Anti-DDoS

Software-Defined Perimeter as a DDoS Prevention Mechanism

The permanent and official location for Software Defined Perimeter Working Group is https://cloudsecurityalliance.org/research/working-groups/software-defined-perimeter/

Acknowledgments

Lead Authors:

Juanita Koilpillai
Jason Garbis
Michael Roza
Nya Murray

CSA Global Staff:

Shamun Mahmud

The Software Defined Perimeter (SDP) Working Group is a Cloud Security Alliance (CSA) research working group with the goal of developing a solution to stop network attacks against application infrastructure. Formed in 2013, the working group designed elements in a control channel-based architecture using standard proven security components. They published a research artifact to determine if there was interest in the concept and called it SDP. The working group research was and will continue to be freely available for use without license fees or restrictions by the CSA.

Table of Contents

Introduction

DDoS and DoS Attacks Defined

A Distributed Denial-of-Service (DDoS) attack is a large-scale attack in which the perpetrator uses more than one unique source IP address (often thousands of them) to launch simultaneous attacks against a target. The goal is to overload the service (or its network), preventing it from being able to deliver its intended services. Since the incoming traffic flooding the victim originates from many different sources, it is impossible to stop the attack by using simple techniques such as ingress filtering or source blacklisting. This also makes it very difficult to distinguish legitimate user traffic from attack traffic when spread across so many points of origin. Some DDoS attacks involve forging IP sender addresses (IP address spoofing), further complicating efforts to identify and defend against the attack[1].

A Denial-of-Service (DoS) is an attack from a single source while as stated above DDoS is an attack from many sources. Both types of attacks are illustrated in the figure below.

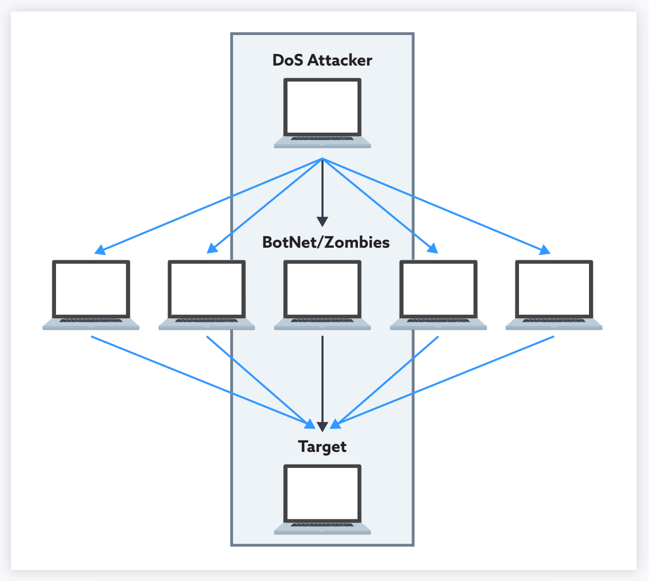


Figure 1: Distinction between DoS and DDoS attacks

Throughout the remainder of this white paper, we will refer only to DDoS attacks, but much of what follows can be applied to DoS attacks as well.

DDoS is ultimately about overwhelming a target and preventing it from delivering its services to legitimate users. DDoS attacks are typically performed against public-facing services running on the internet, such as web servers and DNS servers.

[1] https://en.wikipedia.org/wiki/Denial-of-service_attack

DDoS is and continues to be a problem as identified by the following recent surveys:

> - According to [https://securelist.com/ddos-report-q1-2019/90792/], between Q1 and Q2 of 2019, "statistics show that all DDoS attack indicators increased last quarter. The total number of attacks climbed by 84%, and the number of sustained (over 60 minutes) DDoS sessions precisely doubled";
> - The source/site/article [https://www.darkreading.com/perimeter/ddos-for-hire-services-doubled-in-q1-/d/d-id/1335042] indicates that DDoS-for-hire services doubled between Q4 2018 and Q2 2019.

For the purposes of this analysis, we classify computer-based services into two general types:

Publicly available services, such as DNS servers, web servers, and content distribution networks
These must remain freely accessible on the internet, without requiring identity, authentication, or authorization. Protecting these types of services from DDoS attacks is not the focus of this white paper.

Private services, such as private business applications, employee or customer portals, or email servers
These services are intended to be delivered to a well-defined audience. This audience has known identities and can be authenticated prior to utilizing these services. These private services, which are the focus of this white paper, are well-suited to being protected from DDoS attacks by a Software-Defined Perimeter.

For both types of services, organizations should look at detection and mitigation services available from their network service provider, since many DDoS attacks will impact their network connections and defenses can often be applied "upstream" in the network.

Goals

The primary goal of this document is to increase the awareness and understanding of SDP as a tool to prevent DDoS attacks by demonstrating its efficiency and effectiveness against several well-known attacks, including HTTP Flood, TCP SYN, and UDP Reflection.

Target Audience

The primary target audience for this document are people in security, enterprise architecture, and compliance roles within enterprises. These stakeholders will be largely for the evaluation, design, deployment, or operation of DDoS prevention solutions within their enterprise.

Secondarily, solution providers, service providers, and technology vendors will also benefit from reading this document.

DDoS Attack Vectors

DDoS attack vectors, while broadly classified into resource depletion and bandwidth attacks, can be sub-classified according to the layer they target in the Seven Layer OSI Model as seen in the figure below. Additionally, they can be viewed according to the TCP/IP Model. See Appendix 1 and 2 for a comparison of both models. Note that TCP/IP with its four layers represents how networks are currently set-up and operate in the real world. OSI represents an ideal view and is generally used for teaching and explanation purposes due to its more detailed breakdown. We will use the OSI Model in this paper. The layers highlighted in blue in the figure are generally not the target of DDoS attacks and are not included in our areas of focus. From the remaining layers we selected 3 attacks highlighted in green to focus on.

DDoS Attack Vectors by OSI and TCP/IP Model Layer

No.	OSI Layer	TCP/IP Layer	Protocol Data Unit	Description	Well Known Attacks & Vectors of Focus
7	Application	Application	Data	Network process to application	HTTP Flood & DNS Query Flood
6	Presentation		Data	Data representation & encryption	TLS/SSL Exploits
5	*Session*		*Data*	*Interhost communication*	*N/A*
4	Transport	Transport	Segments	End-to-end connections & reliability	SYN "TCP" Flood
3	Network	Internet	Packets	Path determination addressing	UDP Reflection
2	*Datalinks*	*Network Access*	*Frames*	*Physical addressing*	*N/A*
1	*Physical*		*Bits*	*Media, signal & binary transmission*	*N/A*

Source: https://aws.amazon.com/shield/ddos-attack-protection/

I. Attacks on Applications

Attacks on applications are less common than attacks on Transport and Networks[2] and are generally more sophisticated because they do not rely on brute force. These attacks are typically smaller in volume compared to the Layer 4 and 3 attacks and focus on making a connection with the target to acquire expensive (requiring significant resources = resource depletion) parts of the application, thereby making it unavailable for real users. Examples of this might include at Layer 7 a flood of HTTP requests to a login page or an expensive search API[3].

