Anti-DDoS Pro

Best Practice

Product Documentation

Contents

Best Practice
Remote Protection Scheme with Anti-DDoS Pro

Last updated : 2020-07-07 16:10:31

Background

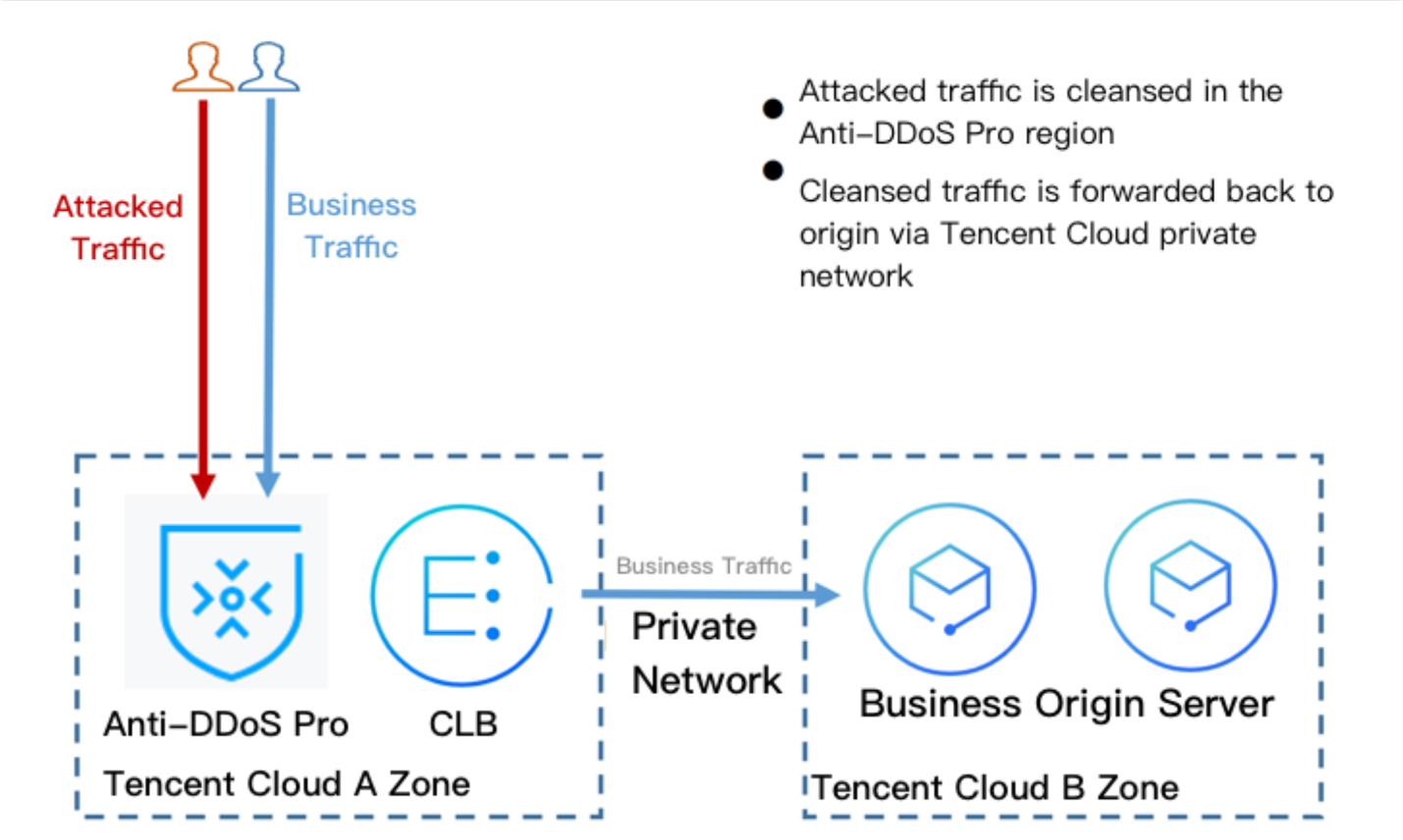
Anti-DDoS Pro provides up to 300 Gbps of protection bandwidth in Shanghai but a lower bandwidth in Guangzhou and Beijing. In addition, Anti-DDoS Pro is not available in Chengdu, Chongqing, and other regions in Mainland China.
If your business real server is deployed in Tencent Cloud and you need to use the DDoS protection capability in regions other than the region where your real server is located, you may consider the following solution.

