Distributed Denial of Service

WHITE PAPER

DDoS Attack Emulation Solutions

CONTENTS

Executive Summary

The need for Distributed Denial-of-Service (DDoS) mitigation and protection for enterprises has gained tremendous significance as a failure to deal with the attacks can affect revenue, productivity, reputation, and user loyalty. With DDoS attacks increasing both in size and complexity, an organization needs a DDoS protection service with a robust network and variety of mitigation techniques to stop any attacks directed at the site. Thus, it is vital to properly deploy DDoS mitigations into enterprises, cloud providers, telecom operators, ISPs, etc. More importantly, these solutions must be thoroughly tested and verified before deployment.

This whitepaper provides a solution from Xena Networks to emulate various extreme-volume DDoS attacks that can place any security solutions under extreme attacks for testing and verification purpose.

DDoS - Major Network Security Threat

Distributed Denial-of-Service (DDoS) attack is a growing threat to business around the world with no sign of abating any time soon. Globally, there was a 776% growth in attacks between 100 Gbps and 400 Gbps YOY from 2018 to 2019, and the total number of DDoS attacks will double from 7.9 million in 2018 to 15.4 million by 2023 [1]. It is estimated that DDoS attacks can make up as much as 10 percent of a country's total internet traffic according to 2016 Visual Networking Index report from Cisco Systems. With the prediction of 14% compound annual growth rate (CAGR), by 2023, the global DDoS attacks can increase up to 15.4 million, 2-fold increase from 2018, as shown in Figure 1.

DDoS attackers use multiple hosts to overwhelm a target with bogus traffic. The network is paralyzed due to the overwhelmed servers, network links or devices (firewalls, routers, switches, etc.), and this can cost the victim millions of dollars. The average size of DDoS attacks is increasing progressively and approaching 1 Gbps with the peak size reaching 500 Gbps in 2015 - enough to bring most organizations offline completely. DDoS attacks not only target individual websites at the edge of the network but also the network infrastructure, such as the aggregating or core routers and switches, or the Domain Name System (DNS) servers in provider networks. These attacks can cause more serious damages due to the size and scale of the victim network.

Many companies are heavily dependent on the internet. Information is stored in the cloud for ubiquitous access and sharing. Mobile apps and websites are developed for user experience and expanding market shares. Financial transactions and mobile payments are processed online. Logistics is monitored and tracked through the internet. Businesses are moving from offline to online. For today's business, a top-notch customer experience is critical for success. That requires providing rich and responsive access to online services through the internet infrastructure.

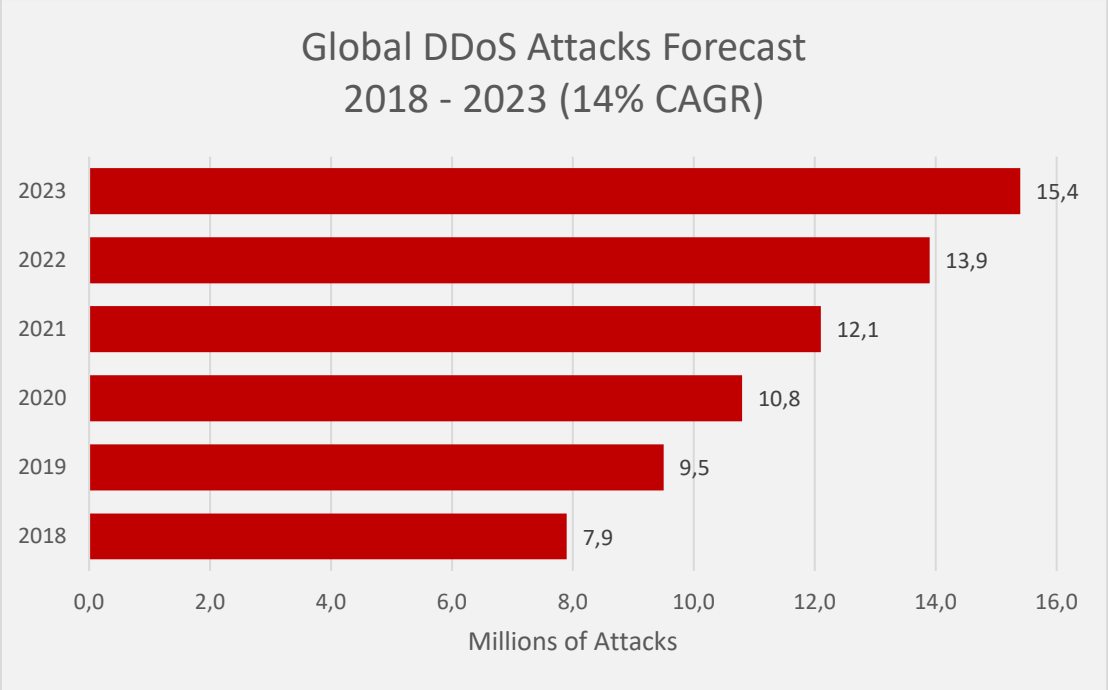


Figure 1: Number of DDoS attacks: Attacks will double to 15.4 million by 2023 globally

Source: Cisco Annual Internet Report, 2018-2023 [1]

DDoS attacks drastically impact access, no matter how much you invest in high-quality mobile experience for users or in data security and availability. By flooding servers with garbage requests to consume network and computing resources, DDoS attacks can slow down or completely bring down server performance, preventing users from accessing the services they need. If the users cannot access their accounts or data on the servers, there is zero experience and zero usage. From the customer perspective, the services appear unstable and potentially insecure. This can result in a huge loss of customers and business.