[2] https://securelist.com/ddos-report-q1-2019/90792/ Distribution of DDoS attacks by duration (hours), Q4 2018 & Q1 2019

[3] https://aws.amazon.com/shield/ddos-attack-protection/

1) HTTP Get requests and HTTP Post requests
Two of the most well-known resource depletion attacks are HTTP Get requests and HTTP Post requests (See HTTP Flood Attack & SDP Defense). A Get request can be used to retrieve data - an image, for example. A Post request initiates actions that need to be processed. Both Get and Post requests can be initiated via an HTTP client (a Web browser) request to an HTTP server (Web server). The Post request is generally more efficient (requiring fewer requests) than the GET request at depleting server resources as its processing (requiring database access for example) is more complex than a Get request.

The recent successful DDoS[4] attack on the Amazon Cloud, Spotify, Twitter and others is an eye-opening incident that requires serious attention from cloud security designers. In the paper (see reference) outlining scalable cloud defenses for the detection, analysis and mitigation of DDoS attacks, the authors outline the state-of-the-art cloud DDoS defenses. Detection of the DDoS attacker's IP address(es) can provide a significant breakthrough in protecting the cloud resources by creating effective deterrence, and some vendors provide this capability. The Internet Engineering Task Force's RFC2827[5] proposes a method for using ingress traffic filtering to prohibit DoS attacks that use forged IP addresses. These IP addresses are generally propagated from the aggregation point of the ISP. Another method is to detect DDoS attacks through monitoring propagation of abrupt traffic changes inside ISP domains followed by characterizing flows that carry attack traffic. The authors maintain that the inherent limitation of any detection mechanism is their ability to detect only known attack patterns. They cannot cope with the attacks launched by smart attackers whose attack patterns are frequently changed.

II. Attacks on Transport and Network

Transport (Layer 4) and Network (Layer 3) Layers are the most common targets of DDoS attacks and include vectors like SYN "TCP" Flood and User Datagram Packet (UDP) attacks. Both TCP and UDP are protocols used to transmit packets. However, UDP does not employ all the flow control and error checking mechanisms embedded in TCP. Layer 4 and 3 attacks are usually large in volume and aim to overload the capacity of the network or the application servers[6].

1) Transmission Control Protocol (TCP) Flood
This attack method (See TCP SYN Flood Attack & SDP Defense) involves the attacker sending via TCP, SYN packets in an attempt to complete three-way handshakes (a completed connection). The target server then responds with SYN ACKs, to which the attacking server is supposed to close the loop by sending ACKs but doesn't. Because the target's servers are configured to keep the TCP connections open waiting for the attacker's ACK to close the loop, a tidal wave of these incomplete connections strains the target's server's resources, including the allowed number of open TCP connections.

[4] Ddos attack hits amazon cloud customer hard. https://www.datacenterdynamics.com/news/major-ddos-attack-on-dyn-disrupts-aws-twitter-spotify-and-more/

[5] https://www.ietf.org/rfc/rfc2827.txt

[6] https://aws.amazon.com/shield/ddos-attack-protection/

2) User Datagram Protocol (UDP) Flood
A simple UDP attack works like a TCP SYN Flood attack in that packets are sent that will result in an incomplete service request that requires resources to handle. More specifically, UDP packets are sent directly by an attacker to a particular server and port of the victim requesting a service.

The target system looks for the non-existing requested service and responds to the attacker with an ICMP "Destination Unreachable" packet indicating that the service can't be reached. A flood of these invalid UDP packets can overwhelm the system similar to the SYN "TCP" Flood[7].

UDP Reflection Attacks:
A slightly different type of UDP attack (See UDP Reflection Attack & SDP Defense) requires the attacker to spoof the target's IP address and launches queries purporting to initiate from this address to open services on the Internet which will solicit a response that is to be delivered to the target. The services used in this methodology are typically selected such that the size of the response to the initial query is many times (x100s) larger than the query itself. The response is returned to the real owner of the faked IP. This attack vector allows attackers to generate huge numbers of packets and therefore of attack traffic, while making it difficult for the target to determine the original sources of the attack traffic. Note that TCP Reflection attacks are also possible[8]. Reflection amplification has been responsible for some of the largest DDoS attacks seen on the Internet during the last decade. See Appendix 4: DDoS Biggest Attacks

DDoS Attack Mitigations (via Non SDP Defenses)

DDoS attacks can be mitigated (excluding SDP mitigations that block) by a combination of detection, diversion, filtering and analysis. The goal of detection is to identify attacks before they reach dangerous levels. After detection traffic is diverted to be filtered then either discarded or parked for analysis. Traffic not discarded can be filtered so that good traffic can flow through. Bad traffic can be discarded or parked for analysis. Parked traffic needs to be analyzed to glean any information that can help make the security system more resilient in the future[9].

Layer 7: Application - Data
One mitigation method is using a Web Application Firewall (WAF) with rules designed to recognize excessive volumes that when detected causes the system to limit the traffic flow (rate limiting).

Layer 6: Presentation - Data
One way to avoid attacks at this layer is to offload Secure Socket Layer (SSL) requests from the origin infrastructure to an application delivery platform (ADP). The platform decrypts, inspects, then re-encrypts requests made via SSL and Transport Layer Security (TLS) protocols. This removes overhead from the web servers (avoiding Resource Depletion) and frees up web application resources that would otherwise be consumed by the DDoS attack.

[7] Here's a clear explanation: https://www.cloudflare.com/learning/ddos/udp-flood-ddos-attack/

[8] https://www.usenix.org/system/files/conference/woot14/woot14-kuhrer.pdf

[9] https://www.incapsula.com/ddos/ddos-mitigation-services.html

Layer 4: Transport - Segments
Null Routing (Black Holing) drives traffic to a non-existent IP Address, sinkholing diverts traffic based on a malicious IP address list, while BGP (Border Gateway Protocol) routing diverts all network packets to a scrubbing server.

