GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Hacker Tools, Techniques, and Incident Handling (Security 504)"
at http://www.giac.org/registration/gcih

Preparing to withstand a DDoS Attack

GIAC (GCIH) Gold Certification

Author: Gaurang K. Pandya, Gaurang_cert@outlook.com

Advisor: Richard Carbone

Accepted: October 31, 2015

Abstract

A Distributed Denial of Service (DDoS) Attack, unlike most other cyber threats, is a lethal form of threat that is almost impossible to eliminate, and its "planned" execution can have a deadly effect on the target. This form of cyberattack is still as dreaded as it was a decade ago. This attack, unlike other forms of cyber-attack, targets the limitations of IT systems. Additionally, tools to generate such attacks are freely available and easy to use. On the other hand, enterprises are ill prepared to handle these attacks.

It is due to this pervasive nature of attack that it is very prevalent and persistent. More often than not, it is capable of bringing a well-crafted and protected service to its knees. It has been noticed that quite often the targeted enterprise does not even realize that they are under a DDoS attack. Worse, even after realizing, they are not able to respond appropriately to it, as they are ill prepared for it.

This paper intends to provide details about the various technical and non-technical aspects that will help an enterprise prepare to withstand a DDoS attack.

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

1 Introduction

The Distributed Denial of Service or DDoS Attack is a distinct form of cyber threat with various aspects that differentiates it from other attack types. The first one being, it targets the inherent limitations that exist in current systems. That is, it targets the memory, network bandwidth, and CPU of target systems. Unlike traditional attacks, this form of attack is generated from an army of compromised hosts known as botnets. It is these factors that make this attack easy to launch and difficult to defend against. When attack traffic is generated by botnets, the attacker will suffer the same problem of resource consumption that the target will. This is the reason behind distributing an attack using several hosts, thus the making attack bigger and less resource intensive. Hence, the name "Distributed" denial of service attack.

The tools to generate DDoS attacks are present in some operating systems and can easily be downloaded and installed in others. Many are free of cost. These include LOIC and HOIC, to name a few. Even a simple utility, like "ping," can cause considerable damage to an unprotected network if used appropriately. On the other hand, there are more sophisticated and organized ways to launch these attacks and there is a growing underground economy around this. Services, like rent-a-botnet and botnet-as-a-service, are specially tailored to the meet needs of an organization trying to bring its competitor, governments, or others down. These attacks are also widely used by hacktivists.

1.1 DDoS attack categories

DDoS attacks can be categorized in several ways; but broadly, they can be put in two categories, based on what they target, and how they target.

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

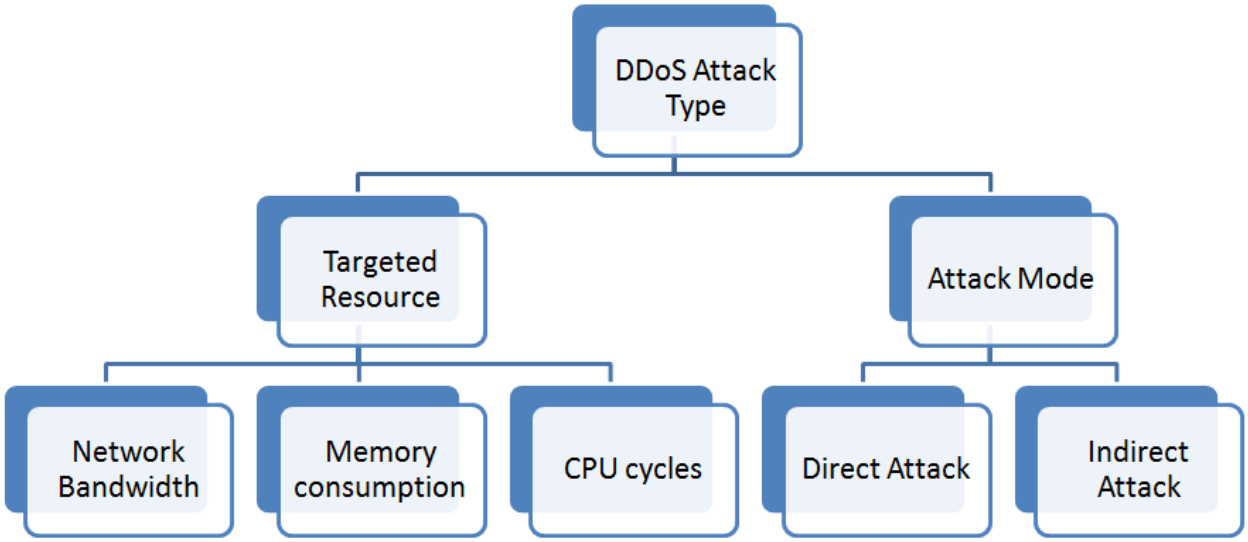

Figure 1: DDoS Attack Types

Commonly DDoS attacks are conducted by pivoting from compromised end user computers, generally referred to as zombies. A collection of zombies is called a botnet, and a host that controls this botnet is known as the command and control server.

There have been instances when government agencies have replaced the malicious command and control server with their own server to help kill the botnet (Bright, 2011). In some instances, the command and control server itself is destroyed, thus orphaning entire botnets and rendering them useless (Bright, 2011).

1.1.1 Network bandwidth consuming attacks

This attack targets available network bandwidth, and consumes it to its maximum limits, leaving no room for legitimate traffic to enter the network, thus denying access to the service. This type of attack is generated by crafting network traffic packets that hold the maximum possible payload data. Table 1: Network bandwidth consuming attacks in the Appendix provides more information about this type of attack.

1.1.2 Memory consuming attacks

This is one of the oldest forms of DDoS attack and is still as effective as it was years ago when the 'Syn flood' was discovered. If a network device is targeted with this attack, the entire network can be brought down, as opposed to a single host. Table 2: Memory consuming attacks in the Appendix provides more information about this type of attack.

© 2015 The SANS Institute Author retains full rights.

1.1.3 CPU consuming attacks

Contrary to network bandwidth consuming attacks, this attack uses many small sized packets to target the host. This consumes many CPU cycles on the target host, thus completing the attack. Table 3: CPU consuming attacks in the Appendix provides more information.

1.1.4 Direct attack

All the above stated attacks, if they directly hit the target host, are then called a direct DDoS attack, and they tend to yield average results as attacking hosts also need to work harder for them to hit the target hard.

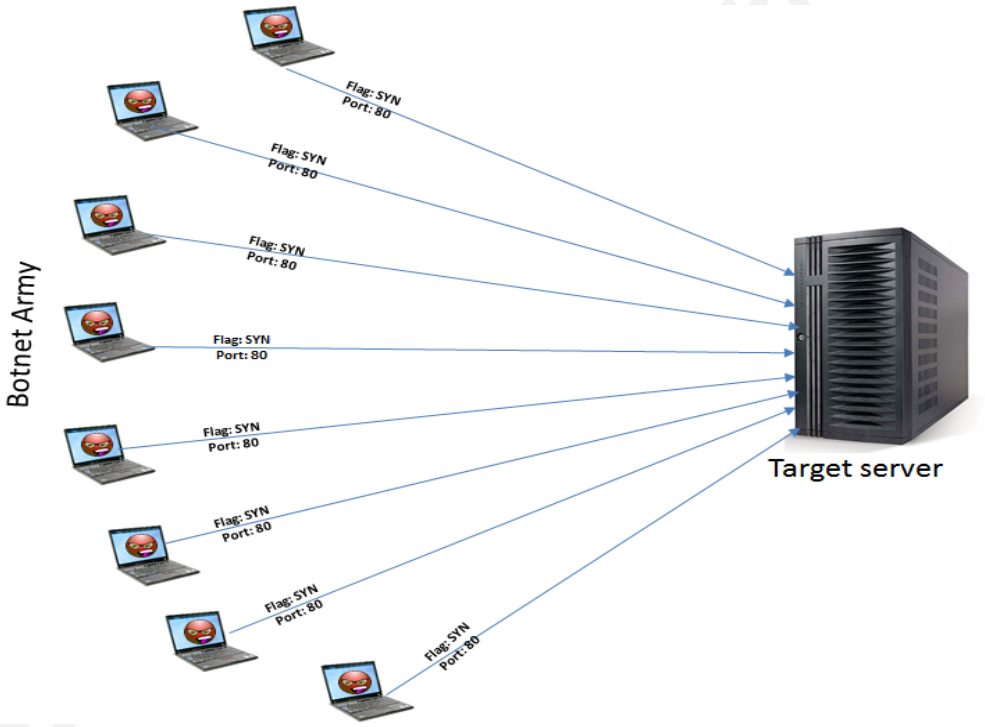

Figure 2: Direct DDoS Attack

This form of attack does not require the source address of packet to be spoofed, and zombies attack the target with their own publicly accessible IP addresses, thus identifying themselves.

1.1.5 Indirect attack

This is a more advanced form of attack, where attack traffic from zombies is directed to other hosts for reflection or amplification. This reflected or amplified traffic is directed at the target. The reason for launching an indirect attack is typically for amplification. However, this attack type can also hide the true attack source, making eradication difficult. In an indirect attack, the

© 2015 The SANS Institute Author retains full rights.

attacker sends malicious traffic to an intermediate host, after manipulating traffic to make it look like it is originating from the target. Thus, when the reflecting host receives the packet, it replies to the target.

In a reflection attack, the goal is to hide the identity of the true attacker, using intermediate hosts. These intermediate hosts are just Internet hosts. However, due to the nature of the service they perform, they are abused by the attacker and used to reflect the attack to the real target.

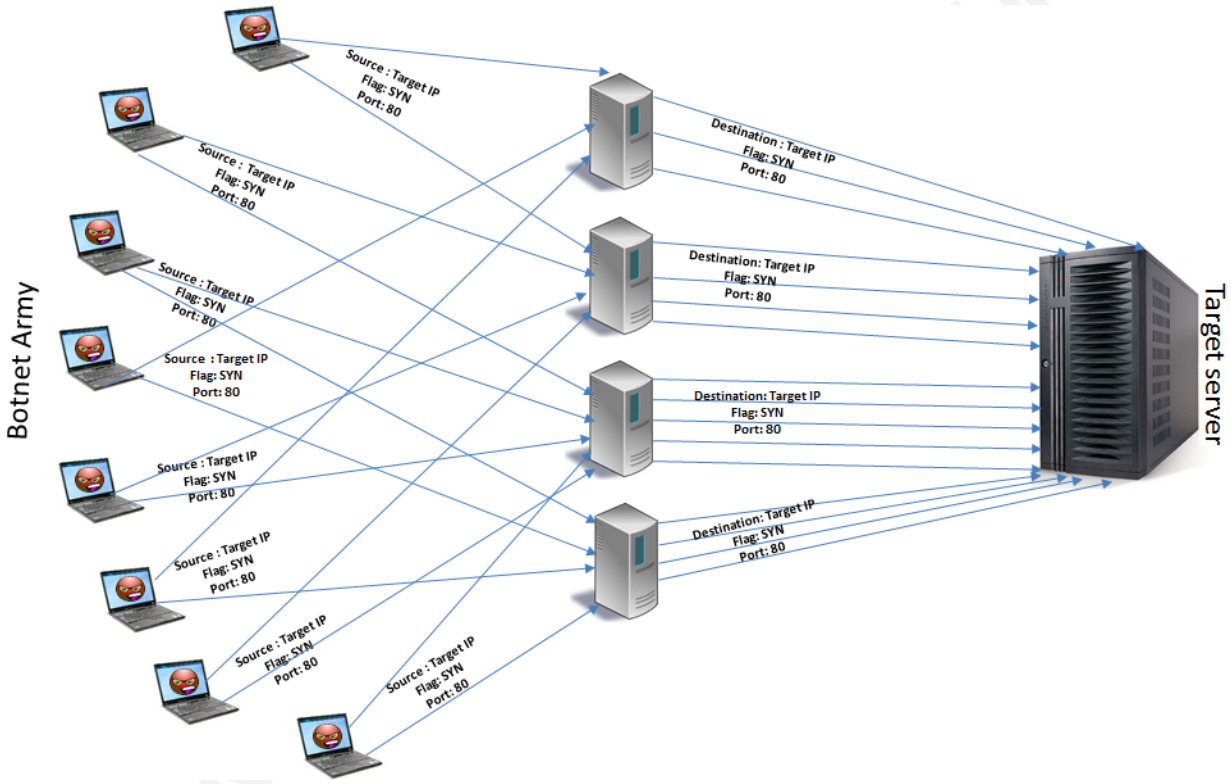

Figure 3: Indirect Reflection DDoS Attack

The attacker can also use legitimate online services like NTP, DNS, SNMP, and ICMP to pivot the attack resulting in an amplification attack.

© 2015 The SANS Institute Author retains full rights.

