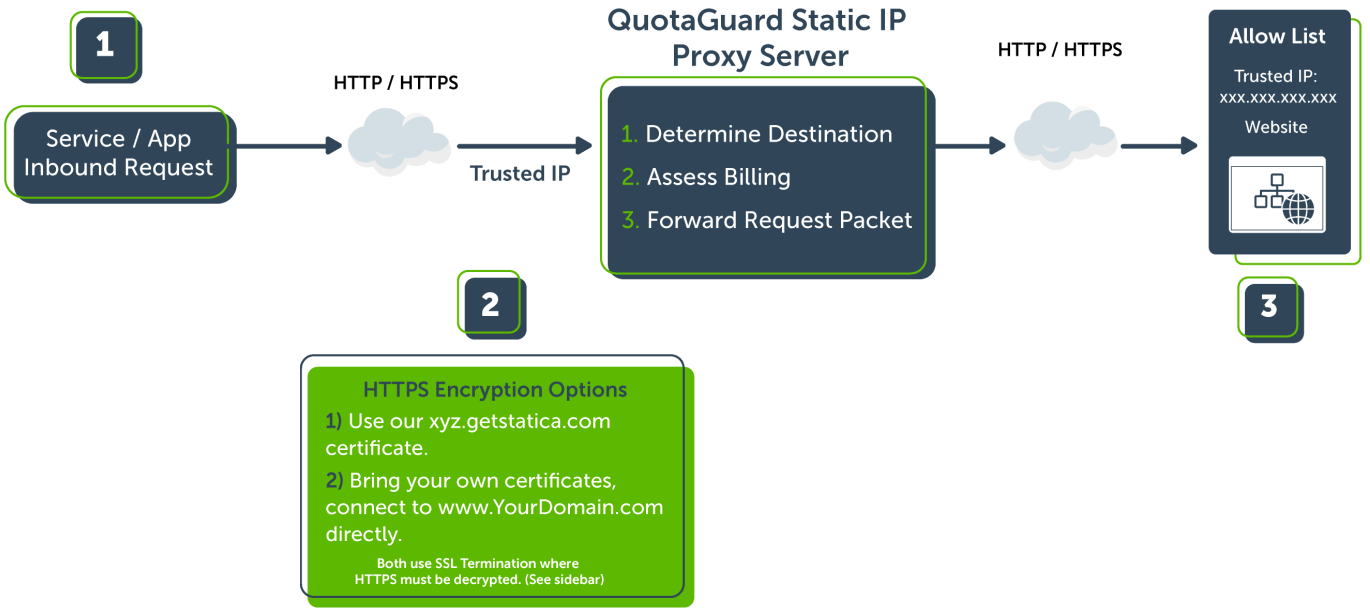
QuotaGuard Static Inbound Requests

HTTP / HTTPS



Inbound Proxy - QG Static vs. QG Shield

WHAT IS SSL TERMINATION / SSL OFFLOADING?

SSL termination (a.k.a. SSL Offloading) decrypts all HTTPS traffic when it reaches the proxy server. At this point, routing is executed and the data proceeds to the destination server as plain HTTP traffic.

If your QuotaGuard implementation uses a HTTPS URL for the forwarding URL (as most customers do), then the data between QuotaGuard and the final destination is encrypted as well.

However, all Static IP proxies have to decrypt the data, using security keys, to determine the next hop and then re-encrypt the data before it is sent to the next point.

1

An outside Service / Application / Website sends a HTTP/HTTPS request to your internal protected resource via our Static IP proxy server.

2

HTTP requests are passed via the proxy server to the internal resources.