Since DDoS attacks originate from multiple hosts across the internet and sometimes looks legitimate to the network operator, it is difficult to block once launched. Thus, the number one priority is to test and verify any DDoS defense and mitigation systems before rolling out services to customers.

Different Types of DDoS Attacks

Any network attack that attempts to make a machine or network resource inaccessible to its intended users can be categorized as a Denial-of-Service (DoS) attack. DoS attacks accomplish this by flooding the target with bogus traffic or sending it information that triggers a crash. When a DoS attack employs very large numbers of attacking computers to overwhelm the target with bogus traffic, it is called a DDoS attack. To achieve the necessary scale, DDoS are often performed by botnets which can co-op millions of infected machines to unknowingly participate in the attack, even though they are not the target of the attack itself.

To test any DDoS protection solutions, **it requires the testing solution be able to emulate various types of DDoS at extremely high volume and bandwidth**. Failing to do so, the DDoS testing traffic can be incapable of placing necessary pressure, thus resulting in unsatisfactory test results. Here are some major types of DDoS attacks that a test solution should be able to emulate:

TCP-based	SYN Flood
	SYN-ACK Flood
	ACK & PUSH ACK Flood
UDP-based	UDP Flood
	UDP Fragmentation
IP-based	Ping of Death
	Ping Flood
	Smurf Attack
	ARP Spoofing
	Teardrop Attack

SYN Flood

A SYN flood is a denial-of-service (DoS) attack that relies on abusing the standard way that a TCP connection is established. Typically, a client sends a SYN packet to an open port on a server asking for a TCP connection. The server then acknowledges the connection by sending SYN-ACK packet back to the client. The client responds to the server with an ACK packet establishing the connection. This process is commonly known as a "three-way handshake".

A SYN flood overwhelms a target machine by sending thousands of connection requests to it using spoofed IP addresses. This causes the target to attempt to open a connection for each malicious request and subsequently wait for an ACK packet that never arrives. A server under a SYN flood attack will continue to wait for a SYN-ACK packet for each connection request. However, the massive number of half-open connections quickly fills up the server's internal table before it can time out any connections out. This process continues for as long as the flood attack continues.

Attackers will sometimes add legitimate information to their requests as well, such as sequence number or source port 0, as this increases a target server's CPU usage on top of causing network congestion and could more effectively cause a DoS condition.

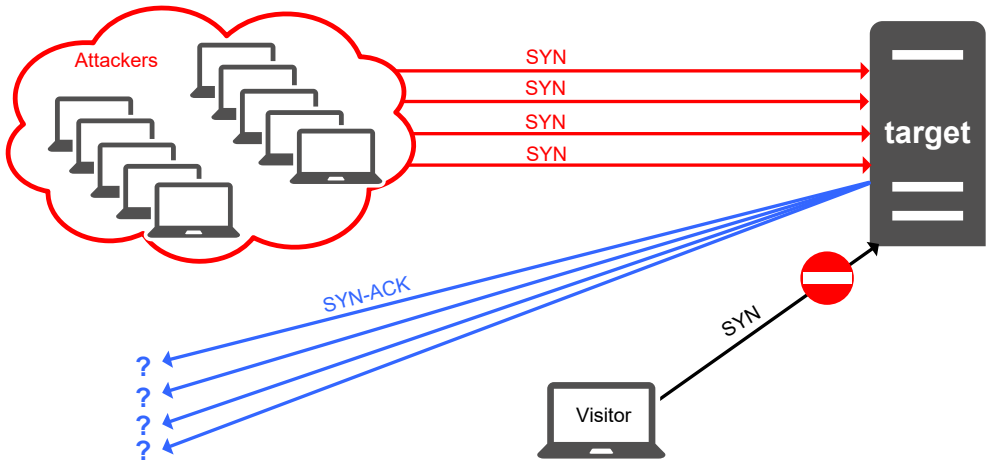


Figure 2: TCP SYN flood attack

SYN-ACK Flood

A SYN-ACK flood is an attack method that involves sending a target server spoofed SYN-ACK packet at a high rate. Because a server requires significant processing power to understand why it is receiving such packets out-of-order (not in accordance with the normal SYN, SYN-ACK, ACK three-way handshake mechanism), it can become so busy handling the attack traffic, that it cannot handle legitimate traffic and hence the attackers achieve a denial-of-service condition.

