How to protect networks, services and users from terabit-level DDoS attacks

DDoS protection requirements for the cloud, 5G and IoT era

White paper

Since we entered the era of the cloud, 5G and the Internet of Things (IoT), terabit-level distributed denial of service (DDoS) attacks have increased in frequency, impact and sophistication. Moreover, since 2022, botnet-generated DDoS has become the dominant type. How bad is the problem? What is causing it? And what can you do to protect your network, services and users?

Read this white paper for answers to these questions.

Contents

Welcome to the terabit era of DDoS attacks	3
What is DDoS?	3
Volumetric DDoS attacks	3
Botnet DDoS	3
Damage from attacks	4
Motivation for attacks	4
The scale of the DDoS problem today	5
Types of DDoS attacks	8
Approaches to DDoS security	10
DDoS detection	10
DDoS mitigation	10
Challenges with current approaches to DDoS security	11
Protection limited to a select few customers or systems	11
Inability to scale	11
Performance degradation	11
Exorbitant cost to scale	12
The growing impact of DDoS attacks	12
Expanded threat and attack surface	12
Increased bandwidth	13
More malware and IoT bots	13
Availability of DDoS toolkits and DDoS for hire	13
Sophistication of new DDoS techniques	13
New DDoS protection requirements for the cloud, 5G and IoT era	14
Protection for everything and everyone	14
Real-time detection with better accuracy	14
Cost-effective, agile, terabit-level mitigation	14
Automation	15
The Nokia approach to DDoS protection	15
Summary	16
Learn more	16
References	17
Abbreviations	17

Welcome to the terabit era of DDoS attacks

In the era of the cloud, 5G and the Internet of Things (IoT), networks matter more than ever. They are critical for business, from manufacturing and supply chains to logistics. They are also critical for the functioning of society, from energy and resources to transportation and the public sector.

As networks have grown in importance, distributed denial of service (DDoS) attacks have also grown —in number, frequency, intensity and sophistication.

What is DDoS?

Distributed Denial of Service or DDoS is malicious traffic that aims to deny access or degrade or stop connectivity for individual users, internet hosts and service provider network infrastructure.

Malicious players have been exploiting IP protocol and systems vulnerabilities for more than a couple of decades to launch DDoS attacks on their targets: network hosts and systems. Some protocols, such as BGP and Domain Name System (DNS), have gained additional security features to make them more robust. Also, industry-wide initiatives using best practices have been implemented to curb DDoS traffic. However, many hosts still use protocols that rely on open principles set by the internet community a long time ago. Some of them never envisaged malicious exploits that could jeopardize the intended operation of router-based networks.

DDoS is another type of IP network traffic—albeit a malicious kind—that has been used to disrupt servers, services or even entire networks by saturating them with a high volume of traffic or high intensity of packets, and flooding internet systems and devices with a high frequency of malformed requests – to confuse them or render them inoperable. The 'distributed' nature of DDoS refers to the fact that DDoS traffic emanates from different locations, which is a result of IP spoofing – techniques used to hide originating IP addresses.

Volumetric DDoS attacks

Of particular concern, because of their damage potential are volumetric attacks — which comprise more than 95 percent of all DDoS traffic. These attacks have increased dramatically in recent years and, around 2016, we entered the era of terabit-level DDoS attacks.

Volumetric attacks can appear as high-bandwidth attacks, described by their bandwidth and expressed in bits per second (b/s). These attacks aim to exhaust transmission capacity by the sheer volume of traffic.

Alternatively, volumetric attacks can appear as high packet-rate attacks, described by their packet intensity and expressed in packets per second (pps). These attacks aim to exhaust the processing capacity of network hosts and other network elements such as routers.

In 2020, both Amazon and Akamai reported high-bandwidth and high packet-intensity attacks. In May of that year, Amazon experienced a 2.3 Tb/s attack. The next month, Akamai reported an attack of 809 Mpps (418 Gb/s).

Botnet DDoS

At the core of most DDoS attacks today are botnets. A botnet is a collection of compromised sets of individual devices – home computers, routers, IP cameras, digital video recorders (DVRs) and even parking meters – end-user devices commonly called bots or zombies because they have been taken over by hackers. The infected machines are usually triggered from a command center - a compromised server or a remote computer used by a hacker or cybercriminal. Once the attack commences, the bots target service or resource with a deluge of traffic, connection requests, malformed packets and messages drowning the system, making it inoperable or degrading its service significantly.

Damage from attacks

DDoS attacks spare no one. Targets range from individual users to networks belonging to service providers, cloud builders and large digital enterprises.

While most DDoS attacks are a nuisance (e.g., to individual gamers), the bandwidth representing high-bandwidth and high packet-intensity volumetric attacks is cause for concern. These attacks can inflict damage on connectivity and service availability and result in damages costing hundreds of thousands or even millions of dollars in production and operational losses.

