



Big IT Networks
CYBER SECURITY NEED ENDS HERE

2022

DDoS Attack Remediation Plan



Shahab Al Yamin Chawdhury
CISO @ BIG IT Networks
Saturday, May 4th, 2022

Document control

Code:	ISMS/IS/PLAN/DDoS-1
Version:	3.0
Date of version:	6 th May 2023
Prepared for:	A partial fulfilment of ISO/IEC-27001, ORM, ERM and BCP
Created by:	SHAHAB AL YAMIN CHAWDHURY
Approved by:	
Confidentiality level:	HIGH BUSINESS IMPACT (HBI)

Change history

Date	Version	Created by	Description of change
6th May 2023	3.0	Shahab Al Yamin Chawdhury	Responsibility matrix, jurisdiction matrix added
4th May 2022	2.0	Shahab Al Yamin Chawdhury	All financials and frameworks updated
2018-03-27	1.0	Shahab Al Yamin Chawdhury	Basic document outline

Signatories

Prepared By	Checked By	Agreed By	Approved By
Signature	Signature	Signature	Signature
Name:	Name:	Name:	Name:
Designation:	Designation:	Designation:	Designation:
Date:	Date:	Date:	Date:

Distribution List

Designation	Copy	Date	Remarks
Managing Director			
CxO's encrypted soft copy			
Department encrypted Copy			
QMS Copy			
Copy Protection			Enabled

Contents

What is a distributed denial of service (DDoS) attack?.....	4
Difference between DOS and DDoS	4
3 common types of DDoS attacks:	4
Volumetric	4
Protocol	5
Application	5
Who are the potential victims?	5
Work mechanism.....	5
Common types of network flooding:.....	6
Top 10 Dangerous DNS Attack Types.....	6
Example of DDoS attack.....	7
Signs of a DDoS attack	7
Balance the Load	7
Solutions: Monitoring is Key to Preventing DDoS Attacks	8
Full DNS Audit Log History: Query Logging and Advanced Analytics	8
10 Ways to Prevent a DDoS Attack	8
1. Know our network’s traffic	8
2. Create a Denial of Service Response Plan	8
3. Make our network resilient	9
4. Practice good cyber hygiene	9
5. Scale up our bandwidth	9
6. Take advantage of anti-DDoS hardware and software	9
7. Move to the cloud	9
8. Know the symptoms of an attack	9
9. Outsource our DDoS protection	10
10. Monitor for unusual activity	10
Summary	10
Team Readiness Requirements	11
Who will do What? What’s the Requirements? Skills Mapping? RACI? Documentations?	13
Responsibility Matrix	13
Decision Tree	16
Solution	16
Team Enablement	16

Team:	17
Program Management	17
Annexure - A (Top DDoS Service Provider).....	18
ANNEXURE - B (Visibility Requirements).....	19
ATTACK POSSIBILITIES BY OSI LAYER.....	20
ATTACK POSSIBILITIES BY OSI LAYER (IOC).....	21
POSSIBLE DDOS TRAFFIC TYPES	22
GLOSSARY	23
MITIGATING LARGE SCALE DoS/DDoS ATTACKS.....	24
REFERENCES.....	24
ANNEUXURE - C (Mitigation Plan)	25
ANNEUXURE - D (Configuration Benchmark)	27
Device Benchmark for CISCO Routers & Switches	27
Device Benchmark: List of Controls.....	28
IG 1 Mapped Recommendations	31
IG 2 Mapped Recommendations	33
IG 3 Mapped Recommendations	35
Approvals for the next level:	39
Validity and Document Management.....	39
Violations.....	40
Approval and Ownership.....	40

What is a distributed denial of service (DDoS) attack?

A distributed denial-of-service (DDoS) attack is an attempt to disrupt the traffic of a targeted server, service, or network by overwhelming it with a flood of Internet traffic. By sending too many requests for information to a server, site, or network, a DDoS can effectively shut down a server – leaving it vulnerable and disrupting the **normal business operations** of an organization.

Difference between DOS and DDoS

DOS	DDOS
DOS Stands for Denial of service attack.	DDOS Stands for Distributed Denial of service attack.
In Dos attack single system targets the victim system.	In DDoS multiple systems attacks the victims system..
Victim PC is loaded from the packet of data sent from a single location.	Victim PC is loaded from the packet of data sent from Multiple location.
Dos attack is slower as compared to DDoS.	DDoS attack is faster than Dos Attack.
Can be blocked easily as only one system is used.	It is difficult to block this attack as multiple devices are sending packets and attacking from multiple locations.
In DOS Attack only single device is used with DOS Attack tools.	In DDoS attack, The volumeBots are used to attack at the same time.
DOS Attacks are Easy to trace.	DDOS Attacks are Difficult to trace.
Volume of traffic in the Dos attack is less as compared to DDos.	DDoS attacks allow the attacker to send massive volumes of traffic to the victim network.
Types of DOS Attacks are: 1. Buffer overflow attacks 2. Ping of Death or ICMP flood 3. Teardrop Attack 4. Flooding Attack	Types of DDOS Attacks are: 1. Volumetric Attacks 2. Fragmentation Attacks 3. Application Layer Attacks 4. Protocol Attack.

3 common types of DDoS attacks:

Volumetric

The most common type of DDoS attack, volumetric attacks flood a machine's or a network's bandwidth with false/fake data requests on every available port. This overwhelms the network, leaving it unable to accept its regular traffic. There are subcategories of volumetric attacks as well. The most common type of volumetric attack is a UDP (User Datagram Protocol) flood, which is often used to send forged UDP packets with false addresses – like the IP address of the victim – to servers for UDP-based applications, generating a flood of reply traffic. ICMP (Internet Control Message Protocol) floods, on the other hand, sends false error requests to a target, tying it up so that it can't respond to normal ones. It will get so busy dropping the illegal ones, the legal ones won't be having any time look after

Types of DDoS	
Volumetric	<ul style="list-style-type: none"> • UDP flood • DNS amplification • NTP amplification
Protocol	<ul style="list-style-type: none"> • SYN flood • ICMP flood • UDP fragments • DNS water-torture
Application	<ul style="list-style-type: none"> • GET/POST flood • Slowloris • STOMP flood • Apache killer

Protocol

Protocol attacks target the protocols used in transferring data to crash a system. One of the most common is a SYN flood, which attacks the process of making a TCP/IP connection by sending a flood of SYN packets asking the victim to synchronize instead of acknowledging a connection, tying up the system while it waits for a connection that never happens. SYN floods are like telling a knock-knock joke that never ends: knock knock, who's there, knock knock, who's there, knock knock...

Application

Similar to protocol attacks, **application attacks** target weaknesses in an application. These attacks focus primarily on direct web traffic and can be hard to catch, because a machine may think it's dealing with nothing more than a particularly high level of Internet traffic.

Who are the potential victims?

DDoS can destroy sites of any scale, from ordinary blogs to major corporations, banks, and other government institutions.

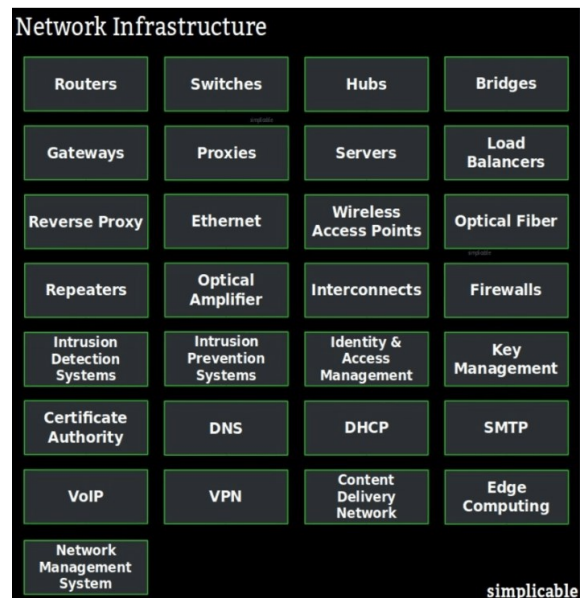
Most often, these types of sites and servers suffer from DDoS attacks:

1. large companies and government agencies
2. financial institutions (banks, management companies)
3. coupon services
4. medical institution
5. payment systems
6. media and information aggregators
7. online stores and e-commerce businesses
8. online games and gaming services
9. cryptocurrency exchanges

Largest growth dynamics in this direction are cyberattacks to disrupt the online sales systems of large stores or shopping centers.

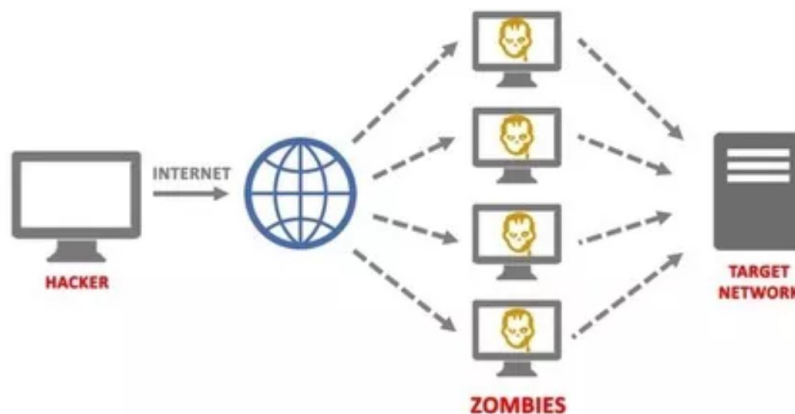
Work mechanism

All web servers have their own limits on the number of requests they can process simultaneously. In addition, there is a limit on the bandwidth of the channel connecting the network and the server. To overwhelm these restrictions, malicious hackers create a computer network with malicious software, called a "botnet" or "zombie network."



DDoS attack

The zombie network



Common types of network flooding:

1. HTTP – A mass of normal or encrypted HTTP messages is sent to the attacked server, clogging communication nodes.
2. ICMP – The attacker's botnet overloads the victim's host machine with service requests, to which it is required to provide echo responses.
3. SYN – These attacks affect one of the basic mechanisms of the TCP Protocol, known as the "triple handshake" principle (the "request-response" algorithm: SYN packet - SYN-ACK packet - ACK packet).
4. UDP – Random ports of the victim's host machine are flooded with UDP packets, the responses to which overload network resources. A type of UDP flood directed to the DNS server is called a "DNS flood."
5. MAC – Targets are network hardware whose ports are clogged with streams of "empty" packets with different MAC addresses.