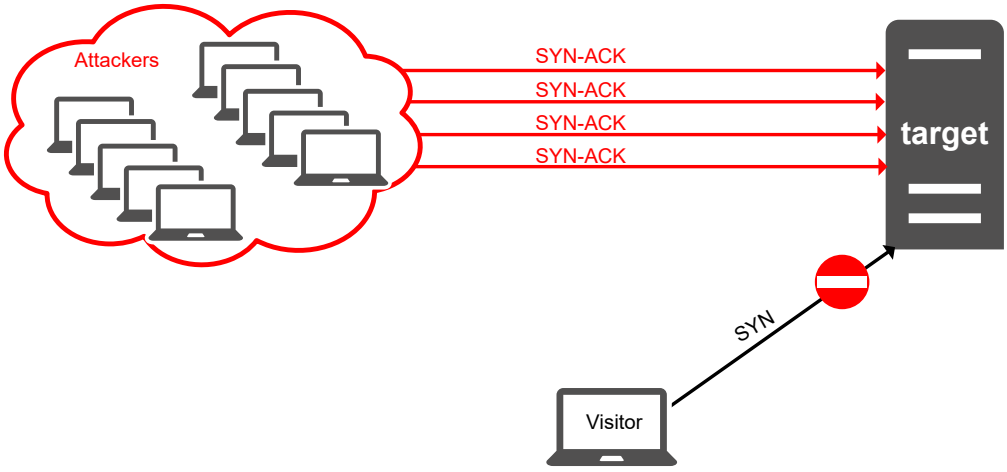


Figure 3: SYN-ACK flood attack

ACK & PUSH ACK Flood

When the connection between the host and the ACK or the PUSH ACK client is established, packets are used to transfer information both ways until the session is closed. The target server attacked by an ACK flood receives fake ACK packets that do not belong to any of the sessions on the server's list of transmissions. The server under attack then wastes all its system resources trying to define where the fabricated packets belong. This results in productivity loss and partial server unavailability.

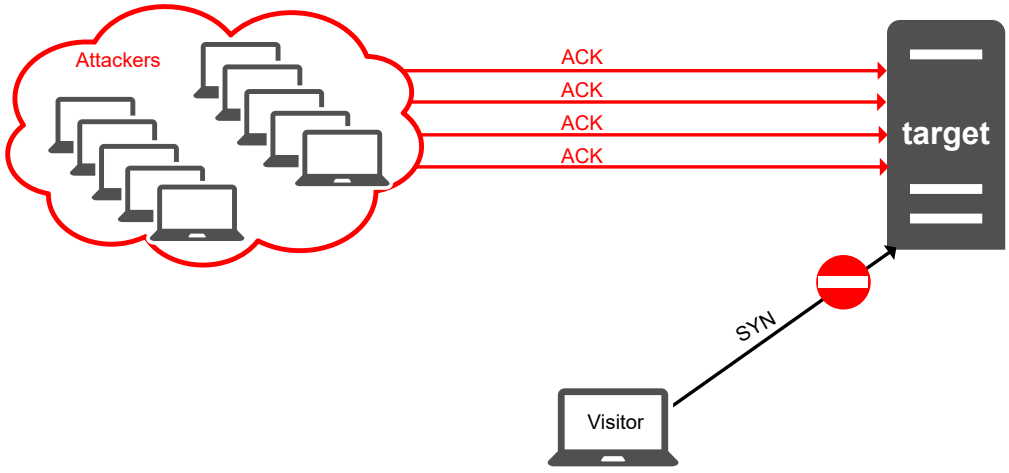


Figure 4: ACK flood attack

TCP Sequence Prediction Attack

A TCP sequence prediction attack is an attack that predicts the sequence number used to identify the packets in a TCP connection, which can be used to counterfeit packets. The attacker hopes to correctly guess the sequence number to be used by the sending host. If they can do this, they will be able to send counterfeit packets to the receiving host which will seem to originate from the sending host, even though the counterfeit packets may in fact originate from some third host controlled by the attacker.

If an attacker can deliver counterfeit packets of this sort, they can cause various sorts of mischief, including injecting data of the attacker's choosing into an existing TCP connection, and prematurely closing existing TCP connections by injecting counterfeit packets with the RST bit set.

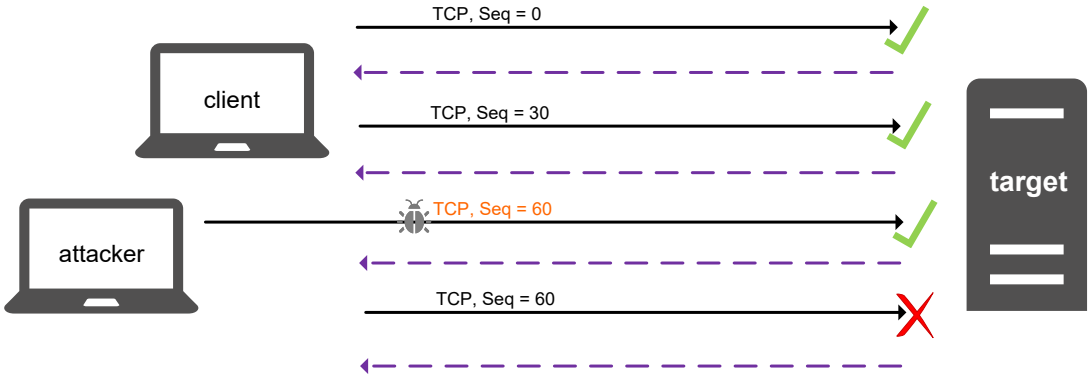


Figure 8: TCP sequence prediction attack

UDP Flood Attack

This DoS attack uses the User Datagram Protocol (UDP), a connectionless computer networking protocol, to send a large number of UDP packets to random ports on a remote host. The target host checks for the application listening at that port, and replies with an ICMP Destination Unreachable packet if the host

