**My Summer Internship Experience at Zscaler**

## **201950-First Summer 2019-ITIS-6198-001-IT Project**

**Graduate Advisor**: Heather Lipford

**Preceptors:** Sachin Kumar, Praveen Thalla, Niranjan Ramakrishnan

**Table of contents**

1. Executive Summary…………………...2

2. Introduction………….……………...…3

3. Methods………………………………..5

4. Results…………………………..….....13

5. Discussion and Conclusions…………..14

**Executive Summary:**

This report summarizes my overall experience and responsibilities as a summer intern.

When I got an internship offer from Zscaler Inc, San Jose, CA, I finally realized my dream of pursuing an internship at a reputable organization with modern Information Technology practices. Zscaler Inc, gave me an internship starting 13th of May 2019, to the 16th of August 2019, a period approximately three months.

During the twelve weeks training, I was attached expected to work on both, the automation of security cases using python and also resolve the customer related bugs and cases.

This training not only helped me gain practical and analytical knowledge and skills, but also to gather a valuable understanding of how the courses that I have learnt so far in my Master’s program can transform into real carriers at the work place.

During this internship, I did not just acquire extensive theoretical knowledge on several important security concepts such as Access Control, Advanced Threat Protection and Data Protection but I also got the opportunity to implement these concepts and contribute my sincere efforts to resolve some crucial customer reported bugs and cases. By this time, I have automated 36 customer cases using Python and have configured several security policies to prevent sensitive data leakage, created my own Regex signatures to detect and block malicious sites, monitored authentication and provisioning of users of a company, have understood and implemented traffic forwarding using both GRE and IPSec Tunnels and much more. This internship experience helped me relate the concepts that I have learned during my Master’s degree at UNCC, and apply them in real life to resolve customer security issues.

**Introduction:**

* **About Zscaler:**

Zscaler is a pioneer and leader in cloud security, enabling the world’s leading organizations to securely transform their networks and applications for the cloud and mobile-first world. Zscaler process over 60 billion transactions a day in its cloud and protects customers from over 125 million security threats every day. It’s global cloud security architecture, delivers the entire gateway security stack as a service; By providing fast, secure connections between users and applications, regardless of device, location, or network.

* **About Zscaler’s Cloud Architecture:**

Zscaler operates the world's largest security-as-a-service (SaaS) cloud platform to provide the industry's only 100% cloud-delivered web and mobile security solution. The highly scalable, global, multi-cloud infrastructure features three key components: the Zscaler Central Authority, Zscaler Enforcement Nodes, and Nanolog clusters. Below I am providing a brief overview of these three key components:

# 🡪Zscaler Central Authority:

The Zscaler Internet Access Central Authority (ZIA-CA) is the brain of a Zscaler cloud. Meaning, the CA is the main entity that monitors the cloud and provides a central location for software and database updates, threat intelligence, policy and configuration settings. The CA consists of an active server and two servers in passive standby mode. The active CA replicates data in real time to the two standby Cas. Hence, any of the passive CAs can become active at any time when the primary CA goes down. Each server is hosted in a separate location to ensure fault tolerance.

# 🡪Zscaler Enforcement Nodes (ZENs):

ZIA Zscaler Enforcement Nodes (ZENs) are the internet security gateways that inspect all internet traffic bi-directionally for malware, and enforce security and compliance policies. An organization can forward its traffic to any ZEN in the world or use the advanced geo-IP resolution capability of Zscaler to direct its users' traffic to the nearest ZEN. When the user moves to a different location, the policy follows the user, with the ZEN downloading the appropriate policy.  Customer traffic is not passed to any other component within the Zscaler infrastructure.

# 🡪Nanolog Clusters

Nanolog clusters store transaction logs and provide reports. Each cluster consists of one active server and two servers in passive standby mode. The active Nanolog immediately replicates data to the other two servers, so any of them can become active at any time, with no data loss. Each Nanolog server is hosted in a separate location to ensure fault tolerance. Every second, a Nanolog cluster receives logs from all over the world, correlates them to a specific customer organization, and writes them to disk for high-speed retrieval of reporting and analytics. A Nanolog cluster processes up to 12+ billion logs per day.

Additionally, each cloud has various support systems and servers, including:

* Sandbox servers, where files selected for behavioral analysis are sent for analysis and reports are stored.
* PAC file servers, which host Zscaler PAC files and custom PAC files uploaded to Zscaler. Configuring browsers to use PAC files is one of the traffic forwarding methods that Zscaler supports.
* Administrative interface servers, which provide an intuitive, multi-tenant interface for policy management and reporting.
* Log Routers, which ensure logs for each organization are stored in the appropriate Nanolog cluster.

