ABC's of DNS, DHCP, and IPAM Security

INCLUDES EFFECTIVE DEFENSE TECHNIQUES THAT SECURITY ANALYSTS CAN USE

ManageEngine
Log360

Table of contents

Chapter 1

What is DDI?

Topics covered:

- Domain Name System (DNS)
- Dynamic Host Configuration Protocol (DHCP)
- IP Address Management (IPAM)

The term DDI was first used by Gartner in 2009 when they released the first MarketScope report.[1] While the term DDI may seem unfamiliar, you might recognize it as the integration of DNS, DHCP, and IPAM.

- **Domain Name System (DNS)** is a protocol that resolves names of websites to their corresponding IP addresses.
- **Dynamic Host Configuration Protocol (DHCP)** is a network protocol in which a DHCP server automatically assigns Internet Protocol (IP) addresses and other network configuration parameters to devices on the IP network.
- **IP Address Management (IPAM)** is a system to manage IP address spaces on a network with the help of DNS and DHCP.

DNS, DHCP, and IPAM are components essential for the functioning of the enterprise network. From diagnosing network issues to reduce downtime, to identifying network breaches and preventing cyberattacks, DDI security has become a vital element in any organization's cybersecurity playbook.

In this e-book, we will discuss each of these components in detail.

Chapter 2

Domain Name System (DNS) – The Resolver

Topics covered:

- 2.1 What is DNS?
- 2.2 How does DNS work?
- 2.3 Threats to DNS
    - 2.3.1 Distributed Denial of Service (DDoS)
    - 2.3.2 DNS cache poisoning
    - 2.3.3 DNS tunneling

2.1 What is DNS?

Just as humans identify things, places, and other humans by names, in the realm of networking, computers and other network devices identify one another by their IP addresses. However, it's difficult for us to remember the IP address of each website we browse. This is where the DNS comes to our rescue. It can be imagined as the contact app on your smartphone that lists people's names along with their phone number, email IDs, and other details. The DNS provides a list of all websites with their corresponding IP addresses. Simply put, the DNS is a translator that converts human readable domain names to machine-understandable numeric IP addresses.

2.2 How does DNS work?

You are having a not-so-great day and you know just the website to brighten your day, "www.cutedogs.com". Let's follow the trail of how cute dog videos end up on your computer or mobile device screen. The following are the steps involved in converting a domain name to an IP address:

STEP 1

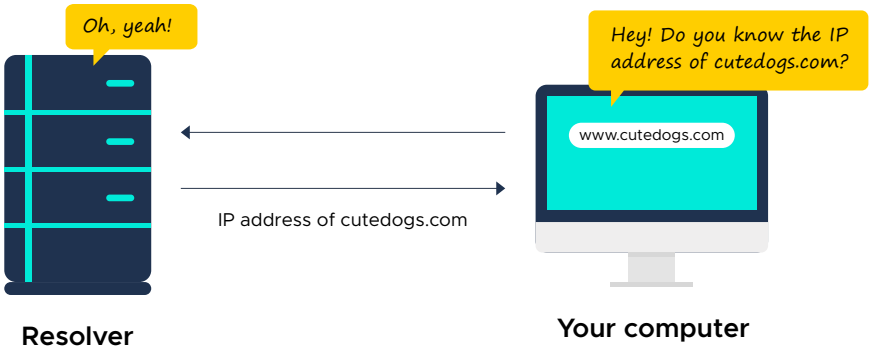
You open your web browser and type "www.cutedogs.com". First, your browser and operating system will search their cache to retrieve the IP address of the website.

If the IP address is found in the cache, the browser directly reaches "cutedogs.com" by referring to it. The IP address will be found in the cache if you have visited this website before, and the details are still stored there. If the IP address isn't found in the cache, Step 2 happens.

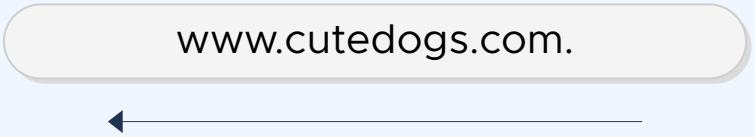
STEP 2

The query "www.cutedogs.com" is sent to the resolver server. The resolver checks its cache memory for the IP address of the received query. If the IP address is found, the value is returned to the client machine, i.e., your computer.

Definition: The **DNS Resolver** also known as **DNS Recursor**, is a server responsible for making additional requests to identify the IP address of the domain name requested by the client. Resolvers are located with the Internet service providers (ISPs) or institutional networks.



Note:
Before we proceed, you need to know that the IP address resolution happens from right to left. The hierarchy of domains descends and becomes more specific while moving from right to left, i.e., the label on the left is a subdivision of the label to the right.

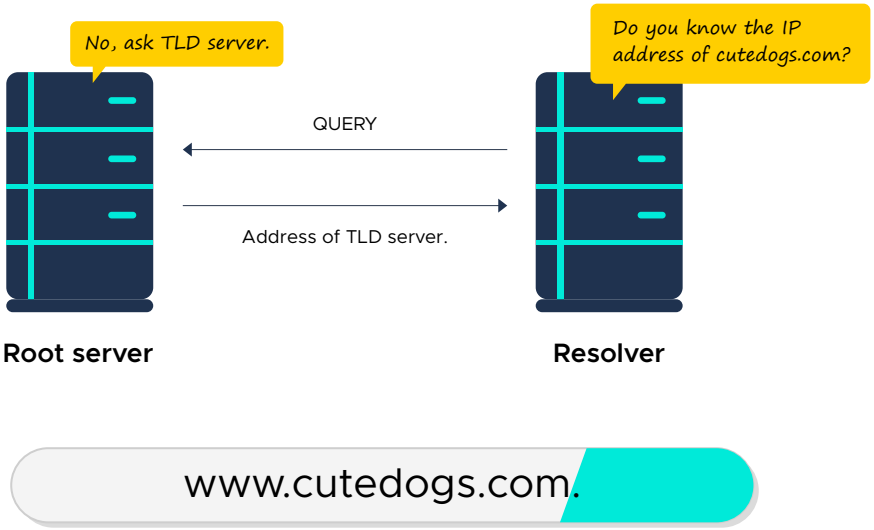


If the IP address is not found in the resolver's cache, the query is forwarded to the root server.

STEP 3

The root server does not contain the IP address of "cutedogs.com", but redirects the resolver to the top-level domain server, or the TLD server, of the .com domain.

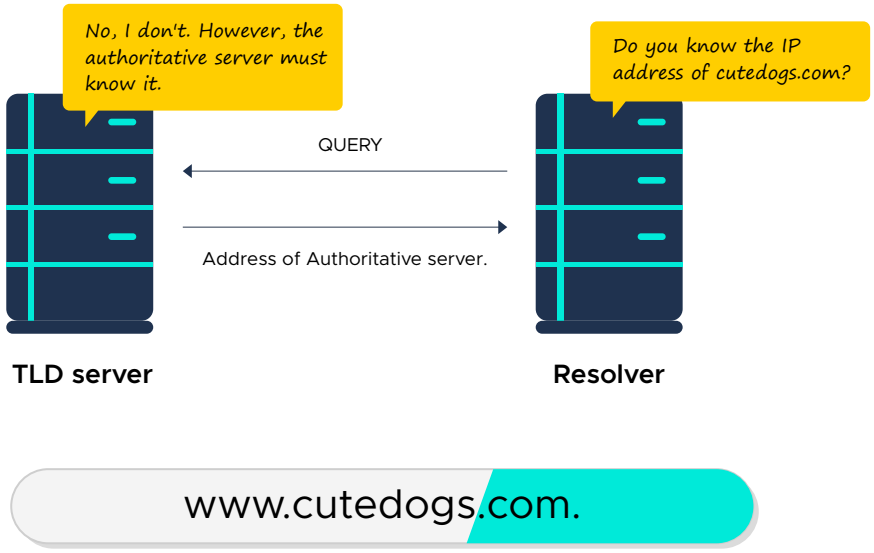
Definition: The **root servers** form the highest level of the DNS hierarchy. There are 13 root servers spread across the globe that are managed by a non-profit organization called the Internet Corporation for Assigned Names and Numbers (ICANN).



STEP 4

The TLD server contains the address information for the top-level domain ".com" of which "cutedogs.com" is a part. The TLD server points the resolver to the authoritative name server of the cutedogs.com domain, which is the final destination.