In most cases, service attacks are more robust to disrupt a networks operation, but the absence of associated service monitoring and SOC's operations like the following will give we no edge but to identify individual port or service transmissions, and drop them manually, this is a very tiresome and old fashioned network management process.

Top 10 Dangerous DNS Attack Types

1. DNS Cache Poisoning Attack
2. Distributed Reflection Denial of Service (DRDoS)
3. DNS Hijacking
4. Phantom Domain Attack
5. TCP SYN Floods
6. Random Subdomain Attack
7. DNS Tunneling
8. DNS Flood Attack
9. Domain Hijacking
10. Botnet-based Attacks

Example of DDoS attack

To create a botnet, cybercriminals distribute a “Trojan” virus via e-mail, social networks, or websites. Computers that are part of the botnet do not have a physical connection to each other. They are united only by “serving” the goals of the host hacker.

A hacker sends commands to the “infected” zombie computers during a DDoS attack, and they begin to attack. The botnet generates a huge amount of traffic that can overload any system. The main objects for DDoS are usually the server’s bandwidth, DNS server, and the internet connection itself.

Another way, a hacker simply sends mail bomb, millions of packets to a destination IP or to a block of IP’s.

Signs of a DDoS attack

When these malicious actions achieve their goal, we can immediately determine this by failures in the server or the hosted resource. But there are several indirect signs that we can detect about a DDoS attack at the very beginning.

1. Server software and OS start to fail frequently and clearly – hang, incorrectly shut down, and so on.
2. A sharply increased load on the server’s hardware capacity, which differs from the average daily indicators.
3. A rapid increase in incoming traffic on one or more ports.
4. Multiple duplicated client actions of the same type on the same resource (going to the site, uploading a file).
5. When analyzing logs (of user actions) of the server, firewall, or network devices, many requests of the same type from different sources to the same port or service were detected. We should be especially wary if the audience for requests differs sharply from the target audience for the site or service.

Balance the Load

Now, let’s take a look at the difference a managed DNS provider like DNS Made Easy, which has an IP Anycast+ network, makes when faced with a Volumetric attack.

1. The attacker floods the target with malicious query traffic, which drowns out the good traffic.
2. In DNS services, malicious traffic is cleaned via a proprietary scrubbing algorithm before it is sent throughout the network.
3. Traffic is dispersed to many Points of Presence (PoPs) to distribute and balance the load.
4. Each PoP then filters traffic throughout comprehensive system of firewalls and intrusion detection services.
5. Once filtered, clean traffic is pushed to the nameservers, which direct and answer query traffic. In contrast to many of our peers who run on a handful of virtual private servers (VPSs) per PoP, with IS instructed hardening-model. This is why our network has been able to handle some of the largest DDoS attacks to ever hit authoritative nameservers with minimum to no ill effect.

Problem Focus or Solutions Focus?



Problem Focus

- What’s wrong?
- What needs fixing?
- Blame and control
- Causes in the past
- The expert knows best
- Deficits and weaknesses
- Complication
- Definitions

Solutions Focus

- What’s wanted
- What’s working
- Progress
- Influence
- Collaboration
- Resources and strengths
- Simplicity
- Actions

Quick Fact: The DNS network is also engineered to protect against many other attacks including TCP State Exhaustion attacks (protocol abuse), Reflection/amplification attacks, and Application attacks (DNS).

Solutions: Monitoring is Key to Preventing DDoS Attacks

Most companies put themselves in a defensive position when it comes to DDoS threats, which ultimately prolongs the attack. With the right tools, however, we can put our organization in an offensive position that allows us to identify threats and stop them before they have a chance to cause damage to our domain.

Advanced DNS Monitoring and Protection: Real-time Anomaly Detection (RTTAD)

Real-time Traffic Anomaly Detection uses machine learning to detect and predict suspicious or unusual activity for our domain. By continuously analyzing our unique traffic, RTTAD learns what is and isn't normal for our domain and sends instant notifications to IT teams if it notices anything out of the ordinary. The longer RTTAD has been enabled, the more accurate it becomes. With real-time alerts and clear visualizations of activity, teams can quickly determine if detected anomalies are legitimate or a threat, and take action accordingly.

Full DNS Audit Log History: Query Logging and Advanced Analytics

With enabling DNS advanced Query logging and Analytics platform, we can review our web traffic's real-time and historical patterns. With this unique data at our fingertips, our team will be able to spot unusual behavior and take appropriate measures before things spiral out of control.

10 Ways to Prevent a DDoS Attack

1. Know our network's traffic

Every organization's infrastructure has typical Internet traffic patterns – know ours. When we understand our organization's normal traffic pattern, we'll have a baseline. That way, when unusual activity occurs, we can identify the symptoms of a **DDoS attack**.

2. Create a Denial of Service Response Plan

Do we know what will happen when and if a DDoS attack happens? How will our organization respond? By defining a plan in advance, we'll be able to respond quickly and efficiently when our network is targeted.

This can take some planning; the more complex our infrastructure, the more detailed our DDoS response plan will be. Regardless of our company's size, however, our plan should include the following:

DDoS Defense	
Bandwidth	<ul style="list-style-type: none"> • Increase bandwidth • Alternate routes • Filter unwanted traffic
Throttle/block	<ul style="list-style-type: none"> • Block unwanted protocol • Block unwanted source • Block unwanted destination • Blackhole upstream (RTBH)
Scrubbing	<ul style="list-style-type: none"> • BGP maneuver traffic (outsource) • Proxy application/CAPTCHA • Authenticate connection
Maneuver	<ul style="list-style-type: none"> • DNS re-allocate resources • BGP maneuver to partner

- A systems checklist
- A trained response team
- Well-defined notification and escalation procedures.
- A list of internal and external contacts that should be informed about the attack
- A communication plan for all other stakeholders, like customers, or vendors by way of email, SMS, social media mentioning the downtime, communicate properly

3. Make our network resilient

Our infrastructure should be as resilient as possible against DDoS attacks. That means more than firewalls because some DDoS attacks target firewalls. Instead consider making sure we're not keeping all our eggs in the same basket – put data centers on different networks, make sure that not all our data centers are in the same physical location, put servers in different data centers or zones, routers and switches are properly configured and benchmarked using a checklist, reduce IP exposure to the internet and be sure that there aren't places where traffic bottlenecks in our network.

4. Practice good cyber hygiene

It goes without saying that our users should be engaging in best security practices, including changing passwords, secure authentication practices, knowing to avoid **phishing attacks**, and so on. The less user error our organization demonstrates, the safer we'll be, even if there's an attack. Moreover, the lesser footprint we have in the internet, the lesser chances we will get affected by DDoS or any attack for that matter.

5. Scale up our bandwidth

If DDoS is creating a traffic jam in our network, one way to make that traffic jam less severe is to widen the highway. By adding more bandwidth, our organization will be able to absorb more to absorb a larger volume of traffic. This solution won't stop all DDoS attacks, however. The size of volumetric DDoS attacks is increasing; in 2018, for example, **a DDoS attack topped 1 Tbps in size for the first time**. That was a record... until a few days later, when a 1.7 Tbps attack occurred, the story goes on. Recently, **Microsoft drops 3.47 Tbps, a record number of DDoS attacks** too.

6. Take advantage of anti-DDoS hardware and software

DDoS attacks have been around for a while and some kinds of attacks are very common. There are plenty of products that are prepared to repel or mitigate certain protocol and application attacks, take advantage of those tools, but do remember, every solution we install, opens up another path to get penetrated.

7. Move to the cloud

While this won't eliminate DDoS attacks, moving to the **cloud for data scrubbing can mitigate** attacks. The cloud has more bandwidth than on-premise resources, for example, and the nature of the cloud means many servers are not located in the same place.

8. Know the symptoms of an attack

Our network slows down inexplicably. The website shuts down. All of a sudden, we're getting a lot of spam. These can all be signs of a DDoS attack. If so, the organization

should investigate. And do remember, there is no way other than to implement cybersecurity framework and practices, its always the technology people, who failed to configure devices properly, never noticed the board, came up short on identifying and remediating, generating risk profiles to mitigate etc.

9. Outsource our DDoS protection

Some companies offer DDoS-as-a-Service. Some of these companies specialize in scaling resources to respond to an attack, others bolster defenses, and still, others mitigate the damage of an ongoing attack.

10. Monitor for unusual activity

MOTO: if we can't see it, no one would. Meaning, our network devices, transmissions, bandwidth, needs to be constantly monitored and the logs needs to be fed into a SIEM service to isolate and notify network managers that an attack is just started. Once we know our typical activity and the signs of an attack, monitor our network for odd traffic.

By monitoring traffic in real-time, our organization will be able to spot a DDoS attack when it starts and mitigate it within minutes, since SOC's primary requirement is just to do that, and they will be preparing to withstand such attacks.

Summary

Whatever we are doing on designing our network, configuring, provision secure access etc. follow standards, not best practices, and employ enterprise grade solutions. As when required, its too late, failed to plan properly, and we are destined to fail, essentially, failure to plan, plan to fail.

In a nutshell: How to survive the DDoS Attack?

