A Cisco Guide to Defending Against Distributed Denial of Service Attacks

---

Contents

Introduction: The Case for Securing Availability and the DDoS Threat

Denial of service (DoS) and distributed denial of service (DDoS) attacks have been quite the topic of discussion over the past year since the widely publicized and very effective DDoS attacks on the financial services industry that came to light in September and October 2012 and resurfaced in March 2013.

The purpose of this white paper is to provide a number of tools, some or all of which may apply to a customer's environment, that can be part of an overall toolkit to help identify and mitigate potential DDoS attacks on customer networks.

The following quotes and excerpts are from several high-profile individuals and organizations that are focused on defending networks from these types of attacks:

"*...recent campaigns against a number of high-profile companies—including U.S. financial institutions—serve as a reminder that any cyber security threat has the potential to create significant disruption, and even irreparable damage, if an organization is not prepared for it.*"

"*Cybercrime is no longer an annoyance or another cost of doing business. We are approaching a tipping point where the economic losses generated*
by cybercrime are threatening to overwhelm the economic benefits created by information technology. Clearly, we need new thinking and approaches to reducing the damage that cybercrime inflicts on the well-being of the world."

The preceding quotes from John Stewart, Cisco Senior Vice President and Chief Security Officer are eye opening considering that the miscreants are using the network infrastructure to financially impact organizations and diminish the purpose of this infrastructure.

"*The bottom line is that unfortunately, no organization is immune to a data breach in this day and age...*"

"*We have the tools today to combat cybercrime, but it's really all about selecting the right ones and using them in the right way.*"

"*In other words, understand your adversary -- know their motives and methods, and prepare your defenses accordingly and always keep your guard up...*"

These quotes from the Verizon 2013 Data Breach Investigations Report (PDF) speak to the point that organizations are befuddled with the number of technologies, features, and processes available to help defend their networks. There is no one-size-fits-all approach. Each entity must determine which solutions meet its requirements and which help mitigate the threats that concern it.

"The number of DDoS attacks in Q1 2013 increased by 21.75 percent over the same period of last year."

"Attacks targeting the infrastructure layer represented more than a third of all attacks observed during the first three months of 2013."

"*What defined this quarter (Q1 2013) was an increase in the targeting of Internet Service Provider (ISP) and carrier router infrastructures...*"

While the preceding statements from Prolexic are certainly keeping service providers' (SP) network security experts awake at night, it is a legitimate fear that everyone should possess. If the core of the Internet is impacted by a malicious attack or inadvertent outage, we will all suffer because the Internet has become our lifeblood in terms of how we work, live, play, and learn.

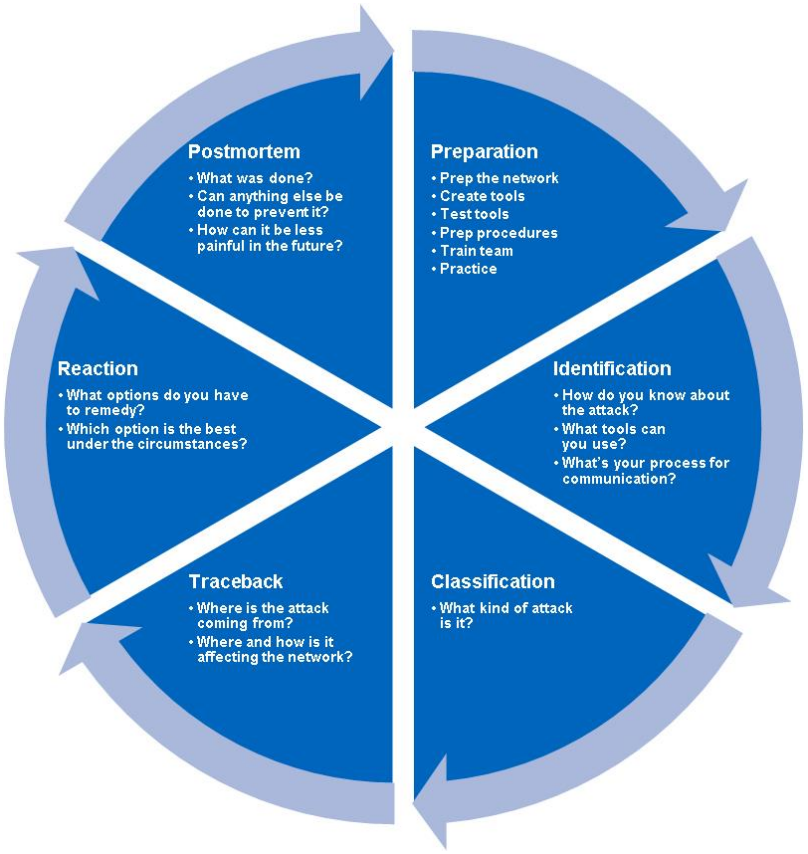
While the actual DDoS attacks garner the headlines, it is imperative that organizations also fully understand the impact of inadvertent, unmalicious outages. Two recent examples of unintentional events are the GoDaddy DNS Infastructure outage that took place in September 2012 and the CloudFlare outage that occurred in March 2013. Although the details of each event differ, the key message is that each outage occurred on a production network, adversely impacted resources that thousands—if not millions—of people used, and was initially reported in the press as an "attack."

At the heart of many customers' concerns is the ability to protect against DDoS attacks. The focus may revolve around customers' own networks and data, network and data services that customers provide to their own customers, or a combination.

While the network landscape and the nature of the assets that require protection will vary among customers and verticals, the general approach to mitigating DDoS attacks should be relatively similar across every environment. This approach should consist of, at a minimum, developing and deploying a solid security foundation that incorporates general best practices to detect the presence of outages and attacks and obtain details about them.

At Cisco we have been espousing the following six-phase methodology to customers and at training conferences, Cisco Live, Black Hat, CanSecWest, and other venues.

Figure 1. Six-Phase Methodology



The *Service Provider Security* white paper provides more information about the six-phase methodology.

Categorization of DDoS Attacks and Problems Caused

DDoS attacks have become a "Swiss army knife" for hacktivists, cyber criminals, and cyber terrorists, and in some cases used in nation-state attacks.

These attackers and their campaigns are becoming sophisticated. Attackers are using evasion techniques outside of the typical volume-based attacks to avoid detection and mitigation, including "low and slow" attack techniques and SSL-based attacks. They are deploying multivulnerability attack campaigns that target every layer of the victim's infrastructure, including the network infrastructure devices, firewalls, servers, and applications.

In the following subsections, we cover the types of DDoS attacks, common methodologies and tools used, and the impact of each attack.

DDoS Attack General Categories

There are three different general categories of DDoS attacks:

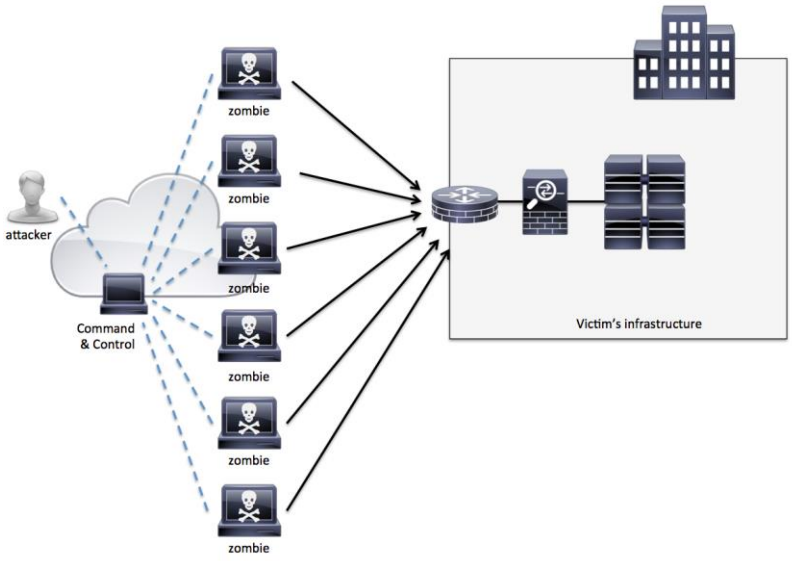
- Volume-based DDoS attacks
- Application DDoS attacks
- Low-rate DoS (LDoS) attacks

Volume-Based DDoS Attacks

In volume-based (or volumetric) DDoS attacks, the attackers typically flood the victim with a high volume of packets or connections, overwhelming networking equipment, servers, or bandwidth resources. These are the most typical DDoS attacks. In the past, volumetric attacks were carried out by numerous compromised systems that were part of a botnet; now hacktivists not only use conventional attack methodologies, but also recruit volunteers to launch these attacks from their own machines. In addition, new waves of huge volumetric attacks are now launched from datacenters of cloud service providers, when attackers either rent or compromise cloud-based systems that have tremendous Internet bandwidth.