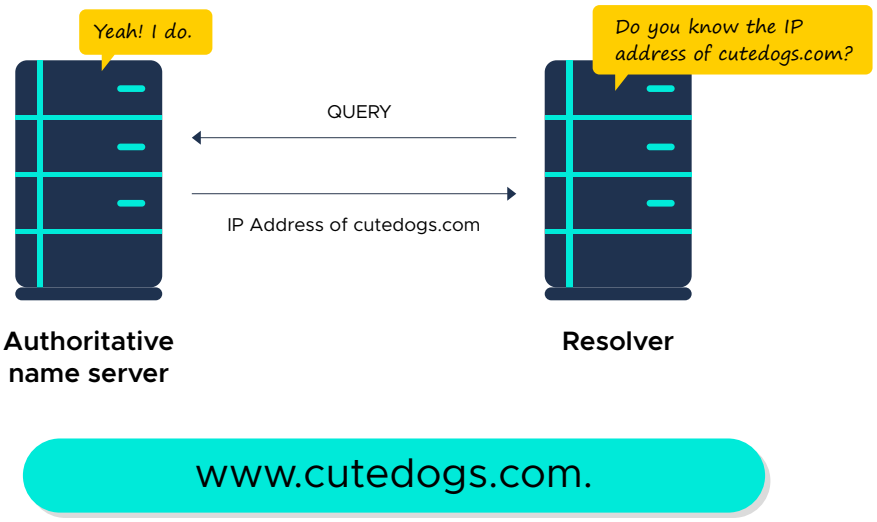
Definition: The **top-level domain (TLD) name server** contains address information for top-level domains such as .com, .net, .gov, etc. The TLD name servers are managed by the Internet Assigned Numbers Authority (IANA), which is a branch of ICANN.



STEP 5

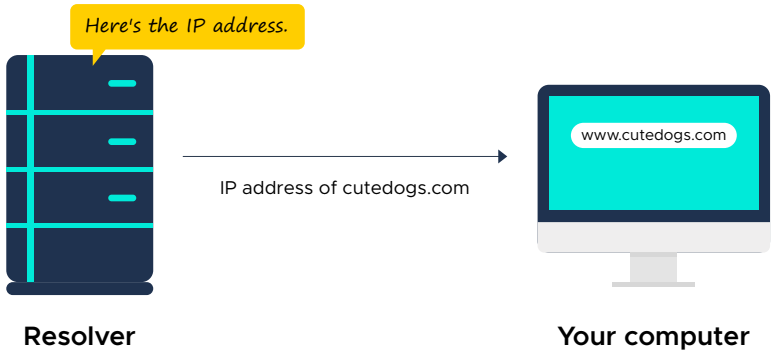
The authoritative name server holds information about a domain. This server provides the resolver with the IP address of "cutedogs.com".

Definition: The **authoritative name server** contains information about any specific domain it serves, and provides the actual answer to the client's query, i.e., the IP address corresponding to the requested domain name.



STEP 6

The resolver returns the IP address of "cutedogs.com" to your computer. Using this information, your browser can now reach "cutedogs.com".



You can now binge-watch cute dog videos and feel happier!

2.3 Threats to DNS

In the previous sections, we have seen how DNS operates in detail. Without DNS, the easy-to-access Internet, as we know it today, wouldn't exist. The DNS is a crucial component of any network that is connected to the Internet for communicating with external networks. The criticality of DNS operations, coupled with the fact that it cannot be completely locked down, makes it a favorite target of cyber attackers.

Statistic: According to the Global DNS Threat Report by IDC, 82 percent of organizations worldwide have faced a DNS attack in 2019.[2]

We will now discuss some of the most prevalent types of DNS attacks.

2.3.1 Distributed Denial of Service (DDoS)

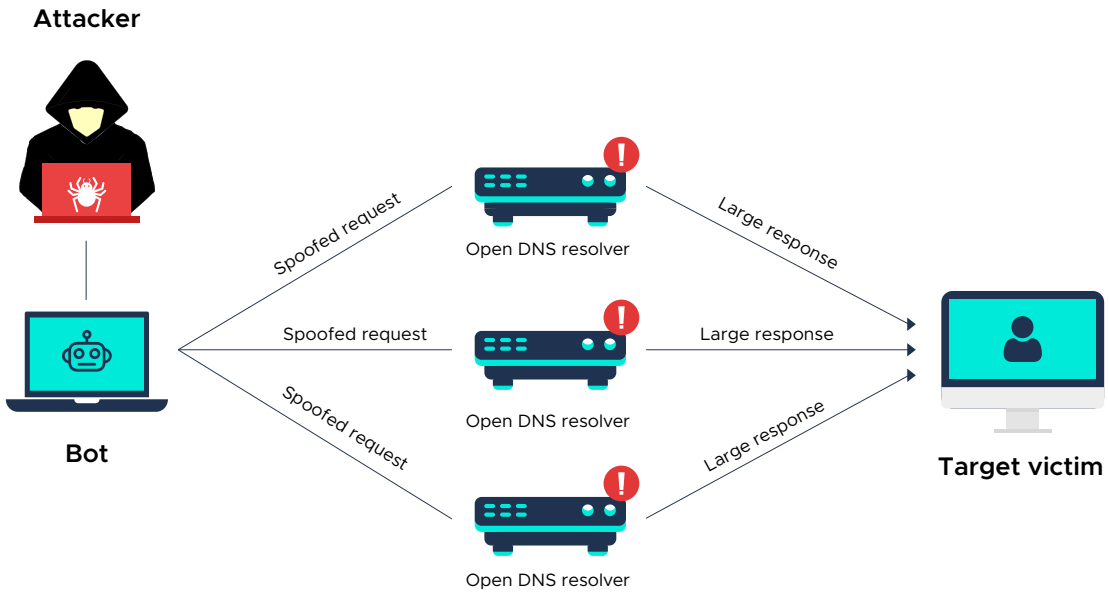
DDoS is a type of cyberattack in which the attacker overwhelms a device or a network with massive traffic, rendering it unusable to intended users. DDoS is not a threat specific to DNS. However, DNS is particularly vulnerable to DDoS attacks, and it can form a logical choke point on a network, since all the devices connected to your network must interact with it to contact the internet.

DNS Amplification attack

The DNS amplification attack is a type of DDoS attack which exploits the way in which DNS functions. Attackers utilize open DNS resolvers and IP spoofing techniques to overwhelm victims with high volume payloads. Open DNS resolvers provide recursive name resolution for any client.

Here's how a DNS amplification attack unfolds:

- Attackers send a DNS request with a spoofed IP address, which points to the target IP, to an open DNS resolver.
- In order to amplify the size of the response from the resolver, the request includes arguments such as "ANY". While a non-malicious DNS query would only request the IP address of a website, a query which includes the "ANY" argument returns information about the entire domain such as subdomains, aliases, mail servers, etc., increasing the size of the payload to as much as 50 times that of the original response.
- Once the resolver receives the request, it sends the amplified payload to the spoofed IP address, overwhelming the target network, resulting in a denial-of-service attack.



2.3.2 DNS cache poisoning

In section 2.2, "How does DNS work?", we saw that the DNS resolver first checks its own cache to find the IP address of the domain that a client has requested. Attackers can manipulate DNS resolvers into caching false information. The act of recording false information into a DNS cache is known as DNS cache poisoning or DNS spoofing. This causes the resolver to return incorrect IP addresses to clients and, in turn, direct them to malicious websites

These are the steps involved in DNS cache poisoning attack:

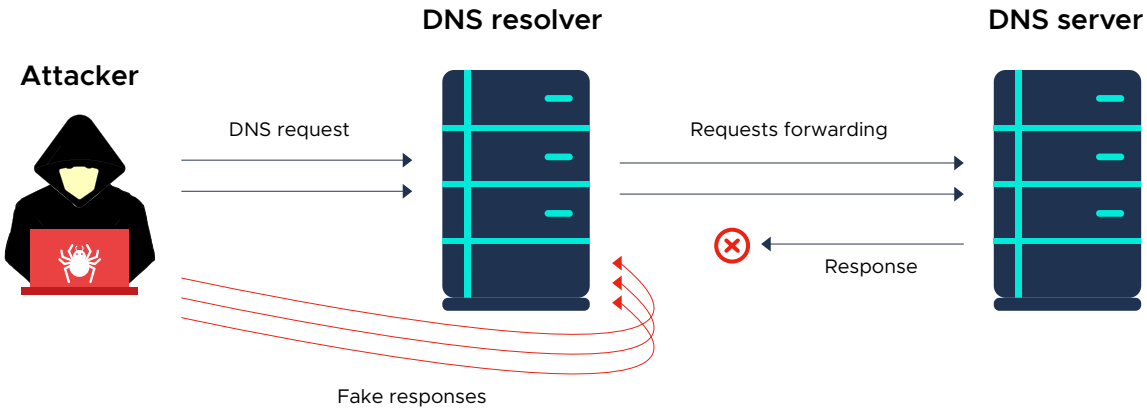
- Attackers send a DNS query to a DNS resolver, which forwards the request to a root server, then to TLD and authoritative name servers.

