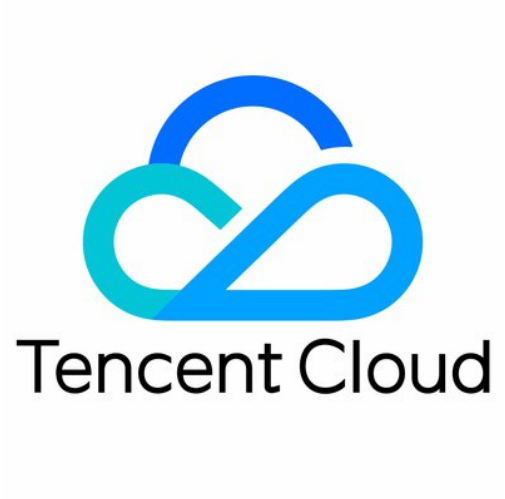
Tencent Cloud Firewall

Practical Tutorial

Product Documentation

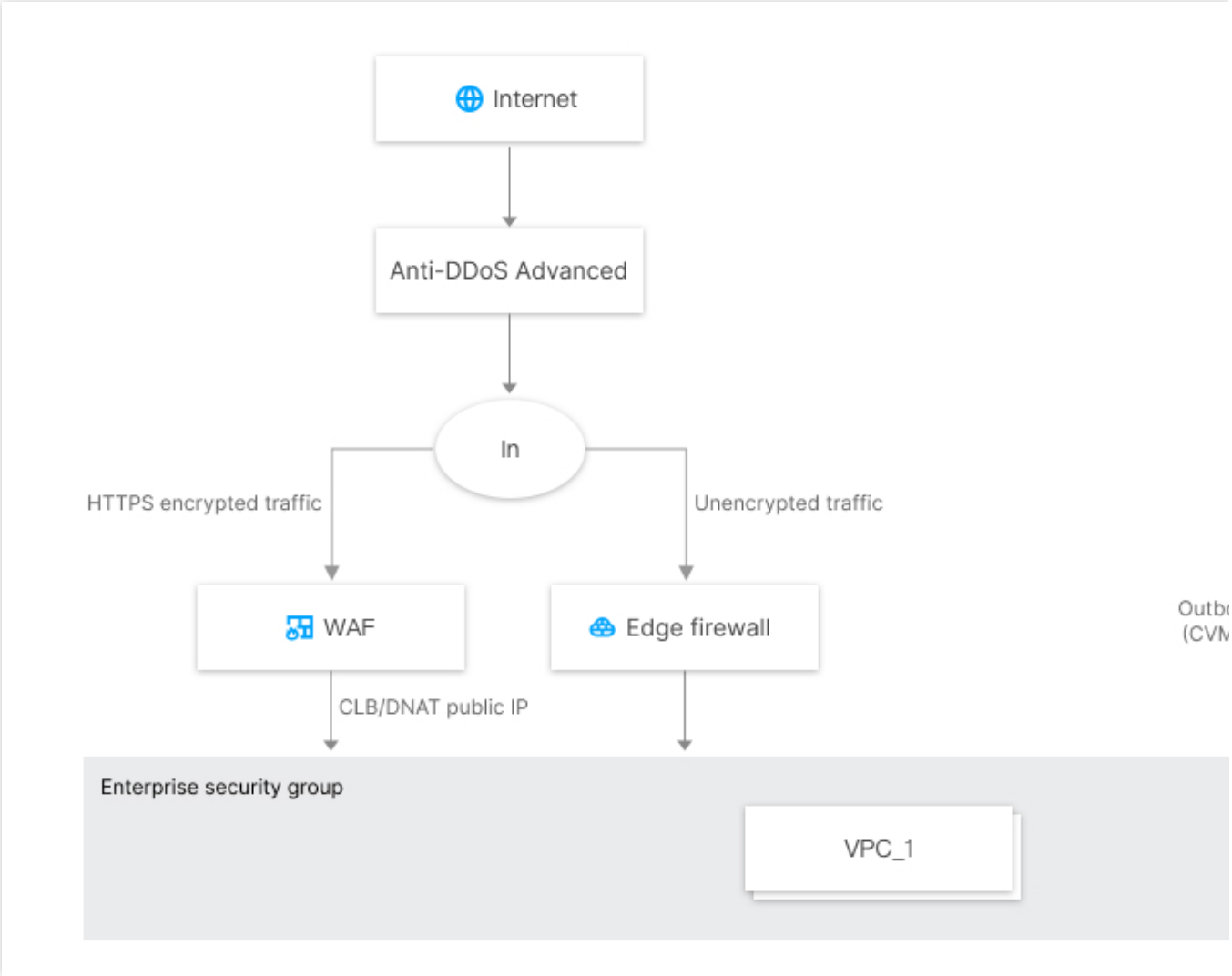


Contents

Practical Tutorial
Use Cloud Firewall with Other Products

Last updated：2024-01-24 16:23:02

Cloud Firewall can be used with Anti-DDoS Advanced, Web Application Firewall (WAF), and Security Group for protection:



For inbound traffic

Cloud Firewall and WAF work together as the overall perimeter protection layer for cloud security. WAF offers protection for encrypted HTTPS traffic, while Cloud Firewall integrates threat intelligence, intrusion prevention system (IPS), and virtual patching to protect unencrypted traffic.

SaaS WAF and the edge firewall work in parallel. After the traffic passes through the SaaS WAF, it does not goes through the edge firewall. However, the traffic can go back to the source DNAT IP of the NAT firewall.

CLB WAF is deployed after Cloud Firewall. Traffic goes through the edge firewall before CLB WAF.

If Tencent Cloud CDN is used, traffic that goes back to CLB or CVM still passes through the edge firewall.

For outbound traffic

The NAT firewall can help control outgoing requests based on CVM and control access based on domain name. With Tencent Threat Intelligence, it can automatically block any malicious IP addresses or domain names for outgoing requests.

If the NAT firewall is not enabled, access control for outbound traffic is only available with the edge firewall after the traffic goes through the NAT gateway. From the perspective of Cloud Firewall, the traffic comes from a public IP address.

Since Cloud Firewall and Security Group are standalone systems, traffic is allowed only when it is allowed by the policies of both systems.

Cloud Firewall Enterprise offers enterprise-grade security group features, which allow flexible access control and blocked request logging between VPCs, subnets in a VPC, and IDC direct connections.

Note

Cloud Firewall offers protection based on public IP addresses, so you can enable it according to your demands:

Only enable protection for certain assets to save costs. We recommend that you enable protection for all your cloud assets to prevent intrusion from non-essential assets if your budget permits.

If only the web services of your cloud assets are exposed and they are protected by WAF, you can just enable outgoing request protection. This way, Cloud Firewall is used with WAF for overall network protection to secure both inbound and outbound connections at a lower cost.

Cloud Firewall has been used in gaming, e-commerce, and many other large-scale scenarios that require a bandwidth of dozens of Gbps. If your business traffic demands exceed 1 Gbps, contact our business manager for a custom business solution.

DNS Firewall Practical Tutorial

Last updated：2024-07-02 15:22:30

When the NAT firewall DNS toggle is enabled, the DNS address of the connected VPC will be changed to direct the DNS traffic to the NAT firewall.

Note

Tencent Cloud's default DNS addresses are 183.60.83.19 and 183.60.82.98.

To configure DNS protection:

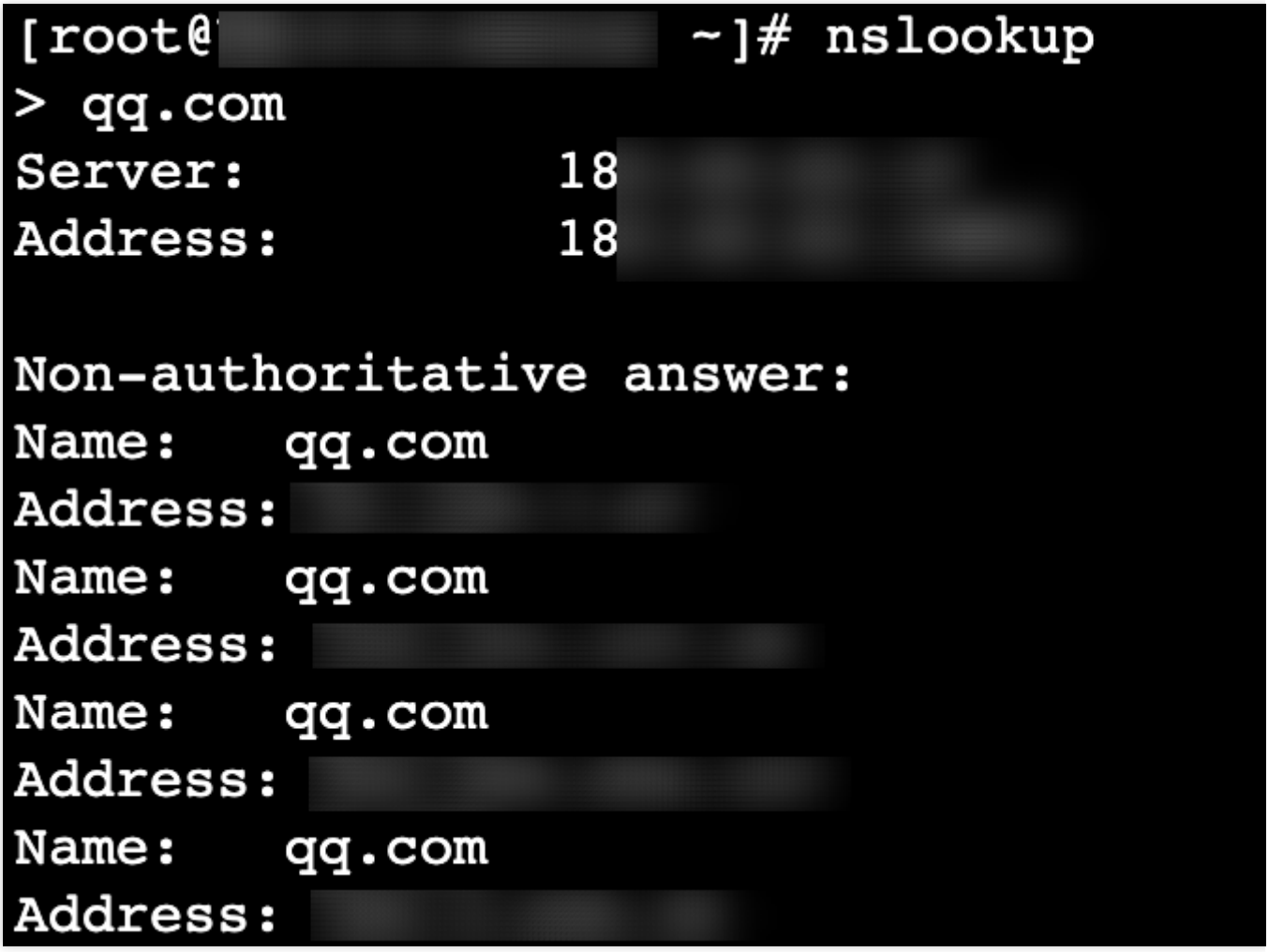
Create a NAT firewall for the region and connect to a VPC.

Enable the NAT firewall to monitor traffic. Any routing changes may lead to network jitter of 1 to 2 seconds.

Enable the DNS toggle to verify the DNS address.