A botnet is a gang of Internet-connected compromised systems that could be used to send spam email messages, participate in DDoS attacks, or perform other illegitimate tasks. The word botnet comes from the words *robot* and *network*. The compromised systems are often called *zombies*. Zombies can be compromised by tricking users into making a "drive-by" download, exploiting web browser vulnerabilities, or convincing the user to run other malware such as a trojan horse program. Figure 2 shows an example of a typical botnet.

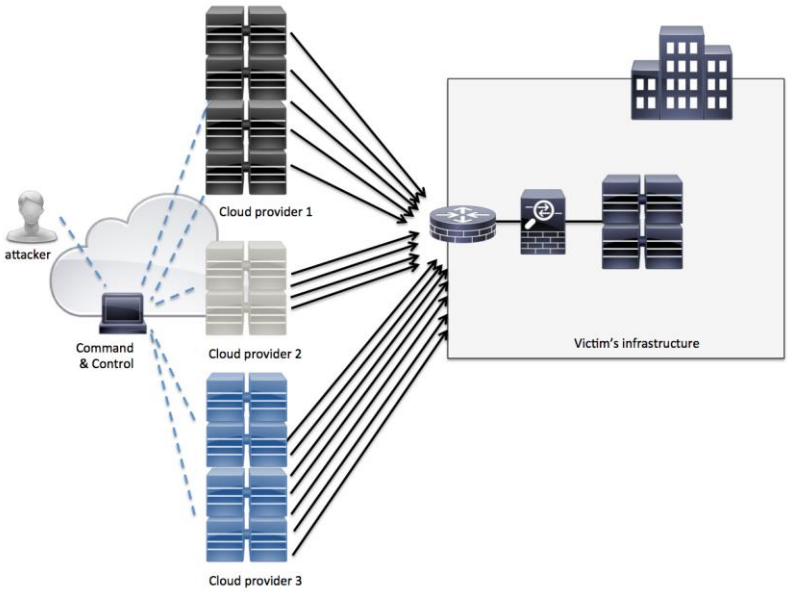
Figure 2. Botnet Example



In this example, an attacker controls the zombies to launch a DDoS attack against the victim's infrastructure. These zombies run a covert channel to communicate with the command-and-control server that the attacker controls. This communication often takes place over Internet Relay Chat (IRC), encrypted channels, bot-specific peer-to-peer networks, and even Twitter.

With the advent of cloud services and providers, a new trend has emerged. Attackers are either renting or compromising large datacenter/cloud machines to launch DDoS attacks. Cloud computing is not only creating new opportunities for legitimate organizations; it's also providing a great platform for cyber criminals because it inexpensively and conveniently allows them to use powerful computing resources to do bad things. This concept is illustrated in Figure 3.

Figure 3. Compromised Cloud Servers



Application DDoS Flood Attacks

Application DDoS attacks can target many different applications; however, the most common target HTTP aiming to exhaust Web servers and services. Some of these attacks are characteristically more effective than others because they require fewer network connections to achieve their goal. For instance, an attacker could launch numerous HTTP GETs or POSTS to exhaust a web server or web application.

On the other hand, other applications such as Voice over IP (VoIP), DNS, and others are often targeted. Examples of these attacks are covered later in this paper.

Low-Rate DoS Attacks

Low-rate DoS (LDoS) attacks often take advantage of application implementation weaknesses and design flaws. A prime example of these types of attacks is Slowloris, a tool that allows an attacker to take down a victim's web server with minimal bandwidth requirements and without launching numerous connections at the same time. Slowloris will be covered in detail later in this paper.

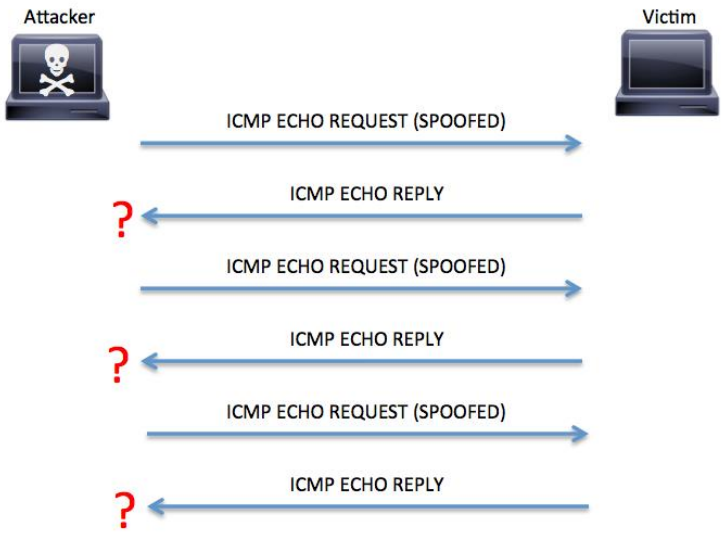
Detailed Examples of DDoS Attacks and Tools

The following are several examples of the more specific types of DDoS attacks and related tools.

Internet Control Message Protocol Floods

Internet Control Message Protocol (ICMP) flood attacks have existed for many years. They are among the oldest types of DoS attacks. In ICMP flood attacks, the attacker overwhelms the targeted resource with ICMP echo request (ping) packets, large ICMP packets, and other ICMP types to significantly saturate and slow down the victim's network infrastructure. This is illustrated in Figure 4.

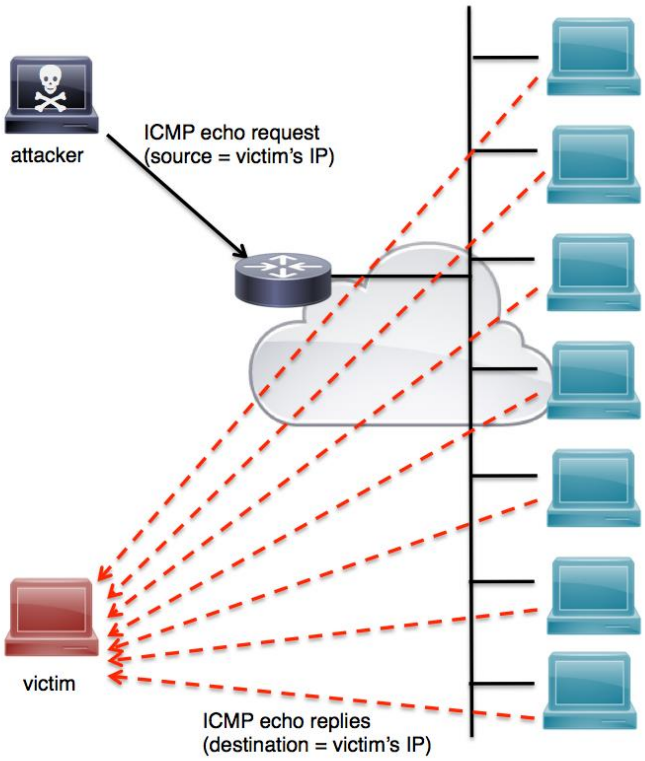
Figure 4. ICMP Flood Example



Smurf Attacks

Another type of ICMP-based attack is a smurf attack. The name *smurf* comes from the original exploit tool source code, *smurf.c*, created by an individual called TFreak in 1997. In a smurf attack, an attacker broadcasts a large number of ICMP packets with the victim's spoofed source IP to a network using an IP broadcast address. This causes devices in the network to respond by sending a reply to the source IP address. This exchange is illustrated in Figure 5.

Figure 5. Smurf Attack



This attack can easily be mitigated on a Cisco IOS device by using the **no ip directed-broadcast** subinterface command, as shown in the following example:

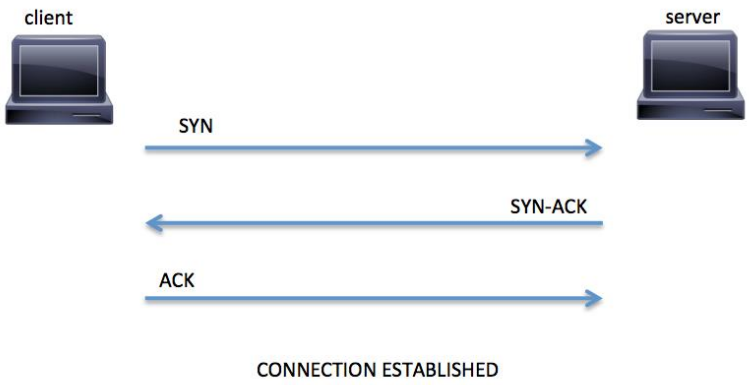
```
Router(config)# interface GigabitEthernet 0
Router(config-if)# no ip directed-broadcast
```

Note: Additional mitigation techniques are covered later in this paper.