Layer 3: Network - Packets
In addition to the above, rate limiting ICMP traffic can be used to restrict the flow of traffic. While rate limiting is configured in the firewall, routers and switches also have limited rate limiting capabilities. In the same way a Flood can be considered brute force attack, rate limiting can be considered a brute force mitigation.

Not Applicable:
Layer 5: Session - Data
Layer 2: Data-Link - Frames
Layer 1: Physical - Bits

SDP as a DDoS Defense Mechanism

The techniques described above to detect, divert, filter and analyze are suitable for a large volume of packets associated with DDoS attacks. Many small malformed packets associated with resource depletion DDoS attacks typically bypass these techniques as they are hard to detect. However, these techniques are expensive and more frequently than not filter out good packets. SDPs are architected to allow ONLY good packets through while dropping all bad packets. In general, with SDPs, hosts are hidden, clients coordinate with (typically with multiple) perimeters so that good packets known to SDPs and upstream routers can be informed about bad packets to block. For the purpose of showing how SDPs can be used as a DDoS defense mechanism, we will use the open source reference implementation as an example. In the reference implementation, clients (users on devices) are cryptographically signed into the perimeter.

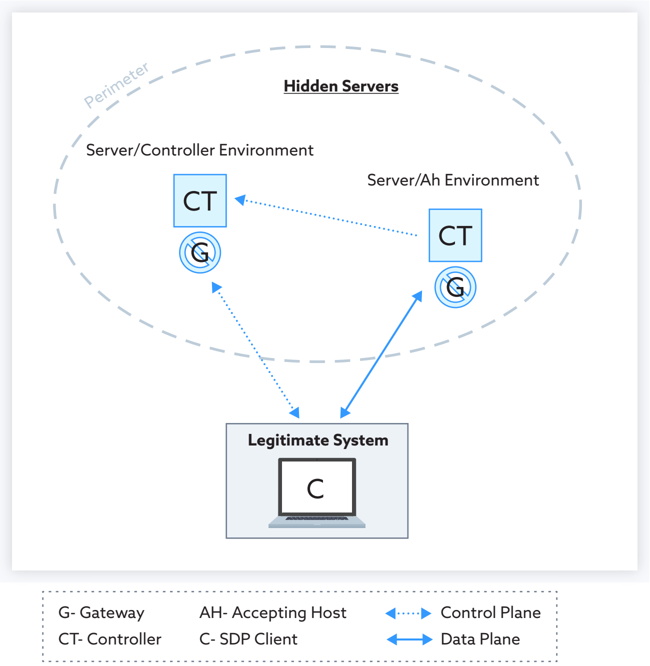


Figure 2: Reference Implementation

Recall that all internet-facing interfaces of servers (AH Environment) are available only after registration in the SDP Controller (CT) and Gateway (G) Environment. The following sequence of events is typically followed to set up an SDP configured as a DDoS defense mechanism:

1. Set up the controller environment and gateway to establish the perimeter; hide the service/servers.
2. Users who wish to connect to these hidden servers are onboarded with a unique ID (per device), a client certificate and encryption keys.
   a. As an option, users can onboard themselves via a self-service website that also verifies the devices they are using to connect to the hidden servers.
   b. As an option, the user's geo location would be logged by the SDP and used as a multi-factor authentication attribute.

3. Users establish a connection to the hidden servers by using an SDP client on their device.
4. An initial Single Packet Authorization (SPA[10]) packet is sent by the client and is checked by the SDP Controller and Gateways to match the user information provided during onboarding.
5. The information in the SPA packet is verified and matched with the client information that was collected during the onboarding process.
6. If the device validation and user information are valid, the users will be granted access into the perimeter. (The IP address can be verified to match the stored location as an option but is not necessary).
7. The Accepting Host Gateway opens up the firewall to allow a connection to the hidden service.

The sequence of events that SDP provides is highly effective in allowing the good packets in while dropping all bad packets. The combination of 1) hiding the services behind a deny-all SDP Gateway, 2) authenticating users on devices prior to opening up the firewall to establish the connection, and 3) using a dynamic firewall mechanism allows SDP to drop packets as fast as the switches serve them up during a DDoS attack. In the research performed and funded by DHS (www.waverleylabs.com/demo), it was shown that more than 80% of the good traffic gets through even under a heavy DDoS attack when the switches get overwhelmed with packets both good and bad. Further research to notify the upstream routers and switches about the bad packets will also help with blocking DDoS attacks that serve large-size non-malformed packets delivered to a single service to overwhelm it, more effectively.

While the services are protected from DDoS attacks, the SDP Gateway and the SDP Controller could bear the brunt of the DDoS attacks. But research has shown that using an initial UDP-based SPA packet greatly reduces the exposure of the SDP Gateway and the SDP Controller. More research on load-balancing the SDP Controller may show other configuration options for the SDP Gateway and SDP Controllers to be effective techniques to reduce the threat from DDoS attacks.

Using the lightweight SPA protocol to initiate entry into the perimeter makes detection of bad packets more effective when compared with the other techniques used to do the same IoT and similar systems can benefit by using the lightweight nature of the SPA combined with a deny-all firewall.

A similar sequence of events can be used in other SDP models different from the client-server model described above. These models are defined in the SDP Architecture Guide.

To summarize, SDPs are resilient against DDoS attacks because they utilize a computationally lightweight mechanism (SPA) to distinguish between authorized and unauthorized users (even from remote systems). The vast majority of DDoS traffic is initiated by unauthorized users; therefore, DDoS traffic can be rejected by SDP Gateways without incurring a heavy computational load on the server. SDPs should be combined with upstream DDoS detection and mitigation services (such as content distributors, i.e. Akamai; network hardware providers, i.e. Avaya; network providers, i.e. Verizon, etc.) from the ISPs for a more effective and preventative stance than is provided today.

The rest of the paper will be devoted to showing the operationalizing of SDP as a DDoS Prevention Mechanism against the following three well-known DDoS attacks all of which are mentioned in DDoS Attack Vectors by OSI and TCP/IP Model Layer Table above: HTTP Flood Attack, UDP Reflection Attack, TCP SYN Flood Attack.

[10] See https://cipherdyne.org/fwknop/docs/SPA.html for details on the concept, and reference the SDP Specification for its usage within SDP.