- The attacker impersonates the authoritative name server, and bombards the resolver with forged responses that don't point to the original website. Since DNS uses the User Datagram Protocol (UDP), there is no mechanism to verify the sender's identity. The resolver, unaware of the poisoned response, stores the value in its cache.

Definition: The **User Datagram Protocol (UDP)** is a communication protocol that is used in loss-tolerating connections. It has low-latency and enables faster data transfer by eliminating the process of establishing and verifying connections between the sender and the receiver.

- Now, when a legitimate user queries this DNS resolver, a forged response which directs the user to a malicious website is returned from the cache.

- Since the DNS resolver typically has no ability to verify the authenticity of the data in its cache, the poisoned value remains until time to live (TTL) expires, or the entry is manually removed.



Note:
For the DNS cache poisoning attack to be successful, the attacker must know or guess several factors:

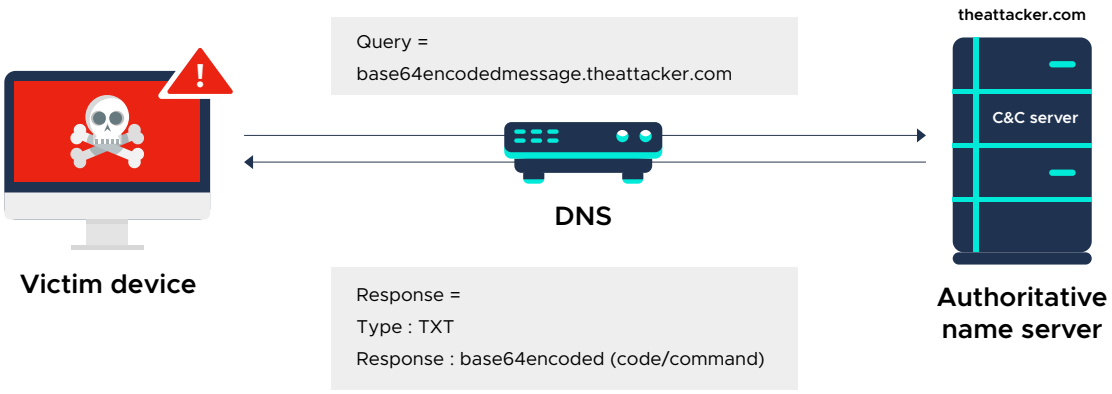
- The DNS queries that are not stored in the resolver's cache, so that it's forwarded to the authoritative name server.
- The authoritative name server the query will be redirected to.
- The port number used by the DNS resolver and request ID number, so that the forged response can be sent to the targeted DNS resolver and its cache poisoned.

2.3.3 DNS tunneling

Similar to DNS cache poisoning, DNS tunneling also abuses the DNS protocol to carry out malicious activity. DNS tunneling is the process of hiding data in DNS queries and responses. DNS tunneling is used by attackers to establish a command and control connection with an already compromised device in a network to execute commands or exfiltrate data.

The following are the steps involved in a DNS tunneling attack:

- Attackers register a domain (e.g., theattacker.com), and set up a command and control (C&C) server that acts as the authoritative name server for "theattacker.com".
- Malware on a compromised device sends an encoded message (base64encodedmessage.theattacker.com) in the form of a DNS query to "theattacker.com", which is directed by the DNS resolver to the C&C server of "theattacker.com".
- The C&C server returns a TXT record to the victim device. The TXT record may contain commands, or codes to be executed by the malicious payload. The established DNS tunnel helps in exchanging information undetected through the perimeter.



Chapter 3

Dynamic Host Configuration Protocol – The Assigner

Topics covered:

- 3.1 What is DHCP?
- 3.2 How does DHCP work?
- 3.3 Threats to DHCP
  - 3.3.1 DHCP starvation
  - 3.3.2 DHCP spoofing

3.1 What is DHCP?

We know that for any computer or device to be identified on a network, it requires an IP address. IP addresses can be assigned to devices in two ways — static and dynamic. In static IP address allocation, the user must manually enter a unique IP address and other network properties for each device.

However, this is not practical in networks that contain numerous devices. This is where DHCP comes into play. DHCP is a network management protocol that automatically allots IP addresses to network devices along with a subnet mask, default gateway, and preferred DNS server.

Definition: The **DHCP server** is a network server that uses the DHCP protocol to automate the allocation of IP addresses, and other network parameters to DHCP clients.

The **DHCP client** is any device connected to a network which uses the DHCP protocol to obtain network parameters from a DHCP server.

Simply put, when a device is added to a network, it sends a request for an IP address. The DHCP server then responds with an IP address, and once the new device accepts the offer, the DHCP server confirms and assigns it to the device. Let's now have a detailed look at the working of DHCP.

Note:
Care must be taken to ensure that each device on a network is allotted a unique local IP address in order to avoid IP conflict. This is similar to why no two houses should have the same physical street address.

Note:
For the dynamic allocation of IP addresses, there are two basic requirements:

- The devices on the network must run a DHCP client.
- At least one DHCP server must be present on the network. Generally, routers have a built-in DHCP server.

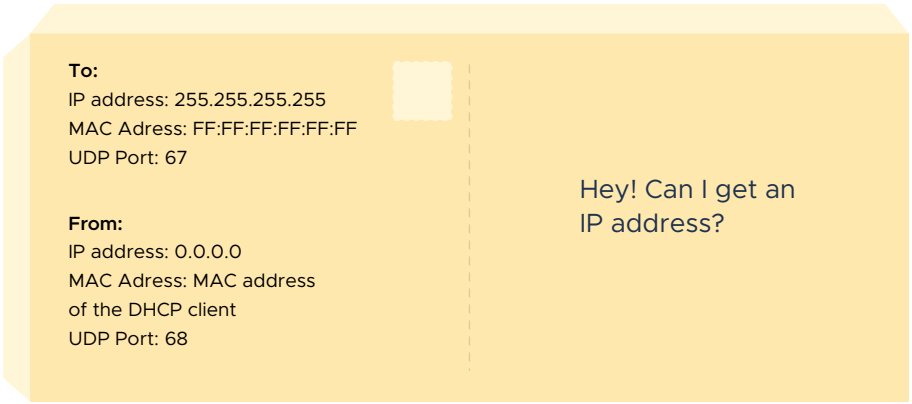
3.2 How does DHCP work?

DHCP follows a four-step process called DORA (Discovery-Offer-Request-Acknowledgment).

STEP 1

DHCP discovery

The DHCP client broadcasts a DHCP discover message to all the devices on the network, since it doesn't know the location of the DHCP server.



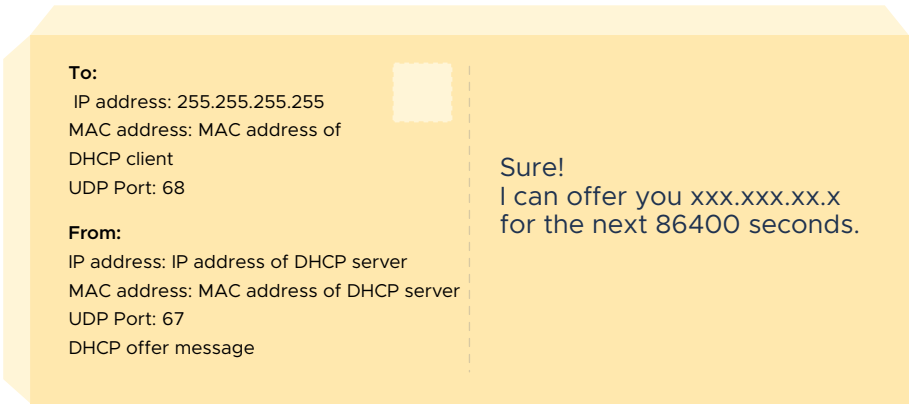
DHCP discovery message

- The receiver's IP address is 255.255.255.255 since it is a broadcast message.
- The receiver's MAC address is FF:FF:FF:FF:FF:FF since the DHCP server's MAC address is unknown yet.
- The sender's IP is 0.0.0.0 since it has not been assigned an IP address yet.
- The UDP port 67 is reserved for DHCP servers, and port 68 is reserved for DHCP clients.