SYN Flood Attacks

When a host (client) initiates a TCP connection to a server, the client and server exchange a series of messages to establish the connection. This connection establishment is called the TCP three-way handshake. This is illustrated in Figure 6.

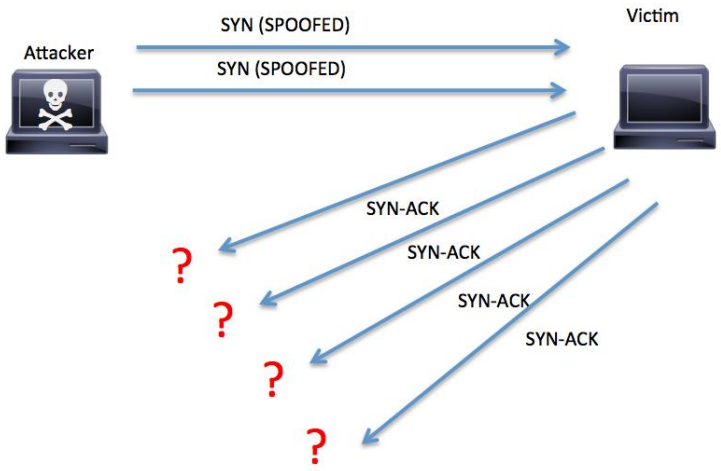
Figure 6. TCP Three-Way Handshake



- The client requests a connection by sending a SYN (synchronize) message to the server
- The server acknowledges this request by sending SYN-ACK back to the client
- The client responds with an ACK (acknowledgement) and the connection is established

In a SYN flood attack, the attacker does not reply to the server with the expected ACK. To do this, the attacker can spoof the source IP address or simply not reply to the SYN-ACK. This is illustrated in Figure 7.

Figure 7. SYN Flood Example



RFC 4987 provides more information about how TCP SYN flood attacks work and common mitigations.

Later in this paper we cover modern techniques for mitigating these types of attacks.

UDP Flood Attacks

Similar to TCP flood attacks, the main goal of the attacker when performing a UDP flood attack is to cause system resource starvation. A UDP flood attack is triggered by sending a large number of UDP packets to random ports on the victim's system. The system will notice that no application listens at that port and reply with an ICMP destination unreachable packet. Subsequently, if a large number of UDP packets are sent, the victim will be forced to send numerous ICMP packets. In most cases, these attacks are accomplished by spoofing the attacker's source IP address. Most modern operating systems now limit the rate at which ICMP responses are sent, minimizing the impact and mitigating this type of DDoS attack.

Teardrop Attacks

Teardrop attacks involve sending crafted packets with overlapping, over-sized payloads to the victim system. Modern operating systems are now immune to this attack, but because of a deficiency in the TCP fragmentation and reassembly implementation of older operating systems, this attack caused a crash of those systems.

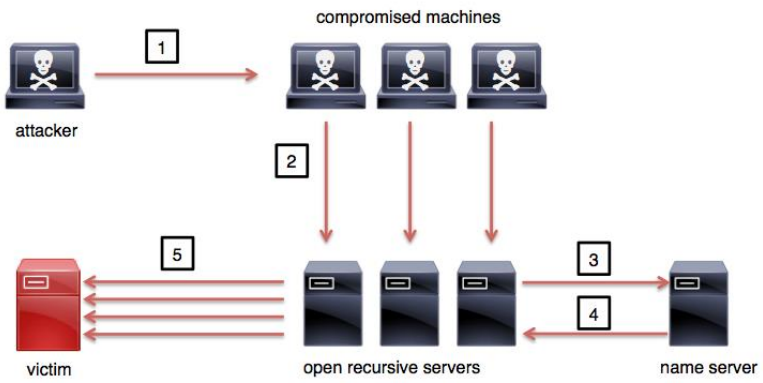
DNS Amplification Attacks

A Domain Name System (DNS) request can be recursive or nonrecursive (or iterative). Client applications, such as Internet browsers, typically request that the DNS server perform recursion by setting a Recursion Desired (RD) flag in the DNS request packet. If the DNS server cannot answer the request either from its cache or zone information, the server will request assistance from other DNS servers. See Recursive and Iterative Queries for an explanation of this process.

Unfortunately, many recursive name servers accept DNS queries from any source. In addition, many DNS implementations allow recursion by default, even when the name server is anticipated to serve only authoritative requests. This is known as an *open resolver*. DNS open resolvers are vulnerable to multiple malicious attacks, such as DNS cache poisoning and DDoS attacks.

A DNS amplification attack is the most common DDoS attack that uses recursive name servers, although some DNS amplifications attacks may not require a recursive server to be successful. DNS amplification attacks are similar to smurf attacks. In a smurf attack, an attacker can send spoofed ICMP echo requests (type 8) to create a DoS condition. In a DNS amplification DDoS attacker, an attacker sends small, spoofed address queries to an open resolver, causing it to send much larger responses to the spoofed-address target. Subsequently, the resolver contributes to the DDoS attack on spoofed addresses. Figure 8 illustrates the basic steps of a DNS amplification DDoS attack.

Figure 8. DNS Amplification Attack



The following steps are illustrated in Figure 8:

1. The attacker triggers and directs the compromised machines to begin the attack
2. The compromised machines send a DNS query for the domain *example.com* and set the source IP address to the victim's IP address
3. The open resolver servers ask the upstream name server(s) the location of *example.com*
4. The name server sends a reply back to the open recursive servers
5. The open recursive servers send DNS responses to the victim

Note: DNS Best Practices, Network Protections, and Attack Identification provides information about general best practices, network protections, and attack identification techniques that operators and administrators can use for DNS implementations:

Additional modern DDoS mitigation techniques are covered later in this paper.

The Open DNS Resolver Project maintains a list of DNS servers that are known open resolvers.

The Measurement Factory is similar to the Open DNS Resolver Project. It keeps a list of Internet-accessible DNS servers and allows the community to search for open recursive resolvers. It also provides a free tool to test a single DNS server to determine whether it allows open recursion.

DNSInspect is another free web-based tool for testing DNS resolvers.

SIP INVITE Flood Attacks

The Session Initiation Protocol (SIP) is a VoIP standard defined in RFC 3261. SIP INVITE messages are used to establish a media session between user and calling agents. In SIP INVITE flood attacks, the attacker sends numerous (often spoofed) INVITE messages to the victim, causing network degradation or a complete DoS condition.

Encrypted SSL DDoS Attacks

Encrypted (SSL-based) DDoS attacks are becoming more prevalent because they allow attackers to gain the following advantages:

- Encrypted DDoS attacks consume more CPU resources during the encryption and decryption process. Consequently, they amplify the impact on the victim system or network.
- Numerous DDoS mitigation technologies do not support decryption of SSL traffic. A large number of these attacks cannot be scrubbed.

Note: Modern mitigation capabilities for SSL DDoS attacks are covered later in this paper.

Slowloris

Slowloris is an attack tool created by RSnake (Robert Hansen) that tries to keep numerous connections open on a web server. The attack works by opening connections on the victim's server and sending a partial request. Intermittently, the attack sends subsequent HTTP headers. However, the attack does not complete the request to maintain these connections as open until the victim is not able to process requests from legitimate clients.

Similar attack tools and methodologies exist. The following are a few examples:

- PyLoris
- QSlowloris (a variant of Slowloris for Windows)
- slowhttptest

Low Orbit Ion Cannon and High Orbit Ion Canon

Low Orbit Ion Cannon (LOIC) and High Orbit Ion Canon (HOIC) have become popular DDoS tools for hacktivist groups such as Anonymous and the Syrian Electronic Army. These tools allow even nontechnical people to create a DDoS attack with a few clicks using their own computers instead of the traditional bot-served attacks.

Zero-Day DDoS Attacks

Zero-day DDoS attacks (often called one-packet-killers) are vulnerabilities in systems that allow an attacker to send one or more packets to an affected system to cause a DoS condition (a crash or device reload). These attacks are often the most stealthy and difficult to detect because they often are unknown to vendors and no patches or workarounds exist. Typically, these type of vulnerabilities and exploits are sold in the underground market, making them one of the biggest threats for any organization. The weaponization of these types of exploits is becoming the new normal for cyber criminals.