There are also legal costs. And it's difficult even to put a price on reputational damage.

Some segments, such as banking, insurance and healthcare, can also be subject to high regulatory fines. In August 2020, an attack on the New Zealand Stock Exchange left the exchange out of service for four days and incurred significant monetary loss and a warning from the country's financial regulator.

On May 4, 2021, a Belgian network provider providing connectivity services to the government, including remote learning and COVID-19 vaccines registration, was hit by a DDoS attack originating from 257,000 IP addresses from 29 countries — leaving many customers without vital connectivity.

It's worth noting that although some big attacks get the headlines, many attacks go unreported because service providers do not want to expose details about their security capabilities or vulnerabilities. Even worse, many attacks go undetected or are reported by users on social media.

Motivation for attacks

The motivation for DDoS attacks varies widely; while some attacks are just a nuisance, others are tools to achieve various goals.

Online gamers do it to win a round of a game as well as get an adrenaline rush.

Hacker activists called "hacktivists" are motivated by ideology and have a political or social agenda.

Extortion is common, with perpetrators using DDoS attacks — or the threat of attacks — to demand ransom from individuals or corporations (ransom DDoS). In some cases, DDoS attacks are combined with other malware attacks used to obfuscate or hide the real attack.

DDoS attacks are made easier with the advent of DDoS-for-hire services and the wider use of cryptocurrency. They have gone from being an annoyance to causing major business and service disruptions. As attack ROI and incentives increase, so do attackers' skill sets.

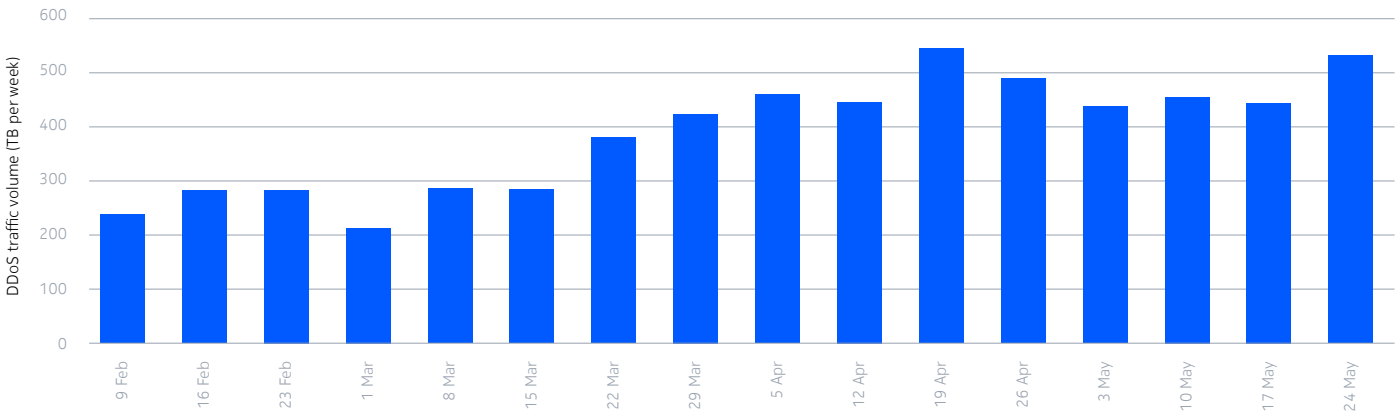
The scale of the DDoS problem today

DDoS attacks have become a daily reality for most networks. Looking at the aggregate DDoS volume levels shows the constant threat to service providers.

DDoS traffic rose significantly in 2020. As shown in Figure 1, in the short period from early February to late May, aggregate DDoS volume levels in the United States rose by more than 40 percent.

Note: The data in Figure 1 were aggregated across multiple US service providers.

Figure 1. Weekly DDoS traffic February - May 2020



Source: Nokia Deepfield Network Intelligence Report, 2020, Page 43.