STEP 2

DHCP offer

The DHCP server receives the discover message and responds with an offer.



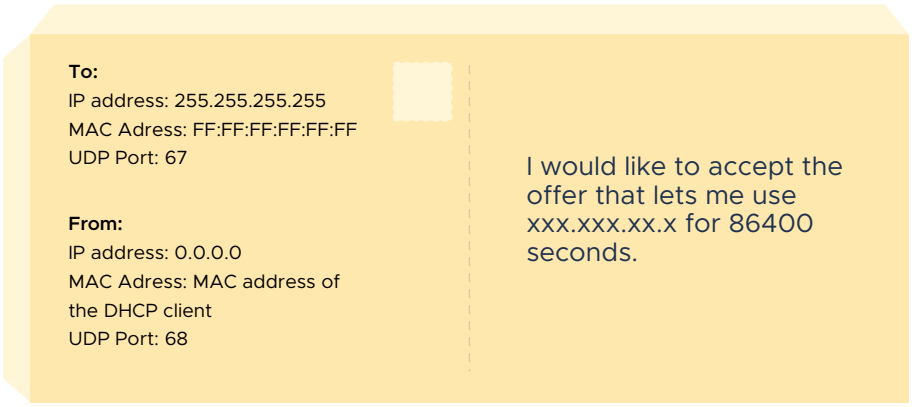
DHCP offer message

- The receiver's IP address is 255.255.255.255 since the client doesn't have an IP address yet.

STEP 3

DHCP request

By now, the DHCP client would have received offers from at least one DHCP server. The client sends out a DHCP request message in which it specifies the preferred IP address.



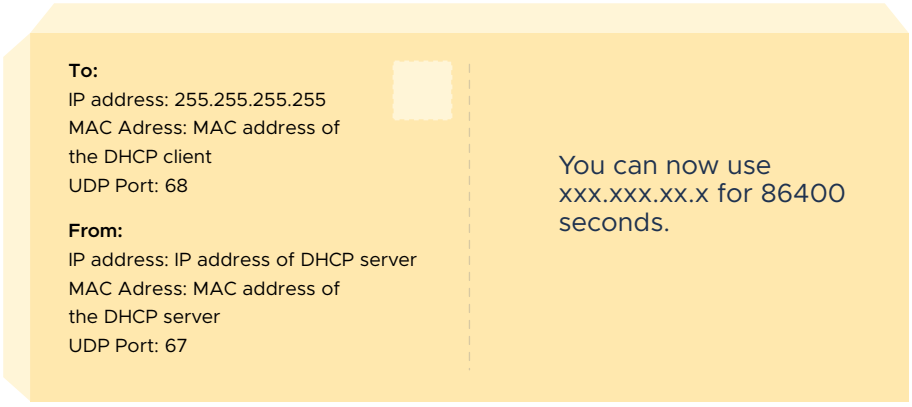
DHCP request message

- The receiver's IP address is still 255.255.255.255 since it would have received offers from more than one DHCP server on the network. The message is broadcast to inform other DHCP servers to release the offered IP address to their available pools again.

STEP 4

DHCP acknowledgement

Through the DHCP acknowledgement message, also referred to as "ACK", the DHCP server confirms to the client that it can start using the IP address for the specified period of time, and that the address has been reserved.



DHCP acknowledgement message

Once this four-step process is complete, the client can start using the new IP address.

3.3 Threats to DHCP

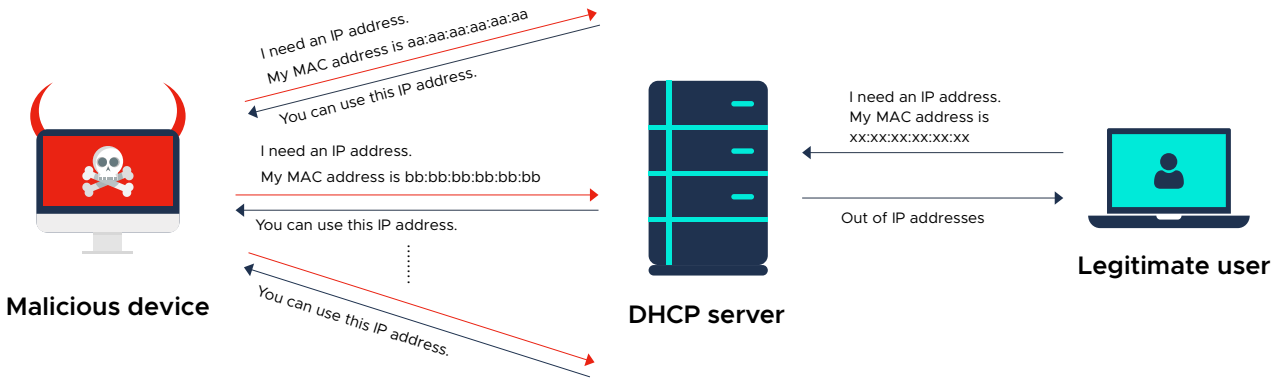
DHCP is one of the most used protocols for host configuration. A DHCP client is also known as a host. Similar to DNS, DHCP also uses UDP as its transport protocol. The fact that DHCP doesn't employ any authentication mechanism to verify the integrity of messages exchanged between clients and servers, makes it easier to exploit.

3.3.1 DHCP starvation

DHCP servers have a pool of IP addresses which they lease to hosts for a specified period of time. A DHCP starvation attack can be thought of as a denial-of-service (DoS) attack on DHCP. In this attack, the attacker floods the DHCP server with a large number of requests. Since the server has no mechanism to distinguish legitimate requests from malicious ones, it could hand out IP addresses to rogue hosts, exhausting the IP address pool, and thus denying service for legitimate network users.

Here are the steps involved in DHCP starvation attack:

- A malicious client gains unauthorized access to a network, and sends numerous DHCP discover messages using spoofed MAC addresses.
- The server, in turn, sends out DHCP offers, to which the malicious client responds with DHCP request messages.
- The server then confirms the request and provides acknowledgement, reserving IP addresses for the bogus clients. The IP addresses in the server's address pool are quickly used up, and legitimate network clients are unable to access the server.

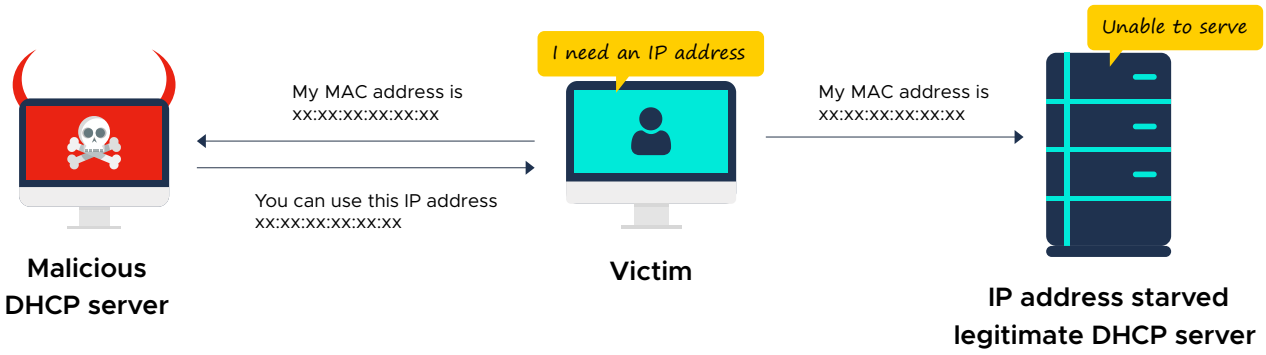


3.3.2 DHCP spoofing

A DHCP spoofing attack is a type of a man-in-the-middle attack. A DHCP spoofing attack generally follows a starvation attack. Here, the attacker is disguised as a DHCP server, and responds to clients with fake IP addresses and erroneous network configurations, such as DNS server, and default gateway. The attacker can now manipulate data packets, and intercept information from users before forwarding it to the real gateway, or direct the clients to fake DNS servers, and launch phishing attacks.