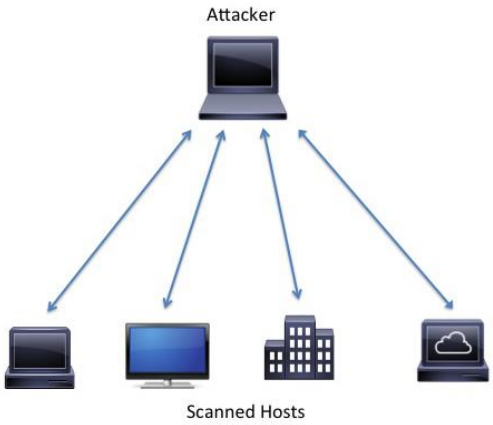
The DDoS Lifecycle

The motives, targets, and scope of a DDoS attack have evolved over the past decade. The primary goal of the attack, however—to deny network users access to resources—has not evolved. The components that make up an attack have not changed much either. To understand the DDoS lifecycle, it is important to first understand the components that make up the infrastructure of an attack. The lifecycle described here focuses primarily on the botnet, or a collection of zombie machines reporting to one or more command-and-control (C2) servers.

Reconnaissance

The beginning of a DDoS attack is characterized by manual or automated attempts to find vulnerable hosts to act as C2 servers or botnet clients. The reconnaissance may come from the attacker in the form of IP probes (also called ping sweeps). These probes can create a smaller list of hosts to probe further with port scans. Port scans provide more information about the host, such as the services offered and the operating system version. The attacker uses this information to determine the easiest way to exploit a vulnerability.

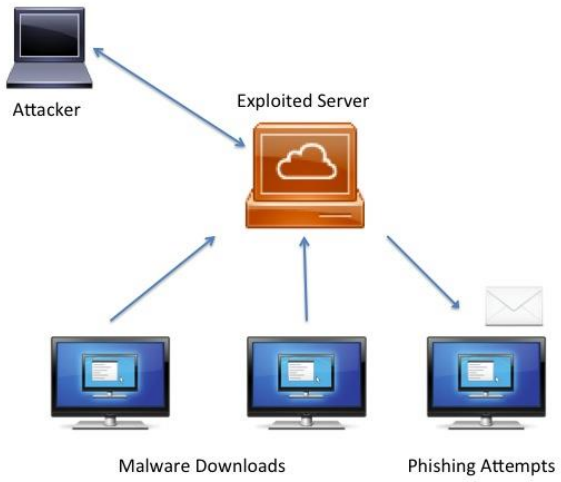
Figure 9. DDoS Reconnaissance



Exploitation and Expansion

After the potential victims are identified, they are targeted for exploitation so that the attacker can control the targeted system. The exploited system can now become a part of the DDoS infrastructure. Depending on the needs of the attacker, the victim machine may become a C2 server, send DDoS traffic, or propagate exploits to other machines. After time has passed, the botnet can grow to thousands, even millions, of hosts.

Figure 10. DDoS Infrastructure Components



It is important to note that not all hosts participating in a DDoS attack are victims of an exploit. Sometimes people who are sympathetic to a political cause willingly install DDoS software to harm a specific target. Likewise, botnets are used for purposes other than DDoS attacks.

Command and Control

Botnets require maintenance. Internet Relay Chat (IRC), a form of real-time text messaging, uses a client/server model and is also a common botnet communication protocol. The zombie clients and the C2 servers must communicate to deliver instructions to the clients, such as timing an attack or updating malware. A peer-to-peer (P2P) botnet model is more difficult to detect and disrupt because the connections are many-to-many, reducing the risk that an offline C2 server will disrupt operations.

Testing

A botnet reaches critical mass when there are enough hosts to generate traffic with enough bandwidth to saturate the victim. When the botnet reaches this point, there will likely be a testing period. Victims of the testing will see a large amount of traffic over a few seconds or minutes. The attacker can assess the effectiveness of the attack and make adjustments prior to creating the sustained attack. Often the traffic in a sustained attack changes over time, and the attacker will test these changes to maximize the impact on the victim.

Sustained Attack

The attacker determines when to instruct the botnet clients to begin sending traffic to the targeted infrastructure. The main body of the DDoS attack may last from hours to weeks, depending on the motives of

the attacker. Layer 7 attacks are becoming more popular, and they come mostly in the form of HTTP GET floods, SSL GET floods, and HTTP POST floods. Amplification attacks are increasing in popularity.

Network Identification Technologies

To be properly prepared to defend the network infrastructure from DDoS attacks, it is extremely important to know as soon as possible that there is anomalous behavior, malicious or otherwise, occurring in the network. Having a pre-emptive awareness of malicious or nefarious behaviors and other incidents in the network will go a long way toward minimizing any downtime that impacts the network's data, resources, and end users.

The following is a partial list of tools and technologies that are available--some of which are probably already present in the network—to help aid in the detection, identification, and subsequent classification of anomalous network events. These tools and technologies will help focus on Indicators of Compromise (IOC).

User/Customer Call

We are all too familiar with the phone call we get from our end user, customer, or even sometimes from our parents and grandparents! It usually starts with "The Internet is down. Can you help me?" Well, in most cases, we can be certain that the entire Internet itself is not down but there is some factor, or factors, that are impeding our ability to connect to the server, application, data, etc. we need to access. Regardless of the specifics of the scenario, we want to prevent an end user from telling us of a problem. Although requests from end users are sometimes the first time we find out about a network problem, we would rather be proactively notified of an issue prior before the users discover it. The balance of our list will help us do just that.

Anomaly Detection

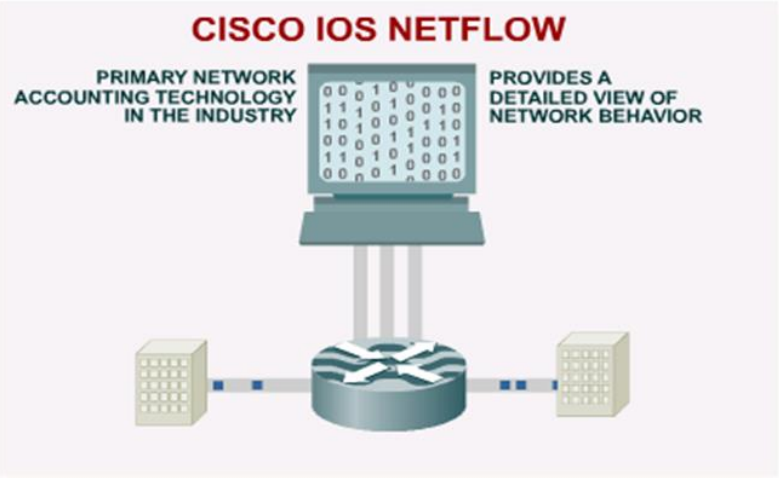
As with many of these techniques, we need established baselines for network performance. These can include, but are not limited to, bandwidth usage, device CPU utilization, and traffic type breakdowns. It is simply impossible to detect changes in the network baseline if we have not established these baselines.

Networks and network-enabled devices constantly create traffic. However, this traffic follows certain patterns according to application and user behavior. Analyzing these patterns allows us to see what is *not* normal. The key is to collect traffic information (NetFlow) and calculate various statistics to compare against a baseline. The resulting abnormalities are then analyzed in more detail.

Cisco IOS NetFlow

Cisco IOS NetFlow is a form of network telemetry that Cisco routers and switches can collect locally or push.

Figure 11. Cisco IOS NetFlow

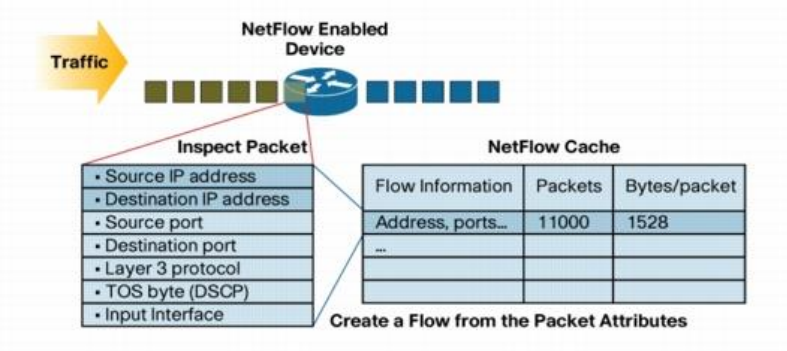


Data provided through NetFlow is similar to information in a phone bill. The user can view who is talking (source and destination IP address) and how long the conversations last (amount of traffic in terms of bytes and packets).