cannot find the application. This forces the target host to transmit excessive ICMP packets, eventually making it unreachable by other clients. The attackers can also spoof the IP address of the UDP packets to ensure the returned ICMP packets do not arrive.

At the most basic level, most operating systems try to mitigate UDP flood attacks by limiting the rate of ICMP responses. UDP mitigation also relies on firewalls to filter out unwanted network traffic. The potential victim will not receive or respond to the malicious UDP packets if the firewall can stop them. However, as firewalls are stateful devices, i.e. can only keep a limited number of sessions due to memory constrains, they can also be vulnerable to flood attacks.

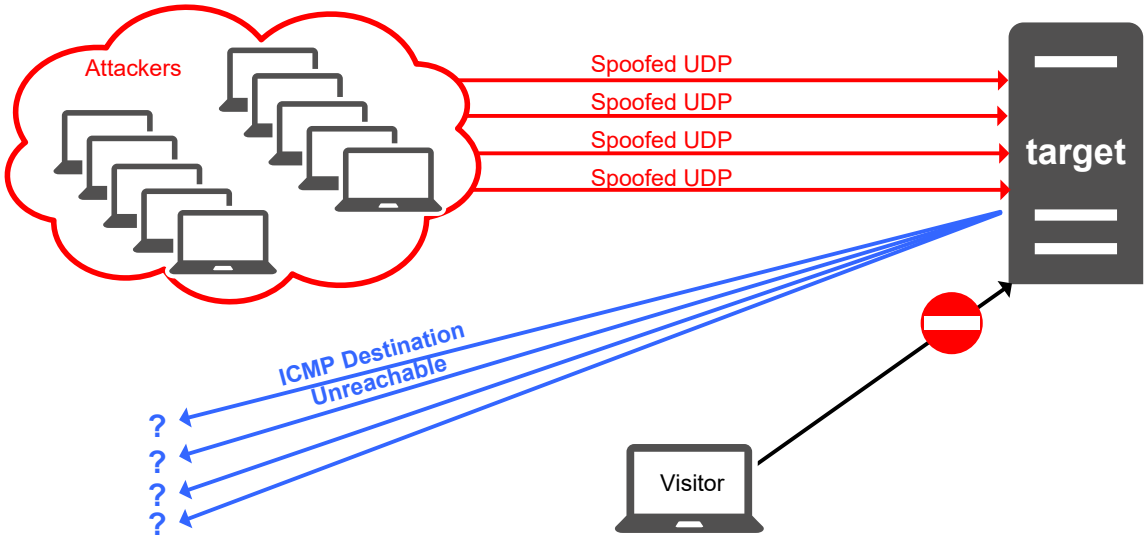


Figure 5: UDP flood attack

UDP Fragmentation

In a UDP Fragmentation attack, attackers send large UDP packets (1500+ bytes) to consume more bandwidth with fewer packets. Since these fragmented packets are normally forged and have no ability to be reassembled, the victim's resources will receive these packets which can possibly consume significant CPU resources. Firewall will begin to indiscriminately drop all good and bad traffic to the destination server being flooded. Some firewalls perform an Early Random Drop process blocking both good and bad traffic. SYN floods are often used to potentially consume all network bandwidth and negatively impact routers, firewalls, IPS/IDS, SLB, WAF as well as the victim servers.

Ping of Death

Ping of Death is a type of DoS attack where the attacker tries to crash the targeted computer or system by sending malformed or malicious ping packets. The correct size of a ping packet is typically 56 bytes. However, any IPv4 packet can be as large as 65,535 bytes. Some historical computer systems simply could not handle larger packets, and would crash if they received one. Since sending a ping packet larger than 65,535 bytes violates the Internet Protocol, attackers would usually send malformed packets in fragments. When fragmentation is performed, each IP fragment needs to carry information about which part of the original IP packet it contains. This information is kept in the Fragment Offset field, in the IP header. When the target system attempts to reassemble the fragments and ends up with an oversized packet, buffer overflow could occur, causing a system crash and potentially allowing the injection of malicious code.

Ping of Death attacks were particularly effective because the attacker's identity could be easily spoofed. A Ping of Death attacker needs no detailed knowledge of the targeted machine, except for its IP address. The problem described above in fact has nothing to do with ICMP, which is used only as the payload. The problem lies in the reassembly process of IP fragments, which may contain any type of protocol.