1. List vulnerable, high priority resources
2. Partner with an upstream provider
3. Create a network traffic baseline
4. Harden against common DDoS attacks
5. Reduce the DDoS attack surface area
6. Patching
7. Network segmentation and access distribution
8. Scrubbing services
9. DDoS stress testing
10. Incident response planning
11. Employee awareness
12. DDoS attacks: Stay vigilant and survive

Team Readiness Requirements

A proper guideline must be set in motion for improvements. These baseline understandings will define how tough a network is to withstand continuous service disruption attacks. Managed DDoS can take place but the understanding of the network components, its configurations always aid in reducing attack surface, where an attack can take place but our attacked nodes will presumably sustain the attack without service interruption. **The below understanding is not bookish, and is a must for the network team who runs and manages any type of access, or distribution network problems will remain systematic and every initiative will deliberately fail. Some standards (NIST 800-53r5 and 171A & MITRE ATT&CK):**

1. [Search | CSRC \(nist.gov\)](#)
2. [Network Security Checklist.pdf \(cisco.com\)](#)
3. [Matrix - Enterprise | MITRE ATT&CK®](#)




000_Mandatory
Requirements_ISO-2'

Mandatory Requirements for ISO 27001 & 22301

1. Advanced DNS Monitoring and Protection: Real-time Anomaly Detection (RTTAD)
2. Full DNS Audit Log History: Query Logging and Advanced Analytics
3. Achieve device-based configuration benchmark
4. Internal security metrics must be able to draw the line where a user cannot install unauthorized software's into their working computers
5. DNS poisoning, recursive query etc. leading to bots and DNS poisoning
6. ACL whitelisting and drop all unrecognized transmissions
7. Properly designed network engineering & transmission engineering
8. Network broadcast flood mitigation
9. Capacity planning, management, current report, and future plan
10. Define Zones: Server zones, Application delivery zones, OTT Zones etc.
11. Transmission design for: VPS, Video Stream, IPTSP, URL filtering, Web Based Access policies, Application based Policy on transmissions, ERP delivery etc.
12. Identity & access management with ACL optimization
13. Broadcast, Anycast, Multicast configuration requirements
14. Network Segmentation by Corporate & Retail
15. Cache, CGNAT, BNG, IIG, CDN Separation and delivery isolation
16. System hardening based on benchmark for CISCO and all relevant services
17. Technology planning & system architecture with zoning for DMZ, servers, storage, VPN, VLAN, DNS, NTP etc

Key Questions That You Must Answer at the end of the Security Investigation

- Which systems were compromised? 
- Where did the attack start?
- Which user account was used to start the attack? Did it move laterally?
 - ▶ If it did, what systems were involved in this movement?
- Did it escalate privilege?
 - ▶ If it did, which privilege account was compromised?
- Did it try to communicate with command and control?
 - ▶ If it did, was it successful?
 - ▶ If it was, did it download anything from there?
 - ▶ If it was, did it send anything to there?
- Did it try to clear evidence?
 - ▶ If it did, was it successful?

18. Properly store VPN keys, recover when required
19. Tech system detail plan and improvement scope definition & requirements
20. Decentralization network design with service mapping, where customers should not be able to scan on north-bound transmission or be able to find any resource. Specifically, TENDA, TP-LINK devices comes with built-in AI engine, they can map and pull internet bandwidth from any DNS resolvers, therefore, it's a critical design configuration that must be in place.
21. Privileged access management on devices and customer's VPN credentials
22. Tech Server & Application systems detailed plan development
23. Networked device licensing & deprecation requirements
24. Networked device OS Types, Upgradability & Extended Support Requirements
25. Networked device: OS patch management, firmware upgrade, this is as vital as it gets
26. Exposed Real-IP list & remediation plan for a private network against purchased IP blocks, How many are assigned & free
27. VM Based Zonal Firewall requirement: Physical Server requirements and develop BoQ
28. LDAP IPA based Installation for all Linux based servers. Ensure PEM file is used to access these critical servers
29. Linux servers credentials, application PEM, Integration with IPA
30. Server configurations: physical or VM. Complete with BIOS, iDRAC and always enable Enterprise BIOS options, or they will be prone to direct attacks.
31. NTP Server and syncing throughout the infrastructure from internal sync servers, should not be any outbound syncing
32. DNS server syncing throughout the infrastructure
33. NMS Dashboard Requirement list with end-to-end visibility
34. Enable end-to-end encryption, install SSL certificate as well
35. Data Collection and Log Shipping Requirements mapping for Security Scanning
36. Initiate internal SMTP integration
37. Systemwide static IP removal and re-design the IP network
38. Customer Data Links list and credentials documentations
39. Enable 2FA for critical resources, use company mobile number
40. Device access streamline using SSH not Telnet, stop Telnet, TTY on all devices
41. Perimeter exposure reduction, by limiting exposed IP
42. Zero trust network access design & implementation
43. Establish & document customer's data links layers, secure their configurations
44. Must use at least 8 alphanumeric characters for any device passwords. Usernames should not be any human readable form.
45. ITIL Based service management portfolio
46. Cryptographic keys alignment and develop a software vault for storing these keys or use HSM server for keys management
47. NAC deployment provisioning
48. Automated IP fabric
49. Enable proper access and distribution network design
50. Enable TACACS for Cisco & RADIUS for Mikrotik - Full IAM
51. Enable policy based services protocol-wise, Bongo, IPTSP etc.
52. Policy based application traffic & protection
53. IIG, BDIX, PNI, CDN data movement monitoring
54. Traffic engineering: Separation of Transit, IIG & CDN, CGNAT, BNG, BRAS

Who will do What? What's the Requirements? Skills Mapping? RACI? Documentations?

1. How the quality of the manpower is ensured even though certified personnel are in place.
2. What were the visibility requirements for attacks? What manpower does technical have as the first responder?
3. Has there been a RACI for jurisdiction metrics? and their JD is optimized for delivery mapped to the skills requirements?
4. Are they capable of doing their job properly? How is it measured?
5. Were all those activities documented? Which can be shared to the new commers? Are there any?
6. Site reliability engineering are in place? Any defined team is there?
7. Where is the DDoS response plan? Who would be involved to mitigate and learn from these attacks? Are they getting documented for future remediations?
8. Insider's Admin credential user's impact are known to the technical?
9. How does technical reporting take place and how KT is performed once someone of managerial responsibility left the organization?
10. Any document developed for any type of compliance? Governance program? ITIL management?
11. Monthly activity summary logs, device configuration backups?
12. Where is the incident response plan? Any ORM, ERM, BCP content generated for this as 'lesson learned'? How is the internal IT Audit responding to these requirements?

Responsibility Matrix

Task Head	Task Sub-head	Current Status	Progress	RACI	Owner	Submit to	Audit
IT, IS Governance Program	Identity & Access Management	N/A		RA	I (IS)	IC (IS)	I
	IS team ensures device configurations , and periodically assess its vulnerabilities. Technical team will continuously configure & IS team will monitor	N/A		RA	I (IS)	IC (IS)	I
	Enterprise Risk Management (ERM) & ORM	N/A		RA	I (IS)	Board	I
	Policy & process development	N/A		RA	I (IS)	Board	I

	Device Configuration standardization for switch, router, LB, FI infrastructure with Licensing modality	N/A	RA	Technical	IC (IS)	I
	IPA & PEM must be enabled for Linux servers and users	N/A	RA	I (IS)	IC (IS)	I
	Networked device access protection or NAC/NAP	N/A	RA	Technical	IC (IS)	I
	ITIL reporting on devices	N/A	RA	Technical	IC (IS)	
	ISO 27001 reporting	N/A	RA	Technical	IC (IS)	I
	Business continuity reporting	N/A	RA	Technical	IC (IS)	I
	Disaster recovery reporting	N/A	RA	Technical	IC (IS)	I
	ERM - Risk identification & management, incident management & reporting	N/A	RA	Technical	IC (IS)	I
	Partnership portal access	N/A	RA	IS	IC (IS)	I
	Device assignment to employees	N/A	RA	IS	IC (IS)	I
	Security consultancy	N/A	RA	IS	Board	I
	Physical servers	N/A	RA	IS	Board	I
	AAA services will be under IS Jurisdiction	N/A	RA	IS	Board	I
Network Monitoring	Back-office network design & maintenance	N/A	RA	IS	Board	I
	Device configurations	N/A	RA	Technical	IC (IS)	I
	NOC room and monitor setup	Silo	RA	Technical	IC (IS)	I

	List of IP's, Ports to monitor in NMS	Not populated	RA	Technical	IC (IS)	
	Active protection placement end-to-end	N/A	RA	Technical	IC (IS)	I
	VPN user access provisioning	In-place	RA	I (IS)	IC (Technical)	I
	Enable audit logs for all networked devices, and log shipping to the SIEM server	N/A	RA	Technical	IC (IS)	I
BTS Inventory	Emergency Contact Card per BTS	N/A	RA	Technical	I (Admin), IC (IS)	I
	Gatekeepers Contact details in HQ & in BTS	N/A	RA	Technical	I (Admin), IC (IS)	I
	Device inventory & cabling efficiency design	N/A	RA	Technical	IC (IS)	I
	BTS power under a breaker	N/A	RA	Technical	I (Admin), IC (IS)	I
	BTS Power consumption & load bearing	N/A	RA	Technical	I (Admin), IC (IS)	I
	BTS earthing provisioning	N/A	RA	Technical	I (Admin), IC (IS)	I
	All types of cable labeling	N/A	RA	Technical	IC (IS)	I
	BTS - Physical security & biometric access	N/A	RA	Technical	I (Admin), IC (IS)	I
	AC maintenance	N/A	RA	Admin		
BTS Monitoring	Power consumption requirement & monitoring	N/A	RA	Technical	I (Admin), IC (IS)	I
	Room temperature monitoring	N/A	RA	Technical	I (Admin), IC (IS)	I
	AC automatic switchover	N/A	RA	Technical	I (Admin), IC (IS)	I

Online UPS switchover	N/A	RA	Technica	I (Admin), IC (IS)	I
STS installation for single PSU devices	N/A	RA	Technica	IC (IS)	I
BTS wise roles and responsibilities	N/A	RA	Technica	I (Admin), IC (IS)	I
BTS Battery & Online UPS functions	N/A	RA	Technica	IC (IS)	I

Decision Tree

1. Tech user's must be disciplined and knowledgeable in certain manner to get along with network security requirements to reduce attack surface area
2. Their **typical activity** exposes the company to an enormous level of attacks.
3. Who is looking into the recent access to devices? AAA?

