Tencent Cloud Firewall

Practical Tutorial

Product Documentation

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

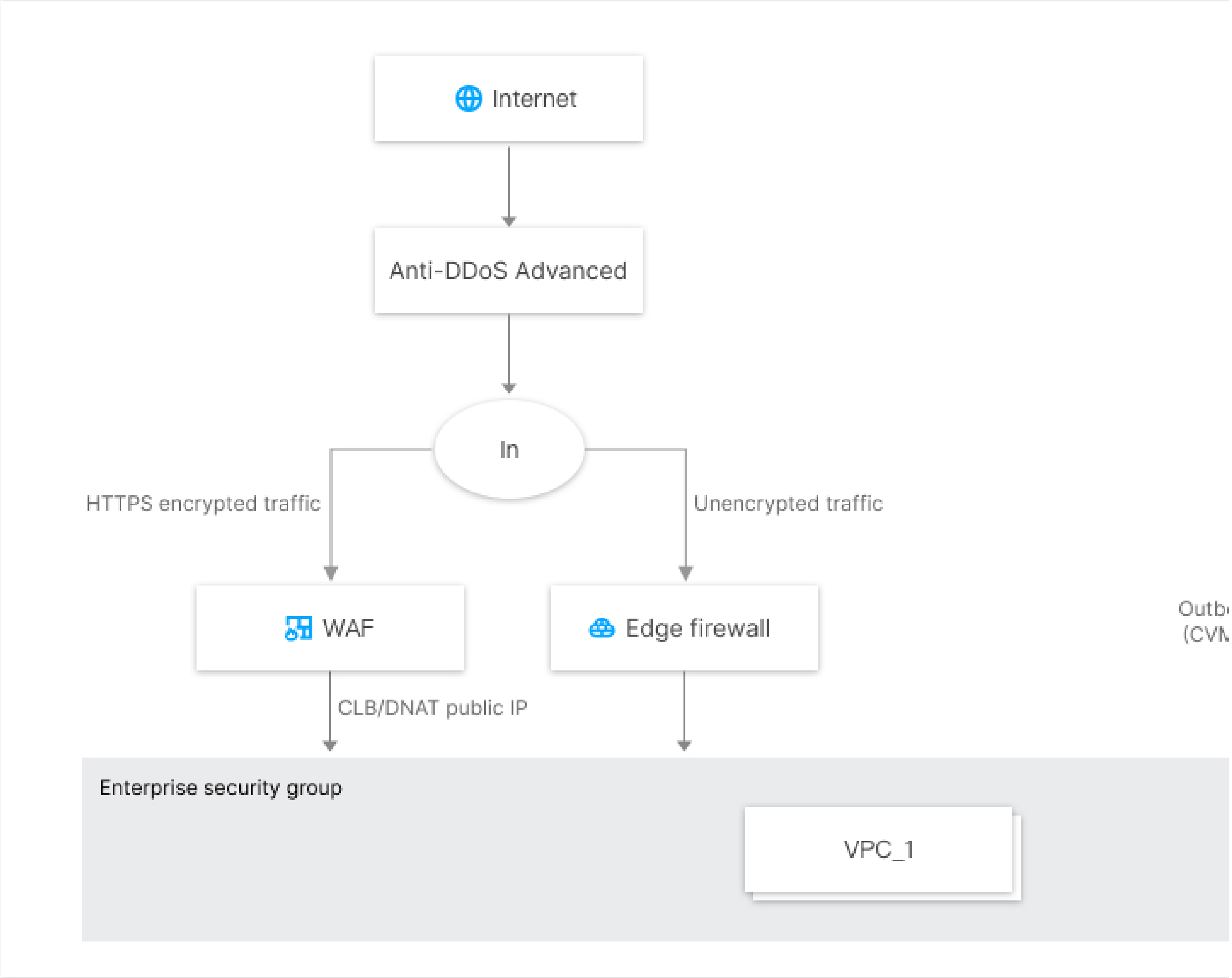
Contents

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:

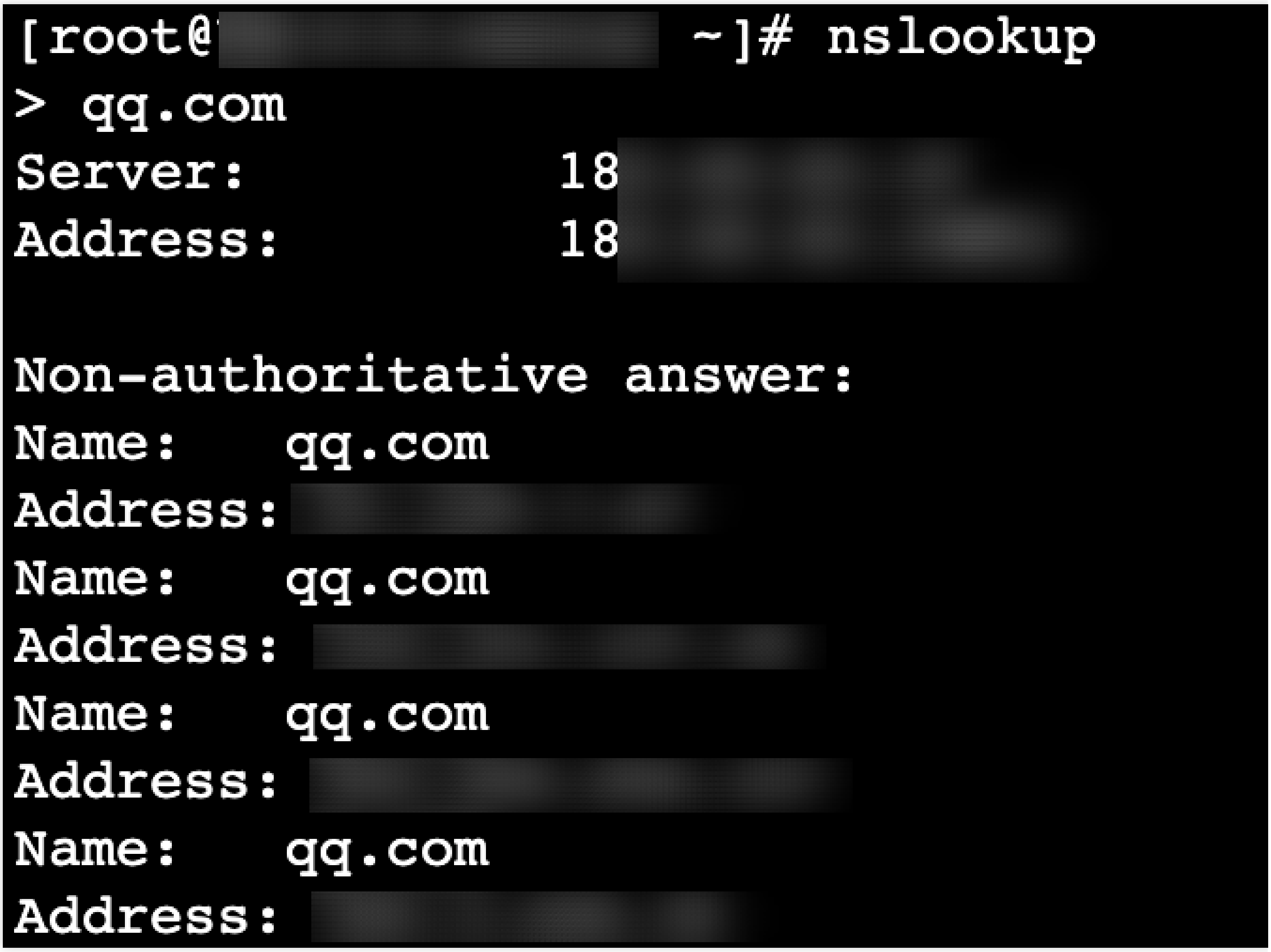
Create a NAT firewall for the region and connect to a VPC.

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:

