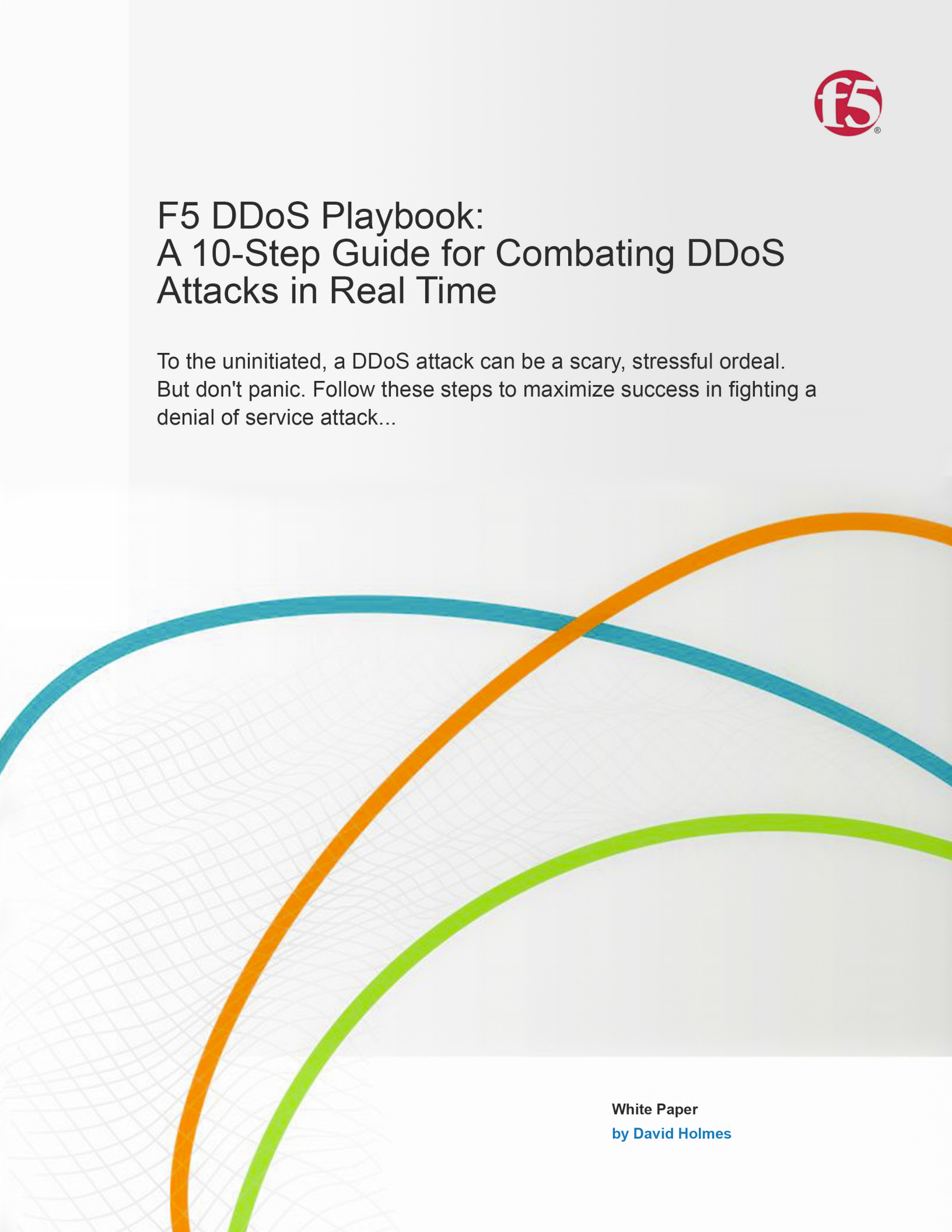

F5 DDoS Playbook: A 10-Step Guide for Combating DDoS Attacks in Real Time

To the uninitiated, a DDoS attack can be a scary, stressful ordeal. But don't panic. Follow these steps to maximize success in fighting a denial of service attack...

White Paper

by David Holmes

Contents

Concept

DDoS

Distributed Denial-of-Service (DDoS) attacks are a top concern for many organizations today. A DDoS attack creates a security breach with a website, saturates the server's connections, renders its services inoperable, and prevents legitimate clients from being able to connect to it. For the uninitiated, it can be a scary and stressful ordeal!