Solution

1. **Enable CASB** based transmission aggregators (Preferably Cloudflare) and cleaners or scrubbing zones. This initiative will call for zonal development, IP planning, customer's search for upward transmissions, server commissioning and fixing of above-mentioned problems.
 - a. Enable for Cloudflare or Radware DefensePipe
2. **Enable Hardware Based DNS Protection** service. This is one service where all the device locations are located, and if this DNS service can be penetrated, all will be lost.
 - a. Enable for Trellix

Team Enablement

Assign team members who would report to the IS lead whose KRA will be looked after by the IS Lead and see through the implementation of the CASB and adequate Level-0 to 1 router & System Hardening. Manpower Requirement follows:

1. Approve the Plan
2. Develop PoC Environment - Approve the Cost Involvement
3. TRAIN - Team's Understanding on How CASB Operates
4. Network Assessment Report Development
5. Driver & Tracker for the Implementation - PMO
6. Implementation Requirements Gathering
7. Formulate and Announce the Team Member's Names
8. Devise the Implementation Plan for the CASB
9. Consensus Agreement from the Stakeholders
10. Rollout the Approved Plan Including Monthly check-in & Progress Metering
11. Maintain compliance on

- a. Documentations
- b. SoP Development
- c. System Configuration Backup
- d. Proper & Exact Design of the Network in Visio

Team:

SL	Name	ID	Email Address	OU	Function
1				Security	Configuration detailing
2				Security	Configuration Security
3				Core-Network	Network Security
4				Core-Network	Network Security
5					
6				BTS	Cabling - Marking, SFP, Fiber, Network Design & Map
7				Core-Network	AAA, DNS, NTP, Back-office Separation etc.
8					

Program Management

The team must be enabled for:

1. Develop plan for which solution to pick,
2. Why it's a better solution than others
3. Why it does go with our MSSP network and BIG IT will benefit from it
4. Approved solution integration design plan

SL	Name	ID	Email Address	OU	Function
1				PMO	Project Movement Tracking
2				Audit	Compliance documentation readiness

Annexure - A (Top DDoS Service Provider)

Top Vendors who are providing Enterprise Grade DDoS protection & remediation services

DDoS Protection	Company Name
KENTIK DDoS Protect	Kentik
A10Networks	A10Networks
Lumen	
CheckPoint DDoS Protector	CheckPoint
CloudFlare DDoS Protection	Cloudflare
PaloAlto DDoS	PaloALto
FortiNet DDoS	FortiNet
F5 DDoS	F5
Trellix	
Arbor Edge Defense	NetScout
Corero	Corero
FastNetMon DDoS detection tool	Fastnetmon
NexusGuard Network Protection Offering	Nexusguard
Anti DDoS	Voxility
DDoS Detection and Mitigation Software: Andrisoft Vanguard	Andrisoft
DDoS Protect Against DDoS Attack Akamai DDoS Protection	Akamai
RioRey	Hardware Based Filtering – RioRey: The DDoS Specialist™
Imperva DDoS	Imperva
DDoS Protection Radware	Radware
DDoS Attack Protection Solutions Neustar	Neustarsecurityservices
Arbor DDoS Protection Solutions NETSCOUT	Netscout
Azure DDoS Protection Standard overview	Microsoft
Telecommunications Software Solutions for Service Providers	Ribboncommunications
FireEye NX series Network & DNS Poisoning of all types	FireEye
Imperva DDoS Protection	Imperva
INDUSFACE AppTrana	Indusface

ANNEXURE - B (Visibility Requirements)

DDOS VECTOR PROTECTION & VISIBILITY REQUIREMENT DETAILS				
Partial fulfillment of ISO, BCP, DRP, ERM				
Document Code: ISMS/ISO/DMS/XX Version: 1.0 Prepared Date: 11th of May 2022				
Next Review Date: 11th of August 2022 Confidentiality Level: HBI				
DDoS Guide: CISA				
SL	Attack Vectors	Details	Protection Type	Visibility
NETWORK LAYER ATTACKS				
	Reflection Attacks	Spoofing IP to make legitimate 3 rd party to send request to Victim	Default Always On - Infrastructure Level	Since protection is at Infra level, site level visibility is not possible
	SMURF Attacks	Vulnerability in ICMP protocol exploited to make network inactive	Default Always On - Infrastructure Level	
	ACK Attacks	Overloading Server with TCP ACK	Default Always On - Infrastructure Level	
	Flood Attacks (UDP Fraggle, Smurf, TCP, ICMP Ping of Death, NTP amplification, Zero days, Advanced Persistent DoS etc.)	Flooding Server with requests to exhaust resource and make server unavailable, volume-based attacks, which use high traffic to inundate the network bandwidth	Default Always On - Infrastructure Level	
	Network Port scanning	Port scans done to exploit vulnerabilities found	Default Always On - Infrastructure Level	
APPLICATION LAYER ATTACKS				
	Slowloris	Send partial HTTP request to Server. Server keeps waiting for rest and gets exhausted	Default Always On - Infrastructure Level	Since protection is at Infra level, site level visibility is not possible
	Slow Read attacks	Sends a request to server but does not read in timely manner from the server	Default Always On - Site Level	Attacks are shown under DDOS Category
	Slow POST attacks	Says to server there is POST request of x length but does not send it or sends it slow	Default Always On - Site Level	Attacks are shown under DDOS Category
	HTTP Flood (GET & POST Attacks)	Requests are sent from zombie armies few request at a time. Hard to detect they remain below threshold	Default Always On - Site Level	Attacks are shown under DDOS Category
	Resource Exhaustion	Identity resource that can be exhausted and attack it. For example memory exhaustion, connection pool exhaustion	Default Always On - Site Level	Attacks are shown under Rules that block exploit of vulnerabilities leading to resource exhaustion
	Brute force attacks	Trial and error method to decrypt sensitive data	Default Always On - Site Level	Attacks are shown under DDOS Category
	Large payload POST Attack	Oversize payload attack where DOM Parser payload is increased to cause memory exhaustion	Default Always On - Infrastructure Level	Since protection is at Infra level, site level visibility is not possible
	SSL exhaustion	Garbage data to SSL server to exhaust SSL pool	Default Always On - Infrastructure Level	Since protection is at Infra level, site level visibility is not possible

	Mimicked User Browsing	Requests mimicking normal user behavior exhausting server	Default Always On - Site Level	Attacks are shown under DDOS Category
	Database connection pool exhaust	Send queries that keeps DDOS connection open and exhaust	Default Always On - Site Level	Attacks are shown under Rules that block exploit of vulnerabilities leading to resource exhaustion

i.e. this is not an exhaustive list and type of attacks

ATTACK POSSIBILITIES BY OSI LAYER

OSI Layer	Protocol Data Unit (PDU)	Layer Description	Protocols	Examples of Denial of Service Techniques at Each Level	Potential Impact of DoS Attack	Mitigation Options for Attack Type
Application Layer (7)	Data	Message and packet creation begins. DB access is on this level. End-user protocols such as FTP, SMTP, Telnet, and RAS work in this layer.	Uses the Protocols FTP, HTTP, POP3, & SMTP and its device is the Gateway	PDF GET requests, HTTP GET, HTTP POST, = website forms (login, uploading photo/video, submitting feedback)	Reach resource limits of services Resource starvation	Application monitoring is the practice of monitoring software applications using dedicated set of algorithms, technologies, and approaches to detect zero day and application layer (Layer 7 attacks). Once identified these attacks can be stopped and traced back to a specific source more easily than other types of DDOS attacks.
Presentation Layer (6)	Data	Translates the data format from sender to receiver.	Use the Protocols Compression & Encryption	Malformed SSL Requests - Inspecting SSL encryption packets is resource intensive. Attackers use SSL to tunnel HTTP attacks to target the server	The affected systems could stop accepting SSL connections or automatically restart	To mitigate, consider options like offloading the SSL from the origin infrastructure and inspecting the application traffic for signs of attacks or violations of policy at an applications delivery platform (ADP). A good ADP will also ensure that our traffic is then re-encrypted and forwarded back to the origin infrastructure with unencrypted content only ever residing in protected memory on a secure bastion host.
Session (5)	Data	Governs establishment, termination, and sync of session within the OS over the network (ex:	Use the Protocol Logon/Logoff	Telnet DDoS-attacker exploits a flaw in a Telnet server software running on the switch, rendering Telnet services unavailable	Prevents administrator from performing switch management functions	Check with our hardware provider to determine if there's a version update or patch to mitigate the vulnerability

		when we log off and on)				
--	--	-------------------------	--	--	--	--

ATTACK POSSIBILITIES BY OSI LAYER (IOC)

OSI Layer	Protocol Data Unit (PDU)	Layer Description	Protocols	Examples of Denial of Service Techniques at Each Level	Potential Impact of DoS Attack	Mitigation Options for Attack Type
Transport (4)	Segment	Ensures error-free transmission between hosts: manages transmission of messages from layers 1 through 3	Uses the Protocols TCP & UDP	SYN Flood, Smurf Attack	Reach bandwidth or connection limits of hosts or networking equipment	DDoS attack blocking, commonly referred to as blackholing, is a method typically used by ISPs to stop a DDoS attack on one of its customers. This approach to block DDoS attacks makes the site in question completely inaccessible to all traffic, both malicious attack traffic and legitimate user traffic. Black holding is typically deployed by the ISP to protect other customers on its network from the adverse effects of DDoS attacks such as slow network performance and isrupted service
Network (3)	Packet	Dedicated to routing and switching information to different networks. LAN or internetworks	Uses the Protocols IP, ICMP, ARP, & RIP and uses Routers as its device	ICMP Flooding - A Layer 3 infrastructure DDoS attack method that uses ICMP messages to overload the targeted network's bandwidth	Can affect available network bandwidth and impose extra load on the firewall	Rate-limit ICMP traffic and prevent the attack from impacting bandwidth and firewall performance
Data Link (2)	Frame	Establishes, maintains, and decides how the transfer is accomplished over the physical layer	Uses the Protocols 802.3 & 802.5 and it's devices are NICs, switches bridges & WAPs	MAC flooding - inundates the network switch with data packets	Disrupts the usual sender to recipient flow of data - blasting across all ports	Many advanced switches can be configured to limit the number of MAC addresses that can be learned on ports connected to end stations; allow discovered MAC addresses to be authenticated against an authentication, authorization and accounting (AAA) server and subsequently filtered

Physical (1)	Bits	Includes, but not limited to cables, jacks, and hubs	Uses the Protocols 100 Base-T & 1000 Base-X and uses Hubs, patch panels, & RJ45 Jacks as devices	Physical destruction, obstruction, manipulation, or malfunction of physical assets	Physical assets will become unresponsive and may need to be repaired to increase availability	Practice defense in-depth tactics, use access controls, accountability, and auditing to track and control physical assets
--------------	------	--	--	--	---	---

