FortiDDoS

DDoS Attack Mitigation Guide

May 1, 2012

28-100-167076-20120501

Technical Documentation: docs.fortinet.com

Knowledge Base: kb.fortinet.com

Customer Service & Support: support.fortinet.com

Training Services: training.fortinet.com

Table of Contents

Introduction

Defining DDoS attacks

Denial of service (DoS) attacks are attacks that are deliberate attacks on your network properties to deny service to legitimate users. When these attacks seemingly come from distributed sources, they become distributed denial of service (DDoS) attacks.

A few years back, it was common to use spoofing techniques where a hacker would actually use very few machines (or just one machine) and spoof multiple IP addresses. To the attacked destination it would seem that the attack is coming from multiple IP addresses. However in the recent times, with the advent of infected PCs, increasing number of smart mobile phones, many botnets are available around the world, which can be used to launch a real DDoS attack.

Attack scenarios

- Under attack, your team does not know details of the attack. They understand the symptoms, but they can't figure out the cause and the solution.
- Your routers and switches are overloaded and they don't have the capability to stop such attacks. Firewalls simply allow these packets. IPS appliances (if you have them), don't have the rules to block such attacks. Your equipment doesn't match up in performance that's required.
- May be, you have multiple links to the Internet. The attackers are attacking from different links.
- The attack is seemingly coming from all over the world. You cannot simply identify a Net-block to deny so that the attack can be stopped! And you cannot simply block everyone!
- The attack is no different from legitimate users accessing your web pages from the point of your edge equipment.
- Your team is unable to figure out the solutions quickly when the attackers are constantly changing the tactics.
- You have too much collateral damage. When attack happens on one part of the network, the others bleed too.
- Software solutions such as mod_evasive, iptables, Apache / LiteSpeed tuning, kernel tuning, not capable of handling the load.
- You are not as rich as others to over-provision your bandwidth and to buy high-bandwidth gear.
- The only tool your service provider has is Null Routing your IP address!

Causes of attacks

- Sometimes hackers' exuberance gets transformed to rivalry and they try to prove their might and you just get involved in their cross fire.

- Sometimes it may simply be your own rivals who are getting at you.
- In some cases, some new hackers may have recently learnt the tricks of the trade. They may be doing this for sheer personal pleasure. They are randomly choosing targets and you just happened to be on their radar by mistake. They may incrementally advance to more sophisticated attacks as they learn the tricks.
- For some attackers it is prestigious to attack you and bring you down despite all your attack defenses. Some times, a software bug on your server may be causing too many users to come to your site again and again. Your servers can't handle the load and they keep trying. It's like an avalanche.
- Sometimes, someone wants you to pay or else they will break your site. May be there is a reason you are not reporting this to authorities – or may be authorities/ ISPs don't help and don't know how to help.

Motivation behind attacks

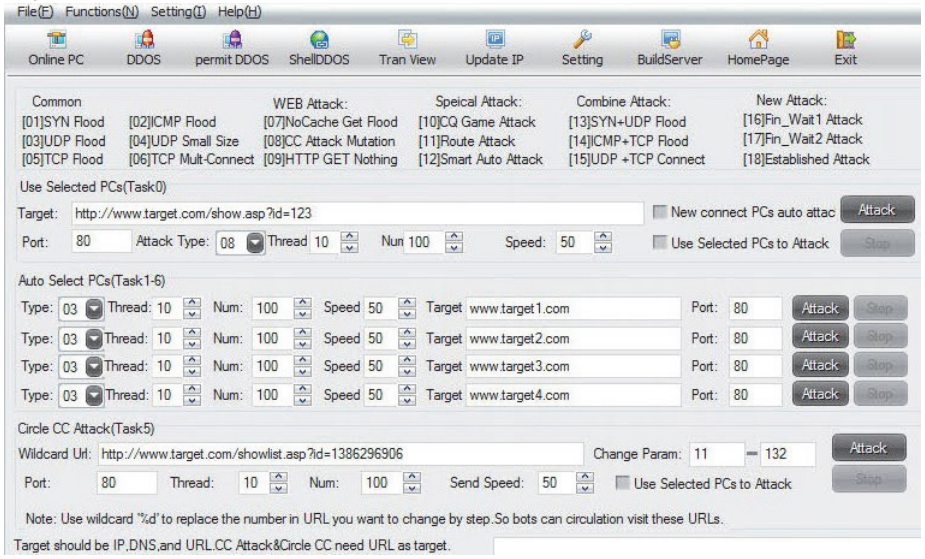
There can be many reasons why DDoS attacks are launched.

- Some attacks are **principle driven attacks**. The attackers desire to silence you since your values are different from theirs. E.g. you own porn sites and they are web-vigilante. Sometimes your rival religious sects may be flooding if you own a religious site. Your web properties may be site capitalistic and the attackers may be anti-capitalism. You may be American and the attackers could be anti-American. You may be managing debt and the attackers may have sympathy with poor or those in debt. Such principle driven attacks are very common and are difficult to solve on the principle grounds. May be you have a gay/lesbian site and someone doesn't agree with you.
- Sometimes attacks are **business driven attacks**. You may be in the way of someone else's business growth. They will then hire a botmaster who will then launch an attack on your properties. Sometimes the attackers may have ethical objection to your business.
- Some attacks are **anger driven attacks**. If you host IRC servers, gambling - especially offshore, or porn sites and you have some angry customers, they may come back to extract revenge. If you have recently banned someone from your servers or if someone has lost a lot of money on your site, they may be behind the attacks.
- Another type of attacks we have seen are **socially driven attacks**. If you are a social networking site and one of the users has written a page against a foreign government. That government may now be after you. Until you remove that page, you will be attacked.

Virus infections, botnets and distributed attack tools

Millions of new users join the Internet daily. These are in the far-flung corners of the world. If you are reading this primer, you are savvy - but they are not. If they get an enticing email from someone, they open it and their machine now has bot code which can be remotely controlled by botmasters. Millions of such machines around the world are under control of bot-herds who buy, sell and rent them for monetary gains. Some foreign governments are also known to control them for possible cyber-warfare.

Figure 1: A Botmaster Console



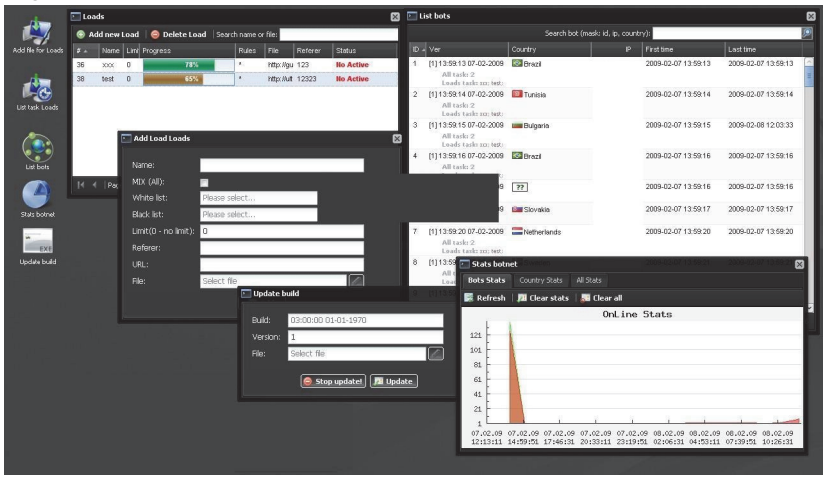
The above pictures shows a bot-controller that can be easily used to launch a DDoS attack sitting somewhere using bots around the world. The renter uses this software after paying the rent. She can simply enter the URL of the target site to be attacked and choose the type of the attack and launch the attacks including a blended attack. This program controls the bots on the Internet.

Following is another example of another bot controller panel. As you can see the panel consists of a display of available bots in different countries and ability to launch different tasks through the bots.

Figure 2: Another Botmaster Console

Another picture below shows ability of the bot-master to upload new functionality into the botnet and update the bots remotely and have an ability to remotely see the status of the bots.

Figure 3: One more Botmaster Console



Most common current generation DDoS attacks

There are many kinds of legacy and current generation attacks that are prevalent today. SYN flood and HTTP GET floods being the most common.

SYN flood

Spoofed SYN Packets fill the connection table of servers, and all other devices in your network path. Low volume SYN flood can be easily stopped by software firewalls. High bandwidth SYN floods needs specialized equipment with SYN proxy capability.

Zombie flood

In zombie or botnet floods, non-spoofed connections overload the services. The attacking IPs are able to do three way handshakes. These are difficult to stop unless you have behavioral mitigation. High bandwidth zombie floods needs specialized logic for discriminating legitimate traffic within zombie flood.

ICMP flood

In these floods, ICMP packets, such as those used for ping, overload the servers and the network pipe. Low volume ICMP flood can be easily stopped by ACLs on routers and switches. High bandwidth ICMP floods needs specialized equipment.

TCP/UDP port flood

In these floods, TCP/UDP packets overload the servers and the pipe on ports not being used for service, e.g. TCP port 81. Low volume port floods on non-service ports are easily stopped by ACLs. Higher volume need specialized equipment for automatic detection and mitigation unless you have totally blocked all non-service ports by default. Sites that use services such as FTP or IRC that use dynamic ports need to be careful with the stateful traffic on the dynamic ports. Most large attacks that are greater than 1 Gbps involve UDP floods because they are easy to generate by spoofing IPs.

When packets overload the servers and the pipe on service ports, e.g. TCP port 80. Firewall, switches, routers, IPS appliances cannot stop these attacks. In these cases, you need specialized equipment for discrimination.

Fragment flood

In these flood, fragmented packets overload the servers. Many firewalls, switches, routers cannot stop these attacks unless they have rulesets for dropping fragmented packets. Sometimes you may need specialized equipment.

Anomalous packet flood

Hackers create most floods with scripts. Sometimes deliberately and sometimes due to errors in scripts, packets are anomalous. These anomalies may be headers at layer 3, 4 or 7. They may be in TCP or UDP states or protocols. These packets overload the CPU of the servers and other networking equipment on the way. Some firewalls, and IPS appliances can stop these attacks. Specialized equipment for DDoS easily stop these attacks.

