Cisco Reverse Proxy Installer

Overview

The Cisco Reverse Proxy Installer (referred to as RP Installer in this document) is a component of the Cisco Unified CCE solution. It offers a ready-made reverse proxy solution (based on OpenResty Nginx) for Unified CCE, featuring built-in, battle-tested configurations. These configurations can be used to proxy other Unified CCE components and external applications, such as ADFS, which are commonly used when deploying Unified CCE.

The RP Installer has been pre-tested and load-qualified for various usage scenarios across the deployment models supported by the Unified CCE solution.

The RP Installer facilitates access to the Unified CCE solution from the internet and is typically set up to provide VPN-less access to the Finesse Agent Desktop or enable advanced functionalities like digital channels that require direct internet ingress.

The RP Installer is intended to be deployed in a Demilitarized Zone (DMZ) on a customer-provided and hardened host running the RHEL 9.4 Operating System. The pre-configured proxying rules allow for the proxying of the following components through data-driven configuration files:

- Cisco Finesse
- Cloud Connect
- Cisco Unified Intelligence Center
- Live Data
- Cisco Identity Service
- Cisco IM&P Server
- Microsoft ADFS 3.0 or 5.0

Attention The term "upstream servers" is used in this guide to refer to all the solution components such as Finesse, CUIC, IdS, and IM&P servers that are configured to be accessed through reverse-proxy.

Prerequisites

To configure VPN-less access to the Finesse desktop:

- Reverse Proxy Installer must be 15.0(1) or above
- Finesse, IdS, and Cisco Unified Intelligence Center must be 12.6(2) ES4 or above.
- In coresident deployments, LiveData and Cisco Unified Intelligence Center should be 12.6(2) or above
- Unified CCE and LiveData standalone must be 12.6(1) or above with the latest ES for the respective versions.
- Cisco IM&P Server
- DMZ with internet connectivity must be available to host the reverse-proxy.

Security

The RP Installer is not an open proxy; it authenticates all requests before forwarding them to the appropriate upstream server. The upstream servers also enforce local authentication before processing the requests.

Beyond authentication, there are several additional security measures available to protect the solution. Details about security can be found in the Security chapter.

For information about security guidelines, see the *Security Guidelines for Reverse-Proxy Deployment* in Security Guide for Cisco Unified ICM/Contact Center Enterprise.

For more information on authentication, refer to Authentication.

Host Mapping File for Network Translation

Reverse proxy deployment relies on a mapping file provided by the administrator to configure the list of externally visible hostname/port combinations and their mapping to the actual server names and ports that are used by the Finesse, IdS, and CUIC servers. This mapping file which is configured on the upstream servers is the key configuration that allows the clients connected over the internet to be redirected to the required hosts and ports that are used on the internet. For more information on mapping, refer to Populate Network Translation Data.

Note It is recommended to use a dedicated web server within the LAN to host the mapping file, rather than using the Reverse Proxy installer for this purpose.

For all the requests that come through the reverse-proxy, the Finesse, IdS, and CUIC servers check the host mapping file, to translate the internal hostnames and ports that are used on the LAN. They are translated to the publicly resolvable hostnames and ports that have to be used on the internet. This mapping file, referred to as the Proxy-config map file, is the key configuration that allows the clients connected over the reverse-proxy to be redirected to the required hosts and ports that are used on the internet.

The Proxy-config map file can be configured by using CLI available on Finesse, IdS, and CUIC servers. For details on the mapping file format and the data configured, refer to the Populate Network Translation Data section. For details on the CLI used to configure the file, refer to the **utils system reverse-proxy config-uri** CLI in the topic Configure Proxy Mapping by Using CLI.

The Proxy-config map file can be configured by using CLI available on Unified CCX servers and Cisco Collaboration Platform servers. For details on the mapping file format and the data configured, refer to the *Populate Network Translation Data* section in *Cisco Unified Contact Center Express Administration and Operations Guide*. For details on the CLI used to configure the file, refer to the *Configure Proxy Mapping by Using CLI* section in *Cisco Unified Contact Center Express Administration and Operations Guide* available at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-maintenance-guides-list.html..