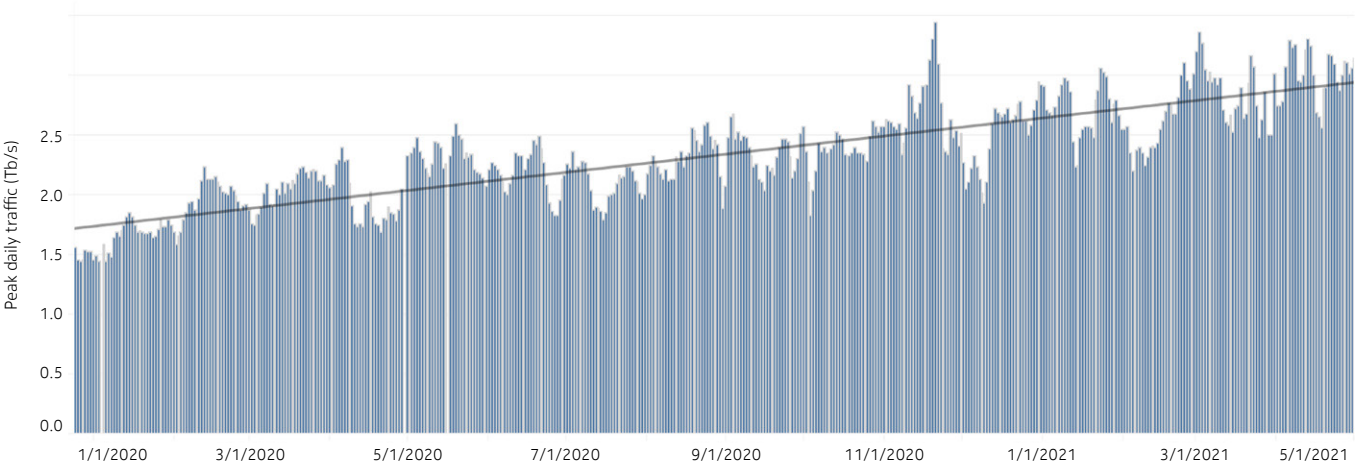
Some might argue that this percentage is skewed because it covered the first wave of the COVID-19 pandemic and lockdowns, when remote work increased significantly, schools and universities went online, and people connected via video conferences (when they weren't gaming or streaming videos).

However, the situation appears even worse when compared over a longer term and globally. As shown in Figure 2, daily DDoS peaks have more than doubled in a little over a year.

In January of 2020, average daily 5-minute peaks were at 1.5 Tb/s. By May 2021, the average daily peaks exceeded 3.0 Tb/s.[1]

1 Nokia Deepfield analysis looking at peak daily DDoS traffic (amplification, reflection and spoofed flood traffic) across a number of service providers of different types (global transit, residential broadband, regional providers, webscale, hosting etc.) from January 2020 to May 2021.

Figure 2. Peak daily DDoS traffic January 2020 - May 2021 across select service providers

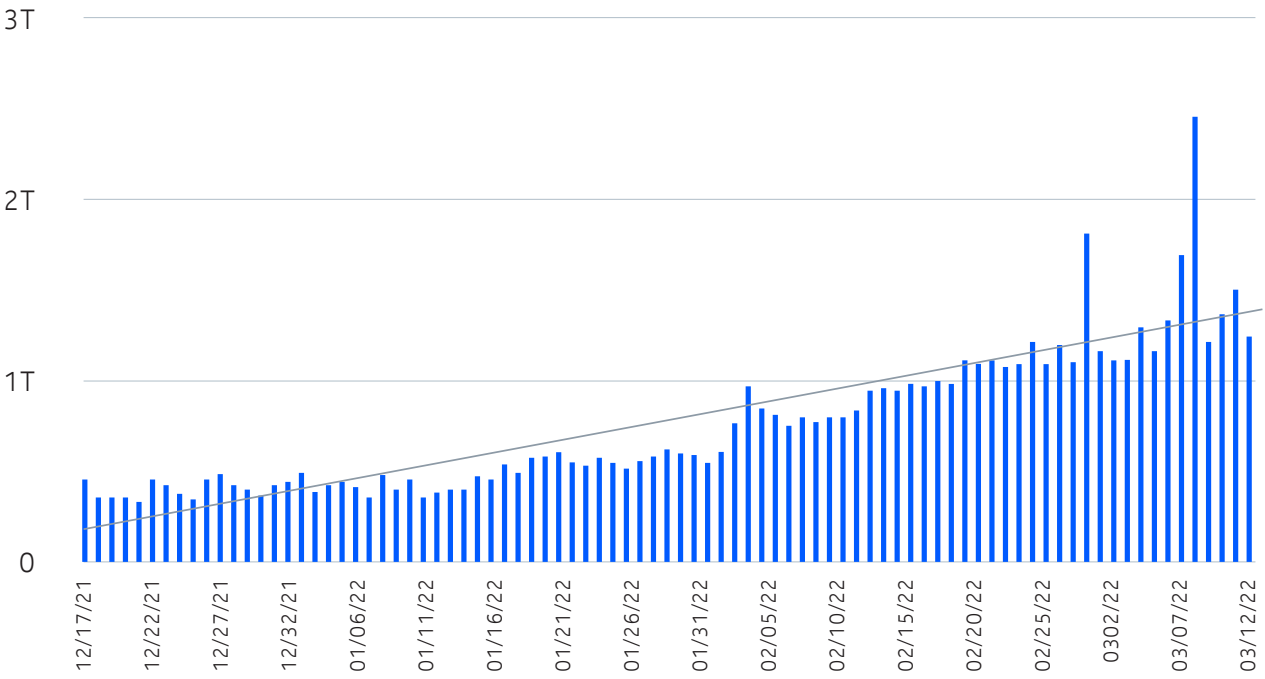


Source: Nokia Deepfield, May 2021.

