**Google Cloud Platform**

**Cloud Armor Report by Paul Ziegler**

**Executive Summary:**

The purpose of the report is to educate the user on the web application firewall, specifically Google Cloud Platform’s Cloud Armor Firewall. The report is meant to explain how web application firewalls fit into network security as it relates to software defined networks like Google Cloud Platform. Section one of the report explains on a high level the architecture of a basic computer network. It than explains what a software defined network is and how it compares to a traditional corporate network. Section two of this report explains what network security is and its main components, one being the firewall. Section three explains the purpose of a web application firewall, which is the focus of this report. Section four of this report introduces Google Cloud Armor, the web application firewall that is the focus of this report. On a high level this section explains its capabilities. Section five explains the preconfigured firewall rules, or the parameters the firewall follows when filtering data. Section six explains how a user could tune those firewall rules depending on how they value data confidentiality, integrity and availability when using a web application on a software defined network.

**Section One, Basic Computer Network & Software Defined Network:**

* 1. **Basic Computer Network:**

A computer network is a set of connected devices commonly referred to as nodes. The devices on a network can be personal computers, mobile devices, servers, and network hardware. These connections can be made up of both wired and wireless telecommunication media. Communication on a network is facilitated by protocols, commonly Internet Protocol or IP. Each mode of communication on a network device is connected to a port on the device. Each port has an IP address which is unique on the network. In network communication the IP address is used to identify a host or a node. Data on the network is enclosed in packets which move across network media from one IP address’s denoted port to another.

 Because mathematically there can only be so many IP addresses, network addressing schemes are separated into subnetworks or subnets. Think your home network, your laptop, desktop, smartphone, and network printer all have a port with a unique IP address within the home network, these devices can communicate with each other unincumbered on the home network. What if you want to communicate with another device on a separate network through the internet? This is where some unique network devices come into play, the switch, and the router. The network switch facilitates communications between hosts within the network, it has many ports or places for devices to connect with their own IP addresses. Any device connected to the switch can send data to any other device on the switch. The switch essentially creates the network. The router on the other hand, like the switch also has ports with assigned IP addresses, it also facilitates network communication however unlike the switch, the router also acts as a gateway and facilitates communication between networks over the internet. One of the ports on the router is connected to an internet service provider like Verizon or Comcast, this gateway port also has a unique IP address assigned to it. As stated, every host within a network has an IP address that is unique on that network, the gateway port on the router has an IP address that is unique on the entire internet. (wikipedia, 2022)

* 1. **Visualization of Basic Computer Network:**



* 1. **Software Defined Network (SDN):**

Section 1.1 and 1.2 explain and show how a basic computer network works. The switch facilitates communication between devices within the network, and the router facilities communication with other networks. This is essentially how all networks work, even large corporate networks. Large corporate networks however can have many interconnected switches and many interconnected routers across different geographical locations. Large corporate networks often must facilitate communication not just between computer and computer but between potentially thousands of computers communicating with each other and with large servers containing central databases. Things get a lot more complicated, and the amount of hardware (routers, switches, network media, servers) begins to add to the cost and complication of maintaining such a network.

Software Defined Networking is an option to eliminate much of the physical hardware infrastructure that defines a corporate network. Instead of physical routers and switches facilitating communication between thousands of hosts and large in-house data servers, a software application in the cloud does it. Instead of large physical data servers existing in an office basement with potentially thousands of employees physically connecting via routers and switches and cable, the data is hosted in the cloud. When data is hosted in the cloud it is stored remotely in a massive data center owned by a web service provider like Amazon or Google. (What is Software-Defined Networking (SDN), 2022)

These datacenters are essentially giant computers primarily made up of storage and processing power, they are connected to the internet. The datacenter runs software programs that dynamically segment the storage and allocate processing power based on customer needs. Not only do these datacenters host customer data, but they also host customer applications where the customer’s users can access them remotely. These customer users are called remote hosts.

With software defined networking, a remote host would connect their personal computer to the internet anywhere, sign into the software defined networking service, then be able to remotely access their organization’s applications and datastores. The communication between the user, their employer’s virtual applications, and virtual data servers would be facilitated by the software defined network, limiting the need to have large scale physical network hardware in an office. The office network would only be setup to allow user devices to connect to a router and access the internet so that they can connect to the software defined network in the cloud. User computers would only need an operating system and a software client to allow them to send data packets to the software defined network. This report focuses on Google’s SDN called Google Cloud Platform.

