Forcepoint Content Gateway and Palo Alto Networks Decryption Broker

Integration Guide

Forcepoint

Integration Guide

Jonathan Knepher
21 June 2021
DRAFT NOT FOR RELEASE

forcepoint.com

Table of Contents

Version	Date	Author	Notes
0.1	23 April 2020	Jonathan Knepher	First draft
0.2	01 May 2020	Jonathan Knepher Mattia Maggioli	Content updates New diagram
0.3	09 June 2020	Jonathan Knepher	Updates and feedback from Sushant Deshpande
0.4	16 July 2020	Jonathan Knepher	Updates to include physical testing
0.5	24 July 2020	Jonathan Knepher	Updates for new HF and script
0.6	20 August 2020	Jonathan Knepher	Additional QA testing results
0.7	02 November 2020	Jonathan Knepher	Additional edits from customer test
0.8	22 January 2021	Jonathan Knepher	Additional edits from customer test
0.9	04 February 2021	Jonathan Knepher Sushant Deshpande	Additional edits from customer test

IMPORTANT NOTE

This document is pre-release and shared under Non-disclosure agreement.

Summary

This guide provides step by step instructions to setup an integration between Forcepoint Content Gateway and Palo Alto Networks Decryption Broker. This is intended to allow customers to use both Forcepoint Web Security and Data Loss Prevention features of the Forcepoint product line with Palo Alto Networks Decryption Broker.

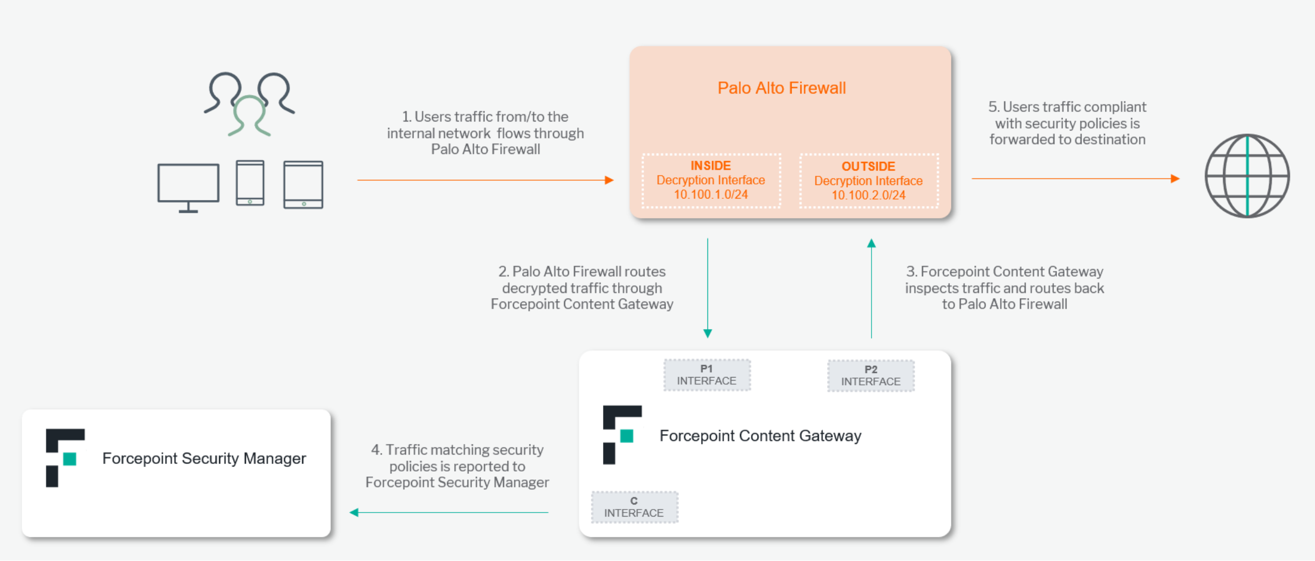
The code and instructions provided enable system administrators to:

→Setup and configure Forcepoint Content Gateway inside a Palo Alto Firewall Decryption Broker service chain

→Customize Palo Alto Firewall Decryption Broker configuration to be compatible with Forcepoint Content Gateway

→Optionally, support clustering of Forcepoint Content Gateway for load balancing and availability

A network diagram for traffic flow between the components involved is provided in this diagram, which depicts the sample IP addresses used in this document:


Palo Alto Firewall
INSIDE
Decryption Interface
10.100.1.0/24
OUTSIDE
Decryption Interface
10.100.2.0/24
1. Users traffic from/to the internal network flows through Palo Alto Firewall
5. Users traffic compliant with security policies is forwarded to destination
2. Palo Alto Firewall routes decrypted traffic through Forcepoint Content Gateway
3. Forcepoint Content Gateway inspects traffic and routes back to Palo Alto Firewall
P1
INTERFACE
P2
INTERFACE
Forcepoint Content Gateway
C
INTERFACE
Forcepoint Security Manager
4. Traffic matching security policies is reported to Forcepoint Security Manager

Caveats

The integration described in this document was developed and tested with the following product versions and licensed features, and has the listed constraints:

- →Forcepoint Products:
  - Minimum required Content Gateway version 8.5.4 HF2
  - Tested versions:
    - Software Content Gateway 8.5.4 HF1 and HF2 in integrated Web and DLP mode, on CentOS 7.6.1810
    - Forcepoint V10000G4R2 running 8.5.4 HF1 and HF2
      - Requires technical support or TAM to update based on this documentation
    - Forcepoint DLP 8.7.2
  - Content Gateway must be in the specific configuration defined in this document and be dedicated to the Decryption Broker traffic. If additional traffic monitoring is required, for example plaintext HTTP, distinct Content Gateways must be deployed to handle that traffic
  - Content Gateway must not allow content caching.
  - When using Palo Alto Security Chain load balancing, and a non-transparent proxy authentication method, users may have to authenticate once for each proxy in the pool per authentication cache interval. Integrated Windows Authentication happens automatically without prompting the user.
  - Only Integrated Windows Authentication is validated
    - Credential caching method must be set to Cache using IP addresses only; cookie authentication is not supported.
  - Advanced File Analysis cannot be performed from within the Decryption Broker service chain.
- →Palo Alto Firewall:
  - The Decryption Broker license must be installed before starting this guide
  - Software Content Gateway was tested with PAN VM-300 Version 9.1.0-h3 on ESX 6.5
  - Appliance and software Content Gateway was tested with PAN PA-3250 Version 10.0.0
  - This integration is confirmed to not work with AWS pay as you go licensed PAN VM instances running version 9.0 and 9.1 due to decryption broker licensing constraints

This interoperability uses:

- →**Palo Alto Firewall Decryption Broker** to intercept and decrypt SSL traffic from protected endpoints
- →**Palo Alto Firewall Service Chain** to provide protected traffic to Forcepoint Content Gateway
- →**Forcepoint Content Gateway** to provide Web Security and Data Loss Prevention features
- →**Forcepoint Security Manager** to configure and provide policy to the Forcepoint products

This interoperability only describes the Decryption Broker integration, and therefore only provides inspection for HTTPS traffic that has been decrypted by Palo Alto Firewall. A traditional Forcepoint implementation is required in parallel to inspect plaintext HTTP traffic, and/or any HTTPS traffic that is not decrypted by the Palo Alto Firewall.

Implementation

Setup Decryption Broker

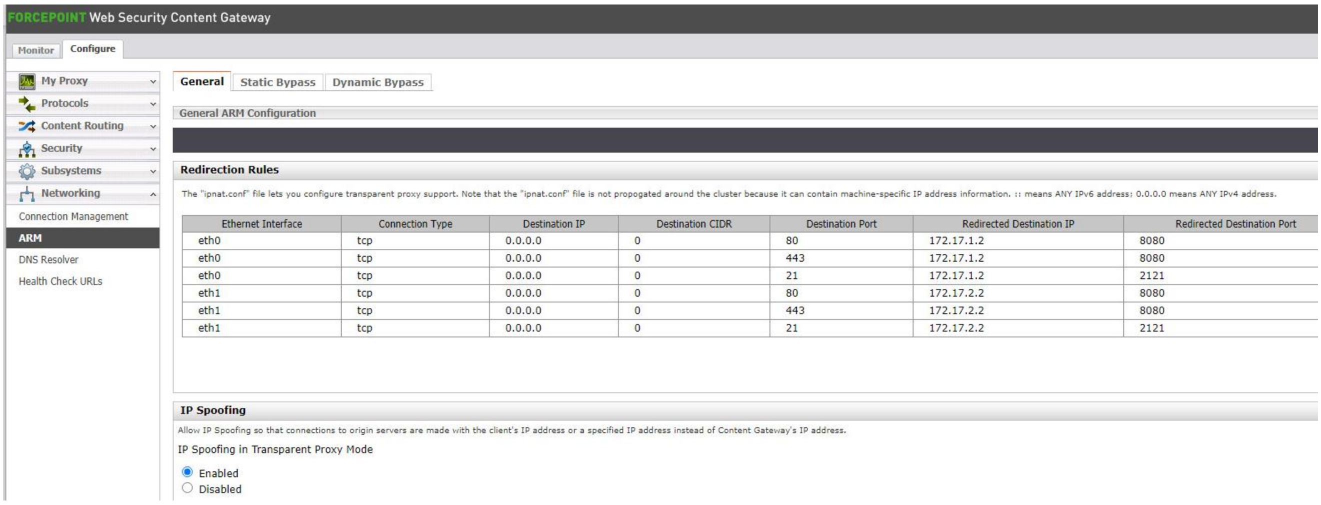
Configure Decryption Broker using Palo Alto Networks' instructions available at: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/decryption/decryption-broker.html. The specific steps for a Layer 3 security chain, which this document requires, is available at: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/decryption/decryption-broker/decryption-broker-configure-with-layer-3-chain.html.