HTTP GET flood

These attacks involved connection-oriented bots overload the servers and the pipe on service ports, e.g. on HTTP, mimicking legitimate users. Since firewalls, switches, routers, IPS appliances don't have behavioral anomaly prevention, they cannot stop these attacks. Therefore you need specialized equipment to stop these attacks.

Blended attacks

When multiple types of above attacks are blended on the server, they confuse the conventional equipment further. Firewall, switches, routers, IPS appliances cannot stop these attacks. You need specialized equipment to stop these attacks

Floods from unwanted geographical areas

These are very common. For example, you have most of your customers in China and you are getting too many packets from Russia. Such floods are easy to stop with simple access control lists in Anti-DDoS equipment or in switches or routers before the network.

Myths and realities about DDoS attacks

- It happens to others

  Most Network and Security Operations engineers only hear about DDoS attacks happening to others. They think that they don’t have enemies. In reality, their perceptions of risk factors and susceptibility is most often misplaced. If you have a web presence, you can be attacked easily – sometimes even by mistake.
- Software fixes can solve DDoS attack issues

  Many engineers think that they can custom compile kernel, set some options in Apache, install mod_dosevasive and DDoS attacks can be taken care of. In Reality, most servers do not have the capacity to handle DDoS attacks. Under most aver-

age sized DDoS attacks, your server CPUs will be too overloaded to give Apache modules a chance.

- IPTABLES can stop DDoS attacks

  Another myth that exists is that simple iptables commands can block DDoS attacks. In reality, NetFilter/iptables can block very tiny attacks and tiny percentage of DDoS attacks. Real DDoS attacks require specialized equipment because the CPU running iptables will be too busy handling attack packets.

- Webhost will take care of DDoS attacks

  Many Network and Security Operations engineers think that their webhosts will take care of DDoS attacks. Many webhosts are happy to just null-route an attacked IP domain unless they have specialized equipment. Many webhosts do not have the skills to manually isolate issues - unless they specially advertise such capability.

- ISPs of the world co-operate

  Some think that their ISPs, to whom their webhosting data center is connected to, cooperate under attack and they can find the source of the attack. Most ISPs are too busy. They have strict and bureaucratic processes to reach each other. Typical response time for ISPs are in days if not in hours – whereas you want the solution now!

- Law Enforcement is easy to approach in case of DDoS attacks

  It is also easy to think that under attack, we can report to law enforcement to solve the problem. In reality, most law enforcement departments will not bother about needle in hay-stack attacks – for them that's what most attacks are. Unless you are important and the attacks are in multiple 10s of Gigabits per second, don't waste their time and yours.

- ACLs on switches/routers can stop DDoS attacks

  You may also think that you can determine that ACLs for your routers and switches to block the attacks. DDoS attacks are moving targets. The hackers are smart, their tools are smarter and techniques are sophisticated.

- Pipes will fill any way - what's the point

  Another myth that surrounds DDoS attacks are filled pipes. Many wonder if there is any point in buying any specialized Anti-DDoS equipment. In reality, 90% of the attacks are sub-1Gbps today and if you have that much pipe, you will be better off having a DDoS mitigation solution than not having one at all. Pain from the most complex attacks can be reduced with specialized equipment. Without the DDoS mitigation equipment, your servers will be thoroughly exposed to even the most ordinary attacks. Take the first step. DDoS mitigation equipment is not as expensive as you may think. DDoS mitigation costs are proportional to number of links, bandwidth, complexity of policies and type of attacks. If you have a reasonable sized business, it should not cost you an arm and a leg. There are cost-effective solutions available that are effective.

Home remedies for simple and small DDoS attacks

- Update kernel to the latest release
- Install all security updates
- Disable unused and insecure services
- Remove unused packages

- Memory resources can be exhausted by filling up various kernel tables that are not tuned to be sufficiently large. Ensure that you understand various kernel tables.
- Network card is gateway to the packets. Better network card means better handling of large number of packets. Better network card driver means better performance.
- Choose a vendor such as Intel and model which is proven and a driver that's already hardened.
- Use NetFilter/iptables firewall to deny bad packets
- Use Hashlimit module to identify IPs that are consuming resources
- Use ipset module to block-lists of up to IP addresses that can be queried, loaded and unloaded from user-space.
- Use command :netstat -plan|grep :80 |awk '{print $5}' |cut -d: -f1 |sort |uniq -c |sort -n to find out if port 80 is being attacked by too many IPs.
- Use modules such as mod_evasive, mod_limitipconn to limit attacks from limited number of IPs.
- Try mod_qos to improve quality of service.
- Apache has its limits. You can try LiteSpeed.

Anti-DDoS appliances

There are primarily following categories of appliances in the market for DDoS mitigation:

Carrier DDoS mitigation solutions

- These solutions are useful for global networks and carriers and ISPs.
- They employ IP flow-based and deep packet inspection technologies, and protect entire networks consisting of multiple routers and switches and services behind them.
- An example of such solutions is Arbor Networks.
- These solutions are too expensive for individual IDCs, webhosts or web properties.
- These solutions have been designed around early 2000 and therefore are not keeping up with the current generation of DDoS attacks which involve botnets that mimic legitimate clients.
- These solutions work very well at global level and the residual attacks from such solutions may be too much for an individual web property which in turn may have to employ a solution such as 2 below.

Custom logic (FPGA or ASIC) based internet data center (IDC), web hosting and web property DDoS mitigation solutions

- These solutions are useful for large IDCs, large web hosts and large web properties.
- They work to protect one or several Internet links.
- The behavioral solutions are implemented in custom hardware logic and provide line rate performance for large attacks.
- The FortiDDoS device has one such solution.
- These solutions are cost-effective and effective for IDCs, webhosts and web properties.

Software based web property DDoS mitigation solutions

- These solutions are useful for smaller web properties with very minimal traffic.
- The behavioral solutions are implemented in off-the-shelf CPUs and have issues at large attack traffic volumes in terms of keeping up.
- Some appliances have IPS functionality implemented in hardware but have their DDoS mitigation logic in software and suffer from the same issues.

Things to look for in Anti-DDoS equipment

Latest technology

- The hackers are pretty up-to-date on techniques. If your DDoS mitigation appliance is built around technology that was developed in early 2000s, it won't help you much as most of the current generation attacks would pass through.

Centralized monitoring

- Look for appliances that allow you to centrally monitor all DDoS events and traffic in your network. You can use SNMP, Cacti, MRTG to monitor traffic and attack levels and attack events. You can configure Syslog to get all attack events on a centralized server as well.

Visibility into normal network traffic patterns

- Look for appliances that allow you to get extremely granular visibility into your network traffic. Typically you should look for a 12 month round robin view of what normal traffic looks like and incorporate this information into a correlation engine for threat detection, alerts, and reporting.

Alerting mechanisms

- Look for appliances that give you a threshold based alerting mechanism for DDoS specific events. You can set threshold for different people to get alerts depending on the quantum of attack. You should be able to query a database for Top Attacks, Top Attackers, Top Attacked Destination, etc. You should be able to create custom queries in your custom applications/reports.

Filtering mechanisms to reduce false positives

- Look for appliances that filter traffic in different network layers as they inspect incoming packets using dynamic profiling (based on monitoring and analysis of normal behavior), anti-spoofing algorithms, and other technology to progressively filter harmful traffic upstream of the network.

Low latency

- Latency, in this context, is the amount of time it takes a packet to go through an appliance. Look for appliances that don't affect your mission critical traffic by adding additional significant latency. Most switches and routers have low latency in the range of a < 50 microseconds. The anti-DDoS equipment should maintain similar latency levels. This latency should be maintained even during attacks.

Hardware logic for Anti-DDoS

- These days it is common for a $100 home router to claim that it has DDoS attack mitigation capability. Such claims have to withstand third party tests and real life. It is also easy to build Intel CPU based appliance running Linux with some behavioral capability built-in to claim anti-DDoS features. Many IPS appliances have IPS in hardware logic but anti-DDoS capability in software. Such appliances cannot handle attacks beyond a certain Mbps.
- Look for custom DDoS mitigation logic implemented in hardware as that alone can withstand large DDoS attacks. A granular approach to DDoS mitigation selectively mitigate attacks at highest possible layer so that attacks are stopped at most specific layer. This reduces the false positives.
- Ability to monitor a large number of ports, sources, destinations, connections etc. helps in proper identification of attacks and attackers.

Bypass and redundancy

- Look for internal or external bypass capability that ensures that your network traffic continues even if the appliance fails. For multiple links, look for ability to cross connect appliances in a fail-over configuration. In addition, look for asymmetric traffic support because you may have traffic coming from one link and going through another.

Extensible architecture

- Anti-DDoS equipment must grow with your business. Look for appliances that have such capability to grow through licenses.
- Third Party Validation
- Look for third party validation for a solution you choose. That will mitigate some risks of your inability to actually do a test in your own labs.

SYN Floods will continue to grow

The size of SYN floods has been growing. SYN Floods are easiest to create and are tough to mitigate as the size in terms of bandwidth grows.

There are many schemes for SYN Flood mitigation. Hardware logic based mitigation is the only practical way to sustain large SYN floods. Software based solution, even those deployed on blade-center platform, do not have the capability to perform SYN flood mitigation at high data rates.

Hardware logic can perform anti-spoofing, depending on the size of the attack and suitability, using:

- SYN Cookies
- ACK Cookies
- SYN Retransmission

Concurrent connection-based attacks will be on the rise

It is easy for hackers to hire a botnet which runs scripts that open connections and leave them in established state after performing a proper 3-way TCP handshake. A limited number of connection from many such botnet machines can easily overwhelm a server. When the number of these attacker IPs is small, you can use software scripts to stop the attack using IPTABLES and TCPKILL like tools. You can try Nginx constellation reverse proxy configuration and DNS round robin mechanism to reduce the pressure. But practically, this doesn't seem to work as it requires multiple machines to be managed.

