Systems Engineering
“How to” Guide
Policy Based Routing on ASA for WSA
Transparent Proxy mode
Redirection

Valter Da Costa
Security Solutions Architect
Security Technology Business Unit

December 2015
# TABLE OF CONTENTS

## CONFIDENTIALITY NOTICE

### PURPOSE OF THIS DOCUMENT

- **PRODUCT KNOWLEDGE REQUIREMENTS**
- Configuring ports on the WSA for access
- Traffic Redirection
- Access Log Output

December 2015
CONFIDENTIALITY NOTICE

This document is Cisco Public.

PURPOSE OF THIS DOCUMENT

This guide is intended to explain how to configure the Cisco Adaptive Security Appliance (ASA) to use Policy Based Routing to transparently forward traffic to be processed by the Web Security Appliance (WSA).

PRODUCT KNOWLEDGE REQUIREMENTS

• Cisco Web Security Appliance
• Cisco Adaptive Security Appliance

Transparent Redirection

Confirm the WSA is configured to use a Layer-4 switch or No Device in the Transparent Redirection Device settings, in the Web UI (Under Network TAB)

Configuring ports on the WSA for access

There are cases where the ASA may need to be configured to transparently re-direct HTTP and HTTPS traffic to the WSA when WCCP is not a viable configuration option. Policy Based Routing Policy Based Routing (PBR) is a mechanism by which traffic is routed through specific paths with a specified QoS using ACLs. ACLs let traffic be classified based on the content of the packet’s Layer 3 and Layer 4 headers. This solution allows Internet service providers and other organizations to route traffic originating from various sets of users through well-defined Internet connections.

Policy Based Routing is supported only in the routed firewall mode. Transparent firewall mode is not supported.
Make sure your ASA is running version 9.4. The following command can be used to check the current version:

```bash
> show version
```

snipped output:

```
ciscoasa> show version

Cisco Adaptive Security Appliance Software Version 9.1(1)
Device Manager Version 7.1(3)
Compiled on Wed 28-Nov-12 11:15 PST by builders
System image file is "disk0:/asa911-smp-k8.bin"
```

**Implementation of PBR**

The ASA uses ACLs to match traffic and then perform routing actions on the traffic. Specifically, you configure a route map that specifies an ACL for matching, and then you specify one or more actions for that traffic. Finally, you associate the route map with an interface where you want to apply PBR on all incoming traffic.

**Equal-Access and Source-Sensitive Routing**

This method is recommended if you have multiple WSA and want to provide equal-access and source-sensitive routing. The traffic (HTTP/HTTPS) can be redirected to the proxies (WSA) using a route-map with an access-list.

**Order of Configuration for ASA Policy Based Routing**

* Define an access-list
  - IPv6 ACLs are not supported.
* Create a route map entry
* Define the match criteria to be applied using an access-list
* Indicate where to output packets that pass a match clause of a route map for policy routing
* Configure one or more actions
* Configure an interface and enter interface configuration mode
* Configure policy based routing for through-the-box traffic

**NOTE**

When multiple set actions are configured, PBR will evaluate them in the following order:

```
set ip next-hop verify-availability
set ip next-hop
set ip next-hop recursive
set interface
set ip default next-hop
set default interface
```
Example

interface GigabitEthernet0/0
  nameif outside
  security-level 0
  ip address 192.168.0.9 255.255.255.0

interface GigabitEthernet0/1
  nameif inside
  security-level 100
  ip address 192.168.1.9 255.255.255.0
  policy-route route-map testmap

interface GigabitEthernet0/5
  nameif DMZ
  security-level 100
  ip address 192.168.2.9 255.255.255.0

object network INSIDE_NETWORK
  nat (inside,outside) dynamic interface
object network DMZ_Network
  nat (DMZ,outside) dynamic interface

access-list newtestacl extended permit tcp host 192.168.1.62 any4 eq https log
access-list newtestacl extended permit tcp host 192.168.1.62 any4 eq www log

route-map testmap permit 1
  match ip address newtestacl
  set ip next-hop 192.168.2.37
  set interface inside DMZ

# WARNING: In the above example, if the access-list "newtestacl" with destination "any4\any4\any6" is used as the match criteria for a route map, and applied to any routing protocol it will have no effect. Instead use a standard ACL or an extended ACL without any/any4/any6 in the destination.