The ubiquitous presence of DDoS traffic in networks today continues to worry many businesses and has become a paramount concern for service providers, cloud builders and large digital enterprises.

DDoS traffic is growing faster than video or other types of internet content. Figure 3 shows the growth of DDoS daily peaks in 2022. From this graph, one can observe that terabit-level attacks have become a daily occurrence.

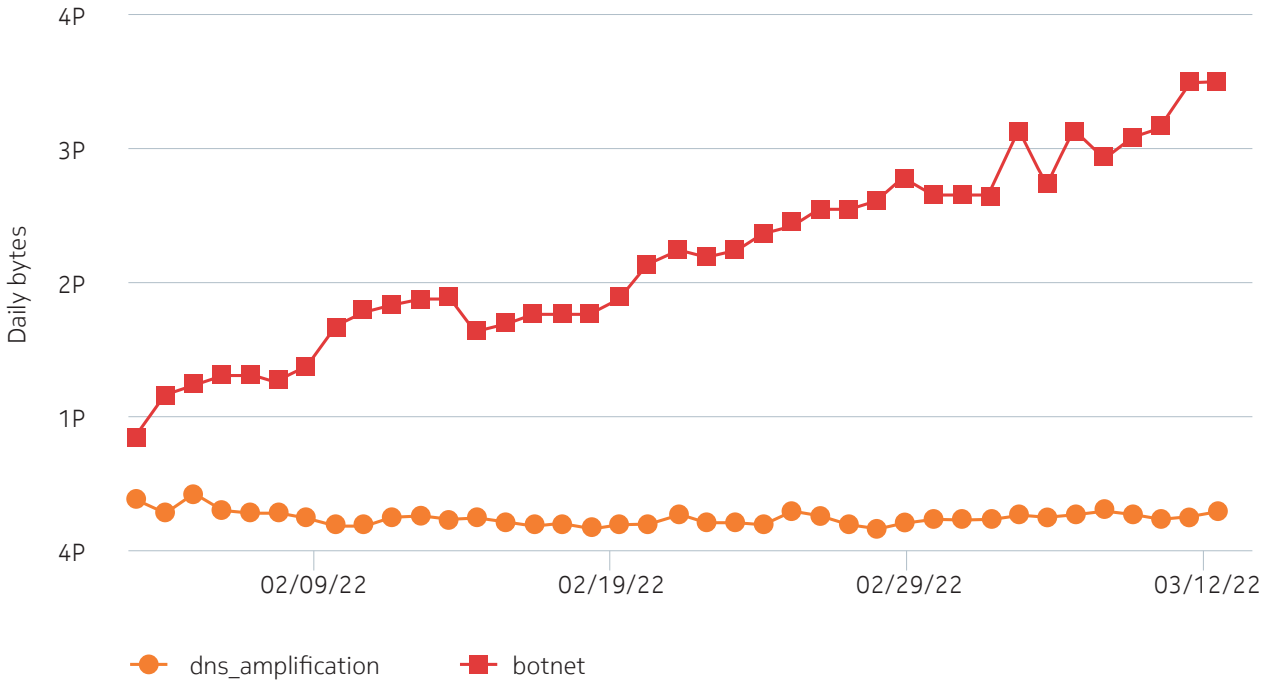
Figure 3. Daily DDoS peaks in Tb/s (December 2021 – March 2022).



Source: Data from Nokia Deepfield collaborating customers.

Botnet DDoS is one type of traffic that has exhibited significant growth since mid-2021. In the second half of the year, in marked contrast to the pre-IoT era, most of the largest DDoS attacks exclusively leveraged large-scale botnets. Today, botnet DDoS is the source of tens of thousands of attacks daily, each involving anywhere between several thousand and several million IP addresses. It is estimated that more than 500,000 active bots are engaged in these attacks.[2]

Figure 4. Comparison between botnet DDoS and DNS amplification (February-March 2022)



2 Source: Nokia Deepfield, May 2023

Types of DDoS attacks

DDoS has been exploiting IP protocol and systems vulnerabilities for over two decades. Some protocols, such as Domain Name System (DNS), have gained additional security features (though these features have not been deployed extensively). However, many protocols still rely on open principles set by the internet community a long time ago.

What are the different types of DDoS?