* 1. **Diagram of a software defined network:**



The above diagram is a visualization of a large software defined network. The infrastructure layer is the only physical part of an SDN that a customer would need to have in house, it closely resembled the basic traditional network shown in 1.2, only its singular requirement would be to facilitate connections between computers and the internet or cloud, where the software defined network lives. The control layer is the software program that replaces the complicated network of routers and switches facilitating in-house communication between many computers and physical inhouse data servers and application servers. The application layer is the part of the software program that hosts the customers applications and data. Everything in the diagram aside from the infrastructure layer lives remotely in a third-party web service host’s data center.

**Section Two, Network Security, and the Firewall:**

**(2.1) Network Security and Authentication:**

Network security is a collection of processes, practices and policies that monitor network traffic to detect and prevent unauthorized network access and to prevent data confidentiality, integrity, and availability from being compromised. In corporations, authentication is very important. Authentication is the act of confirming that a user is who they say they are and has permission to communicate on the network and access the data they need to access. Typically, authentication is done with a username or password. (Network Security, 2022)

**(2.2) Basics of the OSI model**

To understand the different types of firewalls, it is important to have some base knowledge of the OSI model or Open Systems Interconnection model. This model explains in layers how data is packaged, sent and received between devices communicating across one or multiple networks. The highest layer of the OSI model is the application layer where high level protocols dictate resource sharing, think HTTP which is the protocol that dictates communication between web browsers and web servers. The next layer down is the presentation layer where high level application layer data files are encrypted and compressed. Next layer down is the session layer, where connection is established between to nodes to conduct a continuous exchange of back-and-forth data transmissions. At the next layer down, the transport layer, data is segmented as it is sent across a network. The next layer down, layer three is the network layer, where routers operate, taking data packets and moving them between networks based off their addressing. This is the layer where traditional network firewalls operate, monitoring and filtering individual packets based off their addressing to decide whether they are malicious or not. The next layer down is the data link layer where switches unpack the packets into frames and send them to different nodes on the network. At the bottom layer, the physical layer, the data frames are unpacked, and the individual node reads the data as binary. (OSI Model, 2022)

**(2.3) A Diagram of the OSI Model and of an individual packet:**

OSI Model: Note that network firewalls operate at level three



Layer Three Packet: Note the source and destination IP address



**(2.4) The Network Firewall:**

The network firewall is a security system, either a physical piece of hardware connecting the network between the router and the internet or a program on a network device itself. The firewall monitors and controls traffic as it enters and exists ports on the device. The firewall not only monitors and controls what devices hosts intend to communicate with, but they monitor and control specific packets of information flowing between networks hosts and their respective ports. (Firewall (Computing), 2022)

**(2.5) Diagram of Where the Network Firewall fits into a Network:**



**Section Three, The Web Application and Web Application Firewall:**

**(3.1) The Web Application:**

Oftentimes customers will use an SDN to host their web applications. Web applications are pieces of software that are hosted on an SDN where a user can access them through a browser on any device anywhere in the world. These applications are structured in the SDN typically in three tiers, the first being the web browser, this tier entirely resides on the customer user’s machine. It communicates with the second tier hosted remotely on the SDN, this tier communicates directly with the user, and does all software calculations for the user. The second tier than communicates with a third tier also remotely hosted on the SDN. This third tier acts as a database for all information created by the application. The SDN Facilitates communication between the three tiers as if it were a physical infrastructure made up of routers and switches. Most modern web sites or interfaces are web applications, think online banking portals or marketplaces like eBay. In relation to the OSI model, web applications work at layer seven, the highest layer where the high-level HTTP protocol dictates resource sharing between web users and these web applications.

**(3.2) The Web Application Firewall (WAF):**

Considering that the web application has the potential to communicate with any device that has a web browser, any sensitive data stored in tier three and the functions of the web application itself in tier two are vulnerable to cyberattack. Because of this vulnerability, like any physical network, an SDN has a feature to act as a firewall. Monitoring and controlling who communicates with any web applications inside and what kind of data is going back and forth between web applications hosted on the SDN and the wider internet. Web application firewalls differ from network firewalls in that they operate at a higher level on the OSI model. At layer seven the WAF is looking to filter HTTP requests made against whatever web site its protecting. These firewalls are scanning the requests for blocked geolocations, blocked source addresses and then checking the data against a list of preconfigured and custom rules. If the request comes up clean than the request is allowed through to layer tier two. (Web application firewall, 2022)

**(3.3) Architecture of a Web Application on an SDN and how a Web Application Firewall fits in:**

Since this report focuses specifically on the Google Cloud Armor Web Application Firewall, Cloud Armor was used in the below graphic.