All components communicate with each other over an encrypted SSL tunnel.

Finally, Zscaler Feed Central is a separate Zscaler cloud that is used solely for the centralized distribution of various feeds to the Zscaler clouds. Zscaler has a number of partnerships with Microsoft, Google, RSA, Verisign, and others for getting data feeds, including feeds for URL filtering, anti-virus definitions, and IP reputation. Zscaler Feed Central distributes its threat intelligence and other feeds to the CA, which then sends updates to the ZENs, ensuring that every ZEN has the latest version of the URL database and the latest malware and threat information.

* **Methods:**

My first day in the Zscaler HQ office was on May 13th, 2019. I was greeted by the HR **Miss. Kimberly Howel**, who showed my around and then took me for my Orientation. She explained me the history and tradition of Zscaler Inc. She then introduced me to rest of my team which consists of five members: The Team Manager, two Principal Software Engineers and three Cloud Reliability Engineers. I was the only summer intern for the Datapath and Security Team this summer which brought me great excitement to prove my caliber to my team.

Initial two weeks of my internship were spent understanding the Zscaler cloud architecture and the kind of work the QA-Datapath and Security team does. I learned that the team is informally called the “SME” team which is nothing but the team which takes care of everything that happens with the ZENs. The responsibilities included:

* Automating the system and solution test cases using Python, Java, Selenium.
* Interop testing with different vendors, IPsec and GRE http, https solutions.
* Contribute to engineering efforts to solve complex engineering problems in testing and tools.
* Design, develop and extend the automated testing frameworks.
* The cross functional and system testing of the Zscaler Security Solution.
* Writing the system and solution test plan.
* Recreating the customer found defects.

I was diligently given daily assignments and training for two weeks to quickly get me on board with the actual work. My team manager, **Mr. Sachin Kumar** was kind enough to lay out an internship plan for me on the very first day of my arrival, detailing the work that I would be performing over the next three months of my summer internship. The plan was to give me sufficient knowledge of the Zscaler cloud security concepts and get me on-boad with the AGA-17 automation Sprint as well. During my internship, I was told to report my progress to two of my mentors: **Mr. Praveen Thalla and Mr. Niranjan Ramakrishnan.** While Mr. Thalla assigned me tasks on the security side, Mr. Ramakrishnan took care of making me familiar with the automation framework of Zscaler. This way, I was able to improve my security skill-set as well as Python coding skills, which are both imperative to become a cybersecurity engineer.

Throughout my internship, I learnt about several important security features and concepts such as:

|  |  |
| --- | --- |
| * Zscaler Cloud Firewall | * Malware Protection |
| * Advanced Threat Protection | * SSL Inspection |
| * File Type Control | * Data Leak Protection (DLP) |
| * DNS Control | * Authentication |
| * Browser Control | * Sandbox |
| * Rate-Limit | * Closed Proxy |
| * Fragmentation and Re-assembly of Natted Traffic | * Fragmentation and Re-assembly of Proxied Traffic |
| * Creation of Static Routes for GRE Tunnels |  |

Other than my formal training, there were team meetings and brown bag sessions to give the employees additional knowledge of several important features such as: Web-Security, Cloud Application Suite Integration, Configuring Log Streaming etc. These meetings and sessions were not only a good source of gaining knowledge but also a great way to network with people.

**Below, I detail few of the security features that I learnt and worked on during my internship:**

**Authentication:**

In this section, I’ll describe what I have worked on and learnt about user provisioning and authentication using Zscaler. The first thing which I experimented with was user and group authentication. I created my own demo company on Zscaler’s admin portal, enabled various security settings, created a user and departments and experimented with different aspects of authentication like: authentication through a known and unknown location, how frequently the user should be authenticated etc. I did extensive research and learnt that enabling authentication allows the Zscaler service to identify the traffic that it receives so it can enforce the configured location, department, group and user policies, as well as provide user and department logging and reporting.

When a user from an organization (with Zscaler deployed) opens a browser and sends an HTTP request to a site, the request is redirected to the nearest Zscaler Enforcement Node (ZEN), which is the gateway. The ZEN first checks if the request is from a location defined in the Zscaler admin portal (this is a known location aka DPPC), or from a location that was not configured on the admin portal (this is an unknown location aka Road Warrior).

When the Zscaler service receives traffic from a known location, the service automatically applies the location's policies and tracks all the internet activity by the location. An organization must provision the users and enable authentication to leverage granular department, group, and user policies as well as enable the ability to track usage trends by department and user.