HTTP Flood Attack & SDP Defense

Battlefield

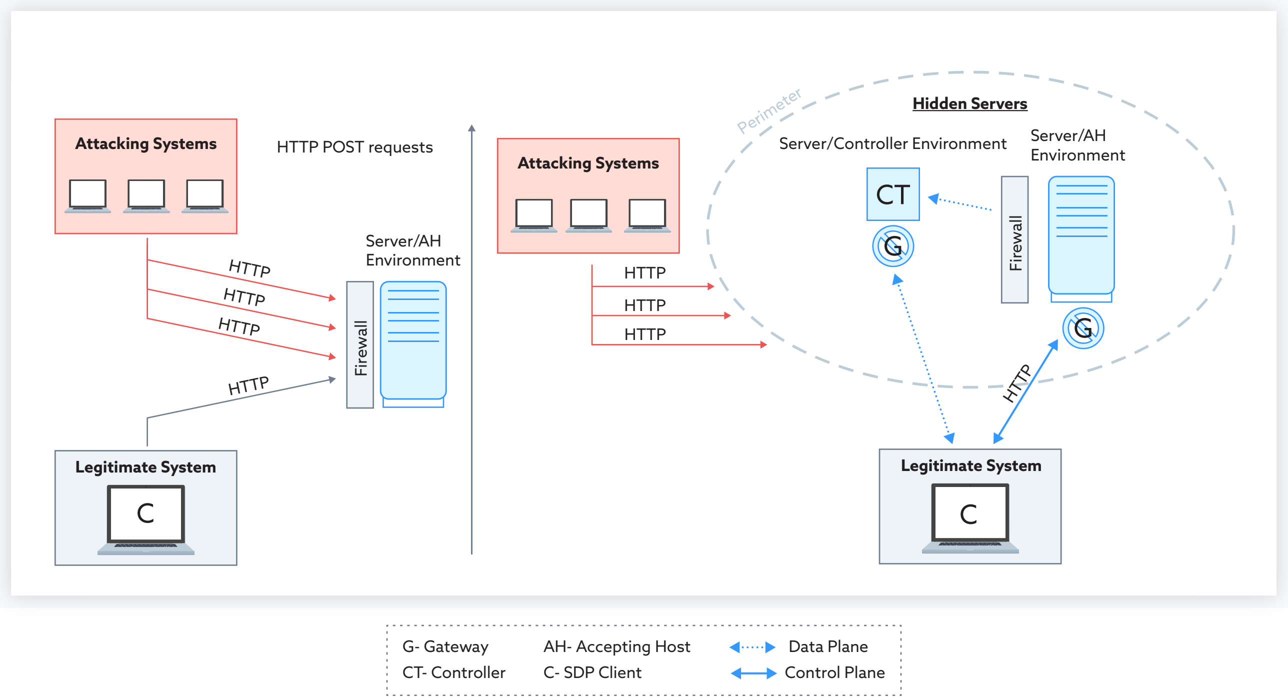


Figure 3: HTTP Flood Attack and the SDP Defense[11]

Attack Explained

This type of attack can be categorized as an OSI Layer 7 Application Attack (see DDoS Attack Vectors by OSI and TCP/IP Model Layer Table in DDoS Attack Vectors because its target is generally a web server/application. Additionally, it can be classified as a resource depletion attack because its objective is to overload resources of the servers/applications. Finally, it is often the case where a large volume of packets is delivered to a single service by a large group of computers (Botnet) controlled by an attacker. Because this attack uses legitimately formed requests from apparently legitimate devices, they are difficult to detect as well as block.

HTTP FLOOD ATTACK:

- Attacker acquires (by phishing or other means) Botnet devices by infecting them with malware;
- Malware is of the Command and Control type allowing an HTTP POST Request to be made;
- The HTTP POST Request contains a form to be processed by the target's database (DB);
- Botnet browsers establish TCP connections (three-way handshake) with the target's web server;
- Botnet web browsers send HTTP POST Requests with forms for entry into the targets DB

[11] The sequence of steps 1-7 in the SDP Defense is described in the previous section.

- Target's web server/application attempts to process the HTTP POST requests
- The high volume and resource hungry processing of the form being entered into the DB depletes the web server/application resources and slows or brings processing to a halt.

Defense Explained

As the key to this attack is to use legitimate-looking devices that want to connect to legitimate-looking Post requests, the most efficient way to thwart this kind of attack is to prevent any connection at all. SDP prevents the attack by making the target's Servers invisible to unauthorized devices.

1. The attacker's botnet cannot identify the target's Web server because the botnet devices have not been registered with the SDP's Controller.
2. The botnet, even if it could find the SDP Gateway hiding the server, cannot connect it to the SDP gateway because its devices do not have the installed SDP client which directs any communication to the SDP Controller.
3. Besides directing the communication, the missing SDP client contains the unique ID (per device), client certificate and encryption keys.
4. The botnet can never connect because the SDP Controller can't approve/validate the single packet authorization packet (SPA) containing the user information provided to an authorized device.
5. Therefore the SDP Controller can never verify and match the required client information.
6. Without the SDP client (with the ID, certificate and encryption keys) installed on the botnet devices and registered with SDP Controller and the SDP Gateway will not grant access to the perimeter.
7. Finally, the SDP Gateway protecting the Web server will not open up the firewall to allow a connection to the hidden service unless authorized by the SDP Controller.

However, should the IP address become public or the attacker by some means locates the IP address, the SDP Gateway will not recognize the devices and will drop any delivered packets (Post requests). If the attacker gets this far, the trail left by the attempted entry and the dropped packets provide evidence and data that can be analyzed to improve defenses and/or to prosecute the attacker.