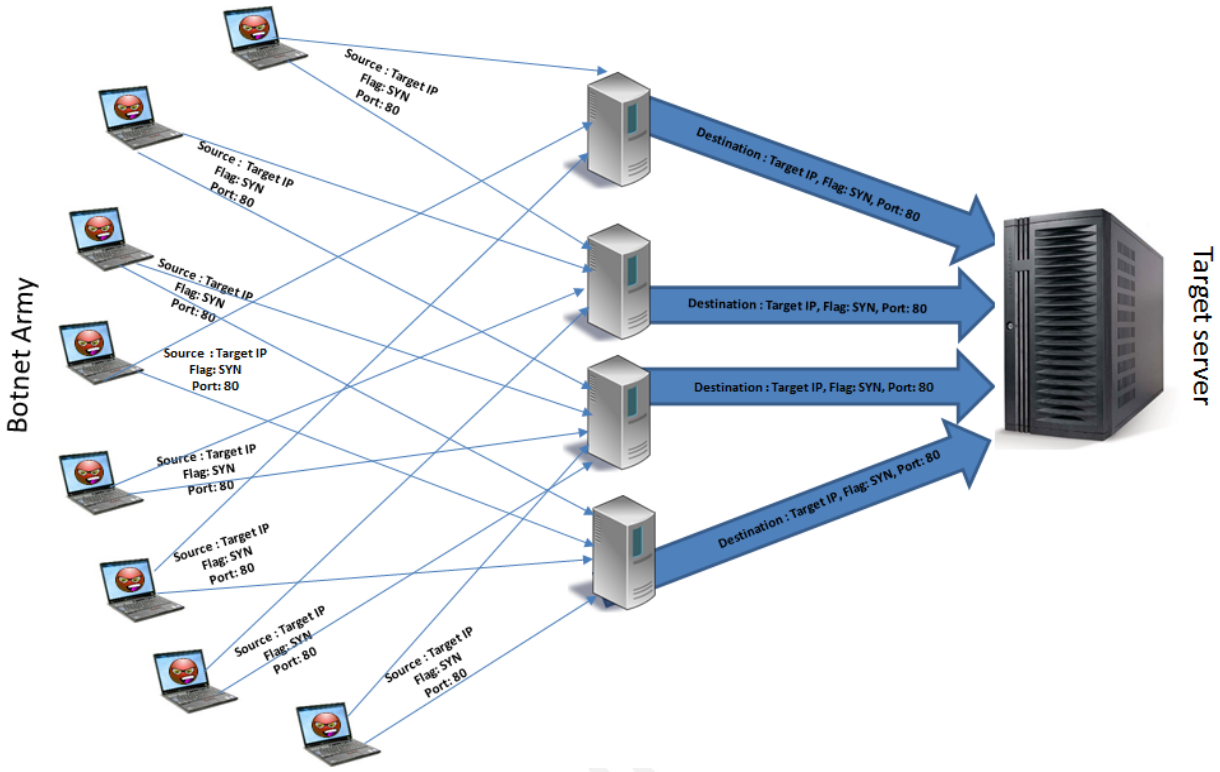

Figure 4: Indirect Amplification DDoS Attack

1.2 Growth in DDoS attacks

As DDoS attacks are highly effective and easy to launch, they have grown tremendously over the past few years. For example, in 2001 the size of a known DDoS attack was 400 M (Reese, 2008) whereas a similar attack in 2014 had gone up to 320 G (Wood, 2014), making it 800 times larger in fourteen years.

© 2015 The SANS Institute Author retains full rights.

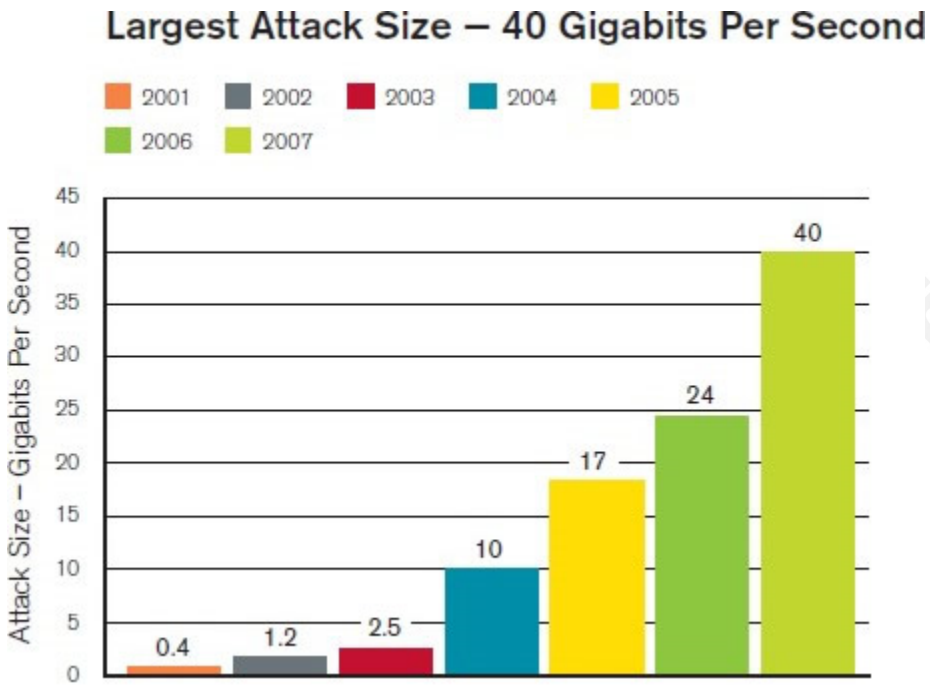

Figure 5: DDoS attack growth, Source: (Reese, 2008)

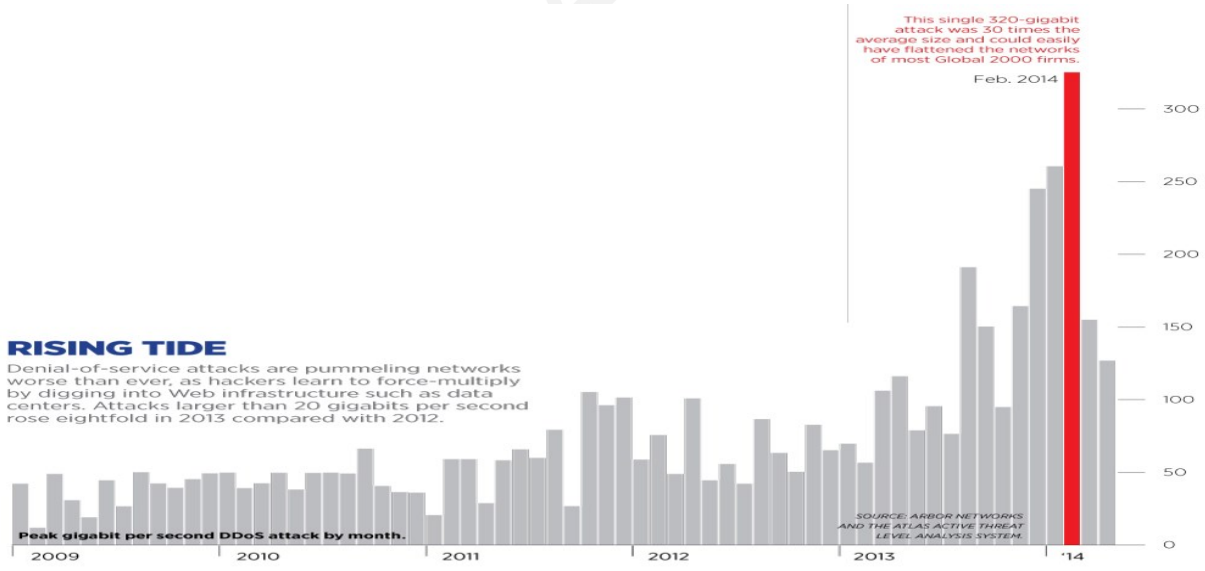

Figure 6: DDoS attack growth, Source: (Wood, 2014)

1.3 Motivations behind DDoS attacks

Since the time of its inception, the DDoS attack has been used for a wide variety of motivations, and knowing them helps deploy the necessary controls to counter them.

© 2015 The SANS Institute Author retains full rights.

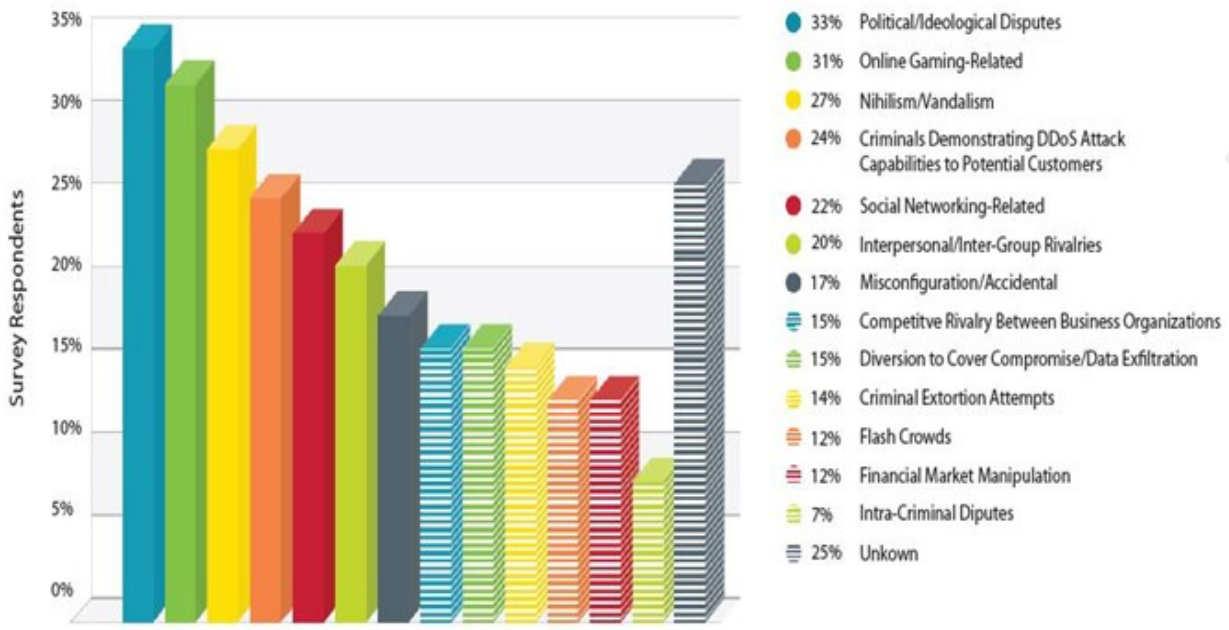

Figure 7: Motivations behind DDoS attacks, Source: (Beardmore, 2013)

Broadly, the motivations can be categorized as follows:

- Revenge, as was used by Anonymous in 2012 (Chen, 2012).
- Extortion, as recently warned by FBI (Fisher, 2015).
- Political, as was used by Russia against Georgia in 2008 (Nazario, 2008).
- Competitive Advantage, as ANZ was attacked in 2012 (Lee, 2012).
- Hacktivism, as Sony was attacked in 2014 (Peters, 2014).
- Distraction, as warned by FBI in 2011(Sanders, 2011).

2 Protection planning

Asides just enterprises, the DDoS protection planning exercise is necessary for every site that needs protection. This approach helps tailor the process for those sites that are non-standard or have fewer resources. The protection planning phases are shown in the following figure:

© 2015 The SANS Institute Author retains full rights.

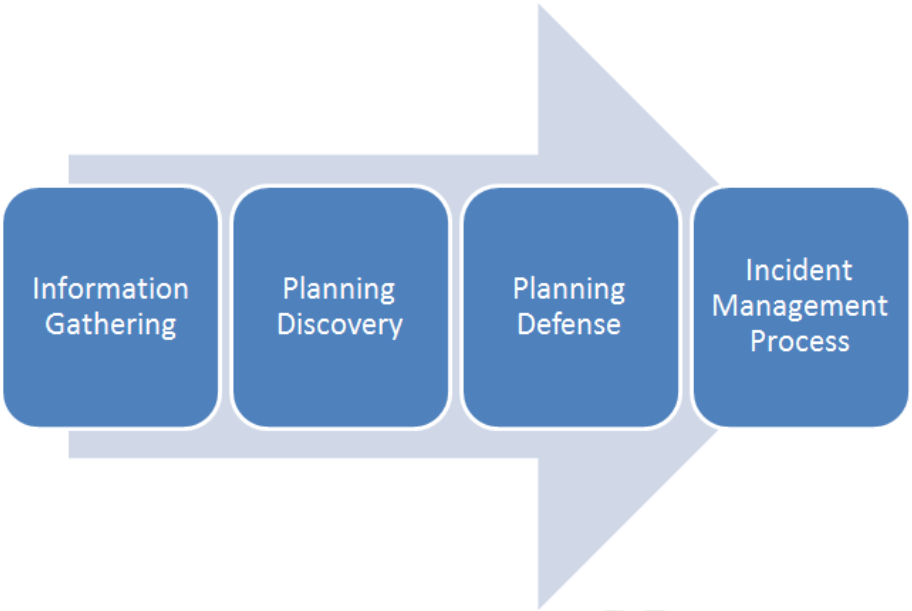

Figure 8: Protection Planning Phases

2.1 Information gathering

This phase helps gather answers to some important questions and establish a base for the entire DDoS protection planning exercise. The questions to ask are:

- What needs to be protected?
- Why it needs to be protected?
- What is the least level of protection required?
- What are available protection options?
- Which is the best option?
- Who will provide the protection?
- How will they provide it?

Once the relevant information in terms of answers to the above questions are arrived at, the rest of the phases will help gauge the available options and determine the best one.

2.2 Planning discovery

The goal of this phase is to achieve an early discovery of a DDoS attack and generate alerts. This phase will help identify the various options available for discovering a DDoS attack and select the best of them for setting up DDoS monitoring and alerting.

© 2015 The SANS Institute Author retains full rights.

In performing effective DDoS discovery, it is vital to appropriately position the monitoring system, and properly configure it. This helps reduce false positives. Along with monitoring, every monitoring system must provide ways of generating alert notifications, and that needs to be carefully planned as well. For example, sending an email to alert about a DDoS attack on email systems is not a good idea.