The following are the steps involved in a DHCP spoofing attack:

- A client broadcasts a DHCP discover message.
- The DHCP server is out of IP addresses due to a DNS starvation attack, and is unable to process the client's request.
- A malicious device posing as DHCP server returns a offer message to the client.
- The client accepts the offer, and an IP address and other network configuration parameters are assigned by the fake DHCP server. The client now becomes a victim as the malicious server intercepts all information from the victim including passwords and other sensitive data.



Chapter 4

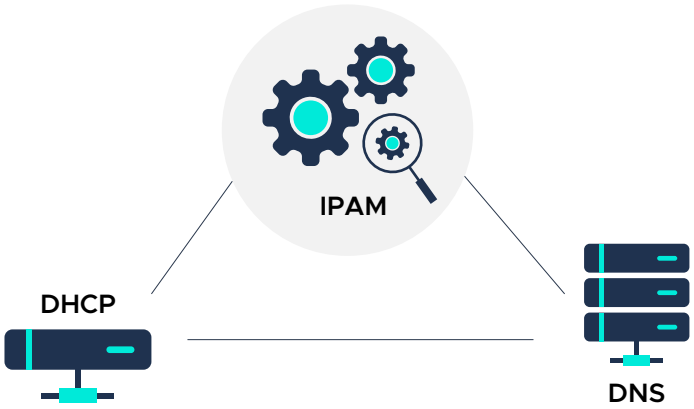
IP Address Management (IPAM) – The Administrator

Topics covered:

- 4.1 What is IPAM?
- 4.2 Is IPAM essential?

4.1 What is IPAM?

IP Address Management (IPAM) is a methodology for planning, deploying, monitoring and managing the network IP addresses. IPAM involves managing services like DHCP and DNS, which are involved in the assigment and resolution of IP addresses, to ensure that the inventory of assignable IP addresses remains updated and precise.



IPAM can be considered as a repository of all information related to the IP addresses belonging to a network, such as:

- IP addresses available for allocation.
- Status of each IP address.
- Host name associated with each IP address.
- Hardware specifications associated with each IP address.
- Details about the subnets in use.

4.2 Is IPAM essential?

There is a popular myth that, unlike DNS and DHCP, which are mandatory components for any device connected to network to communicate, an IPAM solution isn't really indispensable; good old spreadsheets can do the job.

Using spreadsheets to manage IP address spaces is just a makeshift solution and not an efficient method. Let's explore why.

- **Explosion of IP address enabled devices -** In today's world, organizations' network landscapes have become more complex and dynamic due to the increasing use of Internet of Things (IoT) devices and bring your own device (BYOD) policies. The number of IP-enabled devices connected to a network has increased manifold. In such a scenario, it is unrealistic to use spreadsheets and documents to keep track of information, such as IP addresses, subnets, virtual local area networks (VLANs), and connected devices.

- **Conflicts in IP address assignment -** Managing IP addresses manually requires IT administrators to update the spreadsheet every time a new IP is allocated, a device is deprovisioned, or a change in IP address status is noticed. In networks managed by multiple IT admins, errors in synchronization and data inconsistencies may arise. The same IP address may be allocated to different devices, creating multiple use of the address. This will make all the devices unavailable.

- **Network outage -** When spreadsheets aren't updated properly, troubleshooting becomes very complicated, since a number of factors like IP address conflicts, security breaches, and port mismatches need to be considered. This process can be time-consuming and can lead to temporary network outages.

Statistic: According to a study conducted by Ponemon Institute in 2016, the average cost of network downtime is around **$9,000** per minute.[3]

- **Compliance and security standpoint -** Plainly storing all information in a simple spreadsheet is cumbersome, and IT administrators often find it provides few, if any, actionable insights. Furthermore, a spreadsheet does not help defend against a security breach. Instead, it is vulnerable to manipulation and sabotage. Additionally, certain compliance regulations mandate detailed IP assignment logs and reports; this becomes tedious to process manually.

Formulating and deploying an appropriate IPAM strategy isn't mandatory, but it is essential to improve efficiency, security, and visibility of your network.

Chapter 5

Defending DDI

Topics covered:

- 5.1 Measures to protect an organization's DNS, DHCP and IPAM infrastructures
- 5.2 How can Log360 help?

5.1 Measures to protect an organization's DNS, DHCP and IPAM infrastructures

In the previous chapters, we explored in detail what DDI is, and why you should care about it. Now it's time to discuss some of the best practices to keep DDI attacks at bay, and keep your network up and running.

- Update the DNS account passwords periodically. This can prevent unauthorized users from accessing the accounts with rogue or old passwords that they still retain.
- Enable multi-factor authentication for all registry accounts and DNS hosting accounts.
- Ensure that the password and username of network devices, such as routers, are modified from the factory settings.
- Passwords must not be shared with others, stored, or transmitted as clear text, and reused across services.
- Randomization is the key to preventing cache poisoning. Use a random source port, query ID, and upper or lower case letters in domain names.
- Ensure that DNS zone records are Domain Name System Security Extension (DNSSEC) signed, and your DNS resolvers are performing DNSSEC validation.
- Set up DNS servers to only run services that are required. Run resolver and the authoritative name server on separate servers, to limit the attack vector size.
- Implement DHCP snooping to prevent DHCP denial-of-service attack and spoofing attacks. DHCP snooping is a layer 2 security feature which enables switches to drop unauthorized DHCP traffic.
- Enable logging wherever possible so that any activity can be audited.
- Regularly audit the collected logs to identify signs of attack, and take remedial action.
- Employ real-time analytics and behavioral threat detection to help prevent attacks in the early stage before much damage is done.

If reading through this non-exhaustive list of DDI best practices made you exhausted, fret not! Read on to learn how ManageEngine Log360 can do most of the heavy lifting for you.

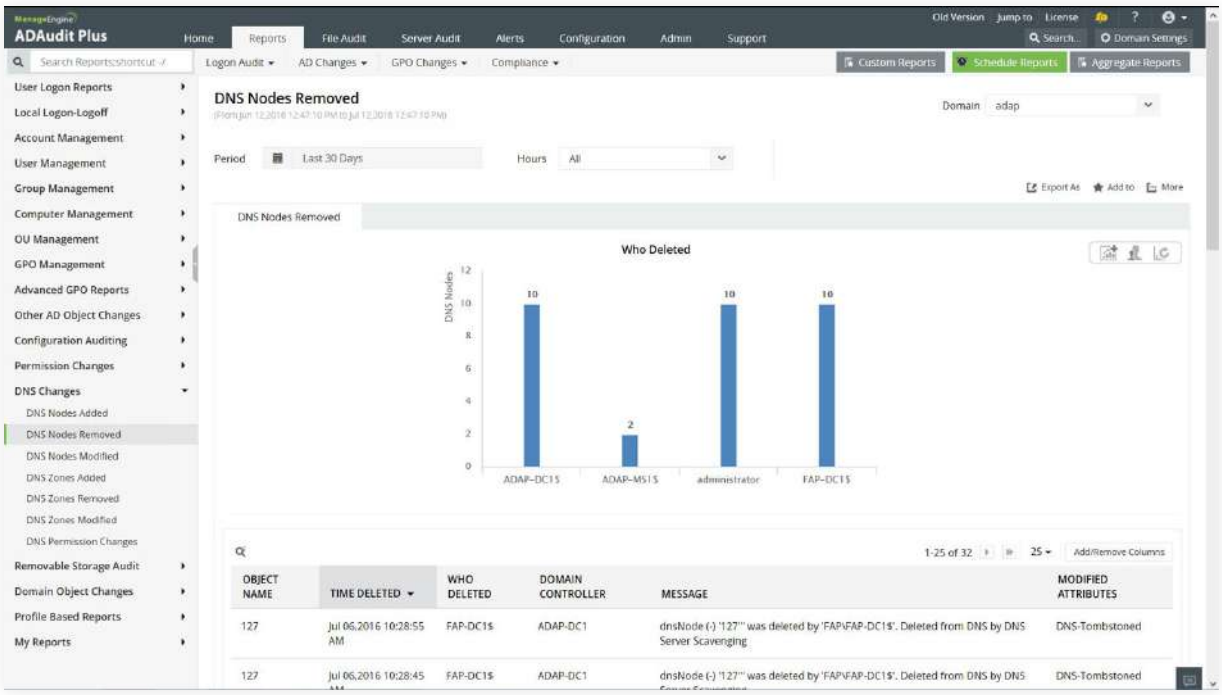
5.2 How can Log360 help?