TCP SYN Flood Attack and SDP Defense

Battlefield

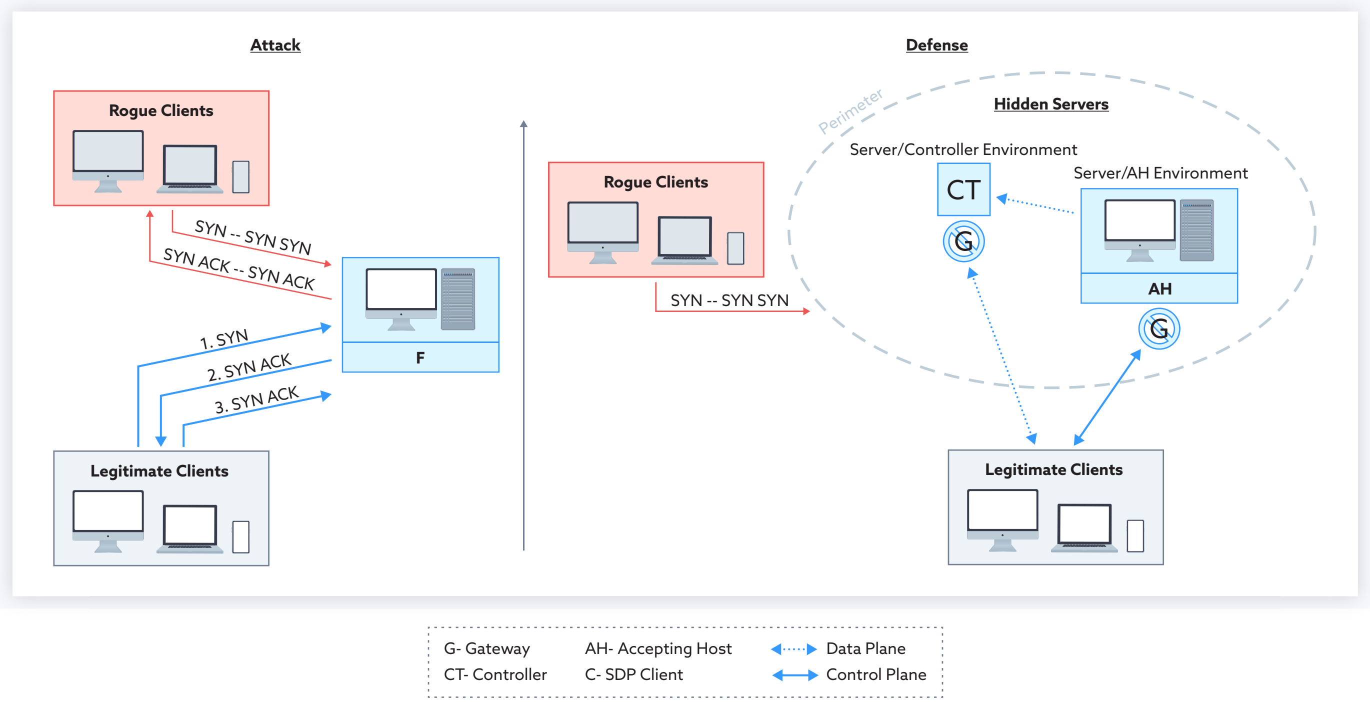


Figure 4: TCP SYN Flood Attack and the SDP Defense[12]

Attack Explained

SYN Flood attacks, like the recent 500 million packets per second DDoS attack, (https://www.darkreading.com/attacks-breaches/massive-ddos-attack-generates-500-million-packets-per-second/d/d-id/1333766) overwhelm the target by initiating but not completing the TCP handshake and flooding it with requests that eventually exhaust its ability to accept more requests thereby causing a denial of service. By using multiple rogue clients performing the same incomplete TCP handshake, attackers are able to increase the number of packets per second (PPS) or packet rate aimed at the target. Large SYN packets or packet volumes can also flood the target causing a denial of service.

Defense Explained

The SDP Gateways provide a shield that drops all packets from rogue clients and allows only packets from legitimate clients into the perimeter that protects the target. Other defense mechanisms that don't distinguish between legitimate and rogue clients throttle even the good packets by provisioning network bandwidth and inspecting packets, making SDP a more effective solution to continue operations under SYN Flood attacks regardless of packet rates or packet volumes.

[12] The sequence of steps 1-7 in the SDP Defense is described in the previous section.

UDP Reflection Attack and SDP Defense

Battlefield

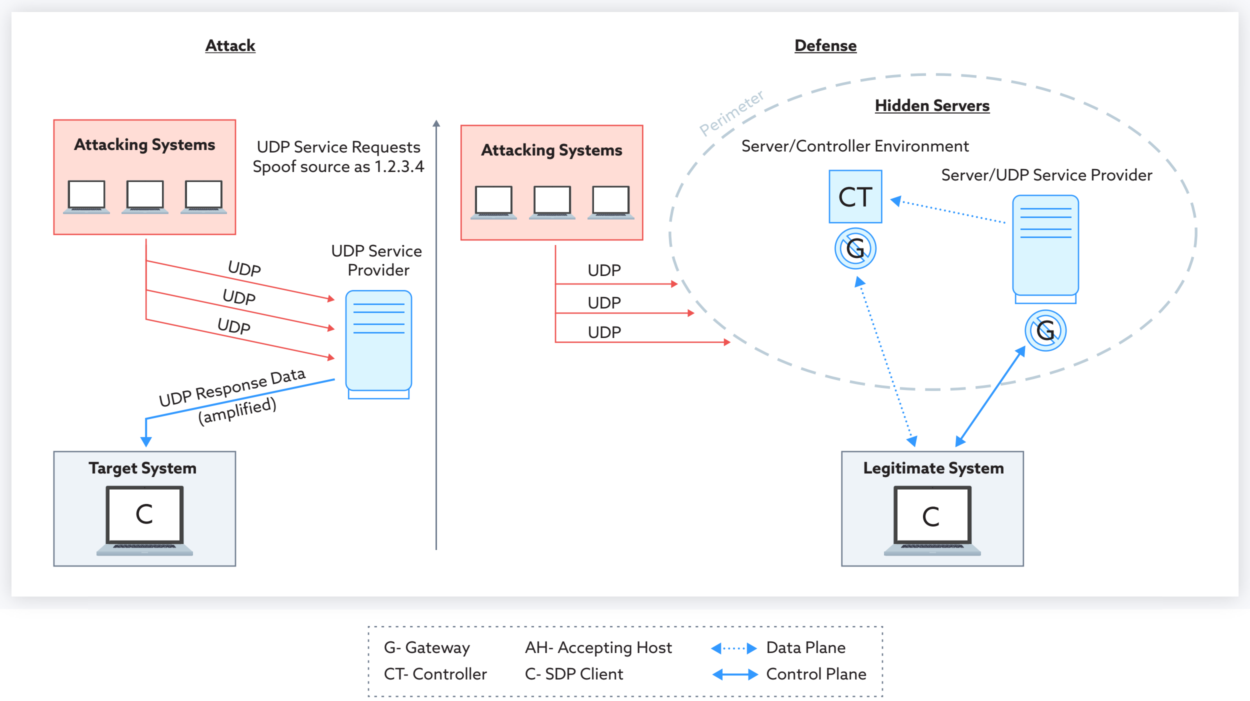


Figure 5: UDP Reflection Attack and the SDP Defense[13]

Attack Explained

This type of attack is based on the inherent insecurity of UDP, as an unauthenticated and connectionless protocol. UDP packets (specifically, their headers) can easily be forged, so that the response to the requested "service" is directed to the victim's IP address which was spoofed in the initial UDP packet. Thus, the response to the UDP request is "reflected" from the attacker to the victim. Amplification is a type of reflection attack, in which the response is disproportionately larger (amplified), thus overwhelming the victim's network or machine. Attackers often choose services with large amplification factors to more effectively DoS their victims.