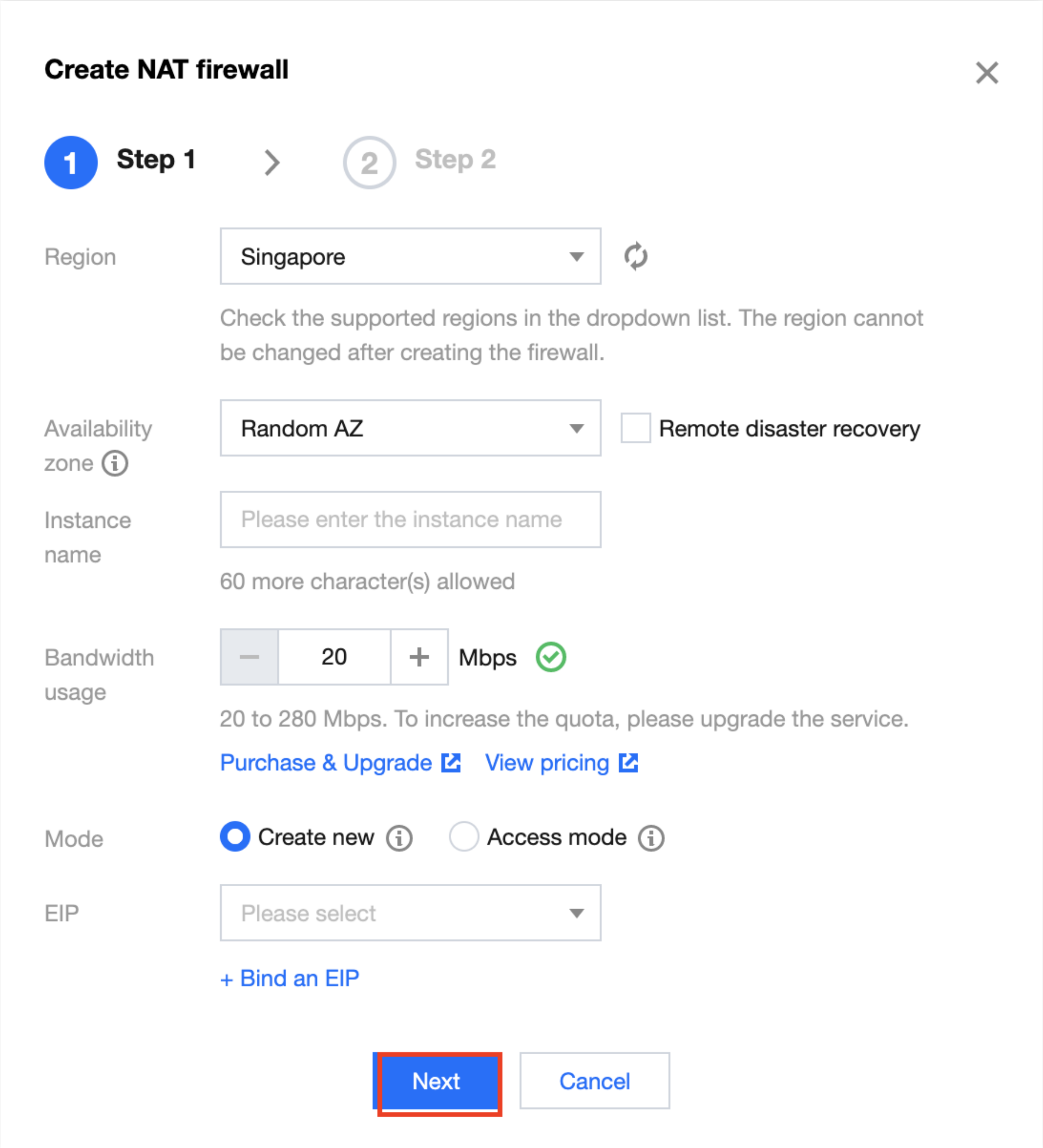


```
[root@[redacted] ~]# nslookup
> qq.com
Server:         18[redacted]
Address:        18[redacted]

Non-authoritative answer:
Name:   qq.com
Address:[redacted]
Name:   qq.com
Address:[redacted]
Name:   qq.com
Address:[redacted]
Name:   qq.com
Address:[redacted]
```

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**.



Create NAT firewall

Step 1 > Step 2

Region: Singapore

Check the supported regions in the dropdown list. The region cannot be changed after creating the firewall.

Availability zone: Random AZ ☐ Remote disaster recovery

Instance name: Please enter the instance name

60 more character(s) allowed

Bandwidth usage: 20 Mbps

20 to 280 Mbps. To increase the quota, please upgrade the service.

Purchase & Upgrade View pricing

Mode: ● Create new ○ Access mode

EIP: Please select

+ Bind an EIP

Next Cancel

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.

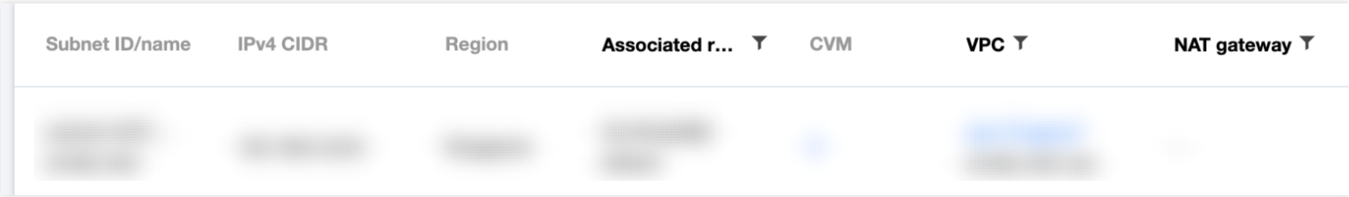
EIP: If you select to create a new EIP, the system automatically requests an EIP for you. Or you can select and bind one of the idle EIPs.

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

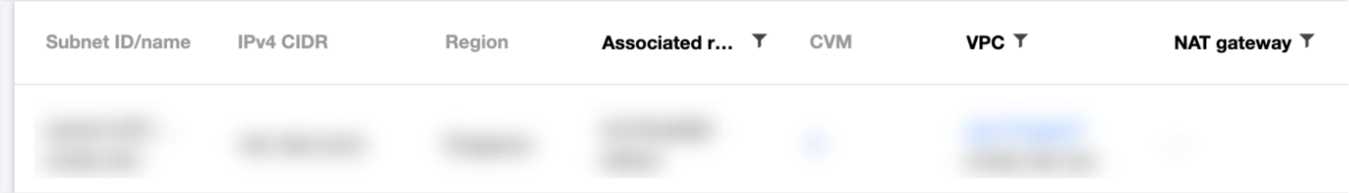
to enable the firewall.



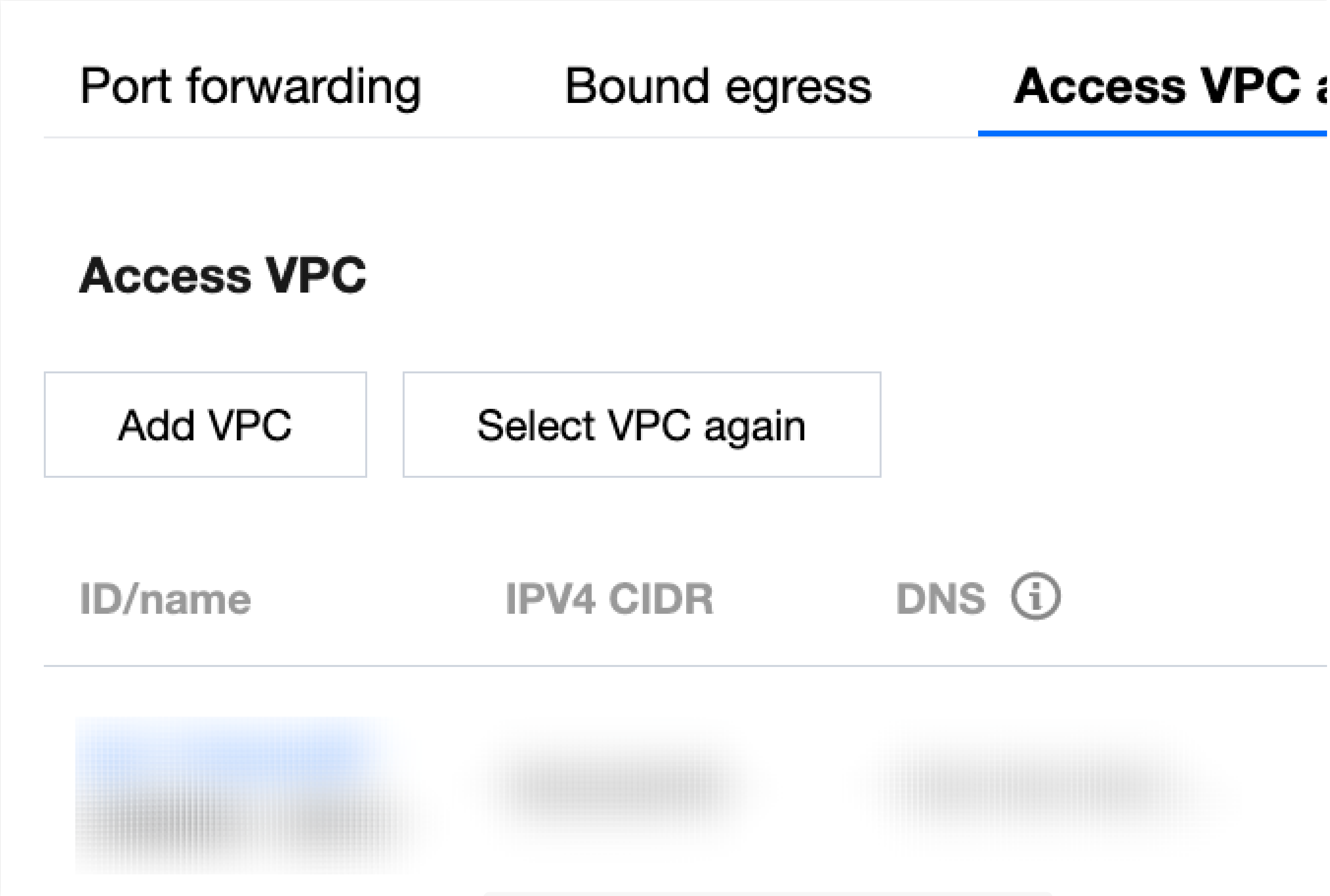
Subnet ID/name	IPv4 CIDR	Region	Associated r...	CVM	VPC	NAT gateway
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Step 3: enable and verify DNS