Log360 is a comprehensive security information and event management (SIEM) solution which helps you combat security threats and attacks, including those described in this e-book. With its in-depth log analysis, Active Directory auditing, machine-learning driven behavioral analytics, real-time correlation, forensic analysis, and incident management capabilities, Log360 can help you detect attacks in real time, and help you block and contain cyberattacks.

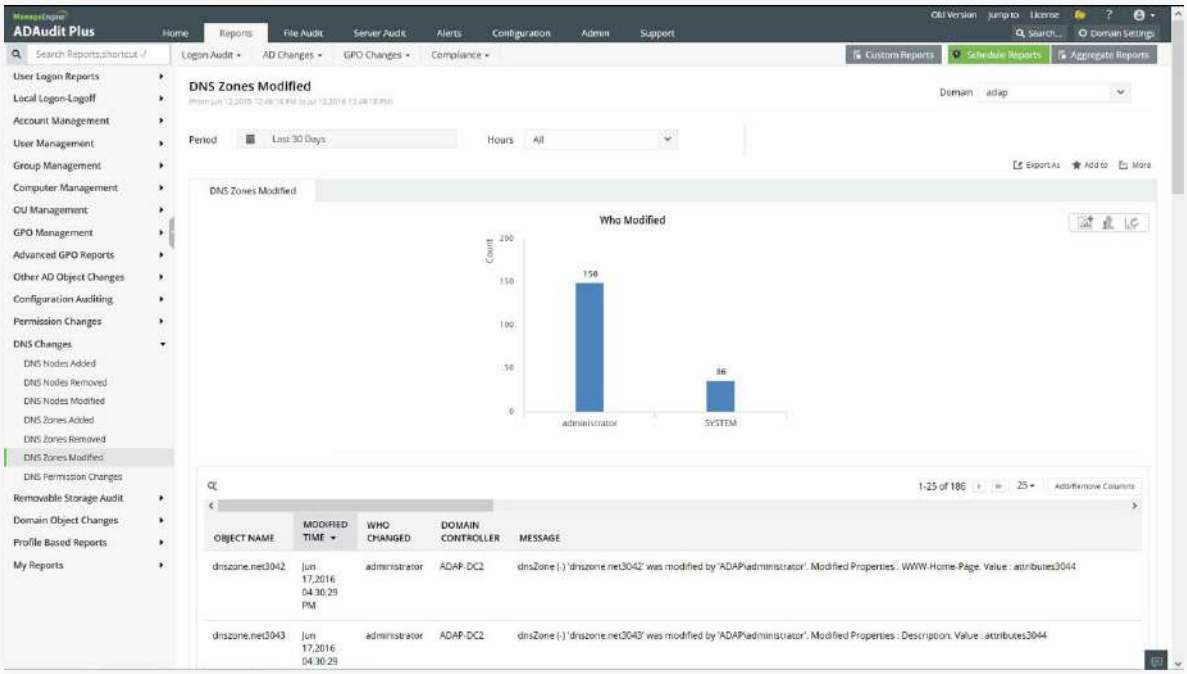
Let's have a look at some of the features of Log360 that can help you identify and thwart DDI attacks.

DNS auditing

Log360 enables real-time DNS auditing, and provides a clear view into the changes made to DNS. It also generates detailed security reports on DNS nodes and DNS zones that have been modified or removed, and DNS zones added along with the crucial DNS permission changes.



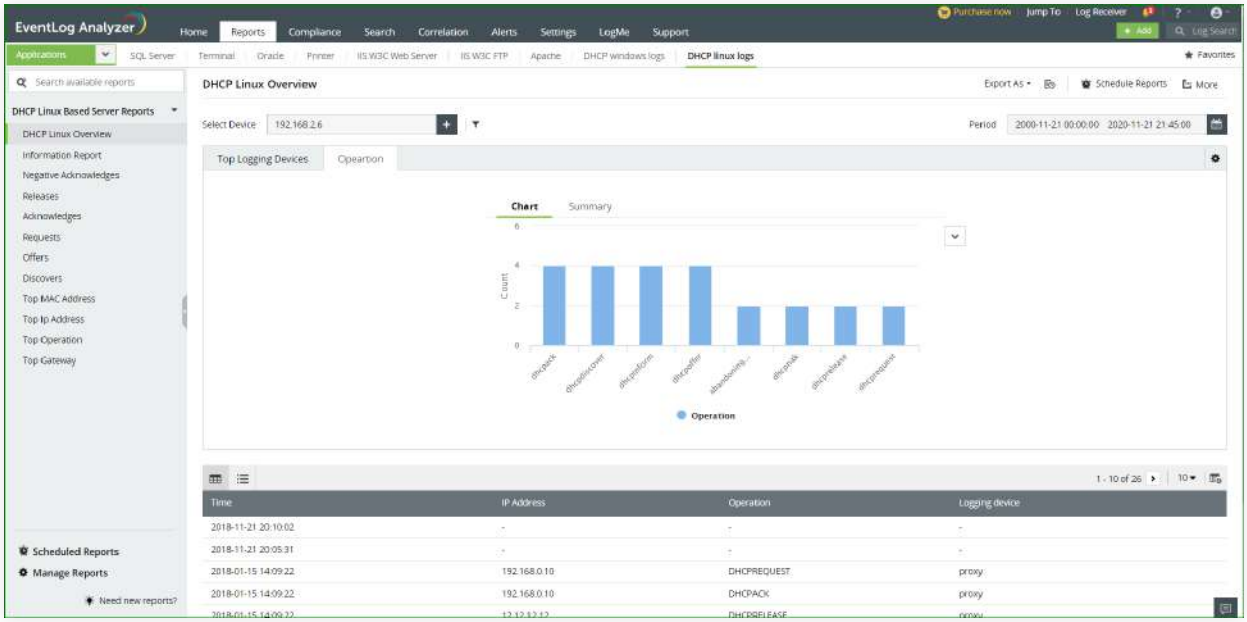
Log360 report indicating DNS nodes removal.



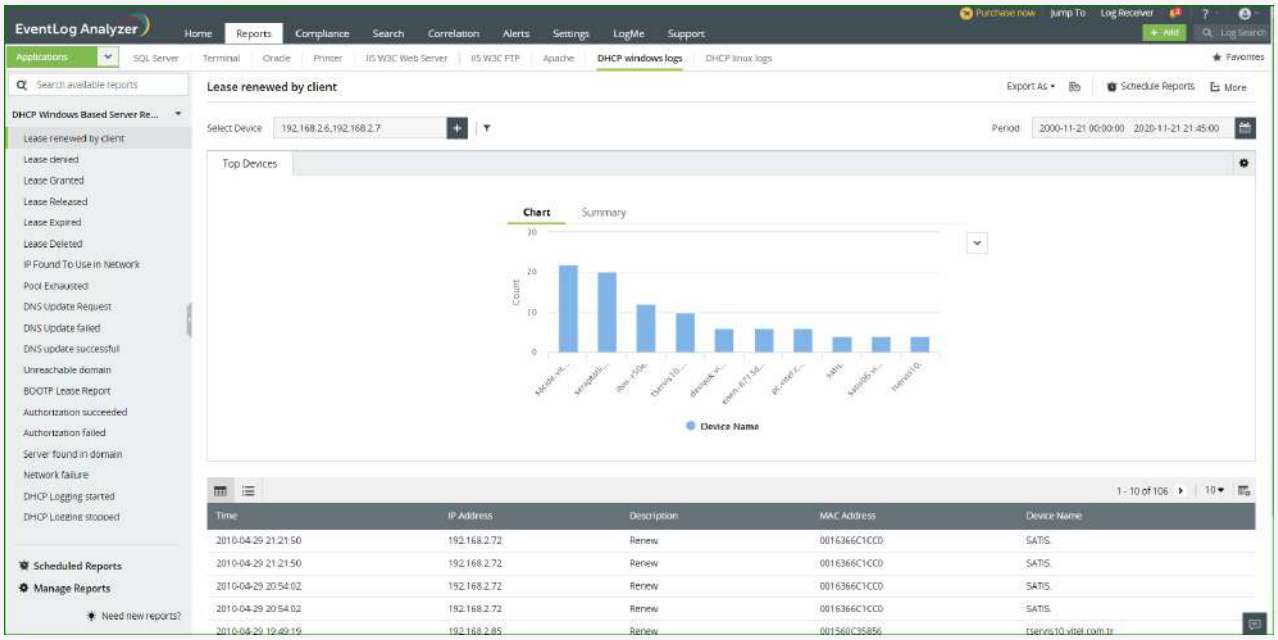
Log360 report indicating DNS zone modifications along with information about who made the change and when.