2.3 Planning defence

Upon successful discovery of a DDoS attack, defending against it will be the next important step. Defence can be one of two broad types. The first is the ability to eradicate the attack in its totality thus allowing zero effect on an organization's day-to-day operations. The second is the organization's ability to weaken the attack's effect on the network and resume normal operations, even if only with a reduced capacity. It is obvious that any organization should aim for the first goal, but the second one may be more practical and affordable.

The defence planning phase focuses on helping an organization achieve either (or both) of these goals by providing various options that can be used to defend against a DDoS attack. Though this phase explores some ways of using existing resources to defend against a DDoS attack, it is not always possible. Traditionally, security devices are deployed in-premises, and when an organization is under targeted DDoS attack the network connectivity will become saturated. Hence, traffic will be dropped much before reaching these security devices for it to be effective. This completes the DDoS attack. To overcome this challenge, the organization will have to fall back on a third-party network or security service providers to handle DDoS attacks on its behalf.

2.4 Incident management process

This phase ties the knowledge obtained from all the other phases together with a set of procedures and processes built around identified people, with the help of selected technologies. The DDoS incident management process should be fully integrated into the organizational security incident management process. This helps achieve the best possible protection from DDoS attacks, and seamless integration within the organizational culture, thus making it easy to perform, and effortless to adapt.

The processes should be designed to reveal at least the following facts:

- How will the DDoS attack be discovered?

© 2015 The SANS Institute Author retains full rights.

- How will it be defended against?
- Who will act and how will they defend against the attack?
- How will the processes be enhanced over time with learnings obtained from various types of defended attacks?

3 Information gathering

Before initiating DDoS protection planning, it is important to identify the assets that need protection throughout an organization. Therefore, it is important to have a detailed asset inventory in place that includes not just information about assets, but has other information as well such as the security policy, list of the stakeholders, their contact information, etc.

3.1 Asset information

While almost all organizations do maintain asset inventory, such a general-purpose inventory lacks some vital information that is required to make informed decisions in the event of an IT security incident. In order to help an organization gather all relevant information about various assets,

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

Table 4: Asset inventory template given in Appendix can be used.

3.2 Network information

Another significant source of information is the network details. Other than physical circuits, organizations have several logical circuits as well in the form of Generic Routing Encapsulation (GRE) tunnel and site-to-site VPN tunnels. It is important to collate all the circuit information as well and document it. Table 5: Network Circuit inventory template and

Table 6: VPN inventory template given the in the Appendix can help organizations gather this vital information.

3.3 Site information

While information stated in the previous sections needs to be documented site-wise, there is some additional information that is required to be documented for the site itself, such as location, criticality, etc., which would help in better assessing the site.

This document should provide a macro-level view of the site as a whole and serve as a ready reference while taking decisions that would affect the entire site. To help gather this information Table 7: Site inventory template given in the Appendix can be used.

3.4 Stakeholder information

DDoS incident management, as with any other security incident, needs a large team to handle an attack and collecting the information regarding the team members is an important requirement. Before starting the individuals' information gathering exercise, it is required to identify a set of teams and their roles in DDoS incident management so that selected people from those teams can be contacted during a DDoS attack, should the need arise. Table 8: Key teams list and their role given in the Appendix can be used to identify those teams within an organization. Once the team is formed, the members' contact information must be collected and maintained in the format given in Table 9: Contact information collection template found in the Appendix.

For the post finalization of team information collection, every team member should be made aware of his or her roles, responsibilities, and expectations from the point of view of the overall DDoS incident management process.

© 2015 The SANS Institute Author retains full rights.

3.5 Security policy and compliance information

This information gathering exercise cannot be complete without collecting appropriate information from various policy documents. Table 10: Security policy documents of the Appendix can be used as reference to gather basic information about different security policies and its contents.

Note: Not every organization will have all of the security policies found in Table 10, but relevant information should be available as they relate to security policy documents.

Security control and configuration directives not only come from security policy documents, additionally, they also are dictated by country, industry specific compliance, and regulatory norms including industry specific standards. Thus, it becomes equally important to understand an organization's compliance and security requirements.

Table 11: Compliance matrix provides information pertaining to various security compliance requirements for various geographies along with their industry, found in the Appendix.

4 Planning discovery

The goal of this phase is to help an organization discover that it is under a DDoS attack, within fifteen minutes of the attack becoming lethal. There are several technologies available. These are either general purpose or purpose-built for DDoS detection that help an organization achieve this goal. On the other hand, various free and commercial tools are also available to help implement those technologies. Details about various technologies and different tools to implement them can be found in following sub-sections.

4.1 Network management server

As discussed in the Introduction (Section 1), DDoS attacks target the resource limitation of an IT infrastructure. While Network Management Servers (NMS) are designed to monitor the

© 2015 The SANS Institute Author retains full rights.

utilization of IT resources, they also serve as an excellent solution for discovering a DDoS attack that is in progress and is consuming monitored resources.

4.1.1 Positioning monitoring station

NMS applications can mostly be deployed in distributed mode with the polling stations positioned at strategic locations reporting to a central monitoring station, to minimize false positives.

To effectively use this feature, an NMS polling station should be deployed in each of the WAN separated locations, and even within the LAN, in segments that are of high importance, making sure all these polling stations report their status back to the centralized monitoring station.

In order to get the end user's perspective of service, the polling stations can be deployed in the user segment, and if user requests are originating from the Internet, a polling station can be deployed with a cloud service provider.

4.1.2 What to monitor?

In order to discover a DDoS attack, it is necessary to monitor critical IT resources along with the complete path of traffic from the polling station. If the NSM system used by an organization provides feature to define relationships between various monitored objects such as "Parent-child," "dependency" or "critical path" then those should be utilized to the fullest. This helps NSM system generate fewer false positive alerts and perform more efficiently.

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

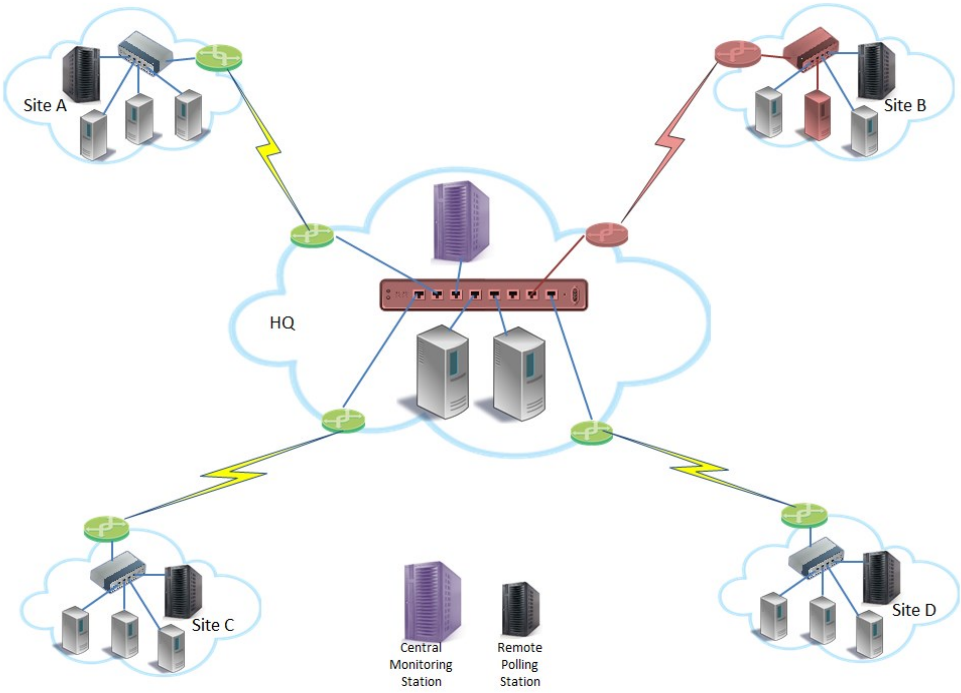

Figure 9: Distributed NMS Deployment

In the above illustration, a critical server located in Site B needs to be monitored for resource utilization using NMS. To provide thorough monitoring for that server, not only should the servers be monitored by a locally deployed polling station, but every link leading to that from HQ should also be monitored from the central monitoring station.

Certain NMS systems provide feature to identify network path failure and disable alerting for resources located behind that. If possible, WAN links between central and remote routers should be configured for such path monitoring, which is sometimes referred as "critical-path" monitoring.

Once host uptime monitoring is configured appropriately, the next step is to configure the NMS system to perform additional checks against monitored hosts as they help discover DDoS attack. Table 12: NMS Checks found in the Appendix provides the list of checks that can be performed on end servers and intermediate hosts such as a router, switch, or firewall.

4.1.3 NMS effectiveness

The NMS based solution for discovering a DDoS attack has its own advantages and disadvantages as highlighted in Table 17: Effectiveness of various technologies in the Appendix.

© 2015 The SANS Institute Author retains full rights.

4.1.4 NMS tools

A table listing of the various commercial and open source NMS tools that an organization can use for system monitoring is given in the Appendix as Table 16.

4.2 Flow monitoring

Another important way to discover a DDoS attack is using Flow monitoring. Network flows are the metadata of network traffic that is flowing through selected devices and consists of the following seven aspects of network traffic as seen by a network device:

- Ingress interface number.
- Source IP Address.
- Destination IP Address.
- IP Protocol.
- Source port.
- Destination port.
- IP TOS.

The Network Flow system was first introduced by Cisco named NetFlow; later prominent networking vendors came up with names for their own versions of flow exporting protocols as given in Table 13: Flow exporting vendors found in the Appendix. The current vendor agnostic flow monitoring protocol is called IPFIX.

4.2.1 Flow monitoring components

There are two important components in setting up flow-based monitoring infrastructure – the monitored and monitoring host. The monitored host can be active or passive; the monitoring host is either a collector or central monitoring station, depending on the deployment type. There are two deployment methods for setting up flow based network monitoring – standalone and distributed deployment.

An actively monitored host is one that exports flows by itself, whereas a passively monitored host relies on external tools for generating and exporting flows on its behalf. The flow generating tool gets a copy of the traffic from the switch or network tap and exports flows.

© 2015 The SANS Institute Author retains full rights.

The flow collector is a server that accepts flows from both types of monitored hosts, and reports back to the central monitoring station. The central monitoring station is responsible for providing user interface, generating alerts, reports, etc.

4.2.2 Flow monitoring architecture

Like NMS deployment, flow-monitoring deployment can be distributed across different geographies while reporting can be done to a central monitoring station. However, that is required only to accommodate a large network where monitored interfaces exceed approximately two hundred. For smaller networks, a stand-alone flow-monitoring server is sufficient.

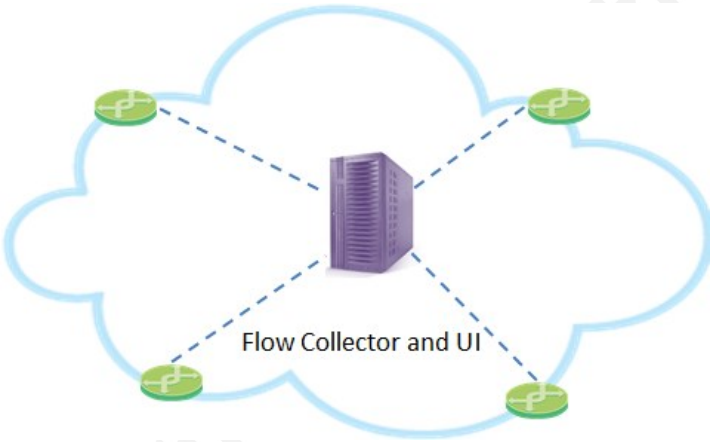

Figure 10: Standalone Flow monitoring deployment

When deployed in a distributed way, the remote collectors perform tasks like flow collection, summarization, caching, and normalization, whereas the central monitoring station performs tasks like graph generation, alert notification, and reporting.

© 2015 The SANS Institute Author retains full rights.

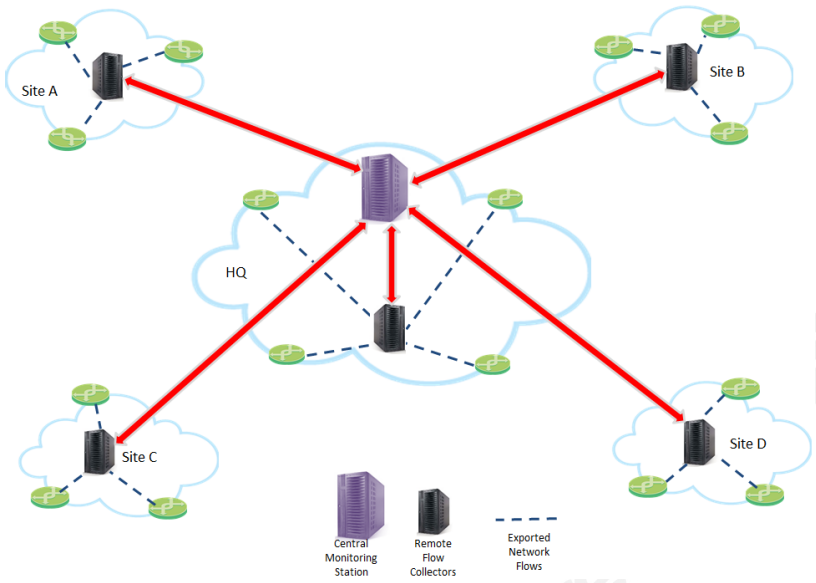

Figure 11: Distributed Flow monitoring deployment

4.2.3 What to monitor?

In order to discover a DDoS attack effectively, choosing the right interface that needs to be under flow monitoring is of prime importance. Since DDoS attacks generally originate from outside of an organization, it is important to monitor the flow from those external facing interfaces.