DDoS attacks are usually coordinated across a large number of client computers (which may have been set up for that purpose), or more likely, have been infected with a virus that allows someone to remotely control the computer, making it participate in the attack.

2014
DDoS
Attack Frequency

Both financially and politically motivated, DDoS attacks are becoming more prevalent. Although a first attack can happen randomly, it often occurs when an attacker with specific knowledge of *your* high-value service, decides to take it off-line. This can cause panic, and instigate costly "ransom-like" decisions to triage and stop the attack.

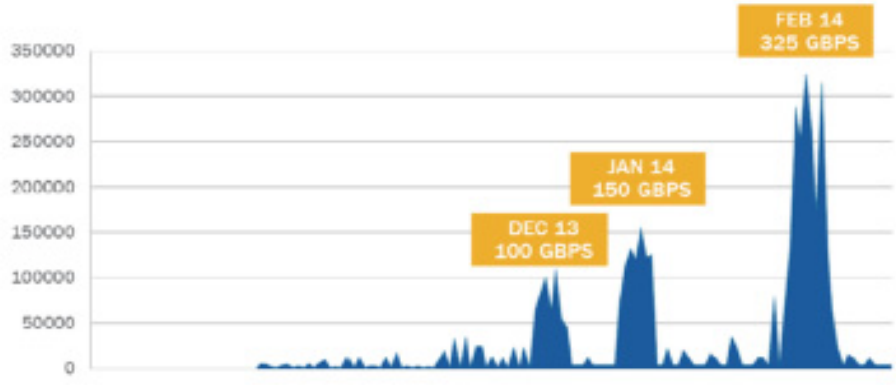

Figure 1. Volumetric Attacks Increase in 2014

Organizations that have defended against multiple DDoS attacks understand the importance of having an objective method to assist in combating them.

What is their solution? **The F5 DDoS Playbook**.

This document can be the basis for developing that tool for your organization.

The Five Worksheets

There are five worksheets to complete that will assist you in repelling a DDoS attack. *Once completed*, these worksheets can be kept in your data center and used for reference purposes.

- **Worksheet 1: Contact List**–Fill it out as you initiate contacts (page 21).
- **Worksheet 2: Whitelists**–Map your partners, users, and services (page 22).
- **Worksheet 3: Application Triage**–Know your own applications (page 23).
- **Worksheet 4: Device Map**–Create a device map (page 24).
- **Worksheet 5: Attack Log**–Note the attack details (page 25).

If you have not recorded this information prior to your first attack, record it as you collect it.

Your organization may have regulatory compliance statutes that require a level of reporting around cyber-attacks, breaches, or even DDoS attacks. "Worksheet 5: Attack Log" on page 25 can assist you in this situation, as you can track and refer to the log later during the reporting process.

Regulatory Compliance

Preparing for a DDoS Attack

DDoS-Resilient Architecture

If you are fortunate enough to be reading this document *prior* to being attacked, then there are steps that you can take now to make your applications, networks, and processes, DDoS-resilient.

Network Defense Architecture Considerations

After you have filled out the worksheets, obtain the *F5 DDos Recommended Practices* document so you can consider how to lay out your network architecture defenses.

Multi-Tier Approach DDoS Architecture

F5 recommends a **Multi-Tier Approach DDoS Architecture**, where Layer 3 and Layer 4 DDoS attacks are mitigated at the Network Tier, with firewalls and IP reputation databases (*see Figure 2. F5 Recommends a Multi-Tier DDoS Approach Architecture*).