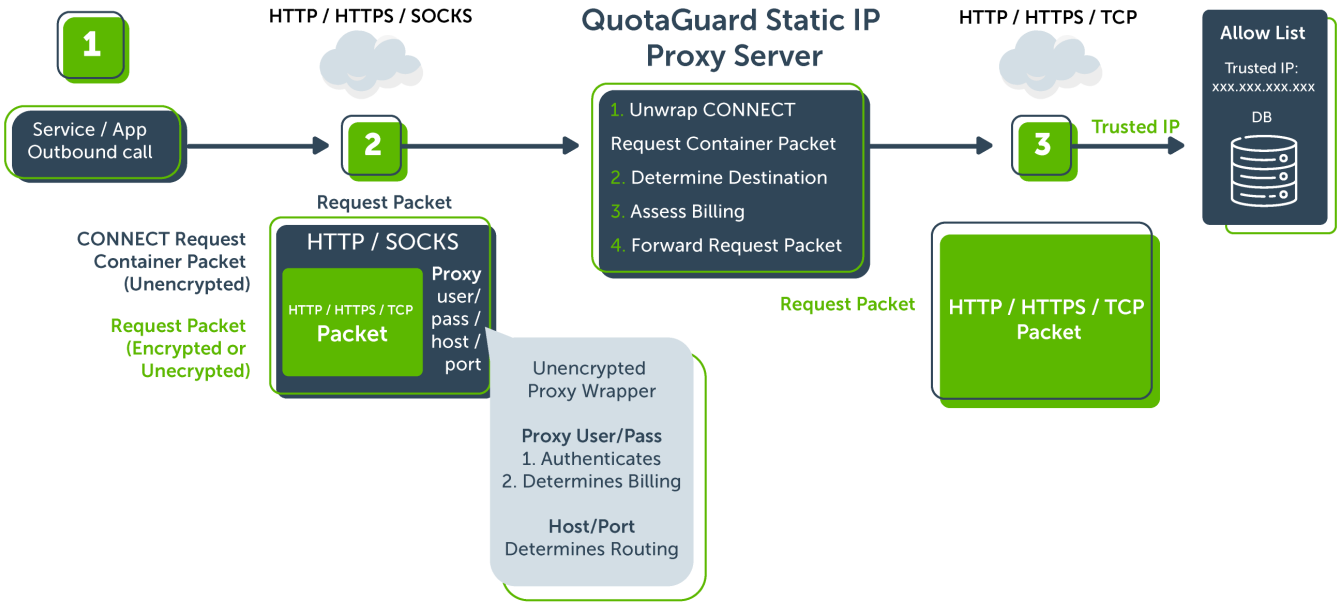
HTTPS requests are decrypted to determine internal routing, then re-encrypted and forwarded to the destination.

3

The destination firewall or server allows the known IP source inbound, processes the request, and the reply would go back to the originating service through the Static IP proxy.

QuotaGuard Static Outbound Requests

HTTP / HTTPS / TCP



Outbound Proxy - QG Static vs. QG Shield

SECURITY RISKS OF HTTPS ON QG STATIC

(and all other Static IP services)

HTTPS outbound traffic is secure, however... the "service to proxy" container CONNECT request is not secure.

TECHNICAL

Bad actors in possession of your Proxy Credentials can send traffic via your Static IP proxy that would appear to originate from your trusted IP address and allow attackers to spoof protected resources/firewalls into allowing in illegitimate traffic.

As such, this solution is not PCI/HIPAA compliant due to the clear text user/pass between the outbound service call and the Static IP proxy server.

MANAGERIAL

Unnecessary billing charges and costs.

1

Your Service / Application / Website initiates a HTTP/HTTPS/TCP request to a remote server.

That request is wrapped in a HTTP or SOCKS container packet for the CONNECT request to connect to our proxy.

The request packet is encrypted (if HTTPS or other encrypted protocols), but the container CONNECT packet is not encrypted.

2

The proxy removes the outside container from the CONNECT connection to read the username and the password for the proxy, as well as the final destination hostname and port.

We use the user/pass to verify the sender and for billing processing.