Monitoring backbone or core router interfaces should be avoided, unless there is a compelling reason for it. This approach does not just help manage loads on already heavily used routers but also eliminates errors, caused by the double counting of flows.

4.2.4 Flow monitoring effectiveness

The effectiveness of a flow monitoring solution depends on the advantages and disadvantages that the solution provides. This has been highlighted in Table 17: Effectiveness of various technologies found in the Appendix.

4.2.5 Flow monitoring tools

Table 16: DDoS protection tools and services provided in the Appendix contains various commercial and open source flow monitoring tools that an organization can use.

© 2015 The SANS Institute Author retains full rights.

4.3 Security information and event management

Security Information and Event Management (SIEM) tools address the problem from a different perspective than flow or NMS do. These tools work on event logs from various network devices and servers. Along with rules configured therein, SIEM tools can help discover DDoS attacks.

4.3.1 SIEM components

Generally, there are three main components in a typical SIEM solution deployment. At a high level, they are the ones that generate event-feeds secondly those that normalize those event-feeds and third one that does correlation with the normalized event-feeds. Each of these components is described below:

- Event Generator: These are servers, devices, or applications that generate event logs to be fed to the SIEM system.
- Event Normalizer: These purpose-built engines take log feeds from event generators, and normalize, compress and redirect them to the correlation engine.
- Event Correlation Engine: This core SIEM component performs event correlation, and generates event notification.

4.3.2 What to monitor?

Unlike technologies discussed thus far, in SIEM monitoring, it is recommended to monitor every component that is delivering or helping to deliver business critical service. This includes servers, infrastructure devices or any other platform that these are dependent on.

To clearly identify service components that require SIEM monitoring, a dependency map can be drawn, showing all the components that help deliver a critical service – be it in the same server or different set of servers. While designing this dependency map one has to remember that there could be multiple components capable of being monitored and that need monitoring residing on same server.

4.3.3 SIEM effectiveness

In order to gauge the effectiveness of SIEM tools for discovering a DDoS attack, Table 17: Effectiveness of various technologies in the Appendix can be consulted, as it lists their advantages and disadvantages.

© 2015 The SANS Institute Author retains full rights.

4.3.4 SIEM tools

Table 16: DDoS protection tools and services contains various commercial and open source SIEM solutions that an organization can use for discovering DDoS attacks.

4.4 Purpose-build anti-DDoS appliances

With advancement in DDoS attacks, there has also been advancement in market for creating solutions around DDoS protection. Thus, there are purpose-built DDoS discovery tools and services available from various vendors. These tools are capable of providing a higher degree of protection with less effort.

There are organization and service provider-based grade appliances available from various prominent vendors that discover as well as eradicate a DDoS attack with high degree of accuracy.

4.4.1 Appliance positioning

Purpose-build Anti-DDoS appliances are generally available in two types, one that can just discover a DDoS attack, and the other that can also defend against it, thus protecting the network. The positioning of such a device in a network varies with its capabilities. Since it is recommended to handle DDoS attacks as early as possible, deploying these devices towards the network edge is preferred.

There are three distinct modes in which Anti-DDoS appliances can be deployed for discovering DDoS attacks.

4.4.2 Modes of deployment

These purpose built Anti-DDoS appliances work In-band or via SPAN/TAP (or Out-of-band modes).

In-band Mode

In this mode of deployment, the appliances are placed in the path of network traffic similar to network firewalls or IPS. The advantage of this mode is that the appliance has complete visibility of network traffic, and provides continuous protection against DDoS attacks. Often, these appliances perform both discovery as well as eradication of DDoS attacks.

© 2015 The SANS Institute Author retains full rights.

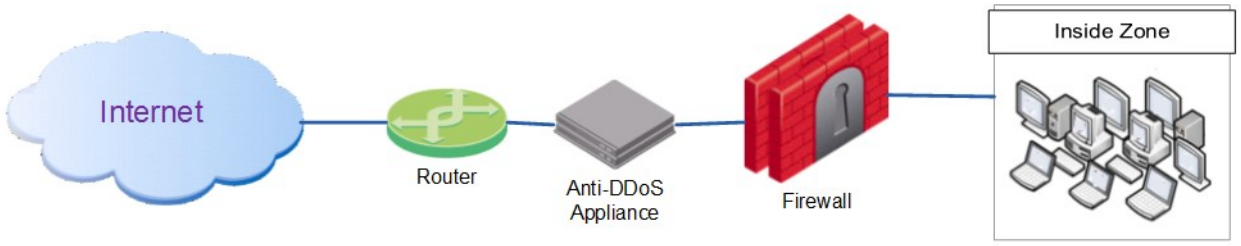

Figure 12: In-band Mode deployment

On the other hand, this deployment increases complexity, and introduces yet another point of failure in the network, as shown in Figure 12.

SPAN/TAP Mode

Unlike the In-band mode, the device deployed in this mode works with a copy of network traffic and performs DDoS discovery based on that traffic. The network traffic copy can be provided to the device by using the SPAN/RPAN facility of a network switch or using a network TAP device. A sample deployment is shown in Figure 13: SPAN/TAP Mode deployment:

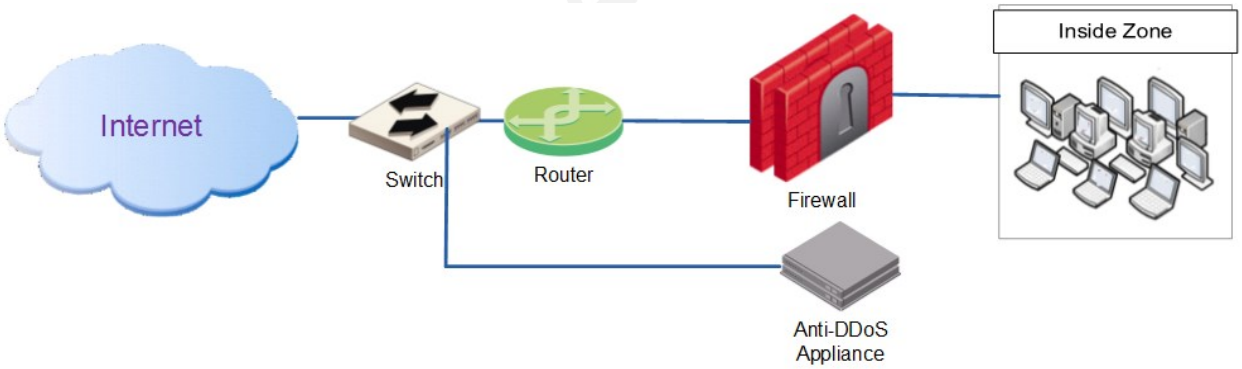

Figure 13: SPAN/TAP Mode deployment

The advantage of this mode is that it does not add another point of failure or any additional layer of complexity like the In-band mode. However, as the traffic is not passing through it, it cannot actively block malicious traffic and will always have to depend on other devices for defending against a DDoS attack.

Out-of-band Mode

In order to deploy an Anti-DDoS appliance in Out-of-band mode, the appliance is placed independently in the network regardless of router's position. However, the metadata of traffic

© 2015 The SANS Institute Author retains full rights.

flowing through designated routers is sent to an Anti-DDoS appliance for it to perform successful discovery of DDoS attack.

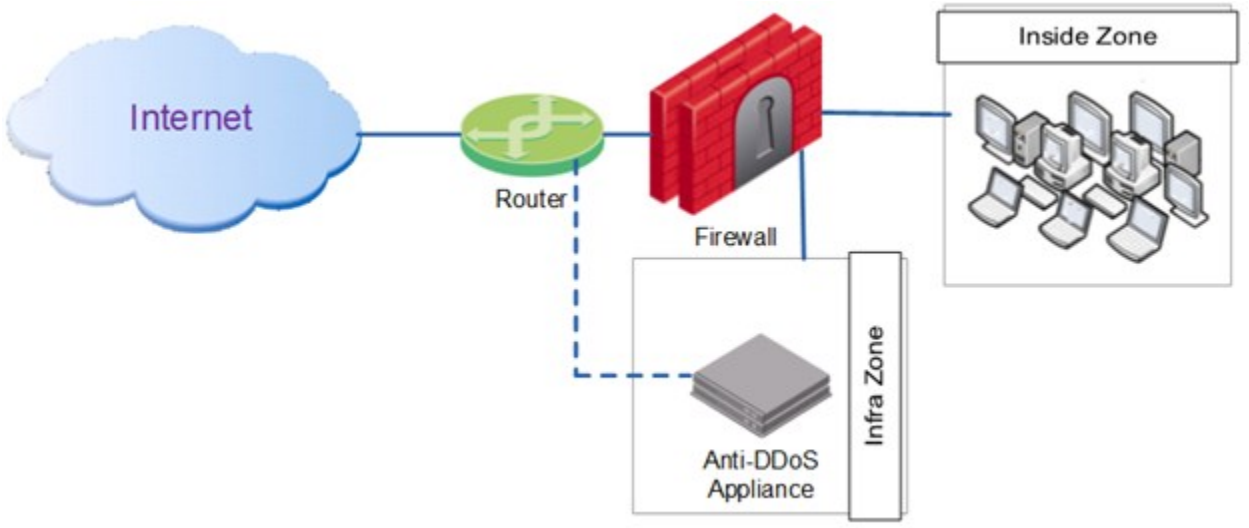

Figure 14: Out-of-band Mode deployment

The mode in which an Anti-DDoS appliance can be deployed depends on the appliance itself, as not all of them are designed to be deployed in this mode.

4.4.3 Purpose-built appliance effectiveness

An in-premises deployed, purpose-built Anti-DDoS appliance is best suited for discovering both SSL based and low/slow-type attacks. While these in-premises solutions are quick in responding to an attack and provide continuous protection, they tend to fail when the organization comes under a high volume, targeted, and persistent attack.

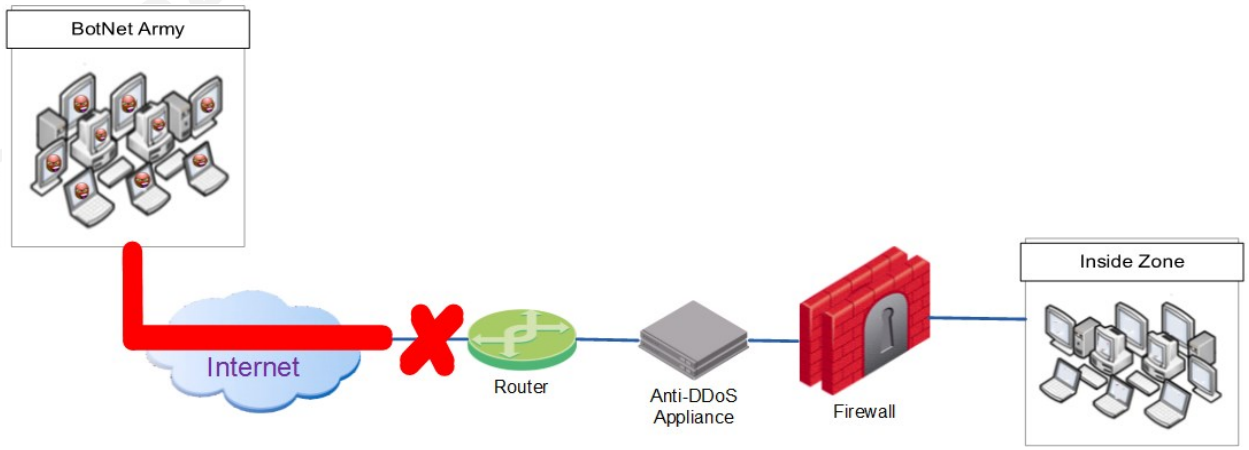

Figure 15: DDoS attack targeting last mile connectivity

© 2015 The SANS Institute Author retains full rights.

This is because the attack traffic, before reaching Anti-DDoS appliances, chokes the "last mile" of network connectivity to the organization, rendering ineffective any solution that is deployed in-premises in protecting against a high profile DDoS attack, as shown in Figure 15: DDoS attack targeting last mile connectivity.

In order to get more clarity on the advantages and disadvantages of this solution, Table 17: Effectiveness of various technologies can be consulted, under the Appendix.

4.4.4 Anti-DDoS appliance providers

Table 16: DDoS protection tools and services provided in the Appendix contains various anti-DDoS appliance providers.

4.5 Purpose-built anti-DDoS service

These purpose-built Anti-DDoS services provide protection from high volume and targeted attacks. These services complement in-premises based purpose-built Anti-DDoS appliance solutions.

There are two types of Anti-DDoS service providers – network service providers or Internet Service Providers (ISP) and Security Service Providers(SSP) who do not generally provide network services nor own cables.

4.5.1 Anti-DDoS service from network providers

Several prominent network service providers provide DDoS protection as a value added service with their network pipes, in many cases calling it a "clean pipe" service.

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

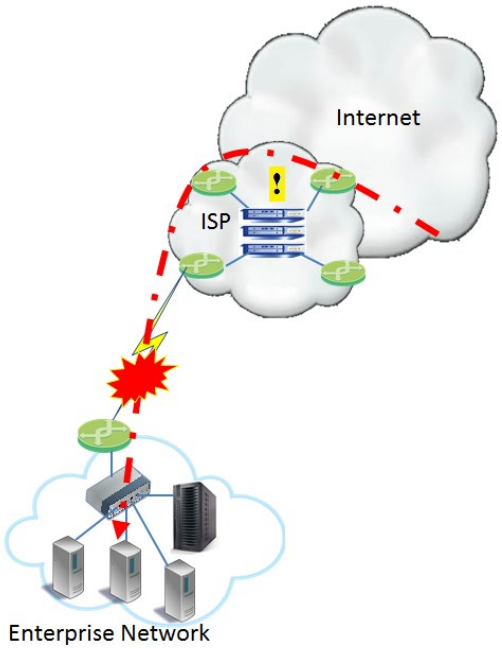

Figure 16: DDoS Discovery at ISP

In order to provide these Anti-DDoS services from their cloud, the network service providers generally deploy various purpose-built Anti-DDoS appliances in their network. In addition, they enable their edge routers to feed information to it. This enables them to perform DDoS discovery on their clients' behalf, as shown in Figure 16: DDoS Discovery at ISP, and alert clients accordingly.