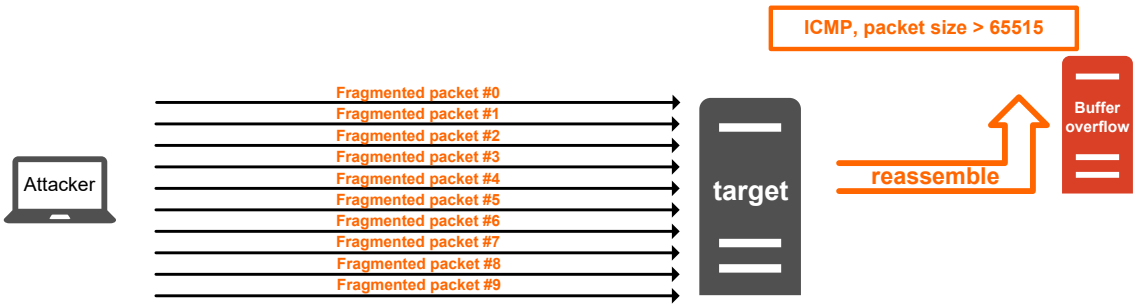


Figure 6: Ping of Death attack

Ping Flood

A ping food attack is a simple DoS attack where the attacker overwhelms the targeted host with ICMP Echo Request (ping) packets. This attack works most effectively by sending ICMP packets as fast as possible without waiting for replies. It is most successful if the attacker has more bandwidth than the victim. This attack seeks to overwhelm the targeted host's ability to respond – consume enough of its CPU cycles for a user to notice a significant slowdown – thereby blocking valid requests.

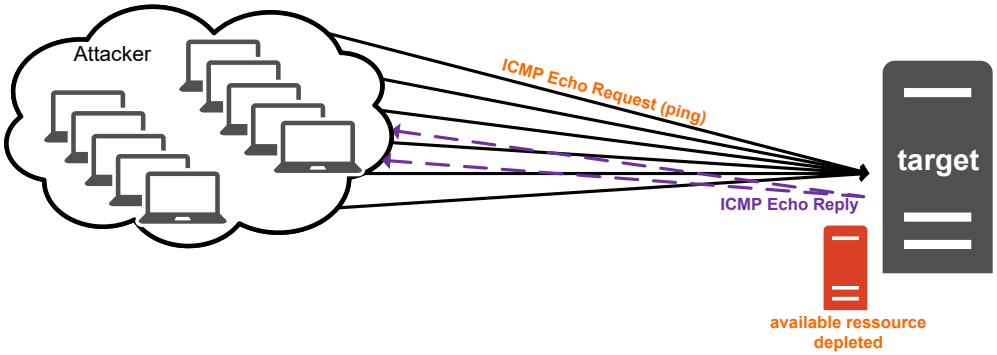


Figure 7: Ping flood attack

Smurf Attack

Smurf attack is a type of DDoS attack in which larger numbers of ICMP packets with the intended victim's spoofed source IP address are broadcast to a computer network using an IP broadcast address. By default, most devices on the network will respond by sending a reply to the source IP address. When the number of devices is larger, the victim's computer will be flooded with replying traffic. This will render the targeted host unresponsive.

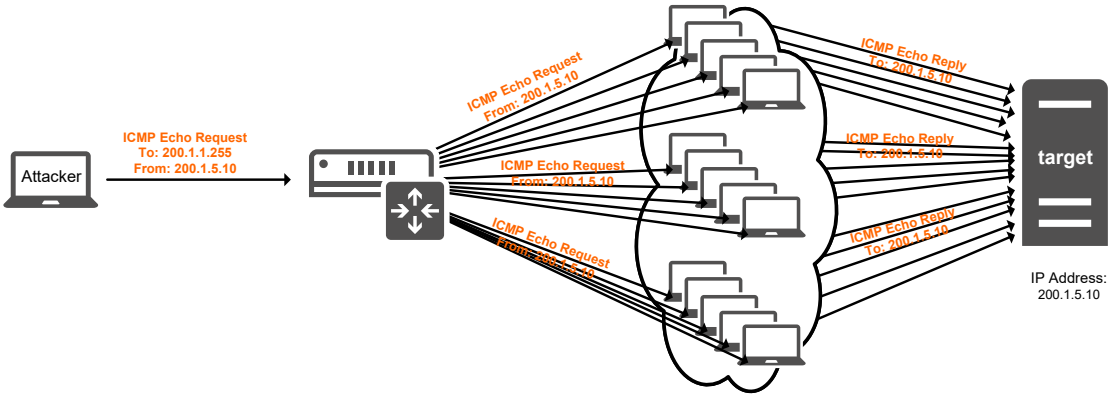


Figure 8: Smurf attack

ARP Spoofing

ARP spoofing, ARP poison routing, or ARP cache poisoning, are all types of attacks where an attacker sends spoofed Address Resolution Protocol (ARP) messages to a local area network (LAN). The aim is to associate the attacker's MAC address with the IP address of another host, such as the default gateway, resulting in any traffic bound for that IP address to be sent to the attacker instead.

