Forcepoint

Remote Browser Isolation

22.06

On-Premises Deployment Guide

Revision A

Published 01 July 2022

Contents

Chapter 1

Introduction

Contents

Forcepoint Remote Browser Isolation (Forcepoint RBI) helps organizations experience a safer internet by proactively stopping web, email, and document-based threats. This document captures the prerequisites for an on-premises deployment of Forcepoint RBI. Details have been provided for recommended network port openings required for communication.

Forcepoint RBI has three major components:

- Control Center Cluster (Master & Worker): The Control Center cluster contains the Forcepoint RBIAdmin Portal and Superadmin Portal. The Portal is responsible for policy management, user authentication, logging, dashboard, and reporting.
- RBC Cluster (Master & Worker): The Remote Browsing Containers (RBCs) house the remote browsers that connect to the Internet to fetch, execute, and render the content.
- Proxy: The proxy handles all traffic redirection from the end user's browser to the RBC.

This document provides the specifications required for the Virtual Machine and Network Communication. Refer to the *Sizing Guide* for hardware specifications for Forcepoint RBI.

Deployment prerequisites

Before deploying Forcepoint RBI in an on-premises environment, review these prerequisites.

- Virtualization platform should be based on any of the following virtualization products:
  - Virt-Manager (KVM)
  - Oracle VirtualBox
  - VMware
- Forcepoint RBI systems should be reachable from endpoint machines (end user systems).
- One IP address is to be assigned to each Forcepoint RBI component (master, worker, proxy).
- Public Wildcard SSL certificate or a Self-Signed SAN-based wild card certificate, including RBI servers IP address as SAN, is required for Forcepoint RBI. Public certificate, Private key, and CA certificates are required.
  For Self-Signed certificates, install the Root CA Chain Certificate on the endpoint machines under **Trusted Root CA Authority**.
- The FQDN names of Forcepoint RBI should be resolved by the endpoint machines by following one of these options:
  - Add DNS entries for Forcepoint RBI FQDNs and URLs to the respective domain.
  - Add the FQDN entries for Forcepoint RBI in the user's endpoint machine host file (`C:\windows\system32\drivers\etc\hosts`). This requires Admin access to the endpoint machine.

  - If there is a local/Internal DNS in place for resolving Intranet/Internal servers and it is configured as a DNS server in the user's endpoint machine, then create a zone for the domain of the FQDN in the Local/Internal DNS and add the host entries to it so that users can resolve the FQDNs through local/Internal DNS.
- The Forcepoint RBI instances need to be provided with DNS servers that can resolve Global domains.
- If a proxy server is in place, then the IP address and the port of the proxy server must be configured in Forcepoint RBI.
- Internet connectivity is required for setting up Forcepoint RBI and for browsing through Forcepoint RBI.
- For final deployment, the actual resource requirements are calculated based on the *Sizing Guide* and on the following:
  - User concurrency
  - Internet usage pattern
- The hardware specification requirement for production deployment will be in accordance with the *Sizing Guide*. Check the *Sizing Guide* details with your administrator or a Forcepoint representative for details on the resources required and number of VMs required for installing and configuring the Forcepoint RBI. The resource requirements are calculated based on the following:
  - User concurrency
  - Internet usage pattern
- The wildcard entry of the Forcepoint RBI base domain is to be bypassed (set exception) in the end user proxy settings.
- According to the *Sizing Guide*, RBI consists of the following components:

Admin Portal	RBC Cluster	RBI Proxy**
Master	Master	Proxy
Worker	Worker-RBC	
	Worker-File Scanning	
	Worker-Control Plane	

  ** RBI Proxy is applicable only in case of Proxy chaining.
- The Master and Worker for the respective cluster (Control Center and RBC) should be hosted in the same LAN segment. The Master and Workers should have no protocol or port restrictions.

Network communication requirements

Forcepoint RBI communicates with the endpoint using WebSocket on custom ports. This section shows the ports that needs to be opened for communication with Forcepoint RBI.