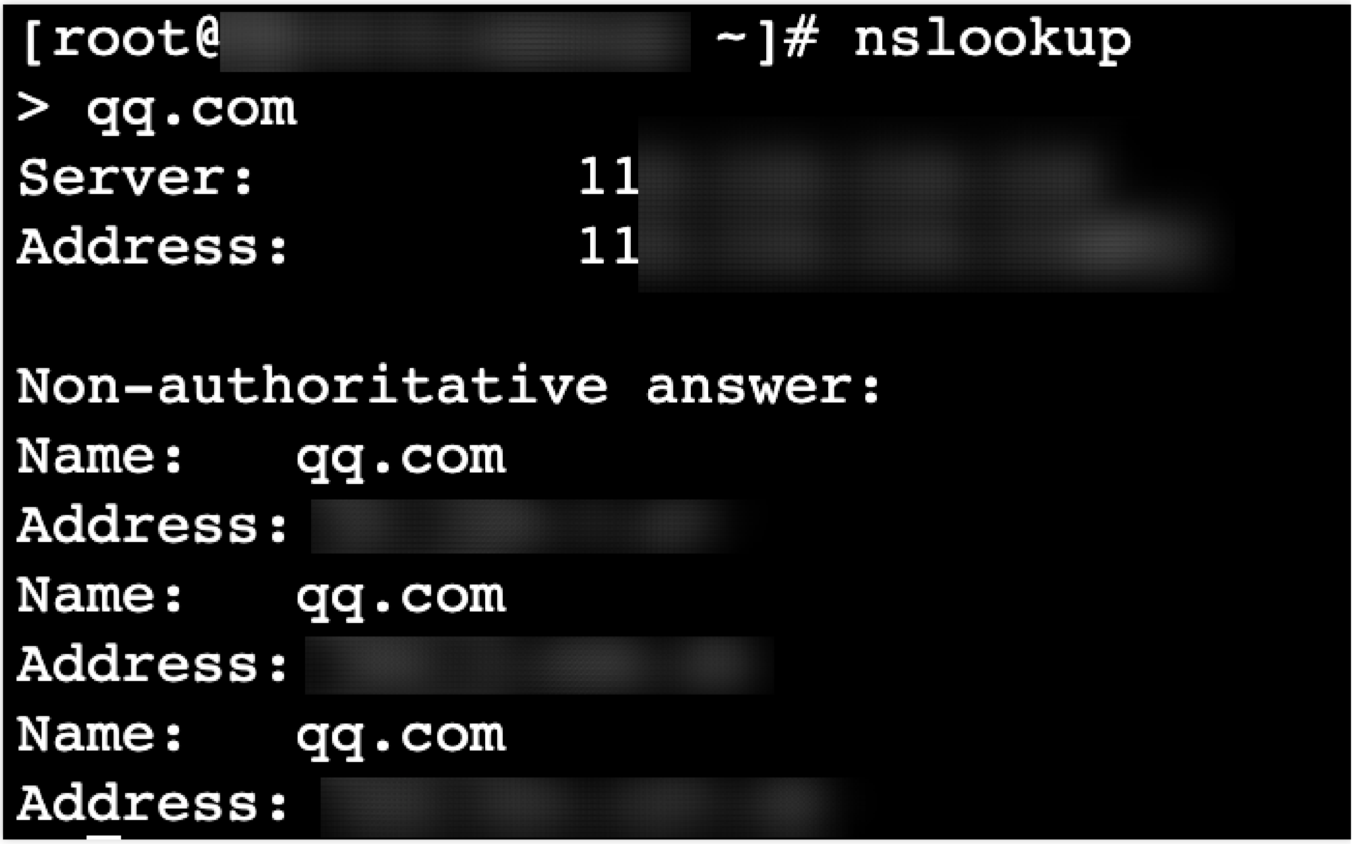
1. On the NAT firewall page, click **Firewall instances**. Then, select the firewall instance that you just created in Step 1, and click **Instance configuration**.



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` .

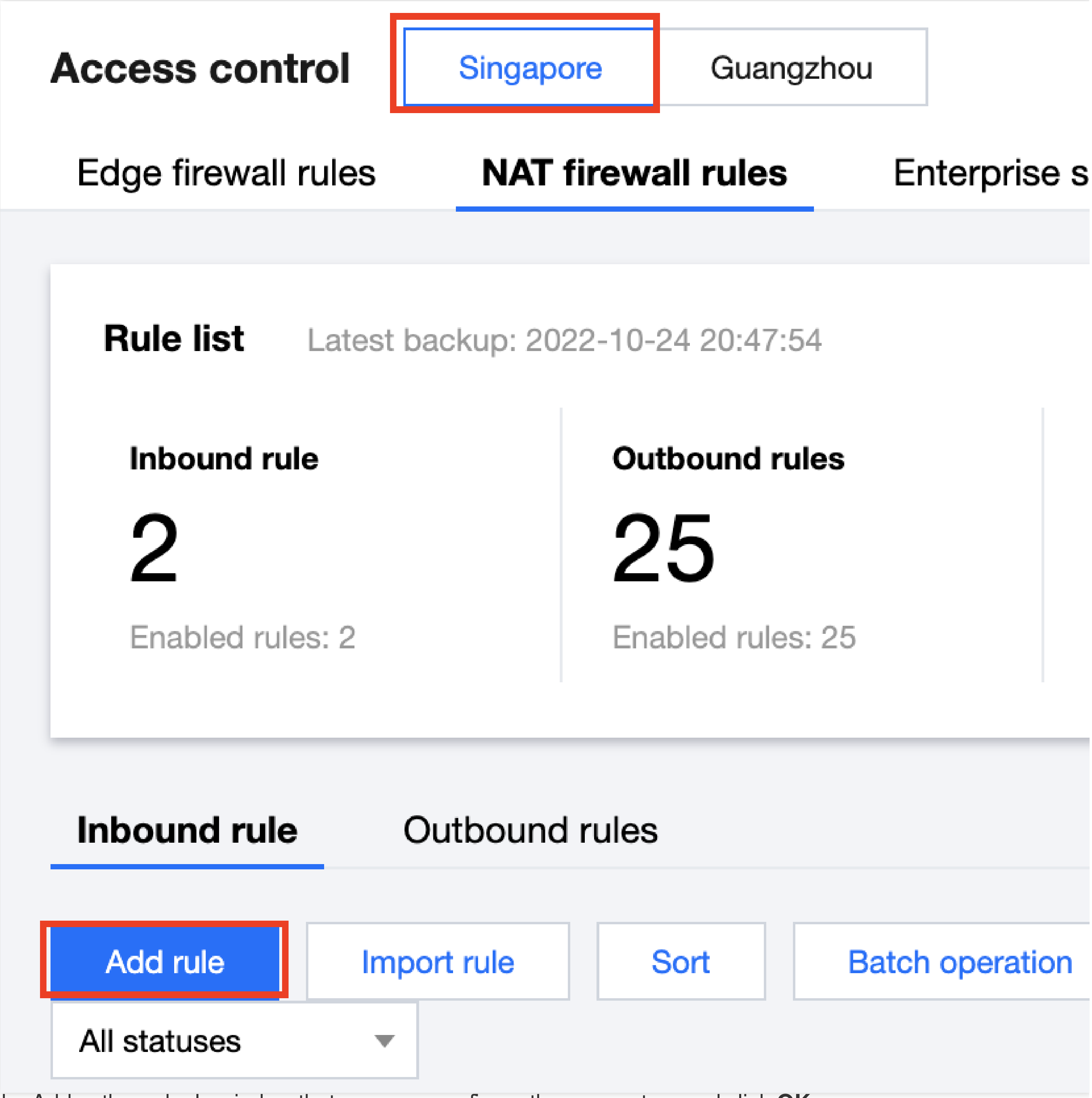


```
[root@[redacted] ~]# nslookup
> qq.com
Server:         11[redacted]
Address:        11

Non-authoritative answer:
Name:   qq.com
Address: [redacted]
Name:   qq.com
Address: [redacted]
Name:   qq.com
Address: [redacted]
```