ARP spoofing attacks are extremely easy to carry out as long as the attacker has control of a machine within the target LAN or is directly connected to it as the ARP protocol was designed for efficiency not for security. ARP spoofing may allow an attacker to intercept data frames on a network, modify the traffic, or stop all traffic, as an opening for other attacks such as man in the middle (MITM), denial of service, or session hijacking.

Defenses against ARP spoofing include static ARP entries and ARP spoofing detection. Static ARP solution requests that the IP-to-MAC address mappings in the local ARP cache be statically configured so the host ignores all ARP replay packets. ARP spoofing detection generally relies on some form of certification or cross-checking of ARP responses. Uncertified ARP responses are blocked. These techniques may be integrated with the DHCP server so that both dynamic and static IP addresses are certified. This capability may be implemented in individual hosts or may be integrated into Ethernet switches or other network equipment.

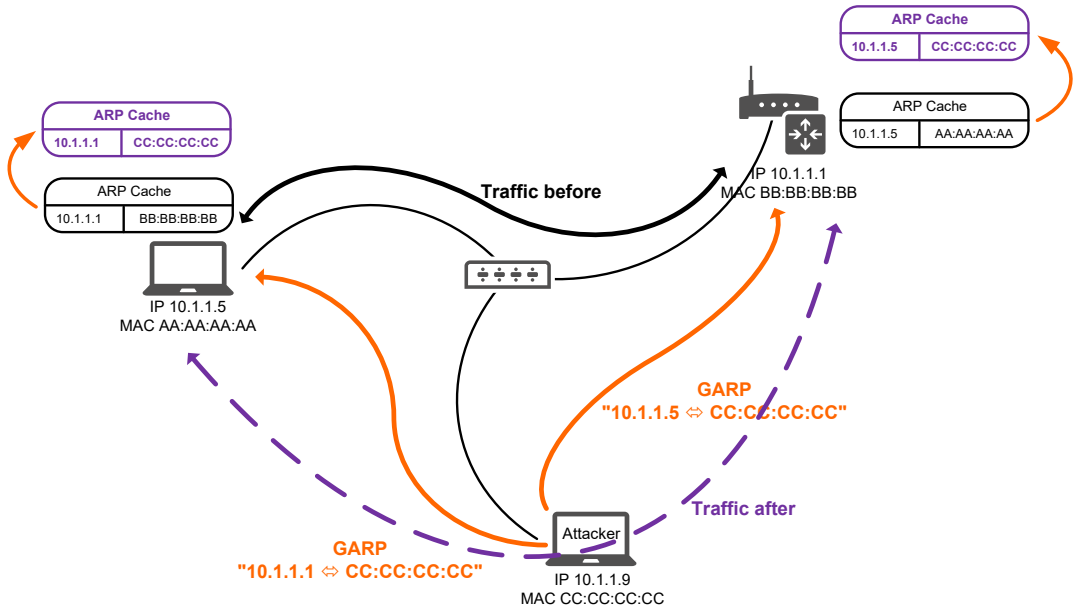


Figure 8: ARP spoofing

Teardrop Attack (IP/ICMP Fragmentation Attack)

A teardrop attack is a DoS attack that involves sending fragmented packets to a target machine. Since the target receiving such packets cannot reassemble them due to a bug in TCP/IP fragmentation reassembly, the packets overlap one another, crashing the target network device.

IP fragmentation is the process of breaking up a single Internet Protocol (IP) datagram into multiple packets of smaller size because every network link has a characteristic size of messages that can be transmitted, called the maximum transmission unit (MTU). The IP layer in the network protocol stack is responsible for the transmission of packets between network endpoints, which includes fragmentation of larger packets into small ones for the supporting datalink frames. The 13-bit Fragment Offset field in the IP header specifies the fragment's position within the original datagram, measured in 8-byte units.

The teardrop attack occurs when two fragments contained within the same IP datagram have offsets that indicate that they overlap each other in positioning within the datagram. This could mean that either fragment A is being completely overwritten by fragment B, or that fragment A is partially being overwritten by fragment B. Some operating systems do not properly handle fragments that overlap in this manner. As a result, the data packets overlap and quickly overwhelm the victim's servers, causing them to fail.