Connection	Required ports
Endpoint machine to Forcepoint RBI Control Center Cluster	tcp 443 (Session initialization)
Endpoint machine to Forcepoint RBI RBC Cluster	tcp 443 (Session initialization) tcp 30000 – 32767 (Secure WebSocket connection (WSS) for Remote Browsing container)

Connection	Required ports
Forcepoint RBI Cluster Communication (Control Center Cluster to RBC Cluster)	tcp 443 (RBI cluster communication)
Internet access to Forcepoint RBI Cluster (RBC Cluster to Internet)	tcp 443 (Internet access to RBC Cluster) tcp “Proxy IP & Proxy Port” (Proxy IP and Proxy port in case Internet access is provisioned through Enterprise Proxy.)
Terminal access (Admin user to Forcepoint RBI instances)	tcp 2200
Forcepoint Web Security Gateway/Proxy settings	Add base domain wildcard (e.g., *.rbi.forcepoint.com) to bypass list in end user Proxy settings.
CDR Service: API call to CDR service from Forcepoint RBI	tcp 80, 443 (destination *.threat-removal.deep-secure.com)
FTIS Service: API call to FTIS service from Forcepoint RBI	tcp 80, 443 (destination *. cloud.threatseeker.com)

Chapter 2

Deploying Forcepoint RBI

Contents

This chapter provides the instructions for deploying Forcepoint RBI in an on-premises environment.

Note

- Read the *Sizing Guide* for the hardware resources required for each VM component before beginning the deployment.
- The VMs and resources are to be provisioned based on the sizing exercise conducted to determine the total number of hardware resources (vCPU, Memory, Disk) needed. The *Sizing Guide* provides the total number of resources required as well resources required for each RBI component.
  - The maximum vCPU per VM/Physical server for Worker (for both Core and RBC) should be 64 vCPU.
  - The minimum vCPU per VM/Physical server for Worker (for both Core and RBC) should be 32 vCPU.

Based on a sample sizing, here is an illustration of the number of virtual machines required for each component:

	Admin Portal		RBC Cluster				RBI Proxy**	Final Total
	Master	Worker	Master	Worker-RBC*	Worker-File Scanning*	Worker-Control Plane*	Proxy	
vCPUs	20	36	20	1024	36	20	24	1180
Memory	80	144	80	4096	144	80	96	4720
Storage SSD (in GB)	40	180	40	1280			40	1580
DB Storage SSD (in GB)								
No.of Vms (64 vCPU each VM)	1 vm/20 vCPUs	1 vm/36 vCPUs	1 vm/20 vCPUs	16 vms/64 vCPU each	1 vm/36 vCPUs	1 vm/20 vCPUs	1 vm/24 vCPUs	
No.of Vms (32 vCPU each VM)	1 vm/20 vCPUs	1 vm/36 vCPUs	1 vm/20 vCPUs	32 vms/32 vCPU each	1 vm/36 vCPUs	1 vm/20 vCPUs	1 vm/24 vCPUs	

*During the RBI setup, add RBC Cluster File Scanning and Control Plane Workers along with RBC cluster Worker section in the `cluster.yaml` file and note the IP address of the RBC Cluster File Scanning and Control Plane nodes. Nodes' labels are changed post-installation.

** RBI Proxy is applicable only in case of Proxy chaining, not applicable for URL based redirection.

- Provision the number of VMs accordingly after reading the RBI sizing guide and conducting the RBI sizing exercise.
- After all of the VMs are configured with IP addresses, proceed with the RBI setup.

Deploy Forcepoint RBI

This topic provides the procedure for deploying Forcepoint RBI in on-premises environments. Before deploying Forcepoint RBI, obtain the ISO from Forcepoint.

Steps

1) Install and deploy the Forcepoint RBI ISO obtained from Forcepoint.

2) Each Forcepoint RBI instance/VM is to be setup using the same ISO.

3) After the VM is ready, SSH to the VM using port 2200 with the login credentials (Username: maint Password: admin), and assign the static IP address to the VM.

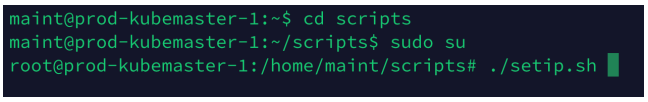
Note

Keep a copy of the IP address, Netmask, Gateway, and DNS details. You will need these details later.