Step 4: restrict DNS resolution

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



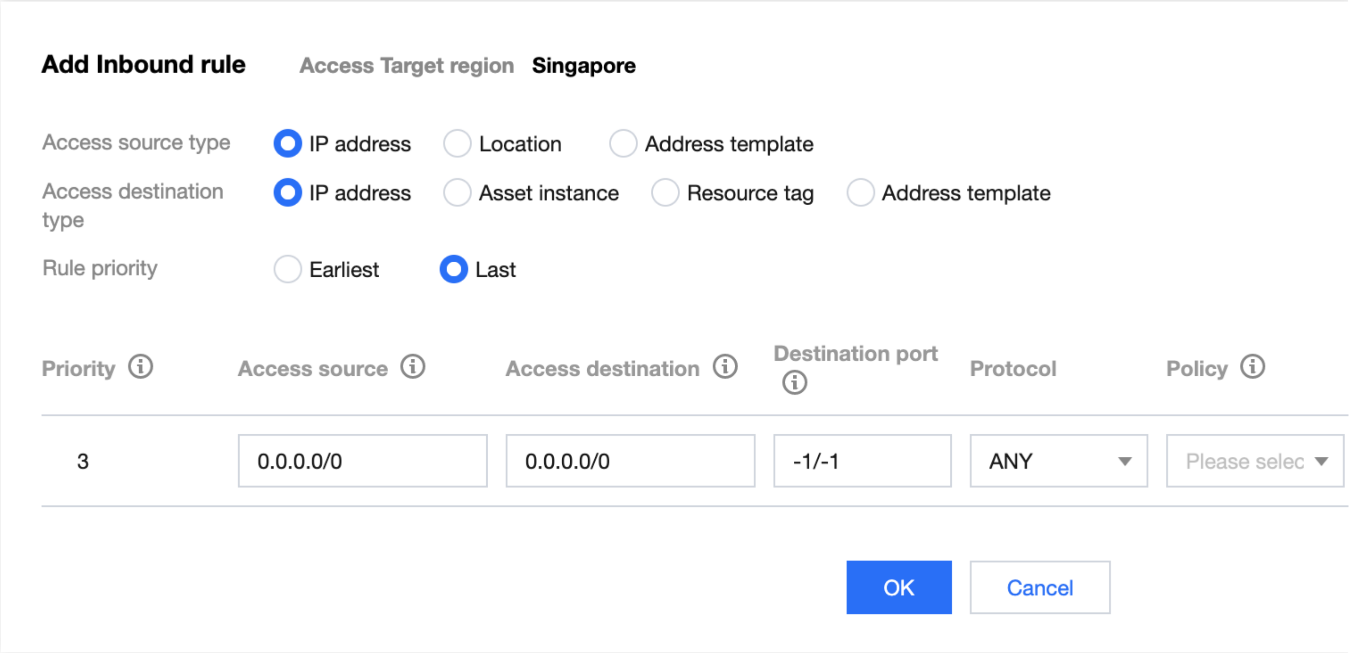
Access control

Rule list Latest backup: 2022-10-24 20:47:54

Inbound rule
2
Enabled rules: 2

Outbound rules
25
Enabled rules: 25

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



Add Inbound rule Access Target region **Singapore**

Access source type: ● IP address ○ Location ○ Address template

Access destination type: ● IP address ○ Asset instance ○ Resource tag ○ Address template

Rule priority: ○ Earliest ● Last

Priority	Access source	Access destination	Destination port	Protocol	Policy
3	0.0.0.0/0	0.0.0.0/0	-1/-1	ANY	Please selec

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:

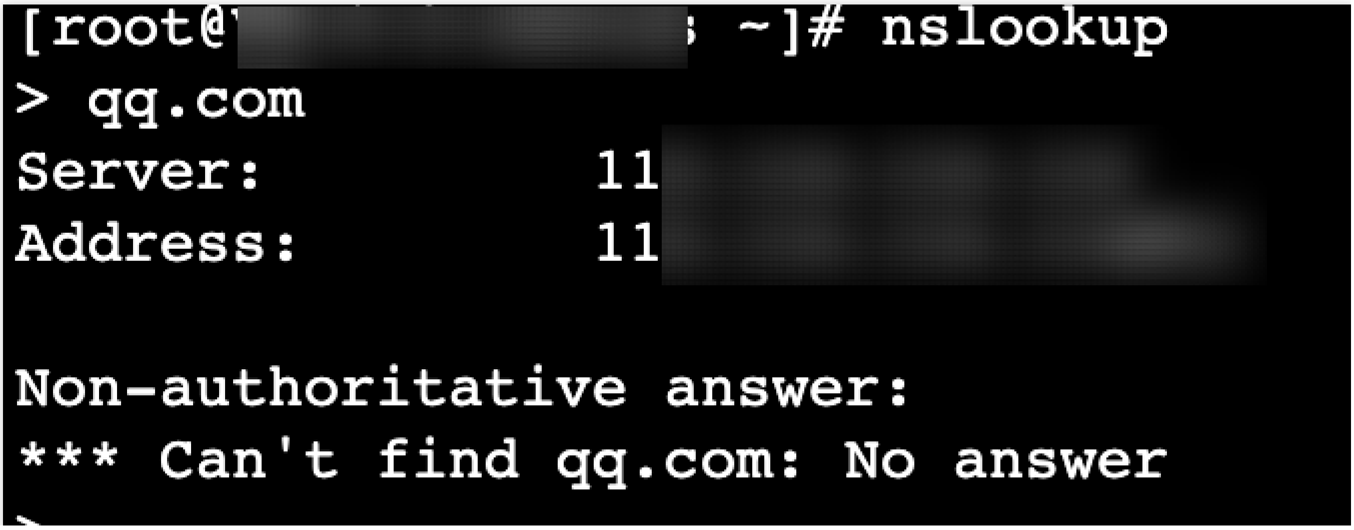
Allow: Allow the matched traffic and record the hit count and traffic logs, but not access control logs.

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.



```
[root@[redacted] ~]# nslookup
> qq.com
Server:         11[redacted]
Address:        11[redacted]

Non-authoritative answer:
*** Can't find qq.com: No answer
>
```

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)

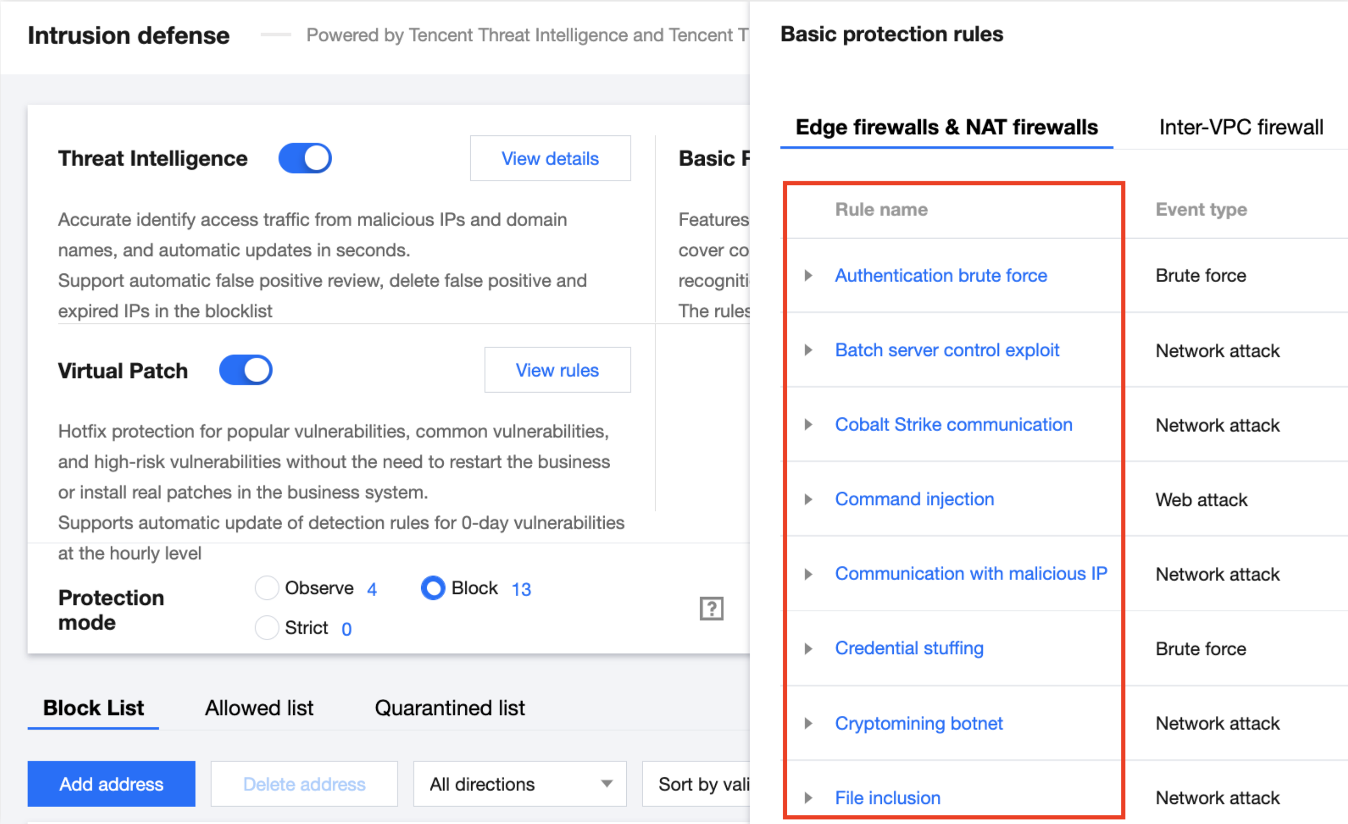
		Docker Remote API unauthorized access (CVE-2019-17671)
		YAPI remote code execution
Component vulnerabilities	JumaMinerH2Minertellyouthepass	Log4j2 remote code execution (CVE-2021-44228)
		Jenkins unauthenticated command execution (CVE-2017-1000353)
		WebLogic remote execution (CVE-2021-2109)
		Hadoop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



Intrusion defense — Powered by Tencent Threat Intelligence and Tencent T

Threat Intelligence — View details

Accurate identify access traffic from malicious IPs and domain names, and automatic updates in seconds.
Support automatic false positive review, delete false positive and expired IPs in the blocklist

Basic F

Features
cover co
recogniti
The rules

Virtual Patch — View rules

Hotfix protection for popular vulnerabilities, common vulnerabilities, and high-risk vulnerabilities without the need to restart the business or install real patches in the business system.
Supports automatic update of detection rules for 0-day vulnerabilities at the hourly level

Protection mode: ○ Observe 4 ● Block 13 ○ Strict 0

Block List | Allowed list | Quarantined list

Add address | Delete address | All directions | Sort by vali

Basic protection rules

Edge firewalls & NAT firewalls | Inter-VPC firewall

Rule name	Event type
Authentication brute force	Brute force
Batch server control exploit	Network attack
Cobalt Strike communication	Network attack
Command injection	Web attack
Communication with malicious IP	Network attack
Credential stuffing	Brute force
Cryptomining botnet	Network attack
File inclusion	Network attack