Solution

This solution involves Anti-DDoS Pro, Cloud Load Balancer (CLB), and your real server. First, you will need to deploy a CLB instance in the region where you have Anti-DDoS Pro resources and bind it to your Anti-DDoS Pro instance. Then, configure the private network forwarding rules for CLB to ensure that your business can be accessed through the public IP of the CLB instance.

- Under normal circumstances, business traffic will be resolved to the public IP of the real server or directly to the public IP of the CLB instance in another region for nearby access to the real server.
- If attacks occur, business traffic will be resolved to the CLB IP for the Anti-DDoS Pro instance to cleanse the traffic. After the traffic is cleansed, CLB will forward the traffic back to the real server through private network Direct Connect.

The following figure describes the details of the solution:



Benefits

- The DDoS protection capability will no longer be limited by regions and can be as high as 300 Gbps.
- The business traffic will be forwarded via private network Direct Connect with high reliability and a low latency.
- You will enjoy all the advantages brought by Tencent Cloud BGP network. All your public IPs will be BGP IPs and the latency will be very low.

Suggestions and Notes

- Deploy Anti-DDoS Pro and CLB instances in advance.
- Establish a business availability monitoring system so that you can promptly detect and respond to any problem with access to the real server if no automatic switching mechanism is deployed.
- Test regularly, familiarize yourself with the solution details, and solve potential problems promptly.