Figure 12 highlights the seven key parameters (as used in NetFlow version 5) that are inspected in each packet to determine whether a new flow should be created. If any of the seven fields differs from flows that have previously been created, a new flow is created and added to the NetFlow cache. The seven fields are as follows:

- Source IP address
- Destination IP address
- Source port
- Destination port
- Layer 3 protocol
- TOS byte
- Input interface

Figure 12. NetFlow Key Parameters



NetFlow data can be exported from network devices to a variety of open source and commercial NetFlow Collection tools. The Cisco Cyber Threat Defense Solution is an effective method of collecting and analyzing NetFlow data. Cyber Threat Defense brings together the work of Cisco and Lancope to quickly and effectively identify anomalous behavior in the network and provide insight into how some of this behavior can be addressed. For more details on this solution, see Cisco Cyber Threat Defense.

NetFlow Output Example: Financial Distributed Denial of Service Attacks Targeting Financial Institutions

Cisco IOS NetFlow data on Cisco IOS routers and switches aided in the identification of IPv4 traffic flows that could have been attempts to perform the DDoS attacks against financial institutions. The following example shows NetFlow output that indicates the types of traffic flows seen during the DDoS events:

```
router#show ip cache flow
IP packet size distribution (90784136 total packets):
  1-32  64  96 128 160 192 224 256 288 320 352 384 416 448 480
  .000 .698 .011 .001 .004 .005 .000 .004 .000 .000 .003 .000 .000 .000 .000
  512 544 576 1024 1536 2048 2560 3072 3584 4096 4608
  .000 .001 .256 .000 .010 .000 .000 .000 .000 .000 .000
IP Flow Switching Cache, 4456704 bytes
 1885 active, 63651 inactive, 59960004 added
 129803821 ager polls, 0 flow alloc failures
 Active flows timeout in 30 minutes
 Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 402056 bytes
 0 active, 16384 inactive, 0 added, 0 added to flow
 0 alloc failures, 0 force free
 1 chunk, 1 chunk added
 last clearing of statistics never
Protocol        Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
-------        Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet    11393421      2.8        1    48      3.1       0.0       1.4
TCP-FTP         236      0.0       12    66      0.0       1.8       4.8
TCP-FTPD         21      0.0    13726  1294      0.0      18.4       4.1
TCP-WWW       22282      0.0       21  1020      0.1       4.1       7.3
TCP-X           719      0.0        1    40      0.0       0.0       1.3
TCP-BGP           1      0.0        1    40      0.0       0.0      15.0
TCP-Frag      70399      0.0        1   688      0.0       0.0      22.7
TCP-other     47861004     11.8        1   211     18.9       0.0       1.3
UDP-DNS         582      0.0        4    73      0.0       3.4      15.4
UDP-NTP       287252      0.0        1    76      0.0       0.0      15.5
UDP-other     310347      0.0        2   230      0.1       0.6      15.9
ICMP          11674      0.0        3    61      0.0      19.8      15.5
IPv6INIP         15      0.0        1  1132      0.0       0.0      15.4
GRE               4      0.0        1    48      0.0       0.0      15.3
Total:        59957957     14.8        1   196     22.5       0.0       1.5
SrcIf       SrcIPaddress    DstIf       DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0       192.168.10.201  Gi0/1       192.168.60.102  06 0984 0050     1
Gi0/0       192.168.11.54   Gi0/1       192.168.60.158  06 0911 0035     3
Gi0/1       192.168.150.60  Gi0/0       10.89.16.226    06 0016 12CA     1
Gi0/0       192.168.10.17   Gi0/1       192.168.60.97   11 0B89 0050     1
```

```
Gi0/0       10.88.226.1     Gi0/1       192.168.202.22  11 007B 007B    1
Gi0/0       192.168.12.185  Gi0/1       192.168.60.239  11 0BD7 0050    1
Gi0/0       10.89.16.226    Gi0/1       192.168.150.60  06 12CA 0016    1
router#
```

In the preceding example, there are multiple flows for **UDP** port **80 (hex value 0050)**. In addition, there are also flows for **TCP** port **53 (hex value 0035)** and **TCP** port **80 (hex value 0050)**.

The packets in these flows may be spoofed and may indicate an attempt to perform these attacks. It is advisable to compare the flows for **TCP** port **53 (hex value 0035)** and **TCP** port **80 (hex value 0050)** to normal baselines to aid in determining whether an attack is in progress.

As shown in the following example, to view only the packets on UDP port 80 (hex value 0050), use the **show ip cache flow | include SrcIf|_11_.*0050** command to display the related Cisco NetFlow records.

UDP Flows

```
router#show ip cache flow | include SrcIf|_11_.*0050
SrcIf     SrcIPaddress   DstIf     DstIPaddress  Pr SrcP DstP Pkts
Gi0/0     192.168.12.110  Gi0/1     192.168.60.163 11 092A 0050   6
Gi0/0     192.168.11.230  Gi0/1     192.168.60.20  11 0C09 0050   1
Gi0/0     192.168.11.131  Gi0/1     192.168.60.245 11 0B66 0050  18
Gi0/0     192.168.13.7    Gi0/1     192.168.60.162 11 0914 0050   1
Gi0/0     192.168.41.86   Gi0/1     192.168.60.27  11 0B7B 0050   2
router#
```

Packet Capture

Whereas NetFlow can provide macro analytic details of the traffic traversing the network, packet captures can provide the micro analytic details, such as the actual data (or words used) in a conversation. There will be certain situations in which there is simply no substitute for looking at the packets on the wire. Packet capture can be accomplished on Cisco network devices in a number of ways:

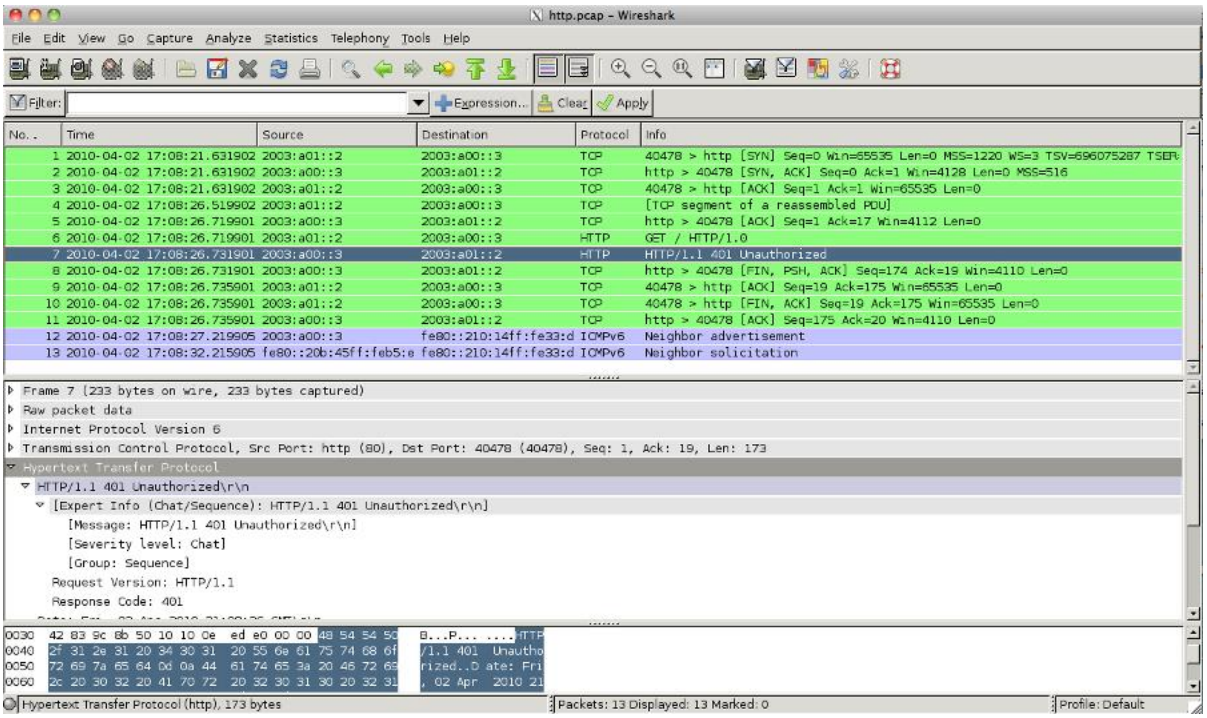
- SPAN/RSPAN/ERSPAN
- VACL Capture
- Router IP Traffic Export (RITE)
- Embedded Packet Capture (EPC)
- Firewall Packet Capture

A number of open source tools, such as tcpdump, snoop, and Wireshark (http://www.wireshark.org), can drill down into the packet contents from packet captures. In addition, it is important to know that some of these tools can look into and match specific fields in the packet (for example, source and destination IP, protocol, and

length.) Some tools can also display the top ports or protocols used in the captures, which could help identify potential DoS activity.