POSSIBLE DDoS TRAFFIC TYPES

HTTP Header	HTTP headers are fields which describe which resources are requested, such as URL, a form, JPEG, etc. HTTP headers also inform the web server what kind of web browser is being used. Common HTTP headers are GET, POST, ACCEPT, LANGUAGE, and USER AGENT. The requester can insert as many headers as they want and can make them communication specific. DDoS attackers can change these and many other HTTP headers to make it more difficult to identify the attack origin. In addition, HTTP headers can be designed to manipulate caching and proxy services. For example, is it possible to ask a caching proxy to not cache the information.
HTTP POST Flood	An HTTP POST Flood is a type of DDoS attack in which the volume of POST requests overwhelms the server so that the server cannot respond to them all. This can result in exceptionally high utilization of system resources and consequently crash the server.
HTTP POST Request	An HTTP POST Request is a method that submits data in the body of the request to be processed by the server. For example, a POST request takes the information in a form and encodes it, then posts the content of the form to the server.
HTTPS Post Flood	An HTTPS POST Flood is an HTTP POST flood sent over an SSL session. Due to the use of SSL it is necessary to decrypt this request in order to inspect it.
HTTPS POST Request	An HTTPS POST Request is an encrypted version of an HTTP POST request. The actual data transferred back and forth is encrypted
HTTPS GET Flood	An HTTPS GET Flood is an HTTP GET flood sent over an SSL session. Due to the SSL, it is necessary to decrypt the requests in order to mitigate the flood.
HTTPS GET Request	An HTTPS GET Request is an HTTP GET Request sent over an SSL session. Due to the use of SSL, it is necessary to decrypt the requests in order to inspect it.
HTTP GET Flood	An HTTP GET Flood is a layer 7 application layer DDoS attack method in which attackers send a huge flood of requests to the server to overwhelm its resources. As a result, the server cannot respond to legitimate requests from the server.
HTTP GET Request	An HTTP GET Request is a method that makes a request for information for the server. A GET request asks the server to give we something such as an image or script so that it may be rendered by our browsers.
SYN Flood (TCP/SYN)	SYN Flood works by establishing half-open connections to a node. When the target receives a SYN packet to an open port, the target will respond with a SYN-ACK and

	try to establish a connection. However, during a SYN flood, the three-way handshake never completes because the client never responds to the server's SYN-ACK. As a result, these "connections" remain in the half-open state until they time out.
UDP Flood	UDP floods are used frequently for larger bandwidth DDoS attacks because they are connectionless and it is easy to generate protocol 17 (UDP) messages from many different scripting and compiled languages.
ICMP Flood	Internet Control Message Protocol (ICMP) is primarily used for error messaging and typically does not exchange data between systems. ICMP packets may accompany TCP packets when connecting to a sever. An ICMP flood is a layer 3 infrastructure DDoS attack method that uses ICMP messages to overload the targeted network's bandwidth.
MAC Flood	A rare attack, in which the attacker sends multiple dummy Ethernet frames, each with a different MAC address, Network switches treat MAC addresses separately, and hence reserve some resources for each request. When all the memory in a switch is used up, it either shuts down or becomes unresponsive. In a few types of routers, a MAC flood attack may cause these to drop their entire routing table, thus disrupting the whole network under its routing domain.

GLOSSARY

Denial of Service	The core concepts of cyber security are availability, integrity, and confidentiality. Denial of Service (DoS) attacks impact the availability of information resources. The DoS is successful if it renders information resources unavailable. Success and impact differ in that impact is relative to the victim. For example, if an actor DoS's a website belonging to a company that relies on e-commerce to drive their business operations, the company may experience financial losses if the DoS is sustained for a period of time. The risk, threat, and impact levels for DoS activity are determined on a case by case basis.
Layer 3 and Layer 4 DDoS Attacks	Layer 3 and Layer 4 DDoS attacks are types of volumetric DDoS attacks on a network infrastructure Layer 3 (network layer) and 4 (transport layer) DDoS attacks rely on extremely high volumes (floods) of data to slow down web server performance, consume bandwidth, and eventually degrade access for legitimate users. These attack types typically include ICMP, SYN, and UDP floods.
Layer 7 DDoS Attack	A Layer 7 DDoS attack is an attack structured to overload specific elements of an application server infrastructure. Layer 7 attacks are especially complex, stealthy, and difficult to detect because they resemble legitimate website traffic. Even simple Layer 7 attacks--for example those targeting login pages with random user IDs and passwords, or repetitive random searches on dynamic websites--can critically overload CPUs and databases. Also, DDoS attackers can randomize or repeatedly change the signatures of a Layer 7 attack, making it more difficult to detect and mitigate.
itsoknoproblembro	The name given to a suite of malicious PHP scripts discovered on multiple compromised hosts. The main functionalities appear to be file uploads, persistence, and DDoS traffic floods. The itsoknoproblembro toolkit includes multiple infrastructure and application-layer attack vectors, such as SYN floods, that can simultaneously attack multiple destination ports and targets, as well as ICMP, UDP, SSL encrypted attack types. A common characteristic of the attacks is a large UDP flood targeting DNS infrastructure. Uniquely, the attacking botnet contains many legitimate (non-spoofed) IP addresses, enabling the attack to bypass most anti-spoofing mechanisms.
PHP Shell, PHP Webshell	A script in the PHP language that can execute commands, view files, and perform other system administrative tasks. PHP shells are often used to take control of web servers via web application vulnerabilities.

Proxy	A proxy is a network device which terminates incoming traffic and then creates a new communication session which is used to send the traffic to the actual destination. The proxy fits between the requestor and the server and mediate all of the communication between the two. Examples of proxy technologies are content switches and load balancers. Proxy servers are most often used for the DNS requests, HTTPS, and HTTP. When HTTPS is being proxied, the proxy server itself must have copies of the public certificate which includes the public key and the private key so it can effectively terminate the SSL/TLS requests. Mitigating Layer 7 DDoS attacks is sometimes carried out using proxies.
Infrastructure DDoS Attack	An infrastructure attack is a DDoS attack that overloads the network infrastructure by consuming large amounts of bandwidth, for example by making excessive connection requests without responding to confirm the connection, as in the case of a SYN flood. A proxy server can protect against these kinds of attacks by using cryptographic hashtags and SYN cookies.
DNS Amplification Attack	A Domain Name Server (DNS) Amplification attack is a popular form of Distributed Denial of Service (DDoS), in which attackers use publicly accessible open DNS servers to flood a target system with DNS response traffic. The primary technique consists of an attacker sending a DNS name lookup request to an open DNS server with the source address spoofed to be the target's address. When the DNS server sends the DNS record response, it is sent instead to the target.

MITIGATING LARGE SCALE DoS/DDoS ATTACKS

DEVICE	LAYER	OPTIMIZED FOR	DOS PROTECTIONS
Firewall	4-7	Flow Inspection, Deep Inspection	Screen, Session Limits, Syn Cookie
Router	3-4	Packet Inspection, Frame Inspection	Line-Rate ACLs, Rate Limits
<p>Some DDoS Mitigation Actions and Hardware</p> <ul style="list-style-type: none"> • Stateful Inspection Firewalls • Stateful SYN Proxy Mechanisms • Limiting the number of SYNs per second per IP • Limiting the number of SYNs per second per destination IP • Set ICMP flood SCREEN settings (thresholds) in the firewall • Set UDP flood SCREEN settings (thresholds) in the firewall <p>Rate limit routers adjacent to the firewall and network</p>			

REFERENCES

- a. https://jncie.files.wordpress.com/2008/09/801003_protecting-the-network-from-denial-of-servicefloods.pdf
- b. https://www.owasp.org/images/4/43/Layer_7_DDOS.pdf
- c. <https://softwareandnetworks.wordpress.com/>
- d. <https://www.wisageek.com/what-is-mac-flooding.htm>
- e. <https://quizlet.com/14023507/lesson-2-defining-networks-with-the-osi-model-flash-cards/>
- f. <http://zuhairmirza-informative.blogspot.com/2013/04/dos-and-ddos-glossary-of-terms-part-2.html>

ANNEUXURE – C (Mitigation Plan)

There are two broad types of DDoS attacks: bandwidth depletion attacks and resources depletion attacks. To halt both types of attacks, we can follow the steps given below:

1. Scan for exposed services and for CVE, CVSS etc.
2. Unify all firmware'
3. If a few computers are the source of the attack, and we have identified the source of those IP, we can put an ACL (access control list) in our firewall blocking those IPs. Change the IP address of the web server for a while, if possible, but it will not be effective when the attacker will start resolving our new IP by querying our DNS servers. Protect our DNS servers at all cost, as if the DNS servers are poisoned, there is no way we can remedy the network in a stipulated time.
4. When we identify that the attacks originating from a specific country, we can think about blocking that country' IP block, at least for a while. Or block the complete IP block if our core router and switches has the latest OS build installed and updated.
5. Create an inbound traffic profile. This way we will know who is regularly visiting our resources. In case we discover an unexpected number of new visitors, we can further investigate the logs and source IPs. Before large scale attacks, we might experience a small-scale DDOS attack that the attacker may use to estimate the strength of our network resilience.
6. The easiest, although a costly, way to defend our network from bandwidth consumption attack is to buy more bandwidth, if we do not have a carrier grade firewall installed. Piecemeal based solution can be used for the time being, but the core bandwidth gateway must have an adequately provisioned firewall and scrubbing services
7. We may deploy more servers, spread around various datacenters, and we must use good load balancing systems with zoning (DMZ or MZ).
8. Make sure our DNS is protected behind the same type of load balancer that we used to protect our web and other resources.
9. Optimize our webserver to handle more visitors without exhausting all resources. If we are using Apache server, we can use Apachebooster plugin, which was designed by integration of varnish and nginx. Apachebooster can cope with sudden spike with traffic and memory usages.
10. Fast DNS-Protect against DNS-based DDoS attacks with a highly scalable DNS infrastructure. We can think about buying CASB business or enterprise plan, which provides protection to DNS and layer 3, 4 and 7 based DDoS attacks.
11. Enable anti IP spoofing features in our firewall and routers. It is much easier to implement anti-spoofing in NGFW firewalls than in the routers. To enable anti-spoof with ASDM. We can prevent spoofing in router using ACL. Create an access control list for our internal IP subnets, and apply that ACL in our Internet facing interface.
12. Hire third party DDoS service to protect our site. There are a number of service providers with robust network who can help our website survive during denial of service attack. We can subscribe to such service for a monthly cost of few hundred dollars only.
13. Pay attention to our networked devices security configuration in order to prevent resource depletion type of DDoS attack.
14. Consult a DDoS or security expert, and make an action plan to carry out when we actually face the attack.
15. Monitor our network and web traffic. If possible, we can set up multiple analytics to understand and gather more data of our traffic patterns.
16. Secure our DNS server against recursive DNS query attacks, and Cache poisoning for DNS and data cache services.