A hardware logic based solution which monitors all connections for behavioral anomalies can easily stop such attacks and aggressively age them both internally and from the servers by sending a TCP RST on behalf of the client.

Botnet floods will be rising

Attacks mimicking legitimate users are on the rise. Even low-bandwidth of such attacks seem to bring down the servers. Existing tools fail to stop such attacks because they don't have visibility and control over such behavioral attacks. Smarter bots will be rising that will obfuscate most algorithmic systems.

Hardware logic which can look simultaneously granularly and deeply into the packet's network and application headers can stop such attacks by determining self-similarity among packets at some level.

Volumetric and application layer DDoS attacks will be converging in 2011 onwards and therefore require DDoS mitigation systems that can intelligently provide solutions for both of them well.

Support for IPv6 will become important

IPV4 space is depleting faster than thought and planned. Support for IPV6is becoming important –especially from a web hosting perspective.

Appliances that support IPV6 will be important in 2012.

Social network attacks will be common

Social sites that publish objectionable material will now be easy target of attacks. 'Objectionable' will be a relative term. This is a new trend. These are different from socially networked attacks where a social network is used for launching attack on a site.

Recently there was a battle between two social networks, viz. 4chan and Tumblr. Members of the two sites launched - a DDoS attack targeted against each other.

Cyber Warfare will start to take shape

Bringing down government websites will become common. Governments bringing down sites will also be common. British military has recently decided to spend £650 million on developing its cyber warfare capabilities.

Collateral damages in multi-tenant environment will grow

When you share resources with others in a multi-tenant hosting environment, it is easy for your network to be affected even though you may not be under attack. Therefore it makes sense for you to protect your infrastructure from DDoS attack using your own private DDoS attack mitigation appliance and insist that your hosting provider acquires one to protect the overall network.

Hosted clouds may kick you out under attack to avoid collateral damage

If you are under severe DDoS attack, your hosts including cloud-based hosts may kick you out.

Amazon.com recently kicked Wikileaks to the curb.

Conclusion

Most DDoS solutions in the market have technology that was developed in early 2000s and have not been updated. Use the leading DDoS solution that keeps up with the current attacks and evolved the hardware logic to keep up with the time and trends.

DDoS Mitigation Techniques

Introduction

Firewalls, switches, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) have been commonly used in the past as security perimeter appliances. A new generation of attacks has now become common that cannot be stopped using the above appliances. Distributed Denial of Service (DDoS) attacks have become very common because of easy availability of botnets. New techniques have evolved in the industry to thwart DDoS attacks. This chapter discusses the new and upcoming techniques.

SYN proxy

This is one of the earliest techniques to handle spoofed DDoS attacks. During SYN flood, a few machines start spoofing IP addresses and start sending SYN packets. When a server receives these connection requests, it responds by sending TCP SYN/ACK packets and adding those connection entries into its own connection table. Since these spoofed IP addresses don't really exist, they don't respond to the SYN/ACK and thus the connection table remains filled for a long duration. This effectively denies the access to new and legitimate connections.

SYN Proxy is a mechanism, usually done by intermediate appliances that sit before the actual server and proxy the responses. Until the spoofed IP or un-spoofed IPs respond with the ACK, the connection requests are not forwarded.

This ensures that under SYN flood, all connection requests are screened and only those that are legitimate are forwarded.

There are other related techniques such as ACK-Proxy and SYN Retransmission that are used as alternatives for anti-spoofing checks. Each techniques has advantages and disadvantages.

Connection limiting

Too many connections can cause a server to be overloaded. By limiting the number of new connection requests, you can temporarily give the server respite. This is done by giving preference to existing connections and limiting the new connection requests.

Aggressive aging

Some botnet attacks involve opening a legitimate connection and not doing anything at all. Such idle connections fill up the connection tables in firewall and servers. By aggressively aging such idle connections, you can provide some relief to them. Aggressive aging involves removing connections from the tables and may also involve sending a TCP RST packet to the server/firewall.

Source rate limiting

When a limited number of sources are available to a bot-master, he/she can use them to aggressive send packets. These high rate packets can burden the server. Multi-threaded attacks cause such patterns of attack. By identifying outlier IP addresses that break norms, you can deny them access to excessive bandwidth. Since IP addresses in such attacks are not predictable, it is important to keep track of millions of IP addresses and their behavior to isolate outliers. Such isolation can only be done in silicon and it is difficult to achieve using software only techniques due to excessive memory bandwidth requirements.

Dynamic filtering

Static filtering is a common technique in firewalls, switches and routers and is usually achieved using Access Control Lists (ACLs). Dynamic filtering is required when the attack and the attackers change constantly. Dynamic filtering is done by identifying undisciplined behavior and punishing that behavior for a short time by creating a short-span filtering rule and removing that rule after that time-span.

Active verification through legitimate IP address matching

While SYN Proxy is a great technique for anti-spoofing, every time there is a SYN flood, within a short duration, if the appliance keeps sending SYN/ACK packets back, that would add too much outbound traffic. To avoid such reverse flood, it is necessary to cache identified legitimate IPs in to a memory table for a limited period of time and then letting them go without the SYN proxy check. It is quite possible for the attackers to misuse such holes, therefore it is necessary to have further checks on legitimate IP addresses by rate limiting zombies which are able to complete 3-way-handshakes.

Anomaly recognition

Most DDoS attacks are written using scripts which continuously vary a few parameters in the network packets. By performing anomaly checks on headers, state and rate, an appliance can filter out most attack packets which otherwise would pass simple firewall rules.

Protocol analysis

Similar to header, state and rate anomalies, further protocol analysis can bring out issues that would otherwise pass through a generic firewall.

Granular rate limiting

DDoS attacks are unpredictable and usually managed using scripted BOTs. The packets which reach the server are different from each other. There is however some self-similarity among all attack packets in a single attacks.

Granular Rate Limiting is a technique that identifies rate violations from past behavior. Rate thresholds are set based on past behavior set during a training session and adjusted adaptively over time.

Granularity refers to various parameters available in layer 3, layer 4 and layer 7 headers. These include packet rates for source, destination, protocol, fragment, ports, and HTTP methods, URLs, User-Agents, Cookie, Host, Referer etc.

White-list, black-list, non-tracked sources

In any network, there will always be some IP addresses that you want to deny or allow. White-listing and Black-listing capability are useful during DDoS attack to ensure that such rules are honored despite rate violations or in spite of rate-violations.

Since rate anomalies are behavioral, all behaviors are learned from past. Therefore if you don't want some behavior not to be learned, you must not track such behavior by creating an exception. Such non-tracked sources include backup IP machines etc. that do large amounts of IOs at specific times or Content Data Network (CDN).

State anomaly recognition

TCP is most commonly used protocol for web infrastructure. TCP is a stateful protocol and follows certain rules. Since most bots are scripted, many a times, they break these rules. A state anomaly recognition engine looks for illegal TCP state transition anomalies, foreign packets (packets in connections that are not properly established) and TCP window-violations.

Stealth attack filtering

Before an attack, there are precursors to attacks. These are in the form of scans. Network scans to discover IP addresses in use are common and so also Port Scans to discover TCP and UDP ports that respond to connections. By identifying, such attacks and corresponding attackers, you can take some precautions for a future full-blown attack.

Dark address scan prevention

Dark addresses are IP addresses that are not yet assigned by IANA. These are also called bogon addresses. Any packets coming from or going to dark addresses are signs of spoofing. By blocking them, you can block a substantial percentage of DDoS packets that are spoofed.

Overview of botnet attacks

Botnet attacks are literally a pain. The main reason for the pain is the inability of current generation of security equipment and solutions to distinguish between legitimate user access and botnet access. Botnet attacks are not spoofed and involve actual TCP-3-way handshake. That makes existing SYN-flood mitigation equipment unable to spot the difference. Since most of these attacks are on a service port such as TCP port - 80, firewalls have to allow such packets and therefore they cannot stop these attacks. A new generation of logic is needed to identify these attacks.

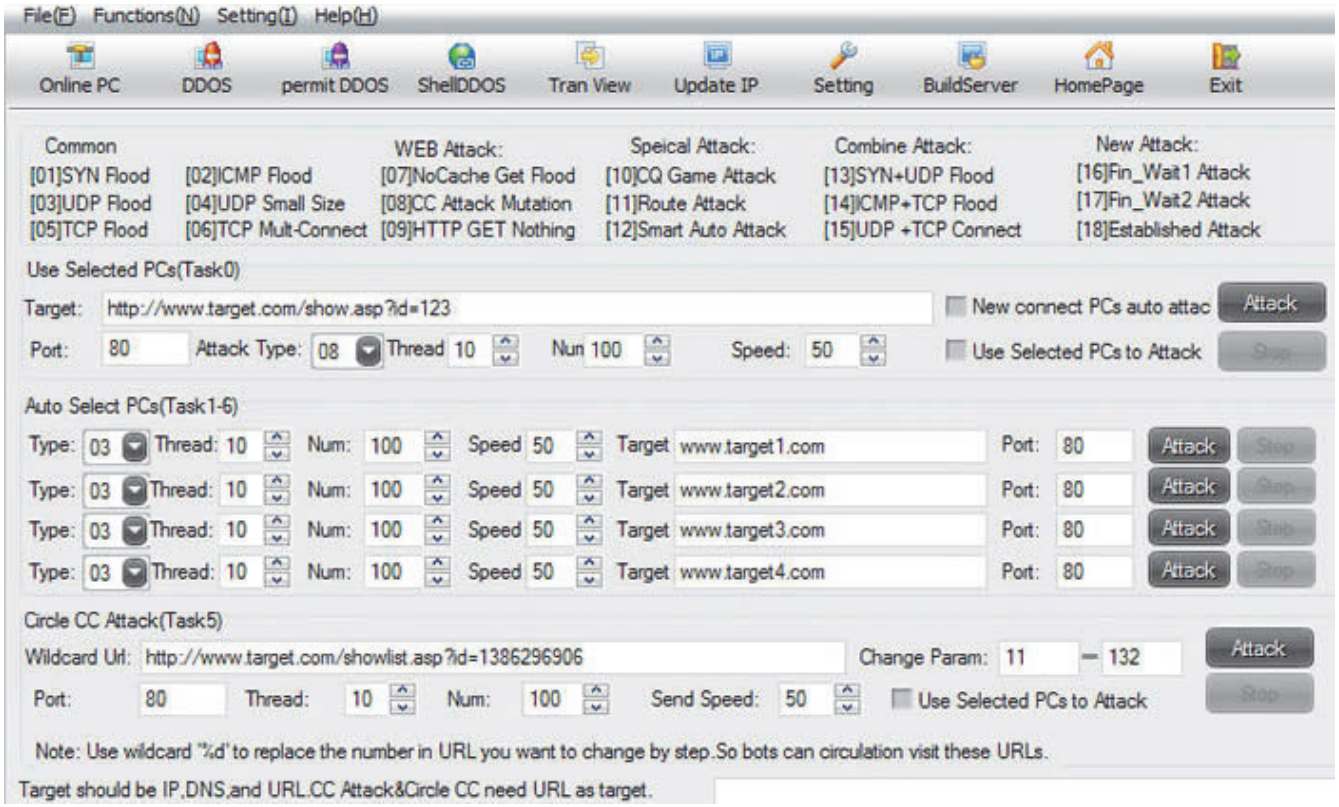
Distributed denial of service attacks using botnets

