QUICK REFERENCE

F5 DDoS Attack Quick Reference Sheets

These templates for quick reference sheets, when filled out in advance, can help you successfully fight a distributed denial-of-service (DDoS) attack.

The following Quick Reference sheets supplement the F5 *10 Steps for Mitigating DDoS in Real Time Playbook*. The 10 steps you should take to mitigate an attack are summarized below. Please revisit the playbook for helpful reminders of how to best use the Quick Reference sheets.

10 steps for mitigating a DDoS attack:

- Step 1: Verify the attack.
- Step 2: Contact team leads.
- Step 3: Triage applications.
- Step 4: Protect partners and remote users.
- Step 5: Identify the attack.
- Step 6: Evaluate source address mitigation options.
- Step 7: Mitigate specific application attacks.
- Step 8: Increase application-level security posture.
- Step 9: Constrain resources.
- Step 10: Manage public relations.

When completed in advance, the Quick Reference sheets will assist you in repelling a DDoS attack. They include:

- Quick Reference 1: Contact List. Fill this out as you initiate contacts.
- Quick Reference 2: Whitelists. Map your partners, users, and services.
- Quick Reference 3: Application Triage. Know your own applications.
- Quick Reference 4: Device Map. Create a device map.
- Quick Reference 5: Attack Log. Note the attack details.

The completed references can be kept in your data center and used for documentation and attack mitigation. If you have not recorded this information prior to your first attack, record it as you collect it to better prepare for a future attack.

Quick Reference 1: Contact List

Many different teams may need to come together to fight a large, hectic DDoS attack. Use this form to collect and maintain contact information for the different teams and agencies that might be required during a DDoS attack. Add rows as necessary.

Team	Name	Phone	Email
Network Security			
Threat Intelligence			
Applications Director			
DNS Manager			
F5 Professional Services		1-888-88-BIG-IP	
Reseller Services			
Bandwidth Service Provider			
Public Relations Director			
Fraud Team Liaison			
Financial Comptroller			

Quick Reference 2: Whitelists

Maintain the list of IP addresses that must always be allowed access.
Addresses that should be recorded here include:

- External monitoring tools.
- Google and the other search engines you do not want to block.
- Your own global traffic managers (GTMs). These will be monitoring your applications throughout the attack.
- Your DDoS cloud-scrubbers such as F5 Silverline DDoS Protection.
- Your other cloud service providers (this could be large list).
- Business partners.

IP Address Range	Maps to?	External Contact	Internal Contact

Quick Reference 3: Application Triage

For all applications at the data center:

1. Decide on and record a priority value indicating whether or not it should be disabled.
2. Record a triage decision. (You can use the priority value to assert a decision like "disabling all applications that are priority 3 or lower").
3. Add application owner contact information if necessary.

A defined set of priorities may enable you to automate tasks. For example, you can write a script to disable (and later re-enable) all applications with a priority of 3 or lower.

Application Name		Priority	Triage	Associated Virtual Server	Location
1	Example Application	2	Disable	dc1-rxspc.example.com	
2					
3					
4					
5					
6					
7					
8					
9					
10					

Quick Reference 4: F5 Device Map

If you engage F5 Professional Services during the DDoS attack to assist with defense, it will be helpful to have a map of available F5® BIG-IP® devices in the data center, along with their serial numbers and the other information here. This information will guide those advising you on defensive strategies. The command below provides the serial number and the platform type:

```
%tmsh show sys hardware
```

Both of the F5 configuration management solutions, F5 Enterprise Manager™ and F5 BIG-IQ® Centralized Management, gather the device information (other than the location) for you and may assist you in filling out this table. Keep this information with Quick Reference 1: Contact List. Better yet, keep all of your quick references in one place.

F5 Device		Model	Modules	Serial Number	Location
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					

Quick Reference 5: Attack Log

Information recorded here can be useful for after-action reporting, lessons learned, and regulatory reporting requirements. Print out several copies of this page and use it as a cover sheet for notes taken during the attack.

DDoS Attack Log	

Source addresses may be turned over to the authorities. If the addresses are isolated to a specific country, the attack may be mitigated via geolocation (see Step 6 in the vF5 DDoS Playbook).

Source Address Analysis
Geolocation:
Source Address:

Once the attack is over, provide a summary that includes a description of the attack, the mitigations that worked, and those that did not work. Include services that were disabled and their weaknesses. Use that information to evolve your services before the next attack.

Attack Summary
Geolocation:
Source Address:

Solutions for
an application world.