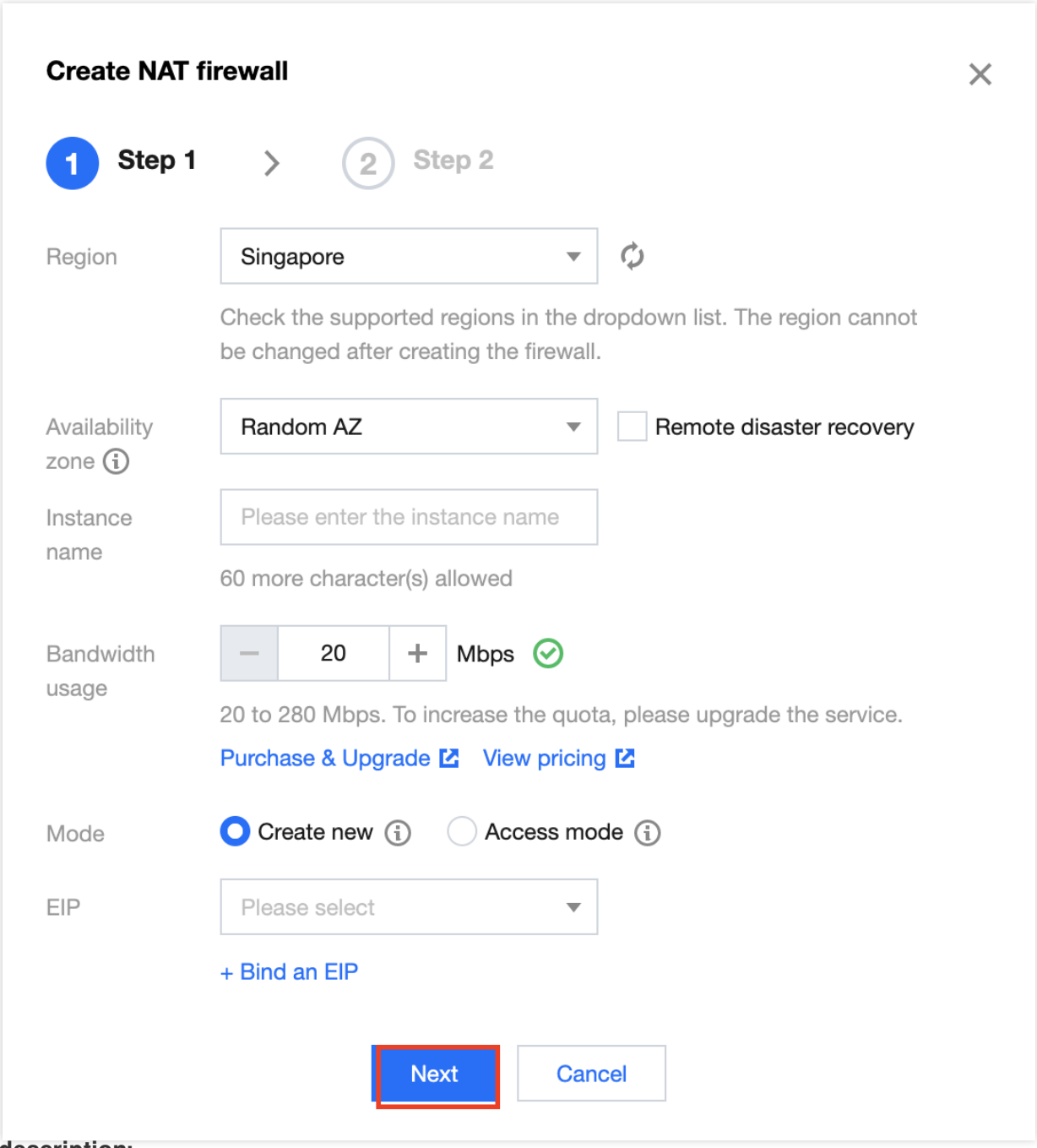
Use NAT firewall's access control feature to restrict DNS resolution (verification).

The CVM public network resource is the default DNS server, as shown in the image below:



Step 1: create a NAT firewall

1. Log in to the Cloud Firewall console, and then click **Firewall Toggles** -> **NAT firewall** -> **Network topology** in the left navigation pane.
2. On the Network Topology page, click **Create instance**, and then select a region.
3. On the Create NAT firewall window that appears, configure the parameters and click **Next**.



Field description:

Region: Select a region for the instance to be created (all regions in China are available). The region cannot be modified after the instance is created.

Note

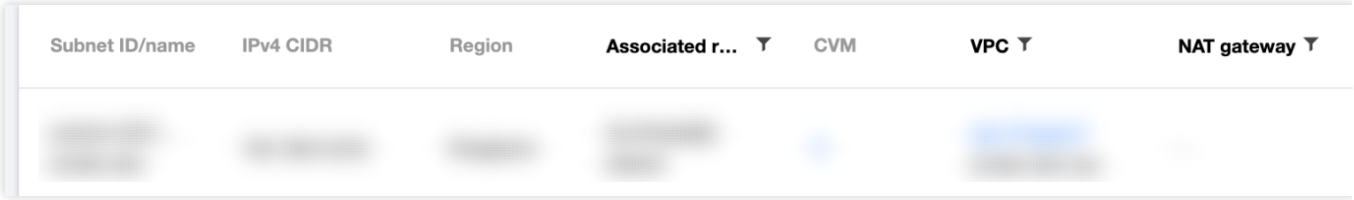
You can select one of the regions in China (including Hong Kong) where you have a VPC. Multiple firewall instances can be created for a single region, but the total bandwidth cannot exceed the quota.

Zone: Select an availability zone according to your needs.
Instance name: Enter the name of the instance.
Bandwidth quota: Select a bandwidth quota according to your needs (at least 20 Mbps). For more bandwidth, upgrade your service.
Note
It must match the bandwidth of the edge firewall. For multiple NAT firewalls, their bandwidth sum must be less than or equal to that of the edge firewall.
Mode: Supports the Create new mode and Use existing mode.
Create new: If no NAT gateway is available in the current region, you can create a new NAT gateway and use it as the NAT firewall for Internet access.
Use existing: If a NAT gateway is available in the current region, or you do not want to change your outbound IP address, you can use the Use existing mode to smoothly add a NAT firewall between the NAT gateway and CVM instance.
EIP: If you select to create a new EIP, the system automatically requests an EIP for you. Or you can select and bind one of the idle EIPs.
4. Select a VPC to connect to, and then click **Create**. You can view the new instance in the firewall instance list after a few minutes.

Step 2: enable the firewall

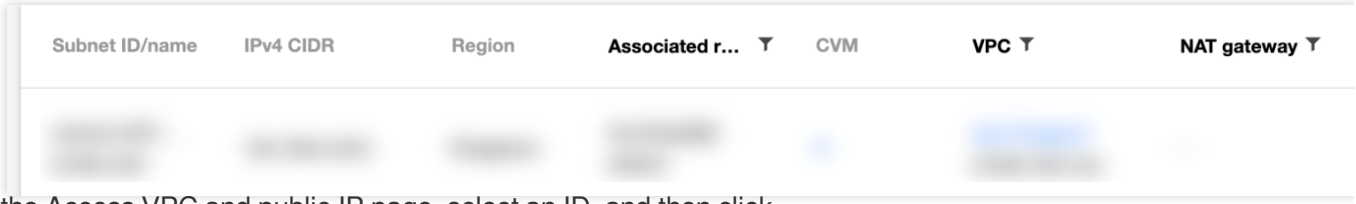
On the NAT firewall page, click **Firewall toggle**. Then, select the subnet for your database based on your actual demands, and click

to enable the firewall.



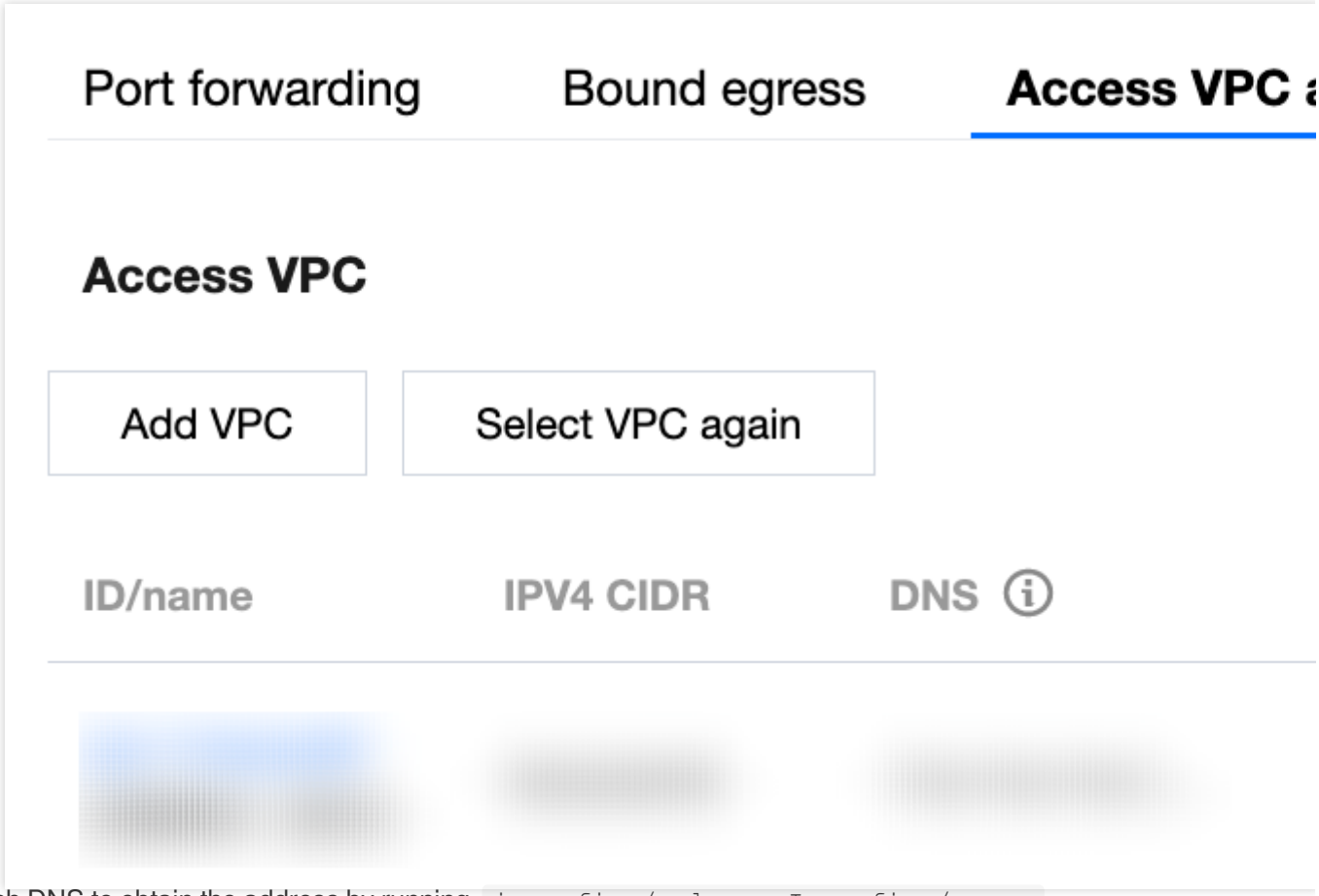
Step 3: enable and verify DNS

1. On the NAT firewall page, click **Firewall instances**. Then, select the firewall instance that you just created in Step 1, and click **Instance configuration**.

