*Figure 5. **Control > Connections** — Using SNAT*



Step 5. Apply the route-map to the appropriate interfaces.

Step a. First, add the ssh-inbound route-map entry to the interface facing the clients:

```
#(config) interface <interface-facing-the-clients>
#(config-if) ip policy route-map scb-inbound
```

Step b. Then add the ssh-outbound route-map entry to the interface facing the servers:

```
#(config) interface <interface-facing-the-servers>
#(config-if) ip policy route-map scb-outbound
```

Expected result:

The traffic from the clients targeting the specified port of the servers is redirected to PSM. Therefore, PSM can be configured to control and audit this traffic.

The full configuration for the above topology:

```
! interface facing the clients
interface FastEthernet0/0
 ip address 192.168.0.254 255.255.255.0
 ip policy route-map scb-inbound
 duplex full
 speed auto
 no mop enabled

! interface facing the SCB
```

```
interface FastEthernet0/1
 ip address 172.16.0.254 255.255.255.0
 duplex full
 speed auto
 no mop enabled

! interface facing the servers
interface FastEthernet1/0
 ip address 10.0.0.254 255.255.255.0
 ip policy route-map scb-outbound
 duplex full
 speed auto
 no mop enabled

! access lists matching the server and client subnets and the SSH port -
incoming packets
ip access-list extended ssh-inbound
 permit tcp 192.168.0.0 0.0.0.255 10.0.0.0 0.0.0.255 eq 22
! access lists matching the server and client subnets and the SSH port -
reply packets
ip access-list extended ssh-outbound
 permit tcp 10.0.0.0 0.0.0.255 eq 22 192.168.0.0 0.0.0.255

! policy routing entry matching on the incoming SSH connections and
! redirecting them to the SCB external interface
route-map scb-inbound permit 10
 match ip address ssh-inbound
 set ip next-hop 172.16.0.1

! the following part is only required for SNAT-based SCB configuration
! policy routing entry matching on the SSH reply packets and
! redirecting them to the SCB external interface
route-map scb-outbound permit 10
 match ip address ssh-outbound
 set ip next-hop 172.16.0.1
```

6.3. Procedure – Configuring advanced routing on Cisco ASA firewalls

The configuration of Cisco ASA firewalls follows the same rules as the Cisco router configuration, however the commands are slightly different.

Warning
Source NAT (IP spoofing) is not supported in case of Cisco ASA firewalls.

This means that with Cisco ASA, you cannot spoof the source IP towards the destination servers, therefore the source of the connections will be SCB's IP address.

Purpose:

To configure a Cisco ASA Firewall to redirect selected traffic to SCB instead of its original destination, complete the following steps. This procedure should work on most modern Cisco ASA software releases, but was specifically tested on Cisco Adaptive Security Appliance Software Version 9.6(2)3

Steps:

Step 1. Define network objects that match the subnets or hosts that you want to monitor:

```
!Define SSH and RDP hosts/subnets as desired below
object network SSHHosts
subnet <SSHHosts Subnet IP> <SSHHosts Subnet Netmask>
object-group network SSHtoSCB
network-object object SSHHosts
object network RDPHost
host <RDPHost IP>
object-group network RDPtoSCB
network-object object RDPHost
```

Step 2. Create an ACL (Access Control List) entry that matches the objects above

```
!Allow RDP and SSH and their reply packets to SCB
access-list acl_pbr_ToSCB extended permit object rdp3389 any object-group
RDPtoSCB
access-list acl_pbr_ToSCB extended permit object rdp3389-response object-group
 RDPtoSCB any
access-list acl_pbr_ToSCB extended permit object ssh22 any object-group
SSHtoSCB
access-list acl_pbr_ToSCB extended permit object ssh22-response object-group
 SSHtoSCB any
```

Keep in mind that whatever is permitted by this ACL is what will be matched, so make sure that the scope of the ACL entry is narrowed down as much as possible.

Tip
Cisco ACLs use inverse netmasks for defining network addresses. To calculate an inverse mask given a subnet mask, simply subtract each octet value from 255.

Step 3. Create a route-map entry. It controls which packets are affected by policy routing and where they should be forwarded to. The `match` commands specify the conditions under which policy routing occurs. The `set` commands specify the routing actions to perform if the criteria enforced by the `match` commands are met. A new route-map can be defined as follows:

```
!Define routing to SCB
route-map ToSCB permit
 match ip address acl_pbr_ToSCB
 set ip next-hop <SCB IP>
```

Apply the route-map to the appropriate interfaces.

```
!Set it on interface as needed
interface <interface-facing-to-the-servers>
 ip policy route-map ToSCB
```

Expected result:

The traffic from the clients targeting the specified port of the servers is redirected to PSM. Therefore, PSM can be configured to control and audit this traffic.

The full configuration for the above topology:

```
!
!Define SSH and RDP hosts/subnets as desired below
object network SSHHosts
 subnet <SSHHosts Subnet IP> <SSHHosts Subnet Netmask>
object-group network SSHtoSCB
 network-object object SSHHosts
object network RDPHost
 host <RDPHost IP>
object-group network RDPtoSCB
 network-object object RDPHost
!
!Allow RDP and SSH and their reply packets to SCB
access-list acl_pbr_ToSCB extended permit object rdp3389 any object-group
RDPtoSCB
access-list acl_pbr_ToSCB extended permit object rdp3389-response object-group
 RDPtoSCB any
access-list acl_pbr_ToSCB extended permit object ssh22 any object-group
SSHtoSCB
access-list acl_pbr_ToSCB extended permit object ssh22-response object-group
 SSHtoSCB any
!
!Define routing to SCB
route-map ToSCB permit
 match ip address acl_pbr_ToSCB
 set ip next-hop <SCB IP>
!
!Set it on interface as needed
interface <interface-facing-to-the-servers>
 ip policy route-map ToSCB
```