In Distributed Denial of Service (DDoS) attacks, hackers write a program that will covertly send itself to dozens, hundreds, or even thousands of other computers. These computers are known as 'agents' or 'zombies', because they will act on behalf of the hackers to launch an attack against target systems. the network of such computers is called a BotNet.

To circumvent detection, attackers are increasingly mimicking the behavior of a large number of clients. The resulting attacks are hard to defend against, using standard techniques, as the malicious requests differ from the legitimate ones in intent but not in content.

Under the control of botmaster, all of these zombies attempt repeated connections to a target site. If the attack is successful, it will deplete all system or network resources, thereby denying service to legitimate users or customers.

E-commerce sites, domain name servers, web servers, and email servers are all vulnerable to these types of attacks. IT managers must take steps to protect their systems - and their businesses- from irreparable damage.

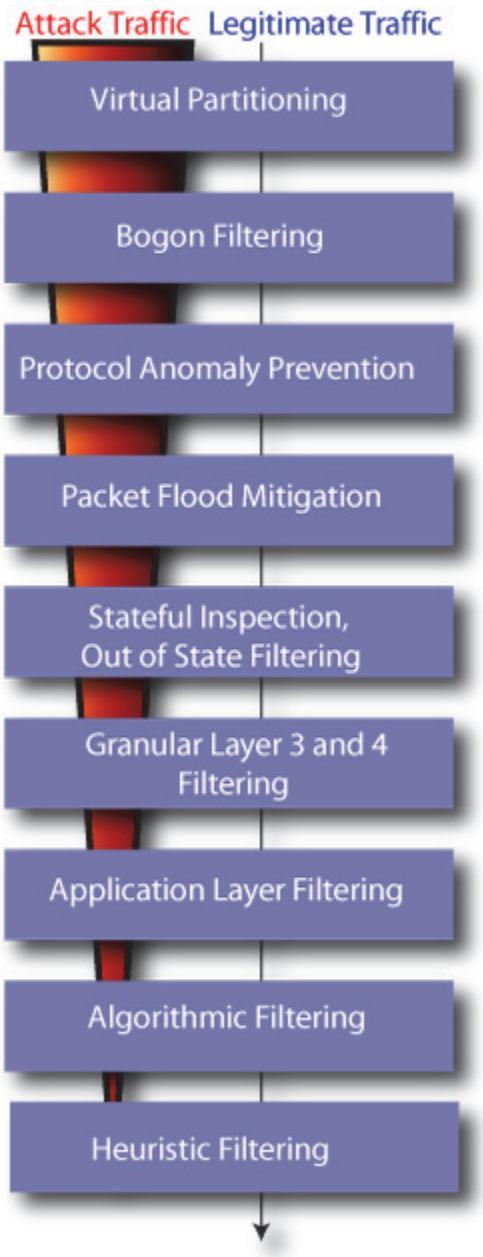


A typical botnet launch pad

Botmasters launch attacks in a way that they cannot be found easily. Bots are available for rent. And when you rent, you get a control panel similar to one shown in the diagram above. You can simply attack a chosen site using attack parameters available to you.

What's common among the botnet attack packets

Botnet attacks are scripted. Despite the botnet script writers' intelligence, there is a trail that is left behind in the attacks in terms of common parameters. These common parameters can be observed in a hardware logic based system such as a FortiDDoS device. These common parameters are usually visible in the application layer headers.



Can you do the same processing in CPU based systems?

CPU based systems get overwhelmed under pressure of botnet attacks. They cannot handle the amount of onslaught that botnets create. A hardware logic based system is designed from ground-up to process every packet without losing steam. The logic processes packets in a massively parallel architecture ensuring that all blocks work together to deliver the allow/deny result quickly.

Blocking botnet attack packets using FortiDDoS appliances

FortiDDoS appliances are implemented using hardware logic and therefore can process all packets at line rate. They have visibility and control at layer 7 HTTP headers and can process many parameters simultaneously without slowing down. The hardware logic can monitor millions of continuously varying parameters per VID and there can be up to 8 VIDs in a system.

The monitoring is associated with adaptive thresholds which are set based on your traffic and therefore if the thresholds exceed, the botnet is caught easily and blocked for a period of time configured by you.

Conclusion

Designing a security strategy for networked assets can be a daunting task. New threats demand new types of security elements. Traditional firewalls and content filters play an essential role in any network strategy, but neither can adequately defend against rate-based attacks such as those that are created using botnets. These systems are now available and extremely affordable, putting true zero-hour prevention within the reach of all network budgets.

Introduction

DDoS attacks pose a huge risk to a company's Internet connectivity and their prevention can save companies millions of dollars a year, especially for companies that depend on the Internet as a business platform and for those who the Internet is an element of their core IT infrastructure.

How do IT managers ensure that their web infrastructure is safe from DDoS attacks? How do they ensure that they don't get a call from their key customers in the middle of the night? How do they ensure that they don't have to search through logs to figure out the attack type and sources and change the router and switch configuration?

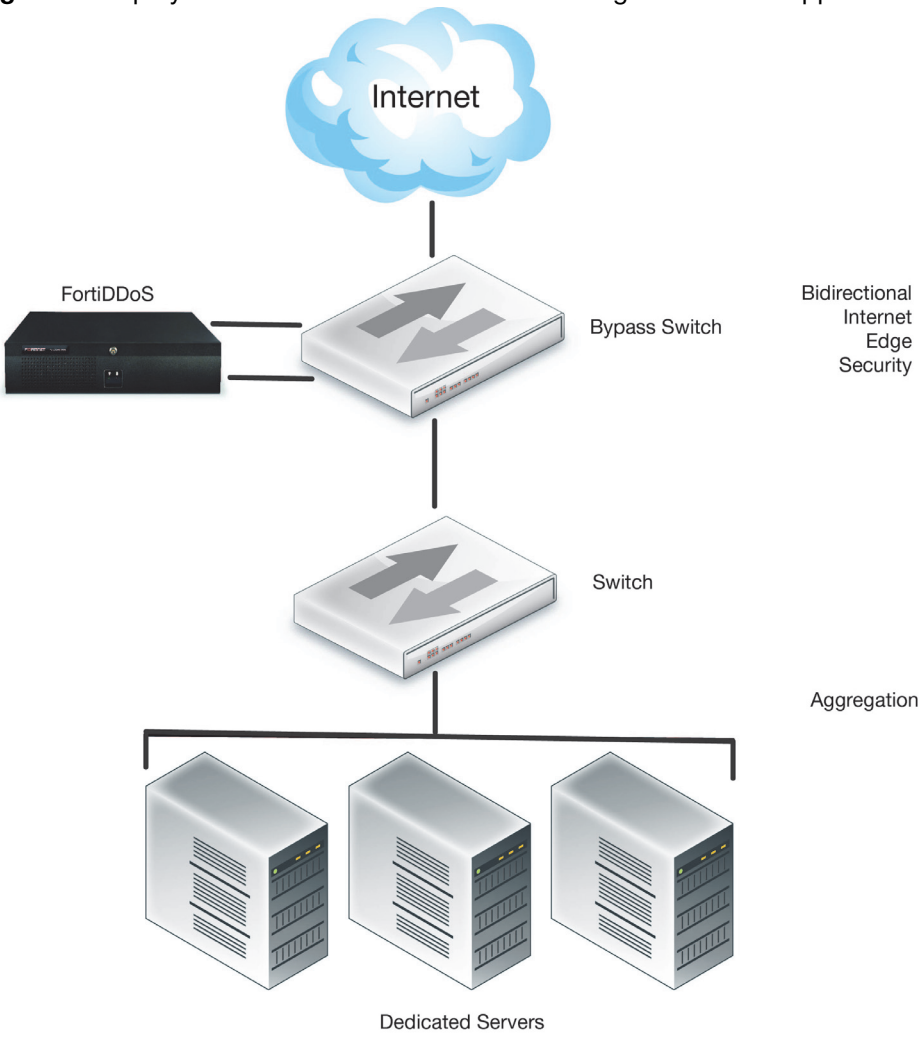
The FortiDDoS device is a solution for this, using hardware logic based appliances.

In the sections below, we describe a few typical configurations.

