Volume 8, No. 2, March 2017 (Special Issue)

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Cisco Umbrella: A Cloud-Based Secure Internet Gateway (SIG) On and Off Network

Bisma Shah
Department of CSE, SEST
Jamia Hamdard, New Delhi, India
shahbisma2009@gmail.com

Abstract: In present era, organizations use cloud in a variety of different service models and deployment models. So the cloud providers must ensure the security of their infrastructure and the protection of clients' data and applications against malwares. Cloud security architecture is effective only if correct defensive implementations are in place.

A secure Web gateway (SWG) is a solution that filters malware from user-initiated Internet traffic to enforce corporate and regulatory policy compliance. SWGs were originally used for bandwidth and access controls; they are nowadays also helpful in threat protection. But they usually do so ineffectively and in an inelegant manner. Moreover deployment of SWG is complex, and in order to avail protection, agents or PAC (Proxy auto- config) files are required to be installed. The SWG is not competent enough to properly secure the users in this mobile, cloud-era. These challenges are addressed and users are protected everywhere effectively by using a new category called Secure Internet Gateway (SIG). A SIG is a cloud-delivered internet gateway that provides safe and secure access to the users wherever they go, even when the users are off the VPN/network. Whenever initiation of internet requests is made, it is first checked and inspected by a SIG. Cisco Umbrella is Cisco's first SIG in the cloud.

The aim of this paper is to gain an insight into the features of Cisco Umbrella - a Cloud-based Secure Internet Gateway.

Keywords: Cisco Umbrella; OpenDNS; Off-Network Security; Threat Intelligence; Cloud-delivered network security**.**

INTRODUCTION

Cisco Umbrella, Cisco's platform for cloud security, provides the first line of defence against threats on the internet whether the users are on or off the corporate network [1]. Umbrella provides complete discernibility into internet activity across entire enterprise locations, network devices, and roaming users, and ensures blocking of threats before they ever reach your network or endpoints. Because it is delivered from the cloud and built into the foundation of the internet, Umbrella is the simplest security product to deploy and provides powerful, effective protection. By scrutinizing and learning from internet activity patterns, Umbrella automatically unmasks the attacker infrastructure organized for attacks, and proactively blocks requests to malicious destinations before a connection is ever established — without adding any latency for users (Figure 1) [2].This global infrastructure handles over 100 billion internet requests a day, which is then analysed by the security engine to learn where attacks are being staged [3]. With Umbrella, you can identify already infected devices faster, prevent data exfiltration and stop phishing and malware infections earlier [4]

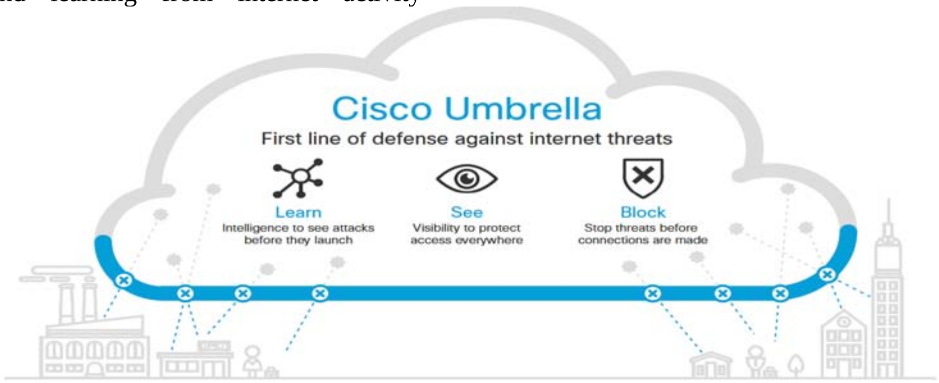
Cisco Umbrella
First line of defense against internet threats
Learn
Intelligence to see attacks before they launch
See
Visibility to protect access everywhere
Block
Stop threats before connections are made

Figure1. Cisco Umbrella

Construction of Cisco Umbrella is based on Open DNS platform, which has been delivered from the cloud since its foundation [5], [6]. Then technologies of the Cisco security portfolio were integrated, including capabilities from the Cloud Web Security proxy, and the Advanced Malware Protection (AMP) file inspection, not just by merging them together, but by re-engineering them to be delivered within Umbrella in such a way that they can be used easily and are capable of delivering even more effective security [7].