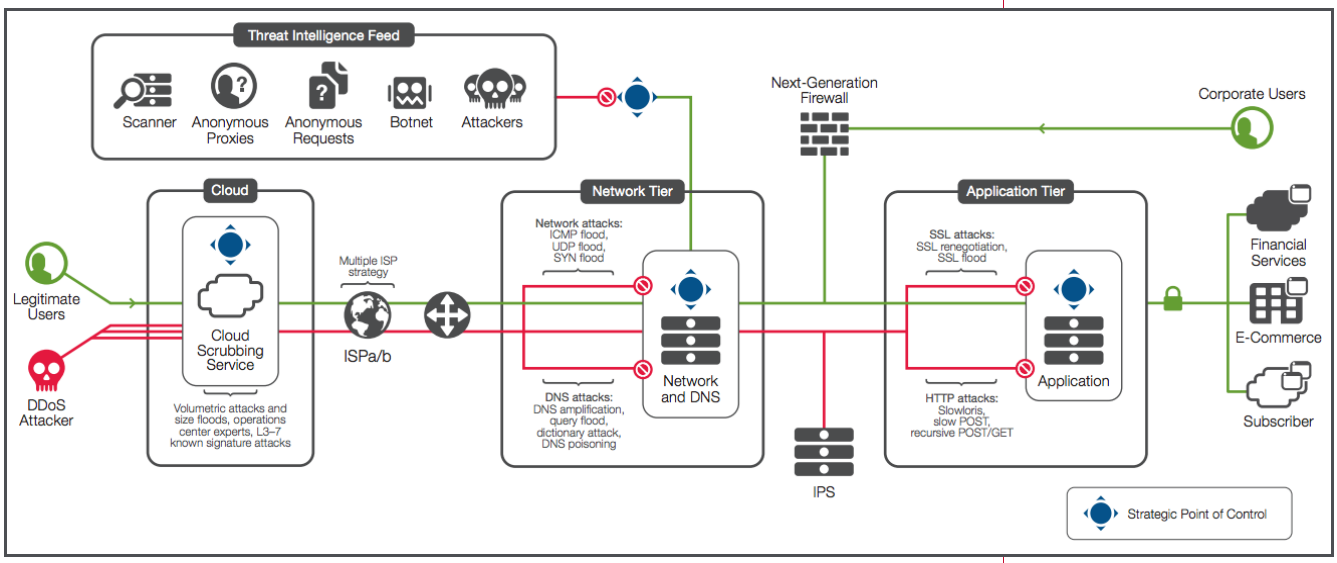

Figure 2. F5 Recommends a Multi-Tier DDoS Approach Architecture

Application Tier

The **Application Tier** handles high-CPU security functions such as SSL termination and web-application firewall functionality.

Cloud-based DDoS Scrubbing Tier

To combat DDoS, a modern organization will need a **Cloud-based DDoS Scrubbing Tier**. These service offerings can scrub hundreds of gigabytes per second and return "clean" traffic to the customer data center.

DNS

DNS is handled in the DMZ and partially protected by the Network Tier.

This **Multi-Tier Approach** can assist in the following attack types and effects:

- Defeat TCP connection floods
- Overcome SNAT port exhaustion
- Turn back SSL floods

These are just some of the recommended practices and considerations. You can obtain additional resources in the comprehensive *F5 DDos Recommended Practices* document.

DDoS Mitigation Steps

If you appear to be suffering a volumetric attack, it can help to have a historical sense of your own traffic patterns. Keep a baseline of normal traffic patterns to compare against.

If you have determined that you are under a DDoS attack, record the "estimated start time" (see "Worksheet 5: Attack Log" on page 25).

You will need to follow *up to* 10 steps for your DDoS Mitigation:

- Step 1–Verify the Attack
- Step 2–Contact Team Leads
- Step 3–Triage the Applications
- Step 4–Identify the Attack
- Step 5–Protect Remote Users and Partners
- 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 Your Public Relations

***Monitoring Volumetric Attacks**: Remember to keep a monitoring web page open to indicate when the attack may be over (or mitigate).*

STEP 1– VERIFY THE ATTACK

Most outages are *not* caused by a DDoS attack DNS misconfiguration. Upstream routing issues and human error are some common causes. You must first rule out these types of *non*-DDoS attacks, and distinguish them from a common outage.

Common Outages

The faster that you can verify the attack is a real DDoS attack, the faster you can respond.Even if the outage was not caused by a misconfiguration or other human error, there may still be other explanations that may resemble a DDoS attack.

Slashdot Effect

The Slashdot Effect occurs when a particular page on your site is featured on a very popular forum or blog. Your investigation must rule out such possibilities.

Outbound Connectivity

Is there outbound connectivity? If not, then the attack is so severe that it is as congesting all inbound and outbound traffic. Check with your usual diagnostic tools (traceroute, ping, dig, etc.), and rule out all such possibilities.