Please follow the Palo Alto instructions above to setup Decryption Broker, with a Layer 3 security chain comprised of a Forcepoint Content Gateway. The following steps below augment Palo Alto's instructions:

1. Configure Content Gateway with at least three interfaces, referred to as C, P1, and P2 in this document, to align with the Forcepoint appliance interface naming.
    - Take note of the operating system names of the interfaces, and the IP addresses assigned, as they will be needed later.
    - The C interface is used for management. Assure that the operating system has a default route that egresses via this interface. This interface is used to provide block pages, authenticate users, download updates, and communicate with Forcepoint Security Manager and other Forcepoint components. **NOTE: For a software install, this interface must be named "internal"; use your OS's networking configuration or udev rules to set this, as explained below.**
    - The P1 interface is the inside interface for the decryption broker chain. As depicted in the diagram above, this interface must be connected via layer 2 and have an IP address in the same subnet as the Palo Alto Networks Decryption Broker's inside interface. This interface must only be used for traffic facing the clients through the Decryption Broker. **NOTE: The routes for this interface are created later. Do not create any OS routes other than the implied connected route. For a software install, this is strongly suggested to be named "eth0".**
    - The P2 interface is the outside interface for the decryption broker chain. This interface must be connected via layer 2 and have an IP address in the same subnet as the Palo Alto Decryption Broker's outside interface. This interface must only be used for traffic facing the origin servers through the Decryption Broker. **NOTE: The routes for this interface are created later. Do not create any OS routes other than the implied connected route. For a software install, this is strongly suggested to be named "eth1"**
    - The suggested method for a RedHat or CentOS software installation to set the interface names is use udev rules to map the MAC addresses of the interfaces to the specific names. Edit or create **/etc/udev/rules.d/70-persistent-net.rules** with the following rules, where you confirm the appropriate MAC addresses with your hardware or virtualization environment:
        - SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", ATTR{address}=="xx:xx:xx:xx:xx:xx", ATTR{type}=="1", NAME="internal"
        - SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", ATTR{address}=="yyy:yy:yy:yy:yy:yy", ATTR{type}=="1", NAME="eth0"
        - SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", ATTR{address}=="zz:zz:zz:zz:zz:zz", ATTR{type}=="1", NAME="eth1"
    - Update the interface NAME and DEVICE values in the following files in **/etc/sysconfig/network-scripts/** for these interfaces:
        - ifcfg-internal
        - ifcfg-eth0
        - ifcfg-eth1
2. Forcepoint Appliance setup: (NOTE: Requires TAM or Technical Support assistance.)
    - Install base 8.5.4 appliance image appliance as normal

   - Add appliance to Forcepoint Security Manager as normal
   - Enable tech-support account, login as tech-support, login as root account
   - Apply HF2)
   - Upload **FP_Configure_Transparent_Decryption_Integration.sh** to **/var/lib/lxc/wcg/rootfs/tmp**
   - Execute the following command once, and then add it to **/etc/rc.local** on the appliance host (not inside the WCG container): **NOTE:** You may need to confirm that **/etc/rc.local** is executable. (Detailed in step 5.)
      - iptables -t nat -I PREROUTING -d (appliance's C interface IP)/32 -p tcp -m tcp --dport 8080 -j DNAT --to-destination 169.254.254.1