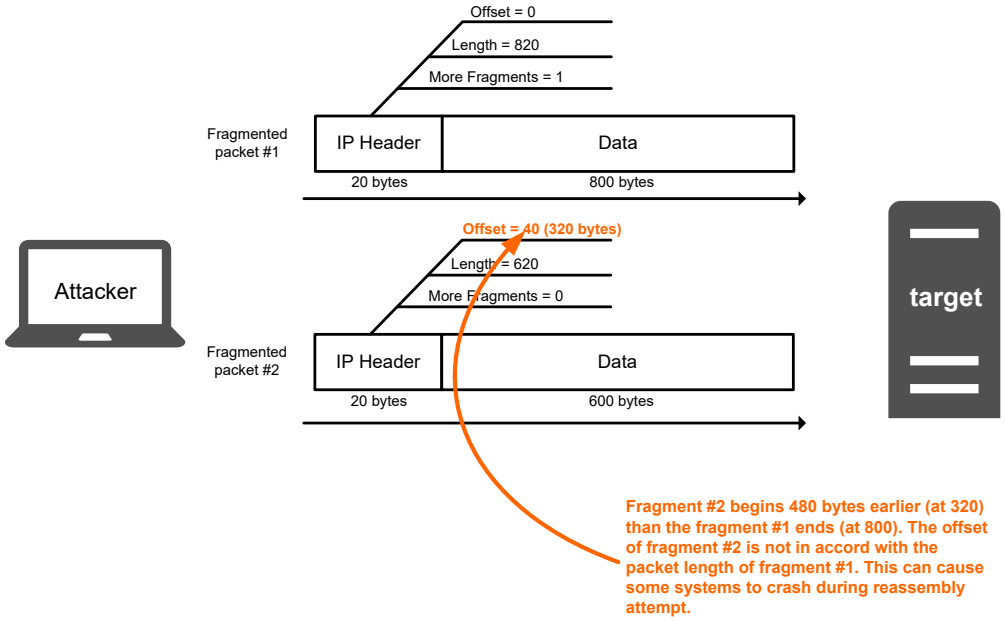
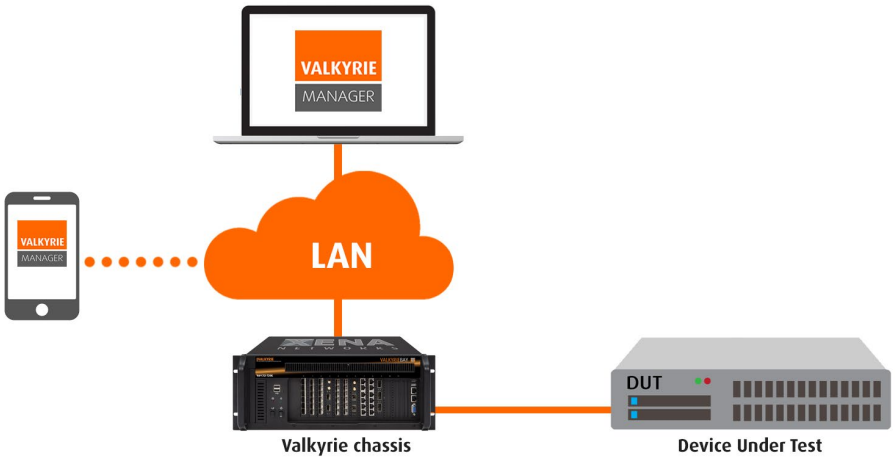


Figure 8: Teardrop attack

Xena Valkyrie DDoS Emulation Solution

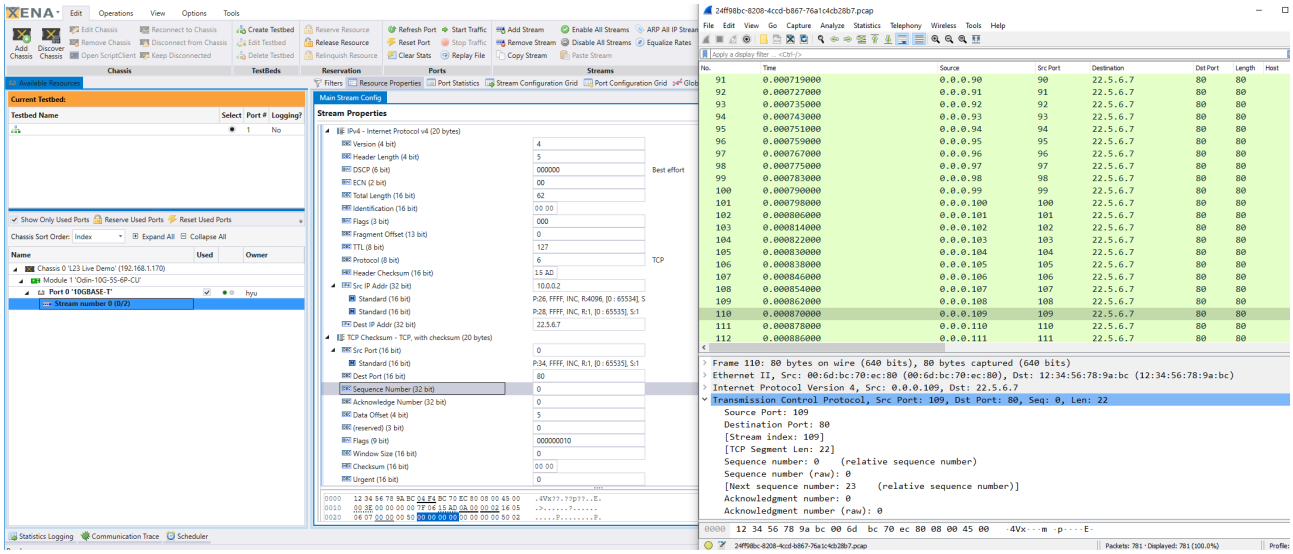
To test any DDoS protection solutions, **it requires the testing solution be able to emulate various types of DDoS at extremely high volume and bandwidth**. Failing to do so, the DDoS testing traffic can be incapable of placing necessary pressure, thus resulting in unsatisfactory test results. With Xena Valkyrie test and analysis platform, users can emulate DDoS attacks with extremely high volume and bandwidth.