# RECOMMENDATION: Unless you have IPv6 hosts, use ANY4 (for IPv4 only).
Although the diagram above shows different network segments, the configuration listed in this document covers a basic scenario on which the WSA will be used to proxy traffic from the inside network. Adding other ACLs and Route-map, will cover other network segments.
Troubleshooting

Various tools can be used to troubleshoot PBR on ASA. Please find some, but not all of the commands below:

**Capture**

Enable packet capture capabilities for packet sniffing and network fault isolation.

capture capture_name [type {asp-drop all [drop-code] | tls-proxy | raw-data | lacp | isakmp [ikev1 | ikev2] | inline-tag [tag] | webvpn user webvpn-user}] [access-list access_list_name] [interface asa_dataplane] [buffer buf_size] [ethernet-type type] [interface interface_name] [reeinject-hide] [packet-length bytes] [circular-buffer] [trace trace_count] [real-time] [trace] [match prot {host source-ip | source-ip mask | any} {host destination-ip | destination-ip mask} [any} {operator port]

Example:

capture IN interface inside match tcp any any eq 80

Reference:
CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide, 9.4

---

**show arp**

To display the Address Resolution Protocol (ARP)

**Packet- tracer**

The trace does policy lookup to test access rules, NAT, routing, and so forth, to see if the packet would be permitted or denied.

packet-tracer input ifc_name {icmp | tcp | udp | rawip} [inline-tag tag] ...

Example:

    packet-tracer input inside tcp 192.168.1.62 12345 5.1.1.1 80 detail
    packet-tracer input inside tcp 192.168.1.62 12345 5.1.1.1 81 detail

Reference:
CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide, 9.4
WSA Logs

1448473822.281 980 192.168.1.62 TCP_CLIENT_REFRESH_MISS_SSL/200 1524 POST
https://www.facebook.com:443/ajax/litestand/newsfeed_count?__pc=EXP13ADEFAULT -
DIRECT/www.facebook.com/application/x-javascript DEFAULT_CASE_12-DefaultGroup-NONE-
NONE-NONE-DefaultGroup <IW_snet,3.8,0,-","0,0,0,1,-","1,-","-","-","-","-","-","-","-","-","-","-","-","-","-","w","Unknown","","Facebook General","Facebook","","","12.44,0,-","Unknown","","-","-","-","-","-","-","-","-","-","-","-","-","-","-","-"> -
"25/Nov/2015:15:50:22 -0200"

1448473834.026 1106 192.168.1.62 TCP_CLIENT_REFRESH_MISS_SSL/200 2530 POST
https://www.facebook.com:443/ajax/chat/buddy_list.php?__pc=EXP13ADEFAULT -
DIRECT/www.facebook.com/application/x-javascript DEFAULT_CASE_12-DefaultGroup-NONE-
NONE-NONE-DefaultGroup <IW_chat,3.8,0,-","0,0,0,1,-","1,-","-","-","-","-","-","-","-","-","-","-","-","-","-","-","Unknown","","Facebook Messages and Chat","Facebook","","","18.30,0,-","Unknown","","-","-","-","-","-","-"> -
"25/Nov/2015:15:50:33 -0200"

1448473835.035 715 192.168.1.62 TCP_CLIENT_REFRESH_MISS_SSL/200 2544 POST
application/x-javascript DEFAULT_CASE_12-DefaultGroup-DefaultGroup-NONE-NONE-DefaultGroup
<IW_chat,3.8,0,-","0,0,0,1,-","1,-","-","-","-","-","-","-","-","-","-","-","-","-","-","Unknown","","Facebook Messages and Chat","Facebook","","","28.46,0,-","Unknown","","-","-","-","-","-","-"> -
"25/Nov/2015:15:50:34 -0200"

1448473865.034 58818 192.168.1.62 TCP_MISS_SSL/200 408 GET https://2-edge-
id=10000753947921&stickey_token=170&stickey_pool=atn1c88_chat-proxy - DIRECT/2-edge-
chat.facebook.com/text/plain DEFAULT_CASE_12-DefaultGroup-DefaultGroup-NONE-NONE-NONE-DefaultGroup
<IW_snet,3.8,0,-","0,0,0,1,-","1,-","-","-","-","-","-","-","-","-","-","Unknown","","Facebook General","Facebook","","","0.06,0,-","Unknown","","-","-","-","-","-","-"> -
"25/Nov/2015:15:51:04 -
0200"

Disclaimer

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2013 Cisco Systems, Inc. All rights reserved.