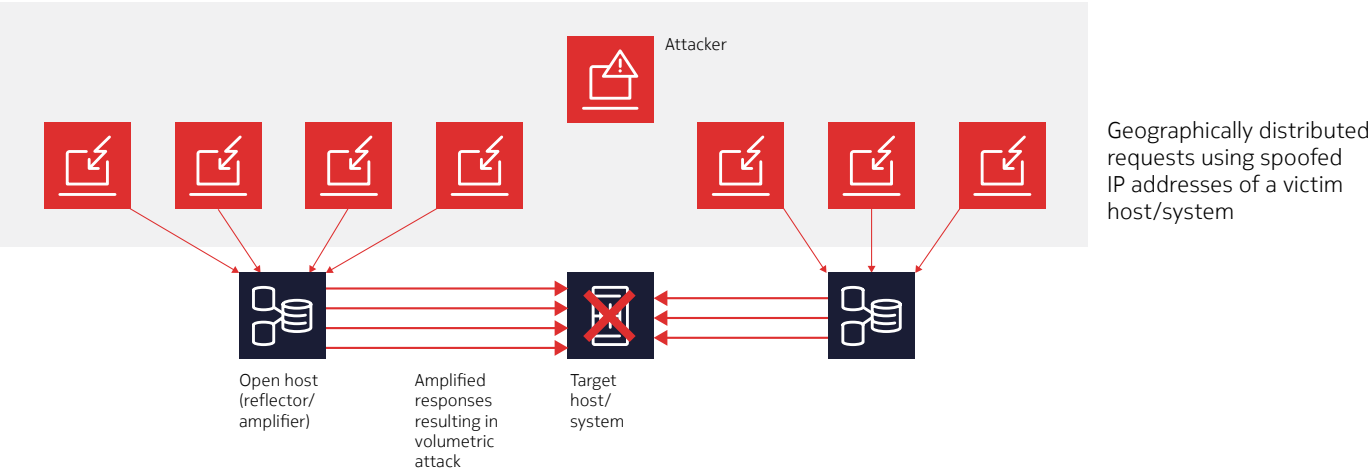
Broadly, all DDoS traffic can be categorized into:

- Amplification and reflection DDoS
- Flooding DDoS traffic (using IP address spoofing or IP header modification, IPHM)
- Application-level DDoS.

Amplification vectors are responsible for all the largest publicly reported DDoS attacks. Most commonly, attackers leverage misconfigured internet services (e.g., DNS, CLDAP or NTP servers) to amplify small 40 to 60-byte attack streams to divert multi-megabyte responses to target systems. The main benefit of amplification for attackers is that they require relatively modest attack resources (server, bandwidth, etc.) to generate a much larger response – in terms of bandwidth (expressed in bits per second, bps) and packet intensity (expressed in packets per second, pps). Amplification attacks typically target routers or upstream link bandwidth (bps or pps) on the path to the target system(s). These attacks are also called volumetric and generally rely on IP address spoofing to hide the originator's IP address(es). Amplification and reflection of responses to spoofed IP traffic can lead to a high volume of traffic going to victims' systems.

Figure 5 shows a reflection/amplification DDoS attack using spoofed, geographically distributed requests.

Figure 5. Reflection and amplification attack using spoofed requests



IP Header Modification (IPHM) flooding attacks are types of attacks that generate floods of specific types of traffic. IPHM here refers to modifying the headers of originating IP packets to obfuscate the origin. This is often referred to as "spoofing" (of IP address).

Most flooding attacks have been generated mostly by "booters" – websites specialized in offering web-based "DDoS services for hire." Booters rent or buy servers in IPHM-friendly hosting companies that would allow IPHM or tolerate such services. Rather than first sending traffic to reflectors/amplifiers, IPHM floods send synthetic traffic floods directly to the target system(s). (We call this traffic synthetic because it is artificially created for DDoS. Direct floods to target systems provide more flexibility in attack payload than amplifiers, as attackers can control all elements of the IP header and payload.)

Booters typically use IPHM to launch high cardinality IP address/session attacks targeting the stateful nature of firewalls or load balancers. Our research and emergency response teams regularly see IPHM flooding attacks, including tens or hundreds of millions of unique forged source IP addresses and headers.

As with amplification and IPHM attacks, booters use hundreds of names to describe the same basic botnet/application attack vectors.

Finally, there are **application-level DDoS attacks**. Application-level attacks are aimed at state exhaustion of the target system at the application level (also called L4-L7 attacks). These higher protocol-level DDoS attacks employ irregular protocol message exchanges to confuse and saturate servers. These include SYN floods and fragmented packet attacks.

Application-level attacks are aimed at state exhaustion of the target system. Attack types include low-and-slow attacks, GET/POST floods, and other attacks targeting specific servers or hosts.

Recent new DDoS techniques such as **carpet bombing** use an extended range of IP addresses as targets (instead of an IP address of a single host) or hide the "real" attack in a range of simultaneous attacks (e.g., a bits-and-pieces attack).