**(3.4) How a Web Application Firewall can protect against common attacks**

DDOS

A DDOS attack is a directed denial of service attack where a malicious actor attempts to disable a web application by overloading it with empty requests in a short time frame. Without a WAF, these requests would be sent right to tier two, where the web app is supposed to process these requests. With tier two unable to process so many requests in a short timeframe, it would crash, brining down the web app.

 A web application firewall would be set with a rule setting a limit on how many requests a single IP address can send at one time. If that rule is violated than the WAF would blacklist or block that specific IP address. This rule would prevent a flood of HTTP requests from overloading the core functions of the web application at tier two. (How to Help Protect Dynamic Web Applications Against DDoS Attacks, 2017)

SQL Injection

While a DDOS attack is dangerous because it can temporarily disable a web application, a SQL injection attack is potentially worse as it can be used to harm the confidentiality and integrity of data stored on a SQL database. SQL databases operate at tier three in a web application. During a SQL injection attack, malicious SQL code is hidden within an HTTP request. Tier two of the web application does not recognize this as malicious code when it processes the HTTP request. The code is then injection into the data servers operating at tier two.

 The WAF can protect against these attacks by reading the request and looking for HTML script tags, event processors and script protocols styled as an attack. The WAF, when it finds this malicious SQL script would than blacklist or block the source IP and reject the request. (How does WAF Detect SQL Injection and XSS Attcks, 2022)

**Section Four, Google Cloud Armor Capabilities as a WAF:**

**(4.1) Cloud Armor’s capabilities as advertised:**

Cloud Armor allows Google Cloud Platform users to set security policies including pre-configured web application firewall rules. Users can also enable adaptive and managed protection including threat intelligence and named IP address lists. The main purpose of Cloud Armor is to protect web applications from distributed denial-of-service (DDoS) attacks and applications attacks including SQL injection. Some of Cloud Armor’s protections are automatically enabled while others need to be manually configured by the user (Google, 2021).

**(4.2) Diagram of How Cloud Armor Interacts with the Internet**



From this graphic we see a mobile device, this mobile device could be located anywhere in the world and owned by anyone. The device is making an HTTP request against a web application hosted on an SDN. We can see that inside the SDN the web application is running three identical instances of the same application. Web applications are often separated out into instances so that a load balancer can proportionally direct traffic to one if another instance gets to many requests to process at once and begins to experience performance shortfalls.

 When an HTTP request comes into the load balancer, it is first directed to the Cloud Armor WAF where its IP address is compared to a list of allowed IP addresses, its geo-location is then analyzed to see if the request is coming from a blocked location, lastly, the requests signature is compared against the WAFs preconfigured and custom rules. If the request does is clean than it will go back to the load balancer to be forwarded to one of the application instances. (Google, 2021)

**Section Five, Built in / pre-configured Cloud Armor Rules:**

The Cloud Armor web application firewall listens to traffic entering the hosted web application. The firewall’s job is to listen to traffic signatures and compare them to attack detection rules. These attack detection rules exist in groups called rule sets. These preconfigured rule sets protect against some of the most common cyberattacks. Essentially the firewall listens to traffic, when it detects a traffic signature that matches a rule in the rule set, then based on the language in that rule, Cloud Armor automatically kicks in a mitigation type. Some of the common web app threats that the Cloud Armor firewall is preconfigured to mitigate are (Google, 2021):

1. Broken Access Control: Access control determined what users of a web app can and can’t access, when a vulnerability in an access control system is exploited, data confidentiality, integrity and availability can be threatened. The Cloud Armor firewall can block requests from unauthorized users.
2. Injection: During an injection attack, user supplied data is not properly validated as it is entered into a web app interface. An injection attack can be used to input malware in a system. This malware can threaten data confidentiality, integrity, and availability. The most common injection attacks include SQL Injection, NoSQL Injection and ORM Injection. The Cloud Armor firewall can block bad data potentially containing injection attacks.
3. Cryptographic Failures: Cryptography is used to protect the confidentiality of web application data by obscuring it. When a cryptographic system fails a vulnerability is created that malicious actors can exploit to threaten data confidentiality. The Cloud Armor firewall can block unencrypted data or traffic to and from data sources that do not encrypt data.