17. Block ICMP in our router. Enable it when we need it for troubleshooting purpose only. Also, we can do the following things with our router: rate limit, filtering packets, timeout half-open connections, drop junk and spoofed packets, set low threshold for TCP SYN, ICMP and UDP flood drop
18. Lastly, setup monitoring for our networked devices of routers, switches, FI, physical servers, applications, and its health, BW, etc.

ANNEUXURE – D (Configuration Benchmark)

Device Benchmark for CISCO Routers & Switches

A standardized device and its configuration plays a vital role in securing the infrastructure as a component. Many of these devices will be housed in the near future and misconfigurations generally leads to:

1. Device penetrations
2. Unable to withstand attacks
3. Missing software patches also will lead to attacks

In order to stay vigilant on misconfigurations, we must ensure that a monitoring system is in place, which primary has device configuration detection capability of:

1. Device type.
2. Identify its manufacturer data collection.
3. Its OS type, version, notify if a newer version is available.
4. Device can be registered to the NMS using SNMP.
5. Device can be configured to access securely.
6. Device can be configured to use SSL certificates.
7. Device can be populated in a single console for management.

This list can go very long on finalizing and configuring on a standard. Therefore, the following checklist is devised, and before a device is shipped to different location, the following checklist must be followed:

1. Update the device OS, firmware to its latest build.
2. Change the default password to an alphanumeric password.
3. Change the default "public" string settings for SNMP and enable health monitoring parameters to populate the device in the central monitoring.
4. Enable data encryption service.
5. Enable local NTP service update periodically, once a month/week.
6. Turn off Telnet service and enable SSH only access.
7. Enable input IP which can be accessible from NOC when its populated.
8. Enable log shipping to the designated storage service.
9. Username & password must be alphanumeric, cannot be readable or detectable human names.

Device Benchmark: List of Controls (CIS-Cisco)

Configure the rest of the requirements following the benchmark stated below:

Control		Set Correctly	
		Yes	No
1	Management Plane		
1.1	Local Authentication, Authorization and Accounting (AAA) Rules		
1.1.1	Enable 'aaa new-model' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2	Enable 'aaa authentication login' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.3	Enable 'aaa authentication enable default' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.4	Set 'login authentication for 'line tty' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.5	Set 'login authentication for 'line vty' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.6	Set 'login authentication for 'ip http' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.7	Set 'aaa accounting' to log all privileged use commands using 'commands 15' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.8	Set 'aaa accounting connection' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.9	Set 'aaa accounting exec' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.10	Set 'aaa accounting network' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.11	Set 'aaa accounting system' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.2	Access Rules		
1.2.1	Set 'privilege 1' for local users (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.2.2	Set 'transport input ssh' for 'line vty' connections (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.2.3	Set 'no exec' for 'line aux 0' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.2.4	Create 'access-list' for use with 'line vty' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.2.5	Set 'access-class' for 'line vty' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.2.6	Set 'exec-timeout' to less than or equal to 10 minutes for 'line aux 0' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.2.7	Set 'exec-timeout' to less than or equal to 10 minutes 'line console 0' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.2.8	Set 'exec-timeout' less than or equal to 10 minutes 'line tty' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.2.9	Set 'exec-timeout' to less than or equal to 10 minutes 'line vty' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.2.10	Set 'transport input none' for 'line aux 0' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.2.11	Set 'http Secure-server' limit (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.2.12	Set 'exec-timeout' to less than or equal to 10 min on 'ip http' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.3	Banner Rules		
1.3.1	Set the 'banner-text' for 'banner exec' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

1.3.2	Set the 'banner-text' for 'banner login' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.3.3	Set the 'banner-text' for 'banner motd' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.3.4	Set the 'banner-text' for 'webauth banner' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.4	Password Rules		
1.4.1	Set 'password' for 'enable secret' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.4.2	Enable 'service password-encryption' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.4.3	Set 'username secret' for all local users (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.5	SNMP Rules		
1.5.1	Set 'no snmp-server' to disable SNMP when unused (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.5.2	Unset 'private' for 'snmp-server community' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.5.3	Unset 'public' for 'snmp-server community' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.5.4	Do not set 'RW' for any 'snmp-server community' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.5.5	Set the ACL for each 'snmp-server community' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.5.6	Create an 'access-list' for use with SNMP (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.5.7	Set 'snmp-server host' when using SNMP (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.5.8	Set 'snmp-server enable traps snmp' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.5.9	Set 'priv' for each 'snmp-server group' using SNMPv3 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.5.10	Require 'aes 128' as minimum for 'snmp-server user' when using SNMPv3 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.6	Login Enhancements		
1.6.1	Configure Login Block (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.6.2	AutoSecure (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.6.3	Configuring Kerberos (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.6.4	Configure Web interface (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2	Control Plane		
2.1	Global Service Rules		
2.1.1	Setup SSH		
2.1.1.1	Configure Prerequisites for the SSH Service		
2.1.1.1.1	Set the 'hostname' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1.1.2	Set the 'ip domain-name' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1.1.3	Set 'modulus' to greater than or equal to 2048 for 'crypto key generate rsa' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1.1.4	Set 'seconds' for 'ip ssh timeout' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

2.1.1.1.5	Set maximum value for 'ip ssh authentication-retries' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1.2	Set version 2 for 'ip ssh version' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.2	Set 'no cdp run' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.3	Set 'no ip bootp server' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.4	Set 'no service dhcp' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.5	Set 'no ip identd' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

2.1.6	Set 'service tcp-keepalives-in' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.7	Set 'service tcp-keepalives-out' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.8	Set 'no service pad' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

2.2	Logging Rules		
------------	----------------------	--	--

2.2.1	Set 'logging enable' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.2	Set 'buffer size' for 'logging buffered' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.3	Set 'logging console critical' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.4	Set IP address for 'logging host' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.5	Set 'logging trap informational' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.6	Set 'service timestamps debug datetime' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.7	Set 'logging source interface' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.8	Set 'login success/failure logging' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

2.3	NTP Rules		
------------	------------------	--	--

2.3.1	Require Encryption Keys for NTP		
--------------	--	--	--

2.3.1.1	Set 'ntp authenticate' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.2	Set 'ntp authentication-key' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.3	Set the 'ntp trusted-key' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4	Set 'key' for each 'ntp server' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2	Set 'ip address' for 'ntp server' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

2.4	Loopback Rules		
------------	-----------------------	--	--

2.4.1	Create a single 'interface loopback' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.2	Set AAA 'source-interface' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.3	Set 'ntp source' to Loopback Interface (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.4	Set 'ip tftp source-interface' to the Loopback Interface (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

3	Data Plane		
----------	-------------------	--	--

3.1	Routing Rules		
------------	----------------------	--	--

3.1.1	Set 'no ip source-route' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.2	Set 'no ip proxy-arp' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

3.1.3	Set 'no interface tunnel' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.4	Set 'ip verify unicast source reachable-via' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.2	Border Router Filtering		
3.2.1	Set 'ip access-list extended' to Forbid Private Source Addresses from External Networks (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.2.2	Set inbound 'ip access-group' on the External Interface (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3	Neighbor Authentication		
3.3.1	Require EIGRP Authentication if Protocol is Used		
3.3.1.1	Set 'key chain' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1.2	Set 'key' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1.3	Set 'key-string' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1.4	Set 'address-family ipv4 autonomous-system' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1.5	Set 'af-interface default' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1.6	Set 'authentication key-chain' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1.7	Set 'authentication mode md5' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1.8	Set 'ip authentication key-chain eigrp' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1.9	Set 'ip authentication mode eigrp' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.2	Require OSPF Authentication if Protocol is Used		
3.3.2.1	Set 'authentication message-digest' for OSPF area (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.2.2	Set 'ip ospf message-digest-key md5' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.3	Require RIPv2 Authentication if Protocol is Used		
3.3.3.1	Set 'key chain' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.3.2	Set 'key' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.3.3	Set 'key-string' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.3.4	Set 'ip rip authentication key-chain' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.3.5	Set 'ip rip authentication mode' to 'md5' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4	Require BGP Authentication if Protocol is Used		
3.3.4.1	Set 'neighbor password' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

IG 1 Mapped Recommendations

Recommendation	Set Correctly	
	Yes	No

1.1.7	Set 'aaa accounting' to log all privileged use commands using 'commands 15'	<input type="checkbox"/>	<input type="checkbox"/>
1.1.9	Set 'aaa accounting exec'	<input type="checkbox"/>	<input type="checkbox"/>
1.1.10	Set 'aaa accounting network'	<input type="checkbox"/>	<input type="checkbox"/>
1.1.11	Set 'aaa accounting system'	<input type="checkbox"/>	<input type="checkbox"/>
1.2.2	Set 'transport input ssh' for 'line vty' connections	<input type="checkbox"/>	<input type="checkbox"/>
1.2.3	Set 'no exec' for 'line aux 0'	<input type="checkbox"/>	<input type="checkbox"/>
1.2.6	Set 'exec-timeout' to less than or equal to 10 minutes for 'line aux 0'	<input type="checkbox"/>	<input type="checkbox"/>
1.2.7	Set 'exec-timeout' to less than or equal to 10 minutes 'line console 0'	<input type="checkbox"/>	<input type="checkbox"/>
1.2.8	Set 'exec-timeout' less than or equal to 10 minutes 'line tty'	<input type="checkbox"/>	<input type="checkbox"/>
1.2.9	Set 'exec-timeout' to less than or equal to 10 minutes 'line vty'	<input type="checkbox"/>	<input type="checkbox"/>
1.2.10	Set 'transport input none' for 'line aux 0'	<input type="checkbox"/>	<input type="checkbox"/>
1.2.11	Set 'http Secure-server' limit	<input type="checkbox"/>	<input type="checkbox"/>
1.2.12	Set 'exec-timeout' to less than or equal to 10 min on 'ip http'	<input type="checkbox"/>	<input type="checkbox"/>
1.3.1	Set the 'banner-text' for 'banner exec'	<input type="checkbox"/>	<input type="checkbox"/>
1.3.2	Set the 'banner-text' for 'banner login'	<input type="checkbox"/>	<input type="checkbox"/>
1.3.3	Set the 'banner-text' for 'banner motd'	<input type="checkbox"/>	<input type="checkbox"/>
1.3.4	Set the 'banner-text' for 'webauth banner'	<input type="checkbox"/>	<input type="checkbox"/>
1.4.1	Set 'password' for 'enable secret'	<input type="checkbox"/>	<input type="checkbox"/>
1.5.1	Set 'no snmp-server' to disable SNMP when unused	<input type="checkbox"/>	<input type="checkbox"/>
1.5.2	Unset 'private' for 'snmp-server community'	<input type="checkbox"/>	<input type="checkbox"/>
1.5.3	Unset 'public' for 'snmp-server community'	<input type="checkbox"/>	<input type="checkbox"/>
1.5.4	Do not set 'RW' for any 'snmp-server community'	<input type="checkbox"/>	<input type="checkbox"/>
1.5.9	Set 'priv' for each 'snmp-server group' using SNMPv3	<input type="checkbox"/>	<input type="checkbox"/>
1.5.10	Require 'aes 128' as minimum for 'snmp-server user' when using SNMPv3	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1.1.1	Set the 'hostname'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1.1.2	Set the 'ip domain-name'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1.1.3	Set 'modulus' to greater than or equal to 2048 for 'crypto key generate rsa'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1.1.4	Set 'seconds' for 'ip ssh timeout'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1.2	Set version 2 for 'ip ssh version'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.2	Set 'no cdp run'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.3	Set 'no ip bootp server'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.4	Set 'no service dhcp'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.5	Set 'no ip identd'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.6	Set 'service tcp-keepalives-in'	<input type="checkbox"/>	<input type="checkbox"/>

