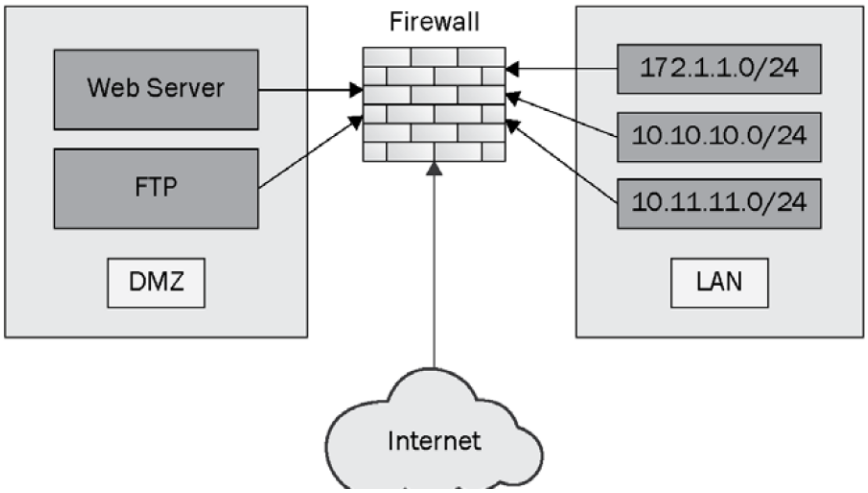
• Chapter 8, Network Firewall Logs Analysis

Organizations usually use a firewall to separate their network into three security zones: **LAN**, **DMZ**, and **WAN**. Each zone consists of a single interface or a group of interfaces, to which security policies and rules are applied. The **LAN** zone is the organization's internal zone, which includes internal servers, workstations, printers, and so on; **DMZ** is the zone that includes the organization's public-facing applications such as email and websites, and the **WAN** zone is the internet and untrusted zone or a zone that is outside the control of the organization.

The firewall's position between the LAN, DMZ, and WAN zones, as well as between the same zone subnets, allows the firewall to provide us with valuable logs so that we can track the communication between subnets and zones. See *Figure 8.1*:



The firewall log fields are called **Log Timestamp**, **Source IP**, **Source Port**, **Destination IP**, **Destination Port**, **Source Interface Zone**, **Destination Interface Zone**, **Device Action**, **Sent Bytes**, **Received Bytes**, **Sent Packets**, **Received Packets**, **Source Geolocation country**, and **Destination Geolocation country**. We'll look at these in detail in the following subsections.

• Chapter 9, Investigating Cyber Threats by Using Firewall Logs

• Investigating reconnaissance attacks

The external reconnaissance phase is usually conducted to collect information about the target victim's emails, IPs,services, open ports, vulnerabilities, and so on

The internal reconnaissance phase is usually conducted by threat actors after gaining initial access to the victim's system to discover the installed binaries and logged-on users on the

infected system, machines in the same network running services such as WinRM and RDP for lateral movement, and so on

• Investigating lateral movement attacks

• Remote desktop application (RDP)

it is crucial to analyze suspicious initiation of RDP
connections and determine whether they originated between regular workstations. This is significant since most RDP connections are typically established from a workstation to a jump server, or from an IT administrator's workstation to another workstation within the network, as part of routine job responsibilities. Additionally, examining the timing of RDP connections is important to detect any connections initiated outside of regular working hours.

• Windows admin shares

• Firstly, you should observe suspicious SMB communications – for example, SMB communications to a non-file-sharing server or between two regular workstations.
• Next, you need to calculate the sum of the transferred bytes from the source workstation to the target workstation, and the received bytes from the target workstation by the source workstation, to understand the attacker's purpose for the SMB communications.

• PowerShell Remoting

Note: If you are running an environment where system admins depend on PowerShell Remoting as a remote administration tool, you can develop detection use cases to detect any PowerShell Remoting activities from non-admin machines to other systems

• Investigating C&C and exfiltration attacks

C&C or command and control is when the attacker's server communicates with the victim's machine by either configuring malware installed on the victim's machine to send reverse shell to the attacker C&C server or exploiting a service run by the victim, such as the SSH or Telnet services, to send instructions and commands to be executed on the victim's machine.