Global Issue

Check the following Internet weather reports to determine if the attack is a global issue:

- Internet Health Report
- Internet Traffic Report

External Network Access

Attempt to access your application from an external network. Services that can perform this kind of monitoring are:

- Keynote Testing and Monitoring
- Gomez℠ –Comprehensive Performance-Monitoring Tool from Compuware®
- HP® SiteScope™ – Agentless monitoring
- SolarWinds® NetFlow Traffic Analyzer
- Down for everyone or just me?

DNS Website Response

Check to see if DNS is responding for your website. The following UNIX command resolves a name against the OpenDNS project server.

```
% dig @208.67.222.222 yourdomain.co
```

STEP 2–CONFIRM DDOS ATTACK

Contact Team Leads

Now it is time to contact the leads of the relevant teams. If you have not filled out "Worksheet 1: Contacts List" on page 21, fill it out now.

When an outage occurs, your organization may hold a formal conference call including various operations and applications teams. If your organization has such a process, leverage the meeting to officially confirm the DDoS attack with team leads.

Contact Your Bandwidth Service Provider

One of the most important calls you can make is to the bandwidth service provider. They can likely confirm your attack, provide information about other customers who might be under attack, and sometimes offer remediation.

Contact Your Fraud Team

It is especially important to **invoke the fraud team as soon as the attack is verified**. DDoS attacks can be used as "cover" to hide an infiltration. Logs that would normally show a penetration may get lost during a DDoS attack. This is why using high-speed, off-box logging is so important.

*The number for your service provider should be listed in **"Worksheet 1: Contacts List" on page 21**.*

STEP 3–TRIAGE APPLICATIONS

If you have not done this exercise yet, now is the time to triage your applications.

When faced with an intense DDoS attack and limited resources, triage decisions have to be made. High-value assets typically generate high-value on-line revenue. These are the applications that you will want to keep alive.

Ultimately, these are financial decisions–make them appropriately.

Low-value applications, regardless of the level of legitimate traffic, should be purposefully disabled so that their CPU and network resources can be put to the aid of the higher-value applications. You may need the input of the team leads to do this.

- Record your choices in “Worksheet 3: Triage Applications” on page 23 for future reference.
- Decide which applications are low-priority and can be disabled (and thus protected) during the attack. This may include internal applications.

Worksheet 3 *takes only a few minutes to fill out, and will greatly assist you in combating an actual DDoS event.*

STEP 4–PROTECT PARTNERS WITH WHITELISTS

Whitelist Partner Addresses

Very likely you have trusted partners that must have access to your applications or network. If you have not already done so, collect the IP addresses that you must always allow access for and maintain that list. Print "Worksheet 2: Whitelists" on page 22, which includes a template for your whitelist collection.

You may have to populate the whitelist in several places through the network, including the firewall, the ADC, and perhaps even with the service provider, in order to guarantee that traffic to and from those addresses is unhindered.

Protect VPN users

Modern organizations will whitelist or provide quality-of-service for the remote SSL-VPN users. Typically this is done at an integrated firewall/VPN server, which can be important if you have a significant number of remote employees.

STEP 5–IDENTIFY THE ATTACK

Determine the Nature of the Attack

Now it is time to gather technical intelligence about the attack. The first question that you need to find the answer to is:

"What are the attack vectors"?

You are trying to determine the *nature* of the attack itself. Is it:

- **Volumetric**–Flood based attacks that can be at Layer 3, 4, or 7?
- **Asymmetric**–Designed to invoke timeouts/session-state changes?
- **Computational**–Designed to consume CPU and memory?
- **Vulnerability-based**–Designed to exploit software vulnerabilities?

4 DDoS Attack Types

You have, by now, called your bandwidth service provider (see "Worksheet 1: Contacts List" on page 21). If the attack is solely volumetric in nature, they will have informed you and may have already taken steps at DDoS remediation.

Even though well-equipped organizations use existing monitoring solutions (such as NetScout®) for deep-packet captures, you may find that there are cases where you have to use procure-packet captures from other devices, such as the application delivery controller (ADC) to assist in diagnosing the problem. These cases include:

- SSL Attack Vectors. If the attack is launched over SSL, there may be no other way to diagnose it other than at the ADC. Capture the packet streams either at the ADC or elsewhere, and then use the ssldump utility to decrypt the stream file.
- FIPS-140. If your ADC is using a FIPS-140 hardware security module (HSM), then you can often still use ssldump to decode the file capture.
- Use a Mirror-Port or Clone Pool. One way to capture packets is to mirror them from the ADC. This high-performance method allows data to flow through the ADC and also to an external device without interruption.

