



# Security Considerations for Reverse Proxy Deployment

---

- [Security Guidelines for Reverse-Proxy Deployment, on page 1](#)

## Security Guidelines for Reverse-Proxy Deployment

To allow VPN-less access, reverse-proxy hosts must be directly accessible from the internet. Therefore, security is crucial in a reverse-proxy deployment. This section provides a set of guidelines to secure a reverse-proxy deployment.



---

**Note** The guidelines and recommendations provided are intended to be used as a minimum required guidance for administrators to secure the deployment. The deployment, configuration, and security of reverse-proxy and the network is the Contact Center's responsibility.

---

## Reverse-Proxy

The reverse-proxy is the first application-level landing point for all requests that come into the Cisco Contact Center network from the internet. The reverse-proxy must have a high level of security to withstand attacks. The following are the guidelines to secure a reverse-proxy deployment:

- Configure TLS 1.2 and turn off other TLS protocols.
- Allow only secure HTTP/1.1 based access.
- Turn off default access and default rules for your proxy to avoid unplanned access to the proxy.
- Ensure that the reverse-proxy and the host systems are up to date with security patches to prevent potential breaches.
- Ensure that the reverse-proxy is not allowed to establish direct outbound connections to the internet.
- Harden your proxy host to ensure its safety when exposed to the Internet. For best practices, refer to <https://www.cisecurity.org/cis-benchmarks/>.
- Conduct regular security audits on reverse-proxy hosts to ensure that their security has not been compromised.

- For security reasons, ensure that API paths other than those explicitly exposed are not available through the configured rules. If OpenResty Nginx reverse-proxy is being deployed, refer to the OpenResty Nginx rules in the [Nginx Technote article](#) to find the paths which are explicitly opened for each Finesse, IdS, and CUIC servers.
- Caching is important from a security perspective because most of the static resources are unsecured. Simple DoS attacks can be prevented by caching these resources on the Finesse server. However, the resources have to be validated periodically with the Finesse, IdS, and CUIC servers to ensure that the resources are the latest.
- Validate the HOST headers to ensure that only the intended domains are accessed by the client.
- Regulate the WebSocket connections of Finesse, IdS, and CUIC servers for each domain corresponding to the expected number of clients.
- It is a best practice to maintain security hardened golden images of the reverse-proxy with updated patches and configuration changes. Installing from these golden images ensure that all the reverse-proxy instances are consistent and are as secure as possible.




---

**Note** For Nginx-based reverse-proxy rules, installation, configuration, and security hardening instructions, refer to the [Nginx TechNote article](#). Any reverse-proxy supporting the required criteria (as mentioned in the **Reverse-Proxy Selection Criteria** section of [Cisco Unified Contact Center Enterprise Features Guide, Release 12.6\(1\)](#)) can be used in place of Nginx for supporting this feature.

---

## Demilitarized Zone Security

Without an ongoing process and related efforts to ensure that the security of the network and the hosts are updated, a reverse-proxy deployment cannot maintain its security posture. The following are the important points to ensure that the DMZ is secure:

- Consider using dual firewalls (instead of a single firewall with multiple interfaces) to separate the DMZ from the internal network.
- Configure rules in the internal firewall to ensure that the requests originating from the DMZ do not reach hosts other than the ones configured in the reverse-proxy.
- Ensure that the DMZ is separated from the internal network with isolated routing and security policies.
- The security of the reverse-proxy deployment depends on the process to keep the configurations and software updated.

## Rate Limit

## Network Security Devices

Network security devices that incorporate Intrusion Prevention System (IPS) functionality must be deployed to offer additional security to the traffic that enters the DMZ. These are devices that can prevent entire class of attacks that a proxy or firewall is not equipped to detect or prevent effectively. While deploying IPS devices, deploy devices that can detect Distributed Denial of Service (DDoS) signatures to guard against DDoS attacks.

### Web Application Firewalls

Web Application Firewall (WAF) provides a higher layer of security for reverse-proxy deployments. The WAF devices extend the security checks into the application layer. This is achieved by inspecting the web application traffic for scripts, headers, cookies, HTTP methods, and so on to find known vulnerabilities and loopholes to block malicious traffic. This prevents diversified cyber-attacks that exploit vulnerabilities that are specific to web applications. You can have devices that integrate IPS and WAF functionalities or use cloud services that provide all the above-mentioned capabilities.

## DDoS Protection

Sophisticated attacks that get past the rate limits by using multiple clients to initiate DoS attacks are referred to as DDoS attacks. Individual systems are often unable to detect or react properly to DDoS attacks. To avoid such attacks, ensure that the traffic is regulated by applying proper rate limits.

One of the most effective ways to handle DDoS attacks is to employ Content Distribution Networks (CDN) that provide a high level of protection against most attacks and can absorb the brunt of these brute force attacks. Incorporating IPS devices, routers, or a firewall that can detect DDoS signatures can also help in preventing such attacks.

## Reverse-Proxy Security Configuration

Reverse-proxy configuration is one of the areas that produces the biggest potential security flaws when configuring a proxy. The rules configured should be compared against known vulnerabilities and must be created to protect the applications that are being configured, such that, only the desired end points are exposed. The proxy, being the initial ingress point, plays a significant role in enhancing the security posture of the deployment. The following are the additional security enhancements included with the Nginx configuration:

- Brute Force Attack Prevention
- Mutual TLS Verification
- SELinux Rules