The following is an example of packet capture output that is being further analyzed by Wireshark:

Figure 13. Wireshark Packet Capture Analysis



ACLs and Firewall Rules

Although the primary purpose of access control lists (ACLs) and firewall rules is to filter traffic to and through various ingress and egress points of the network, they can also enhance the visibility of the traffic flowing through the network.

The following documents provide guidelines for using various types of ACLs to filter traffic and describe how ACL logging can be used to gain an understanding of the type of traffic that is allowed and denied throughout the network:

- Understanding Access Control List Logging
- Transit Access Control Lists: Filtering at Your Edge
- Protecting Your Core: Infrastructure Protection Access Control Lists

Firewall Syslog Output Example: Financial Distributed Denial of Service Attacks Targeting Financial Institutions

The following example of firewall syslog messages indicates the types of traffic being sent, and subsequently dropped, by firewalls during the DDoS events that took place against financial institutions in September and October 2012.

```
firewall#show logging | grep 106023
 Oct 04 2012 00:15:13: %ASA-4-106023: Deny udp src outside:192.0.2.18/2944
    dst inside:192.168.60.191/80 by access-group "tACL-Policy"
 Sep 04 2012 00:15:13: %ASA-4-106023: Deny udp src outside:192.0.2.200/2945
    dst inside:192.168.60.33/80 by access-group "tACL-Policy"
firewall#
```

In the preceding example, the messages logged for the tACL *tACL-Policy* show potentially spoofed **IPv4** packets for **UDP port 80** sent and dropped by the firewall. This was the type of traffic being seen during DDoS attacks against financial institutions.

The following document provides information about using syslog to identify incidents: Identifying Incidents Using Firewall and Cisco IOS Router Syslog Events.

DNS

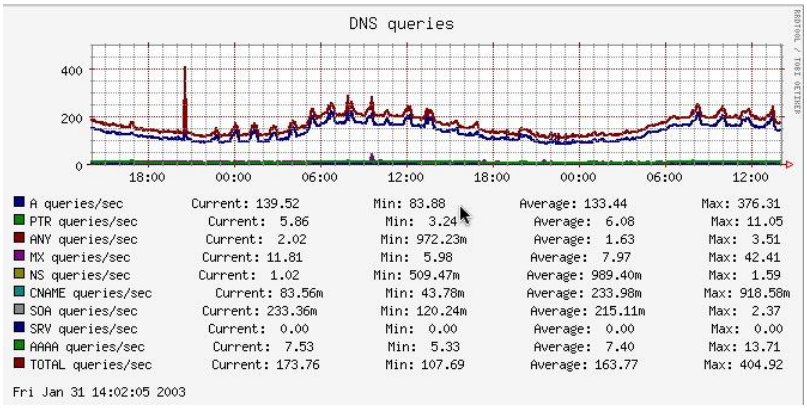
DNS is a "background" service we do not often think about, but it is actually used many times each day by every user in every organization. A profusion of application types use name-based lookups using DNS. These include the following:

- Web browsers
- Email servers
- Web servers
- Malware such as trojans and bots running on compromised hosts

Administrators can *and should* examine DNS logs and statistics as regularly as possible. This DNS-related information should then be correlated with other forms of telemetry (such as NetFlow, packet capture, and application logs) discussed in this section to further investigate potential malicious behavior in the network. For example, there may be a baseline level of DNS queries from certain sources and for certain domains/sites, and a spike or change can indicate potential malicious behavior in the network.

The following chart from http://oss.oetiker.ch/rrdtool/ provides a snapshot of the types, and corresponding amounts, of DNS queries. Although the graph itself is dated, it is easy to see the spike in DNS A(lias) queries that took place between 20:00 and 21:00 the previous night. After averaging roughly 133 A queries per second over a period of time (which is undetermined from the graph), the number of A queries per second surged to a peak of 376. This type of anomalous behavior can be quickly identified, and subsequently analyzed, using DNS analytics.

Figure 14. DNS Query Snapshot



http://oss.oetiker.ch/rrdtool/

Other warning signs, as detailed in the following article, include the presence of new domains (*young domains*) being queried, domains that only a handful of employees are referencing (*esoteric domains*), and a large number of failed DNS queries or lookups (*lookup failures*). For more information, see Three Signs of Malware Revealed in DNS Traffic.

For additional information about general best practices, network protections, and attack identification techniques that operators and administrators can use for implementations of the DNS protocol, see DNS Best Practices, Network Protections, and Attack Identification.

Sinkholes

Sinkholes are an often-overlooked source of pertinent network traffic details because they are frequently viewed as simply a means of diverting traffic to an unused area of the network. While blackholing traffic is used to deflect undesirable traffic from end user devices and data, sinkholing traffic provides additional advantages. Within the sinkhole network, it is advantageous to include tools and devices that can provide monitoring and added visibility into the traffic that is diverted there.

For additional information about using sinkholes to capture and analyze anomalous or undesirable network traffic, see Sinkholes in *Worm Mitigation Technical Details*.

Intrusion Prevention/Detection System Alarms

Another good source of network IOCs are the Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) devices that are deployed at strategic points in the network. IDS shuns sources and performs TCP resets of suspect connections, and IPS helps prevent compromises by dropping traffic inline. Although the focus of IDS and IPS is to detect and prevent bad traffic, it is advisable to use the alarms and log messages from these devices as early warning indicators of anomalous, and potentially malicious, traffic in the network. False

positives can be expected when using IPS, so not all IPS-related alarms indicate an attack or even unexpected network activity. Even so, the visibility provided by IPS devices is valuable and should be correlated with the other types of identification information detailed throughout this section.

The following table provides an overview of the Cisco IPS signatures that could trigger events on potential attempts that were associated with the DDoS attacks against financial institutions that took place in September and October 2012.

CVE ID	Signature Release	Signature ID	Signature Name	Enabled	Severity	Fidelity*	Notes
NA	S672	1493/0	Distributed Denial of Service on Financial Institutions	Yes	High	90	—
NA	S593	2152/0	ICMP Flood	No	Medium	100	Retired
NA	S572	4002/0	UDP Host Flood	No	Low	75	Retired
NA	S520	4004/0	DNS Flood Attack	No	Medium	85	Retired
NA	S593	6009/0	SYN Flood DoS	No	Medium	85	Retired
NA	S573	6901/0	Net Flood ICMP Reply	No	Informational	100	Retired
NA	S573	6902/0	Net Flood ICMP Request	No	Informational	100	Retired
NA	S573	6903/0	Net Flood ICMP Any	No	Informational	100	Retired
NA	S573	6910/0	Net Flood UDP	No	Informational	100	Retired
NA	S573	6920/0	Net Flood TCP	No	Informational	100	Retired

* Fidelity is also referred to as Signature Fidelity Rating (SFR) and is the relative measure of the accuracy of the signature (predefined). The value ranges from 0 through 100 and is set by Cisco Systems, Inc.

Administrators could configure Cisco IPS sensors to perform an event action when an attack was detected and one of the signatures in the preceding table was triggered. The configured event action would result in preventive or deterrent controls to help protect against an attack that was attempting to carry out the attacks. As the notes in the table indicate, all but one of the signatures has been retired to increase the performance of Cisco IPS sensors while focusing on more current threats. That being said, if DDoS attacks are a concern for your organization, it is recommended that these signatures be enabled. The event action does not necessarily

have to be a preventative measure, such as dropping or resetting an existing connection; the action can be to notify administrators of potential DDoS attack attempts using alarms or log messages.

ASA Threat Detection

Cisco ASA threat detection consists of different levels of statistics gathering for various threats, as well as scanning threat detection, which determines when a host is performing a scan. Administrators can optionally shun any hosts determined to be a scanning threat.

Threat detection statistics can help administrators manage threats to the Cisco ASA; for example, enabling scanning threat detection provides statistics to help analyze the threat. Administrators can configure two types of threat detection statistics:

Basic threat detection statistics: Include information about attack activity for the system as a whole. Basic threat detection statistics are enabled by default and have no performance impact.