• Suspicious traffic to external IPs

If you have a suspicion of C&C communications traffic from the internal victim machine to the external attacker server, you need to use the firewall logs to investigate the following attributes (Destination IP,Suspicious ports,Suspicious communication patterns)
Note:communications, including a huge number of requests from the victim's
machine (source IP) to the attacker's server (destination IP) and heartbeat requests, which are

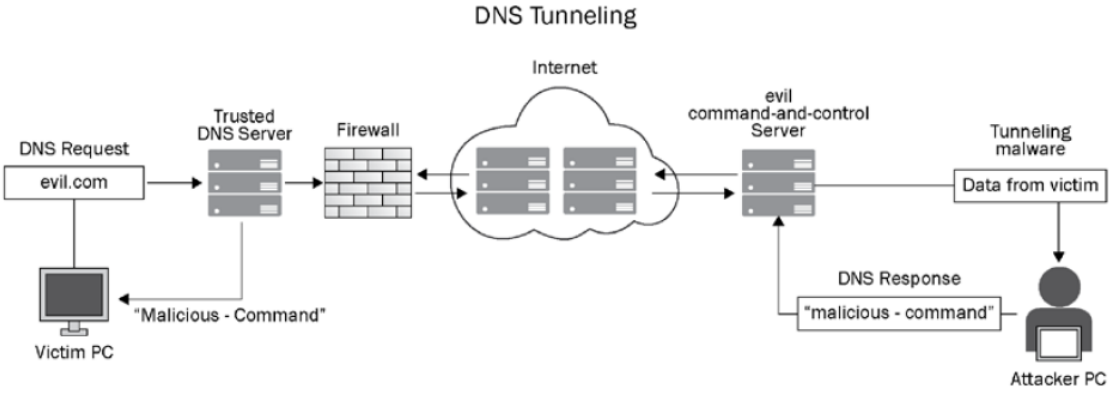
also called **malware beaconing communication**. **Malware beaconing** is when the attacker configures their malware to send requests from the victim's machine to the attacker's server asking for instructions or delivering gathered data at regular intervals (such as daily, every 7 hours, every hour, every 10 minutes, and so on). This strategy is employed by attackers to evade detection

• DNS tunneling

DNS tunneling is when an attacker abuses the DNS traffic by tunneling another protocol through it. DNS tunneling can be used for both C&C and data exfiltration

To understand simply how DNS tunneling works in C&C attacks, let's break it down into the following steps (see also *Figure 9.9*):

1. The attacker registers a domain (`evil.com`) and maps it to the IP address of the server under their control.
2. The attacker compromises a victim's system with configured malware to communicate with its C&C server by using the DNS tunneling technique. The malware starts sending DNS requests to resolve the attacker's domain (`evil.com`).
3. Then, the recursive DNS server routes the DNS query until it reaches the authoritative DNS server that is controlled by the attacker.
4. The attacker's server contains the DNS tunneling software that answers the DNS query with instructions to be executed by the installed malware on the victim's system.



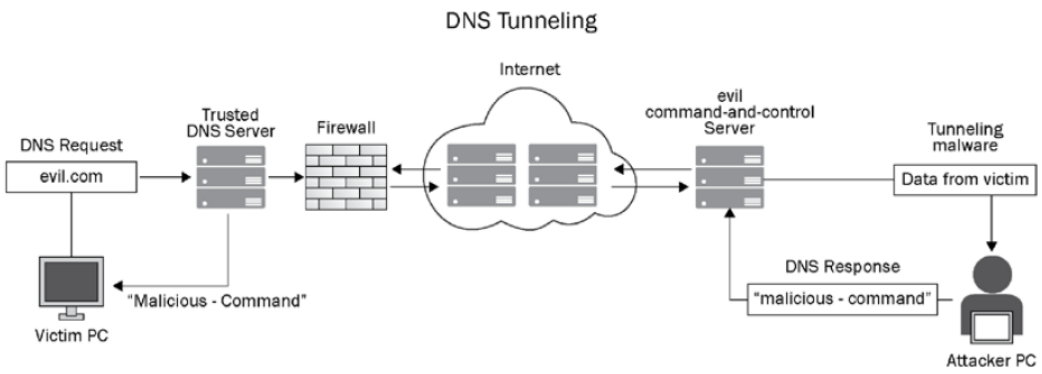


Figure 9.9 – Establishing command and control channel by using the DNS tunneling technique