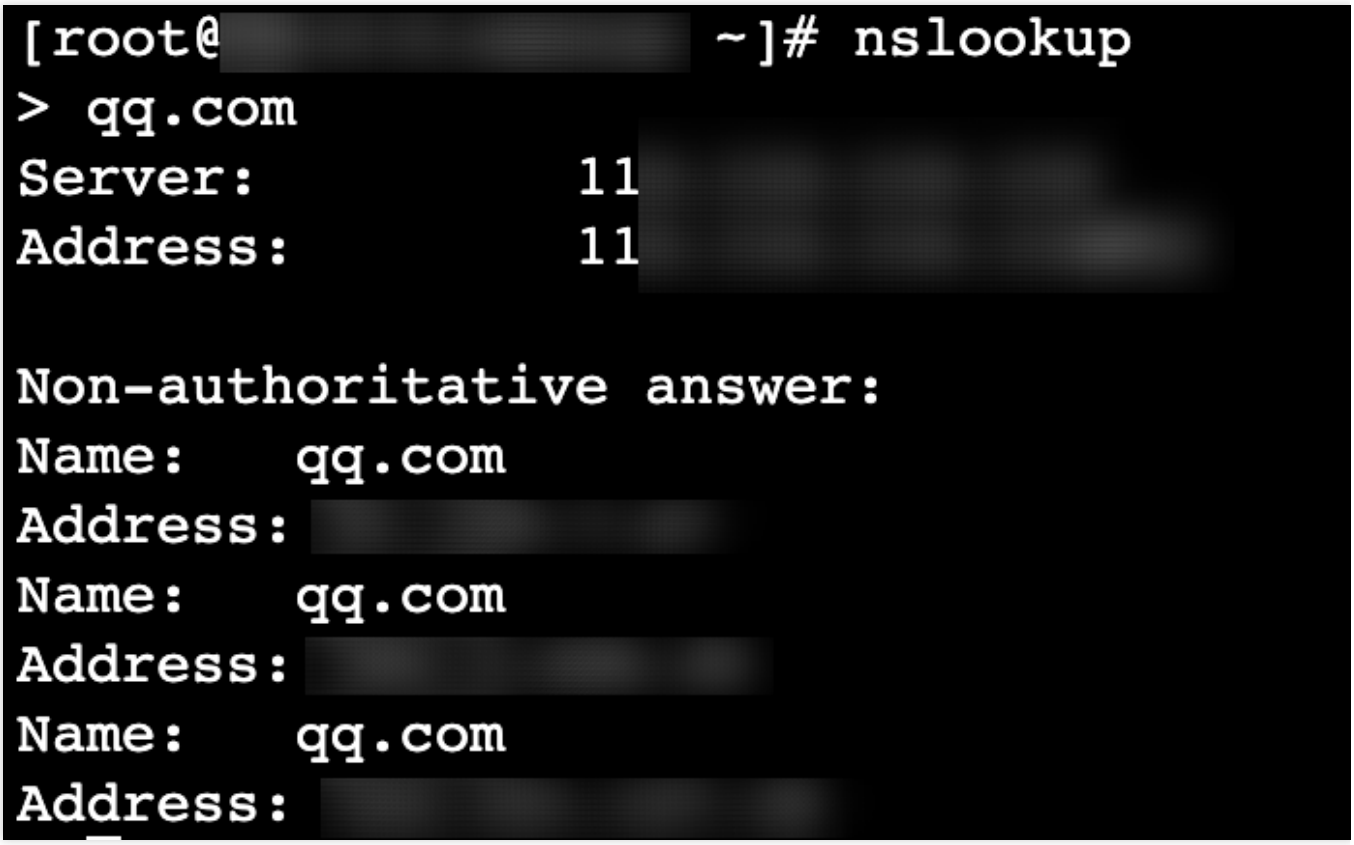


2. On the Access VPC and public IP page, select an ID, and then click

to enable DNS traffic.

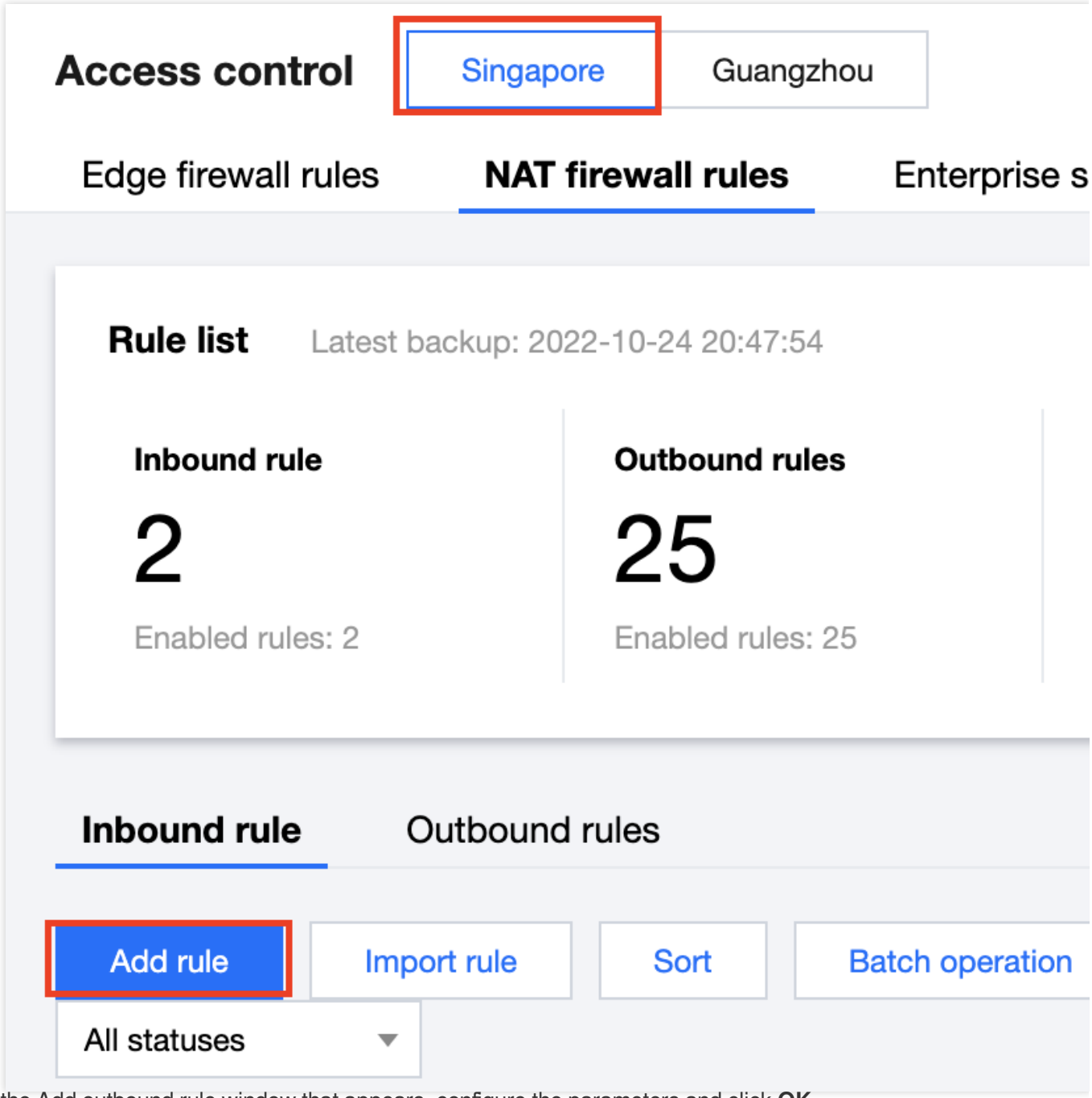


3. Flush DNS to obtain the address by running `ipconfig /release Ipconfig /renew` .

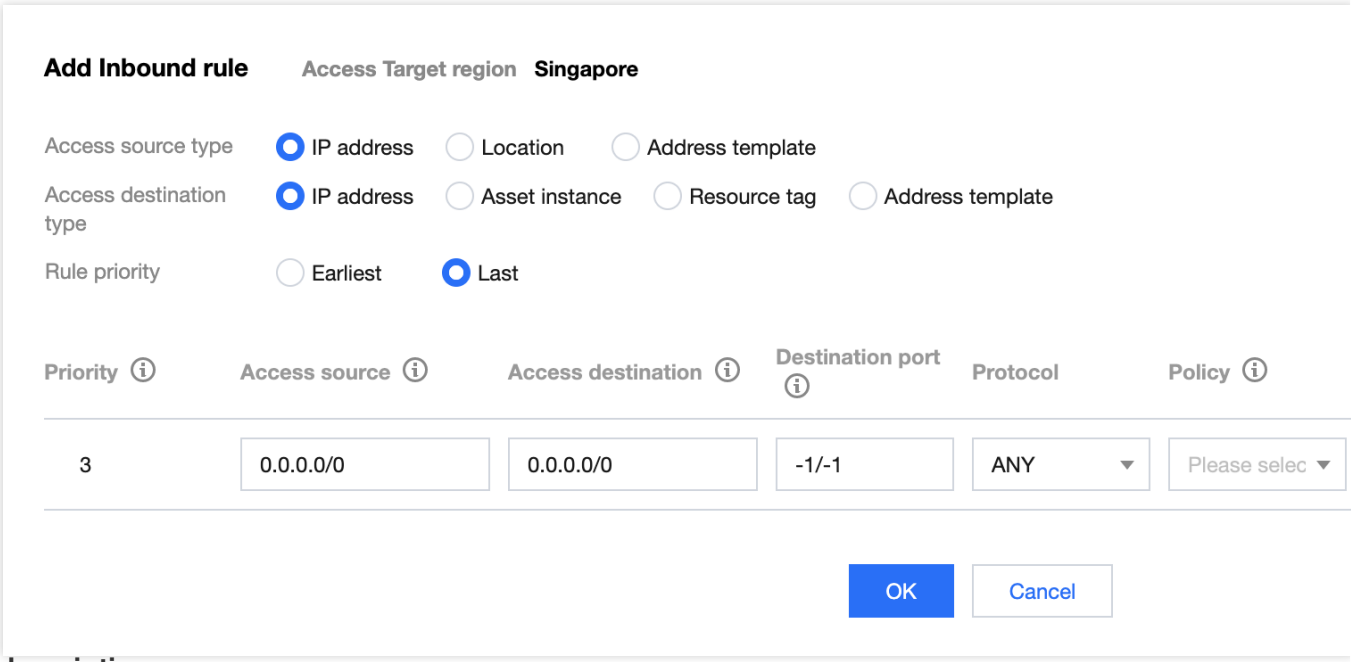


Step 4: restrict DNS resolution

1. On the NAT firewall rules page, select a region, and then click **Outbound rules** -> **Add rule**.



2. On the Add outbound rule window that appears, configure the parameters and click **OK**.



Field description:

Priority: Indicates the priority of the access control rule. The priorities of outbound and inbound rules are independent of each other. The rule with the highest priority is evaluated first. If a given rule is matched, rules with lower priorities will not be evaluated. When you modify the priority of a given rule, the priorities of the original rule with that priority and all the subsequent rules will increase by 1. When you delete a given rule, the priorities of all the following rules will decrease by 1.

Access source: For outbound rules, the access source is a private network asset in the current region, and can be an IP or CIDR.

Access destination: For outbound rules, the access destination is a public IP address or domain name, and can be an IP, CIDR, domain name, or geographic location.

Destination port:

TCP/UDP/ANY rules support a single port number, a port range with '/', and multiple ports separated by commas, such as "80", "80/80", "-1/-1", "1/65535", and "80,443,3380/3389".

HTTP/HTTPS/SMTP/SMTPS/FTP rules only support a single port number. SMTP and FTP rules cannot use the same port.

No port is required for ICMP rules.

Protocol: ANY, TCP, UDP, and ICMP are available for outbound rules.