Valkyrie is a full-featured Layer 2-3 stateless traffic generator and analysis platform. It is used to configure and generate Ethernet traffic up at all speeds up to 400GE and analyze how network devices and services perform in response, making it perfect for most lab-based data-plane test scenarios. Valkyrie offers a choice of two chassis that can be equipped with an extensive range of copper and optical Gigabit Ethernet test modules supporting all Ethernet speeds up to 400GE, including 2.5GE, 5GE, 25GE and 50GE. The chassis

and test modules are controlled via ValkyrieManager, a Windows GUI client provided for ad-hoc test execution, and remote management of test equipment located in multiple locations.

Xena offers a complete test solution for DDoS mitigation on e.g. firewalls, routers, and servers, based on its high-performance network test and measurement products. For example, the user can simply configure a stream and use field modifiers to emulate 4096 x 65536 (268,435,456) IP addresses bombarding TCP SYN at any port speed, from 100M to 400GE. This massive emulated attack will be able to test the functional performance of a DDoS mitigation solution and push the DUT to its limit.



In terms of DDoS emulation, Xena is capable of:

- Importing captured traffic as a template.
- Blasting user-defined packet streams from layer 2 up to layer 7.
- Transmitting and receiving traffic at rates ranging from a few Kbps to 100 Gbps.
- Real-time analysis and reporting.
- Ready-to-use port configuration files, step-by-step guidelines, and pcap examples

Importing Captured Traffic as Template

Users can emulate a basic types of DDoS attacks at low transmission rate, e.g. ping the target from one IP address, and capture the traffic into a pcap file. This file can then be imported into the Xena Valkyrie platform that will parse and analyze the file and generate a packet template based on the user's selection. The simple attack packet thus becomes the template for a more complex DDoS attack.

Packets can be completely configured by users, or Ethernet, Ethernet II, VLAN, ARP, IPv4, IPv6, UDP, TCP, LLC, SNAP, GTP, ICMP, RTP, RTCP, STP, SCTP, MPLS, PBB, FCoE, IGMPv2/3, or fully user-specified. Any field in a packet template can be set to an invalid value for negative testing.

Blasting User-Defined DDoS Attack Traffic

Xena Valkyrie allows up to six field modifiers to be applied to any field in a packet, per stream. A field modifier can be set to increment or decrement or be random within a specified range. The modifiers can be chained together so that a simple attack can grow into a complex distributed attack with various combinations. For instance, the user can add a modifier to the source IP address of the ICMP Echo Request (ping) packet and randomize it. This lets the user generate a large amount of distributed ping traffic towards a single destination – the ping flood attack is therefore ready.

Transmitting and Receiving Traffic at Different Rates

With well-defined traffic, users can select different bandwidth distribution, constant (uniform) or burst distributions. Traffic loads can be specified as percentages of line rate, frames per second, or Mbps. For example, if the link is a 100G link, the user can set the traffic load to 50% with constant bandwidth and generate a ping flood attack at 50 Gbps.

Real-Time Analysis

Packets can be captured and exported for further analysis using WireShark. Triggers and filters can be set up to trigger on specific events, and to capture packets meeting particular criteria. Multiple capture criteria can be specified using AND/OR expressions.

Ready-to-Use Port Configuration Files, Guidelines, and Pcap Examples

Xena Valkyrie offers port configuration files for the basic DDoS attacks. User can download these configuration files from Xena's support website and import to the test ports. The configurations can be adjusted as needed after importing, depending on different scenarios or requirements.

In addition to the port configuration files, there are step-by-step guides for users to download. These guides offer detailed information about each DDoS attack and how to configure DDoS streams using the pcap examples provided.

Conclusion

DDoS attacks will continue to grow in both scale and severity. Our ever-increasing dependence on the internet make businesses vulnerable to malicious attacks. As the cost of attacks rise, various DDoS mitigation and network security solutions, products, and systems are developed.

The battle against DDoS attack shows no sign of diminishing. On the contrary, firewalls, routers and servers require constant upgrades to patch bugs and improve security. Thus, benchmarking test and verification of these products become vital.

Xena Valkyrie test platform delivers extreme performance for DDoS attack emulation, and also provides ready-to-use port configuration files, step-by-step guides and pcap examples to help users quickly learn and configure DDoS attack streams for testing.

Going beyond generating DDoS traffic, Xena helps companies performance test their security products, find performance flaws, so the companies can ensure business continuity and preserve business integrity with strong protection solutions.

>> Request for FREE Valkyrie demo

>> Book a FREE consultation with an Xena expert

References

[1] Cisco Annual Internet Report (2018–2023) White Paper, https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html