However, if [authentication is disabled](https://help.zscaler.com/zia/configuring-locations#EnforceAuthentication) for a known location, users are able to access any website. This however, will be prevented if there are location-based category or website block policies configured. Even if the users are approaching from a location with an unregistered domain, the service will still know the actual location because the IP address is registered with Zscaler. Hence, location-based policies are still applied to these users. But here, the service will not know who the users are and to which domain they belong to because authentication is disabled.

**Cloud Firewall:**  
I got the opportunity to work a lot on Zscaler’s next-generation firewall which has the capabilities to allow granular control over an organization’s outbound TCP, UDP, and ICMP traffic.

Here are the ways I learned to configure different firewall policies:

* [**Firewall Filtering Policy**](https://help.zscaler.com/zia/configuring-firewall-filtering-policy)**:** Here one can add rules to allow or block specified types of traffic from a network to the internet. It gives the advantage to specify how the sessions are logged.
* [**NAT Control Policy**](https://help.zscaler.com/zia/about-nat-control)**:** Here I added rules to perform destination NAT and redirected traffic to specific IP addresses and ports.
* [**DNS Control Policy**](https://help.zscaler.com/zia/about-dns-control)**:** In this policy type, I added several rules to allow as well as block DNS requests. I redirected requests to a different DNS server, redirected the DNS responses by substituting the IP address in a DNS response with a preconfigured IP address.
* [**IPS Control Policy**](https://help.zscaler.com/zia/about-ips-control)**:** Using IPS Control, I configured rules to manage and protect traffic from intrusion over all ports and protocols using signature-based detection.

To sum it all up, I learnt that [configuring Firewall Policies](https://help.zscaler.com/zia/configuring-firewall-policies) requires the following:

* Organizations must forward their IP traffic from a **known location**.
* One must configure the four policies above as applicable and then [enable the firewall](https://help.zscaler.com/zia/enabling-firewall-locations) for one’s locations.
* If an organization wants to apply firewall policies at the user level, enabling user authentication and surrogate IP (discussed later) is a must, or else the firewall service applies organization and location policies.

**Firewall Filtering:**

By default, the Zscaler firewall allows all non-HTTP/HTTPS traffic from your network to the internet. But with the feature of Firewall Filtering, one is able to configure policies that can allow or block certain type of traffic from specific sources and to specific destinations.

**Bandwidth Control:**

Bandwidth control allows you to preserve access to your business-critical applications regardless of your internet pipe consumption. This enables you to things like adding more restrictive rules around social media and streaming media. For example, you can allocate a maximum of 10% of the bandwidth to the Streaming Media, Social Media, and File Share bandwidth classes. When bandwidth is restricted, these classes are not guaranteed any bandwidth and are restricted to 10% of the bandwidth when it is available.

[**How Bandwidth Control Works**](https://help.zscaler.com/zia/about-bandwidth-control#bw-works)**:**

First, you specify the maximum upload and download bandwidth limits for each location in your organization. About 5% of TCP traffic is overhead, such as packet headers. The Zscaler service does not include these in its bandwidth calculations. It only includes the application traffic.

Next, you [define your bandwidth classes](https://help.zscaler.com/zia/about-bandwidth-classes), specifying what URL categories and applications belong to a given bandwidth class. You can then reference those bandwidth classes in your bandwidth control policy − a set of prioritized rules that tell the service how to allocate the bandwidth when contention occurs. Each rule defines a maximum and minimum bandwidth for the bandwidth classes in the rule along with other parameters, like location and time of day.

Based on the bandwidth policy, Zscaler will distribute the bandwidth to each rule from top to bottom by looking at the minimum bandwidth first. Once completed, it will pass through each rule a second time to allocate the remaining bandwidth and distribute it based on the maximum bandwidth configuration.

The maximum bandwidth specifies the maximum percentage of the total bandwidth that the configured bandwidth class can use at a given point in time, and the minimum bandwidth specifies the guaranteed minimum bandwidth percentage that is available for the bandwidth class.

The maximum bandwidth percentage is applied at all times. Because of this, traffic can only take up to the percentage specified of the location's bandwidth, whether or not there is any congestion. This is useful to users who wish to suppress, but not block, non-business traffic.

The minimum bandwidth percentage is only enforced when there is contention on a location's connection and when traffic from the specified bandwidth classes is present. This allows a bandwidth class full bandwidth utilization until there is contention for the bandwidth by a traffic class with a higher priority. When bandwidth classes compete for bandwidth, the service allocates the guaranteed minimum bandwidth percentages to the bandwidth classes and allocates the remaining bandwidth according to the prioritized rules. Therefore, the total minimum bandwidth must be less than 100%.