Policy description:

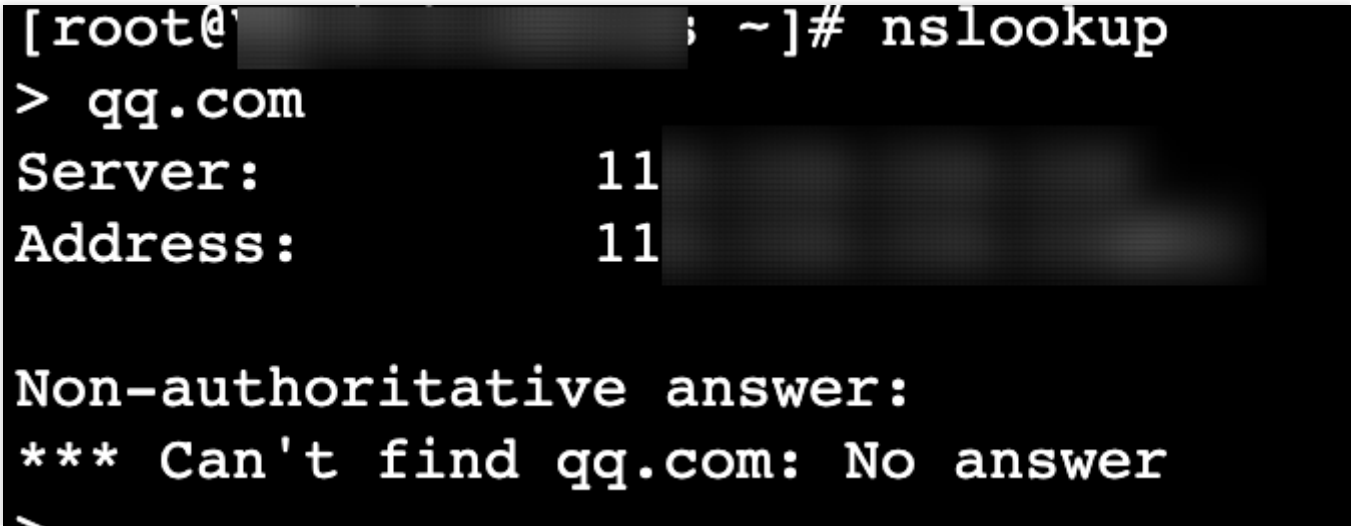
Allow: Allow the matched traffic and record the hit count and traffic logs, but not access control logs.

Observe: Allow the matched traffic and record the hit count, access control logs, and traffic logs.

Block: Block the matched traffic and record the hit count and access control logs, but not traffic logs.

Description: Rule description with up to 50 characters.

3. After configuration, verify if the DNS server can be connected.



Practical Tutorial for Protecting Against Mining Attacks

Last updated：2024-07-02 15:18:44

This topic describes how to use Cloud Firewall to defend against common cryptomining worms and covers attack prevention, detection, and recovery in an actual cloud environment.

Important notes

Cloud Firewall offers an intrusion defense module to protect against cryptomining worms. The intrusion defense feature is available in Cloud Firewall IPS, Premium, Enterprise, and Ultimate to help users defend against mining attacks. Generally, attackers compromise a server in your private network with Trojans or botnets and exploit your resources to send requests to the Internet. To accurately locate the risky server in the private network, you need the NAT firewall feature. Hence, **we recommend that you purchase Premium, Enterprise, or Ultimate Edition**.

How do mining worms spread?

In most cases, attackers exploit network vulnerabilities, including general and zero-day/n-day vulnerabilities, to spread mining worms.

General vulnerabilities

Mining worms often exploit general vulnerabilities in applications or websites, such as code defects, configuration errors, and weak passwords, to continuously scan and attack servers on the Internet. Attacks that exploit general vulnerabilities include SSH/RDP brute-force attacks, command injection, credential stuffing, Webshell communication, and outgoing access to malicious IPs. Typical intrusion methods that exploit general vulnerabilities are listed in the following table:

Intrusion type	Malware family	Typical intrusion method
Brute-force attacks	MyKingsMrbMinerLoggerMinerGuardMinerDDG RDPMiner	MongoDB brute-force attack
		SSH brute-force attack
		Tomcat brute-force attack
		MySQL brute-force attack
		PostgreSQL brute-force

		attack
		SQL Server brute-force attack
		FTP brute-force attack
		RDP brute-force attack
		SMB brute-force attack
		Telnet brute-force attack

Zero-day/N-day vulnerabilities

When a zero-day or n-day vulnerability is exploited, it can easily lead to large-scale infection before it is fixed and can bring huge damage to your services.
Common zero-day and n-day vulnerabilities include WebLogic vulnerability, deserialization vulnerability, EternalBlue, and Tomcat remote code execution vulnerability.
Typical intrusion methods that exploit zero-day/n-day vulnerabilities are listed in the following table:

Intrusion type	Malware family	Typical intrusion method
System vulnerabilities	WannaMine	MS17-010 EternalBlue (CVE-2017-0143)
Application vulnerabilities	8220MinerBashMinerkworkersMinerTraceMinerCarbonMiner	Confluence remote code execution (CVE-2021-26084)
		Confluence remote command execution (CVE-2019-3396)
		Gitlab exiftool remote command execution (CVE-2021-22205)
		Apache NIFI remote code execution (CVE-2020-9491)
		Yonyou NC Cloud remote code execution (CNVD-2021-30167)

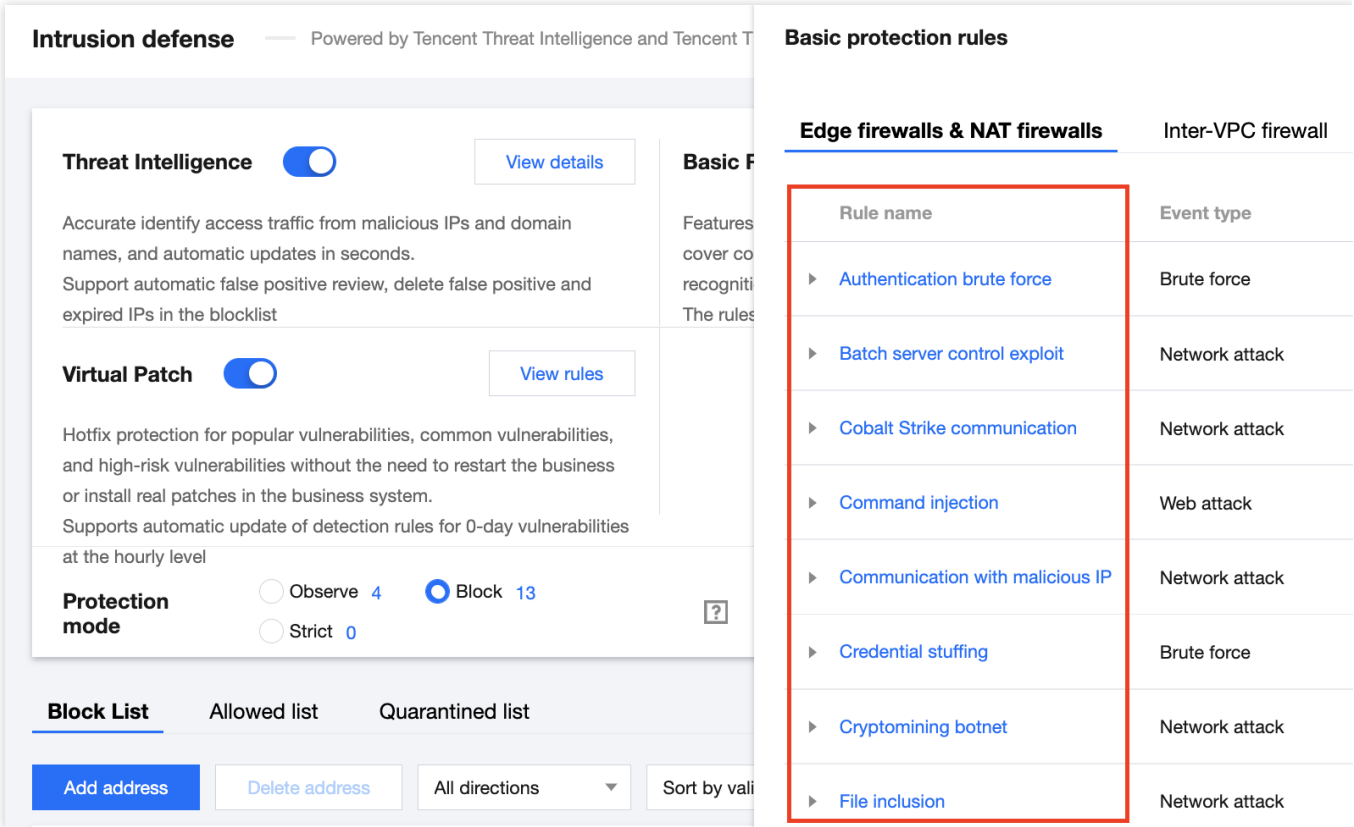
		Docker Remote API unauthorized access (CVE-2019-17671)
		YAPI remote code execution
Component vulnerabilities	JumaMinerH2Minertellyouthepass	Log4j2 remote code execution (CVE-2021-44228)
		Jenkins unauthenticated command execution (CVE-2017-1000353)
		WebLogic remote execution (CVE-2021-2109)
		Hadoop Yarn unauthorized access

How does Cloud Firewall defend against mining worms?

Cloud Firewall detects incoming and outgoing traffic in real time. Detected malicious traffic is automatically blocked to protect against mining worms. It works in the following two ways:

Defense against general vulnerabilities

General vulnerabilities are often exploited to launch RDP/SSH brute-force attacks and system command injection attacks. To protect against such attacks, Cloud Firewall offers a basic protection module for intrusion defense. The basic protection module integrates the intrusion detection rules based on Tencent Cloud's extensive anti-attack experience, covering common network attacks and malicious code, as shown in the image below:



To **enable the basic protection feature to defend against mining worms that exploit general vulnerabilities**:

1. Log in to the Cloud Firewall console, and then click **Intrusion Protection System** in the left navigation pane.
2. On the Intrusion Defense page, click

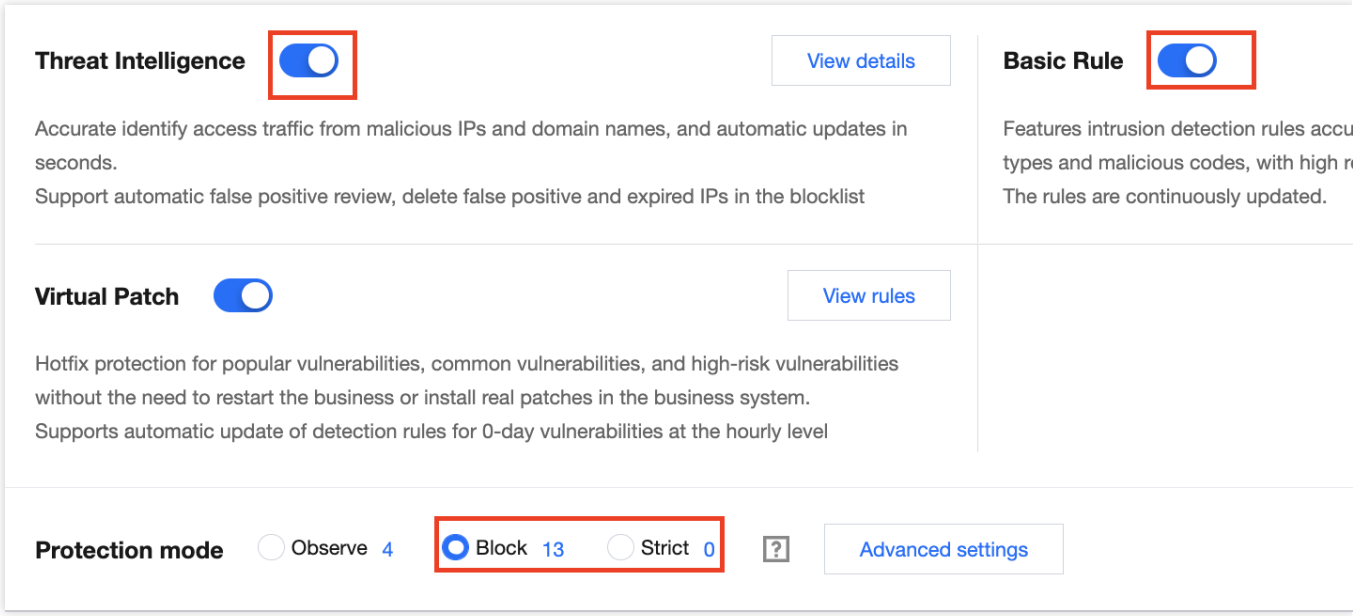
to enable threat intelligence and basic protection, and then select "Block" or "Strict" for the protection mode.