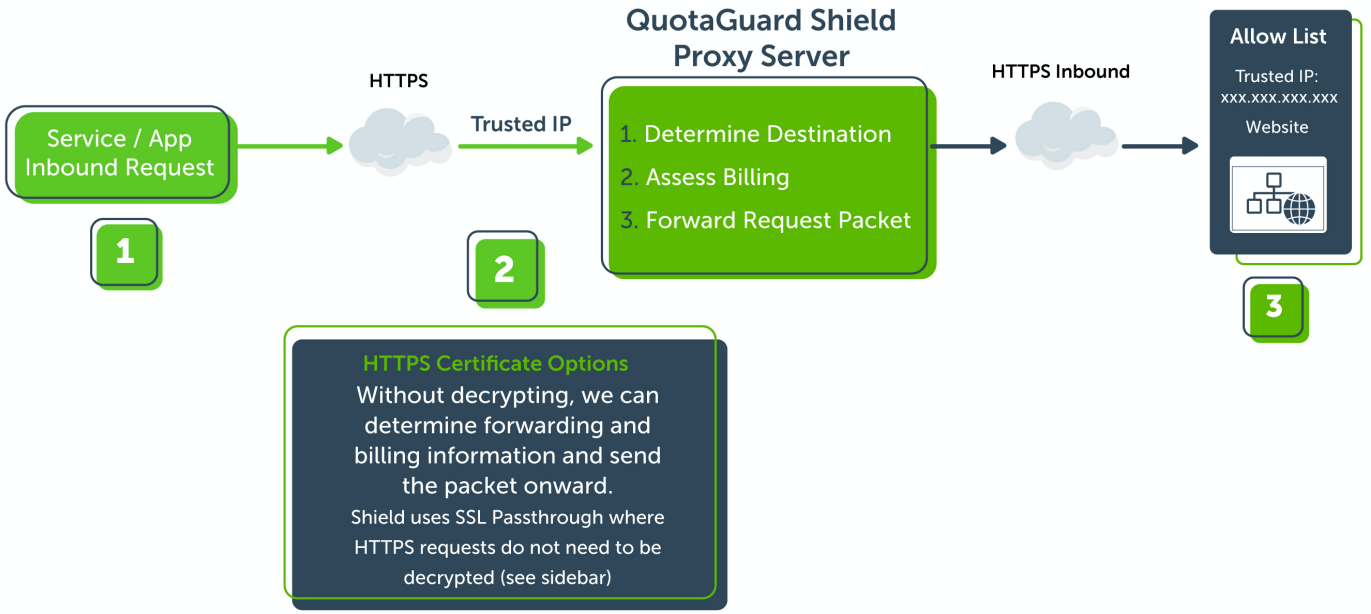
The inner packet (HTTP/HTTPS/TCP) is then forwarded on to the destination server.

3

The destination firewall or server allows the known IP source inbound, processes the request, and the reply would go back to the originating service back through the proxy.

QuotaGuard Shield Inbound Requests

HTTPS Required



Inbound Proxy - QG Static vs. QG Shield

WHY IS SHIELD MORE SECURE AND EASIER TO USE?

1) HTTPS is never decrypted on the QG Shield Proxy server.
2) Final destination hostname and port are secure, helping prevent bad actors from determining what services are open to the proxy's IPs.

3) QuotaGuard never needs access to your security keys.

4) Significantly easier to set up since you control the security settings and requires no coordination with QG.

WHAT IS SSL PASSTHROUGH?

SSL passthrough passes encrypted HTTPS traffic all the way to the backend server **without** decrypting the traffic on the proxy.

QuotaGuard Shield uses SNI to determine billing and routing.

Therefore, traffic passes through the proxy encrypted and the destination server (web application server, database server, etc.) does the decryption process to read the data.

1

An outside Service / Application / Website sends a HTTPS request to your internal protected resource via our Static IP proxy server.

2

HTTPS requests are decrypted to determine internal routing, then re-encrypted and forwarded to the destination.