Amplification factors roughly range from 1 (no amplification) for an ICMP ping command, to around 28-54 for certain DNS attacks, and around 550 for certain NTP attacks. Other services can result in much larger amplifications – most notably memcached, which, depending on the database contents, can result in amplifications of up to 50,000.

Link: https://www.us-cert.gov/ncas/alerts/TA14-017A\
https://www.cloudflare.com/learning/ddos/memcached-ddos-attack/

[13] The sequence of steps 1-7 in the SDP Defense is described in the previous section.

UDP reflection attacks can be effective and stealthy since there’s no need for any direct communication between the attacker and the target. These attacks are often launched from a distributed set of hijacked systems (botnets), further obfuscating the actual source of the attack.

Defense Explained

UDP based services cannot, by themselves, be secured, since UDP is inherently an open mechanism for delivering packets without authentication or authorization. Some public-facing UDP services, such as NTP or DNS, must remain public and are therefore subject to being exploited to participate in this type of DoS attack. However, non-public services – that is, services only intended to be consumed by an identifiable population of users or servers – are well-suited for protection by SDP.

By placing these services behind an SDP Gateway, organizations can enforce access controls so that only authorized users (or devices, or servers) can send UDP packets to the service. This eliminates attackers’ abilities to use these UDP services for a reflection attack.

Note that an authorized client device with malicious software running on it could, of course, be used to initiate this type of reflection attack.

Summary

The goal of this paper is to increase the awareness and understanding of SDP as a tool to prevent DDoS attacks by demonstrating its efficiency and effectiveness against several well- known attacks.

To that end we presented in the Introduction definitions of DDoS and DoS attacks. Then in the next section DDoS Attack Vectors, we presented a table DDoS attack Vectors by OSI and TCP/IP layers. From this table we selected as our focus three well-known attacks:

> 1. Layer 7 Application - HTTP Flood Attacks
> 2. Layer 4 Transport - SYN "TCP" Flood
> 3. Layer 3 Network - UDP Reflection Attacks

After selecting the vectors and attacks of focus we explained them conceptually in detail. This was followed by a section DDoS Attack Mitigations via Non SDP Defenses where we described non SDP mitigations that are available for use at various OSI layers.

We followed this up with SDP as DDoS Defense Mechanism. Here we first described the sequence of events that are followed to set up and configure SDP as a DDoS defense. Then we enumerated the protections afforded by the setup including

> 1. Invisible services behind a deny-all SDP Gateway;
> 2. Authenticating users on devices prior to opening up the firewall to establish connections;
> 3. Using a dynamic firewall mechanism, to allow or which allows SDP to drop packets as fast as the switches serve them up during a DDoS attack.

Finally, we looked at the following three attacks using SDP as a defense mechanism:

> - HTTP Flood Attack & SDP Defense
> - TCP SYN Flood Attack & SDP Defense
> - UDP Reflection Attack & SDP Defense

For each of the above we presented the attack and defense visually then followed the visualization with detailed explanations. For each of the attacks we concluded that SDP provided an adequate defense.

In conclusion, SDP functions as an efficient and effective DDoS defense mechanism against the attacks reviewed. Certain attributes of the SDP configuration such as Deny All Gateways and SPA can also be used against a variety of other attacks. If you combine SDP with upstream DDoS detection and mitigation services from an ISP as well as content and network providers, you have comprehensive DDoS defense in depth.

Glossary

BGP	The Border Gateway Protocol is the control protocol used to distribute and compute paths between the tens of thousands of autonomous networks that comprise the Internet.
Botnet/ Zombies	These are computers that have been compromised by an attacker to be used to perform malicious attacks.
ICMP	Internet Control Message Protocol, unlike TCP and UDP, is primarily used for error, operational or diagnostics messages/purposes such as requested service is not available, host or router could not be reached or for ping or traceroute analysis.
Ingress Filtering	This is a means to ensure that packets identified as coming from a particular address actually come from that address. There are a variety of ways to implement this process, the best of which are documented in Internet Engineering Task Force in BCP 38 and BCP 84.
IP Address Spoofing	When IP Packets are created using a fake source IP address, this is called spoofing. This is done to hide the identity of an attacker.
Malformed Packet	This is any packet that can't be dissected by the protocol dissector. The packet does not adhere to the protocol specifications used - TCP or UDP for example.
Signature (Attack)	Data, traffic or events inherent to an attack. This information is used by Intrusion Detection Systems (IDS) to identify that an attack is occurring followed by issuance of an alert.

Other Reading

Cybersecurity Framework DDoS Profile, by the Coalition for Cybersecurity Policy & Law Made Public July 28, 2017, Available @ https://www.cybersecuritycoalition.org/threat-profile-ddos-nist-framework

NIST, Advanced DDoS Mitigation Techniques Project, by NIST, Department of Homeland / Security Science and Technology Directorate / Cyber Security Division / Distributed DDoS Defense Program, Available @ https://www.nist.gov/programs-projects/advanced-ddos-mitigation-techniques

NIST, SP 800-137 Information Security Continuous Monitoring (ISCM) for Federal Info. Systems and Organizations, by Kelley Dempsey (NIST), Nirali Chawla (PwC), L. Johnson (NIST), Ronald Johnston (DoD), Alicia Jones (BAH), Angela Orebaugh (BAH), Matthew Scholl and Kevin Stine (NIST), Sep. 2011, Available @ https://csrc.nist.gov/publications/detail/sp/800-137/final

ENISA, DoS & DDoS Portal, European Union Agency for Network & Info. Sec. Resilience & Sec. of Comm. Infrastructure, Networks & Services, Oct. 2018, Available @ https://resilience.enisa.europa.eu/internet-infrastructure-security-and-resilience-reference-group/dos-and-ddos

ENISA, Threat Landscape Report 2017 15 Top Cyber-Threats and Trends, by ENISA ETL Stakeholder group: Pierluigi Paganini, Chief, Security Info. Officer, IT, Paul Samwel, Banking, NL, Jason Finlayson, Consulting, IR, Stavros Lingris, CERT, EU, Jart Armin, Worldwide Coalitions/Initiatives, Int'l., Thomas Häberlen, Member State, DE, Neil Thacker, Consulting, UK, Shin Adachi, Security Analyst, US, R. Jane Ginn, Consulting, US, Andreas Sfakianakis, Industry and CYjAX, NL. T Final Version,1.0, ETL 2017, Chapter 3.6 Denial of Service, January 2018, Available @ https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017