Advanced threat detection: Statistics track activity at an object level so the Cisco ASA can report activity for individual hosts, ports, protocols, or access lists. Advanced threat detection statistics can have a major performance impact, depending on the statistics gathered, so only the access list statistics are enabled by default.

Visit Configuring Threat Detection for more information about this feature.

Modern Tendencies in Defending Against DDoS Attacks

Challenges in Defending DDoS Attacks

The challenge in preventing DDoS attacks lies in the nature of the traffic and the nature of the "attack" because most often the traffic is legitimate as defined by protocol. Therefore, there is not a straightforward approach or method to filter or block the offending traffic. Furthermore, the difference between volumetric and application-level attack traffic must also be understood.

Volumetric attacks use an increased attack footprint that seeks to overwhelm the target. This traffic can be application specific, but it is most often simply random traffic sent at a high intensity to over-utilize the target's available resources. Volumetric attacks generally use botnets to amplify the attack footprint. Additional examples of volumetric attacks are DNS amplification attacks and SYN floods.

Application-level attacks exploit specific applications or services on the targeted system. They typically bombard a protocol and port a specific service uses to render the service useless. Most often, these attacks target common services and ports, such as HTTP (TCP port 80) or DNS (TCP/UDP port 53). For further details about mitigating application-level attacks, see Identifying and Mitigating the Distributed Denial of Service Attacks Targeting Financial Institutions.

Stateful Devices

Stateful devices do not provide complete coverage and mitigation for DDoS attacks because of their ability to monitor connection states and maintain a state table. Maintaining such information is CPU and memory intensive. When bombarded with an influx of traffic, the stateful device spends most, if not all, of its resources tracking states and further connection-oriented details. This effort often causes the stateful device to be the "choke point" or succumb to the attack.

For further information about stateful inspection, see the Stateful Inspection Overview section of the *Cisco ASA 5500 Series Configuration Guide*. Common stateful inspection devices and their role in threat mitigation are firewalls, IDS/IPS devices, load balancers, and web application firewalls.

Firewalls represent the most common stateful inspection devices in today's threat mitigation arsenal. In stateful firewall solutions, there is a component commonly known as the stateful packet inspection (SPI) engine. This is also referred to as DPI (deep packet inspection). This engine provides intelligence by looking into the packet flow to determine and define connection information and application-level details. For more details about firewall stateful inspection, see the Cisco IOS Software Stateful Packet Inspection section of the *Cisco IOS Firewall Design Guide*.

IDS/IPS devices are often deployed at the network core and/or edge and provide intelligent decision capabilities by using DPI to analyze and mitigate an array of attacks and threats. Moreover, DPI allows the IDS/IPS device to react to network events and traffic in real time, providing alerts or inline mitigation. For more details about IDS/IPS stateful inspection, see Cisco IOS Intrusion Prevention System.

Load balancers use SPI to make decisions based on the connections that traverse the load balancer function. For more details about the load balancer stateful inspection engine, see Is Your Load Balancer A Firewall?

Web application firewalls use SPI to evaluate web-based application flows, such as GET requests. For details about SPI in web application firewalls, see the Web Application Firewall page documented by the Open Web Application Security Project (OWASP).

Route Filtering Techniques

Remotely triggered black hole (RTBH) filtering can drop undesirable traffic before it enters a protected network. Network black holes are places where traffic is forwarded and dropped. When an attack has been detected, black holing can be used to drop all attack traffic at the network edge based on either destination or source IP address. For further information regarding RTBH filtering, see the Remotely Triggered Black Hole Filtering -- Destination Based and Source Based (PDF).

Note: RTBH filtering is supported on Cisco IOS, Cisco IOS-XE, and Cisco IOS-XR platforms. For more details, including using RTBH filtering for IPv6, see Remotely Triggered Black Hole Filtering in IP Version 6 for Cisco IOS, Cisco IOS XE, and Cisco IOS XR Software.

Unicast Reverse Path Forwarding

Network administrators can use Unicast Reverse Path Forwarding (uRPF) to help limit malicious traffic flows occurring on a network, as is often the case with DDoS attacks. This security feature works by enabling a router to verify the "reachability" of the source address in packets being forwarded. This capability can limit the appearance of spoofed addresses on a network. If the source IP address is not valid, the packet is discarded.

uRPF guards against IP spoofing by ensuring that all packets have a source IP address that matches the correct source interface according to the routing table. Normally, the security appliance examines only the destination address when determining where to forward the packet. uRPF instructs the security appliance to look also at the source address. For any traffic to be allowed through the security appliance, the security appliance routing table must include a route back to the source address. See RFC 2267 for more information.

To enable uRPF, enter this command: hostname(config)#**ip verify reverse-path interface** *interface_name*

uRPF works in two different modes: strict mode and loose mode. When administrators use uRPF in strict mode, the packet must be received on the interface that the security device would use to forward the return packet. uRPF in strict mode may drop legitimate traffic that is received on an interface that was not the firewall's choice for sending return traffic. Dropping this legitimate traffic could occur when asymmetric routing paths exist in the network.

When administrators use uRPF in loose mode, the source address must appear in the routing table. Administrators can change this behavior using the **allow-default** option, which allows the use of the default route in the source verification process. In addition, a packet that contains a source address for which the return route points to the Null 0 interface will be dropped. An access list may also be specified that permits or denies certain source addresses in uRPF loose mode.
Care must be taken to ensure that the appropriate uRPF mode (loose or strict) is configured during the deployment of this feature because it can drop legitimate traffic. Although asymmetric traffic flows may be a

concern when deploying this feature, uRPF loose mode is a scalable option for networks that contain asymmetric routing paths.

Geographic Dispersion (Global Resources Anycast)

A newer solution for mitigating DDoS attacks dilutes attack effects by distributing the footprint of DDoS attacks so that the target(s) are not individually saturated by the volume of attack traffic. This solution uses a routing concept known as Anycast. Anycast is a routing methodology that allows traffic from a source to be routed to various nodes (representing the same destination address) via the nearest hop/node in a group of potential transit points. This solution effectively provides "geographic dispersion." For details regarding geographic dispersion that uses Anycast to dilute a DDoS attack, see How whitehats stopped the DDoS attack that knocked Spamhaus offline.

Tightening Connection Limits and Timeouts

Antispoofing measures such as limiting connections and enforcing timeouts in a network environment seek to ensure that DDoS attacks are not launched or spread from inside the network either intentionally or unintentionally. Administrators are advised to leverage these solutions to enable antispoofing and thwart random DDoS attacks on the inside "zones" or internal network. To use connection limits and timeouts for DDoS defense purposes, see the Configuring Connection Limits and Timeouts section of the *Cisco ASA 5500 Series Configuration Guide*.

Caution: Oversubscription of stateful processes can cause a device to fail. For more details, see Stateful Devices.

Reputation-Based Blocking

Reputation-based blocking has become an essential component to today's web filtering arsenal. A common trend of malware, botnet activity, and other web-based threats is to provide a URL that users must visit for a compromise to occur. Most often such techniques as spam, viruses, and phishing attacks direct users to the malicious URL.

Reputation-based technology provides URL analysis and establishes a reputation for each URL. Reputation technology has two aspects. The intelligence aspect couples world-wide threat telemetry, intelligence engineers, and analytics/modeling. The decision aspect focuses on the trustworthiness of a URL. Reputation-based blocking limits the impact of untrustworthy URLs. For details about web reputation technology, see Cisco Web Reputation Technology. An example of reputation-based solutions is the Cisco Web Security Appliance and Cisco Email Security Appliance.

Global and crowd-sourced reputation information provides the most coverage in web reputation technology, and administrators may question which reputation engine or service to use and whether one is enough. The recommendation is to use multiple engines or services, such as the following:

- WatchGuard Reputation Authority
- WebSEO Analytics

Moreover, web reputation solutions with high coverage include Cisco Web Security Appliance, Imperva, Trend Micro, and others.

Another evolution is on the horizon for web reputation. Beyond the traditional attack, there is a continuous threat to the brand and business reputation. Many tools and services are available for organizations to protect manage their reputations. See References for more details regarding the available tools.

Access Control Lists

ACLs provide a flexible option to a variety of security threats and exploits, including DDoS. ACLs provide day zero or reactive mitigation for DDoS attacks, as well as a first-level mitigation for application-level attacks. An ACL is an ordered set of rules that filter traffic. Each rule specifies a set of conditions that a packet must satisfy to match the rule. Firewalls, routers, and even switches support ACLs. When the device determines that an ACL applies to a packet, it tests the packet against the conditions of all rules. The first match determines whether the packet is permitted or denied. If there is no match, the switch applies the applicable default rule (generally an implicit "deny all"). The device continues processing packets that are permitted and drops packets that are denied.