DHCP auditing

By analyzing DHCP server logs, Log360 is able to provide information about requests for IP addresses and corresponding acknowledgements, successful and failed lease grants, and depletion of the DHCP server's IP address pool.



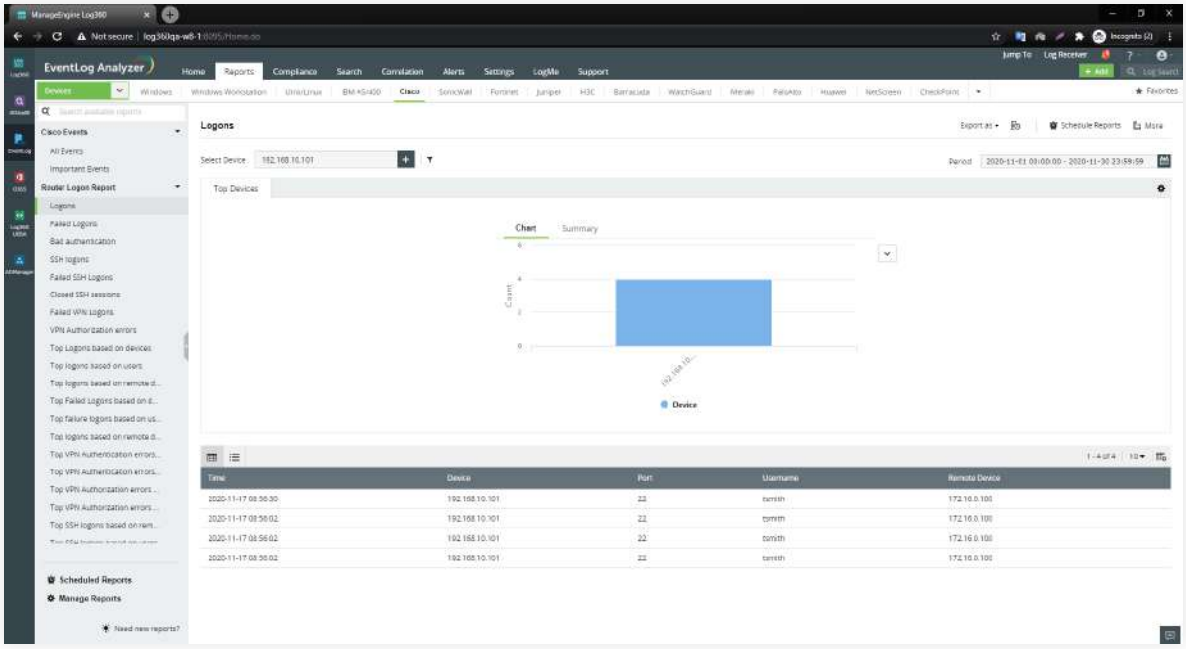
DHCP Linux Overview report summarizing all DHCP log events.



Report listing all IP address leases renewed by clients.

Router auditing

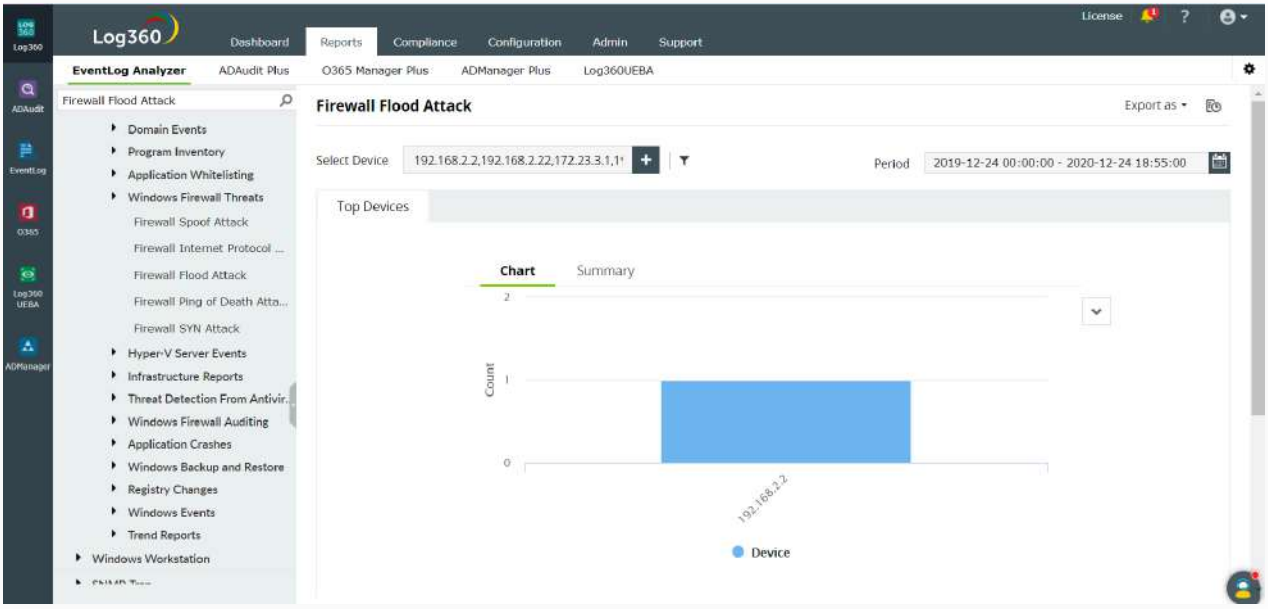
With the massive amounts of traffic that pass through the routers regularly, monitoring router activity can be challenging. But auditing routers and other network devices is a breeze with Log360. It scans your network and discovers routers and other syslog devices that can be added for monitoring. With Log360's real-time alerts you can detect suspicious activity instantly, and the predefined router log reports give you insights into network activity.



Report depicting router logons.

Firewall monitoring

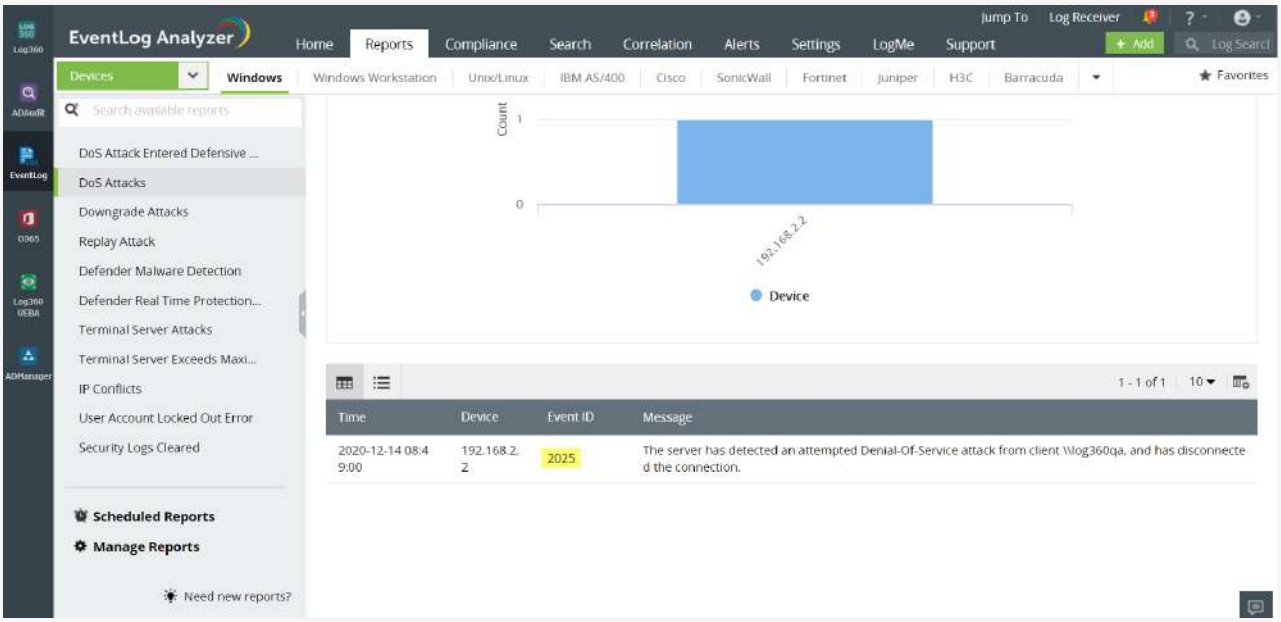
Firewalls act as a regulator of your network traffic, ensuring that only trusted parties are accessing the resources, and protecting your hosts from network attacks. Keeping track of changes made to firewall rules, configurations, and settings can help you ensure that it is set up properly to combat flood attacks, SYN attacks, spoof attacks, half-scan attacks, and Ping of Death attacks.