To understand simply how DNS tunneling works in data exfiltration attacks, let's break it down into the following steps (see also *Figure 9.10*):

1. The attacker registers a domain (`evil.com`) and maps it to the IP address of the server under their control.
2. The attacker compromises a victim's system with configured malware to exfiltrate the data to their own server by using the DNS tunneling technique.
3. The malware starts to exfiltrate the data by adding it as a subdomain to the attacker's domain. For example, if the malware wants to exfiltrate the `P@ssw0rd` word, it requires sending DNS requests to resolve `P@ssw0rd.evil.com`.
4. Then, the recursive DNS server routes the DNS query until it reaches the authoritative DNS server that is controlled by the attacker.

detect and investigate DNS tunneling activities using the firewall logs

- ❖ Policy violation
- ❖ High number of DNS requests: Investigate a high number of DNS requests from a single host.
- ❖ High volume of DNS traffic
- ❖ Geographic location of DNS server
- ❖ Cross-reference with known threat intelligence

• Date exfiltration

To investigate potential data exfiltration activities, you should focus on the following attributes of the firewall logs (Number of connections per day,Volume of sent bytes,Volume of sent bytes per day,Reputation and category of destination IP address)

• Investigating DoS attacks

meant to consume resources such as machines, websites,
applications, or networks, making them inaccessible to their intended users

- **Distributed denial-of-service** :These are like DoS attacks, except that requests are sent from many clients instead of just one.
- **Application layer DoS attacks**: This occurs when the attacker attacks the application itself to make it inaccessible to its intended users. The application could be a website, email portal,and so on. The most common type of application layer attack is the HTTP flood attack. This is when the attacker configures its controlled bots into sending various HTTP requests to a specific URL of the website by using different IP addresses.
- **Protocol DoS attacks :**

  - **Protocol DoS attacks**: This occurs when the attacker exploits the work method of the protocol to exhaust the system resources, making it unavailable to legitimate traffic. An example of a protocol DoS attack is the **SYN flood attack**. In a SYN flood attack, the attacker takes advantage of the **TCP three-way handshake** process that requires the server to respond to the client with a `SYN-ACK` packet and wait for them to complete the aforementioned process. The attacker sends several `SYN` packets to the server by using several spoofed IP addresses. The server responds to each packet via a `SYN-ACK` packet, requesting the client to complete the three-way handshake process. The spoofed IPs never respond, and the server keeps waiting until it crashes due to the long wait for those many responses. See *Figure 9.14*:

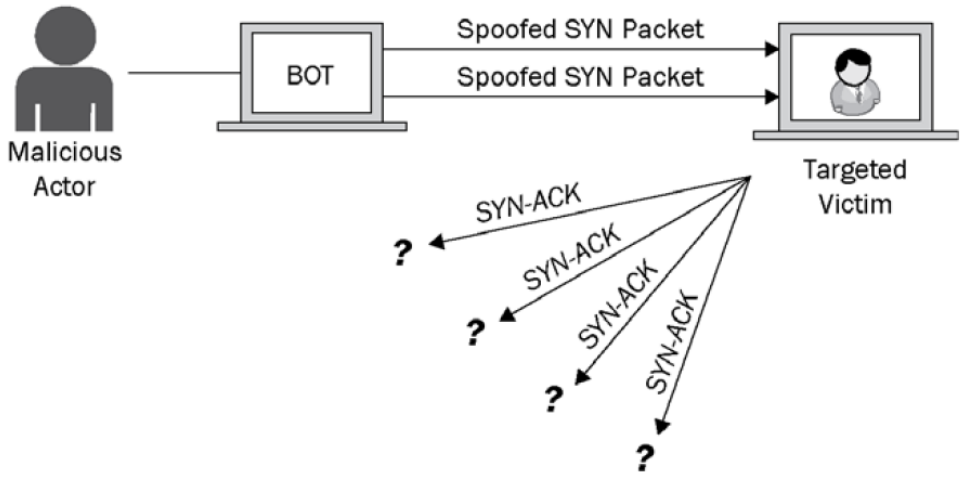


Figure 9.14 – SYN flood attack

- **Volumetric DoS attacks**: This occurs when the attacker uses his server(s) to generate massive volumes of traffic to completely consume the victim's line bandwidth and create a traffic jam that makes the target resources unreachable to legitimate traffic. An example of a volumetric attack is the **DNS amplification attack**. To conduct a DNS amplification attack, the attacker must follow the following steps (see also *Figure 9.15*):

