# F5® Silverline™ DDoS Protection Onboarding: Technical Note

# F5 Silverline DDoS Protection onboarding

F5 Networks® is the first leading application services company to offer a single-vendor hybrid solution for DDoS protection on-premises and as a cloud-based service with F5® Silverline™ DDoS Protection.

By combining F5 Networks' on-premises DDoS protection solutions with Silverline DDoS Protection cloud scrubbing service, you can keep your businesses online when under DDoS attack with a reduced risk of downtime, the fastest DDoS mitigation response times, unparalleled visibility and reporting, and cost efficiencies that cannot be achieved with other multi-vendor choices for on-premises and cloud-based services.

## Terminology

*Border Gateway Protocol (BGP)* is a standardized exterior gateway protocol designed to exchange routing and reachability information between autonomous systems (AS) on the Internet.

*Generic Routing Encapsulation (GRE)*, defined by RFC 2784, is a simple IP packet encapsulation protocol. GRE is used when IP packets need to be sent from one network to another, without being parsed or treated like IP packets by any intervening routers. GRE is supported by all major Edge routers.

## Detecting a DDoS attack

The simplest way to know if you are under attack is looking at your bandwidth graph. 24 hours of normal traffic looks like nice bell curves. DDoS attacks hit all at once. It looks like a plateau instead of a rolling hill. One minute normal traffic, the next minute you see 10 times what you would expect. Not a gradual rise, you see the effect of 50,000 bots all attacking at the exact same second. From the portal dashboard, you can see a sudden but consistent increase in network traffic when an attack is in progress.

## Activating your service

Most configuration can be completed using the Silverline DDoS Protection portal at http://portal.defense.net. Using your username and password provided to you, sign in to the user portal. Then set up the passphrase that is used to verify the customers communicating by phone.

Silverline DDoS Protection utilizes two methods to protect users from DDoS attacks and send the clean traffic to the appropriate destinations.

## Routed Mode

Silverline DDoS Protection leverages Border Gateway Protocol (BGP) to route all the traffic to its scrubbing and protection center and utilizes a GRE tunnel to send the clean traffic back to the customer network. *Routed mode* configuration is a very scalable design for enterprises with large network deployments. Routed mode configuration does not require any application specific configuration, and provides an easy option to turn on or off the Silverline DDoS Protection.

### Requirements

In order to leverage the Routed Mode, the Silverline DDoS Protection requires a Class C (/24) IP address range.

The customer needs to have Edge Router that can terminate GRE tunnels with addressing outside of the IP address blocks to protect the termination to these tunnels. In most cases, this can be IP address space provided by the Internet Service Provider (ISP) on the transit link.

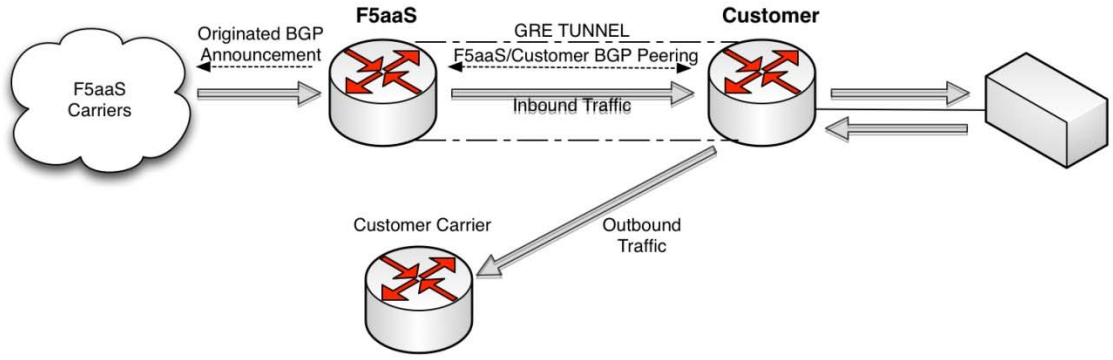
The customer must have an eBGP (external BGP) relationship with their ISP.