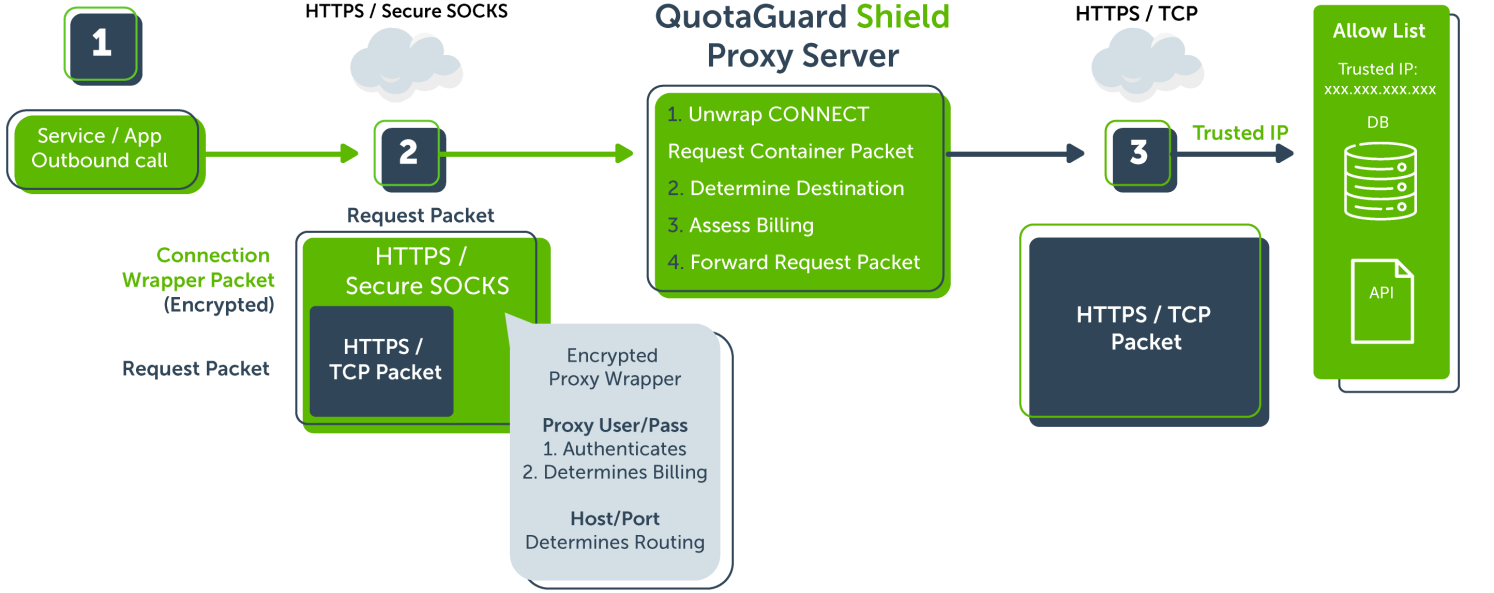
3

The destination firewall or server allows the known IP source inbound, processes the request, and the reply would go back to the originating service through the Shield Static IP proxy.

QuotaGuard Shield Outbound Requests

Outbound Proxy - QG Static vs. QG Shield

HTTPS / Secure SOCKS



WHY IS SHIELD MORE SECURE AND EASIER TO USE

1. Proxy Credentials are secure, preventing bad actors from impersonating your application.
2. Final destination hostname and port are secure, helping prevent bad actors from determining what services are open to the proxy's IPs.

1

Your Service / Application / Website initiates a HTTPS/TCP request to a remote server.

That request is wrapped in a HTTPS or Secure SOCKS container packet for the CONNECT request to connect to our proxy.

The request packet is encrypted and the container CONNECT packet is encrypted.

2

The proxy decrypts the outside container from the CONNECT connection to read the username and the password for the proxy.

We use the user/pass to verify the sender and for billing processing.

The inner packet is then forwarded on to the destination server.

3

The destination firewall or server allows the known IP source inbound, processes the request, and the reply would go back to the originating service back through the proxy.