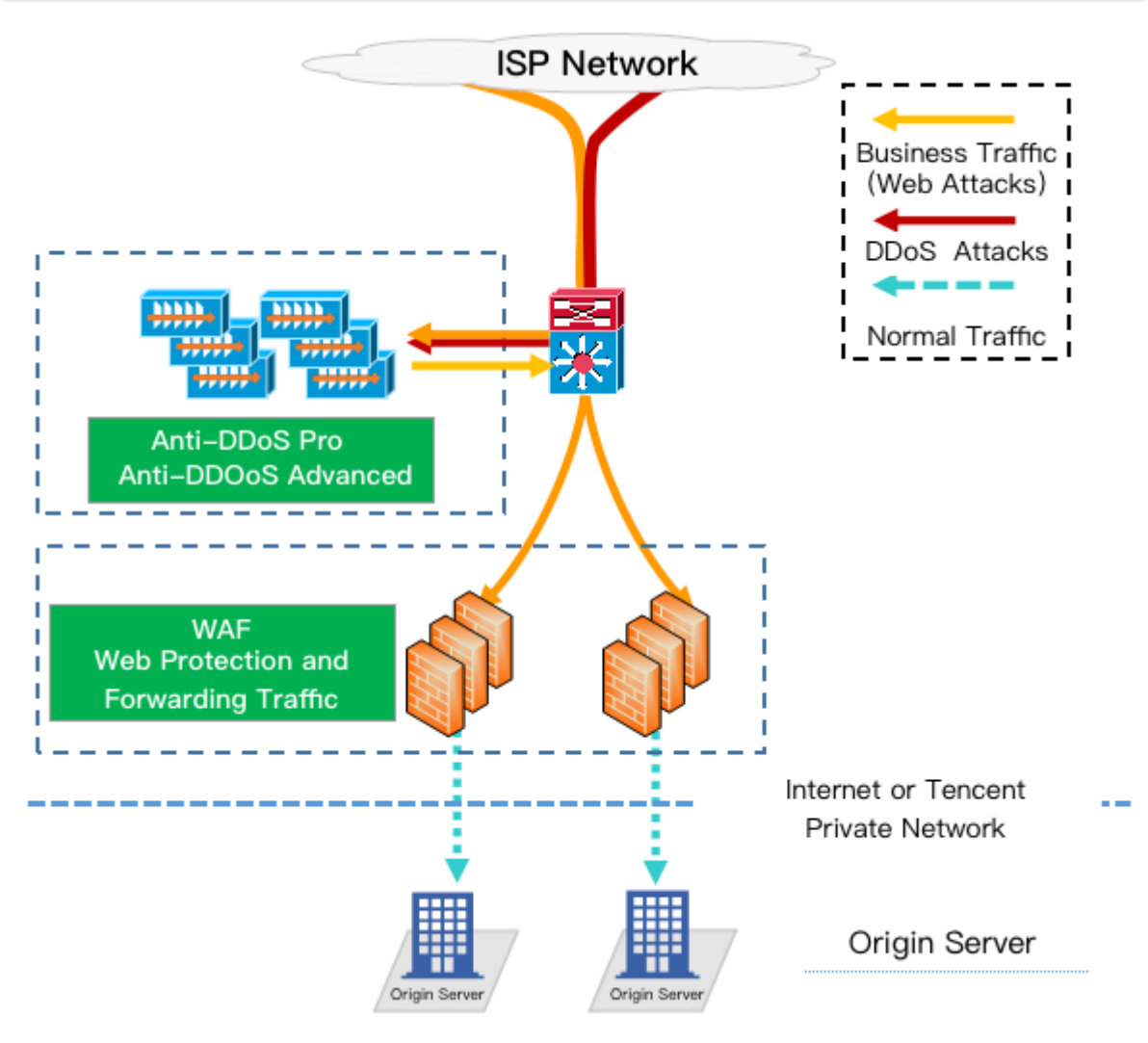
Using Anti-DDoS Pro Together with WFA

Last updated : 2020-07-07 16:10:32

Anti-DDoS Pro can be used together with Web Application Firewall (WAF) to provide you with comprehensive protection.

- Providing DDoS protection capability of hundreds of Gbps at one click, Anti-DDoS Pro can easily defend against DDoS attacks and ensure the smooth operation of your business.
- WAF can block web attacks in real time to ensure the security of your business data and information.