Cisco Umbrella fills the off-network security gap that exists in many organizations with remote and mobile workers [8]. Umbrella enforces security at the DNS and IP layers, preventing malicious IP connections from being established or malware from being downloaded. Umbrella prevents command-and-control (C2) callbacks, malware, and phishing over any port or protocol. And Umbrella provides DNS-

© 2015-19, IJARCS All Rights Reserved

layer network security for any device, regardless of location [8].

All the Umbrella identification and enforcement services reside in the cloud, running within the Cisco Umbrella global network of 25 data centers around the world. Internet requests and all other traffic from customers whose employees are working on corporate networks can be automatically directed to the Umbrella cloud service. And when roaming users fail to log onto their corporate VPNs, Cisco leverages a lightweight endpoint footprint that intercepts external DNS requests issued by the laptop and redirects them to Umbrella, a cloud security platform built into the foundation of the internet. The client software also adds a unique identifier so that Umbrella can identify which organization and which device each request comes from. As a result, Umbrella can apply the correct policy to each request and also create logs of individual laptop activity [8].

FEATURES OF CISCO UMBRELLA

First line of defense against threats.

Cisco Umbrella is a cloud security platform that is built into the foundation of the internet. Enforcing security at the **DNSand IP layers**, Umbrella blocks requests to malicious and unwanted destinations even before a connection is ever established — thereby stopping threats over any port or protocol before they reach your network or endpoints (Figure 2) [9].

Visibility and protection everywhere.

As a cloud-delivered service, Umbrella provides the discernability needed to protect internet access across all network devices, office locations, and roaming users. Umbrella logs all internet activities and categorizes them by the type of security threat or web content, and the action taken — whether it was blocked or allowed [9]. Logs of all activity can be retained as long as needed and easily recalled for investigation. You can even uncover cloud apps and Internet of Things (IoT) devices in use across your company.

Threat Intelligence (see attacks before they launch).

This global network infrastructure handles over 100 billion internet requests a day, which gives a unique view of relationships among domains, IPs, networks, and malware across the internet. Just like Amazon, that learns from patterns of shopping to suggest the next purchase, Umbrella learns from patterns of internet activity to automatically identify attacker infrastructure being used for the next threat, and then block users from going to malicious destinations in the future [9].

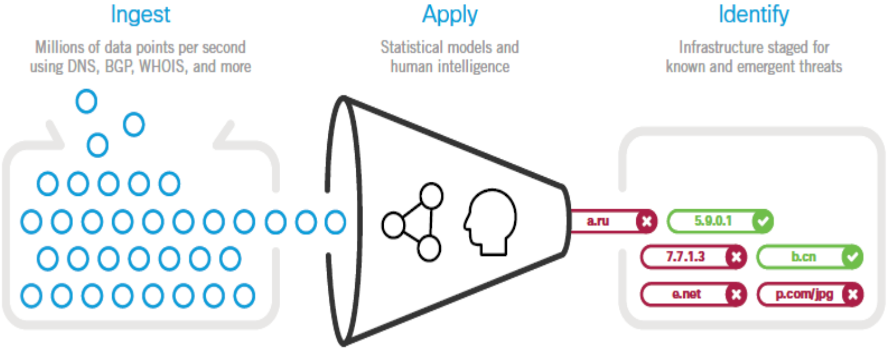
Ingest
Millions of data points per second using DNS, BGP, WHOIS, and more
Apply
Statistical models and human intelligence
Identify
Infrastructure staged for known and emergent threats
a.ru
5.9.0.1
7.7.1.3
b.cn
e.net
p.com/jpg

Figure 2. Threat Intelligence

Enterprise-wide deployment in minutes.

