Barracuda WAF-as-a-Service and CloudGen Access

https://campus.barracuda.com/doc/98225834/

Introduction

Barracuda CloudGen Access is an innovative ZTNA (Zero Trust Network Access) solution that provides secure access to applications and workloads from any device and location. CloudGen Access continuously verifies that only the right person, with the right device, and the right permissions can access company data or apps.

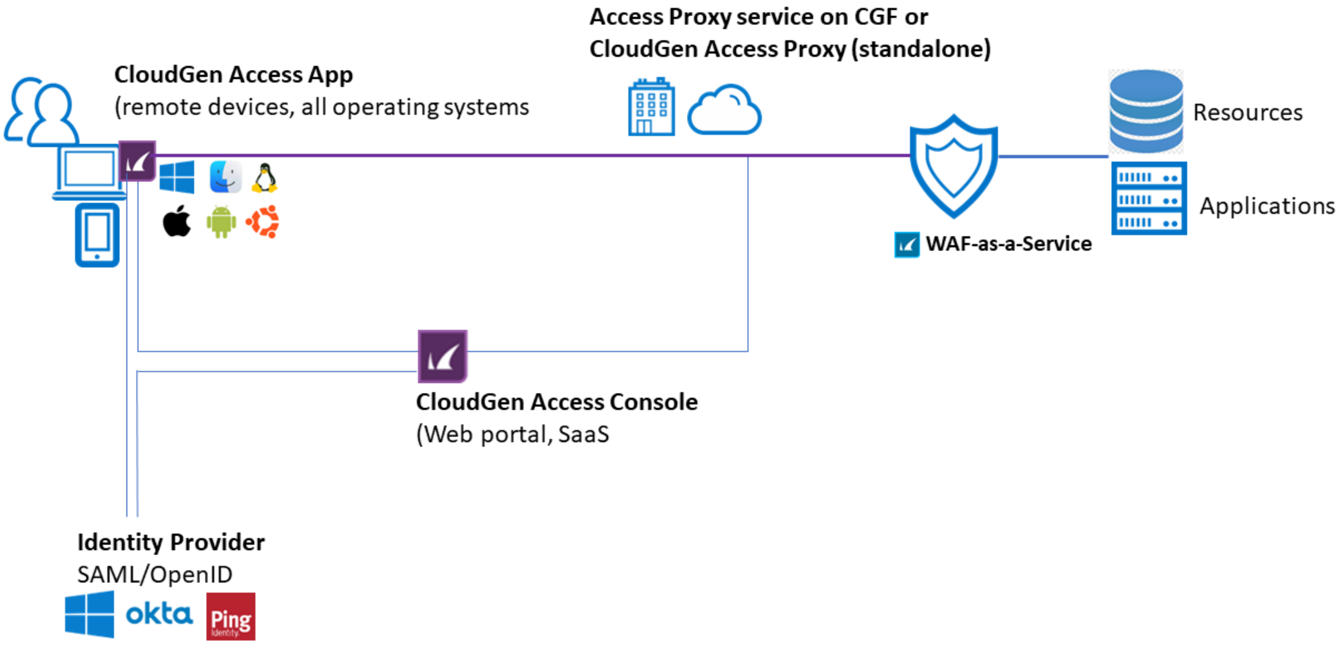
Barracuda CloudGen Access can be deployed with Barracuda WAAS to provide secure access with layer 7 controls to an organization’s web resources. Built on Barracuda’s proven security effectiveness, Barracuda WAF-as-a-Service protects against advanced layer 7 attacks such as DDoS (Distributed Denial of Service), SQL injection, zero-day threats, AJAX and JSON payloads, the OWASP (Open Web Application Security Project) Top Ten, and others.

Barracuda CloudGen Access is available for use as part of the Barracuda WAAS Premium license.

Use Cases

The following are two use cases to illustrate the value of deploying CloudGen Access and WAAS together.