3. Utilize the automated deployment script to setup Content Gateway, or skip to step 4 to manually setup the configuration if desired.
   - Connect to Content Gateway by entering 'ssh wcg'
   - Edit the initial section of the FP_Configure_Transparent_Decryption_Integration.sh script with appropriate parameters for your network
      - ETH0 is the P1 interface, do not edit on appliance
      - ETH1 is the P2 interface, do not edit on the appliance
      - USER_NETWORK is a network specification to identify the traffic bound to the users. For the diagram above, this would be 10.200.1.0/24; typical customer installations may be 10.0.0.0/8
      - PA_INSIDE_IP should be set to the Palo Alto's decryption broker IP address. For the diagram above, this would be 10.100.1.1.
      - PA_OUTSIDE_IP should be set the to Palo Alto's decryption broker outside iIP address. For the diagram above, this would be 10.100.2.1
      - Run ./FP_Configure_Transparent_Decryption_Integration.sh enable
   - Continue to step 5
4. Use these steps to do a manual setup only if you skipped step 4 above. Setup Content Gateway with the following configuration in the Content Gateway management interface:
   - In the Configure | Basic | General tab, set the following:
      - HTTPS: disabled
      - Authentication: none, or IWA (requires normal IWA configuration)
   - In the Configure | HTTP | General tab, set the following:
      - Reverse DNS: disabled
      - Tunnel ports: Remove 443
      - HTTPS ports: Change to 4443 (must not be 443, or any other port that is being decrypted by decryption broker)
   - In the Configure | Networking | ARM tab, set the following:
      - Redirection Rules
         - Configure a redirection rule for the decrypted HTTPS traffic for the P1 interface using the OS's interface name "eth0", tcp, destination 0.0.0.0, port 443, redirected destination IP of the P1 interface, and redirected destination port of 8080
         - Configure a redirection rule for the plaintext HTTP health-checks for the P1 interface and port 80, with the other parameters the same as above
         - Enable IP Spoofing in Transparent Proxy Mode



General ARM Configuration

Redirection Rules

The "ipnat.conf" file lets you configure transparent proxy support. Note that the "ipnat.conf" file is not propogated around the cluster because it can contain machine-specific IP address information. :: means ANY IPv6 address; 0.0.0.0 means ANY IPv4 address.

Ethernet Interface	Connection Type	Destination IP	Destination CIDR	Destination Port	Redirected Destination IP	Redirected Destination Port
eth0	tcp	0.0.0.0	0	80	172.17.1.2	8080
eth0	tcp	0.0.0.0	0	443	172.17.1.2	8080
eth0	tcp	0.0.0.0	0	21	172.17.1.2	2121
eth1	tcp	0.0.0.0	0	80	172.17.2.2	8080
eth1	tcp	0.0.0.0	0	443	172.17.2.2	8080
eth1	tcp	0.0.0.0	0	21	172.17.2.2	2121

IP Spoofing

Allow IP Spoofing so that connections to origin servers are made with the client's IP address or a specified IP address instead of Content Gateway's IP address.

IP Spoofing in Transparent Proxy Mode

● Enabled
○ Disabled

- Make the following additional changes in /opt/WCG/config/records.config. Change the values on the existing lines in the config files if they differ:
    - CONFIG proxy.config.arm.ignore_ifp INT 0
    - CONFIG proxy.config.arm.always_query_dest INT 1
    - CONFIG proxy.config.arm.enable_transparent_decryption_integration INT 1
    - CONFIG proxy.config.http.outgoing_transparent_ip_spoofing_enabled INT 1
    - CONFIG proxy.config.http.keep_alive_no_activity_timeout_in INT 10
    - CONFIG proxy.config.http.keep_alive_no_activity_timeout_out INT 10
    - CONFIG proxy.config.http.transaction_no_activity_timeout_in INT 120
    - CONFIG proxy.config.http.transaction_no_activity_timeout_out INT 120
    - CONFIG proxy.config.http.cache.ftp INT 0
    - CONFIG proxy.config.http.cache.http INT 0
    - CONFIG proxy.config.cache.ram_cache.size INT 0

- Edit the /etc/sysctl.conf file, updating or adding these lines to the end of the file as appropriate, replacing eth0, eth1, and eth2 with the appropriate OS names of the C, P1, and P2 interfaces if they differ.
    - sysctl net.netfilter.nf_conntrack_tcp_be_liberal = 1
    - sysctl net.ipv4.conf.all.rp_filter=0
    - sysctl net.ipv4.conf.default.rp_filter=0
    - sysctl net.ipv4.conf.eth0.rp_filter=0
    - sysctl net.ipv4.conf.eth1.rp_filter=0
    - sysctl net.ipv4.conf.internal.rp_filter=0
- Exectute “sysctl -p” to have these values take effect without restarting.
- Add the following line to the end of /etc/iproute2/rt_tables:
    - 300 outbound
- Add the following commands to the end of a local startup script, such as /etc/rc.local, with the noted replacements:
    - Replacements:
        - 10.200.1.0/24 should be replaced by a network CIDR that covers the internal user