Botnet-generated DDoS represents the largest majority of DDoS today and poses the fastest growing and most significant DDoS threat to service providers and data center networks.

While botnets are responsible for some of the largest high-bandwidth and high packet-intensity DDoS attacks (volumetric attacks) today, botnets also generate the majority of application-level attacks. Botnet DDoS brings significant new challenges to DDoS detection and mitigation.

Approaches to DDoS security

The great variety of DDoS techniques and continued efforts to combine/evolve them and change attack dynamics make DDoS detection and mitigation very challenging.

Legacy DDoS detection and mitigation approaches that used to be effective no longer work.

DDoS detection

Historically, DDoS detection was done using tools and technologies that provide additional insight into traffic and services: dedicated hardware network probes, inline traffic processing and deep packet inspection (DPI) technology. Detection techniques focused on recognizing known traffic patterns of DDoS traffic or monitoring traffic volumes for irregularities.

This approach evolved to the distributed gathering of DDoS intelligence: obtaining insights from a network of distributed data plane probes (hardware or software). This information was passed to a centralized location for further processing.

When a specific threat or attack was detected, the knowledge about that threat/attack was then disseminated to all network-wide data collection points to be added to their localized knowledge bases and used for localized DDoS mitigation.

DDoS detection techniques and approaches have included:

- DDoS signature analysis
- Heuristic and behavioral analysis
- Traffic anomalies monitoring
- Analysis of traffic packet samples.

DDoS mitigation

Because DDoS traffic manifests itself at the network level, network-level protection using IP addresses has been the main protection mechanism.

DDoS mitigation techniques included DNS-based blocking, but DNS-based protection can be circumvented easily. More effective approaches have focused on IP address-based filtering.

Filtering techniques have included:

- Inline mitigation
- Remotely triggered blackhole routing (RTBH)
- BGP Flowspec
- Traffic scrubbing.

Challenges with current approaches to DDoS security

There are several challenges with the current approaches to DDoS security:

- Protection limited to a select few customers or systems
- Inability to scale
- Performance degradation
- Exorbitant cost to scale.

Protection limited to a select few customers or systems

Traditionally, DDoS protection has been offered only to the most valuable and demanding customers or the most critical systems in the network. The concept of a select number of "monitored objects" dictated this strategy. The result was selective DDoS protection capabilities.

This approach left many small and medium enterprises and residential broadband customers without comprehensive DDoS protection.

Now that "always-on" broadband connectivity is becoming a must for everyone, DDoS protection must extend to the whole network and all services, systems and customers.

Inability to scale

The proliferation of new and distributed network architectures such as content delivery networks (CDNs) and edge cloud) and the introduction of internet protocol exchange (IPX) points have expanded the number of systems and interfaces and greatly increased connectivity. This, in turn, has raised the number of interfaces and endpoints that can be affected by DDoS.

The number of IP flows that need to be monitored for anomalies and malicious activity has also increased exponentially.

The challenge of monitoring the wider and more dynamic network environment for a much larger and ever-evolving threat landscape makes current DDoS detection and mitigation approaches inadequate for the cloud, 5G and IoT era.

Performance degradation

BGP Flowspec provided a framework for DDoS mitigation through improved filtering and policing capabilities across BGP peering routers. However, until now, BGP Flowspec has not been widely adopted for DDoS mitigation for two main reasons:

- A service provider needs to have BGP Flowspec-capable routers with Flowspec activated on them. Many providers have had concerns about performance degradation on routers that need to perform many more tasks (e.g., Flowspec filtering) in addition to their core routing functions. In addition, Flowspec announcements need to be carefully programmed on routers.

  Misconfiguration or incorrect order of BGP Flowspec announcements can impact services or even other service providers. One example is the Century Link outage, which resulted in widespread collateral damage.
- By the time routers become advanced enough to have minimal performance degradation when Flowspec is running, and service providers became comfortable using it, DDoS had evolved so much that only a very dynamic application of very large sets of access control list (ACL) filters is now adequate for comprehensive DDoS protection.

As a result, Flowspec is an effective and viable DDoS mitigation approach, but only if DDoS detection is agile enough to create or activate large sets of ACL filters and if routers engaged in DDoS mitigation can install and remove those ACLs filters in real time. In addition, NETCONF has appeared as another option that can facilitate the agile activation of large ACL sets on routers.

Exorbitant cost to scale

One approach that has become a de-facto standard for fighting DDoS, based on the use of scrubbing centers, has been severely challenged by the exponential rise in network traffic, including volumetric DDoS threats. This rise requires the proportional scaling of scrubbing centers. The continual addition of required capacity in the scrubbing centers is becoming cost-prohibitive.