A very simple deployment

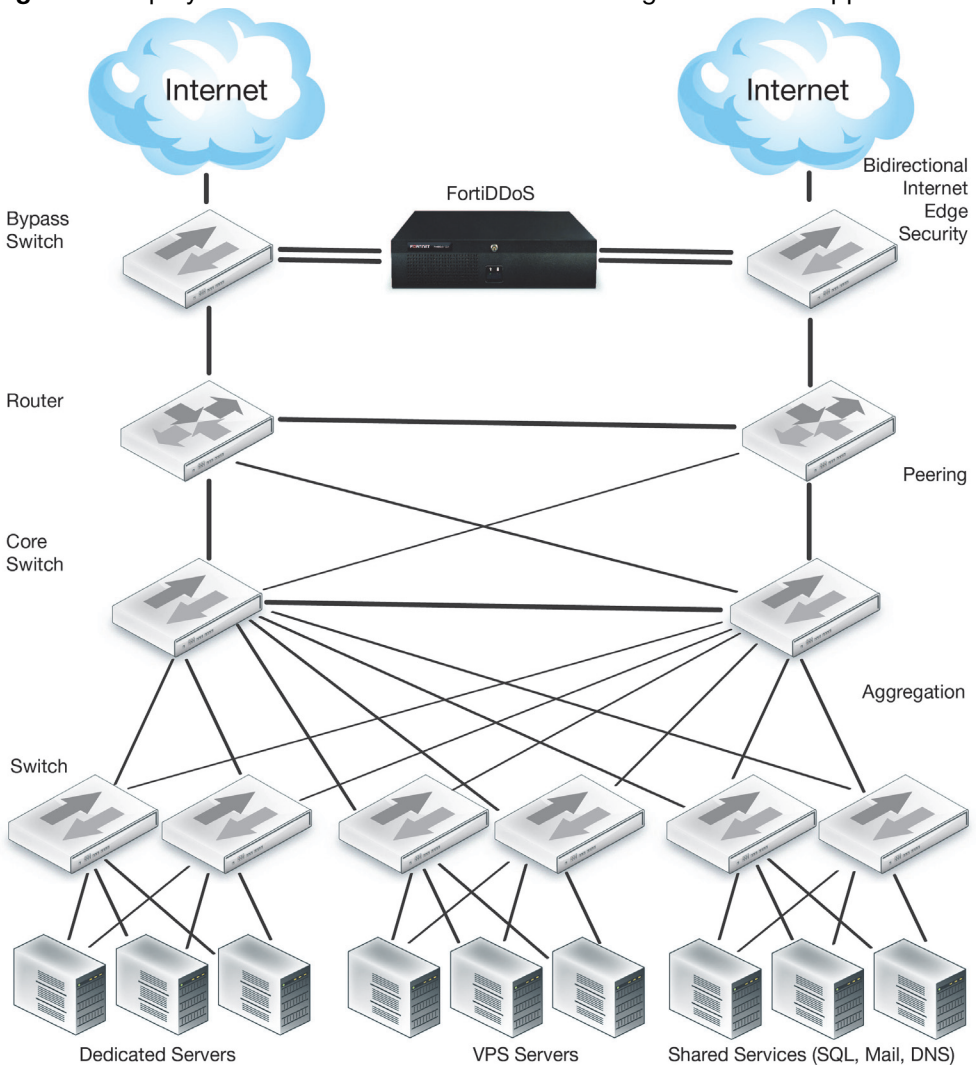
Following diagram shows a simple deployment. In this deployment with a set of dedicated servers in a co-location environment, a single FortiDDoS appliance is required. To ensure that there is no connectivity failure under critical failure of the appliance or power failure, there is a bypass switch. The bypass switch is inline with the traffic and passes traffic through the FortiDDoS unless there is a failure there.

Figure 4: Deployment with one internet link and a single FortiDDoS appliance



Dual WAN link deployment with a single appliance

Figure 5: Deployment with two internet links and a single FortiDDoS appliance

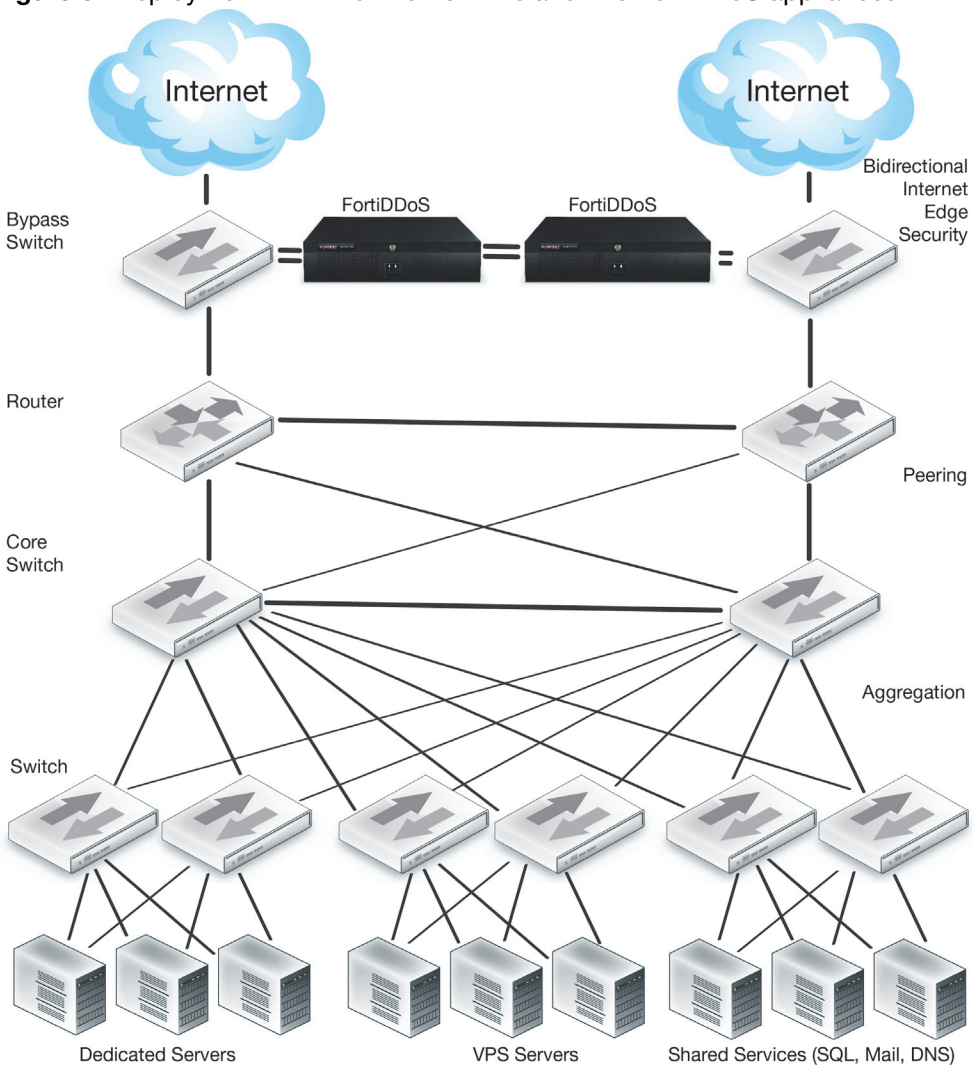


Typical deployment for an internet data center with two links protected by two independent devices in active configuration

In this configuration, the two appliances share states with each other through a proprietary connection/protocol. Traffic can be asymmetric.

In this configuration, the two FortDDoS appliances are cross connected and share states and therefore the traffic can move from one link to the other and the appliances will remain in sync with each other.The total traffic in this case can be 1 Gbps full duplex.

Figure 6: Deployment with two internet links and two FortiDDoS appliances

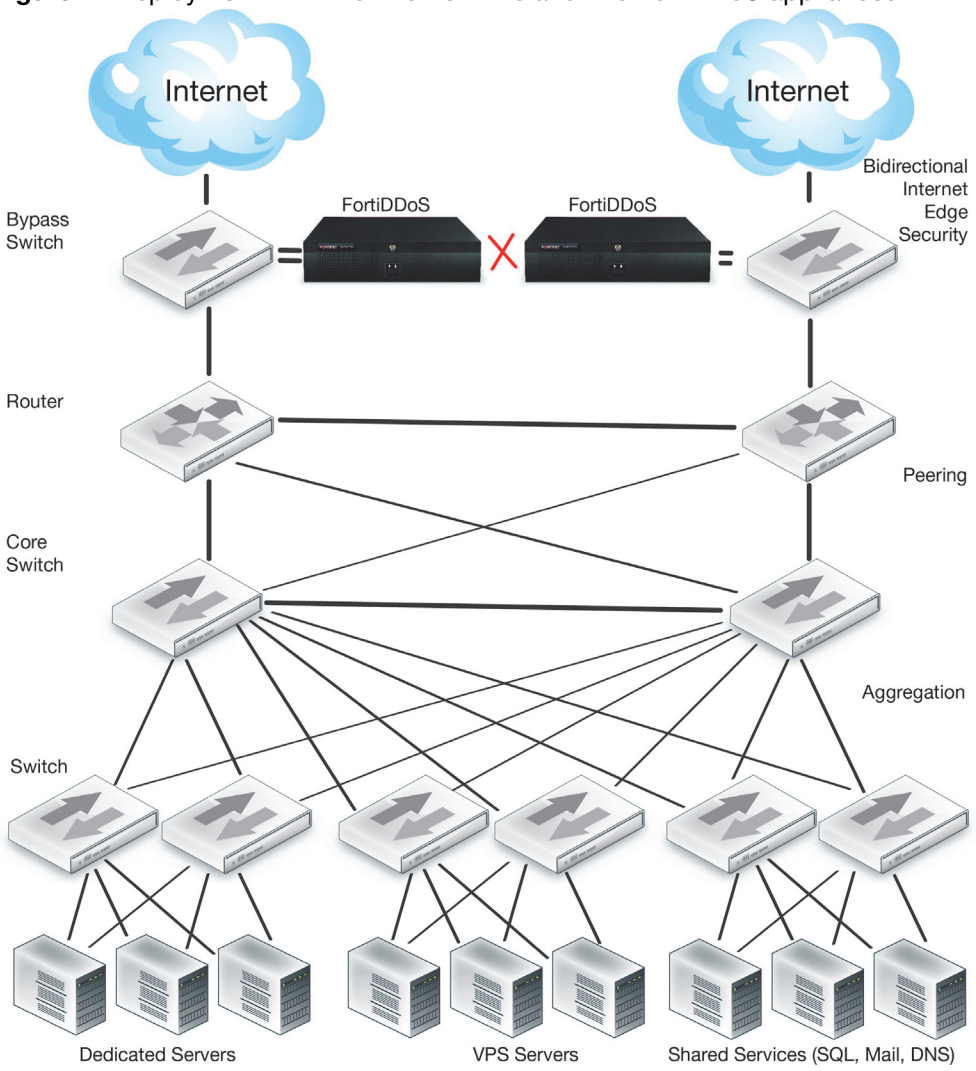


Typical deployment for an internet data center with two links protected by two independent devices

In this configuration, the two appliances share states with each other through a proprietary connection/protocol. Traffic can be asymmetric.