Umbrella protects all of your users in minutes in the fastest and easiest way. It is powerful, effective security without the typical operational complexity. By performing everything in the cloud with 100% uptime, there is no need to install any hardware, and no need to manually update any software [9].

API-based integrations to the rest of your security stack.

Umbrella’s API enables you to integrate with your existing security stack including security appliances, intelligence platforms, and cloud access security broker (CASB) controls to amplify protection [10]. These security controls provide advanced threat defences (ATDs) like data file analysis, network traffic analysis, endpoint behavioural analysis, and threat intelligence services. By influencing Umbrella’s platform, joint customers extend and use the intelligence of these security controls globally, even when users are off the corporate network [1]. Umbrella can push log data about internet activity to your SIEM (Security Information and Event Management) or log management systems, and using Umbrella’s enforcement API, you can programmatically send malicious domains to Umbrella for blocking. This allows you to amplify existing investments, and easily extend protection everywhere.

Enforcement built into the foundation of the internet.

The internet’s infrastructure is used by Cisco Umbrella to block virulent destinations before a connection is ever established, with no hardware to install and no software to maintain. By delivering security from the cloud, not only does this save money, but also provide more effective security [4].

Umbrella uses DNS as one of the main mechanisms to get traffic to cisco’s cloud platform, and then uses it to enforce security, too. When Umbrella receives a DNS request, it uses intelligence

© 2015-19, IJARCS All Rights Reserved

to determine if the request is safe, malicious or risky — meaning the domain contains both malicious and legitimate content. Safe and malicious requests are routed as usual or blocked, respectively. Risky requests are routed to cisco's cloud-based proxy for deeper inspection. The Umbrella proxy uses Cisco Talos web reputation and other third-party feeds to determine if a URL is malicious. Cisco's proxy also inspects files attempted to be downloaded from those risky sites using anti-virus (AV) engines and Cisco Advanced Malware Protection (AMP). And, based on the outcome of this inspection, the connection is allowed or blocked [2].

Cisco Umbrella Roaming (Security when you're off the VPN).

To protect the employees of an organization against threats even when they are not using the office VPN/network, a cloud-based security service of Cisco Umbrella, that is, Cisco Umbrella Roaming can be used, acting as Cisco firewall for next-generation (Figure 3). No installation of additional agents is required. We simply need to activate in the Cisco AnyConnect client, Umbrella functionality, to get seamless protection against malware, phishing, and command-and-control (C2) callbacks wherever the users go [11].

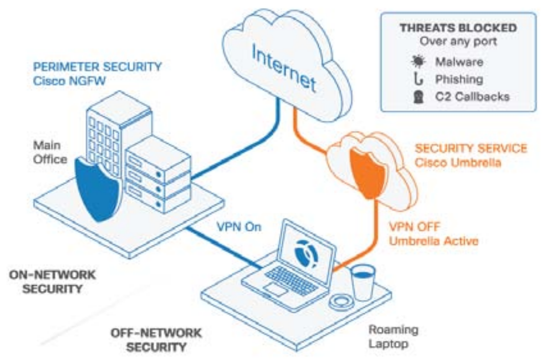

Figure 3. Cisco Umbrella providing protection to corporate users both on and off the VPN

Two new security categories for Umbrella: DNS Tunneling VPN and Potentially Harmful [12]

1) DNS Tunneling VPN :

The data of other programs or protocols in DNS queries and responses can be concealed by using a process called DNS Tunneling. DNS tunneling can be used for legitimate reasons, for example, anti-virus programs and security services use it to fetch signatures. But, there are possibilities of using DNS Tunneling illegitimately as well. DNS tunneling can be used to conceal data that is shared through an internet connection and to hide outbound traffic. To prevent this, a new security category within Cisco Umbrella, **DNS tunneling VPN** is used. Servers of commercial DNS tunneling VPN services are classified by DNS tunneling VPN. We can false front outgoing traffic as DNS queries by these services, thereby opposing its appropriate use, prevention of data loss, or security policies. Hence overall discernability into threats is reduced. Moreover the danger of DNS tunneling and potential data loss is minimized by DNS tunneling VPN security category.