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

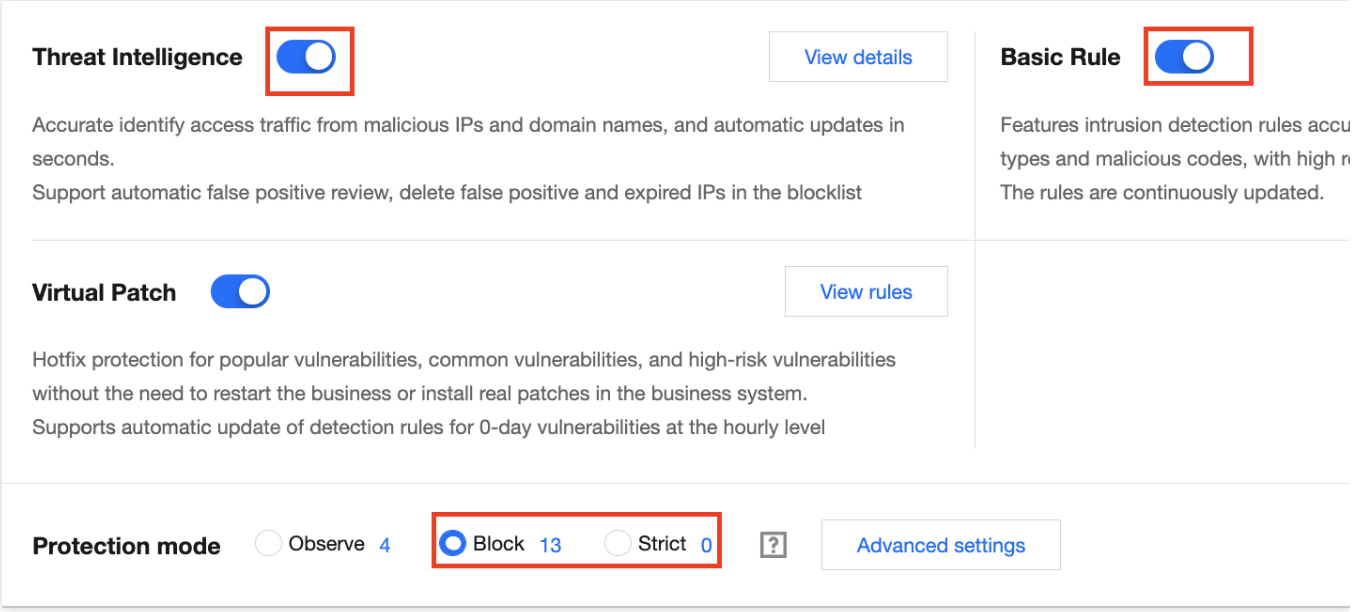
to enable threat intelligence and basic protection, and then select "Block" or "Strict" for the protection mode.

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.



Threat Intelligence

Accurate identify access traffic from malicious IPs and domain names, and automatic updates in seconds.
Support automatic false positive review, delete false positive and expired IPs in the blocklist

Basic Rule

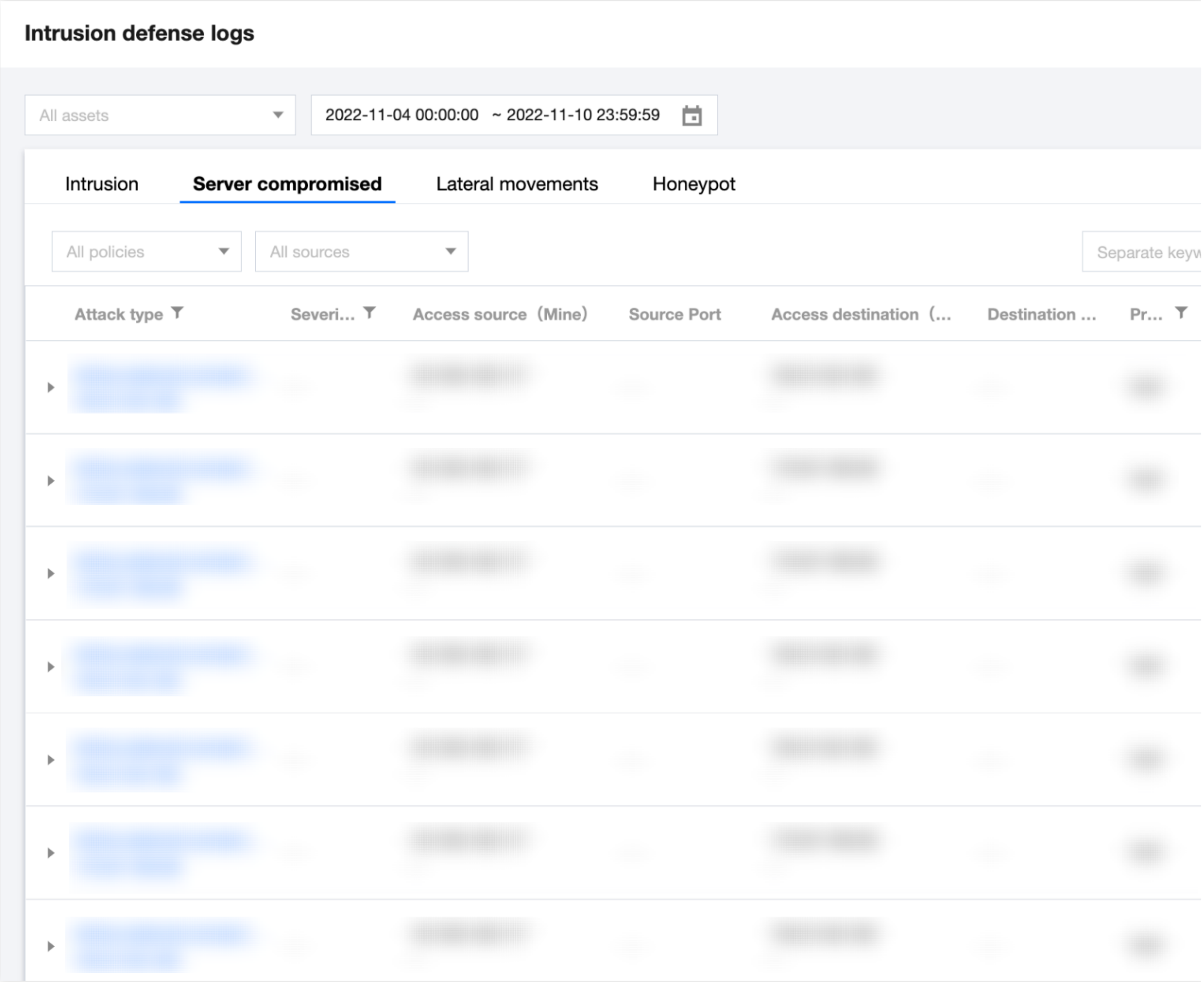
Features intrusion detection rules accu
types and malicious codes, with high r
The rules are continuously updated.

Virtual Patch

Hotfix protection for popular vulnerabilities, common vulnerabilities, and high-risk vulnerabilities without the need to restart the business or install real patches in the business system.
Supports automatic update of detection rules for 0-day vulnerabilities at the hourly level