Scrubbing also introduces additional latency because all traffic sent to scrubbing centers must be processed and cleaned. Finally, scrubbing introduces additional costs related to backhauling network traffic — from the network to scrubbers and back.

Cost efficiency is a paramount concern for service providers and cloud builders as they work to reduce the overall costs of DDoS protection, especially as they aim to drive down a key metric: the cost per protected customer or protected network infrastructure object.

The growing impact of DDoS attacks

Historically, most DDoS attacks have been from the internet, across peering and transit links. These are called inbound or ingress DDoS attacks.

Now, however, a growing number of attacks originate from within service providers' networks and are aimed at targets within the network or outside of it. These are called outbound or egress attacks.

Many attacks are also launched from cloud infrastructures as insecure loads that may be hosted in data centers.

Several factors are driving the increased severity and damage caused by DDoS attacks:

- Expanded threat and attack surface
- Increased bandwidth
- More malware and IoT bots
- Availability of DDoS toolkits and DDoS for hire
- Sophistication of new DDoS techniques.

Expanded threat and attack surface

DDoS threats and attacks are becoming common and more damaging in the era of the cloud, 5G and the IoT.

The growth of all-IP networks has extended the security perimeter and expanded the threat and attack surface. The number of IP addresses has grown exponentially because of new technologies and services. Examples of these new technologies include:

- Localized content delivery networks that deliver streaming services
- Connecting cloud points of presence (PoPs) in new metro architectures
- 5G adoption of edge cloud architectures such as Multi-access Edge Computing (MEC).

This expanded threat and attack surface allows threats known for more than a decade, such as combined amplification and reflection attacks (e.g., DNS/NTP/TCP reflection attacks), to aim at a wider range of targets.

Increased bandwidth

Today's users have broadband connections ranging from tens of megabits to gigabits. This increased bandwidth is available to all users and devices, including malicious users and DDoS-capable devices that launch and orchestrate DDoS attacks.

Combining individual high-bandwidth connections with well-known reflection and amplification techniques can easily result in terabit-level attacks and high packet-intensity attacks that employ millions of packets per second.

The sheer volume of attack traffic can take a victim's system out of service, degrade its performance, or make its services unavailable. This allows for much larger and more damaging attacks. Volumetric attacks can simultaneously affect thousands or millions of users.

The rollout of technologies such as 5G, fiber-to-the-home (FTTH) and DOCSIS 4.0 with continued and accelerated delivery of gigabit access speeds will provide additional power for DDoS attacks.

More malware and IoT bots

The huge proliferation of IoT devices also includes many devices with substandard or default security that can easily be compromised.

Nokia Threat Intelligence Center's research shows that it can take only minutes for an insecure IoT device with a public IP address to be compromised and potentially be used as a remotely controlled device ("bot") that can be exploited in a DDoS attack.

With high projected IoT growth, these bots (and botnets created out of them) represent a significant threat potential for increased frequency and impact of DDoS attacks.

Availability of DDoS toolkits and DDoS for hire

Throughout the darknet (areas of the internet that mostly act as criminal marketplaces) and advertised in online gaming circles, there is a growing number of websites where DDoS toolkits can be downloaded, or DDoS services can be hired for a low fee.

These toolkits and usage of DDoS-as-a-service put the destructive power into the hands of a broader set of malicious actors to launch DDoS attacks.

Sophistication of new DDoS techniques

Attackers use combinations of attack techniques and vectors to "shape-shift" their attacks, changing the mix and intensity of DDoS attacks over time and across different parts of the network.

New DDoS protection requirements for the cloud, 5G and IoT era

A new, forward-looking approach to DDoS protection is vital to overall network security. The DDoS defense must be context-aware to protect from the new generation of threats.

The DDoS defense must provide cloud-era visibility beyond IP addresses and include visibility into services, CDNs, websites and IoT devices. Finally, an effective defense must be flexible and capable of detecting new and emerging threats as they develop and evolve.

Hybrid network architectures, combining physical and virtualized network domains, are proliferating and creating even more distributed sets of network boundaries that need to be monitored for both ingress and egress DDoS.

With the increased number of endpoints that need to be protected — customers, end devices and systems, plus network infrastructure — DDoS security must deliver improved performance with scalability and automation.

The DDoS threats of today and tomorrow demand a whole new way of thinking about DDoS protection.

Protection for everything and everyone

The new global networking environment, with its ever-evolving technologies, requires a new type of protection that will encompass all customers, services and the network infrastructure. This is a major paradigm shift from the legacy approach in which DDoS protection was reserved for the most valuable and demanding customers and critical network entities.

In addition to protecting the hosts and servers, next-generation DDoS protection must include the ability to monitor network infrastructure within the entire network perimeter, from the peering edge to centralized and distributed data centers to the service edge.