The sensitivity of the Cloud Armor firewall can be tuned up or down depending on what kind of traffic the Google Cloud Platform user wants to filter out. The firewall is tuned to levels called paranoia levels.

**Section Six, Cloud Armor Paranoia Levels:**

As stated in section two, Cloud Armor listens for web traffic signatures. When the firewall matches a signature to a rule, mitigation is enabled based off the language in that rule. Each signature also has a corresponding paranoia level between zero and four. The higher the paranoia level, the more rules will be enabled based off how secure you want your hosted web application to be. When tuning cloud armor you select the paranoia level, if zero is selected your web application will be most vulnerable as no rules will be enabled, choosing level four would mean the most rules are enabled and your hosted web application is most secure. Each paranoia level should be considered by the Cloud Armor user based on how much they value data confidentiality, integrity, and availability. Cloud Armor bases its paranoia levels on the Open Web Application Security Project’s Mod Security Core Rule Set. Below is a description of each paranoia level and a recommendation for when a firm should tune the Cloud Armor firewall to it (OWASP, 2021):

1. Level One: this is the baseline paranoia level with no additional rules turned on. Being that this level is the least strict many false positive suspicious traffic will not be filtered. To maintain data confidentiality, integrity, and availability, this is the bare minimum level of Cloud Armor security for any firm hosting a web server.
2. Level Two: at this paranoia level additional rules are enabled to filter traffic at a much stricter level than at paranoia level one. As this level is stricter, expect more false positives. It is recommended that a firm dealing with any sort of customer data on its web servers enable at bare minimum level two.
3. Level Three: level three is even more strict than level two. At this level, false positives should be expected. Firms may need to create rule exclusions if these false positives become a hinderance to normal web activities. This paranoia level is considered the norm for any web server facilitating online banking.
4. Level Four: This is the strictest paranoia level an organization can set. The amount of false positives Cloud Armor rules will filter at this level is very high. This level should be set if a breach in data confidentiality, integrity and availability would result in a firm suffering a catastrophic incident.

**Glossary:**

Network Media, how network communicating travels, cables or wireless

Network packet, a unit of data travelling through network media

Network Host, any device connected to a computer network

HTTP, an acronym for hypertext transfer protocol, this protocol governs web traffic

Web Server, a set of computer hardware and software that facilitates HTTP requests

Web Application, also referred to as a web app, a web application is a piece of software remotely hosted on a web server and accessed via an internet browser.

IP Address, the unique address that each device has on the internet or on a local network

Firewall, a key piece of network security that listens to (monitors) web ingoing and outgoing web traffic based on configured security rules.

Rule, a regulation or set of parameters set on a firewall, basically it is a piece of language coded into the firewall where when it listens for and detects a matching signature, a set of mitigation parameters are activated.

Signature, a protocol that confirms the authenticity of a piece of data

**Bibliography:**

# Bibliography

*Firewall (Computing)*. (2022, December 6). Retrieved from wikipedia.com: https://en.wikipedia.org/wiki/Firewall\_(computing)

Google. (2021, November 28). *Introducing Cloud Armor features to help improve efficacy: advanced rule tuning and auto deploy*. Retrieved from Google.com: https://cloud.google.com/blog/products/identity-security/introducing-cloud-armor-features-to-help-improve-efficacy

*Network Security*. (2022, December 6). Retrieved from Wikipedia.com: https://en.wikipedia.org/wiki/Network\_security

OWASP. (2021, October 28). *Working with Paranoia Levels*. Retrieved from coreruleset.org: https://coreruleset.org/20211028/working-with-paranoia-levels/

*Web application firewall*. (2022, December 6). Retrieved from wikipedia.com: https://en.wikipedia.org/wiki/Web\_application\_firewall

*What is Software-Defined Networking (SDN)*. (2022, December 6). Retrieved from vmware.com: https://www.vmware.com/topics/glossary/content/software-defined-networking.html

wikipedia. (2022, December 6). *Computer Network*. Retrieved from wikipedia.com: https://en.wikipedia.org/wiki/Computer\_network