Note

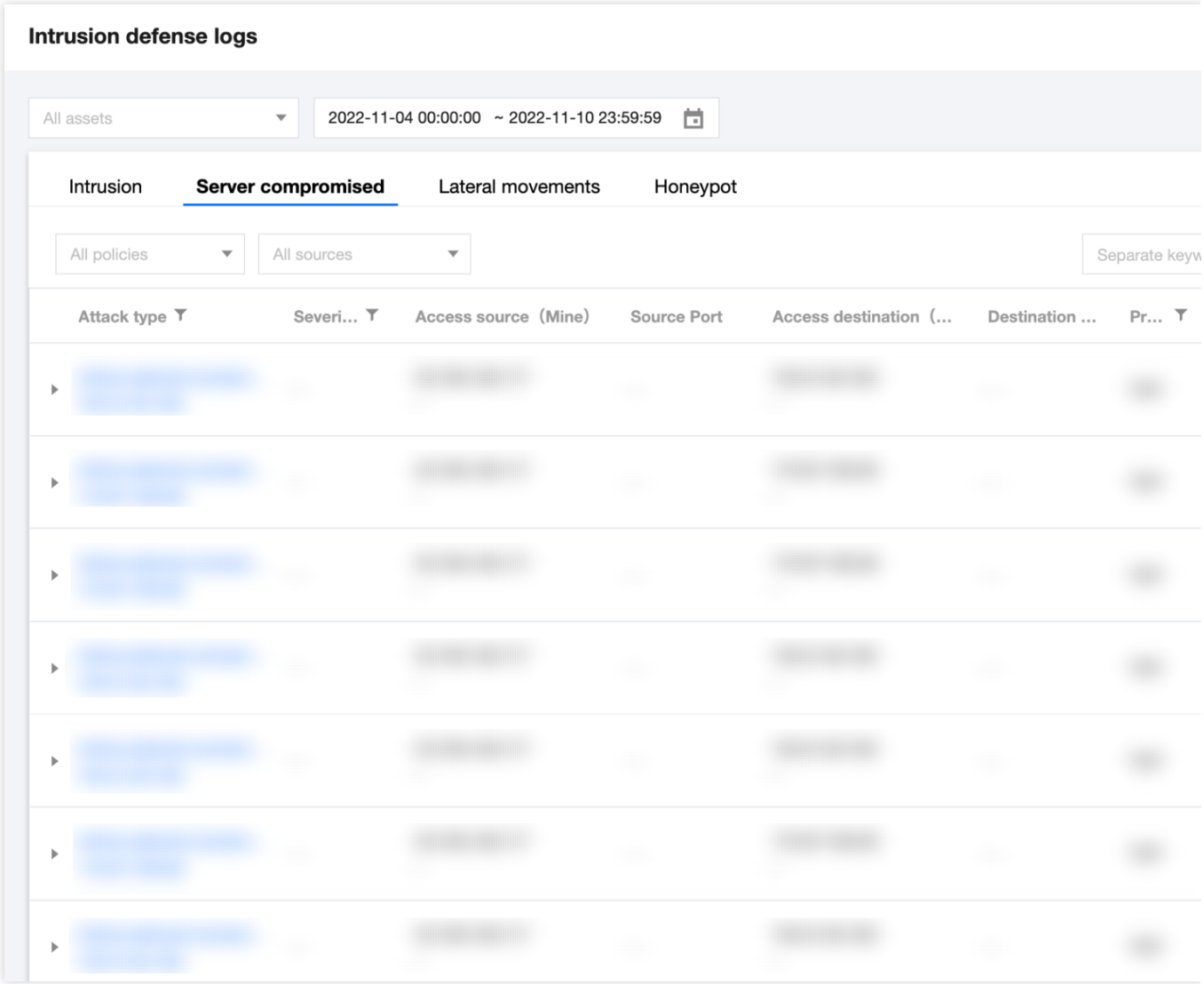
In observe mode, any mining worms detected are recorded in Alert Management but are not automatically blocked.

In block mode, the threat intelligence module can automatically block malicious outgoing requests, and the basic protection module can automatically block traffic that hit the high-confidence preset rules.

In strict mode, all detected security events or suspicious IPs are blocked or added to the blocklist by the threat intelligence and basic protection modules.

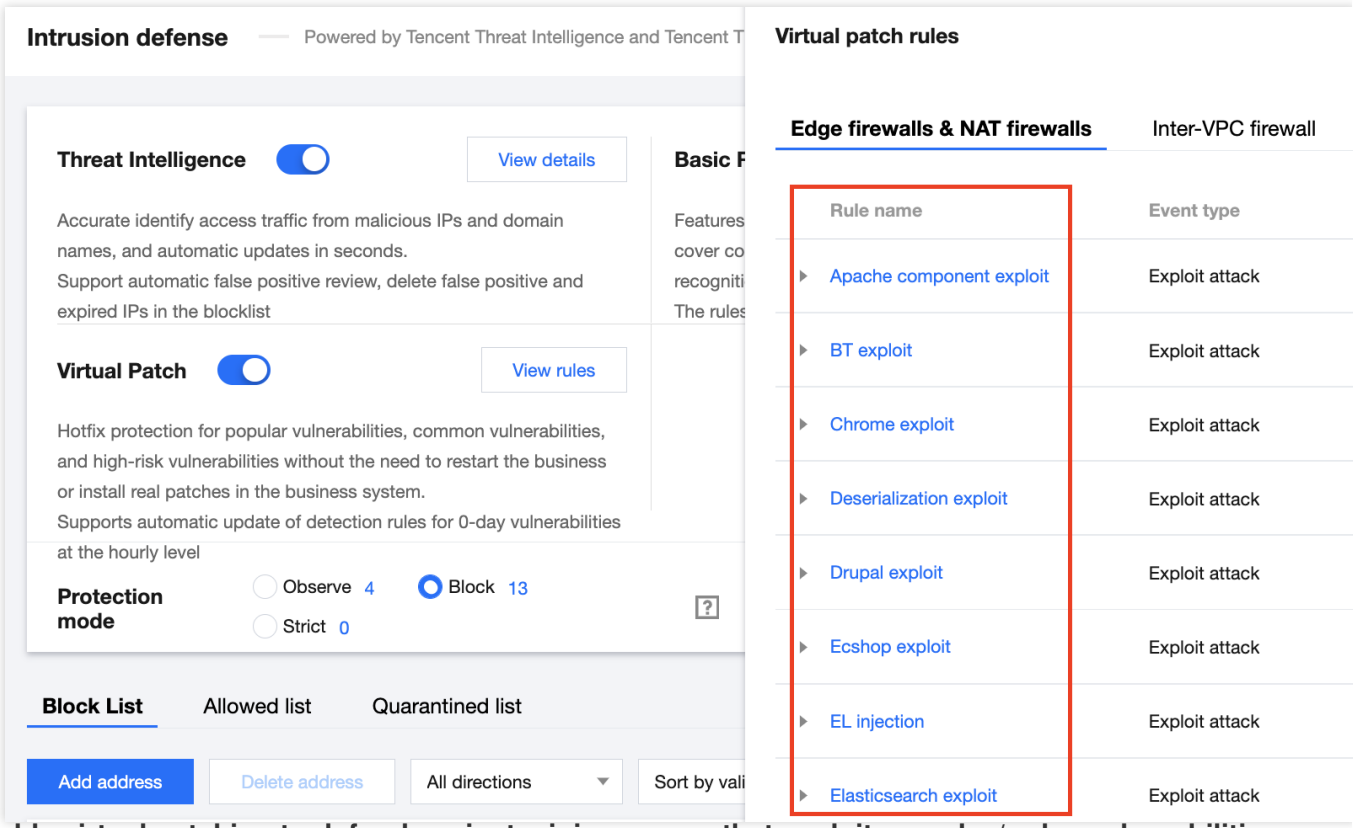


3. On the Intrusion Defense Log page, you can view the details of intrusion logs.



Defense against zero-day/n-day vulnerabilities

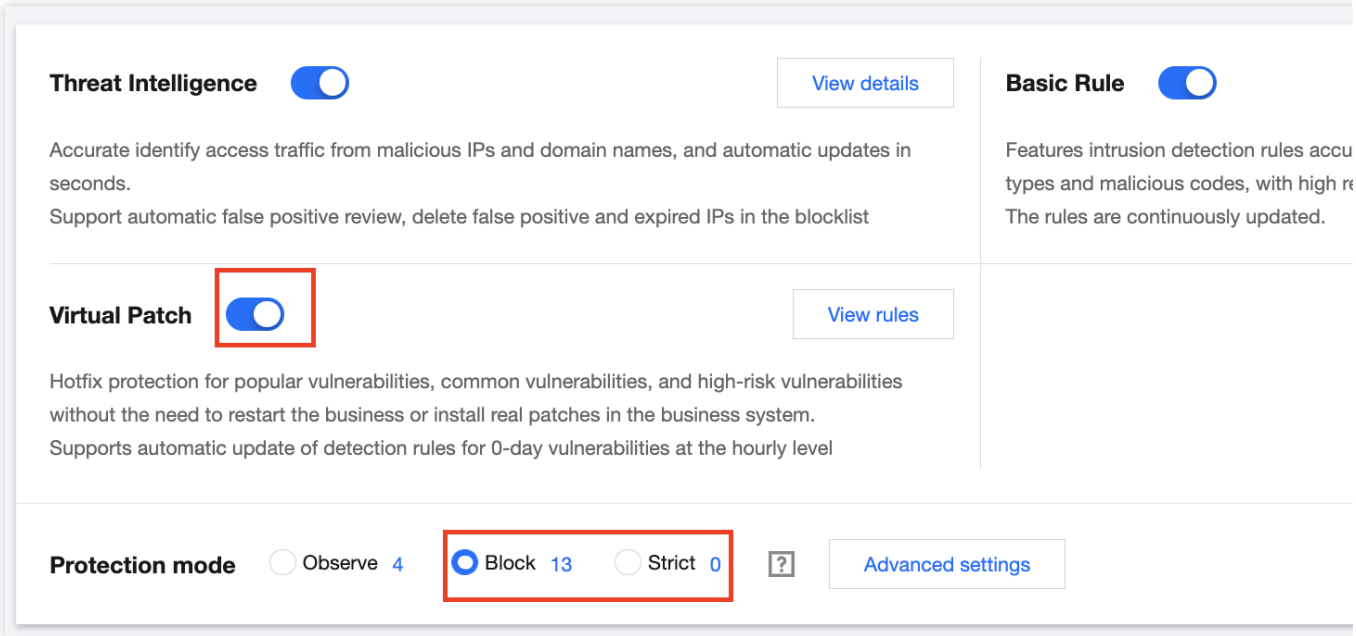
Some common zero-day/n-day vulnerabilities are likely to be exploited by mining worms if they are not fixed in a timely manner. By obtaining vulnerability intelligence from the Tencent Cloud Threat Intelligence X in real time, Cloud Firewall can promptly detect zero-day/n-day vulnerabilities, obtain the proofs of concept (POCs), and generate a rule base for virtual patching. This way, Cloud Firewall can take actions before hackers do, as shown in the image below:



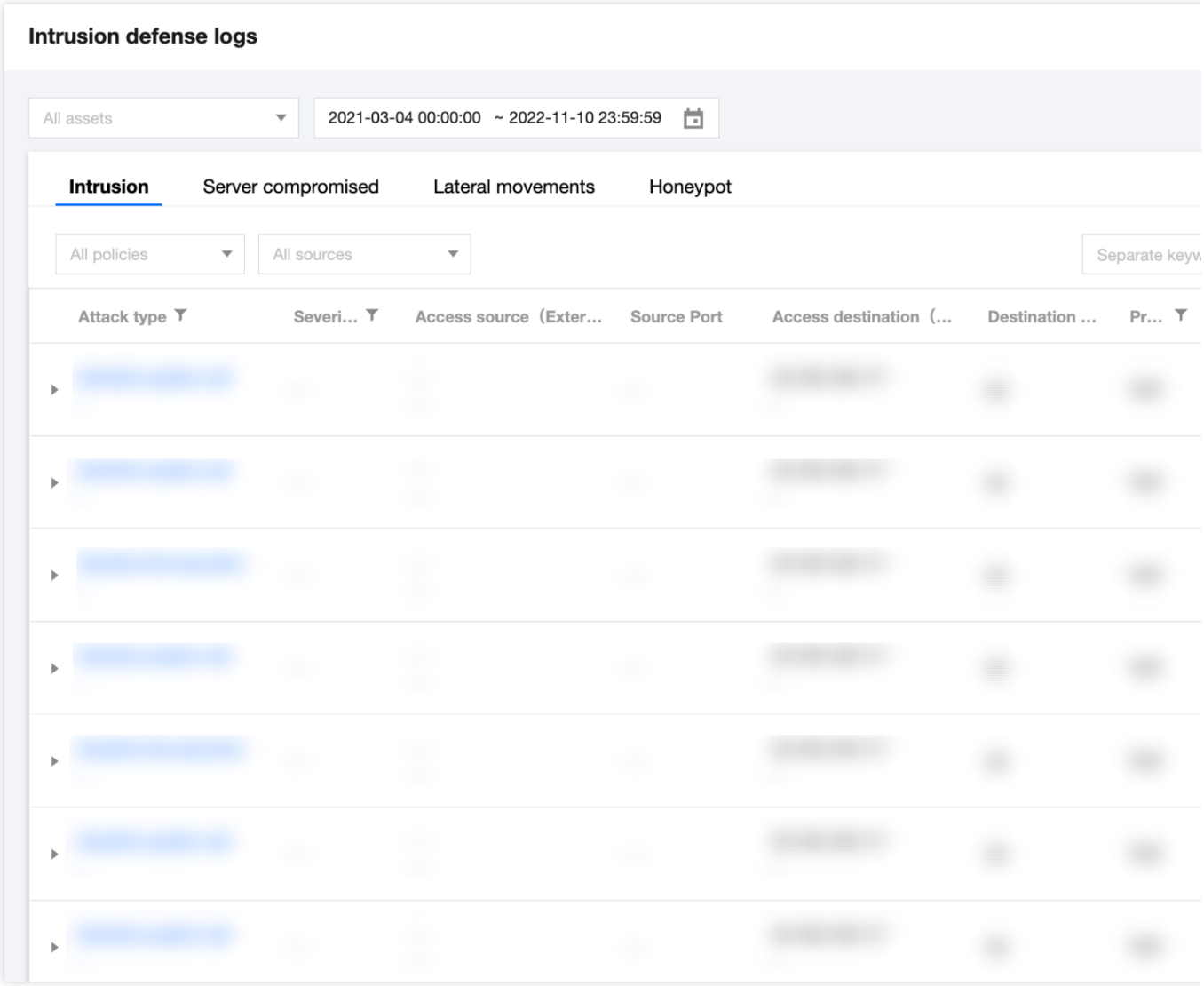
To **enable virtual patching to defend against mining worms that exploit zero-day/n-day vulnerabilities**:

1. Log in to the Cloud Firewall console, and then click **Intrusion Protection System** in the left navigation pane.
2. On the Intrusion Defense page, click

to enable virtual patching, and then select the "Block" or "Strict" for the protection mode.

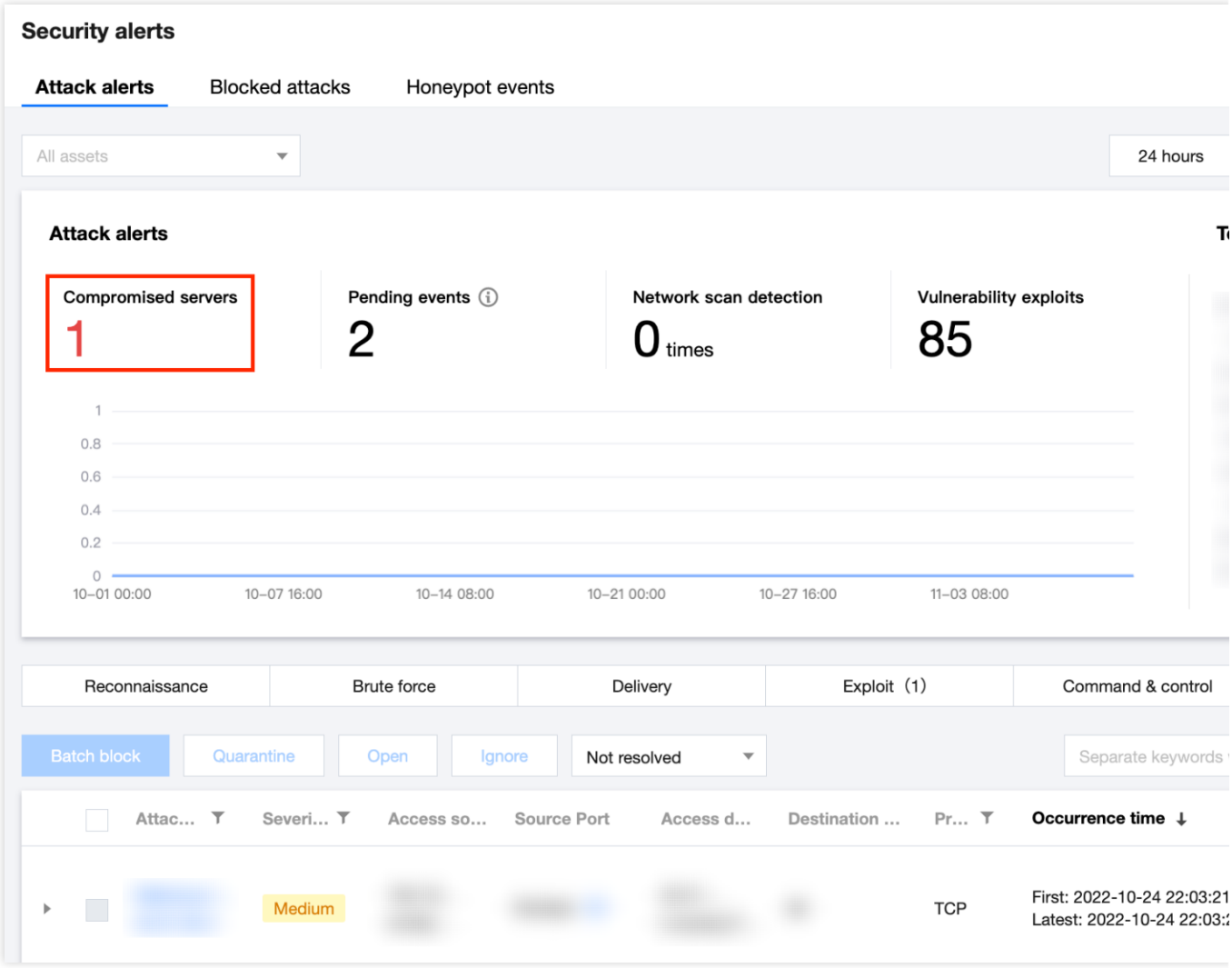


3. On the Intrusion Defense Log page, you can view the details of intrusion logs.



How does Cloud Firewall detect mining worms?

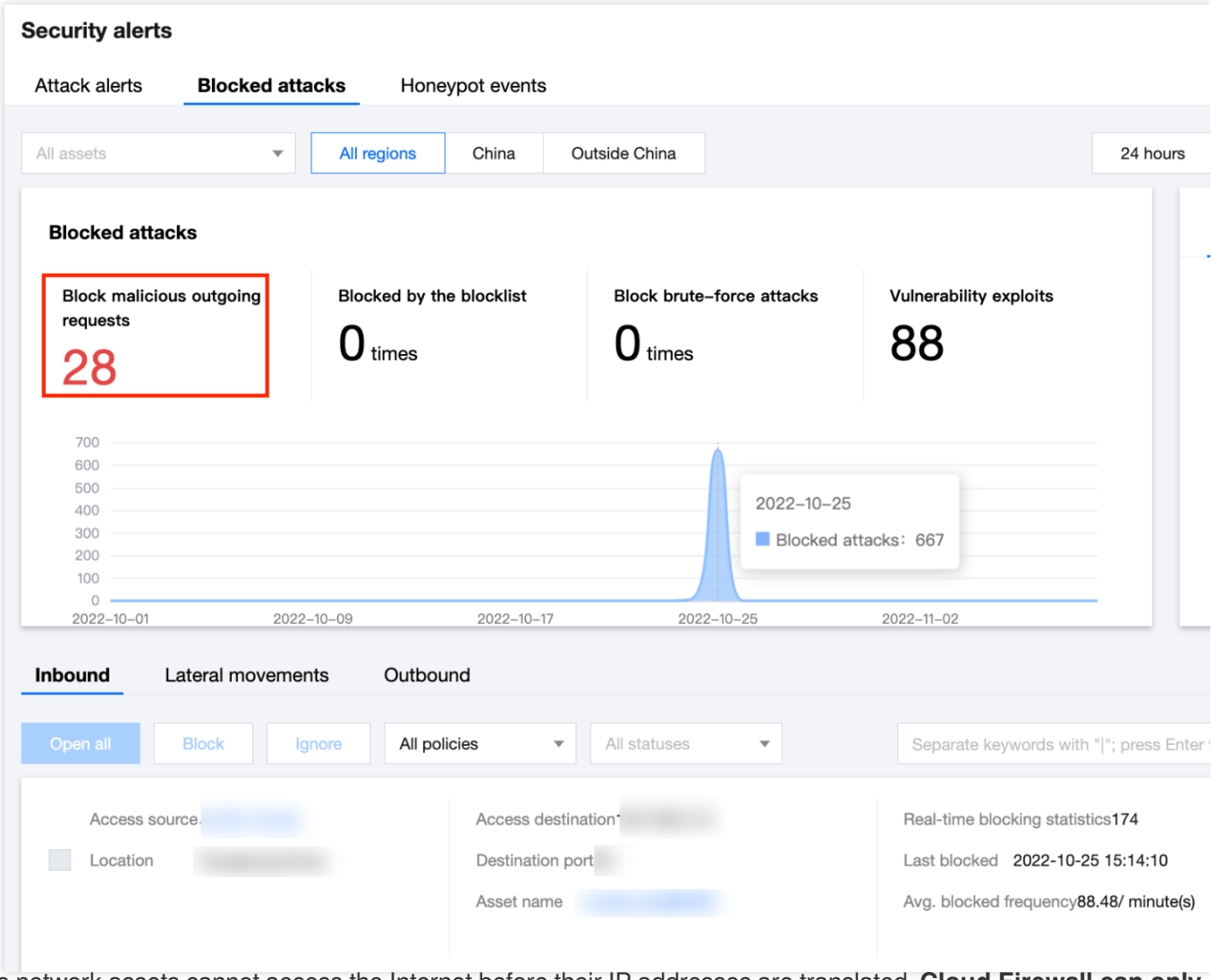
Tencent Cloud's threat intelligence module detects malicious outgoing traffic in real time. Thanks to the built-in Tencent Security threat intelligence and detection, the module can precisely identify any traffic from malicious IPs and domain names, and automatically update in seconds. Any traffic from or to the assets in the public and private network is monitored by Cloud Firewall. If mining worm attacks are detected, the servers concerned are labeled as compromised, and displayed in the Alert Management.