4) Set the IP addresses and network details:

   a) Open a command prompt or terminal and run the following two commands:

```
# cd scripts
# sudo ./setip.sh
```



   b) Select **interface 1** or the serial number against the interface name connected to the virtual network, then press **Enter**.

   c) For **Do you want to use DHCP for this interface (y/n)**, type **n**, then press **Enter**. (Please set the static IP address)

   d) Enter the **IP Address** (for example, **192.168.2.201**), then press **Enter**. (Please select your IP address)

   e) Enter the **Subnet mask** (for example, **255.255.255.0**), then press **Enter**. (Please select your subnet mask)

   f) Enter the **Gateway** (for example, **192.168.2.1**), then press **Enter**. (Please select your gateway)

g) Enter the **DNS IP** (for example, **8.8.8.8**), then press **Enter**. If you are entering multiple DNS IP addresses, separate the IP addresses with commas. (Please select your DNS)

h) Repeat these steps on all required VMs.

5) Verify the IP address with the following command:

```
ip a
```

```
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:b9:ea:d8 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.201/24 brd 192.168.2.255 scope global ens33
       valid_lft forever preferred_lft forever
    inet6 fd15:4ba5:5a2b:1002:20c:29ff:feb9:ead8/64 scope global tentative mngtmpaddr dynamic
       valid_lft 86400sec preferred_lft 14400sec
    inet6 fe80::20c:29ff:feb9:ead8/64 scope link
       valid_lft forever preferred_lft forever
```

6) Shut down the VM, then start the VM again.

```
sudo shutdown -h now
```

Note

- Make sure all the VMs required for the RBI components are created before you proceed with RBI setup and installation.
- Note down the IP address of all the VMs in a spread sheet.
- To relate the VMs to the RBI components, tag the respective VMs against the respective RBI component.
- Use one of the primary VMs from the RBI Admin portal Master component to download the RBI deb package and run the setup.
- Before running the RBI setup, make sure all the VMs are powered ON and reachable via port 2200.

7) SSH to the primary VM (Admin Portal Master VM) using port 2200 with the login credentials (Username:maint Password: admin).

8) Using WinSCP or scp, copy the deb package provided by Forcepoint, then install:

```
sudo dpkg -i <debpackage>
```

9) Update `/opt/rbi/rbi-installer/cluster.yaml` with the following required details:

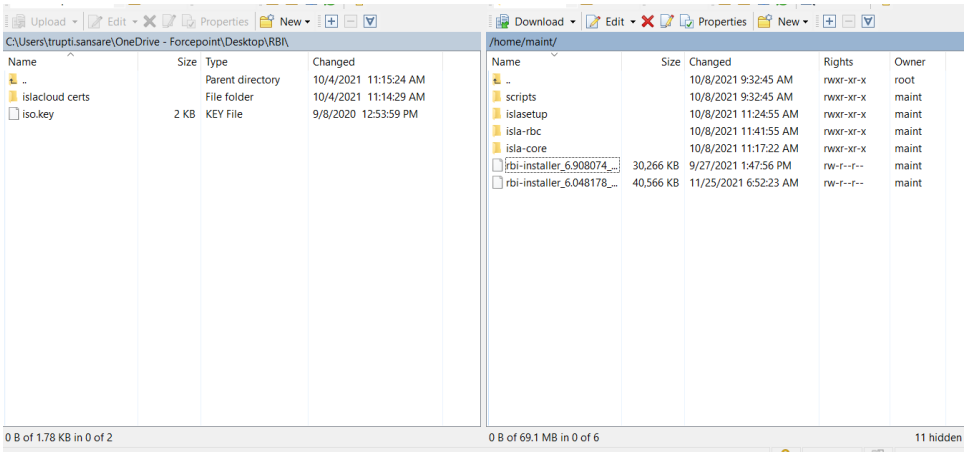
```
nano /opt/rbi/rbi-installer/cluster.yaml
```

a) Add the client certificates.

```
kubernetes:
  certs:
    publickey: keys/fp.dev.crt
    privatekey: keys/fp.dev-domain.key
    ca: keys/fp.dev-CA.crt
```

Note

Use WinSCP or the `scp` command to copy the required certificate and key to `/opt/rbi/rbi-installer/keys`.



b) Add the Core master node 1 IP address (Admin Portal Master VM IP address):

```
loadbalancer:
  ip: ""
baseurl: .fp.dev
cluster:
  core:
    masters:
    - node: 1
      ip: 192.168.122.231
      sshport: 2200
      sshuser: maint
      reset: 0
```

Note

For Single cluster Multi master setup (Core master IPs = RBC master IPs),

Prerequisites:

- We recommend that you use your own Load Balancer. If you are using the RBI Load Balancer, then follow the below steps:

  i) Go to script placed in `/opt/rbi/rbi-installer/helperscripts/archive/loadbalancer.sh`

  ii) Run it on the server you want to configure as the Load Balancer in below format:

  ```
  ./loadbalancer.sh lbip,master1_ip,matesr2_ip,master3_ip
  ```

- Three Master VM Nodes are required
  Perform the below steps in `cluster.yaml`

  i) Add the Load Balancer IP in `cluster.yaml`.

  ```
  loadbalancer:
    ip: "192.168.122.100"
  ```

  ii) Add two more Master node entries.

  ```
  core:
    masters:
    - node: 1
      ip: 192.168.122.41
      sshport: 2200
      sshuser: maint
      reset: 1
    - node: 2
      ip: 192.168.122.42
      sshport: 2200
      sshuser: maint
      reset: 1
    - node: 3
      ip: 192.168.122.43
      sshport: 2200
      sshuser: maint
      reset: 1
  ```

c) Add the Core worker node 1 IP address (Admin Portal Worker VM IP address):

```
workers:
- node: 1
  ip: 192.168.122.231
  sshport: 2200
  sshuser: maint
  reset: 0
```

If there are multiple workers, add entries for each worker (for example, from node to reset for each worker).

```
workers:
- node: 1
  ip: 192.168.122.166
  sshport: 2200
  sshuser: maint
  reset: 1
- node: 2
  ip: 192.168.122.213
  sshport: 2200
  sshuser: maint
  reset: 1
```

d) Add the RBC master node 1 IP address (RBC Cluster Master VM IP address):

```
rbc:
  masters:
  - node: 1
    ip: 192.168.122.231
    sshport: 2200
    sshuser: maint
    reset: 0
```

Note

In case of Single cluster Multi master setup (Core master IP Addresses = RBC masters' IP Addresses), add 2 more master entries under RBC cluster.

```
rbc:
  masters:
  - node: 1
    ip: 192.168.122.41
    sshport: 2200
    sshuser: maint
    reset: 0
  - node: 2
    ip: 192.168.122.42
    sshport: 2200
    sshuser: maint
    reset: 0
  - node: 3
    ip: 192.168.122.43
    sshport: 2200
    sshuser: maint
    reset: 0
```

e) Add the RBC worker node 1 IP address (RBC Cluster Worker VM IP address):

```
workers:
- node: 1
  ip: 192.168.122.231
  sshport: 2200
  sshuser: maint
  reset: 0
```

If there are multiple workers, add entries for each worker (for example, from node to reset for each worker).

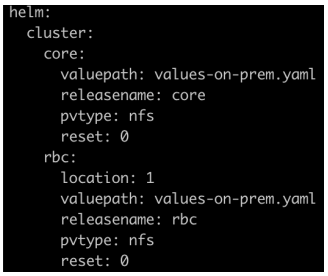
```
workers:
- node: 1
  ip: 192.168.122.240
  sshport: 2200
  sshuser: maint
  reset: 1
- node: 2
  ip: 192.168.122.128
  sshport: 2200
  sshuser: maint
  reset: 1
```

Note

- During the RBI setup, add RBC Cluster File Scanning and Control Plane Workers along with RBC cluster Worker section in the `cluster.yaml` file and note the IP address of the RBC Cluster File Scanning and Control Plane nodes. Nodes' labels are changed post-installation.
- If the Core and RBC workers IP addresses different for Single cluster Multi Master deployment, then add the RBC workers IP addresses in the Core Worker section.

f) Add cluster information. For example:

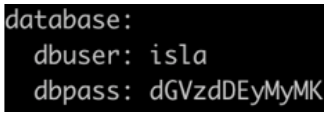
```
data:
                    core:
                        valuepath: values-on-prem.yaml ( File which needs to be used for
 helm core installation)
                        releasename: core (Name of the release for core)
                        pvtype: nfs
                        reset: 0
                    rbc:
                        location: 1 ( Based on the region. USA = 1, UK = 2)
valuepath: values-on-prem.yaml ( File which needs to be used for helm rbc installation)
                        releasename: rbc (Name of the release for rbc)
                        pvtype: nfs
                        reset: 0
```



Note

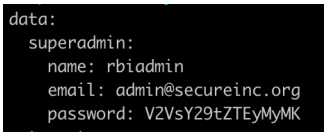
If the Core Master and RBC Master IP addresses are the same, then select **values-on-prem-single.yaml** instead of **values-on-prem.yaml** for both the **core** and **rbc** clusters.