2) Potentially Harmful :

There exist uses of other ambiguous and unsafe types of DNS tunnelling, beyond DNS tunneling VPNs. These uses and other suspicious domains should be audited and blocked. Potentially harmful category was developed to give customers discernability into these domains. Domains likely to be malicious, that is, those having a lower level of confidence are contained in this category, while the domains having higher level of confidence are classified in the normal block lists. For example, this security category includes those services of DNS tunneling that cannot be related to a specific type of service. One more example comes from the Spike rank model [13]. High traffic on the Spike rank domain will automatically be categorized as malicious, whereas, Potentially Harmful category will include the lower threshold traffic on Spike rank domain.

CONCLUSION

Gathering prior information or intelligence on advanced attacks that strike your networks is essential, but it is not sufficient. Today, employees work across many locations, using multiple devices, and they areincreasingly employing public cloud services. An organization's intellectual property or customer information will be accessed necessarily from uncontrolled network locations [1][15]. Security needs to log and block all malicious activity regardless of employee locale [14]. You cannot have a check on all your roaming employees to always turn on their VPN. If VPNs are not always on, only antivirus can provide defense from advanced attacks. Attackers increasingly target this weak link between roaming employees and the corporate network. To close this gap, we need to use the intelligence that advanced threat defences gather and use them locally at the perimeter and extend it to all endpoints. Cisco Umbrella, through integration partnerships, extends and imposes the local intelligencefrom existing security stack to protect your employees, whether they're working **onoroff the corporate network.**

REFERENCES

[1] "Extend your threat protection to any device, anywhere," https://learn-umbrella.cisco.com/solution-briefs/extend-threat-protection, 2016.

[2] "Cisco Umbrella at a glance,"https://learn-umbrella.cisco.com/datasheets/cisco-umbrella-at-a-glance, 2017.

[3] "Cloud security platform and threat intelligence," https://learn-umbrella.cisco.com/datasheets/umbrella-product-overview, 2016.

[4] "Cisco Umbrella + Cloudlock," https://learn-umbrella.cisco.com/solution-briefs/umbrella-cloudlock-solution-brief, 2017.

[5] "Introducing cisco Umbrella,the industry's first secure internet gateway in the cloud," http://blogs.cisco.com/security/cisco-umbrella-secure-internet-gateway, Feb 9,2017.

[6] "OpenDNS Advances Predictive Security Using Data Science and Sound Wave Technology,"

© 2015-19, IJARCS All Rights Reserved

https://umbrella.cisco.com/blog/2015/11/19/opendns-cracks-predictive-security/.

[7] “Cisco Launches "Umbrella" Secure Internet Gateway,” http://www.securityweek.com/cisco-launches-umbrella-secure-internet-gateway, Feb 10, 2017.

[8] Your users have left the perimeter. Are you ready?, 1st ed. U.S, 2016, p. 4.

[9] “Cisco Umbrella : Insights Package,” https://learn-umbrella.cisco.com/datasheets/umbrella-insights , 2017.

[10] “Avoid the aftermath with a before strategy,” https://umbrella.cisco.com/products/features.

[11] “Cisco Umbrella Roaming,” http://www.cisco.com/c/en/us/products/security/firewalls/umbrella-roaming.html, 2016.

[12] “Announcing two new security categories for Cisco Umbrella,” https://blog.opendns.com/2017/01/17/announcing-two-new-security-categories-cisco-umbrella/ , January 17,2017.

[13] “SPRank and IP Space Monitoring at BruCON & Hack.Iu,” https://blog.opendns.com/2015/11/19/sprank-and-ip-space-monitoring/, November 19, 2015.

[14] “New dog, new tricks,” https://umbrella.cisco.com/products/secure-internet-gateway, 2017.

[15] Farheen Siddiqui "State of Art Ontological Infrastructure For Cloud Computing” International Journal of Computer & Organization Trends (IJCOT) – Volume 36 Number1 – October 2016 ISSN: 2249-2593 Pg22-26

© 2015-19, IJARCS All Rights Reserved