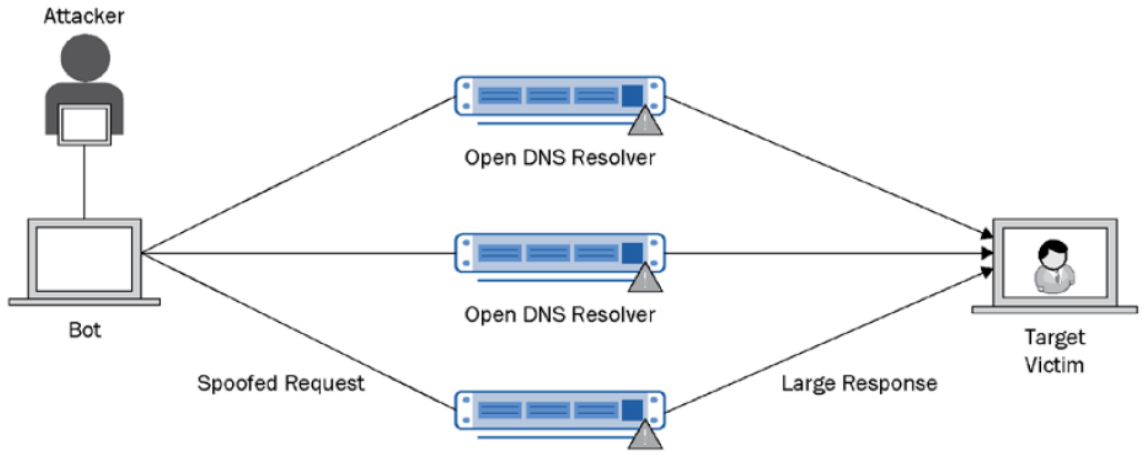
  I. Locate several DNS servers that can perform recursive lookups.

  II. Send queries to those servers to get a DNS record of the domain that the attacker controls by sending a recursive lookup query to their own DNS server.

  III. Respond with a 4,000-byte `TXT` record. The response is cached and saved on those DNS servers.

  IV. Ask his bots to send **spoofed DNS requests** (which seem to be sent from the victim's IP) to the legit DNS servers located in the first step, often passing an argument such as *any* with the DNS request in order to receive the largest possible response.

  V. The legit DNS servers send the huge answer (response) to the spoofed (victim) IP.



• Chapter 10, Web Proxy Logs Analysis

The objective of this chapter is to learn the value of the web proxy logs and the provided information in the proxy logs and understand the valuable fields of the proxy logs, such as the (log timestamp, source IP, source port, destination IP, destination port, response status code, username, user agent, device action, sent bytes, received bytes, referrer URL, accessed domain and URL, HTTP method, and website category.)

❖ The response status code (sc-status):

- 1xx – Informational: Means the request was received
- 2xx – Successful: Means the request was successfully received and accepted
- 3xx – Redirection: Means the request to a specific page was redirected to another
- 4xx – Client error: Means the request can't be proceeded due to a client error, such as requesting a non existent page or unauthorization to perform such request

- 5xx – Server error: Means the server failed to respond to the valid request

❖ The HTTP method (cs-method)
The HTTP method is the method used by the client in the HTTP request to access the web server resources; in other words, this field shows the way that the client wants to deal with the web server.

- GET: Used to request and retrieve data from the web server
- POST: Used to send data to the web server
- HEAD: Same as GET, but it is used to just request headers
- DELETE: Used to delete data from the web server
- CONNECT: Used to create a tunnel through the proxy server for secure protocols, such as HTTPS
- OPTIONS: Used to get the allowed HTTP methods by the web server

The MIME type (Content-Type)

The media type (also known as **Multipurpose Internet Mail Extensions**, or the **MIME** type) signifies the characteristics and structure of a document, file, or collection of bytes employed in the communication between the client and server. The content type field value format is (`type/subtype;parameter=value`), for example, `text/plain;charset=UTF-8`.