g) Add database password (Default password is test123# encoded to base64).



h) Add superadmin details under the data tag. For example:

```
data:
                    superadmin:
                        name: rbiadmin (This will become the superadmin url e.g. https://
rbiadmin.secureinc.org
                        email: admin@secureinc.org (Administrators email address)
                        password: Default password is “Welcome123#” encoded to base64.
```



i) Add tenant details under the data tag. For example:

```
tenants:
                        host: rbi (This will become the tenant url e.g. https://
rbi.secureinc.org
                           email: admin@rbiinc.org (Administrators email address)
                           password: Default password is “Welcome123#” encoded to base64.
```

```
tenants:
- host: rbi-tenant-ggg
  name: Rbi-tenant
  squidport:
  admin:
    name: Rbi-tenant
    email: admin@rbi-tenant.org
    password: V2VsY29tZTEyMyMK
```

j) Add the tenant hostname in appliance-rbi:

```
appliances:
- name: appliance-rbi
  tenanthost: rbi
  minnodes: 2
  maxnodes: 2
  racversion: ract-direct:r89-5.5.11
  racurl: https://rbc-cluster-down.fp.dev
```

k) Add the **rac-url** (RBI server url) in **appliances-racurl**. Also, based on the license, modify the **minnodes** and **maxnodes**. For example, if the license is for 1,000 sessions, then minnodes can be 100 and maxnodes can be 1000.

```
  minnodes: 2
  maxnodes: 2
  racversion: ract-direct:beta-92-6.0.3
  racurl: rbc-cluster-gg.fp.dev
```

10) Edit the **values-on-prem.yaml** under **isla-rbc** for self-signed certificates.

```
nano /opt/rbi/rbi-installer/isla-rbc/values-on-prem.yaml
```

Note

- Edit the **values-onprem-single.yaml** instead of **values-onprem.yaml** if the Core Master and RBC Master IP addresses are the same.
- Add a row for CA in **isla-rbc-cluster-admin** section.
- Ensure that the CA is base64 encoded.

11) Run the **islasetup** from `/opt/rbi/rbi-installer`.

```
./islasetup cluster.yaml
```

Note

- If the Core and RBC workers IP addresses different for Single cluster Multi Master deployment, then run the below commands:

  a) Run `kubectl get nodes` and get the name against the worker(s).

```
maint@core-kubemaster-1:~$ kubectl get nodes
NAME                STATUS   ROLES                  AGE   VERSION
core-kubemaster-1   Ready    control-plane,master   19h   v1.20.4
core-kubeworker-1   Ready    <none>                 19h   v1.20.4
```

  b) The workers that needs to function for Core cluster make rbc labels false for the Core worker(s).

```
kubectl label nodes <core-kubeworker-#> isla/rbc-document-handler-node-
 isla/document-handling-node- isla/rbc-node-
```

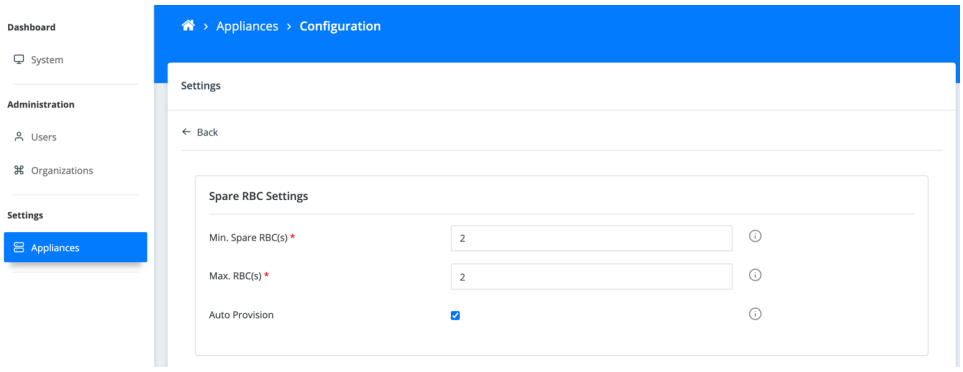
  c) The workers that needs to function for RBC cluster make core labels false for the RBC worker(s).

```
kubectl label nodes <core-kubeworker-#> isla/rbc-core-services- isla/cc-
core-services-
```

12) Add the required host file entries if DNS is not added to the public domain. For example:

```
Core Master ip rbiadmin.secureinc.org rbi.secureinc.org
RBC Master ip rbi-cluster.secureinc.org
RBC Worker1 ip(say x.x.x.x) rbchost-x-x-x-x.secureinc.org
RBC Worker2 ip(say y.y.y.y) rbchost-y-y-y-y.secureinc.org
```

13) After the installation, sign in to the Forcepoint RBI superadmin portal and select **Auto Provision** under **Settings** > **Appliances**.