2.1.8	Set 'no service pad'	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1	Create a single 'interface loopback'	<input type="checkbox"/>	<input type="checkbox"/>
2.4.4	Set 'ip tftp source-interface' to the Loopback Interface	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1	Set 'no ip source-route'	<input type="checkbox"/>	<input type="checkbox"/>
3.1.2	Set 'no ip proxy-arp'	<input type="checkbox"/>	<input type="checkbox"/>
3.1.3	Set 'no interface tunnel'	<input type="checkbox"/>	<input type="checkbox"/>
3.1.4	Set 'ip verify unicast source reachable-via'	<input type="checkbox"/>	<input type="checkbox"/>
3.2.1	Set 'ip access-list extended' to Forbid Private Source Addresses from External Networks	<input type="checkbox"/>	<input type="checkbox"/>
3.2.2	Set inbound 'ip access-group' on the External Interface	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1.1	Set 'key chain'	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1.2	Set 'key'	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1.3	Set 'key-string'	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1.4	Set 'address-family ipv4 autonomous-system'	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1.5	Set 'af-interface default'	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1.6	Set 'authentication key-chain'	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1.7	Set 'authentication mode md5'	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1.8	Set 'ip authentication key-chain eigrp'	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1.9	Set 'ip authentication mode eigrp'	<input type="checkbox"/>	<input type="checkbox"/>

IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1	Enable 'aaa new-model'	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2	Enable 'aaa authentication login'	<input type="checkbox"/>	<input type="checkbox"/>
1.1.3	Enable 'aaa authentication enable default'	<input type="checkbox"/>	<input type="checkbox"/>
1.1.4	Set 'login authentication for 'line tty'	<input type="checkbox"/>	<input type="checkbox"/>
1.1.5	Set 'login authentication for 'line vty'	<input type="checkbox"/>	<input type="checkbox"/>
1.1.6	Set 'login authentication for 'ip http'	<input type="checkbox"/>	<input type="checkbox"/>
1.1.7	Set 'aaa accounting' to log all privileged use commands using 'commands 15'	<input type="checkbox"/>	<input type="checkbox"/>
1.1.8	Set 'aaa accounting connection'	<input type="checkbox"/>	<input type="checkbox"/>
1.1.9	Set 'aaa accounting exec'	<input type="checkbox"/>	<input type="checkbox"/>
1.1.10	Set 'aaa accounting network'	<input type="checkbox"/>	<input type="checkbox"/>
1.1.11	Set 'aaa accounting system'	<input type="checkbox"/>	<input type="checkbox"/>
1.2.2	Set 'transport input ssh' for 'line vty' connections	<input type="checkbox"/>	<input type="checkbox"/>
1.2.3	Set 'no exec' for 'line aux 0'	<input type="checkbox"/>	<input type="checkbox"/>

1.2.6	Set 'exec-timeout' to less than or equal to 10 minutes for 'line aux 0'	<input type="checkbox"/>	<input type="checkbox"/>
1.2.7	Set 'exec-timeout' to less than or equal to 10 minutes 'line console 0'	<input type="checkbox"/>	<input type="checkbox"/>
1.2.8	Set 'exec-timeout' less than or equal to 10 minutes 'line tty'	<input type="checkbox"/>	<input type="checkbox"/>
1.2.9	Set 'exec-timeout' to less than or equal to 10 minutes 'line vty'	<input type="checkbox"/>	<input type="checkbox"/>
1.2.10	Set 'transport input none' for 'line aux 0'	<input type="checkbox"/>	<input type="checkbox"/>
1.2.11	Set 'http Secure-server' limit	<input type="checkbox"/>	<input type="checkbox"/>
1.2.12	Set 'exec-timeout' to less than or equal to 10 min on 'ip http'	<input type="checkbox"/>	<input type="checkbox"/>
1.3.1	Set the 'banner-text' for 'banner exec'	<input type="checkbox"/>	<input type="checkbox"/>
1.3.2	Set the 'banner-text' for 'banner login'	<input type="checkbox"/>	<input type="checkbox"/>
1.3.3	Set the 'banner-text' for 'banner motd'	<input type="checkbox"/>	<input type="checkbox"/>
1.3.4	Set the 'banner-text' for 'webauth banner'	<input type="checkbox"/>	<input type="checkbox"/>
1.4.1	Set 'password' for 'enable secret'	<input type="checkbox"/>	<input type="checkbox"/>
1.4.2	Enable 'service password-encryption'	<input type="checkbox"/>	<input type="checkbox"/>
1.4.3	Set 'username secret' for all local users	<input type="checkbox"/>	<input type="checkbox"/>
1.5.1	Set 'no snmp-server' to disable SNMP when unused	<input type="checkbox"/>	<input type="checkbox"/>
1.5.2	Unset 'private' for 'snmp-server community'	<input type="checkbox"/>	<input type="checkbox"/>
1.5.3	Unset 'public' for 'snmp-server community'	<input type="checkbox"/>	<input type="checkbox"/>

1.5.4	Do not set 'RW' for any 'snmp-server community'	<input type="checkbox"/>	<input type="checkbox"/>
1.5.9	Set 'priv' for each 'snmp-server group' using SNMPv3	<input type="checkbox"/>	<input type="checkbox"/>
1.5.10	Require 'aes 128' as minimum for 'snmp-server user' when using SNMPv3	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1.1.1	Set the 'hostname'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1.1.2	Set the 'ip domain-name'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1.1.3	Set 'modulus' to greater than or equal to 2048 for 'crypto key generate rsa'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1.1.4	Set 'seconds' for 'ip ssh timeout'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1.1.5	Set maximum value for 'ip ssh authentication-retries'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1.2	Set version 2 for 'ip ssh version'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.2	Set 'no cdp run'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.3	Set 'no ip bootp server'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.4	Set 'no service dhcp'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.5	Set 'no ip identd'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.6	Set 'service tcp-keepalives-in'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.8	Set 'no service pad'	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1	Set 'logging enable'	<input type="checkbox"/>	<input type="checkbox"/>
2.2.2	Set 'buffer size' for 'logging buffered'	<input type="checkbox"/>	<input type="checkbox"/>

2.2.3	Set 'logging console critical'	<input type="checkbox"/>	<input type="checkbox"/>
2.2.4	Set IP address for 'logging host'	<input type="checkbox"/>	<input type="checkbox"/>
2.2.5	Set 'logging trap informational'	<input type="checkbox"/>	<input type="checkbox"/>
2.2.6	Set 'service timestamps debug datetime'	<input type="checkbox"/>	<input type="checkbox"/>
2.2.7	Set 'logging source interface'	<input type="checkbox"/>	<input type="checkbox"/>
2.2.8	Set 'login success/failure logging'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.1	Set 'ntp authenticate'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.2	Set 'ntp authentication-key'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.3	Set the 'ntp trusted-key'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4	Set 'key' for each 'ntp server'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2	Set 'ip address' for 'ntp server'	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1	Create a single 'interface loopback'	<input type="checkbox"/>	<input type="checkbox"/>
2.4.2	Set AAA 'source-interface'	<input type="checkbox"/>	<input type="checkbox"/>
2.4.3	Set 'ntp source' to Loopback Interface	<input type="checkbox"/>	<input type="checkbox"/>
2.4.4	Set 'ip tftp source-interface' to the Loopback Interface	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1	Set 'no ip source-route'	<input type="checkbox"/>	<input type="checkbox"/>
3.1.2	Set 'no ip proxy-arp'	<input type="checkbox"/>	<input type="checkbox"/>
3.1.3	Set 'no interface tunnel'	<input type="checkbox"/>	<input type="checkbox"/>
3.1.4	Set 'ip verify unicast source reachable-via'	<input type="checkbox"/>	<input type="checkbox"/>
3.2.1	Set 'ip access-list extended' to Forbid Private Source Addresses from External Networks	<input type="checkbox"/>	<input type="checkbox"/>
3.2.2	Set inbound 'ip access-group' on the External Interface	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1.1	Set 'key chain'	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1.2	Set 'key'	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1.3	Set 'key-string'	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1.4	Set 'address-family ipv4 autonomous-system'	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1.5	Set 'af-interface default'	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1.6	Set 'authentication key-chain'	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1.7	Set 'authentication mode md5'	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1.8	Set 'ip authentication key-chain eigrp'	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1.9	Set 'ip authentication mode eigrp'	<input type="checkbox"/>	<input type="checkbox"/>

IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1	Enable 'aaa new-model'	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2	Enable 'aaa authentication login'	<input type="checkbox"/>	<input type="checkbox"/>