In this configuration, the two FortiDDoS appliances are not connected to each other protect the two links independently. The total traffic in this case can be 2 Gbps full duplex.

Figure 7: Deployment with two internet links and two FortiDDoS appliances



Impact of third party dependence on your business

The trend to use software as a service for an existing e-commerce website is making the issue even more complicated. Dependence on third parties for site-analytics, search engine optimization, blogging, social networking engines, shopping carts, shopping-experience management, payment and fulfillment, renewals and email-marketing makes your web-infrastructure talk to several others. Most e-commerce vendors do not question their SaaS vendors for their vulnerability to DDoS or botnet attacks. Most Software as a Service (SaaS) vendors are not well-protected themselves. Figure below shows some of the sub-systems used in an e-commerce site. Some of these may be used by you from third party vendors using the SaaS model increasing your vulnerability to DDoS.

Selling online involves a range of activities. Your product has to be in your online catalog. The customers expect to see search capability and ability to add items to shopping carts. The e-commerce system has to do order processing. This involves an automated workflow based system, which typically includes credit card processing, fraud prevention, backorders, shipping, order tracking and returns. Your customers expect customer service, receiving full access to view orders online, reprint receipts and invoices, create customer service requests, track shipments automatically, check gift certificate and download status, and much more.

When you build an online e-commerce site today, it is quite possible that you don't build all these systems yourselves. You have a choice of using third party toolkits to take care of the building blocks or using Software-As-A-Service (SaaS) for these components. There is definitely a trend towards SaaS.

Availability of your website and its uptime must be a key concern. Business continuity can be seriously affected by Distributed Denial of Service (DDoS) and botnet attacks. Reputation is at stake too when you are under attack for too long without protection.

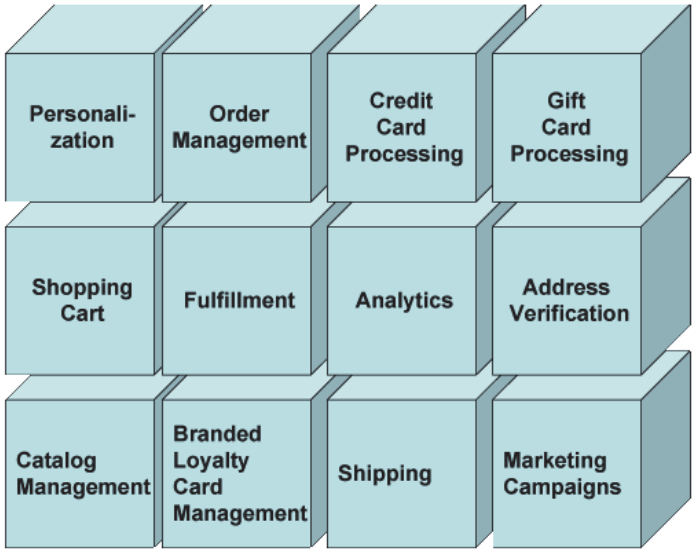
This chapter discusses effect of DDoS on an E-Commerce infrastructure that depends on the SaaS model for its components. It is aimed at a non-technical audience and provides a high-level view of E-commerce Security. Where methodologies have been mentioned they are provided as examples only and do not constitute recommendations or advice.

Use of third party services in eCommerce

The trend to use SaaS for an existing e-commerce website is making the issue more complicated. Dependence on third parties for site-analytics, search engine optimization, blogging, social networking engines, shopping carts, shopping-experience management, payment and fulfillment, renewals and email-marketing makes your web-infrastructure talk to several others. Most e-commerce vendors do not question their SaaS vendors for their vulnerability to DDoS or botnet attacks. Most SaaS vendors are not well-protected themselves. Figure below shows some of the sub-systems used in an e-commerce site. Some of these may be used by you from third party vendors using the SaaS model increasing your vulnerability to DDoS.

The reason people go for outsourcing components instead of doing a custom development is because it is lot less work to manage. In most cases it will cost less and take considerably less time than if you attempt to design and develop the site yourself. The services are prepackaged and with little worry about bugs and glitches. Your vendor will also track new technology for you, and you can benefit from its development and upgrades to service.

Figure 8: Some building blocks of an eCommerce site



The issue with third party dependence on infrastructure

When your site depends on third parties for critical services, you are vulnerable. You not only have to ensure that your infrastructure is protected from Internet attacks, but you have to ensure that services that you depend on, remain up all the time.

With botnets on the rise and criminal gangs on the prowl all the time, keeping higher uptime is difficult. These enemies can bring down your business, sometimes directly and now indirectly as well.

To deal with these insecurities, you must now ensure that your infrastructure is secure from Internet attacks and further ensure that your SaaS vendors have that protection as well.

Conclusion

Besides ensuring your availability and continuity, eCommerce vendors must ensure that their SaaS vendors are protected as well. A weak-link in the whole system can bring down the system. DDoS mitigation systems are affordable now and prices for these systems are on the downward path due to higher volumes. Small-to-medium size business owners can afford them now.

Introduction

Knowledge of DDoS attacks is mostly through hearsay. Most people purchasing DDoS mitigation systems do not know how to decide one system from the other. This chapter discusses a minimum feature set that you must test and benchmark to see the functionality and performance of a given DDoS mitigation system.

Distributed Denial of Service (DDoS) attacks are becoming common now with the proliferation of botnets. Network managers and security managers are deploying DDoS mitigation systems. Since most DDoS mitigation systems are fewer than 5 year old today, there is a trust issue with them. Those that have been tested by third parties such as Tolly Group are fewer. Most people would rather test them in their own lab before deploying them.

There are well know criteria for testing firewalls and Intrusion Prevention Systems (IPS). For DDoS mitigation systems, there is a need for a comprehensive test conditions.

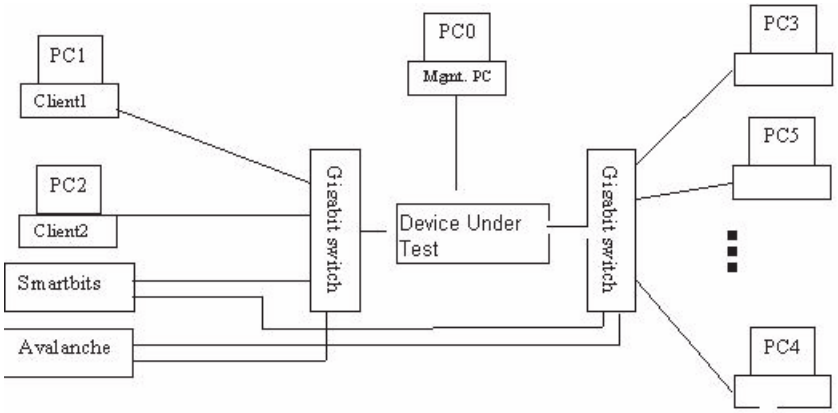
This chapter therefore focuses on identifying different kind of floods that can be tested using DDoS mitigation systems.

The reader is expected to create test-benches and test scripts to create these tests.

Typical test benches

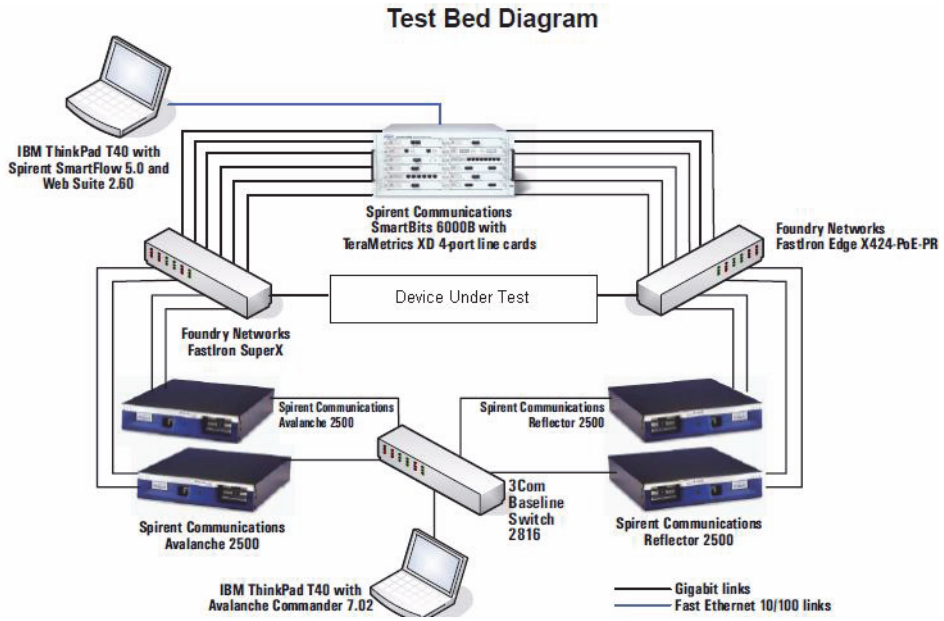
Following diagram shows a simple test bed. The appliances SmartBits and Avalanche are packet generator. Smartbits is used for creating session-less attack packets and Avalanche is used for creating sessions or attack sessions. Client PCs (PC1, PC2) and Server PCs (PC3 etc.) are used to seeing the results of mitigation.SmartBits and Avalanche here can be replaced with PCs running Linux/Windows with attack scripts.