14) For anonymous browsing, the URL will be **https://<replace_With_tenant_url>/viewer/loader?tenantId=<replace_with_tenantid>&username=<replace_with_username>url=<replace_with_site_navigate>**. The Tenant ID can be found in the Forcepoint RBI Admin Portal.

Chapter 3

Post-Deployment Steps

Contents

As part of the post-deployment steps, this chapter discusses implementing custom DNS, cipher implementation, and configuring SMTP.

Custom DNS implementation

This topic provides the procedure for implementing custom DNS when the public certificates are pointing to specific IP address.

Steps

1) Open the file in the editor.

```
sudo vim /etc/dnsmasq.conf
```

2) Update the file with following lines.

```
listen-address= <ip address of master>
interface= <Name of the interface>
# Nameservers
server= <DNS server IP>
server= <if having multiple DNS servers, add lines accordingly>
```

3) Make sure Master has `/etc/hosts` entries for the domain.

4) Update the `/etc/hosts` file with the below entries.

```
sudo nano /etc/hosts
```

```
RBC Worker1 ip(say x.x.x.x) rbchost-x-x-x-x.secureinc.org
RBC Worker2 ip(say y.y.y.y) rbchost-y-y-y-y.secureinc.org
```

5) Execute the below command to restart `dnsmasq` service.

```
sudo systemctl restart dnsmasq
```

6) Patch the core dns of the Kubernetes with IP address of master in config map.

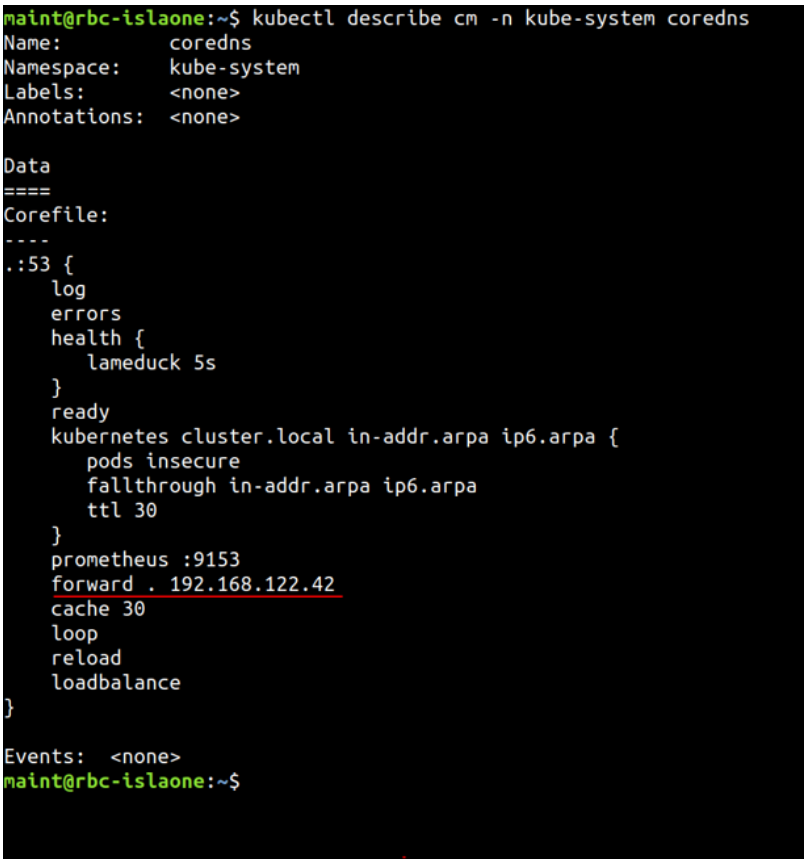
```
kubectl patch configmaps/coredns -n kube-system -p '{"data":{"Corefile":".:53
{\n errors\n health {\n lameduck 5s\n }\n ready\n kubernetes cluster.local
in-addr.arpa ip6.arpa {\n pods insecure\n fallthrough in-addr.arpa ip6.arpa\n
ttl 30\n }\n prometheus :9153\n forward . <ip address of master> {\n
max_concurrent 1000\n }\n cache 30\n loop\n reload\n loadbalance\n}\n\n"}}'
```