**URL Filtering:**

During the initial phases of my internship I started by creating several URL policies and observing their actions on different users and groups. Basically, through URL filtering, one can limit the exposure to liability by managing access to web content based on a site's categorization. The URL filtering policy consists of [rules](https://help.zscaler.com/zia/how-do-i-configure-url-filtering-policy) that you define. When you add a rule, you specify criteria, such as [URL categories](https://help.zscaler.com/zia/about-url-categories), [users](https://help.zscaler.com/zia/about-users), [groups](https://help.zscaler.com/zia/about-groups), [departments](https://help.zscaler.com/zia/about-departments), [locations](https://help.zscaler.com/zia/about-locations), and [time intervals](https://help.zscaler.com/zia/about-time-intervals). There is also a [recommended policy](https://help.zscaler.com/zia/recommended-url-cloud-app-control-policy) for URL filtering.

To allow granular control of filtering, the service organizes URLs into a hierarchy of categories. To learn more about URL categories, see [About URL Categories](https://help.zscaler.com/zia/about-url-categories).

By default, the Cloud App Control policy takes precedence over the URL filtering policy. The service will apply the Cloud App Control policy to a web transaction before applying the URL Filtering policy. To change this setting and have the service apply the URL Filtering policy even if it has already applied a Cloud App Control policy, go to Advanced Settings and enable [Allow Cascading to URL Filtering](https://help.zscaler.com/zia/about-advanced-settings). For information on the order in which the service enforces all policies, including this policy, see [About Policy Enforcement](https://help.zscaler.com/zia/about-policy-enforcement).

I created several URL Policy rules with ‘Allow’, ‘Caution’ and ‘Block’ actions, below is a description of what these actions do:

* **Allow**:The service allows access to the URLs in the selected categories. You can still restrict access by specifying a daily quota for bandwidth and time. For example, you can allow your users to access Entertainment and Recreation sites, but restrict the bandwidth allowed for these sites so they don't interfere with business-critical applications. The daily time quota is based on the time that the rule is created. For example, if the rule is created at 11 a.m. PST, then the quota is renewed at 11 a.m. PST the next day.
* **Caution**:When a user tries to access a site, the service displays a [Caution notification](https://help.zscaler.com/zia/about-acceptable-use-policy-and-end-user-notifications#caution). You can use the system-defined notification, customize the text, or create your own notification and direct users to it.
* **Block**:The service displays a [Block notification](https://help.zscaler.com/zia/about-acceptable-use-policy-and-end-user-notifications#block). You can use the system-defined notification, customize the text, or create your own notification and direct users to it. [See image.](https://help.zscaler.com/zia/about-url-filtering#Image2)

**DNS Control:**

This was a concept which I only read about but never got to have any hand-on experience with. Finally, with the help of this internship, I could know how to work DNS control. Here’s what I have learnt about DNS control at Zscaler:

The Domain Name System (DNS) is a key part of the internet, offering the power of translating quickly between the human language of the URL and computer language of the IP address. With DNS Control, you can define rules that control DNS requests and responses.

However, DNS traffic often goes unmonitored and does not go through traditional firewalls. Because of this, DNS traffic can be abused through techniques such as tunneling. DNS Control also allows you to detect and prevent DNS tunneling occurring on your network.

The DNS Control policy has default rules that allow all DNS traffic. These rules always maintain the lowest precedence. You can modify their actions, but you cannot delete them.

## **Using Zscaler's DNS Servers:**

When you send your DNS traffic to Zscaler’s DNS servers, only recursive queries are supported. For Windows servers, forwarders are supported as they use recursive queries, while root hints are not supported as they use iterative queries.

On the DNS Control page, one can do the following:

1. [Configure a DNS Filtering rule](https://help.zscaler.com/zia/configuring-dns-control-policy).
2. View a list of all configured DNS Filtering policy rules. Here you can see the following:
   * **Rule Order**: The policy rule's order number. DNS Control policy rules are evaluated in ascending numerical order. You can sort this column.
   * **Admin Rank**: The assigned [admin rank](https://help.zscaler.com/zia/about-admin-rank) for the rule. This is visible only if admin ranking is enabled in the [Advanced Settings](https://help.zscaler.com/zia/about-advanced-settings#admin-ranking). You can sort this column.
   * **Rule Name**: The name of this rule. You can sort this column.
   * **Criteria**: A description of the different criteria that have been added to this rule.
   * **Action**: Whether the policy is set to Allow, Block, Redirect Request, or Redirect Response
   * **Description**: An optional description of the rule. You can sort this column.
3. [Edit or duplicate a DNS Filtering policy rule](https://help.zscaler.com/zia/how-do-i-edit-delete-or-duplicate-items-admin-portal).
4. [Modify the table and its columns](https://help.zscaler.com/zia/how-do-i-use-tables-admin-portal).
5. Search for a DNS Filtering policy rule.