Protection mode ○ Observe 4 ● Block 13 ○ Strict 0

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



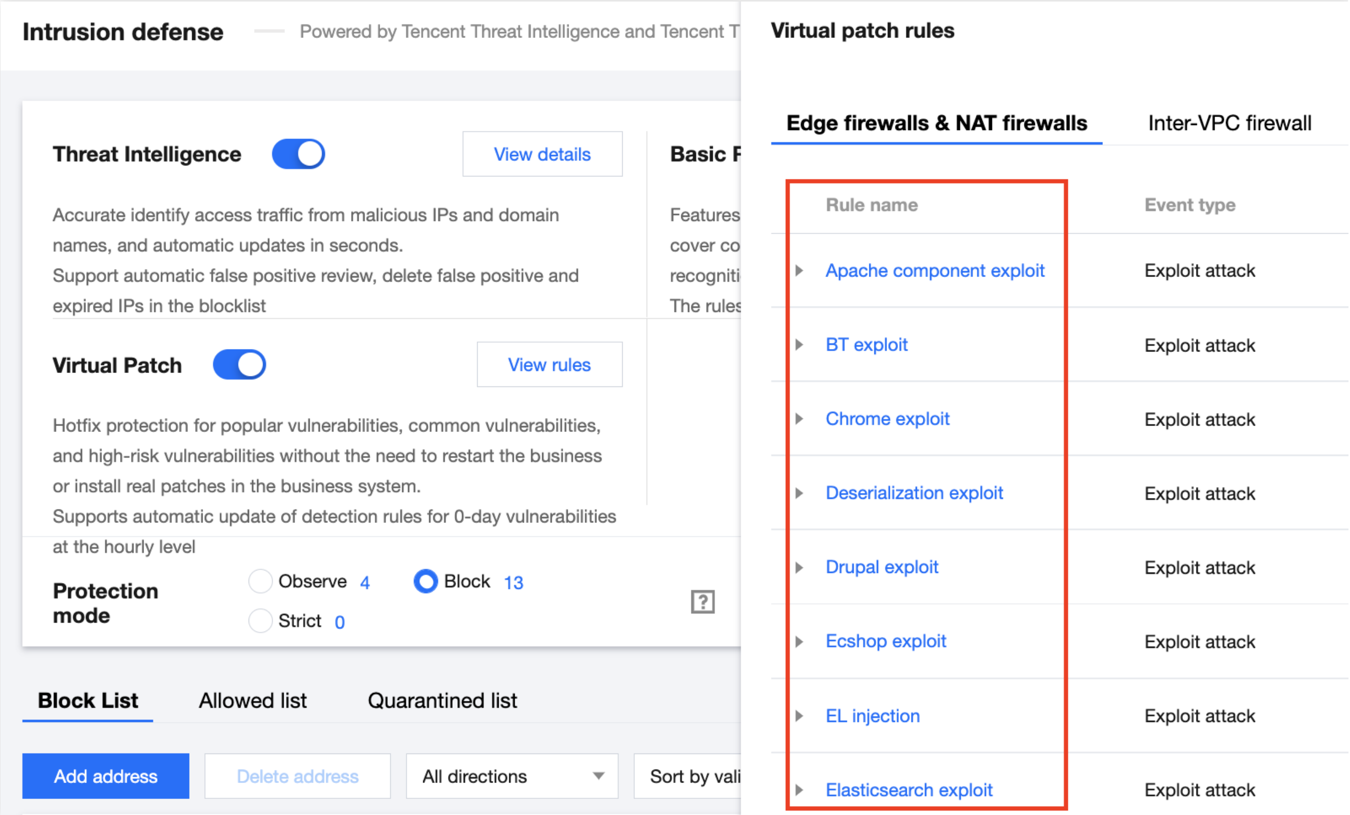
Intrusion defense logs

All assets | 2022-11-04 00:00:00 ~ 2022-11-10 23:59:59

Attack type	Severi...	Access source（Mine）	Source Port	Access destination（...	Destination ...	Pr...
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

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:



Intrusion defense — Powered by Tencent Threat Intelligence and Tencent T

Threat Intelligence View details

Accurate identify access traffic from malicious IPs and domain names, and automatic updates in seconds.
Support automatic false positive review, delete false positive and expired IPs in the blocklist

Basic F

Features
cover co
recogniti
The rules

Virtual Patch View rules

Hotfix protection for popular vulnerabilities, common vulnerabilities, and high-risk vulnerabilities without the need to restart the business or install real patches in the business system.
Supports automatic update of detection rules for 0-day vulnerabilities at the hourly level

Protection mode ○ Observe 4 ● Block 13 ○ Strict 0

Block List Allowed list Quarantined list

Add address Delete address All directions Sort by vali

Virtual patch rules

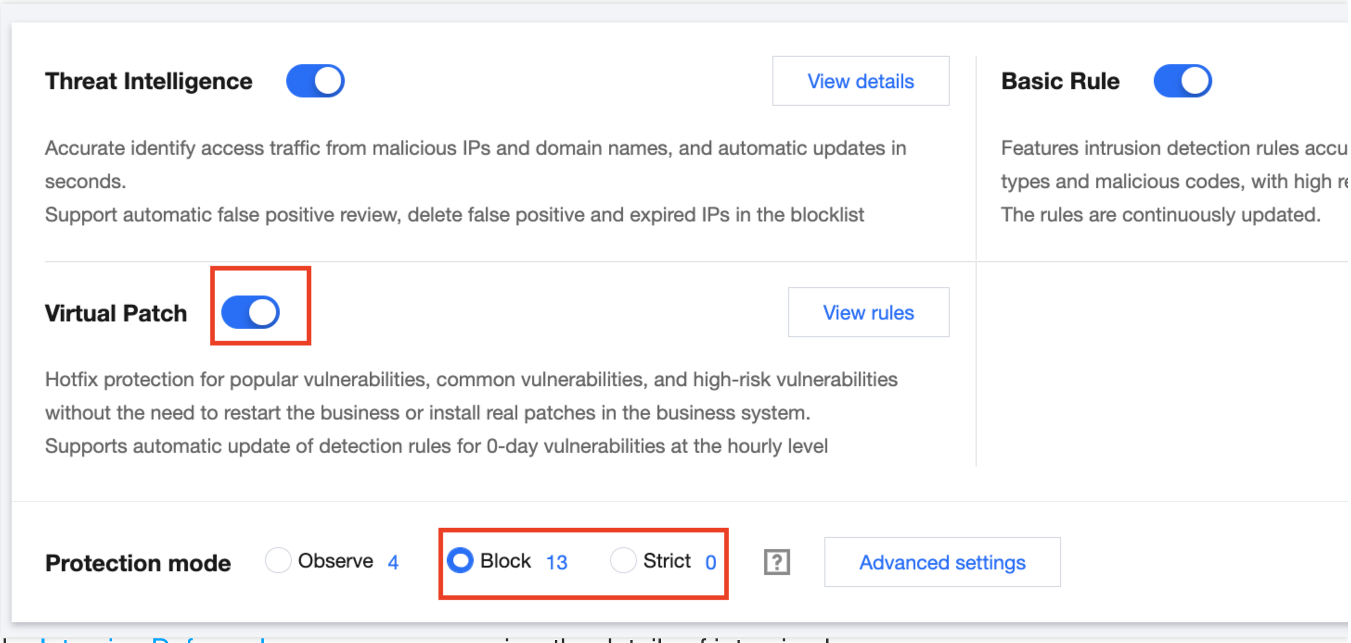
Edge firewalls & NAT firewalls Inter-VPC firewall

Rule name	Event type
Apache component exploit	Exploit attack
BT exploit	Exploit attack
Chrome exploit	Exploit attack
Deserialization exploit	Exploit attack
Drupal exploit	Exploit attack
Ecshop exploit	Exploit attack
EL injection	Exploit attack
Elasticsearch exploit	Exploit attack

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.



Threat Intelligence View details

Accurate identify access traffic from malicious IPs and domain names, and automatic updates in seconds.
Support automatic false positive review, delete false positive and expired IPs in the blocklist

Basic Rule

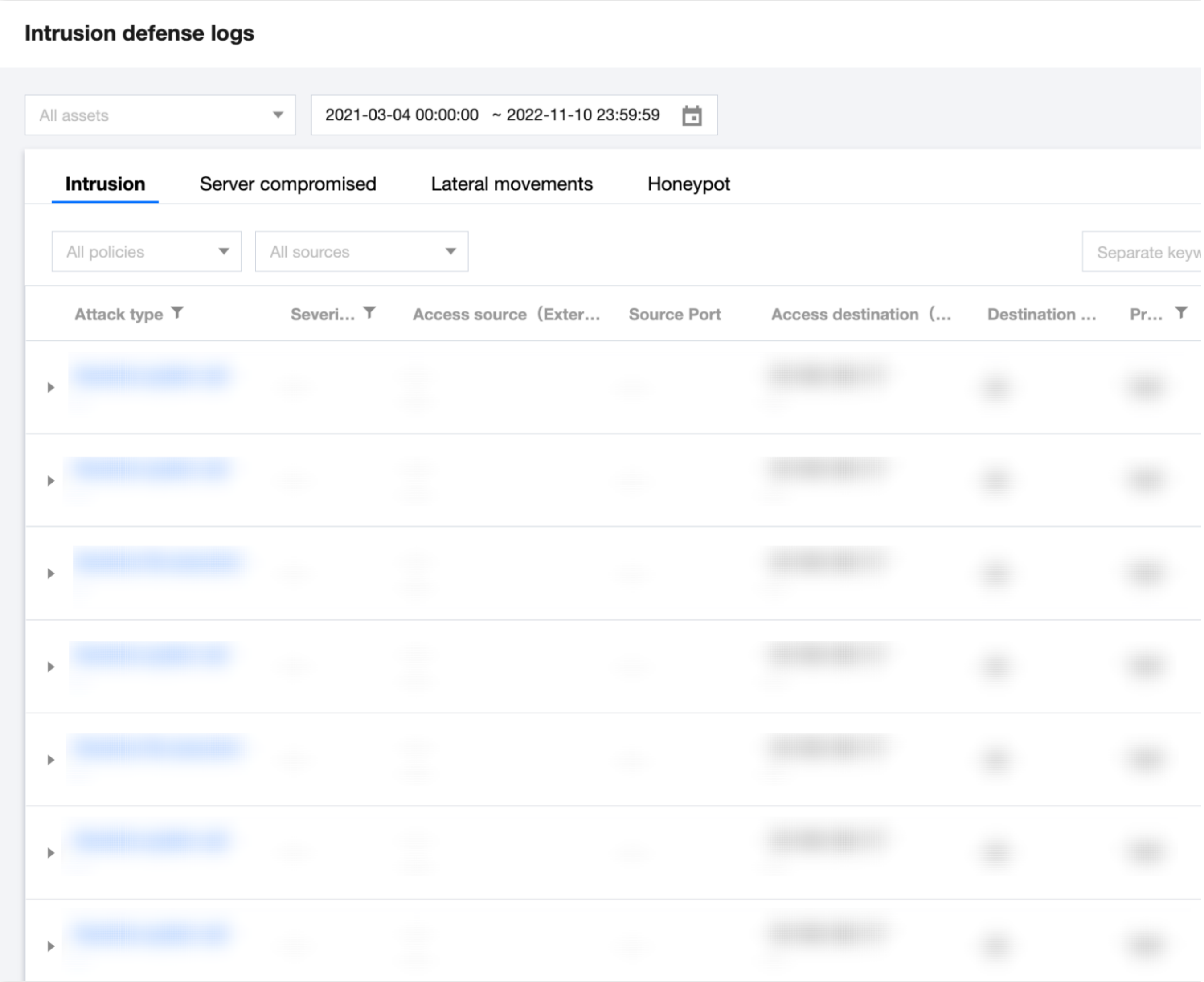
Features intrusion detection rules accu
types and malicious codes, with high r
The rules are continuously updated.