Step 6–Evaluate Source Addresses Mitigation Options

If Step 5 has identified that the campaign has advanced attack vectors that your service provider cannot mitigate (such as slow-and-low attacks, application attacks, or SSL attacks), then the next step is to consider the following question:

"How many sources are there"?

If the list of attacking IP addresses is small, you can block them at your firewall. Another option would be to ask your bandwidth provider to block these addresses for you.

The list of attacking IP address may be too large to block at the firewall. Each address that you add to the block list will slow processing and increase CPU. You may still be able to block the attackers if they are all in the same geographic regions that you can temporarily block.

For example, if the majority of your attacks appear to be coming from Southeast Asia, evaluate the revenue you will lose if you block all traffic from that region. Be deliberate about geo-blocking.

***Geo-blocking**: The decision to block entire regions via geo-location must be made as a business decision.*

Finally, if there are many attackers in many regions, but you don't care about any region except your own, you may also use geo-location as a defense by blocking all traffic except that originating from your region.

Mitigating Multiple Attack Vectors

If there are too many attackers to make blocking by IP address or region feasible, you may have to develop a plan to unwind the attack by mitigating "backwards" – that is, defending the site from database Tier, to the application Tier, to the web servers, load balancers, and then firewalls.

You may be under pressure to remediate the opposite way– for example, mitigating at Layer 4 to bring the firewall back up. However, be aware that as you do this, attacks will start to reach further into the data center.

As you identify the different mix of attack vectors, “Attack Remediation” on page 16 can assist in showing you exactly where to find the remediation specific to the individual attacks.

Attack Vector	Firewall	On-Premises DDoS	Application Delivery Controller	Cloud Scrubber
SYN-Flood	X	X	X	X
ICMP-Flood	X	X	X	X
UDP-Flood	X	X	X	X
TCP-Flood			X	X
DNS-Flood		X	X	X
Apache Killer		X	X	
Slowloris		X	X	
Keep Dead		X	X	
HTTP Recursive GET		X	X	

Table 1. Attack Remediation

STEP 7–MITIGATE SPECIFIC APPLICATION LAYER ATTACKS

You have reached this step because the DDoS attack is sufficiently sophisticated to render mitigation by the source address ineffective. Attacks that fall into this category may be generated by tools such as the "Low Orbit Ion Cannon," the "Apache Killer" or the "bro-bot."
These attacks look like normal traffic at Layer 4, but have anomalies to disrupt services in the server, application or database Tier.

To combat these attacks, you must begin enabling or constructing defenses at the application-delivery Tier.

Mitigate Specific Attack Tools

You have analyzed the traffic in Step 4. If it appears to be an application layer attack, the important questions are:

Can you identify the malicious traffic?

Does it appear to be generated by a known attack tool?

Specific application-Layer attacks can be mitigated on a case-by-case basis with specific F5 countermeasures. Attackers today often use multiple types of DDoS attack vectors, but most of those vectors are around Layers 3 and 4, with only one or two application-Layer attacks thrown in. Hopefully this is the case for you, which means you are nearly done with your DDoS attack.

*To learn about each **common attack tool** and **mitigation strategy**, see "The Taxonomy of Application Attacks" in the "F5 DDoS Recommended Practices" document.*

Step 8–Increase Application-Level Security Posture

If you have reached this step in the DDoS attack, you've already mitigated at Layer 3 and 4 and evaluated mitigations for specific application attacks, and you are still experiencing issues.

Asymmetric Application Attack

Very likely you are being confronted with one of the most difficult of modern attacks: the asymmetric application attack. This kind of attack can be:

- A flood of recursive GETs of the entire application.
- A repeated request of some large, public object (such as a MP4 or PDF file).
- A repeated invocation of an expensive database query.

If you implemented a subset of the architectural recommendations discussed in the introduction, you may be able to make use of those defenses now.