Figure 9: A simple test bench



Following diagram shows a more complex test bed. The appliances SmartBits and Avalanche are packet generators. Such setups are typically used for third-party performance tests.

Figure 10: A more complex test bench



DDoS attack test conditions - a broad classification

DDoS attacks can be broadly classified into following categories:

Spoofed floods vs. non-spoofed floods

A spoofed flood sends packets that seem to come from an IP that either does not exist or did not actually send the packet.

A non-spoofed flood on the other hand comes from real IP addresses. Due to proliferation of botnets, it is quite common these days to see non-spoofed attacks coming from a large number of sources.

Anomalous header floods

These are packets which are typically generated by scripts. Scripts simple use loops to increment certain header parameters. Since many of these header parameter values may not be valid from standards perspective, they are anomalous. Examples of these attacks are packets with invalid TCP flag combinations. If a packet has flags such as RST, FIN, SYN, and ACK set simultaneously, it is anomalous.

Anomalous state floods

Protocols such as TCP are stateful. They follow predefined state transition rules. When scripted bots generate attacks, they violate many of these rules. Examples of such attacks are ACK packets coming without connection establishment, out of TCP window packets etc.

Limited sources versus large number of sources floods

Some DDoS attacks are launched using very limited number of sources while some others are launched with a very large number of sources. It is easy to launch a spoofed attack with a seemingly large number of sources. To launch a non-spoofed large number source attack, you need a control over a large botnet.

Layer 3, 4 or 7 DDoS attack

It is possible to launch DDoS attacks on different network layers.

Over the Internet, one can launch Layer 3, 4 or 7 attacks.

Example of Layer 3 attacks are protocol floods such as ICMP floods, TCP floods, fragment floods. These are created using a variation in the layer 3 headers.

Example of layer 4 floods are port floods (TCP or UDP). In these attacks, a single port is continuously attacked. ICMP echo flood are also of this kind.

Example of layer 7 floods are URL floods. In this attack, a single URL is continuously attacked from multiple sources.

Random header parameter attack

It is easy to create DDoS attacks in which some specific header parameter is continuously varying. Examples are TCP random flag flooding, IP option flooding, TCP option flooding etc.

Blended attack

It is easy to create DDoS attacks in which many attacks are combined to further confuse the destination. Examples are port floods on TCP and UDP simultaneously.

Attacks to test functionality and performance

Spoofed syn flood attack

This is a layer 4 spoofed flood in which the attacker sends TCP SYN packets in which the IP addresses are continuously changing.

Spoofed UDP attack

This is a spoofed flood in which the protocol is UDP and source address keeps changing.

Spoofed ICMP attack

This is a spoofed flood in which the protocol is ICMP and source address keeps changing.

Spoofed TCP SYN-ACK attack

This is a spoofed TCP flood in which SYN-ACK packets are sent in an anomalous state manner. Connections are not established prior to this through a SYN packet.

Spoofed TCP FIN-ACK attack

This is a spoofed TCP flood in which FIN-ACK packets are sent in an anomalous state manner. Connections are not established prior to this through a SYN packet.

Spoofed IP attack

This is a spoofed IP protocol flood. Packets may not necessarily be TCP, UDP or ICMP and can be any protocol.

Spoofed IP fragments attack

This is a spoofed IP flood in which packets are fragmented - the fragment bit is set in the layer-3 IP header.

IP-UDP fragments attack

This is a IP flood in which packets are fragmented - the fragment bit is set in the layer-3 IP header and packets belong to protocol 17 (UDP).

IP-ICMP fragments attack

This is a IP flood in which packets are fragmented - the fragment bit is set in the layer-3 IP header and packets belong to protocol 1 (ICMP).

TCP/UDP destination port attack

This is a layer 4 flood in which packets attack either a TCP or UDP destination port.

Spoofed TCP-SYN / UDP / ICMP blended attack

This is a blended attack in which source IP addresses are spoofed and at the same time, the protocol keeps changing as TCP, UDP and ICMP. The TCP packets are SYN packets.

Non-spoofed TCP SYN-ACK

This is a limited source layer 4 flood in which TCP SYN-ACK packets are sent continuously without a formal connection establishment.

Non-spoofed TCP SYN attack

This is a limited source layer 4 flood in which TCP SYN packets are sent continuously without further sending more packets within the connection. The connections will stay on the server until they timeout from the SYN-state.

Non-spoofed TCP FIN-ACK attack

This is a limited source layer 4 flood in which TCP FIN-ACK packets are continuously sent without establishing formal connections.

Non-spoofed TCP ACK attack

This is a limited source layer 4 flood in which TCP ACK packets are continuously sent without establishing formal connections.

HTTP half-connection attack

Half-connections or embryonic connections are connections that have not completed. When such a SYN flood occurs on HTTP port (80), it is called HTTP half-connection attack. This is obviously a spoofed layer 4 attack.

Non-spoofed UDP attack

This is a limited source layer 3 protocol flood in which the sources send IP protocol 17 - UDP packets. Remember that this would be a layer 4 flood if the UDP port is fixed in all the packets.

Non-spoofed DNS attack

This is a limited source layer 4 flood in which the sources send UDP packets with destination port set to 53 which corresponds to DNS protocol.

Non-spoofed ICMP attack

This is a limited source layer 3 protocol flood in which the sources send IP protocol 1 which corresponds to ICMP. Remember that this would be a layer 4 ICMP type and code flood, if a specific ICMP type and code is used in the attack packets.

Non-spoofed TCP ACK flood

This is a limited source layer 4 flood in which TCP ACK packets are continuously sent without establishing formal connections.

Spoofed TCP ACK flood

This is a spoofed layer 4 flood in which TCP ACK packets are continuously sent without establishing formal connections.

Non-spoofed TCP NULL flood

This is a limited source layer 4 flood in which TCP packets are continuously sent without establishing formal connections. These packets don't have any flags set in them and therefore have a header anomaly in layer 4 header.

Spoofed TCP NULL flood

This is a spoofed layer 4 flood in which TCP packets are continuously sent without establishing formal connections. These packets don't have any flags set in them and therefore have a header anomaly in layer 4 header.

Non-spoofed TCP random flag flood

This is a limited source layer 4 flood in which TCP packets are continuously sent with randomly changing TCP flags. Due to the randomization, there may be a header anomaly in layer 4 header. Some flag combinations are illegal. Example of legal combinations are SYN-ACK, FIN-ACK. Examples of illegal flag combinations are SYN-FIN-RST-ACK, SYN-RST etc.

Spoofed TCP random flag flood

This is a spoofed layer 4 flood in which TCP packets are continuously sent with randomly changing TCP flags. Due to the randomization, there may be a header anomaly in layer 4 header. Some flag combinations are illegal. Example of legal combinations are SYN-ACK, FIN-ACK. Examples of illegal flag combinations are SYN-FIN-RST-ACK, SYN-RST etc.

TCP random sequence, acknowledgement numbers

TCP is a connection-based stateful protocol to complete datagram oriented IP protocol which it uses as an underlying protocol. It uses sequence numbers and acknowledgement numbers to ensure proper windowing and end-to-end ordered

delivery. Normally sequence numbers are randomly chosen in a given connection. Once chosen, they follow a discipline. In a random sequence or acknowledgement number attack, these numbers are randomly chosen and varied. It can confuse the receiving end-point stack.

TCP random window size

TCP is a connection-based stateful protocol to complete datagram oriented IP protocol which it uses as an underlying protocol. It uses windowing to break large application packets to ensure proper end-to-end ordered delivery. The window size determines the number of bytes of data that can be sent before an acknowledgement from the receiver is necessary. In a random window size attack, the window sizes are randomly chosen and varied. It can confuse the receiving end-point stack.

TCP random option value

The TCP Options are located at the end of the TCP Header. These options have been used to enhance TCP protocol. TCP options include Maximum Segment Size (MSS), Window Scaling, Selective Acknowledgement (SACK), etc. In a random option value flood, the option values are changed randomly. Some of the combinations may be anomalous while some values may be anomalous too as they may be unassigned values.

TCP random data length

The length of TCP payload is dependent on the MTU (Maximum Transmission Unit) supported by the network, for normal ethernet the MTU is 1500. This is the maximum amount of data available to IP, TCP, and the application, it excludes the bytes for the ethernet header and trailer. From this 1500 you need to subtract bytes for the IP and TCP headers (normally 20 bytes each) leaving 1460 bytes available to the application. If the RFC1323 Timestamp option is used (fairly common nowadays) it extends the TCP header by 12 bytes leaving 1448 bytes. In a random data length attack, the payload size is randomly chosen.

TCP checksum error flood

TCP checksum field is the 16 bit one's complement of the one's complement sum of all 16 bit words in the header and text. The checksum also covers a 96 bit pseudo header conceptually prefixed to the TCP header. This pseudo header contains the Source Address, the Destination Address, the Protocol, and TCP length. This gives the TCP protection against misrouted segments. In a TCP checksum error flood, TCP segments with bad checksums are sent to overload the checksum validation logic.

IP random identification flood

The IP-Identification (IP-ID) field value in the IP header is used to uniquely identify the fragments of a particular datagram. Fragments of a particular datagram are assembled if they have the same source, destination, protocol, and Identifier. The IP identifier field

can have 65,536 different values. It is important for an operating system to have some sort of a mechanism in order to control the identification numbers correctly. In this flood, the IP-ID file is randomly varied.

IP random fragment flag, offset flood

IP-V4 header has a field called Flags related to fragmentation. This 3-bit flag has a reserved bit followed by Don't Fragment (DF) and More Fragment (MF) bits. A flood that continuously varies the above bits can confuse network devices. Just after the flags, there is a 13-bit fragment offset field. A flood that continuously varies this field can also cause confusion.

IP random TTL flood

IPv4 header has an eight-bit time-to-live (TTL) field that helps prevent datagrams from going in circles on the Internet. Each packet intermediate network appliance that a datagram crosses decrements the TTL field by one. When the TTL field hits zero, the packet is no longer forwarded by a packet switch and is discarded. This flood sends packets with random TTL values.