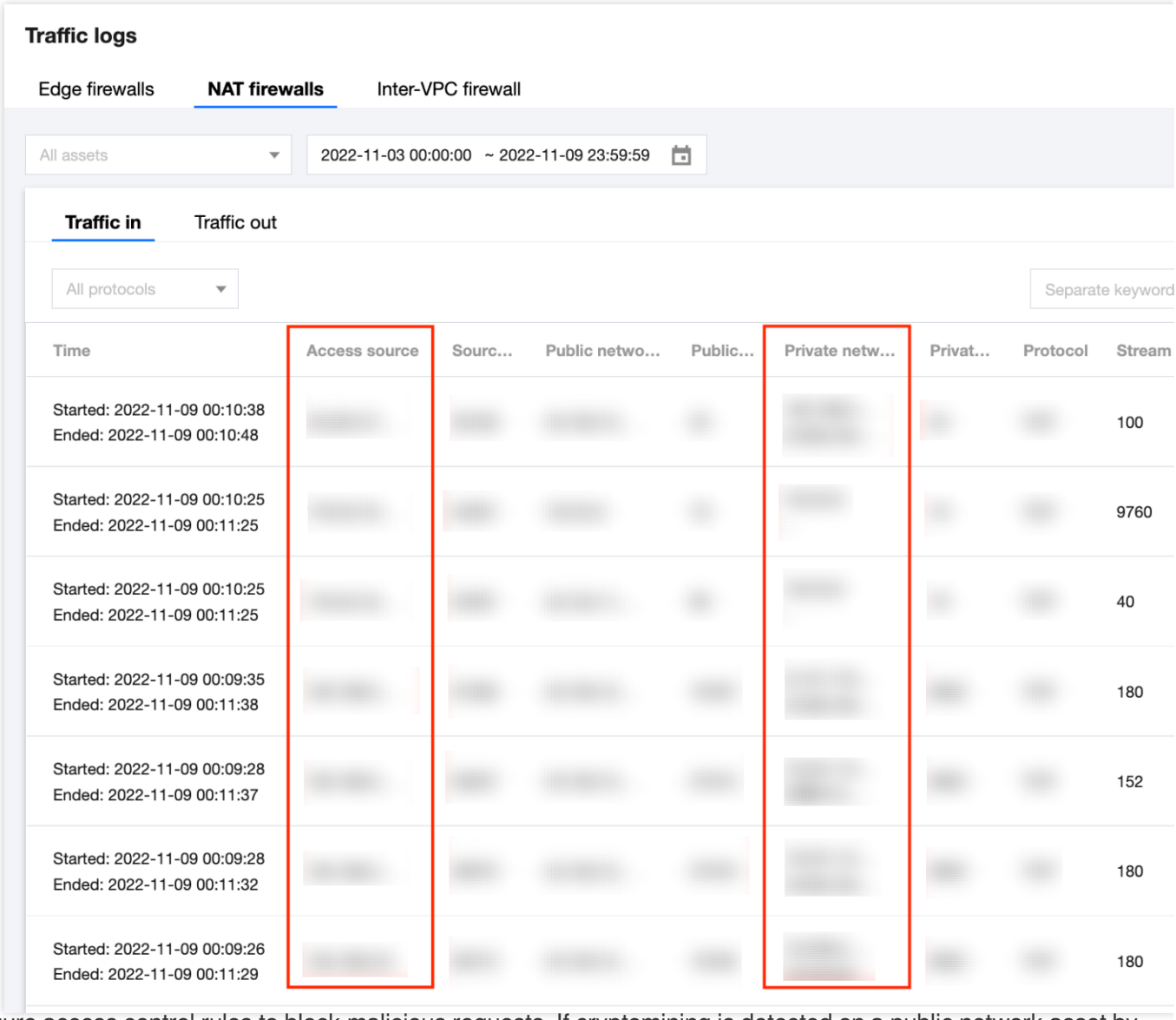
How to use Cloud Firewall to quickly recover from cryptomining attacks

If a server is compromised by mining worms, Cloud Firewall can help you quickly locate the infected server, and then remove the mining worms using Cloud Workload Protection Platform. This can prevent hackers from uploading malicious files and avoid information leakage.

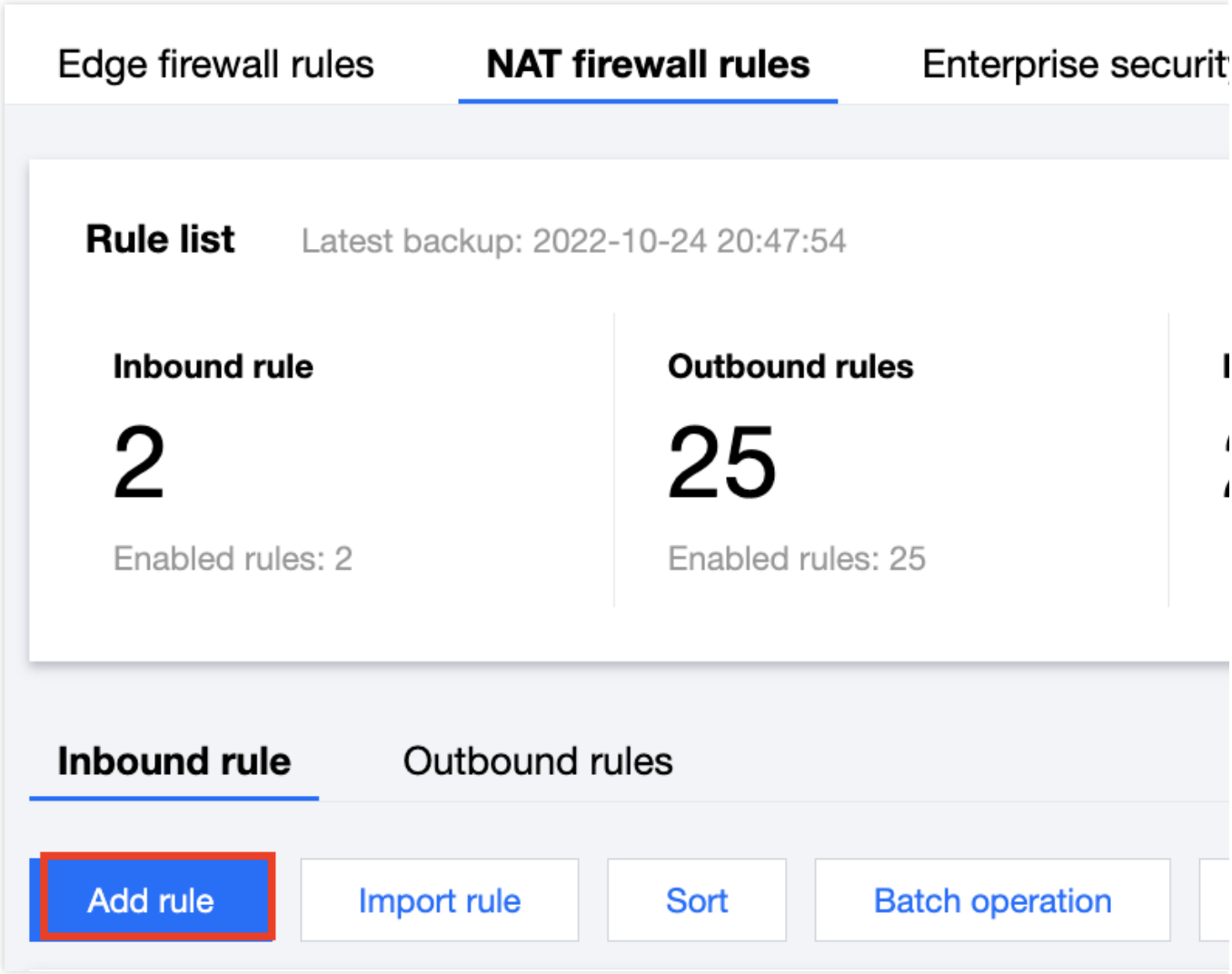
Threats in public network assets can be detected by the CFW edge firewall. Threat Intelligence can immediately locate the infected public asset to block cryptomining requests.



Private network assets cannot access the Internet before their IP addresses are translated. **Cloud Firewall can only locate the NAT public IP addresses**. Hence, if a given private network asset is infected by mining worms, you need to **enable NAT firewall for the private network asset** to see that a request is sent from the NAT public IP to the IP or domain name of a mining pool in Alert Management. With the IP or domain name of the mining pool, you can precisely locate the source server by obtaining the compromised private network asset in the traffic logs of the NAT firewall.



Configure access control rules to block malicious requests. If cryptomining is detected on a public network asset by intrusion defense, you can configure blocking rules in Access control -> **Edge firewall rules** -> **Outbound rules**. If cryptomining is detected on a private network asset, you can configure blocking rules in Access control -> **NAT firewall rules** -> **Outbound rules**.