Leveraging Your Security Perimeter

The best defense against these asymmetric attacks depends on your application. For example, financial organizations know their customers and are able to use login-walls to turn away bad traffic.
Entertainment industry applications (such as hotel websites), on the other hand, often do not know the user until the user agrees to make the reservation. For them, a CAPTCHA might be a better deterrent.

Choose the application-level defense that makes the most sense for your application:

- Login-wall
- Human Detection
- Real Browser Enforcement

Login-wall

A **Login-wall** is a logical defense that requires a client to be logged in as a known user before it can access any high-value asset or run a database query. Login-walls can be implemented at a Service Provider, a Web Application Firewall, or an Application Delivery Controller.

The drawback to this otherwise perfect solution is that not every application has a tight integration with known users. For example, hoteliers must serve room availability applications that do not require the user to login.

Human Detection

Human Detection is the second-best approach. Validating that the client connection is at least being controlled by a human (instead of a malicious bot) can go a long way to turning back a Layer 7 DDoS attack. Usually this is done with a CAPTCHA of some kind.

CAPTCHAs

A **CAPTCHA** is an acronym for "Completely Automated Public Turning test to tell Computers and Humans apart"–it is a challenge used in computing to tell whether or not the user is human.The drawback to **CAPTCHAs** (and the reason that they do not protect every resource all the time), is that they will turn away some percentage of legitimate users. Flexible applications will allow CAPTCHAs to be turned ON during an attack and then OFF again afterward.

Figure 3. A typical CAPTCHA

Real Browser Enforcement

Real browser enforcement is the third option. Some web application firewalls provide this functionality by inserting a JavaScript redirect to new connections, and then blacklisting them if they do not follow the redirect. This is a nice approach because it foils the majority of bots without interfering with real users using real browsers.

Step 9–Constrain Resources

If all the previous steps fail to stop the DDoS attack, you may be forced to simply constrain resources to survive the attack.

Rate Shaping

This technique turns away both good and bad traffic. In fact, rate limiting often turns away 90–99% of *good* traffic while still enabling the attacker to drive up costs at your data center. For many organizations, it is better to just disable or "blackhole" an application rather than rate-limit it.

If you find that you must rate-limit, you can provide constraints at both sides of a multi-Tier DDoS architecture. At Tier 1, where Layer 3 and Layer 4 security services reside, use rate shaping to prevent TCP floods from overwhelming your firewalls and other Layer 4 devices.

Connection Limits

Connection limits can be an effective mitigation technique, but they do not work well with the connection-multiplexing features. The Tier 2 connection limits should provide the best protection to prevent too much throughput from overwhelming your web servers and application middleware.

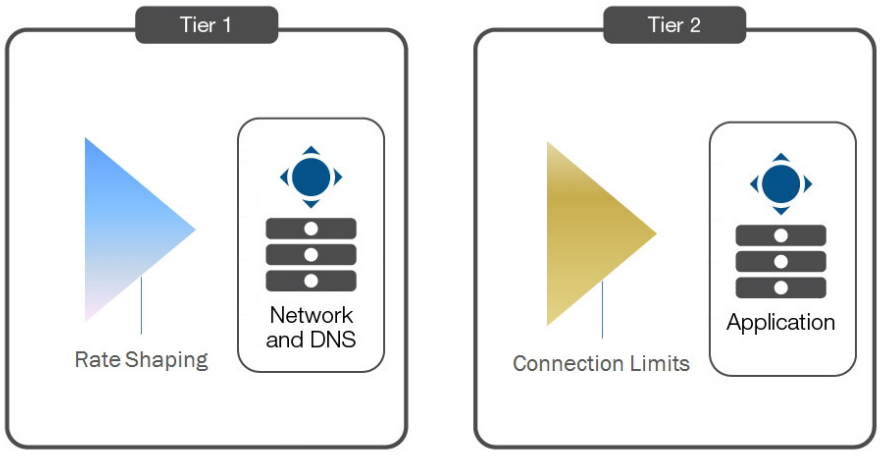

Figure 4. Resource Constraints– Tier 1 and Tier 2

Step 10–Manage Your Public Relations

Hacktivist organizations today make use of the media to draw attention to their causes. Many hackers have been informed that an attack is underway, and may contact the target company during the attack.