Report indicating flood attack on a firewall.

Detecting DoS attacks

Log360 audits log data from your network security devices, like firewalls, intrusion detection systems (IDS) and intrusion prevention systems (IPS). The solution instantly detects DoS attacks and alerts you in real time. Log360 also helps you track web server activity to detect when a specific IP keeps sending repeated connection requests, a tell-tale sign of a DoS attack.

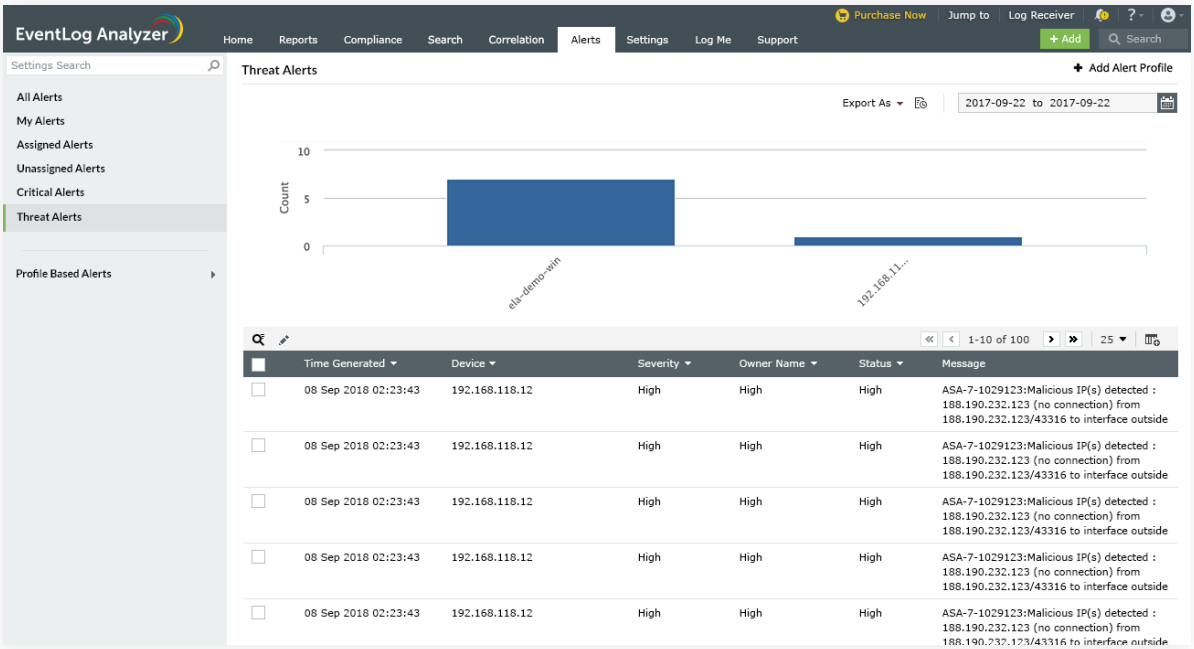


Log360 detecting a DoS attempt and preventing the onset of an attack.

Advanced threat analytics

Log360's threat intelligence module helps detect any communications with various known external malicious sources, and comes bundled with the Global Threat Intelligence Database that hosts over 600 million malicious IP addresses. This database is updated dynamically on a regular basis, and Log360 instantly correlates this data with the incoming and outgoing traffic details to spot malicious traffic in your network in real time. The solution also supports threat feeds in the STIX, TAXII, and OTX formats.

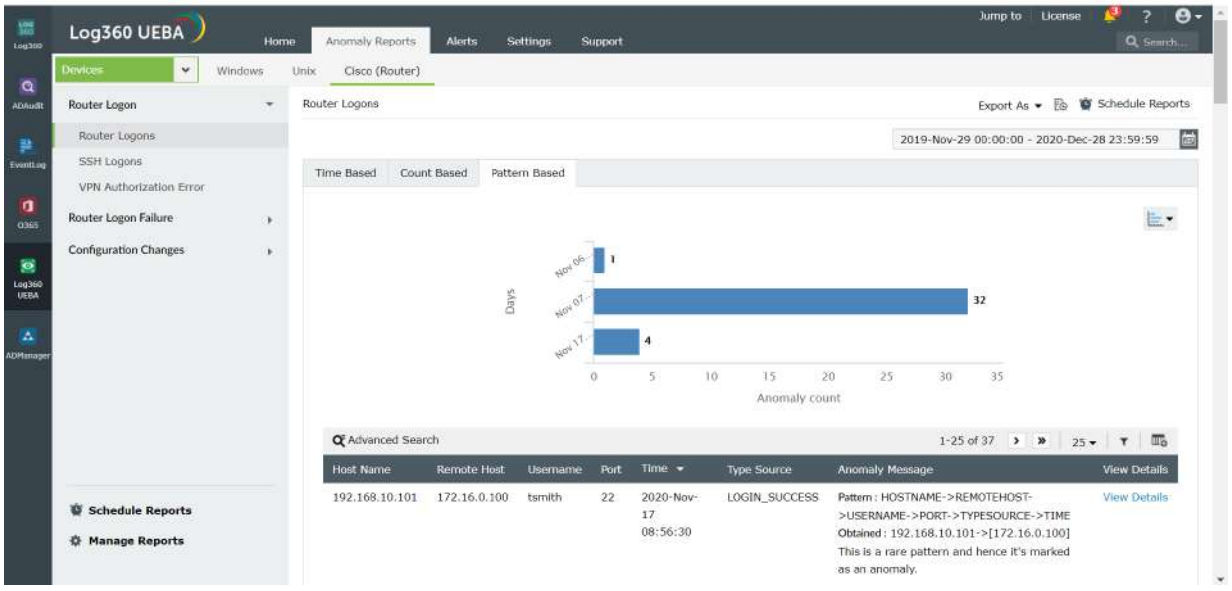
Log360 can easily be equipped with the Advanced Threat Analytics add-on that provides deeper insights into threat actors, such as geo-location of the malicious actor, threat category, reputation score of the malicious source, and more.



Log360 showing traffic from malicious IP addresses.

User and entity behavior analytics (UEBA)

Log360 uses machine learning to identify the behavior patterns of users and entities in a network, enabling it to create a baseline behavior. Every activity performed by the users and entities is then compared to the baseline to spot anomalies that could indicate a potential problem.



Report displaying suspicious router logons.

In addition to the numerous reports discussed above, Log360 provides more than 400 out-of-the-box reports that help you track all the activities of users and entities across your organization, and conduct forensic analysis in a jiffy when the need arises. From helping you meet stringent regulations of compliance mandates, like HIPAA, GDPR, etc., to enabling you to create customized need-based alerts, Log360 is your one-stop solution.

References

1 Rick Rumbarger. "Network complexity: Three trends that are contributing to a 'perfect storm' ". https://www.circleid.com/posts/20100923_network_complexity_three_trends_contributing_to_a_perfect_storm/

2 Virendra Soni. "Average cost per DNS attack is now whopping $1.07 million: Report". https://www.dailyhostnews.com/average-cost-per-dns-attack-is-1-07-million

3 Ponemon Institute LLC. "Cost of Data Centre Outages". http://files.server-rack-online.com/2016-Cost-of-Data-Center-Outages.pdf