Deployment Scheme



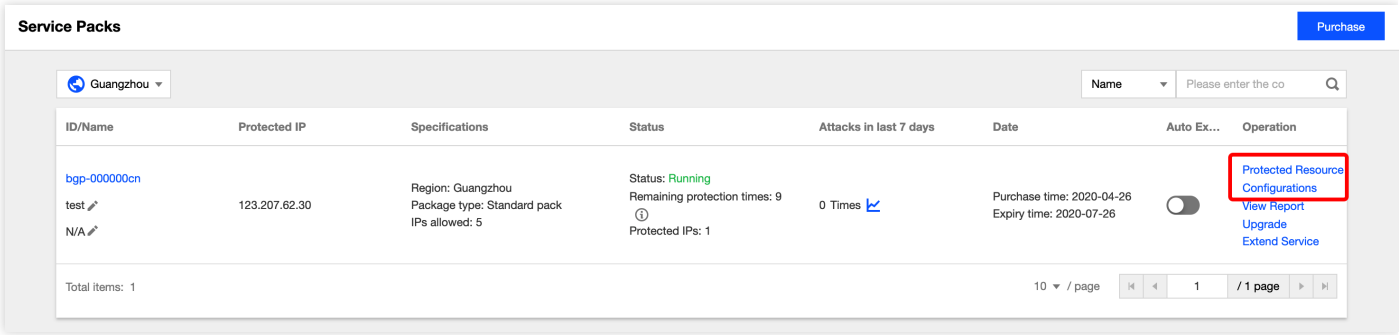
Directions

Configuring WAF

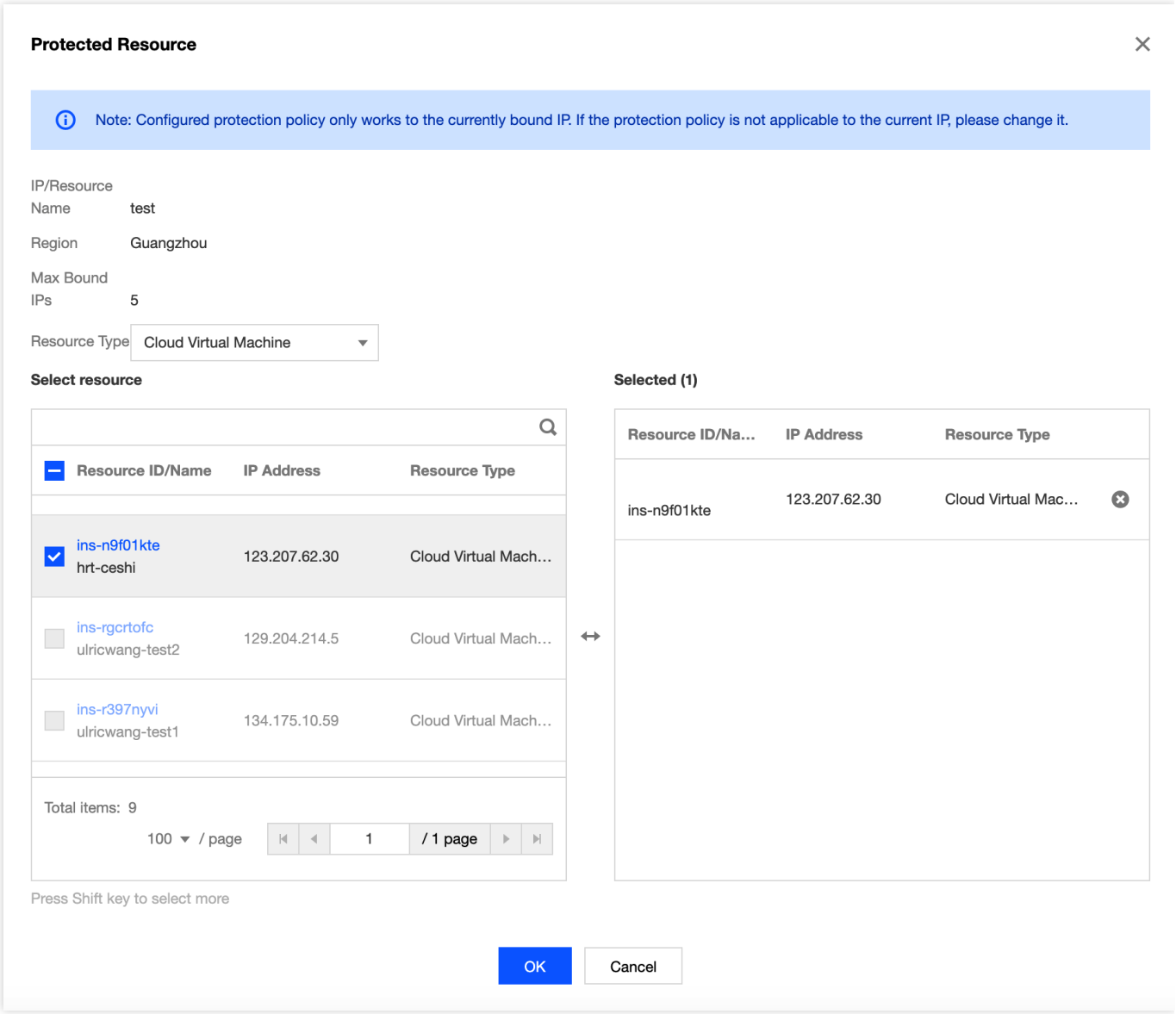
For more information on quick integration with WAF, please see Getting Started with WAF.

Configuring Anti-DDoS Pro

1. Log in to the new Anti-DDoS Pro Console and click **Anti-DDoS Pro Instance** on the left sidebar.
2. Select the region of the target Anti-DDoS Pro instance and click **Manage Protected Object** in the "Operation" column of the instance.