Understanding DDoS Attack & Its Effect In Cloud Environment by Rashmi V. Deshmukha, Kailas K. Devadkarb, Procedia Computer Science Volume 49, 2015, Pages 202-210, December 2015, Available @ https://www.sciencedirect.com/science/article/pii/S1877050915007541

DDoS Attacks: Tools, Mitigation Approaches, and Probable Impact on Private Cloud Environment, by R. K. Deka and D. K. Bhattacharyya; Department of Computer Science and Engineering, Tezpur University, Napaam, Assam, India, and J. Kalita; Department of Computer Science, College of Engineering and Applied Science, University of Colorado, Boulder, CO, United States, October 25, 2017, Available @ https://arxiv.org/pdf/1710.08628.pdf

Defence for Distributed Denial of Service Attacks in Cloud Computing, Andrew Carlin and Mohammad Hammoudeh, School of Computer, Mathematics & Digital Technology, Manchester Metropolitan University, Manchester, UK, Omar Aldabbas, Faculty of Eng., Al-Balqa Applied University, Jordan, 2015, Available @ https://www.sciencedirect.com/science/article/pii/S1877050915034985

Guide to DDoS Attacks November 2017, Center for Internet Security (CIS), Multi-State Information Sharing and Analysis Center (MS-ISAC), November 2017, Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.http://www.us-cert.gov/tlp, Available @ https://www.cisecurity.org/white-papers/technical-white-paper-guide-to-ddos-attacks/

NIST, SP 800-54 Border Gateway Protocol Security, by Rick Kuhn (NIST), Kotikalapudi Sriram (NIST), Doug Montgomery (NIST), July 2007, to be superceded by SP 800-119 below, Available @ https://csrc.nist.gov/publications/detail/sp/800-54/final

NIST, SP 800-189 Secure Interdomain Traffic Exchange: BGP Robustness and DDoS Mitigation, by Kotikalapudi Sriram (NIST), Douglas Montgomery (NIST), March 2019, Available @ https://csrc.nist.gov/publications/detail/sp/800-189/draft

NIST, SP 800-119, Guidelines for the Secure Deployment of IPv6, by Sheila Frankel of the National Institute of Standards and Technology (NIST), Richard Graveman of RFG Security, John Pearce of Booz Allen Hamilton and Mark Rooks of L-1 Identity Solutions (formerly of Booz Allen Hamilton), December 2010, Available @ https://csrc.nist.gov/publications/detail/sp/800-119/final

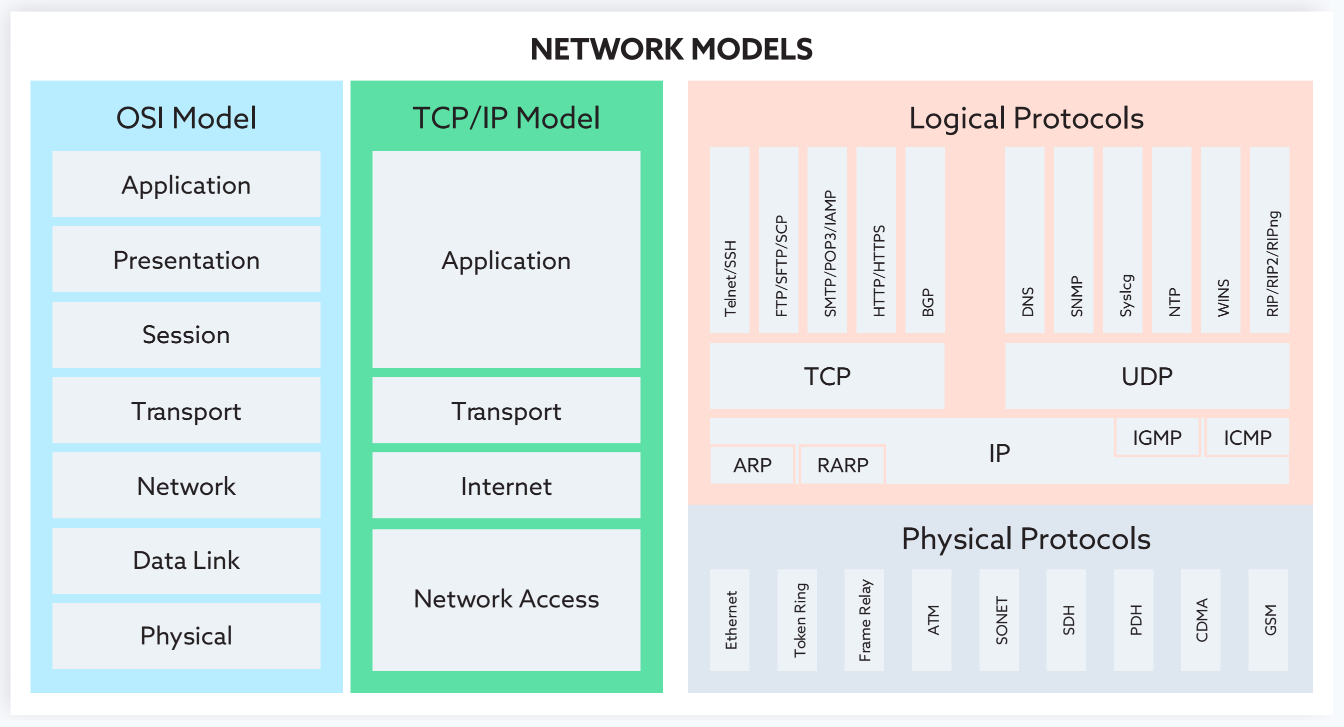
Beginner's Guide to Brute Force & DDoS Attacks, WHAT TO DO WHEN THE BARBARIANS ARE AT YOUR DOOR, Alienvault, Available @ https://www.alienvault.com/resource-center/white-papers/beginners-guide-to-brute-force-and-ddos-attacks

DDoS Quick Guide, The Department of Homeland Security (DHS), National Cybersecurity and Communications Integration Center, January 2014, Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls. http://www.us-cert.gov/tlp, Available @ https://www.us-cert.gov/security-publications/DDoS-Quick-Guide

Cybersecurity Framework DDoS and Botnet Prevention and Mitigation Profile(s), Coalition for Cybersecurity Policy & Law, February 2018, Available @ https://www.cybersecuritycoalition.org/botnet-framework

Scalable Cloud Defenses for Detection, Analysis and Mitigation of DDoS Attacks
Towards the Future Internet, G. Tselentis et al. (Eds.), IOS Press, 2010, Available @
https://pdfs.semanticscholar.org/d44f/98844c5bfc38f6c867edbeab3f0957f913d0.pdf

Appendix 1: OSI & TCP/IP Layers & Logical Protocols



Source: https://www.inetdaemon.com/tutorials/basic_concepts/network_models/comparison.shtm

OSI and TCP/IP Similarities include:

- Both have layers.
- Both have application layers, though they include very different services.
- Both have comparable transport and network layers.
- Both models need to be known by networking professionals.
- Both assume packets are switched. This means that individual packets may take different paths to reach the same destination. This is contrasted with circuit-switched networks where all the packets take the same path.