The advantage of opting for an added DDoS discovery and alerting service from the network service provider is that it involves minimal to no efforts from the organization's side. Network service providers are already aware of which network segments are used by an organization; all they have to do is enable monitoring on those segments. The flip side of this service is if an organization has connections from multiple ISPs, and one/some of them are not providing such a service, then effectively, the organization is unprotected.

4.5.2 Anti-DDoS service from security service providers

When Security Service Providers (SSP) that do not own cable infrastructure provide these Anti-DDoS services they take advantage of subscribing to multiple high-bandwidth connections from various Tier-1 network service providers. This gives them the flexibility of choosing a network provider and achieving network level redundancy.

© 2015 The SANS Institute Author retains full rights.

In order to discover a DDoS attack, these SSPs either take network traffic metadata from their client's edge routers over a secure tunnel or get their client's DNS changed to their DNS, as elaborated on in Section 5.4.2.

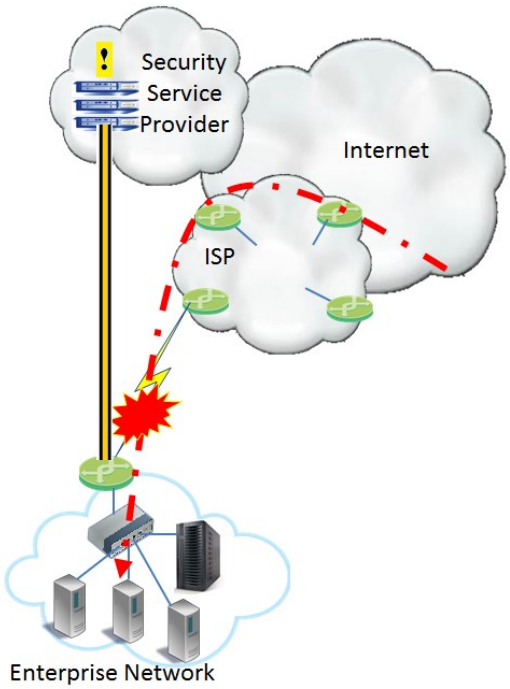

Figure 17: DDoS Discovery by Security Service Providers

Since these SSPs are network agnostic, they provide protection to their clients regardless of the network provider.

4.5.3 Purpose-built anti-DDoS service effectiveness

Much like any other solution, even this approach for handling DDoS attacks has various advantages and disadvantages as documented in Table 17: Effectiveness of various technologies found in the Appendix.

4.5.4 Purpose-built anti-DDoS service providers

Table 16: DDoS protection tools and services found in the Appendix contains information about various Anti-DDoS service providers.

© 2015 The SANS Institute Author retains full rights.

4.6 Hybrid DDoS discovery solution

This, arguably, is the most efficient approach for discovering a DDoS attack. This approach combines the best of both worlds. The solution involves deployment of an in-premises Anti-DDoS appliance, and the subscription of an Anti-DDoS service from a network provider. With this approach, the organization is able to discover most attacks at the provider's network edge, which provides the organization with an early warning before the malicious traffic hits their edge. In situations where the provider is unable to detect an attack, the in-premises deployed Anti-DDoS appliance will detect it. This ensures that a DDoS attack is discovered, whatever the case may be.

5 Planning defence

The battle against DDoS attacks is partially won when the organization has succeeded in discovering an attack within fifteen minutes of it starting to affect them. The next logical step is to start eradicating it, achieving complete defence from the attack.

5.1 General purpose in-premises security appliances

Traditional network and security appliances already deployed in an organization can also provide basic levels of protection from DDoS attacks. Once an attack is discovered by any of the previously mentioned means, the attack information can be obtained from those tools and fed into these traditional network and security appliances in order to eradicate the attack.

5.1.1 Firewalls

These appliances can provide protection if the attack is simple and is originating from a few specific sources. Firewalls also offer "Syn protection" that prevents a Syn Flood attack from spoofed sources. They also provide Geo-IP and Bogon/Dark IP-based filtering, which can help effectively eliminate an attack originating from unintended or non-existent IP address ranges.

5.1.2 Routers

Modern routers provide firewall like functionality, and the same can be utilized to eradicate DDoS attacks, as discussed in the previous section. Additionally, routers also provide the traffic-shaping and rate-limiting feature that can be used to reduce the impact of an attack on networks located behind the router.

© 2015 The SANS Institute Author retains full rights.

5.1.3 Intrusion prevention system

One unique capability this device has over others, as previously mentioned, is that it has application level visibility in network packets. Hence, if there are attacks that are targeting a legitimate service, they cannot be blocked using firewalls but can be eradicated by creating custom signatures and applying them in the IPS.

For example, when an attack is targeting a legitimate DNS server, and DNS requests packets from the attacker have a unique domain name, then that can be taken as a pattern, and any packets that matches the pattern can be dropped using IPS.

5.1.4 Web application firewall

Much like IPS, these devices also have application level visibility but only for HTTP(S) packets. Hence, in situations where an attack is targeting legitimate HTTP servers, and if malicious HTTP requests follow a pattern, those can be blocked using this appliance. For example, when the attack is targeting a legitimate HTTP server and the request packets have a unique "User-agent" string in it, a rule can be written to block every request with that specific string. This effectively defends against the DDoS attack.

5.2 Purpose-built in-premises Anti-DDoS appliance

The DDoS protection mechanisms discussed thus far are only partially useful in protecting a network from DDoS attacks, as they can protect from only certain types of attack. There are purpose-built Anti-DDoS appliances available from various vendors that provide thorough protection against attacks. These appliances provide a blend of defence mechanisms that are more effective than all the other security appliances discussed so far.

These purpose-built Anti-DDoS appliances can be deployed in two modes – In-band deployment, and Out-of-band deployment.

5.2.1 Appliance positioning

Much like purpose-built DDoS discovery devices, even defensive devices should be deployed towards the edge of network. This protects entire the network behind it from attack when the device is deployed in In-band mode. When the device is deployed in Out-of-band mode, it must be configured to do network route injection in edge router, using dynamic routing protocols. This helps the device become inline when there is need for scrubbing attack traffic. In order to avoid

© 2015 The SANS Institute Author retains full rights.

convergence and route injection delays, the appliance itself should be plugged into one of the interfaces of that edge router.

5.2.2 Mode of deployment

Purpose-built Anti-DDoS appliances work mostly in In-band and Out-of-band modes.

In-band deployment mode

In this mode, the appliance is always in the path of traffic and hence able to provide continuous protection to networks behind it from DDoS attacks, as shown in Figure 12: In-band Mode deployment.

The advantage of this type of deployment is that the network is continuously protected from DDoS attack as traffic is always flowing through these appliances. On the other hand, these additional devices add to network complexity, as they introduce yet another point of failure.

Out-of-band deployment mode

The Anti-DDoS appliance when deployed in this mode is positioned in a separate infrastructure zone within a network, as shown in Figure 18: Out-of-band mode deployment.This device is generally not in the path of the network, but it introduces itself within the network path whenever the network is under attack. It does this by performing route manipulation, using pre-configured dynamic routing protocol.

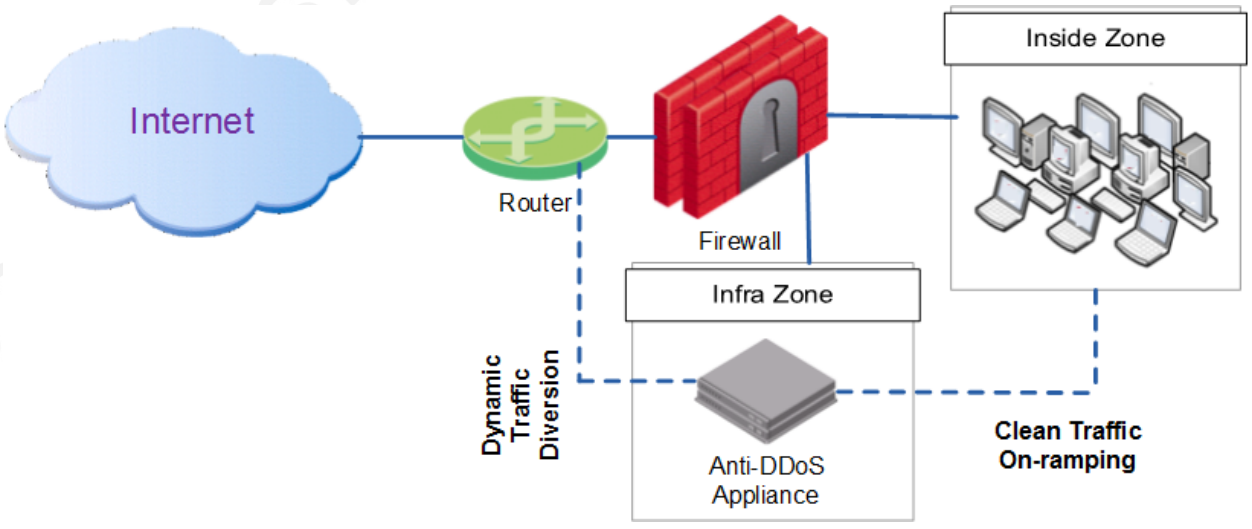

Figure 18: Out-of-band mode deployment

© 2015 The SANS Institute Author retains full rights.

These are generally purpose-built for DDoS eradication only, and they rely on other methods for attack discovery itself. These are generally deployed by network and security service providers in their cloud to provide DDoS eradication services to their clients.

5.2.3 Purpose-built appliance effectiveness

Though this approach of handling DDoS attack provides a good mix of both affordability and protection, this still has some disadvantages, as stated in Table 17: Effectiveness of various technologies under the Appendix.

5.2.4 Anti-DDoS appliance providers

Table 16: DDoS protection tools and services contains a list of Table 16: DDoS protection tools and services, as shown in the Appendix. It contains several options for purpose-built Anti-DDoS appliance based solutions that can be used for both discovery and defence.

5.3 DDoS eradication using RTBH

Remotely Triggered Black Hole (RTBH) is a capability that many ISPs provide to their clients. This service redirects the traffic destined to a particular network address range to a 'black hole,' effectively blocking traffic to that IP prefix without sending any notification back to the source.

5.3.1 Enterprise advertised RTBH route

It is common for ISPs to provide a specific BGP community for automated route black holing. This method of black holing gives control of traffic back to the organization and is available for large organizations that have their own IP address range and are running the BGP routing protocol with their ISP.

When an organization wants to use this service, it can advertise an additional, more specific route by attaching the above-stated RTBH community to it. Since this is a more specific route, it takes precedence over existing routes. In addition, since this route also has the RTBH community attached to it, routers will start dropping traffic just for that specific IP prefix, as advertised by the organization.

5.3.2 Enterprise initiated black holing

This method of black holing is useful for those small and medium organizations that do not hold their own range IP addresses, but depend on their ISP to provide their public IP address space.

© 2015 The SANS Institute Author retains full rights.

When they want traffic towards any of their public IP address prefixes to be black-holed, they communicate this to their ISP, and their job is done. Later they configure their network with necessary black-holing thus dropping traffic to a specific requested IP prefix.

5.3.3 RTBH effectiveness

Though RTBH does not eradicate a DDoS attack, it still has a role to play in DDoS defence strategy. It is important to understand its advantages and disadvantages as given in Table 17: Effectiveness of various technologies found in the Appendix.

5.4 Purpose-built anti-DDoS service

These Anti-DDoS services provided by various network and security service providers already discussed provide thorough protection against high volume, targeted and persistent attacks that are prevalent today.

These service providers are able to provide a greater degree of DDoS protection by deploying high-power and high capacity Anti-DDoS scrubbing centres throughout multiple countries and continents. Most of them have tens to hundreds of Gigabits of network and scrubbing capacity.

5.4.1 Traffic redirection using route injection

As soon as an Anti-DDoS service subscribed client faces a DDoS attack, their traffic towards targeted host(s) will be diverted to the nearest scrubbing centre for cleaning purposes. Post removal of malicious traffic redirect the clean traffic back to the client's network, effectively eradicating the DDoS attack for them, providing them with only clean traffic.