Virtual Patch View rules

Hotfix protection for popular vulnerabilities, common vulnerabilities, and high-risk vulnerabilities without the need to restart the business or install real patches in the business system.
Supports automatic update of detection rules for 0-day vulnerabilities at the hourly level

Protection mode ○ Observe 4 ● Block 13 ○ Strict 0 Advanced settings

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



Intrusion defense logs

All assets

2021-03-04 00:00:00 ~ 2022-11-10 23:59:59

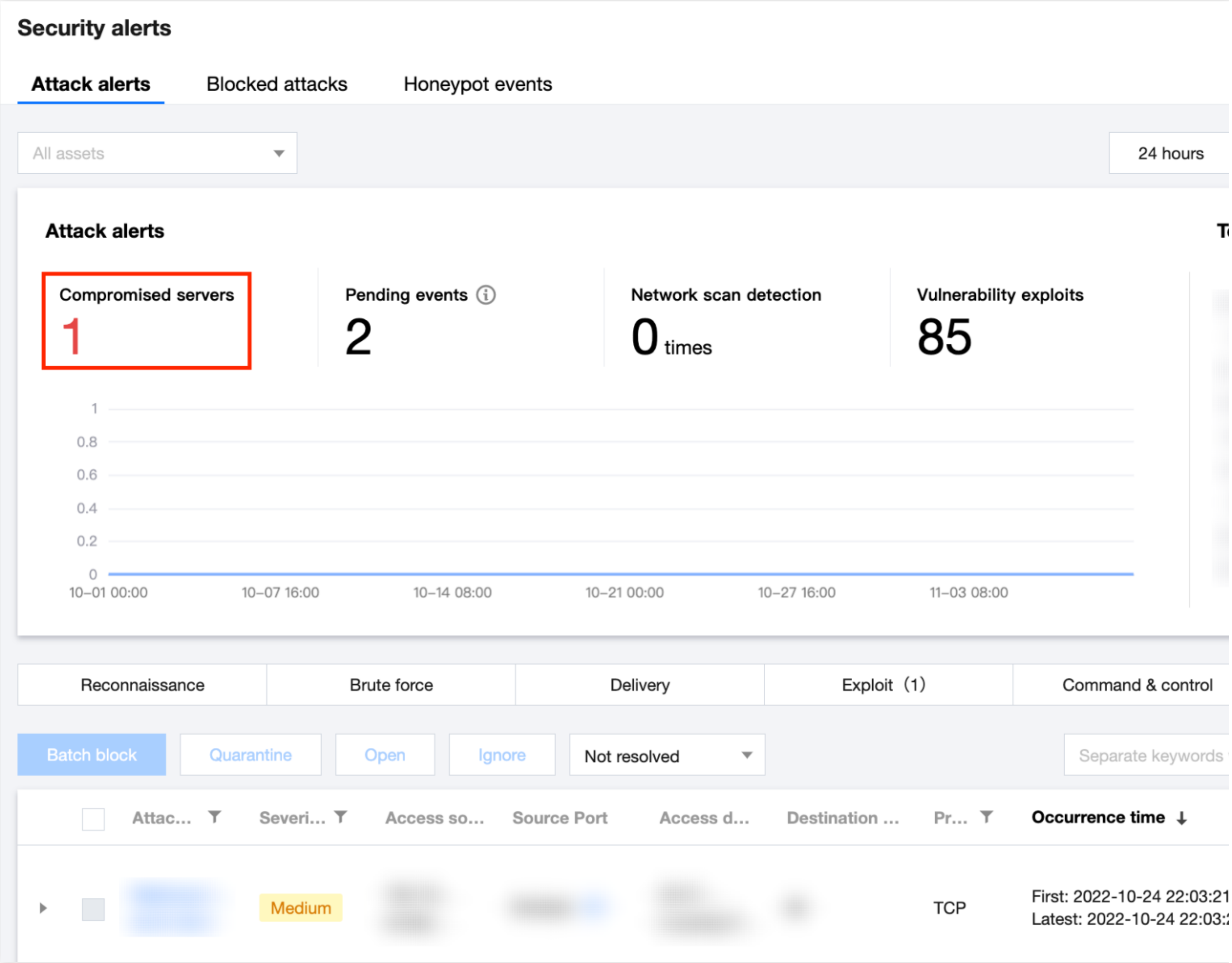
Intrusion | Server compromised | Lateral movements | Honeypot

All policies | All sources | Separate keyw

Attack type	Severi...	Access source（Exter...	Source Port	Access destination（...	Destination ...	Pr...

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.



Security alerts

Attack alerts | Blocked attacks | Honeypot events

All assets | 24 hours

Attack alerts

Compromised servers 1 | Pending events 2 | Network scan detection 0 times | Vulnerability exploits 85

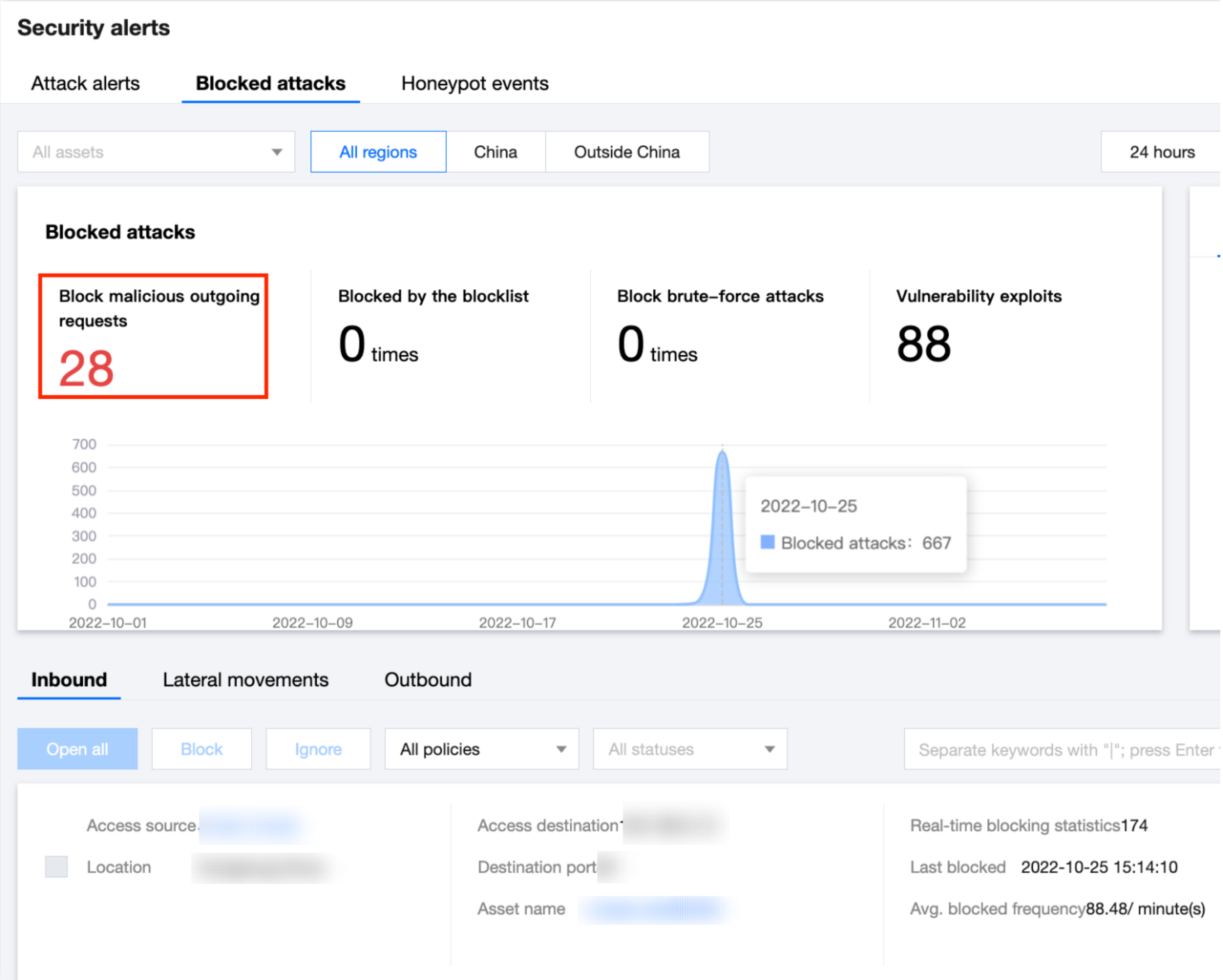
Reconnaissance | Brute force | Delivery | Exploit (1) | Command & control

Attac...	Severi...	Access so...	Source Port	Access d...	Destination ...	Pr...	Occurrence time
[illegible]	Medium	[illegible]	[illegible]	[illegible]	[illegible]	TCP	First: 2022-10-24 22:03:21 Latest: 2022-10-24 22:03:

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.