Note: Switches support port and VLAN ACLs.

ACLs are often used to protect networks and specific hosts from unnecessary or unwanted traffic via protocol/port filtering, although filtering may also be based on TCP options and flags. For example, ACLs can disallow HTTP traffic from a high-security network to the Internet. You could also use ACLs to allow HTTP traffic only to specific sites, using the IP address of the site to identify it in an IP ACL.

ACL filtering provides flexible mitigation options. The following list provides additional examples of the available filtering options:

- Layer 4 protocol
- TCP and UDP ports
- ICMP types and codes
- IGMP types
- Precedence level

- Differentiated Services Code Point (DSCP) value
- TCP packets with the ACK, FIN, PSH, RST, SYN, or URG bit set
- Established TCP connections

The following resources provide more details about ACL configuration and management:

- Configuring Commonly Used IP ACLs
- Configuring IP Access Lists
- Cisco Nexus 5500 Series NX-OS Software Configuration Guide - Configuring ACLs

DDoS Run Books

Early in 2013, the concept of DDoS run books gained a bit of prevalence. The premise behind a DDoS run book is simply to provide a "playbook" for an organization in the event that a DDoS attack arises. In essence, the run book provides crisis management (better known as an incident response plan) in the event of a DDoS attack. The run book provides details about who owns which aspects of the network environment, which rules or regulations must still be adhered to, and when to activate/instrument certain process, solutions, and mitigation plans. A case study and an example template for DDoS run books are in References.

Manual Responses to DDoS Attacks

It is worth nothing that manual responses to DDoS attacks focus on measures and solutions that are based on details administrators discover about the attack. For example, when an attack such as an HTTP GET/POST flood occurs, given the information known, an organization can create an ACL to filtering known bad actors or bad IPs and domains. When an attack such as Slowloris arises, administrators can configure or tune firewalls or load balancers to limit connection attempts, as discussed in Tightening Connection Limits and Timeouts. Manual responses also include obscuring IP addressing schemes, using Network Address Translation (NAT), and creating custom IPS signatures or application layer inspection policies based on attack traffic, baselines, and industry events.

The response process is often overlooked. As mentioned in DDoS Run Books, organizations often do not have a process or a plan and thus rely exclusively on manual responses. Proactive solutions and constant monitoring and configuration updates should be the common practice, with manual responses regarded as rare solutions.

Traffic Scrubbing and Diversion

Because of the prevalence of DDoS attacks in recent years, numerous organizations and businesses now provide DDoS protection as a service. While there are various ways to accomplish DDoS protection and attack mitigation, most providers offer an inline solution in which an organization's traffic can be sent to or through the

service entity. The service then filters out the offending traffic and reinjects the good traffic into the organization. A few of the most prevalent in the industry are in the following list:

- Prolexic Technologies: DoS and DDoS Protection
- AT&T Internet Protect: Distributed Denial of Service Defense
- Verizon: DoS Defense Services
- Arbor Networks: Pravail Availability Protection System (APS)

At its core, the Prolexic DDoS Solution uses Prolexic's PLX routed platform service (the most basic Prolexic DDoS mitigation solution). In general it allows a customer to route traffic to the Prolexic environment where it will be inspected and filtered based on anomalies, known misbehaviors, and provided details. Subsequently the "clean" traffic will be routed back into the customer environment. For more details regarding the PLXrouted solution, see the PLXrouted datasheet (PDF). For more details regarding Prolexic solutions, see their DDoS mitigation service portal.

The AT&T Internet Protect: Distributed Denial of Service Defense solution is for AT&T customers looking for DDoS protection. Because AT&T already runs the network that the customer's traffic is traversing, AT&T uses its expertise and intelligent solutions in the backbone to filter any malicious or ill-advised traffic before it enters the customer environment. In addition, the defense solution analyzes netflow. If any flows pose a threat, they are routed to a "scrubbing environment" where the traffic is filtered, allowing the remaining "good" traffic to continue to the customer environment. For more details about the AT&T Internet Protect - Distributed Denial of Service Defense solution, see AT&T Internet Protect - Distributed Denial of Service Defense Solution Product Brief (PDF).

The Verizon DoS Defense Service works much like those previously discussed in that it monitors traffic and routes traffic through the Verizon environment to be scrubbed, allowing the good traffic to be routed back to the protected customer environment. For details, including Service Level Agreement (SLA) information, see the Verizon DoS Defense page.

The Arbor Networks Pravail Availability Protection System (APS) solution is an example of an onsite (on premise) solution. The unit sits inline in a customer environment and has a connection back to the Arbor intelligence backend. This service incorporates intelligence and information learned from the Arbor Security Engineering and Response Team (ASERT). Coupled with techniques such as baselining and anomaly detection, Arbor APS is a prominent DDoS solution. See the Pravail Availability Protection System solution page.

Conclusion

With the number of DDoS attacks increasing over the past year, it is important that network engineers, designers, and operators build services and monitor networks in the context of defending against DDoS attacks.

This document presented the different attack types, their categories, and the techniques they use. It presented classic and current methodologies in the identification, classification, and mitigation of DDoS attacks. Because networks vary, we do not aim to provide an all-inclusive DDoS mitigation document that applies to every organization, but we have attempted to describe the tools available for dealing with DDoS attacks.

Using the Cisco six-phase DDoS mitigation model is a good start, and may also be continuously revisited when creating a sound DDoS policy. Preparation is a key part of any DDoS strategy. Ensure that the tools to be used for DDoS identification are tested, functioning, and in the proper locations and that networking staff is trained and capable of operating the necessary tools for DDoS identification.

There is nothing worse than having a network impaired or down and not having a good plan to identify and classify the problem. DDoS attacks can be hard to identify. Many network problems have the look and feel of a DDoS at the beginning, but then complete analysis rules out a DDoS attack. Knowing the baseline traffic and network utilization is the key to understanding a suspected DDoS condition.

The techniques in this white paper provide network administrators with information and tools necessary to identify and mitigate DDoS problems.

References

Cisco IOS Firewall Design Guide
//www.cisco.com/en/US/prod/collateral/vpndevc/ps5708/ps5710/ps1018/product_implementation_design_guide09186a00800fd670.html
DNS Best Practices, Network Protections, and Attack Identification
//www.cisco.com/web/about/security/intelligence/dns-bcp.html
Deep Inside a DNS Amplification DDoS Attack
http://blog.cloudflare.com/deep-inside-a-dns-amplification-ddos-attack
Real World DNS Abuse: Finding Common Ground
http://blogs.cisco.com/security/real-world-dns-abuse-finding-common-ground/
Defenses Against TCP SYN Flooding Attacks
//www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_9-4/syn_flooding_attacks.html
How whitehats stopped the DDoS attack that knocked spamhaus offline
http://arstechnica.com/security/2013/03/how-whitehats-stopped-the-ddos-attack-that-knocked-spamhaus-

offline/
Identifying and Mitigating the Distributed Denial of Service Attacks Targeting Financial Institutions
http://tools.cisco.com/security/center/viewAMBAlert.x?alertId=27115
Remotely Triggered Black Hole Filtering in IP Version 6 for Cisco IOS, Cisco IOS XE, and Cisco IOS XR Software
//www.cisco.com/web/about/security/intelligence/ipv6_rtbh.html

NetFlow

How Cisco IT Uses NetFlow to Capture Network Behavior, Security, and Capacity Data
//www.cisco.com/web/about/ciscoitatwork/network_systems/network_data_monitoring_and_reporting_web.html
Cisco IOS NetFlow
http://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-netflow/index.html
NetFlow collectors help with collection, analysis, and display of NetFlow data exported from network devices:

- NFDUMP
  http://nfdump.sourceforge.net/
- NfSen is a graphical web-based front end for the *nfdump* tools:
  http://nfsen.sourceforge.net/

Reputation Management Tools

http://searchengineland.com/5-free-deep-reputation-management-checking-tools-163551
https://www.openforum.com/articles/online-reputation-management-tools/
http://socialmouths.com/blog/2013/04/25/manage-your-online-reputation/

DDoS Run Book Case Study and Template

https://www.sans.org/reading-room/whitepapers/incident/practical-social-media-incident-runbook-34252 (PDF)
https://www.whitehatsec.com/blog/checklist-to-prepare-yourself-in-advance-of-a-ddos-attack/

---

materials linked from the document is at your own risk. Cisco reserves the right to change or update this document without notice at any time.

Back to Top