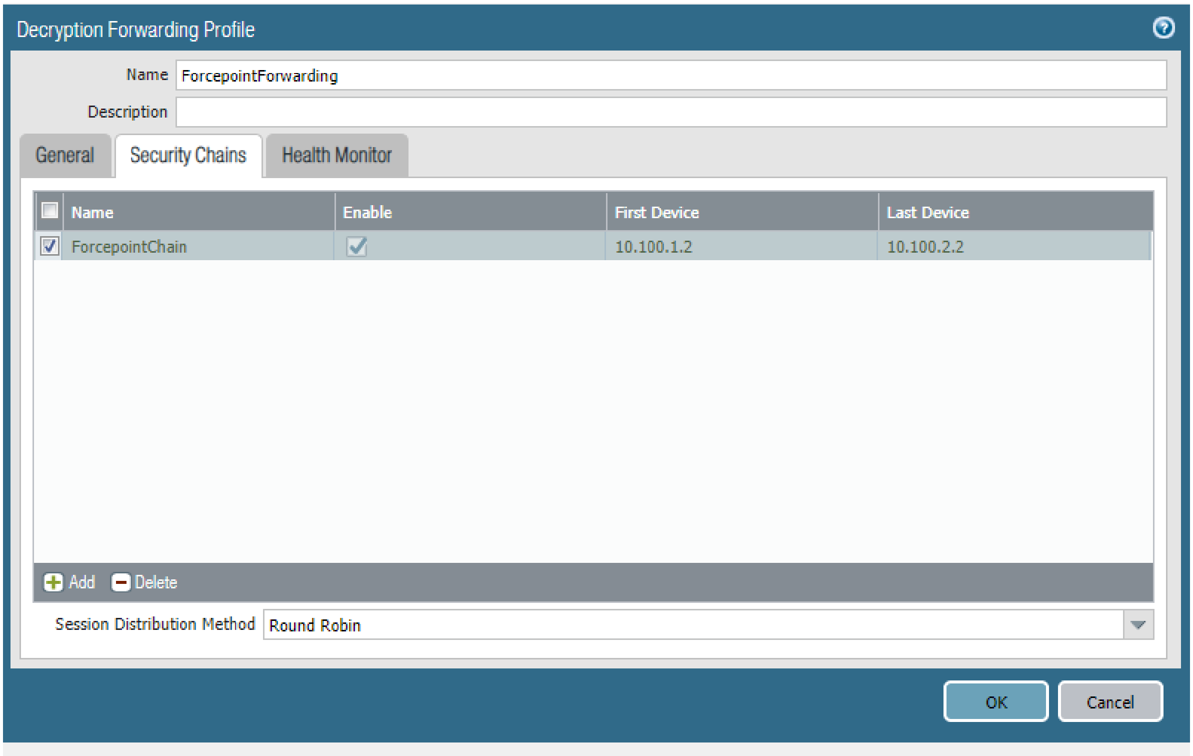
networks

- 10.100.1.1 should be replaced by the Palo Alto Networks' inside decryption broker ip address
- 10.100.2.1 should be replaced by the Palo Alto Networks' outside decryption broker ip address

- ip rule add from all fwmark 4 table outbound
- ip route add 10.200.1.0/24 via 10.100.1.1 dev eth0 table outbound
  - Note: This may be repeated if additional internal routes to client machines are required
- ip route add default via 10.100.2.1 dev eth1 table outbound
- iptables -t mangle -F OUTPUT
- iptables -t mangle -A OUTPUT -j CONNMARK --restore-mark --nfmask 0x7 --ctmask 0x7
- iptables -t mangle -A OUTPUT -m mark --mark 0x1 -j MARK --set-xmark 0x4/0x7
- iptables -I INPUT -m mark --mark 0x1/0x1 -j CONNMARK --save-mark --nfmask 0x1 --ctmask 0x1