Financial Organizations

Financial organizations have policies (related to liability), that prevent them from admitting an attack is underway. This can become a sticky situation for the public relations manager. The manager may say something like: "We are currently experiencing some technical challenges, but we are optimistic that our customers will soon have full access to our on-line services."

Reporters

Reporters, however, may not accept this information (especially if the site really does appear to be fully off-line). In one recent case a reporter has called a local bank branch manager and asked that person how the attack was proceeding. The branch manager, who had not received media coaching responded: "It's awful, we're getting killed!"

If the DDoS attack appears to be a high-profile hacktivist attack, prepare two statements:

1. **For the press**. If your industry policies allow you to admit when you are being externally attacked, do so and be forthright about it. If policy dictates that you must deflect the inquiry, then cite technical challenges but be sure to prepare the next statement.

2. **For your internal staff- *for distribution to anyone who might be contacted by the press***. Your internal statement should provide cues about what to say and what not to say to media, or even better, simply instruct your staff to direct all inquiries related to the event back to the PR manager and include a phone number.

Conclusion

If this Playbook information has been helpful, create a custom playbook for your organization.

- Include the worksheets in the next section–print them, fill them out and laminate them.
- Use them to create the start of your physical playbook, or put them on the wall in the data center.

As you defend yourself against DDoS attacks, you can refine your playbook and improve the resilience of your applications.

Worksheet 1: Contacts List

Many different teams may need to come together to fight a large, hectic DDoS attack.

- Use this worksheet to collect and maintain the 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			

Worksheet 2: Whitelists

Maintain the list of IP addresses that must always be allowed access.

Addresses that should be included in this list are:

- External monitoring tools (Gomez℠, etc.).
- Google and the other search engines that you do not want to block.
- Your own Global Traffic Managers (GTMs)–these will be monitoring your applications throughout the attack.
- Vulnerability scanners and your DDoS cloud-scrubbers such as Prolexic.
- Your other cloud service providers service providers (this could be large checklist).
- Business partners.

IP Address Range	Maps To?	External Contact	Internal Contact

Worksheet 3: Triage Applications

For all applications at the data center:

- Record a priority decision about whether or not it should be disabled.
- Record a triage decision. (You can use the priority value to assert a decision like “disabling all applications that are priority 3 or lower”).
- Add a column for the 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 priority 3 or less.

	Application Name	Priority	Triage	Associated Virtual Server	Location
1	Example Application	2	Disable	dc1-rxspc.example.com	BIG-IP2, Rack 5, 192.168.11.5
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					

Worksheet 4: F5 Device Map

If you engage F5 professional services to assist the defense (*during the DDoS attack*), it will be helpful to have a map of available F5 devices within the data center.

The serial numbers for the BIG-IP will help the engagement, and the remaining information will be helpful to those advising you on defensive strategies. The **%tmsh show sys hardware** command provides the serial number and the platform type.

Both of the F5 configuration management solutions, F5 EM and F5 BIG-IQ, gather the device information (minus the location) for you, and may assist you in filling out this table.

Keep this information with "Worksheet 1: Contacts List" on page 21.

	F5 Device	Model	Modules	Serial Number	Location
1	bigip2-dmz.dcxnet.com	1600	GTM	f5-wtax-exgw	Data Center 1, DMZ, Rack 5, 192.168.11.5
2					
3					
4					
5					
6					
7					
8					
9					
10					

Worksheet 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	
Attack Started	Date & Time
Attack Stopped	Date & Time
Fraud Team Alerted	Date & Time
Intrusion Detected	Date & Time
Assets Exposed (if any)	
DDoS Attack Vectors (circle)	ICMP UDP TCP DNS HTTP HTTPS
Attribution (attackers identified)	

Source addresses may be turned over to the authorities. If attacking source addresses are isolated to a specific country, the attack may be mitigated via geo-location (see “Step 6–Evaluate Source Addresses Mitigation Options” on page 13).

Source Address Analysis
Geo-Location:
Source Address:

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 for the next attack.

Attack Summary (complete at end)
Geo-Location:
Source Address:

F5 Networks, Inc.
401 Elliott Avenue West, Seattle, WA 98119
888-882-4447 www.f5.com

Americas
info@f5.com

Asia-Pacific
emeainfo@f5.com

Europe/Middle-East/Africa
apacinfo@f5.com

Japan
f5j-info@f5.com