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

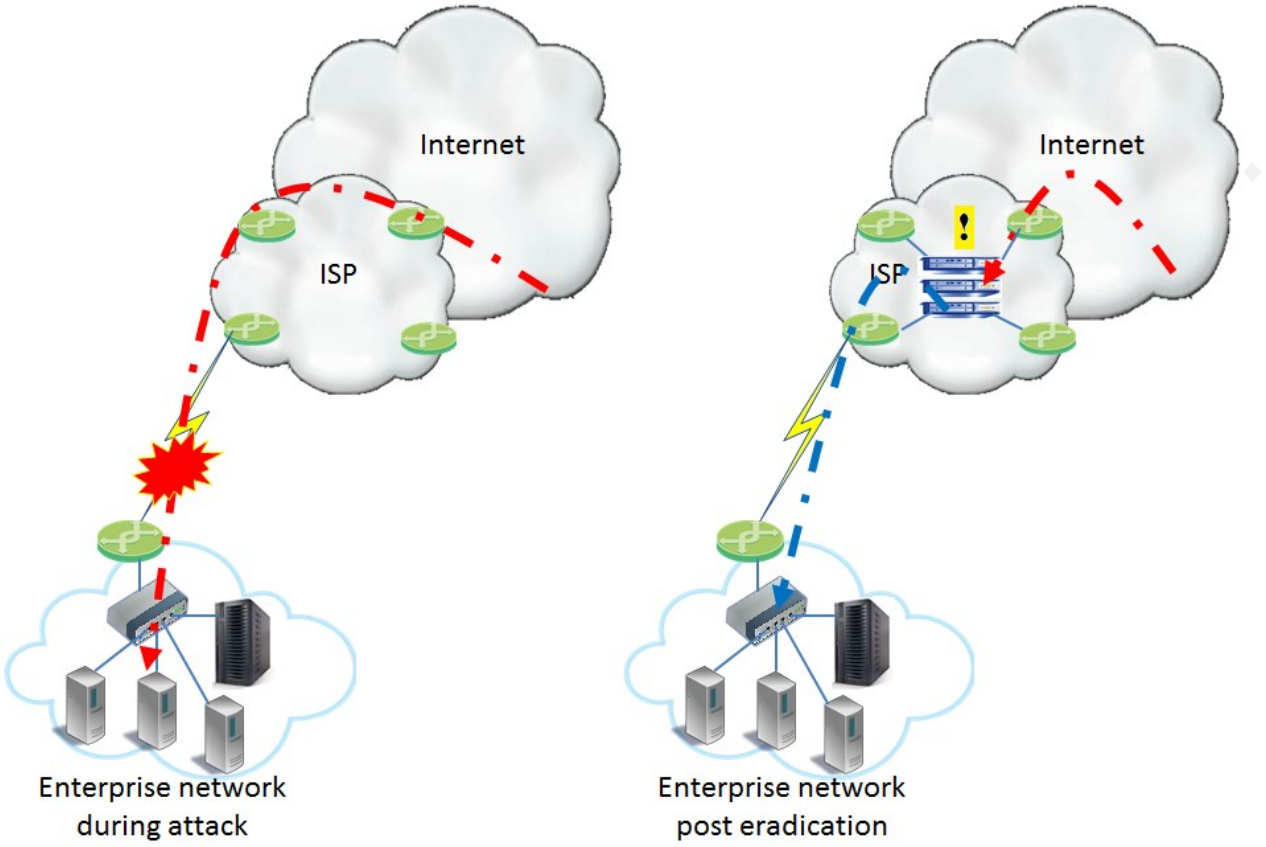

Figure 19: Traffic cleaning by Anti-DDoS service providers

5.4.2 Traffic redirection using DNS change

Another way that an organization can perform traffic redirection is by performing a DNS change. In this case, when its public facing resources are targeted by a DDoS attack, it changes its IP address for that of the target host in the DNS to one provided by their Anti-DDoS service provider. Once this DNS change is effective globally, the attack traffic that was earlier flowing directly to the target enterprise will now start flowing to their Anti-DDoS service providers, who then use their regional scrubbing centres, as shown in Figure 19: Traffic cleaning by Anti-DDoS service providers.

5.4.3 Purpose-built anti-DDoS service effectiveness

Table 16: DDoS protection tools and services given in the Appendix provides advantages and disadvantages of using purpose-built Anti-DDoS service.

© 2015 The SANS Institute Author retains full rights.

5.4.4 Purpose-built anti-DDoS service providers

Table 16: DDoS protection tools and services, found in the Appendix, contains several options for purpose-built Anti-DDoS service providers that can be used for both discovery and defence based services.

5.5 Hybrid DDoS defence solution

Much like the hybrid DDoS discovery solution described earlier, the hybrid DDoS defence solution provides best of both worlds. The solution combines in-premises purpose-built DDoS eradication based appliances that are deployed in in-band mode towards the edge of the network, along with a subscription for purpose-built Anti-DDoS service that performs traffic redirection through route injection.

This approach provides continuous protection from DDoS attacks with the help of in premises deployed, purpose-built Anti-DDoS appliance, and protection from high volume, targeted, and persistent attacks with the help of Anti-DDoS service from a service provider.

6 Developing incident management process

The DDoS protection appliances, services and solutions discussed thus far will only be effective in protecting an enterprise when it is tightly integrated with an enterprise security incident management practice. An ideal incident management process should follow the cycle shown in Figure 20: Incident Management Life cycle:

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

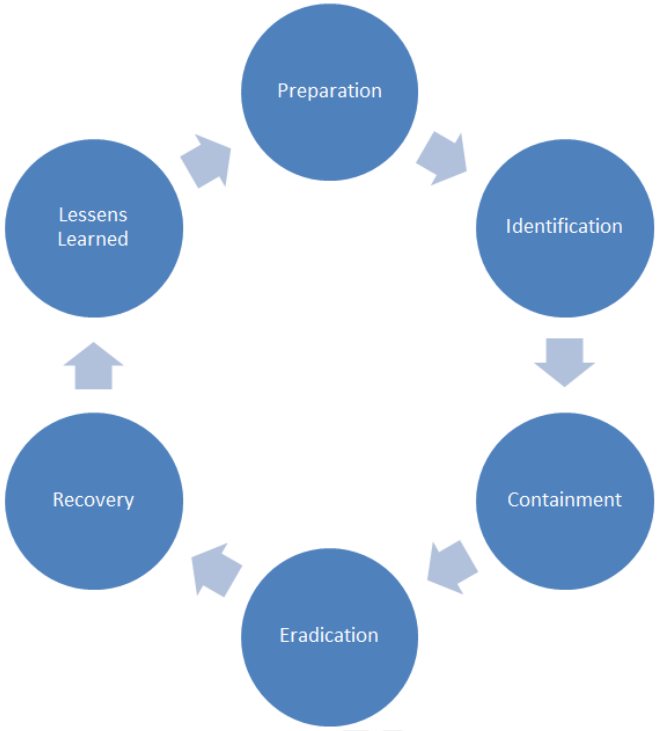

Figure 20: Incident Management Life cycle

6.1 Preparation phase

The goal of this phase is to prepare an organization to handle a DDoS attack and respond in a timely manner. This phase will use information that was gathered in Section 3.

6.1.1 Site Identification

To help identify the site that needs DDoS protection, the : Site inventory template that was prepared earlier in Section 3.3 can be used. A site would qualify for getting DDoS protection if it possesses at least the following two properties:

- A site that is hosting a public datacentre.
- The site has a criticality level of Mission Critical or Business Essential.

If there are multiple sites that qualify as per the above criteria, then initial protection should be provided for Mission Critical and Business Essential sites.

6.1.2 Protection requirement

For each identified site with category of "Mission critical" or "Business Essential," a superior degree of protection should be planned, this includes providing best possible DDoS discovery

© 2015 The SANS Institute Author retains full rights.

and eradication solution available in organization. For other site categories, the organization can choose to either provide a DDoS discovery service or provide DDoS defence service, or both. In order to get site-specific information and make informed decision, the site inventory list can be consulted.

6.1.3 DDoS discovery options

To discover an attack for a site, the discovery tools need not reside in the site itself, they can be located in remote sites. Regardless of the location of tools, an organization should make sure that necessary devices that needs to be monitored are configured to send feeds to the designated discovery tools for performing DDoS discovery. Depending on the available assets, one or more options discussed earlier for can be chosen. This could include DDoS protection service from third-party service provider or even a hybrid solution.

6.1.4 DDoS defence options

Much like DDoS discovery tools, these defence tools can also reside within the site that needs protection, or in another site, depending on network topology and routing architecture.

When choosing existing devices for performing DDoS defence, capabilities that were highlighted in Section 5.1, should be reviewed against defensive requirements. This is to make sure the proposed defence method is able to meet the site requirements. It should be noted that sites with high-security requirements might need purpose-built DDoS protection service from third-party providers or even hybrid solutions, depending on site requirements.

6.1.5 Documentation

After the necessary site protection mechanisms and requirements are finalized, along with DDoS discovery and defence, these same items should be updated in the various documents and templates. These include the site inventory, asset inventory, and even incident management process. The updated set of documents should include at least the following information:

- DDoS protection requirement for the site.
- Chosen detection method.
- Chosen defence method.
- Capabilities provided by the chosen detection method.
- Capabilities provided by the chosen defence method.

© 2015 The SANS Institute Author retains full rights.

- Triggering mechanism for defending a DDoS attack.
- Team responsible for managing DDoS protection.
- Escalation matrix for the team stated above.
- Persons to contact should the attackers demand a ransom.

The documentation helps gather updated security posture of a site and other related information, should the need arise in future.

6.2 Incident management process components

The incident management process is considered complete only when it addresses the following key requirements that help manage an incident throughout its lifecycle.

6.2.1 Incident report

The first thing that happens in an incident lifecycle is "incident occurrence," but it becomes actionable only after it has been reported and is known to Cyber Emergency Response Team (CERT) within the organization. There are two types of reporting.

Manual reporting:

In this form of incident reporting, the incident is noticed by an individual who can be either within or outside of the organization. Generally, it is noticed by an individual as "something-is-wrong" and is hindering his normal work, where an end user of some service is not able to access it, and thus reports the issue to the service desk. Thus, initial manual reporting of a DDoS incident to CERT is generally received from the service desk team.

This type of manual DDoS attack reporting is generally noticed in organizations that are least prepared to handle them; and even after reporting, they miss the bigger picture to see it as an attack.

Automated reporting:

This is done with the help of the DDoS discovery tools discussed earlier in this paper and is usually integrated into a corporate ticketing system. The CERT would generally have various monitoring consoles open that should quickly be able to discover a DDoS attack after it has exceeded a pre-set threshold.

© 2015 The SANS Institute Author retains full rights.

6.2.2 Incident registration

This is the process of making sure every reported incident is registered for future reference, usually with some kind of ticketing system. Most available DDoS discovery tools do support some form of automated ticketing system integration. This makes the incident registration task simpler. The discovery tool itself creates a ticket in the ticketing system and will be assigned to the CERT for action to be taken.

In case the incident was reported manually, it is the responsibility of the CERT member to make sure that every reported incident is registered in the ticketing system and followed up based on priority.

6.2.3 Incident analysis

This is an important part of any incident management process, as it creates a baseline in the system for a registered incident. Depending on the outcome of this phase, the future course of action for that incident is decided. Usually analysis includes one or more of the following tasks to be performed by a CERT member.

Incident scoping:

Many large organizations have multiple geographically distributed CERTs, and an incident can be discovered by more than one of those teams. In such a case, the CERT member should first identify and scope the incident. This is to decide if an incident falls within their scope of work and initiate the registration process after the appropriate scope is identified for the incident.

Incident verification:

This process will start the post registration of an incident, and helps segregate true incidents from a collection of false reports. Regardless of how the incident was reported, a CERT member should verify the incident details and take decision whether the reported incident was true. This can be a simple or involved task, depending on the complexity of the reported incident. However, it is important to verify an incident; as once it is identified as false, the incident will be closed and no further action taken on it.

© 2015 The SANS Institute Author retains full rights.

Incident pre-categorization:

This process involves gauging the impact of an attack with the information available at this stage, all while not considering the information for the targeted system. It is important to see the attack itself and gauge its impact in isolation regardless of what it is targeting. Depending on the organizational incident response program, the categorization can be High, Medium, Low, or any other agreed to categorization as per the organizational standard. In order to properly pre-categorize an incident one or more of following attack parameters can be considered:

- How many hosts are being targeted?
- What is the volume of attack?
- Impact on any end host that is running targeted service.

Incident prioritization:

This process involves combining incident pre-categorization along with endpoint information to conclude the criticality level of an incident. This process helps putting a particular incident in queue with other incidents for being addressed at a specific position, depending on the incident priority. A high priority incident should be addressed with top priority over other incidents.

Table 15, as found in the Appendix, can help a CERT member prioritize an incident based on its target asset and incident pre-categorization values.

6.2.4 Incident assignment

This step of incident management involves assigning an owner to a prioritized incident so that it can be worked upon and brought to a logical conclusion. There could be multiple ways for doing this; the first way is to just assign the incident to the handler who did the analysis of attack, or to some other handler, depending on his location or specialization. Once the incident is identified and assigned to a handler, he becomes the 'owner' of that incident. The owner can still work with or accept help from others depending on the complexity of the incident and specialization of the handler. However, ownership of the incident would remain with the original handler.

6.2.5 Incident resolution

This is the stage where the assigned incident handler works towards eradicating a DDoS attack. He would have multiple options for performing the task in hand, depending on options available

© 2015 The SANS Institute Author retains full rights.

for the site. Here the approach that an incident handler should take is to make sure he uses the appropriate tools for eradicating the attack and chooses appropriate configuration options in the tool(s) to make the best use of it.

More often than not, the resolution process is circular. In order to eradicate a DDoS attack, the incident handler goes through a set of tasks more than a few times. This helps him refine the eradication parameters at each pass, making the eradication of attack more effective than in the previous cycle.

Upon receiving attack details from the CERT, the network or security team performs feasibility checks to identify any immediate ill effects for the blocking of traffic at the perimeters of the targeted site(s). Once the feasibility checks are done and ill effecting parameters are eliminated, they configure necessary rules in perimeter devices of various sites to block similar attack from targeting those sites as well. Most likely, such rules are temporary and should remain active only for a few days or weeks, as systems involved in the attack are generally legitimate user machines that had been turned into a botnet. Hence keeping them blocked forever could result in potential business loss.