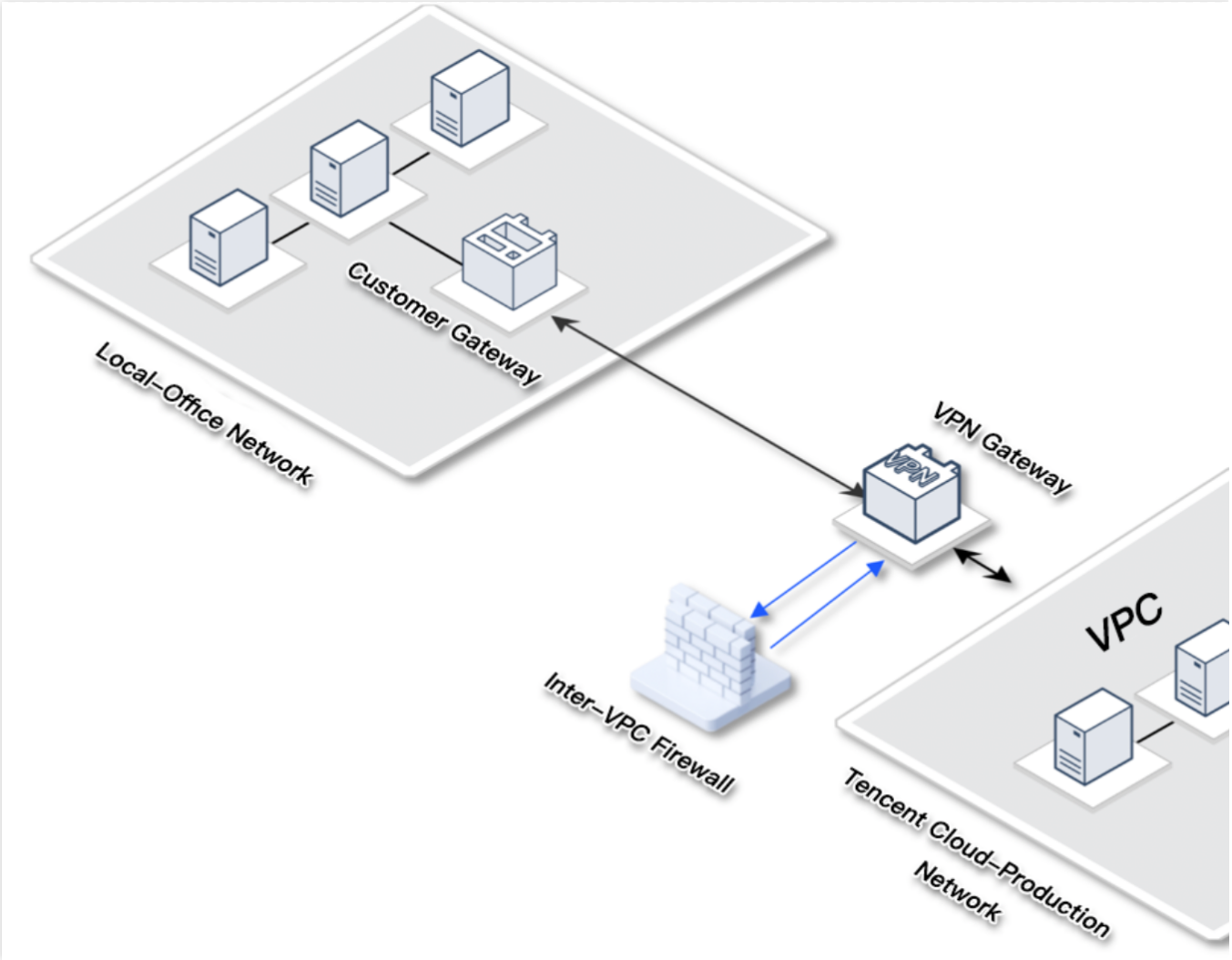


Inter-VPC Firewall Practice Tutorial

Last updated：2024-09-06 17:57:45

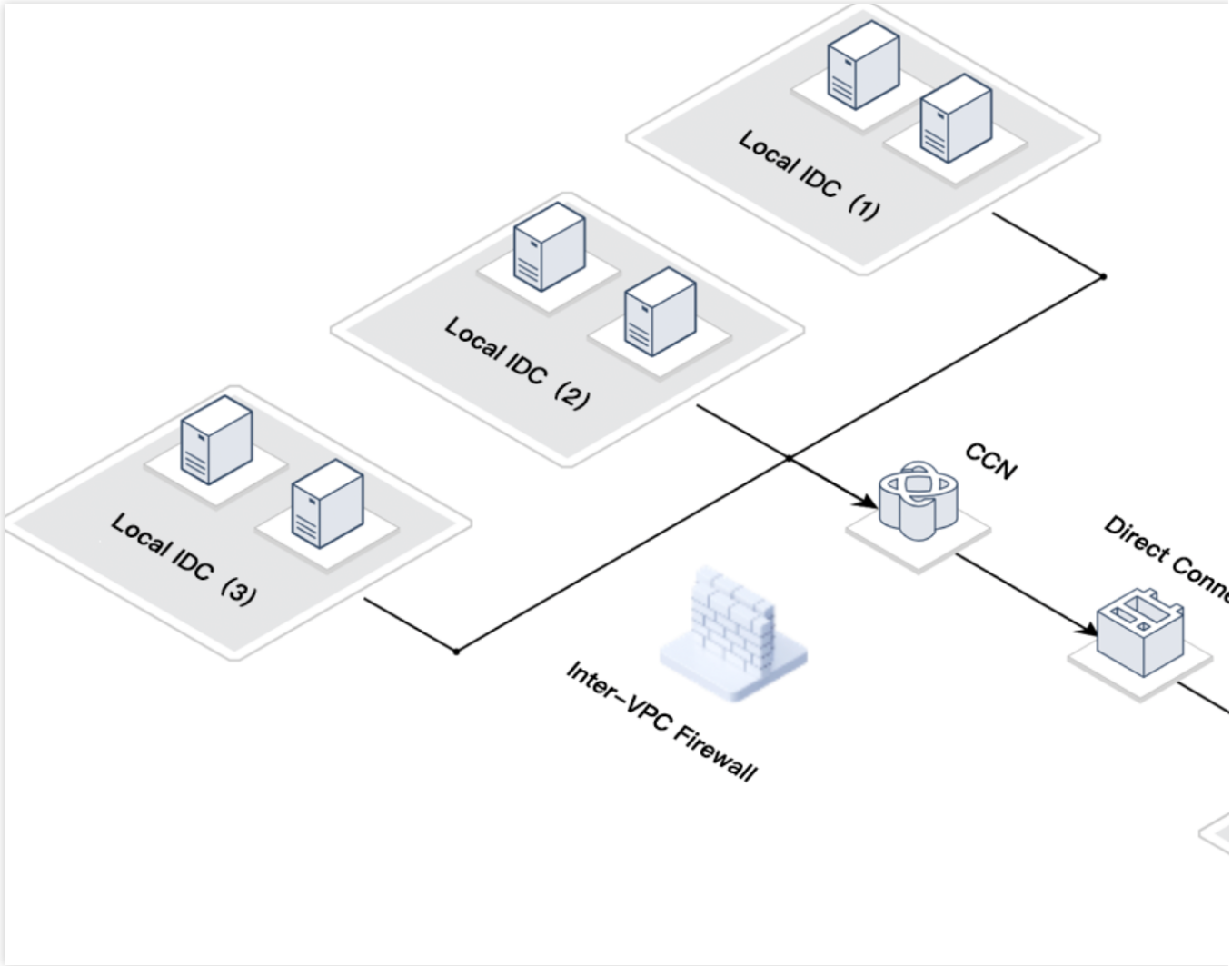
VPN Cloud Migration Scenarios

User requirement: Adopt VPN connections for Office Network and Public Cloud, with core business and data residing on the public cloud. Security monitoring of the office network is lower than the production network.
Business challenge: When the local office network is compromised due to attacks such as phishing, attackers can easily attack core business on the cloud via VPC Private Line.
Solution: Integrate Inter-VPC Firewall and enable intrusion defense block mode to automatically block and monitor the office network's access to cloud services, intercepting scanning and attack traffic.
Practical configuration: See Create Inter-VPC Firewallf for configuration, select **CCN mode** for integration, select **Auto** for Inter-VPC Firewall, and select **Point to point** for the routing mode.



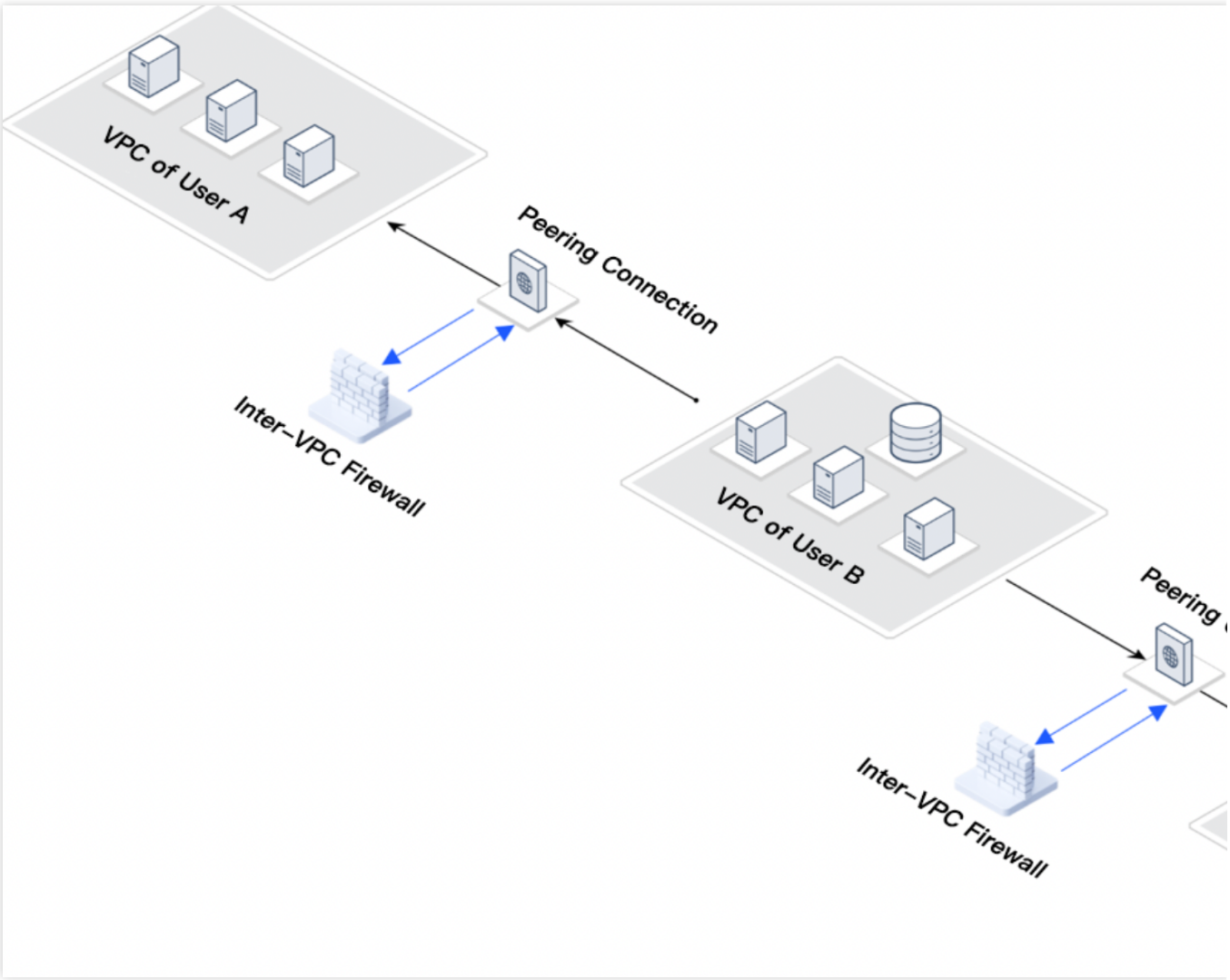
Hybrid Cloud Scenario

User requirement: The client has multiple local IDCs that are interconnected via CCN and uses private lines to connect to Public Cloud VPC.
Business challenge: When certain IDCs are isolated to prevent accessing public cloud services, it is also necessary to prevent lateral movement to the cloud if a local IDC is compromised.
Solution: Integrate Inter-VPC Firewall and enable Intrusion Defense. Set access control rules to block certain IDCs' source addresses.
Practical configuration: See Create Inter-VPC Firewall for configuration, select **CCN mode** for integration, select **Auto** for Inter-VPC Firewall, and select **Point to multipoint** for the routing mode (if there are fewer local IDCs, point to point can be selected).



Cross-Account Peering Connection Scenario

User requirement: User B's cloud business needs to retrieve data from User A and User C, with a requirement for data inflow only.
Business challenge: User B VPC need to access User A and User C VPCs, but to ensure data security, User A VPC and User C VPC need to be blocked from accessing User B.
Solution: Integrate Inter-VPC Firewall and configure access control rules to block all traffic destined for User B VPC.
Practical configuration: See Create Inter-VPC Firewall for configuration, select **VPC mode** for integration, select **Auto** for Inter-VPC Firewall, and select **Point to point** for the routing mode.



FAQs

Does Integrating an Inter-VPC Firewall Affect Business?

There will be a very brief interruption during integration. It is recommended to choose a less busy period for this. CFW can provide R&D support, and based on experience, the integration of the Inter-VPC Firewall has minimal impact on the business. If concerned, you can try it in a test environment.

Can Security Groups Replace Inter-VPC Firewall?

Inter-VPC Firewall can perform log audits, observe rule matched and allowed traffic. However, server security groups do not have this feature. Additionally, the intrusion defense feature of the Inter-VPC Firewall can address threats in the traffic, monitor scanning traffic and attack traffic, while security groups do not have this feature.