7) To watch `kube-system pod`, execute the below command:

```
watch kubectl get po -n kube-system
```

8) Confirm the changes in config map of `coredns`, once the `coredns` pods are restarted.

```
kubectl describe cm -n kube-system coredns
```



Cipher implementation

This topic provides the procedure for implementing the Forcepoint-approved ciphers.

Steps

1) SSH to the Core Master and edit kubelet config.yaml:

```
sudo vim /var/lib/kubelet/config.yaml
```

2) Add the following content to the end of the file:

```
tlsCipherSuites: [TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305,
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384]
```

3) Restart kubelet.service:

```
sudo systemctl restart kubelet.service
```

4) Edit kube-apiserver.yaml:

```
sudo vim /etc/kubernetes/manifests/kube-apiserver.yaml
```

5) Add the following content at the end of the **Command** section:

```
- --tls-cipher-suites=TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305,
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
```

6) Check that the nodes are up:

```
kubectl get node
```

7) Repeat these cipher implementation steps for all Masters.

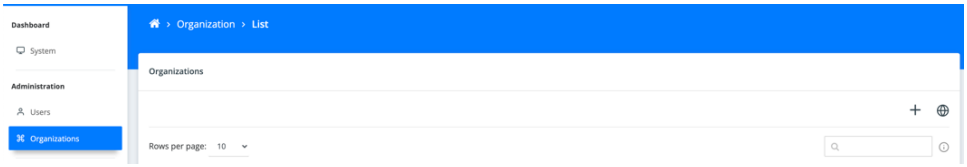
Configure SMTP

Simple Mail Transfer Protocol (SMTP) configuration enables email notifications to administrators through the Forcepoint RBI Portal.

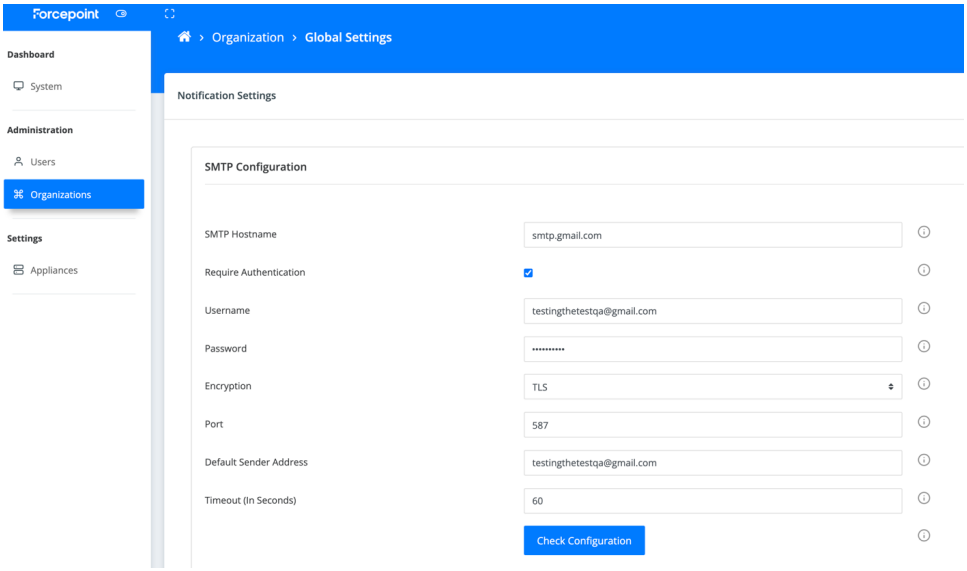
Steps

1) Sign in to the Forcepoint RBI superadmin portal and go to **Organizations**.

2) Click the globe icon to open Global Settings.



3) In **Global Settings**, enter the SMTP configuration shown in the following image:



4) Click **Check Configuration**. If the entered configuration settings are correct, then a **SMTP Configured Successfully** banner is shown at the top of the portal.

Note

If you are configuring a Gmail account to set up SMTP in the Control Center, then you need to enable **Less Secure App Access** under the account settings in Google.