The common MIME types are given in the following table:

File Extension	File Type	MIME Type
`.csv`	Comma-separated values (CSV)	`text/csv`
`.doc`	Microsoft Word	`application/msword`
`.gz`	GZip compressed archive	`application/gzip`
`.exe`	Executable file	`application/octet-stream`

Table 10.1 – Samples of MIME types used in web communications

• Chapter 11, Investigating Suspicious Outbound Communications (C&C Communications) by Using Proxy Logs

• Suspicious outbound communications alerts

• Investigating suspicious outbound communications (C&C communications)

• Investigating the web domain reputation
• Investigating suspicious web target domain names

TLD Domain	Preference Reason
.xyz	Easy registration and widespread usage
.top	Popularity and low cost
.info	General-purpose TLD with broad usage
.pw	Easy registration and low cost
.ru	High number of legitimate websites
.cn	High number of legitimate websites
.tk	Widespread usage and free registration
.biz	General-purpose TLD with broad usage
.online	Widespread usage and easy registration

Table 11.1 – Sample of TLDs used for malicious activities

• Investigating the requested web resources

- ❖ Domain generation algorithm (DGA)

serves as a strategic technique employed by malware authors
to establish communication between the malware and multiple dynamically generated domains that serve as C&C servers. The DGA algorithm is integrated into the malware installed on the victim's system to generate a list of hundreds or even thousands of domains for the C&C communications.

- ❖ Dynamic DNS (DDNS) domain

A Dynamic DNS (DDNS) domain is a web domain that provides a legitimate service to business owners to host their applications and websites as a hostname (subdomain) under the DDNS service provider domain. For example, if you requested to host a subdomain called mostafa from the DDNSProvider.com DDNS, then your full domain name will be mostafa.DDNS-Provider.com.

Attackers prefer DDNS services because they are cheap, provide a legitimate SSL encryption certificate, and enable them to evade reputation-based blocking from the security controls, as DDNS service provider domains are categorized as legit and non-malicious domains.

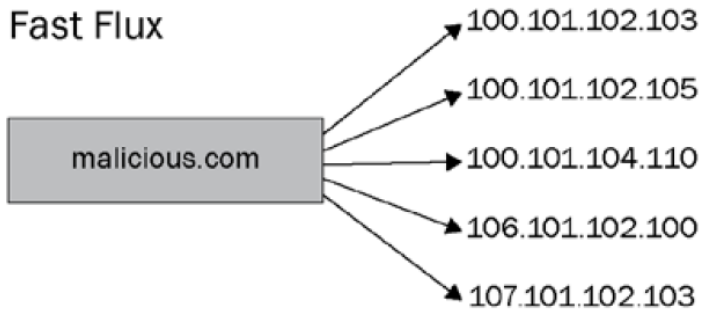
• Investigating the referrer URL

> **Important note**
>
> As we mentioned several times, there are certain situations where the referrer URL does not exist in the web request logs, so you may wonder how to find it. We can solve such a lack of information by analyzing the timeline of the source machine's web requests. By examining the proxy logs, we can review the web URLs accessed within a 5-minute timeframe preceding the investigated web request so we may observe access to search engine URLs, content delivery networks, media hosting websites, and so on. Then, if we suspect a URL to be the referrer URL of the communications and want to go further in our investigation, we can analyze our findings by using an online sandbox such as `ANYRUN`, try to access the suspected URL, and simulate user behaviors such as opening files and clicking links hosted on the website, and see whether we redirected to the same `URL\Domain` we are investigating or not.

• Investigating the communications user agent
• Investigating the communications, destination port
• Investigating the received and sent bytes, HTTP method, and Content-Type
• Investigating command and control techniques

- ❖ **Malware beaconing technique**
- ❖ **Fast flux technique**

  The fast flux technique represents the illegal utilization of the legitimate round-robin DNS technique designed for load distribution and balancing purposes. In the context of fast flux, multiple IP address
  records are mapped to a single malicious web domain on the DNS servers. The DNS records, such as the IP address records of the malicious domain, have very low time-to-live (TTL) values, which



Attackers usually use the fast flux technique for two reasons:

- To hide and protect their servers from being taken down by law enforcement
- To evade being blocked by security defenders by using non-domain-aware devices such as firewalls