## Configuration

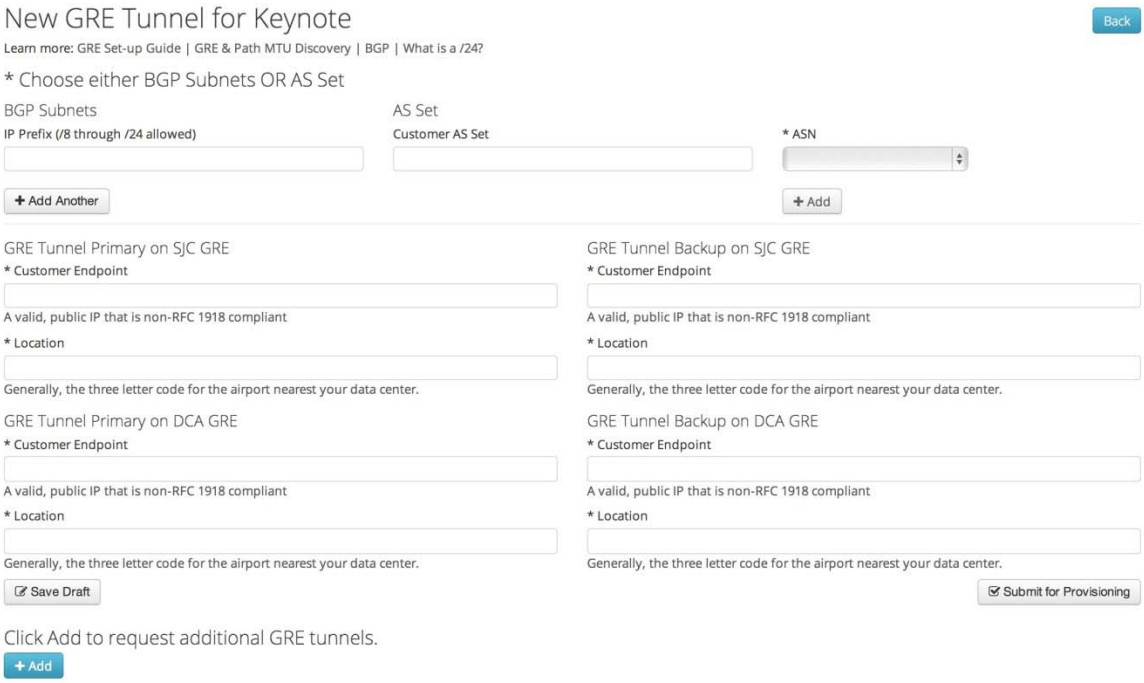
When a customer subscribes to Silverline DDoS Protection, the customer has to do the following steps once the F5 service is configured.

1. Enter configuration data into the Silverline DDoS Protection portal.
2. F5 will complete configuration, including GRE tunnels and BGP sessions (will be inactive).
3. Customer configures GRE tunnels. Verifies functionality.
4. F5 and customer coordinate activating BGP sessions.
5. Customer announces affected subnet via BGP.
6. Once a verified announcement is propagating to F5 carriers, the customer may retract routes from normal carriers to ensure that ALL traffic flows through F5 scrubbing centers.

Once the service is activated, all traffic starts to flow to this service:




**Additional details about setup can be found at the customer portal under Settings-> Configuration**




## Proxy Mode

Customers who do not control a full Class C network or prefer to protect only a few applications can use the Proxy Mode to protect their applications and networks. Customers can support a wide variety of applications with Proxy mode including IPv4, IPv6, SIP, FTP and many more TCP, UDP and IPsec based applications. The Proxy mode can be set up very quickly with minimum impact to the customer's existing network setup.