Blocked attacks

Block malicious outgoing requests 28

Blocked by the blocklist 0 times

Block brute–force attacks 0 times

Vulnerability exploits 88

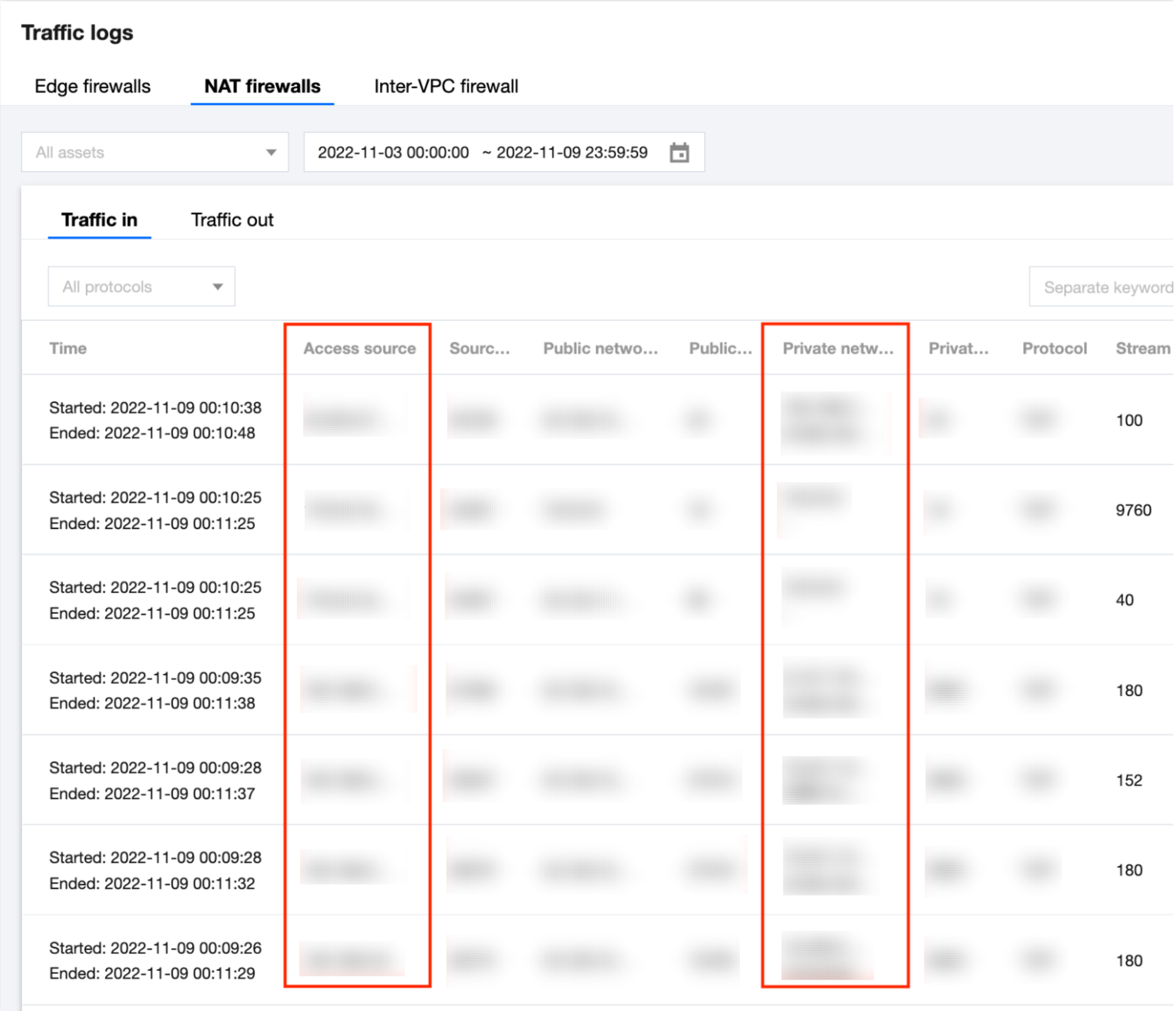
2022–10–25
Blocked attacks: 667

Access source [redacted]
Location [redacted]

Access destination [redacted]
Destination port [redacted]
Asset name [redacted]

Real-time blocking statistics174
Last blocked 2022-10-25 15:14:10
Avg. blocked frequency88.48/ minute(s)

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.



Traffic logs

Edge firewalls | **NAT firewalls** | Inter-VPC firewall

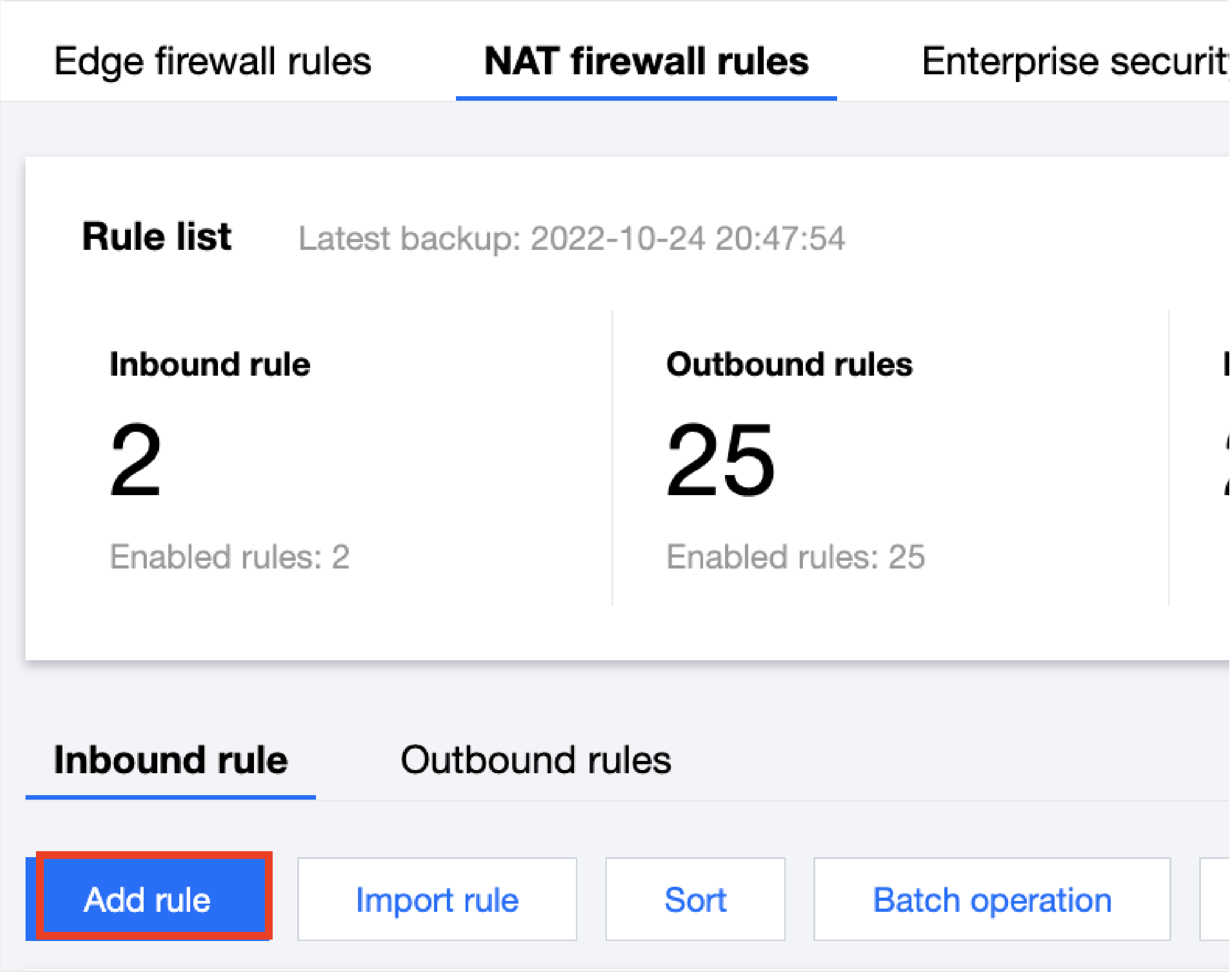
All assets ▾ | 2022-11-03 00:00:00 ~ 2022-11-09 23:59:59

Traffic in | Traffic out

All protocols ▾ | Separate keyword

Time	Access source	Sourc...	Public netwo...	Public...	Private netw...	Privat...	Protocol	Stream
Started: 2022-11-09 00:10:38 Ended: 2022-11-09 00:10:48	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	100
Started: 2022-11-09 00:10:25 Ended: 2022-11-09 00:11:25	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	9760
Started: 2022-11-09 00:10:25 Ended: 2022-11-09 00:11:25	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	40
Started: 2022-11-09 00:09:35 Ended: 2022-11-09 00:11:38	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	180
Started: 2022-11-09 00:09:28 Ended: 2022-11-09 00:11:37	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	152
Started: 2022-11-09 00:09:28 Ended: 2022-11-09 00:11:32	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	180
Started: 2022-11-09 00:09:26 Ended: 2022-11-09 00:11:29	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	180

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**.



Edge firewall rules | NAT firewall rules | Enterprise securit

Rule list Latest backup: 2022-10-24 20:47:54

Inbound rule
2
Enabled rules: 2

Outbound rules
25
Enabled rules: 25