6.2.6 Incident closure

Once configured eradication is no longer dropping any traffic for at least several hours, and operations normal, then, it can be concluded that the attack is no longer active. Hence, the related incident ticket must be closed with a final update from handler. This update should include all possible eradication information including tools and parameters used to eradicate the attack.

6.2.7 Lessons learned

This is the final step in the incident management process, and it leads the organization to the path of continuous improvement. At this stage, the handler, along with others involved in the handling of the incident, prepare a set of lessons that they had learned while handling that particular incident, which is shared with a wider audience.

Preparation:

This activity must happen as soon as the incident is closed. The handler should document the highlights of the attack using some pre-defined format, stating items or issues that were unusual and discuss how they were managed. This ‘lessons learned’ document has to be prepared with

© 2015 The SANS Institute Author retains full rights.

the help of other handlers involved. In post preparation, the document should be reviewed and approved by fellow handlers.

Dissemination:

Once the lessons learned are documented and published, they should be discussed with wider audience of incident handlers as knowledge sharing session that are done on regular basis. It is not necessary for each incident to be discussed in that knowledge sharing session, but certainly complex and targeted ones should be discussed.

The meeting should be organized and conducted to meet the following goals of identifying:

- What was different about the attack?
- How differently the attack was eradicated?
- Benefits of the way in which attack was handled.
- Drawbacks of the way in which attack was handled.
- Points in the incident handling process, where a different strategy could have been used.

One of the key takeaways of this meeting could be the improvement of the overall security infrastructure within the organization. Some of the brainstorming ideas can be converted into rules and policies that can immediately be applied to the organization, thus making its security stronger, one-step at a time.

7 Conclusion

Distributed Denial of Service attacks are becoming inevitable in the present age, with even small handheld devices providing more power and capable of accessing large bandwidths that were once on available to large enterprises. With the consumerization of IT, the increasing availability of these high-power devices, awareness among owners to keep them safe is not increasing at the same pace. Hence, a large number of devices are vulnerable to various types of abuses. These devices are easily being converted into botnets and used to launch DDoS attacks against various public and private sector organizations, including national/state departments.

This high bandwidth and power provides increased power in attacker's hands, and thus the size and shape of DDoS attacks has been increasing day by day. To add to this, point and click tools

© 2015 The SANS Institute Author retains full rights.

to launch such attacks are freely available. In addition, since these attacks have a high possibility of creating an impact on some target, an economy has been built around it. Hence an ill-intended and cash rich organization can opt to rent a botnet to launch an attack by themselves, or avail DDoS Attack as a service where they pay for launching a DDoS attack on their behalf to a DDoS Attack service provider and get the attack launched, towards target organization.

While launching such attacks has become simpler and attack vectors became bigger, it has become complex and more resource consuming for an enterprise to defend itself. Enterprises cannot depend only on the traditional security devices and processes that they have been using. In order to defend against a DDoS attack, the enterprise should have the right infrastructure, skilled people, and tested processes. Thus, any organization that is serious about its IT security should be prepared to withstand a DDoS attack.

This paper has presented various ways in which organizations of different sizes and capabilities can prepare themselves to handle a DDoS attack. The paper provided initial preparation steps that are mandatory not just for withstanding a DDoS attack but for any IT security incident management program initiation. Later it provides various options that would help an organization to discover that they are under an active DDoS attack. Here the goal was to discover it within fifteen minutes of attack becoming lethal. Then similarly, different options were provided that will help an organization eradicate the attack post detection of same.

The paper also offers ways in which enterprises can reuse their existing infrastructure to achieve some level of protection from DDoS attack. It also gave ways in which protection can be strengthened by deploying purpose-built anti-DDoS appliances. Later it was clarified that discovering and eradicating a DDoS attack are two independent activities, and nothing that is deployed on enterprise premises will be able to provide adequate protection due to nature of DDoS attacks. That is because a powerful and targeted attack can choke organizations' last mile network connectivity, thus making everything on-premises ineffective. Therefore cloud based solutions were suggested, where service providers would be able to help the enterprise with DDoS eradication in one way or other, thus making sure last mile internet connectivity is not saturated.

Gaurang K. Pandya, Gaurang_cert@outlook.com

© 2015 The SANS Institute Author retains full rights.

However, it was later hinted that the most appropriate way to handle a DDoS attack was to have a custom-built hybrid model for both detection and eradication. This ensures that the enterprise gets best of both worlds – that is, quicker protection from on premises devices, and assured protection from large and persistent attacks with the help of security service providers.

Towards the end, this paper tied everything up by proposing changes to an existing Incident Management process and listing necessary information that should be collected by an enterprise that is willing to start their Anti-DDoS program. Finally, the paper also gives various steps that can be done during an Incident Management process and how they should be used and documented in order to achieve the best possible protection from DDoS attacks using available resources.

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

8 References

Akamai. (n.d.). *DDoS*. Retrieved from www.akamai.com: https://www.akamai.com/us/en/resources/protect-against-ddos-attacks.jsp

AntiDDOS, H. (n.d.). *Huawei AntiDDOS*. Retrieved from huawei.com: http://www.huawei.com/en/products/data-communication/network-security/Anti-DDoSSystem/index.htm

AT&T. (n.d.). *Denial of Service Protection* . Retrieved from att.com: http://www.business.att.com/enterprise/Service/network-security/threat-vulnerability-management/ddos-protection/

Beardmore, K. (2013, May 1). The Truth about DDoS Attacks: Part 1. *carbon60.com*, p. 1.

Bright, P. (2011, Apr 14). *DoJ, FBI set up command-and-control servers, take down botnet*. Retrieved from arstechnica.com: http://arstechnica.com/security/2011/04/doj-fbi-set-up-command-and-control-servers-take-down-botnet/

Bright, P. (2011, March 22). *How Operation b107 decapitated the Rustock botnet*. Retrieved from arstechnica.com: http://arstechnica.com/information-technology/2011/03/how-operation-b107-decapitated-the-rustock-botnet/

CERT NetSA Security Suite. (n.d.). Retrieved from SiLK: http://tools.netsa.cert.org/silk/index.html

Chen, A. (2012, January 19). *The Evil New Tactic Behind Anonymous' Massive Megaupload Revenge Attack*. Retrieved from gawker.com: http://gawker.com/5877707/the-evil-new-tactic-behind-anonymous-massive-revenge-attack

Communications, T. (n.d.). *TATA Communications DDoS*. Retrieved from www.tatacommunications.com: http://www.tatacommunications.com/sites/default/files/DDOS%20-%20Service%20Differentiators_0.pdf

Defense4All. (n.d.). *Defense4All*. Retrieved from opendaylight.org: https://wiki.opendaylight.org/view/Project_Proposals:Defense4All

© 2015 The SANS Institute Author retains full rights.

Fisher, D. (2015, July 31). *FBI Warns of Increase in DDoS Extortion Scams*. Retrieved from threatpost.com: https://threatpost.com/fbi-warns-of-increase-in-ddos-extortion-scams/114092

FortiDDoS. (n.d.). *FortiDDoS*. Retrieved from fortinet.com: http://www.fortinet.com/products/fortiddos/index.html

HP. (n.d.). *OPERATIONS MANAGER*. Retrieved from hp.com: http://www8.hp.com/us/en/software-solutions/operations-manager-infrastructure-monitoring/index.html?&jumpid=reg_r1002_usen_c-001_title_r0001HP

IBM. (n.d.). *IBM Qradar*. Retrieved from ibm.com: http://www-03.ibm.com/software/products/en/qradar-siem/

IBM. (n.d.). *IBM Tivoli Datasheet.* Retrieved from IBM.COM: http://www-05.ibm.com/za/office/pdf/Tivoli_Monitoring.pdf

IBM. (n.d.). *IBM Tivoli Monitoring*. Retrieved from ibm.com: http://www-01.ibm.com/support/knowledgecenter/SSDKXQ_6.3.1/com.ibm.itm.doc_6.3fp2/itm63fp2_qsg_en.htm

Lee, M. (2012, January 5). *ANZ E*Trade outage actually DDoS attack*. Retrieved from ZDNet: http://www.zdnet.com/article/anz-etrade-outage-actually-ddos-attack/#!

ManageEngine. (n.d.). Retrieved from Netflow Analyzer: https://www.manageengine.com/products/netflow/

MozDef. (n.d.). *MozDef*. Retrieved from github.com: https://github.com/jeffbryner/MozDef

Nagios. (n.d.). *Nagios*. Retrieved from nagios.org: http://www.nagios.org

Nazario, J. (2008, August 12). *Georgia DDoS Attacks – A Quick Summary of Observations*. Retrieved from arbornetworks.com: https://asert.arbornetworks.com/georgia-ddos-attacks-a-quick-summary-of-observations/

Netflow Auditor. (n.d.). Retrieved from Netflow Auditor: http://www.netflowauditor.com/netflow_anomaly_detection_tools.php

Gaurang K. Pandya, Gaurang_cert@outlook.com

© 2015 The SANS Institute Author retains full rights.

NfSen. (n.d.). Retrieved from http://nfsen.sourceforge.net/

NitroSecurity, M. (n.d.). *Mcafee NitroSecurity*. Retrieved from mcafee.com: http://www.mcafee.com/us/about/mcafee-nitrosecurity.aspx

OpenNMS. (n.d.). *OpenNMS*. Retrieved from OpenNMS: http://www.OpenNMS.org

OSSIM. (n.d.). *OSSIM*. Retrieved from sourceforge.net: http://sourceforge.net/projects/os-sim/

Peters, S. (2014, August 26). *Sony, XBox Victims Of DDoS, Hacktivist Threats*. Retrieved from darkreading.com: http://www.darkreading.com/sony-xbox-victims-of-ddos-hacktivist-threats/d/d-id/1306656

Protector, C. D. (n.d.). *Checkpoint DDoS Protector*. Retrieved from checkpoint.com: http://www.checkpoint.com/products/ddos-protector/index.html

Radware. (n.d.). *Radware DefensePro*. Retrieved from Radware.com: http://www.radware.com/Products/DefensePro/

Reese, B. (2008, November 18). Cisco technology partner: DDoS attack sizes may be on pace to approach 100 gigabits by this time next year. *networkworld.com*, p. 1.

Sanders, A. E. (2011, November 23). *FBI Denver Cyber Squad Advises Citizens to be Aware of a New Phishing Campaign* . Retrieved from fbi.gov: https://www.fbi.gov/denver/press-releases/2011/fbi-denver-cyber-squad-advises-citizens-to-be-aware-of-a-new-phishing-campaign

SIEM. (n.d.). *HP SIEM*. Retrieved from HP.COM: http://www8.hp.com/us/en/software-solutions/siem-security-information-event-management/index.html

TDS, C. S. (n.d.). *Corero SmartWall TDS*. Retrieved from corero.com: http://www.corero.com/products/Corero_SmartWall_Threat_Defense_System.html

Verisign. (n.d.). *DDoS Protection*. Retrieved from verisign.com: http://www.verisign.com/en_US/security-services/ddos-protection/index.xhtml

Wocteam. (2009, September 1). *Application Criticality.* Retrieved from technet.com: http://blogs.technet.com/b/itbizval/archive/2009/09/01/application-criticality.aspx

Gaurang K. Pandya, Gaurang_cert@outlook.com

© 2015 The SANS Institute Author retains full rights.

Wood, B. (2014, August 7). Analyze This: Denial of Service Attacks. *americanis.net*, p. 1.

© 2015 SANS Institute, Author retains full rights.

Gaurang K. Pandya, Gaurang_cert@outlook.com

© 2015 The SANS Institute Author retains full rights.

9 Appendix

Table 1: Network bandwidth consuming attacks

Attack	Attack Vector	Resource targeted
ICMP Flood or Smurf Attack	Layer 3 Protocol	Network bandwidth
UDP Flood	Layer 4 Protocol	Network bandwidth
LOIC	Layer 4 Protocol	Network bandwidth

Table 2: Memory consuming attacks

Attack	Attack Vector	Resource targeted
Syn Flood	Layer 4 Protocol	Memory utilization
Slowloris attack	Layer 7 Protocol	Memory utilization
PyLoris attack	Layer 7 Protocol	Memory utilization
HOIC	Layer 7 Protocol	Memory utilization

Table 3: CPU consuming attacks

Attack	Attack Vector	Resource targeted
Christmas tree	Layer 4 Protocol	CPU utilization
TTL Expiry	Layer 3 Protocol	CPU utilization

© 2015 The SANS Institute Author retains full rights.

Table 4: Asset inventory template

<HostName/FQDN>

Physical Aspects

Asset id			
Location		**Serial no.**	
Manufacturer		**Install Date**	
Model		**Asset Type**	Server/Appliance
Memory		**CPU/ Cores/ Speed**	
Hard disk count/ Capacity of each / Type		**NIC count / Type /**	
Available/Used RAM slots		**Available/Used CPU Slots**	
Available/Used Hard disk slots		**Available/Used PCI slots**	
NIC to Switch connections		**Switch connected to**	
Power to Socket connections		**Power socket/ UPS connected to**	
Is Virtual	Yes/No	**If virtual, Host asset id**	

Logical Aspects

Operating System with Flavor		**Host Name**	
Service pack or Update No.		**Interface Name/IP Address/ MAC Address**	
Bit Architecture		**Asset Criticality**	Mission Critical/ Business Essential/ Business Core/ Business Supporting Source: (Wocteam, 2009)
Asset Purpose		**Scheduled Down time and Impact**	
Asset Status	In use/ Inactive/ Retired	**Translated Addresses**	
Is public facing	Yes/No	**Is partner facing**	Yes/No

© 2015 The SANS Institute Author retains full rights.