**Cloud Sandbox:**

Sandbox provides an additional layer of security against zero-day threats and Advanced Persistent Threats (APTs) through Sandbox analysis, an integrated file behavioral analysis. To ensure your organization's web security, the Zscaler service runs and analyzes files in a virtual environment to detect malicious behavior. It propagates a hash of malicious files to all Zscaler Enforcement Nodes (ZENs) throughout the cloud, effectively maintaining a real time blacklist so it can prevent users anywhere in the world from downloading malicious files.

# I configured Zscaler’s Sandbox policy rules to analyze Windows executable files (.exe) and Windows library files downloaded from URLs in suspicious URL categories and allow/block suspicious traffic. The suspicious URL categories include the following:

* + Nudity
  + Pornography
  + Anonymizer
  + FileHost
  + Shareware Download
  + Web Host
  + Miscellaneous
  + Other Miscellaneous

The service also analyzes these files if they’re contained in ZIP archive files (.zip). Note that with the default Sandbox policy, the service only analyzes files that are equal to 2 MB or less. My other experiments on this module are as follows:

* Configured Sandbox rules to block files that contain the following types of malicious files:
  + **Adware**: Files that automatically render advertisements/install adware.
  + **Malware & Botnets**: Files that behave like APTs, exploits, botnets, trojans, keyloggers, spyware, and other malware.
  + **P2P & Anonymizers**: Anonymizers and P2P clients.
* Configured Sandbox rules to block malicious file downloads from any of the following protocols:
  + **FTP over HTTP**: File downloads from FTP over HTTP websites. (Requires the Advanced Firewall subscription.)
  + **HTTP**: File downloads from HTTP websites.
  + **HTTPS**: File downloads from HTTP websites encrypted by TLS/SSL
  + **Native FTP**: File downloads from native FTP servers
* **Results:**

My expectations from this summer internship were to actually implement what I have learnt through my courses at UNCC. In the coursework, Malware Analysis, I learnt how a malware functions and what it does, however, I did not know how a malware can be identified, blocked and reported. Through my summer internship at Zscaler, I not only got to get my hands dirty with actual malware but I also wrote my own signatures to capture and block such malicious files and sites. Through my Cyber Defense coursework, I knew what Data Leak Prevention is but I had never implemented it in real life. At Zscaler, I configured policies to prevent upload and download of sensitive data such as Social Security Numbers and Credit Card Numbers. Through the coursework of Applied Cryptography, I knew the concepts such as certificates, Key-Encryption-Key and OCSP (Online Certificate Status Protocol), I am proud to say that during my internship, I have not only mastered these concepts but have also automated actual customer cases related to all of the three concepts. There is absolutely nothing that I envisioned and did not achieve through this internship. All the credit goes to the constant efforts of my professors at UNCC who built up the foundation of my learnings and my mentors at Zscaler, who polished my knowledge and gave me enough work to implement these concepts practically.

The Zscaler training portal was also one of my biggest supports during my initial training phase. It consists of basic to advance videos explain each and every security feature that Zscaler deals with. There are several Zscaler certifications that employees can take to make them just better at what they are doing

* **Discussion and Conclusions:**

Working as a QA-Datapath and Security Intern with Zscaler this summer has been a very promising experience. I am worked on almost 50 to 60 customer reported security bugs and also security cases while creating security policies and learning implementation of GRE, IPSEC tunnels for secure traffic forwarding. I automated 36 cases related to the KEK and OCSP which are major security concepts. I made a decision to take up an online summer course ITCS-6190-Cloud Computing for Data Analytics, in order to understand the cloud architecture better. This course was definitely helpful towards my internship not only because it taught me about the cloud architecture but also because the daily assignments after my work at Zscaler kept me busy and focused and taught me how to manage time better.

At Zscaler, I got many opportunities to interact with members of different teams and the CEO Mr. Jay Chaudhary and get a better picture of Zscaler’s cloud security framework.

Now, towards the end of this summer internship, I have got the opportunity to present my three-months of work to the general public in San Jose via an Intern Expo organized by Zscaler. This opportunity would teach me how to integrate my work into a presentation and teach me people-skills as I would be required to present my work to both technical and non-technical audience. Additionally, in the last few days of my internship, I am hoping to work on some new security features and newly reported security bugs. This has definitely been a wonderful learning experience and I gained expertise in industry level cloud and information security standards.