3. On the protected object management page, select "Resource Type" and "Resource Instance" as needed.
   - Resource Type: resources with public network IPs in the public cloud are supported, such as CVM, CLB, and WAF.
   - Resource Instance: you can select multiple instances (no more than the number of "bindable IPs").



4. After completing the configuration, click **OK**.

> If the WAF instance is in CLB type, then on the resource binding page, set "Resource Type" as "CLB", and select the public IP of the corresponding CLB instance in the "Resources to Associate" section.

Suggestions on Stress Test for Business System

Last updated : 2020-07-07 16:10:33

A stress test is designed to simulate DDoS attacks. To ensure the quality of the test, you are recommended to read this document carefully before conducting a stress test.

> The following suggestions are mainly about the impact of DDoS protection on stress testing. You may also need to consider other test-related factors, such as network bandwidth, linkage loads, and other basic resources.

Adjusting Protection Policies

- Disable CC protection policies, or set the HTTP request threshold for CC protection to a value higher than the maximum value of your stress test.
- Disable DDoS protection policies, or set the cleansing threshold for DDoS protection to a value higher than the maximum value of your stress test.

Limiting Traffic and Number of Requests in Stress Test

- The bandwidth of your stress test should be lower than 1 Gbps; otherwise, attack protection may be triggered.
- The number of HTTP requests in your stress test should be no more than 20,000 requests per second (QPS); otherwise, attack protection may be triggered.
- The number of new connections established per second, the maximum number of connections, and the number of inbound packets per second in your stress test should be less than 50,000, 2,000,000, and 200,000, respectively.

> If the traffic and number of requests in your stress test will exceed the above ranges, please contact Tencent Cloud Technical Support. We will offer support during your stress test.

Evaluating Impact of Stress Test in Advance

You are recommended to contact Tencent Cloud solution architects or Tencent Cloud Technical Support before you conduct the stress test to evaluate possible consequences and develop risk aversion measures.

Solution to Exposed Real Server IP

Last updated : 2020-07-07 16:10:34

Some attackers may record real server IP history, and the exposed IPs allow them to bypass Anti-DDoS Pro and directly attack your real server. In this case, you are recommended to change the actual real server IP.
You can refer to this document before changing the real server IP to check the risk factors and prevent the new IP from disclosure.

Checklist

Checking DNS resolution history

Check all the DNS resolution records of the attacked real server IP, including resolution records of sub-domain names, MX (mail exchanger) records of mail servers, and NS (name server) records. Make sure that all these records are configured to the protected IP so that the DNS will not resolve to the new real server IP.

Checking for information disclosure and command execution vulnerabilities

- Check your websites or business systems for possible information disclosure vulnerabilities, such as phpinfo() disclosure and sensitive information leakage on GitHub.
- Check your websites or business systems for command execution vulnerabilities.

Checking for trojans and backdoors

Check your real server for potential trojans, backdoors, and other hidden risks.

Other Suggestions

- To prevent attackers from scanning C range or other similar IP range, you are not recommended to use the same IP or an IP similar to the old IP as the new real server IP.
- You are recommended to prepare the standby linkage and IP in advance.
- You are recommended to set the scope of access sources to prevent malicious scanning.

Configuration Directions and Notes on CC Protection Policy

Last updated : 2021-02-02 19:37:35

Anti-DDoS Pro provides CC attack protection, the protection policy features protection level, cleansing threshold, precise protection, and CC frequency limit, etc. After connecting your business, you can configure CC attack protection policy as instructed in this document to use Anti-DDoS Pro to safeguard your business.

Configuration Directions

1. Log in to the Anti-DDoS console and click **Anti-DDoS Pro (New)** -> **Configurations** on the left sidebar.
2. Select an instance ID from the left list, e.g., `bgp-000000co` , and then open the **Domain name protection** tab.
3. **Set the CC protection cleansing threshold**: You can set a threshold value in the **CC Protection Policy** section.