Contact Information

Business owner - Primary		**BO Primary Contact info and contact hours**	
Business owner - Backup		**BO Backup Contact info and contact hours**	
Technical Owner - Primary		**TO Primary Contact info and contact hours**	
Technical Owner - Backup		**TO Backup Contact info and contact hours**	

Monitoring Information

Services Monitored		**NMS collector**	
Logs forwarded		**Log collector**	
Flow exported	Yes/No	**Flow collector**	
Monitored from Outside	Yes/No	**Services monitored from Outside**	

BCP/DR Information

Role	Primary/Backup	**Redundant for**	
Data Sync type	Real time/Batch	**Data sync frequency**	
Backup configured	Yes/No	**Directories/ Items Backed up**	
Backup Schedule		**Test restore schedule**	
SAN/NAS connectivity	Yes/No	**SAN/NAS connected to**	
Drives/ Directories used of SAN/NAS			
Dependent of this asset		**This asset depending on**	

© 2015 The SANS Institute Author retains full rights.

Other important information

Table 5: Network Circuit inventory template

<Circuit Name>

Circuit Information

Circuit id			
Location – Point A		**Location – Point B**	
Provider		**Circuit Type**	Internet/ MPLS/ Point-to-Point
Install Date		**Renewal Date**	
Limitations	Bandwidth: Traffic Cap:	**Circuit Features**	With protection/ with redundancy etc.
Cable provider/ Route Used		**Physical Media**	
Provider Point of Contact (POC)		**Provider Escalation POC**	
Provider POC contact hours		**Provider Escalation POC contact hours**	
Provider SLA		**Provider Capabilities**	*<VAS that provider can provide currently but is not subscribed for>*

BCP/DR Information

Is backup available	Yes/No	**Backup Type**	Active/Active or Active/Standby
Primary of		**Backup of**	

© 2015 The SANS Institute Author retains full rights.

Point A L1 Termination		**Point B L1 Termination**	
Point A L2/3 Termination and Type - Primary	Terminating Asset id: Asset Type: Firewall/Router/Switch	**Point B L2/3 Termination and Type- Primary**	Terminating Asset id: Asset Type: Firewall/Router/Switch
Point A L2/3 Termination and Type - Backup	Terminating Asset id: Asset Type: Firewall/Router/Switch	**Point B L2/3 Termination and Type- Backup**	Terminating Asset id: Asset Type: Firewall/Router/Switch

Usage information

Expected Data	%	**Expected Data**	<absolute>
Expected Voice	%	**Expected Voice**	<absolute>
Expected Mission critical traffic	%	**Expected Mission critical traffic**	<absolute>
QOS Implemented	Yes/No	**QOS Details**	

Network Diagram/Other important information

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

Table 6: VPN inventory template

<Site to Site VPN/GRE Tunnel Name>

Connection Information

Local GW IP/Host Name	Primary: Backup:	**Remote GW IP/Host Name**	Primary: Backup:
Local Protected subnets		**Remote Protected Subnets**	
Is traffic filtered	Yes/No	**Filtering ACL Name/Number**	
This is depending on		**Services that depends on this**	
Type	GRE/IPSec		

IPSec VPN Negotiation Information

IKE Version	½	**Phase 1 encryption**	
Phase 1 authentication		**Phase 1 hashing algorithm**	
Phase 1 DH group		**PF secrecy**	
Phase 1 Lifetime		**Phase 2 encryption**	
Phase 2 hashing algorithm		**Phase 2 lifetime**	
Phase 2 group			

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

Table 7: Site inventory template

<Site Name>

Physical Information

Site Code		**Site Address**	
Seating capacity		**Occupancy**	
Multi-tenanted	Yes/No	**Facility Management Contact info**	
Hosting Internal Datacenter	Yes/No	**Hosting Public Datacenter**	Yes/No
Operational Functions		**Operating 24x7**	Yes/No
Site Criticality	Mission Critical/ Business Essential/ Business Core/ Business Supporting		

Connectivity Information

Physical Circuits	<Circuit id1 .. n>	**Virtual Circuits**	<Circuit id1 .. n>
Incoming Circuits	<Circuit id1 .. n>	**Outgoing Circuits**	<Circuit id1 .. n>
Internet connected	Yes/No	**Internet used for**	Just VPN/Other data traffic/Both

BCP/DR Information

Site Redundancy available	Yes/No	**Redundancy Type**	Active/Active or Active/Standby
This site	Primary/Backup	**Other site**	Primary/backup
Other site – Site code		**Site replication strategy**	Real-time/ Batch/ None

Other important information

© 2015 The SANS Institute Author retains full rights.

Table 8: Key teams list and their role

Team	Role
Cyber Emergency Response Team (CERT)	This is the Emergency response team that will perform Incident Management.
IT Security	This is core team that gets involved during an IT security incident management.
Network	As DDoS is network based attack and depends on network for discovery and eradication; getting this team involved in a DDoS incident management process is of prime importance.
Server Management	As DDoS attacks target servers or their availability, having this team involved is mandatory. A representative from each server type is required, for example Windows, Linux/Unix, Mainframe etc.
Business Continuity and Disaster Management	This team will help identify alternative methods of bringing up critical services from an alternative location, should the primary location get hit by DDoS attack.
Business Management	Members of this team will help analyse impact of an attack and provide valuable inputs during containment and eradication phase of incident management lifecycle.
Legal advisory	Individuals from this team will help in following situations. • Identify compliance requirement for incident management program. • Help in situations where a ransom demand is made during active DDoS attack • Identify the legal liability of an organization during a DDoS attack. • Identity legal options that an organization has that will help eradicate an attack.
Corporate Communications and Public Relations	Members of this team will help manage internal and external communications regarding an attack, and help maintain organization's public image.

Table 9: Contact information collection template

Contact Person	Team	Primary /Secondary	Contact Information	Contact Hours

© 2015 The SANS Institute Author retains full rights.

Table 10: Security policy documents

Required Information	Policy Document
In event of DDoS attack, which services should be brought up from disaster recovery site, and what service level would be applicable for the site?	Disaster recovery policy
What are the various response strategies that can be used during a DDoS attack?	Security response Policy
Can users work from home during emergency as a contingency plan for primary site going down? If so what is permitted and what not?	Remote access policy
How should network devices be configured to protect themselves as well as the network behind them?	• Router and switch security policy • Communication equipment security policy
In order to help early detection of an attack, what information can be logged, where, and how can that information be used?	• Information logging policy • Server security policy • Router and switch security policy • Server audit policy
Minimum security controls that a server should be configured with when working in a particular security cleared zone.	• Server security policy • Information logging policy
How should the servers and network devices be monitored for uptime and health checks? And how does alerting happen for health issues?	• Server security policy • Router and switch security policy
How should management access to servers and network devices be protected to have minimum impact during an attack?	• Server security policy • Router and switch security policy
How should patch deployment be handled for servers and network devices?	• Server security policy • Router and switch security policy
How should backup be configured and how frequently restoration testing done?	• Disaster recovery policy • Server security policy • Router and switch security policy
How should connectivity with clients and third parties be secured?	Extranet security policy

© 2015 The SANS Institute Author retains full rights.

Table 11: Compliance matrix

Regulation	Country	Industry	Short Description
SOX	United States	Various	Regulates auditing and accounting practices for public corporate organizations
PCI DSS	N/A	Various	Sets standards for organizations that handle credit cards and its data from major cards schemes including VISA, MarsterCard, American Express, Discover and JCB.
GLBA	United States	BFSI	Provides framework for BFSI organizations to enhance competition in the industry.
HIPAA	United States	Health	Mandates standard-based implementation of IT security controls for creation, storage, and transmission of electronically protected health information.
HITECH	United States	Health	Relates directly with HIPAA and requires healthcare organizations to apply "meaningful use" of security technology for data protection.
FISMA	United States	US Federal	Mandates every US federal agency to develop, document and implement agency-wide Information security practice.
EU Data Retention Directive	European Union	Telecommunication	Mandates retention of citizen's telecommunication data retention from minimum of 6 to maximum of 24 months.
BASEL II and III	G-10 Nations	Banking	Provides recommendations to banks for holding capital in order to guard against various financial and operational risks
NERC/CIP	North American Region	Various	Mandates protection of critical infrastructure.
FERPA	United States	Education	Mandates all US schools to protect their students' education records.
SSAE 16	United States	Service Organization	Sets series of accounting standards to measure control of financial information.
EU Data Protection Directive	European Union	Various	Mandates protection of individuals with regard to protection of personal data.

© 2015 The SANS Institute Author retains full rights.

Table 12: NMS Checks

Resource Monitoring Checks	
Memory utilization	Count of open network sockets for a specific service
Partition wise disk utilization	Critical service up-down
Disk I/O utilization	Service up-down for all services that depends on Critical service
Network interface up-down	Service up-down for all services that critical service depends on
Network utilization per interface	Remote management and monitoring service up-down (ex: rdp, ssh, snmp etc.,)
Errors and drops in every network interface	Total count of arp entries in cache
Total count of open network sockets or connections	Total count of entries in routing table
Total count of half-open network sockets or connections	Total count of entries in routing per VRF

Table 13: Flow exporting vendors

Vendor	Network Flow exporter
Cisco	NetFlow
Juniper Networks	JFlow
3Com/HP	NetStream
Huawei Technologies	NetStream
Alcatel-Lucent	CFlowd
Ericsson	Rflow
Citrix	AppFlow

Table 14: Site protection identifying table

<Site Name>			
	Using appliance deployed at the site	**Using appliance deployed in other site**	**Using cloud based service**
Discovery using general methods			
Discovery using purpose-built appliances			
Defense using general security appliances			
Defense using purpose-built appliances			

© 2015 The SANS Institute Author retains full rights.

Table 15: Incident prioritization table

Target Asset Category / Incident pre-category	Mission Critical	Business Essential	Business Core	Business Supporting
High	High	High	High	Medium
Medium	Medium	Medium	Medium	Low
Low	Low	Low	Low	Low

Table 16: DDoS protection tools and services

Technology	Commercial Tool/ Service Providers	Free/Opensource Tools	Comments
NMS Tool	HP Operations Manager (HP, n.d.) IBM Tivoli Monitoring (IBM, IBM Tivoli Monitoring, n.d.)	Nagios (Nagios, n.d.) OpenNMS (OpenNMS, n.d.)	• Features discussed in section are available in Nagios, OpenNMS. • IBM Tivoli Monitoring provides "dynamic thresholding" which can address one of challenges of NMS system (IBM).
Flow Monitoring	nfsen (NfSen, n.d.) SiLK (CERT NetSA Security Suite, n.d.)	NetFlow Auditor (Netflow Auditor, n.d.) NetFlow Analyzer (ManageEngine, n.d.)	
SIEM Tool	HP Arcsight (SIEM, n.d.), McAfee Nitro (NitroSecurity, n.d.), IBM QRadar (IBM, IBM Qradar, n.d.)	OSSIM (OSSIM, n.d.), Mozdef (MozDef, n.d.)	

© 2015 The SANS Institute Author retains full rights.

Anti-DDoS Appliances	RadwareDefensePro, (Radware, n.d.) Checkpoint DDoS Protector (Protector, n.d.), FortinetFortiDDoS (FortiDDoS, n.d.), HuaweiAntiDDOS (AntiDDOS, n.d.), CoreroSmartWall TDS (TDS, n.d.)	Defence4All (Defense4All, n.d.) from Radware	Defence4All is capable of performing only DDoS discovery and traffic redirection for further action by other solutions. Defence4All is SDN based project, and works with OpenDaylight SDN project
Anti-DDoS Services	• **Network Providers with DDoS Solution:** TATA Communications (Communications, n.d.), AT&T (AT&T, n.d.) • **Security Service providers:** Akamai (Akamai, n.d.) Verisign (Verisign, n.d.)		

Table 17: Effectiveness of various technologies

Technology	Advantages	Disadvantages
Network Management Service	• Cost effective • Efficient monitoring • SNMP Traps provide quick discovery of event	• Ineffective during peak season as thresholds are static • Works by polling devices, hence discovery of attack can take time
Flow Monitoring	• Cost effective • Provides early warning • Less resource intensive	• Could produce incorrect results if interface for collecting flows is not chosen wisely • Depending on tool used, the thresholds can be static.
Security Information and Event Management	• Does correlation with other feeds and avoids false positives • Provides more actionable intelligence • Complements other security tools and works with them • Provides near real-time	• Effectiveness depends heavily on rules built in system • Requires more effort in setting up right monitoring for DDoS discovery than any other tool • Might not be able to take feeds from all necessary devices.

© 2015 The SANS Institute Author retains full rights.

	alerting	
Remotely Triggered black holing	• Generally provided free of cost by network providers • Most effective when target is non-existent or dark IP address range.	• Unless BGP based solution is used, the triggering can take time. • If not used carefully, can complete attack for malicious user.
Anti-DDoS appliance	• Easier to deploy and manage • Provides complete protection using various countermeasures • Provides continuous protection as this can be deployed in-line to traffic path • Protects from low and slow as well as SSL based attacks	• Generally costlier than other solutions • Requires skilled people to manage the solution • Deployment can be complex • Cannot defend against high-volume, and persistent attacks
Anti-DDoS service	• Easy to avail protection if network providers provide this service as well • Protects an organization from high-volume and persistent attacks • Does not require any footprint in enterprise, as it can be completely cloud based	• Unless all the links are protected, the entire infrastructure is not protected • Initiating protection could introduce some delay, which could result in service outage • Cannot protect effectively from low and slow and SSL based attacks.

© 2015 SANS

© 2015 The SANS Institute Author retains full rights.