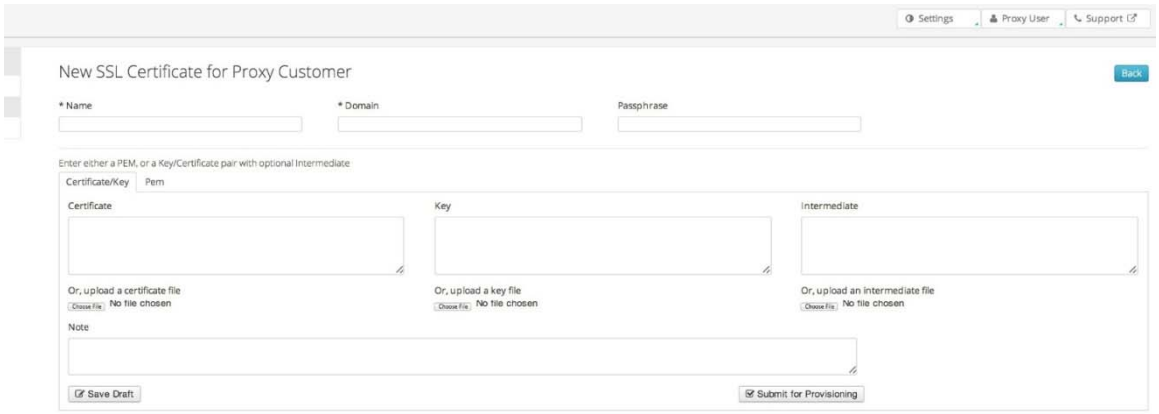
## Requirements

The requirements for setting up proxy mode are minimal. It requires the ability to block IP addresses at the Provider Edge (PE), and the ability to update DNS settings for the applications to be protected.

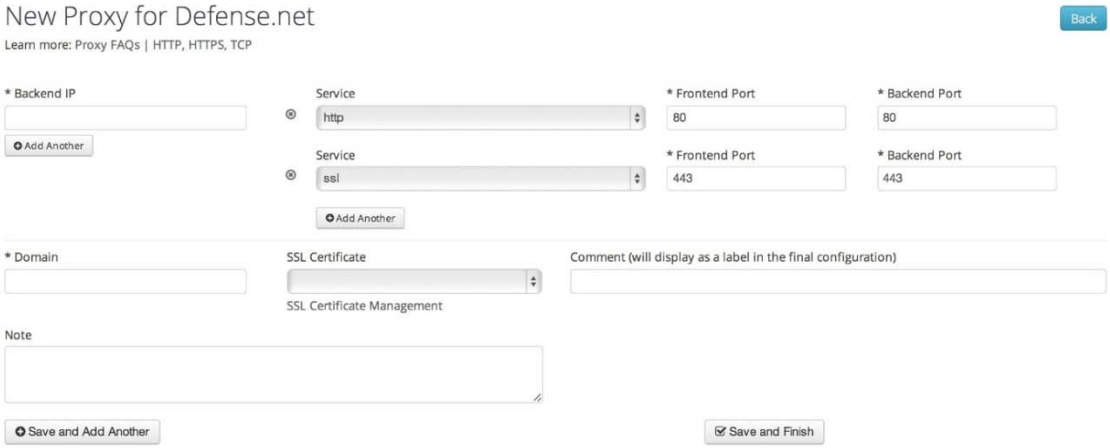
## Configuration

In order to set up the proxy mode, log in to the portal and navigate to the configuration section and make the following changes:

1. Import SSL keys to the proxy for SSL traffic.




2. Complete proxy configuration on the portal, the server IP also known as backend IP, service, and ports, are required to configure a proxy set-up. Multiple ports can be configured on the same frontend/backend IP pair.




3. Change or request your DNS provider to change the DNS for the domain and point to the IP addresses which are provided by F5.
4. Optionally, the customer can request their carrier to implement ACL, which whitelists F5 IP addresses, blacklisting all others.

# Legal Notices

## Copyright



## Trademarks



## Patents

This product may be protected by one or more patents indicated at http://www.f5.com/about/guidelines-policies/patents.

# Index