DDoS protection also needs to encompass aggregation networks that serve wireline and wireless access.

Most importantly, DDoS protection must cover the majority of customers — or all customers — and protect them from attacks from any direction.

Attacks aimed at service provider infrastructure are also rising, so providers need to be able to protect their entire IP infrastructure:

- All systems that enable connectivity and provide services
- Wherever systems are located: In the access/edge/backbone network; in cloud data centers, where servers host CDNs and other services; in a software-defined network; and in hybrid network domains.

Real-time detection with better accuracy

Next-generation DDoS security must detect DDoS threats and attacks in real time with improved accuracy, resulting in a lower percentage of false positives and negatives.

Cost-effective, agile, terabit-level mitigation

Protection against the most damaging DDoS attacks needs to minimize the impact of DDoS traffic on target and victim systems and users.

DDoS protection also needs to limit the side-effects on the network: congestion of network bandwidth by wasteful and malicious traffic.

In addition, DDoS protection needs to scale across the whole network — and cost-effectively so that costs do not increase in line with bandwidth.

Automation

A forward-looking DDoS solution for millions of users, services and network infrastructure entities must be able to scale operationally. This will only be possible with a solution that allows automated mitigation of complex security policies to drive real-time surgical removal of DDoS threats and attacks.

The Nokia approach to DDoS protection

The Nokia Deepfield DDoS solution combines the power of Nokia Deepfield big-data IP analytics with high-performance IP networks to protect the whole network from all volumetric DDoS attacks, at a petabyte-level scale, with zero-touch automation.

The Deepfield DDoS solution is composed of:

- Deepfield Defender: Highly scalable software system which uses big data-driven analytics for real-time DDoS detection, detailed reporting and agile mitigation
- Deepfield Secure Genome®: Up-to-date, detailed, internet-related security data feed for improved DDoS detection accuracy
- An advanced, high-performance IP network (based on sophisticated and programmable routers such as FP4, FP5 or FPcx-based Nokia IP routers.
- Next-generation DDoS mitigation system – Nokia 7750 Defender Mitigation System.

The Nokia DDoS solution provides 360-degree protection for your whole network, all services and all users. The solution equips service providers, cloud builders and large digital enterprises with advanced security capabilities to minimize the threats and impact of DDoS attacks. It is an element of Nokia IP network security – a visionary approach that embeds security into the DNA of every layer of our IP network infrastructure, providing high-performance, fully-featured and at-scale protection for your mission-critical IP networks.

Summary

In the cloud, 5G and Internet of Things (IoT) era, we have also entered the era of terabit-level distributed denial of service (DDoS) attacks.

DDoS attacks have grown, both in number and in their frequency, intensity and sophistication. There are application-level, protocol-level, and, worst of all, volumetric attacks — which comprise more than 95 percent of all DDoS traffic. Botnet DDoS has grown to be a major source of DDoS attacks, generating terabit-level attacks daily in many networks worldwide.

Current approaches to DDoS detection and mitigation present several challenges. They protect only a select number of customers or systems. They result in performance degradation. They aren't scalable — and even if they were, the cost would be exorbitant.

A new, forward-looking approach to DDoS protection is required. To protect from the new generation of threats, the DDoS defense must:

- Protect everything and everyone
- Provide real-time detection with better accuracy
- Deliver cost-effective, agile, terabit-level mitigation
- Automate mitigation of complex security policies to drive real-time surgical removal of DDoS threats and attacks.

The Nokia Deepfield DDoS solution provides 360-degree protection for your whole network, all services and all users — to equip you with advanced security capabilities that minimize the threats and impact of DDoS attacks.

Learn more

To learn more about the Nokia approach to DDoS protection:

- Visit the Deepfield Defender web page
- Read the Deepfield Defender datasheet
- Learn more about Nokia IP Network Security.

References

1. DDoS in 2021 Nokia Deepfield report, February 2022
2. Belnet: More than 250,000 IP addresses from 29 countries used to launch a cyberattack (article). RTBF.BE, May 5, 2021.
3. CenturyLink outage led to a 3.5% drop in global web traffic (article). ZDNet, August 30, 2020.
4. How a Dated Cyber-Attack Brought a Stock Exchange to its Knees (article). Bloomberg Businessweek, February 4, 2021.
5. Nokia Deepfield Network Intelligence Report, 2020.
6. Nokia Threat Intelligence Report 2021, November 2021.

Abbreviations

ACL	access control list
BGP	Border Gateway Protocol
CDN	content delivery network
DDoS	distributed denial of service
DNS	Domain Name System
Flowspec	flow specification
ICMP	Internet Control Message Protocol
IoT	Internet of Things
NTP	Network Time Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

Nokia OYJ
Karakaari 7
02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Document code: CID210500 (September)