Port Management

One of the main design aspects in deploying a reverse proxy are the domain and the ports used to access the application. These aspects are interdependent and influence each other when designing the deployment.

The reverse proxy must be able to determine, to which upstream server, an incoming request can be forwarded to where an incoming request should be forwarded to. This can be accomplished by changing either the port or the hostname used to access the application. Essentially, the combination of host and port must be unique in order for the proxy to differentiate and route traffic to the correct upstream component, and it is a requirement for the proxy to even start correctly.

These are therefore the options available to design the domain and port access:

- Use a common domain and differentiate application access using multiple ports.
- Use a common port and differentiate application access using multiple domains

Once the domain and the port distribution is determined, the following steps needs to be taken:

1. Proxy map configuration has to be changed to match the port and domain required. See Configure Proxy Mapping by Using CLI.
2. The respective upstream component environment configuration in the reverse proxy installer has to be configured with the required hostname and port, see Configure deployment environment configurations

Using a common domain with multiple ports

The following example illustrates how multiple application servers can be configured using this access pattern:

- FinesseA = ReverseProxyDomain.com:8445
- FinesseB = ReverseProxyDomain.com:8446
- Finesse1A = ReverseProxyDomain.com:8447
- Finesse2B = ReverseProxyDomain.com:8448

The following are the benefits of using multiple ports:

- More granular packet level rate-limits applicable to each application can be applied at the ingress point to control rate-limits. Domain-level access means that the rate-limits can't be granular.
- A single-domain requires only a single SSL certificate to access the application. It could be a factor in reducing costs, unlike a multiple-domain application which requires a wildcard certificate.

The following are the disadvantages in using multiple ports:

- Certain network deployments like CDNs don't support custom ports.
- Security devices that automatically apply security rules might require custom configurations with non-standard ports.
- Multiple ports must be opened in the DMZ firewall (10–15 ports are required for a standard 2k deployment). This isn't recommended by the network security teams.
- There's an increased overhead regarding the port manageability.
- Deploying new instances of the application requires firewall/network changes.

Note Ports other than the ones mentioned in the ProxyMap must be blocked and shouldn't be available for access on the reverse proxy host. This must be blocked at the ingress point as the proxy doesn't currently have rules to block this access at network level.

The Cisco provided installer supports running multiple instances which cater to different sets of upstream servers, to aid in ease of maintenance. Multiple instances of the installer don't allow to use the same ports across different instances of the proxy. Only one process can bind to the same TCP port.

Consider the above two points when deciding the port management strategy against proxy installer configuration.

Using a common port and with multiple domains

The following example illustrates how multiple application servers can be configured using this access pattern.:

- FinesseA = FinesseA-ReverseProxyDomain.com:443
- FinesseB = FinesseB-ReverseProxyDomain.com:443
- Finesse1A = Finesse1A-ReverseProxyDomain.com:443
- Finesse2B = Finesse2B-ReverseProxyDomain.com:443

The single port configuration reverses the pros and cons listed above with the multiple port configuration.

Note Supporting a single port of access requires Unified Intelligence Center and LiveData components to be on 12.6(2)versions.

DNS Configuration for Finesse, IdS, and CUIC Servers

Each Finesse, IdS, CUIC, IM&P, and third-party component servers corresponding to a host that needs Internet access must be addressable from the Internet. This calls for a hostname and associated port which is resolvable from the Internet to be mapped to the public port and matching IP of the reverse-proxy so that the traffic is directed to the respective component servers.

DNS registration of the publicly resolvable hostnames and the corresponding IP addresses is mandatory before the requests reach the reverse-proxy.

SSL Certificates

For the hostnames that are configured, corresponding to each unique hostname that is used by the internet client, the respective certificates must be acquired and configured on the reverse-proxy. Even though self-signed certificates are supported, they are risky because the users access directly from the internet. The clients can be more secure by using CA-signed certificates. The best practice is to get CA certificates for proxy servers and third-party-gadget servers.