1.1.3	Enable 'aaa authentication enable default'	<input type="checkbox"/>	<input type="checkbox"/>
1.1.4	Set 'login authentication for 'line tty'	<input type="checkbox"/>	<input type="checkbox"/>
1.1.5	Set 'login authentication for 'line vty'	<input type="checkbox"/>	<input type="checkbox"/>
1.1.6	Set 'login authentication for 'ip http'	<input type="checkbox"/>	<input type="checkbox"/>
1.1.7	Set 'aaa accounting' to log all privileged use commands using 'commands 15'	<input type="checkbox"/>	<input type="checkbox"/>
1.1.8	Set 'aaa accounting connection'	<input type="checkbox"/>	<input type="checkbox"/>
1.1.9	Set 'aaa accounting exec'	<input type="checkbox"/>	<input type="checkbox"/>
1.1.10	Set 'aaa accounting network'	<input type="checkbox"/>	<input type="checkbox"/>
1.1.11	Set 'aaa accounting system'	<input type="checkbox"/>	<input type="checkbox"/>
1.2.2	Set 'transport input ssh' for 'line vty' connections	<input type="checkbox"/>	<input type="checkbox"/>
1.2.3	Set 'no exec' for 'line aux 0'	<input type="checkbox"/>	<input type="checkbox"/>
1.2.4	Create 'access-list' for use with 'line vty'	<input type="checkbox"/>	<input type="checkbox"/>
1.2.5	Set 'access-class' for 'line vty'	<input type="checkbox"/>	<input type="checkbox"/>
1.2.6	Set 'exec-timeout' to less than or equal to 10 minutes for 'line aux 0'	<input type="checkbox"/>	<input type="checkbox"/>
1.2.7	Set 'exec-timeout' to less than or equal to 10 minutes 'line console 0'	<input type="checkbox"/>	<input type="checkbox"/>
1.2.8	Set 'exec-timeout' less than or equal to 10 minutes 'line tty'	<input type="checkbox"/>	<input type="checkbox"/>
1.2.9	Set 'exec-timeout' to less than or equal to 10 minutes 'line vty'	<input type="checkbox"/>	<input type="checkbox"/>
1.2.10	Set 'transport input none' for 'line aux 0'	<input type="checkbox"/>	<input type="checkbox"/>
1.2.11	Set 'http Secure-server' limit	<input type="checkbox"/>	<input type="checkbox"/>
1.2.12	Set 'exec-timeout' to less than or equal to 10 min on 'ip http'	<input type="checkbox"/>	<input type="checkbox"/>
1.3.1	Set the 'banner-text' for 'banner exec'	<input type="checkbox"/>	<input type="checkbox"/>
1.3.2	Set the 'banner-text' for 'banner login'	<input type="checkbox"/>	<input type="checkbox"/>
1.3.3	Set the 'banner-text' for 'banner motd'	<input type="checkbox"/>	<input type="checkbox"/>
1.3.4	Set the 'banner-text' for 'webauth banner'	<input type="checkbox"/>	<input type="checkbox"/>
1.4.1	Set 'password' for 'enable secret'	<input type="checkbox"/>	<input type="checkbox"/>
1.4.2	Enable 'service password-encryption'	<input type="checkbox"/>	<input type="checkbox"/>
1.4.3	Set 'enable secret' for 'enable secret'	<input type="checkbox"/>	<input type="checkbox"/>
1.5.1	Set 'no snmp-server' to disable SNMP when unused	<input type="checkbox"/>	<input type="checkbox"/>
1.5.2	Unset 'private' for 'snmp-server community'	<input type="checkbox"/>	<input type="checkbox"/>
1.5.3	Unset 'public' for 'snmp-server community'	<input type="checkbox"/>	<input type="checkbox"/>
1.5.4	Do not set 'RW' for any 'snmp-server community'	<input type="checkbox"/>	<input type="checkbox"/>
1.5.5	Set the ACL for each 'snmp-server community'	<input type="checkbox"/>	<input type="checkbox"/>
1.5.6	Create an 'access-list' for use with SNMP	<input type="checkbox"/>	<input type="checkbox"/>
1.5.7	Set 'snmp-server host' when using SNMP	<input type="checkbox"/>	<input type="checkbox"/>
1.5.8	Set 'snmp-server enable traps snmp'	<input type="checkbox"/>	<input type="checkbox"/>

1.5.9	Set 'priv' for each 'snmp-server group' using SNMPv3	<input type="checkbox"/>	<input type="checkbox"/>
1.5.10	Require 'aes 128' as minimum for 'snmp-server user' when using SNMPv3	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1.1.1	Set the 'hostname'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1.1.2	Set the 'ip domain-name'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1.1.3	Set 'modulus' to greater than or equal to 2048 for 'crypto key generate rsa'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1.1.4	Set 'seconds' for 'ip ssh timeout'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1.1.5	Set maximum value for 'ip ssh authentication-retries'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1.2	Set version 2 for 'ip ssh version'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.2	Set 'no cdp run'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.3	Set 'no ip bootp server'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.4	Set 'no service dhcp'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.5	Set 'no ip identd'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.6	Set 'service tcp-keepalives-in'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.8	Set 'no service pad'	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1	Set 'logging enable'	<input type="checkbox"/>	<input type="checkbox"/>
2.2.2	Set 'buffer size' for 'logging buffered'	<input type="checkbox"/>	<input type="checkbox"/>
2.2.3	Set 'logging console critical'	<input type="checkbox"/>	<input type="checkbox"/>
2.2.4	Set IP address for 'logging host'	<input type="checkbox"/>	<input type="checkbox"/>
2.2.5	Set 'logging trap informational'	<input type="checkbox"/>	<input type="checkbox"/>
2.2.6	Set 'service timestamps debug datetime'	<input type="checkbox"/>	<input type="checkbox"/>
2.2.7	Set 'logging source interface'	<input type="checkbox"/>	<input type="checkbox"/>
2.2.8	Set 'login success/failure logging'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.1	Set 'ntp authenticate'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.2	Set 'ntp authentication-key'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.3	Set the 'ntp trusted-key'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4	Set 'key' for each 'ntp server'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2	Set 'ip address' for 'ntp server'	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1	Create a single 'interface loopback'	<input type="checkbox"/>	<input type="checkbox"/>
2.4.2	Set AAA 'source-interface'	<input type="checkbox"/>	<input type="checkbox"/>
2.4.3	Set 'ntp source' to Loopback Interface	<input type="checkbox"/>	<input type="checkbox"/>
2.4.4	Set 'ip tftp source-interface' to the Loopback Interface	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1	Set 'no ip source-route'	<input type="checkbox"/>	<input type="checkbox"/>
3.1.2	Set 'no ip proxy-arp'	<input type="checkbox"/>	<input type="checkbox"/>
3.1.3	Set 'no interface tunnel'	<input type="checkbox"/>	<input type="checkbox"/>
3.1.4	Set 'ip verify unicast source reachable-via'	<input type="checkbox"/>	<input type="checkbox"/>
3.2.1	Set 'ip access-list extended' to Forbid Private Source Addresses from External Networks	<input type="checkbox"/>	<input type="checkbox"/>

3.2.2	Set inbound 'ip access-group' on the External Interface	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1.1	Set 'key chain'	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1.2	Set 'key'	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1.3	Set 'key-string'	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1.4	Set 'address-family ipv4 autonomous-system'	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1.5	Set 'af-interface default'	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1.6	Set 'authentication key-chain'	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1.7	Set 'authentication mode md5'	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1.8	Set 'ip authentication key-chain eigrp'	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1.9	Set 'ip authentication mode eigrp'	<input type="checkbox"/>	<input type="checkbox"/>

Approvals for the next level:

- a. Sign the NDA prior sharing any critical resources
- b. Partner with potential service providers, including appliance or VM based solution. Combine with Firewall and separate DDoS protection; identify which one could be a good fit, as DDoS service is an integrated feature of an NGFW
- c. Prepare a requirement checklist of what needs to be done and which solution can meet our requirement
- d. Provision for PoC
- e. Identify potential to secure IIG, BTS, B-RAS level
- f. Map products, quantity, I/O requirements
- g. Map manpower and their deliverables
- h. Deploy and provide training in parallel
- i. Document every deployment and update the network design

Validity and Document Management

The owner of this document is the CISO of BIG IT Networks, currently Shahab Al Yamin Chawdhury, who must check and, if necessary, update the document as organizational requirement changes.

When evaluating the effectiveness and adequacy of this document, the following criteria needs to be considered:

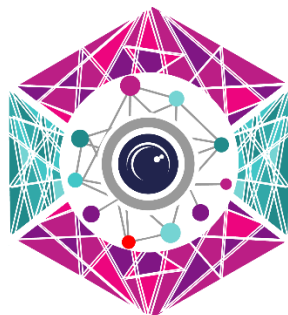
- All IT Team members (IT, NOC, SOC, Ops, Dev, DevOps, DevSecOps, SecOps etc.) are responsible to provide adequate resource access and provide validated documentations or reports either generated from system tools or manually.
- Number of incidents arising from unclear definition of the ITIL scope.
- Number of corrective actions taken due to an inadequately defined ITIL scope.
- Time put in by employees implementing the ITIL to resolve dilemmas concerning the unclear scope.
- Update and approve amendments accordingly, when organizational requirements change or ITIL itself changes its version requirements.

Violations

This plan is devised to fulfill organizational compliance requirements for IT, Dev, SecOps, DevOPS, DevSecOPS, on various levels, anyone in conflict of this approved plan document, will be subjected to the respective policy violations.

Approval and Ownership

Owner	Title	Signature
DDoS Plan Initiator		
Stakeholder		
Stakeholder		
Approved By	Title	Signature
Executive Sponsor		



Big IT Networks

CYBER SECURITY NEED ENDS HERE

DISCLAIMER

The information contained in this document (a) represents different partner's current statement of the features, functions, and capabilities of the products and services described herein, which is subject to change at any time without notice to us, (b) is for our internal evaluation purposes only and should not be interpreted as a binding offer or commitment on the part of BIG IT Networks to provide any product or service described herein; and (c) constitutes BIG IT Networks's trade secret information and may not be disclosed to any third party. Any procurement that may result from this information is subject to negotiation and execution of a definitive agreement between customer and its chosen authorized BIG IT Networks reseller incorporating applicable commercial terms. BIG IT Networks does not guarantee the accuracy of any information presented and assumes no liability arising from our use of the information. BIG IT NETWORKS MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

The descriptions of other companies' products in this document, if any, are provided only as a convenience to us. Any such references should not be considered an endorsement or support by BIG IT Networks or any other companies. BIG IT Networks cannot guarantee their accuracy, and the products may change over time. Also, the descriptions are intended as brief highlights to aid understanding, rather than as thorough coverage. For authoritative descriptions of these products, please consult their respective manufacturers.

All trademarks are the property of their respective companies.

©2024 BIG IT Networks, All rights reserved.