5. If using Forcepoint Content Gateway authentication, setup an authentication filtering rule for Palo Alto Networks Decryption Broker health-checks to be allowed without authentication:
   - In the Configure | Security | Access Controls | Filtering tab, create an additional rule of Type allow, for the Source IP of the Palo Alto Decryption Broker's inside interface, 10.100.1.1 in this example.
   - If using an appliance with IWA authentication, create an iptables rule for the C interface in the nat table on the PREROUTING chain to nat the traffic to the WCG container:

     iptables -t nat -I PREROUTING –d <appliance C interface IP>/32 -p tcp –m tcp --dport 8080 -j DNAT --to-destination 169.254.254.1
6. Create a Decryption Profile on the Palo Alto Networks firewall with the following configuration:
   - Decryption Mirroring Interface should be set to None, as Mirroring Interfaces are not used by this interoperability
   - On the SSL Decryption | SSL Forward Proxy tab, Client Extension | Strip ALPN MUST be checked
   - The remaining parameters can be configured per your security policy
7. Assure that the Palo Alto Networks Decryption Broker has the service chain defined with the P1 and P2 interfaces
   - In Objects | Decryption | Forwarding Profile, create a profile for forwarding to Forcepoint.
   - In the General tab, set the Security Chain Type to Routed (Layer 3)
   - Set Flow Direction to Bidirectional
   - Select the appropriate primary and secondary interfaces dedicated on the Palo Alto to Decryption Broker
   - In the Security Chains tab, add a new chain, setting the First Device address to the P1 interface's IP address, and the Last Device to the P2 interface's IP address.
   - If you desire load balancing, you may create additional chains for additional Content Gateways, and select an appropriate load balancing method for your environment. Utilize IP Hash or IP Modulo load balancing methods.
   - In the Health Monitoring tab, select your desired mode for Check Failure.
   - Select the HTTP Monitoring option, with a count of 3 and an interval of 3 seconds.



Name: ForcepointForwarding

Description:

☐	Name	Enable	First Device	Last Device
☑	ForcepointChain	✓	10.100.1.2	10.100.2.2

Session Distribution Method: Round Robin

Troubleshooting

Follow these steps to identify issues impacting the normal operation of the integration described in this document.

Traditional Implementation

Validate the prerequisites

Make sure the prerequisites described in the **Summary** chapter are all satisfied:

- Check the versions of Forcepoint Content Gateway and Palo Alto NGFW in use are listed as compatible
- Confirm that Decryption Broker is properly licensed

Check network connectivity

Make sure firewalls or other security appliances are not impacting the network connectivity necessary for the operation of all components involved into this integration:

- Assure connectivity on each of the proxy interfaces using arping. Repeat the below for P1 and P2. This configuration may not allow ICMP Echo.

```
arping -c5 -I eth1 10.100.2.1
```

- Replacing the example URL/IP address with the current one used. Once done check the result is similar to below:

```
ARPING 10.100.2.1 from 10.100.2.2 eth1
Unicast reply from 10.100.2.1 [xx:xx:xx:xx:xx:xx]  0.858ms
Unicast reply from 10.100.2.1 [xx:xx:xx:xx:xx:xx]  0.790ms
Unicast reply from 10.100.2.1 [xx:xx:xx:xx:xx:xx]  0.758ms
Unicast reply from 10.100.2.1 [xx:xx:xx:xx:xx:xx]  0.864ms
Unicast reply from 10.100.2.1 [xx:xx:xx:xx:xx:xx]  0.536ms
```

Confirm routing table is correct

Make sure that the installation script or manual setup process created the appropriate routes. There should be a route to the clients and the Decryption Broker interface on P1 / eth0, and a default route on interface P2 / eth1.

- Use the ip route list command to check the existence of the policy route rule and routes:

```
ip rule list
ip route list table outbound
```

- Replacing the example network address as appropriate, check the result is similar to below:

```
A
[root@wcg ~]# ip rule list
0:      from all lookup local
32764:  from all fwmark 0x4 lookup outbound
32765:  from all fwmark 0x1 lookup nc-reserved
32766:  from all lookup main
32767:  from all lookup default

[root@wcg ~]# ip route list table outbound
default via 10.100.2.1 dev eth1
10.0.0.0/8 via 10.100.1.1 dev eth0
10.100.1.0/24 dev eth0
10.100.2.0/24 dev eth1
```

forcepoint.com/contact

About Forcepoint

Forcepoint is the global human-centric cybersecurity company transforming the digital enterprise by continuously adapting security response to the dynamic risk posed by individual users and machines. The Forcepoint human point system delivers risk-adaptive protection to continuously ensure trusted use of data and systems. Based in Austin, Texas, Forcepoint protects the human point for thousands of enterprise and government customers in more than 150 countries.