> **Note :**
>
> - The Anti-DDoS Pro CC protection will be enabled once you set a cleansing threshold. A value that 1.5 times your normal business peak is recommended.
> - The Anti-DDoS Pro cleansing feature will remain disabled if no threshold value is set, and the protection level, precise protection, and CC frequency limit you configured in the console will not be in effect even when your business is under CC attacks. For more information, please see Protection Level and Cleansing Threshold.

4. **Set the CC protection level**:
   ① Click **Set** in the **CC Protection Policy** section to enter the configuration page.
   ② You can now create a new protection level or modify an old one.

> **Note :**
>
> If the Anti-DDoS Pro CC attack protection is enabled, the cleansing will be triggered when there is attack traffic, of which the detection strictness is the protection level. There are three available levels for you to select based on actual attacks: **Loose**, **Medium**, and **Strict**. For more information, please see Protection Level and Cleansing Threshold.

5. **Configure the precise protection policy**:
   When your business is under attack, we recommend deriving the attack characteristics from the specific attack request information obtained through packet capture, middleware access log, and other protection devices to configure your precise protection policy based on your business.
   You can enable the precise protection to configure protection policies combining multiple conditions of common HTTP fields, such as URI, UA, Cookie, Referer, and Accept to screen access requests. For the requests that match the conditions, you can configure CAPTCHA to verify requesters or a policy to automatically discard the packets.
   ① On the **Configurations** page, click **Set** in the **Precise Protection** section to view the precise protection rule list.
   ② Click **Create**, fill in the rule fields, and click **OK** to create a new precise protection rule. For more information, please see Precise Protection.

> ⚠ **Note :**
>
> - If a policy involves multiple HTTP fields, the policy can be matched if all conditions are met.
> - Anti-DDoS Pro supports configuring precise protection for HTTPS businesses.

Field description:

Field	Field Description
URI	The URI of an access request.
User-Agent	The identifier and other information of the client browser that initiates an access request.
Cookie	The cookie information in an access request.
Referer	The source website of an access request, from which the access request is redirected.
Accept	The data type to be received by the client that initiates the access request.
Match Condition	CAPTCHA and discard • Discard: discards packets without verifying the requester. • CAPTCHA: verifies the requester through algorithms.

6. **Set the CC frequency limit**:
   Anti-DDoS Pro supports configuring CC frequency policy for connected web businesses to restrict the access frequency of source IPs. You can customize a frequency policy to apply CAPTCHA and discard on source IPs if any IP accesses a certain page too frequently in a short time.
   ① On the **Configurations** page, click **Set** in the **CC Frequency Limit** section to view the frequency limit rule list.
   ② Click **Create**, fill in the rule fields, and click **OK** to create a new rule.

> ⚠ **Note :**
>
> - When configuring a CC frequency limit policy targeting the URI field, you need to configure a frequency limit on the directory `/` first and the match mode must be "equals to". Then you can configure the URI access frequency limit on other directories.
> - If a source IP accesses the `/` directory of the domain name for more than the set number of times in the set period, the set action (**CAPTCHA** or **Discard**) will be triggered.
> - If a frequency limit policy is configured for the `/` directory of a domain name, then the frequency of the domain name's other directories must be the same.
> - If the request URI contains any unfixed string, you can set the match mode to "include", so that URIs with the set prefix will be matched.

Field description:

Field	Field Description
Cookie	The cookie information in an access request.
User-Agent	The identifier and other information of the client browser that initiates an access request.
URI	The URI of an access request.
Frequency limit policy	CAPTCHA and discard • Discard: discards packets without verifying the requester. • CAPTCHA: verifies the requester through algorithms.
Check Condition	Set the access frequency based on your business, for which a value 2 to 3 times the normal number of access requests is recommended. For example, if your website is accessed averagely 20 times per minute, you can configure the value to 40 to 60 times per minute or adjust it according to the attack severity.

Field	Field Description
Punishment Time	The longest period is a whole day.