OSI and TCP/IP Differences include:

- TCP/IP combines the presentation and session layer issues into its application layer.
- TCP/IP combines the OSI data link and physical layers into the network access layer.
- TCP/IP appears simpler because it has fewer layers.
- TCP/IP protocols are the standards around which the Internet developed, so the TCP/IP model gains credibility just because of its protocols. In contrast, networks are not usually built on the OSI protocol, even though the OSI model is used as a guide.

Source: http://basicitnetworking.blogspot.com/2009/11/osi-layers-peer-to-peer-communications.html

Appendix 2: DDoS Attacks by OSI & TCP/IP Layers

OSI Layers	7	6	5	4	3	2	1
TCP/IP Layers	4			3	2	1	
DDoS Attack Name	Application	Present	Session	Transport	Network	Data	Physical
Smurf			N/A		X	N/A	N/A
ICMP Flood			N/A		X	N/A	N/A
IP/ICMP Fragmentation			N/A		X	N/A	N/A
SYN Flood			N/A	X		N/A	N/A
UDP Flood			N/A	X		N/A	N/A
Other TCP Floods (Spoof/Non)			N/A	X		N/A	N/A
TCP Connection Exhaustion			N/A	X		N/A	N/A
IPSec Flood IKE/ ISAKMP Assoc.			N/A	X		N/A	N/A
Slow Transfer Rate			N/A	X		N/A	N/A
Long Lived TCP Sessions			N/A	X		N/A	N/A
Other Connection Flood			N/A	X		N/A	N/A
SSL Exhaustion		X	N/A			N/A	N/A
Fake Certificates		X	N/A			N/A	N/A
Man-in-the-middle		X	N/A			N/A	N/A
Reflection/Amp (DNS, NTP...)	X		N/A			N/A	N/A
Application Request Floods	X		N/A			N/A	N/A
Other Floods (SMTP, DNS, SNMP, FTP, SIP, etc.)	X		N/A			N/A	N/A

Targeted Application	X		N/A			N/A	N/A
DB Connection Pool Exhaustion	X		N/A			N/A	N/A
Resource Exhaustion	X		N/A			N/A	N/A
HTTP POST Request Exhaustion	X		N/A			N/A	N/A
HTTP Get Request Exhaustion	X		N/A			N/A	N/A
Mimicked User Browsing	X		N/A			N/A	N/A
Slow read	X		N/A			N/A	N/A
Slow POST	X		N/A			N/A	N/A
Slow loris	X		N/A			N/A	N/A

http://resources.arbornetworks.com/wp-content/uploads/INFO_DDoSAttackTypes_EN.pdf

Appendix 3: DDoS & Other Attack Monitoring Maps

There are 2 attack maps that primarily track DDoS activity:

> 1. Digital Attack Map - https://www.digitalattackmap.com/about/
>   a. Updated daily
> 2. A10 - https://threats.a10networks.com/
>   a. Updated in real-time

There are 9 attack maps that track a variety of activities that can include DdoS:

> 1. Security Incidents - https://www.ibm.com/security/resources/xforce/xfisi/
>   a. Updated through Jan 2018 - one-year lag
> 2. Checkpoint - https://threatmap.checkpoint.com/ThreatPortal/livemap.html
>   a. Updated daily
> 3. Kaspersky - https://cybermap.kaspersky.com/
>   a. Updated in real-time
> 4. Fortinet - https://threatmap.fortiguard.com/
>   a. Update frequency unclear
> 5. FireEye - https://www.fireeye.com/cyber-map/threat-map.html
>   a. Update frequency unclear
> 6. Bitdefender - https://threatmap.bitdefender.com/
>   a. Updated in real-time
> 7. Threatbutt - https://threatbutt.com/map/
>   a. Updated in real-time
> 8. Deteque - https://www.deteque.com/live-threat-map/
>   a. Updated in real-time
> 9. Akami - https://www.akamai.com/us/en/resources/visualizing-akamai/real-time-web-monitor.jsp
>   a. Updated in real-time

Appendix 4: DDoS Biggest Attacks

Date	Target	Terabytes Per Sec	Attack Vehicle	Vehicle Vulnerabilities	Used for Attack Type
Mar 2018[14]	US SP	1.7	Memcached Servers	Access Authentication	"Reflection Amplification"
Feb 2018[15]	Github	1.3	Memcached Servers	Access Authentication	"Reflection Amplification"
Oct 2016[16,17]	Dyn DNS	1.2	Millions of IoT Devices	Authentication	TCP UDP Floods

Memcached Servers[18,19]

Memcached servers allow applications that need to access a lot of data from an external database to cache some of the data in memory, which can be accessed much more quickly by the application than having to travel out to a database to fetch something important.

These servers are meant to be accessible within a trusted network because they communicate on TCP using UDP (port 11211) by default, which does not require authentication. However, it was estimated on Mar 8, 2018 just after the two largest attacks that approximately 50,000[20] servers were openly exposed.

There are at least three measures available to mitigate this vulnerability. Move servers to trusted networks, install a new memcached version that disables the UDP protocol by default and finally close port 11211.

Currently, there appear to be about 31,000 Memcached servers still open[21].

[14] https://www.theregister.co.uk/2018/03/05/worlds_biggest_ddos_attack_record_broken_after_just_five_days/

[15] https://www.theregister.co.uk/2018/03/05/worlds_biggest_ddos_attack_record_broken_after_just_five_days/

[16] https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/

[17] See Page 7, Infrastructure attacks SYN "TCP" floods and Syn "UDP" Floods

[18] https://www.globaldots.com/memecached-servers-ddos-attacks-complete-analysis/

[19] https://www.geekwire.com/2018/memcached-servers-used-launch-record-setting-ddos-attacks/

[20] https://memcachedscan.shadowserver.org/stats/

[21] https://memcachedscan.shadowserver.org/stats/