IP random protocol

IPV4 protocol supports up to 256 protocol types. In this flood, the protocol field value is randomly changed while (may be) keeping rest of the packet header values similar.

UDP checksum error

UDP header has a checksum field. By sending a wrongly computed checksum value, packets with anomalous header can be flooded on the network.

Non-spoofed ICMP echo reply flood

ICMP echo request is typically used to identify the presence of a machine on the network. The machine responds with a ICMP echo reply. This flood that continuously sends ICMP echo replies to an IP address. The sources are non-spoofed.

Spoofed ICMP echo reply

Unlike above, this flood uses spoofed IP addresses to send ICMP echo replies.

Un-spoofed ICMP type/code flooding

ICMP allows 65535 combinations of type/codes. This is an un-spoofed flood from limited number of sources that randomly send a type/code flood.

Spoofed ICMP random type/code flooding

This is a spoofed flood where a single but random ICMP type/code is flooded. Rest of the packet header may be similar in the packets.

Non-IP flooding

Ethernet header allows different protocols. IP version 4 or version 6 are just two of them. There are other protocols too. In a non-IP flood, un-common values of the protocol values are used.

Conclusion

There are many ways to test DDoS mitigation equipment. Conditions given above are just some examples. DDoS mitigation is a police and thief game. The hackers come up with new techniques and therefore the testers and equipment makers have to come up new techniques to test and benchmark the equipment.

Choosing a DDoS Mitigation System

Introduction

Shopping for a DDoS mitigation solution can be intimidating if you've never done it before. However, with a little background knowledge, an understanding of features, and knowing what questions to ask the vendors, you'll end up with just the right solution for your data center.

A DDoS solution is a barrier between your data center infrastructure and the rest of the world, regulating access between your infrastructure and the Internet and preventing hackers from denying service access to your legitimate users.

Hardware logic or software appliance

One of the first things you need to figure out is what type of solution best suits your needs. There are two types of appliances: software and hardware (such as those built like Cisco or Juniper routers). Both may claim identical functions. When packets of information enter your network, the appliances are expected to examine the packets granularly. The appliances do this by comparing the incoming information to the criteria set or established by the policies. If the information passes scrutiny, the information is forwarded on to its destination. Any unacceptable packet is blocked before it reaches your infrastructure.

Why does it matter whether an appliance is software or hardware based? The reason is because DDoS mitigation is all about figuring out self-similarity in traffic from thousands of angles, and quickly without any sampling of data. This kind of multi-dimensional inline processing can only be done in massively parallel hardware logic and not in a multi-core CPU. Somewhere the performance will show.

Customization

A good DDoS solution is customizable. This means that you can add or remove policies according to your needs. With a good appliance, you can set up parameters to restrict data that is allowed to enter your network. Practically speaking, these rules give you control. Users can grant or deny access to specific IP addresses, subnets, and countries. In addition, administrator should be able to grant or deny accesses to protocols, ports, ICMP type/codes, URLs, user-agents, hosts, 'referers' etc. It is always useful to lock down unused areas of network be it protocol, ports, URLs etc.

If you have trained programming staff, besides GUI control, look for Command Line Interface (CLI) tools for expert scripting of the appliance.

Virtual partitioning and multiple policies

If you are in the market looking for DDoS attack mitigation appliances, chances are that you have more than one machine in your network. Each of your subnets/servers has different traffic behavior and user behavior. You need an appliance that can create different policies for these subnets so that a. the attacks are isolated b. each subnet is treated differently. For example, your e-commerce users need to be treated differently from people casually browsing your websites. If you are a webhost, different servers need to have different policies based on your revenue model with them.

Bidirectional attack mitigation

In addition to monitoring traffic from the Internet, DDoS appliances control traffic flow outbound from your own local network. While this might not be important for an individual website, it can be critical on a large web hosting network, for example, to keep some machines from getting hacked and participating in outbound floods.

Connectivity

When choosing a DDoS appliance, be sure to check connectivity. Copper, fiber (Single Mode and Multi-Mode) interfaces are common and you should expect your vendor to provide them. A bypass feature in case of critical failure of the appliance or power should be present. Both internal and external bypass features are common.

Also, ensure that the appliance itself doesn't have MAC address or IP address in the path of the packets. Such appliances are called Layer-2 Transparent Bridges. That way, no one should know its presence in the network.

Legacy DDoS attack mitigation systems

Most security issues have a shelf-life and hackers always come up with new attack mechanisms. Ensure that your vendor has a capability for firmware/software updates.

DDoS attacks have changed drastically over the past year, and DDoS mitigation technology has evolved to meet those new, more demanding needs. An appliance that has an early 2000 vintage may not withstand today’s attacks. 10 years is legacy in the DDoS attack mitigation field. Ask your vendor for a history of updates and future update frequencies.

Network layer and application layer attacks

While network layer floods are still common, application layer floods are smarter and require a technology that’s updated to withstand 2011 attacks. Example of network layer floods are SYN floods, ICMP floods etc. Application layer floods mimic legitimate user traffic and are very difficult to discriminate using conventional tools and

techniques. Make sure your vendor blocks these below-the-radar attacks without false positives.

Hardware redundancy

If your business is mission critical and not having protection is not acceptable, look for hardware redundancy in appliances and also look for systems that support active-active fail-over configurations to ensure your links are always protected.

Centralized monitoring, alerts and reports

If you have multiple appliances in your network, using SNMP, Cacti, MRTG etc. makes life easier for your operators. Ensure that your vendor supports integration with such tools. Management reporting and alerting is another key criteria for selection. Threshold based email/pager alerts make life easier for your operations staff to know that all is well.

Performance and capacity

While performance is very important, do not forget the capacity aspect of DDoS attack mitigation. How many protocols, ports, IPs, connections, URLs, Hosts, User-Agents, 'Referers', cookies etc. can the appliance monitor? The more granular an appliance is, more controls and visibility you will have in attack mitigation.

Openness in specifications

DDoS attack mitigation is not as black-magic as it is made out to be. The technology and features that you look for should be clear to you. You should be aware of what visibility do you get and what controls you get under attack. The appliance should not be on auto-pilot without clearly specifying what it is doing. Look for well laid-out clear specification of DDoS attack mitigation techniques, and controls available to you.

Field upgrades

Your network traffic and requirements grow as your business grows.You want an appliance that grows with you. Look for an appliance that can handle 100 Mbps today for your Internet traffic needs and grow to 1000 Mbps license later in time without a hardware replacement.

A solution that looks like the least expensive based on list price for the appliance might end up costing much more when you purchase all the necessary licenses and add-on modules or services.

Role based management and audit trails

As your network traffic grows, you may have multiple operators/administrators in your network. Do ensure that different users have different roles and each modification or access is logged into trails that are maintained for audit purposes.

Performance and reputed third party validation

After buying a DDoS attack mitigation appliance, you don't want to regret later that you didn't have time to do your proof of concept – which all vendors avoid. Therefore it makes sense to have a third party validation from a reputed agency and not just a customer. How many packets/second can the appliance handle under attack? How many SYN packets per second can the appliance handle under attack? How many new TCP connections per second can the appliance handle under attack? How much latency does the appliance add to the packets as the packets pass through it?

Appliance throughput can range from 100Mbps to over 1Gbps. When comparing vendors' throughput claims, look closely to be sure you aren't comparing apples and oranges.

Post sales support

DDoS attack mitigation appliances are a new generation of appliances. You would not have seen the GUI elsewhere. You therefore need post-sales deployment help and help during attacks. Make sure that your vendor is known for its service. If the appliance has a GUI that's too simple to configure, it may not provide you sufficient control and visibility into attacks. If it is too complex, you may not be able to afford trained and skilled staff or will have to pay for the service. Find a good balance.

Customer reference is the best validation

While most users of a DDoS appliance avoid publicity, some users proudly publish their success. Look for public press releases by reputed organizations for an appliance. The more the better.

A sample matrix for solution comparison

Table 1: Feature matrix for DDoS solution comparison

Feature.
Packet Inspection Technology
Multi-Verification Process
Flood Prevention Schemes
Packet Inspection Depth

Table 1: Feature matrix for DDoS solution comparison (Continued)

Layer 3 Floods Handled
Layer 4 Floods Handled
Layer 7 Floods Handled
Realtime diagnostics
Visibility, ACLs, Bandwidth Controls
Traffic and Event Analysis
Reconnaissance and
Header and State Anomaly Prevention
No. of Virtual Partitions
No. of Networks/ Partition
Aggregate Throughput
Simultaneous Connections
Session Setup/Teardown Rate
SYN Flood Handling capacity
Latency
DDoS Attack Mitigation Response Time
Physical Interfaces (number and types)
Redundancy
Propgate Link State Change (PLSC)/ Link Down Synchronization
Chassis
Field Upgradability
Management
Centralized Event Reporting
Audit and Access Trails
Links Protected
Power Supply
Hard Disk Space (GB)
Interface speed Mbps
Packets per second handling capability under attack
Attack Mitigation Time
Dark Address Subnets (for blocking continents, countries, subnets)
Non-tracked Subnets (for whitelisting networks)
No. of Sources monitored
No. of Destinations monitored
No. of Concurrent Connections monitored
No. of concurrent three-way handshakes monitored
No. of TCP/UDP ports, ICMP type/code combinations monitored
No. of HTTP URLs, cookies, user-agents, hostnames and referers tracked

Conclusion

Buying a DDoS attack mitigation solution for your data center can be a daunting task, but it is made easier by being properly prepared. That means taking future growth and features into account. There are many decisions to make when you start to evaluate the solutions. In this chapter, I have discussed just a few of the items you should consider.

There is no single perfect DDoS attack mitigation appliance. Each product has strengths and weaknesses, and after you've evaluated your needs and decided which features are most important for your organization, you should carefully compare the technical specs and data-sheets of different products to determine which meet your own needs and budget the best.

FORTINET®