For the below-mentioned use cases, traffic is tunneled from the CGA Access Client to the CGA Proxy, which in turn connects to the Application through the Barracuda WAAS.



Use Case 1 - Protecting Sensitive URL Spaces of an Application (Layer 7 Access Control):

Many CMS platforms, such as WordPress and Drupal, allow customizing the layout and content of the application via an administration console. For example, when a WordPress application's design template or site theme needs to be updated, the site administrator would login and access /wp-admin/* part of the site. While the application in general is accessible to all, including unauthenticated users, the administration page and beyond should be accessed only by authenticated users with valid permissions.

Solution

Combine WAAS and CGA

While the CGA can perform user authentication, WAAS can be used to provide L7 access control by disallowing access to the /wp-admin/* URL space for internet users.

> You can access the application without CGA i.e., by directly going through the WAAS, but access to the sensitive URL will be granted only for users initiating traffic through the CGA.

1. Onboard the CMS application through WAAS – Follow the 3-step wizard to deploy the CMS application on WAAS.
2. Deploy the Barracuda CloudGen Access Proxy using your preferred deployment method.
3. Configure access on the Barracuda CloudGen console:
    1. Add the resource – The resource to be accessed would be the WAAS endpoint domain

which is deployed in front of the CMS application.
    2. Add the proxy created in **Step 2**.
    3. Enroll users and their devices to authorize access.
4. Create a URL ACL (Access Control List) to block access to the internet users to the sensitive URL (/wp-admin/*) and configure the extended match such as (client-ip neq <CGA access proxy>) to allow access only from the CloudGen Access Proxy IP address.

Use Case 2 – Prevent Insider Threats by protecting Internal applications:

Internal applications can be an organization's payroll or travel reimbursement applications, which must be accessed only by the organization's employees. Traditionally, these apps would be accessed over a VPN tunnel. However, VPN tunnels have many disadvantages.

CloudGen Access (ZTNA) vs Traditional VPN		
	CloudGen Access (ZTNA)	**Traditional VPN**
Access to internal network applications	Yes	Yes
Network-level access ("teleport" device into the office network / VNET)	No	Yes
Reduce the attack surface by only granting access to required apps	Yes	No
Per-User and Per-Application security, visibility, reporting	Yes	No
Always on "VPN" without the hassle of connecting/disconnecting	Yes	No
Scale demand coming from remote (WFH) employees automatically	Yes	No
Easily provision company, employee-owned or contractor devices	Yes	No
Ongoing validation of device posture to prevent unauthorized/insecure access	Yes	No
Ongoing validation of user/privilege to prevent unauthorized access	Yes	No
Control and Log access to SaaS services	Yes	No

Solution

Combine WAAS and CGA

Barracuda WAAS can be deployed with CGA in these deployments to prevent insider threats by offering L7 security such as DDoS, SQL injection, zero-day threats, AJAX and JSON payloads, the OWASP Top Ten, and others.

With the CGA Integration, WAAS can be configured to block all external traffic and only allow traffic originating through the CloudGen Access Proxy.

How to combine WAAS and CGA:

1. Onboard the Internal application through WAAS – Follow the 3-step wizard to deploy the application.
2. Deploy the Barracuda CloudGen Access Proxy using your preferred deployment method.
3. Configure access on the Barracuda CloudGen console:
    1. Add the resource – The resource to be accessed would be the WAAS endpoint domain that is configured for the application.
    2. Add the proxy created in **Step 2**.
    3. Enroll users and their devices to authorize access.
4. Create a URL ACL or IP Block List Rule to block access to the internet users and only allow access only from the CloudGen Access Proxy IP address.

Related Articles

- Getting started with Barracuda WAAS
- Getting started with Barracuda Cloud Gen Access
- Deploying Barracuda CloudGen Access Proxy
- Barracuda CloudGen Access Proxy requirements
- Zero-Trust Network Access - https://www.barracuda.com/products/network-security/cloudgen-access

Figures