

Alibaba Cloud

Cloud Firewall Best Practices

Document Version: 20220704

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.
2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.
3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.
4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).
5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.
6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions









Style	Description	Example
 Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 Danger: Resetting will result in the loss of user configuration data.
 Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 Warning: Restarting will cause business interruption. About 10 minutes are required to restart an instance.
 Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: If the weight is set to 0, the server no longer receives new requests.
 Note	A note indicates supplemental instructions, best practices, tips, and other content.	 Note: You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click Settings > Network > Set network type .
Bold	Bold formatting is used for buttons, menus, page names, and other UI elements.	Click OK .
Courier font	Courier font is used for commands	Run the <code>cd /d C:/window</code> command to enter the Windows system folder.
<i>Italic</i>	Italic formatting is used for parameters and variables.	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	This format is used for a required value, where only one item can be selected.	<code>switch {active stand}</code>

Table of Contents

1.Cloud Firewall best practices	05
2.Best practices to defend against worms from C&C servers	07
3.Best practices for database security defense	10
4.Best practices for system security defense	12
5.Configure the access control policy that only allow access to a... ..	15
6.Create an outbound access control policy to allow traffic destin... ..	17
7.Best practices to defend against unauthorized access to a Mon... ..	19
8.Best practices to protect bastion hosts	23
9.Defend against mining programs	26
10.Import the traffic logs of Cloud Firewall to a third-party syste... ..	33
11.Block access from regions outside China	35
12.Best practices of Cloud Firewall based on ATT&CK	37
12.1. Disclaimer	37
12.2. Overview	37
12.3. Disable the installation of unauthorized tools	39
12.4. Disable uninstallation of cloud security software such as	40
12.5. Disable remote control software	40
12.6. Disable script downloading	41
12.7. Disable proxies	42
12.8. Disable leaks of critical system information	42
12.9. Disable remote debugging in the cloud	43
12.10. Disable information detection	43
12.11. Disable DoH	44
12.12. Disable access to .onion proxy domain	44

1. Cloud Firewall best practices

How to choose the appropriate Cloud Firewall edition

Cloud Firewall includes the Advanced Edition, Enterprise Edition, and Flagship Edition. The features and asset or bandwidth scaling specifications vary according to the edition. For more information, see [Features](#).

Configure access policies for out-in traffic

In access policies for out-in traffic, do not allow access to all ports from public IP addresses. Open only necessary Internet IP addresses and ports. **Block** access to all the other ports.

1. Allow access traffic to necessary applications or ports.

On the **Access Control** page, click the **Out-In Traffic** tab. Add an access policy. Set the source to `0.0.0.0/0` or a specific IP address. You can also set the source to the default address book **ANY** (`0.0.0.0/0`) or a specific IP address. Set the destination to the IP address that needs to be accessed or a specific IP address. Set the protocol to **ANY** or a specific protocol based on business requirements. Set the action to **Allow**.

IP Address Books					
<div> <div>Search by name or description.</div> <div>All Types</div> <div>Search</div> <div>+Create Address Book</div> </div>					
Address Book Name	Type	IP/ECS Tag	Description	References	Actions
	ECS Tags	1	11	0	Modify Delete
	ECS Tags	10	test	4	Modify Delete

Example:

Port 80 is a Web service port that needs to be opened to all public IP addresses. Therefore, set the source to `0.0.0.0/0` for port 80. Ports 1433 and 3389 are SQL Server and RDP service ports, respectively. They are opened only to specific sources. Therefore, set the source to the specific sources for ports 1433 and 3389 respectively.

2. Block all the other out-in traffic.

On the **Access Control** page, click the **Out-In Traffic** tab. Add an access policy. Set the source to `0.0.0.0/0` or the default address book **ANY** (`0.0.0.0/0`). Set both the destination and protocol to **ANY**. Set the action to **Block**.

Configure access policies for in-out traffic

We recommend that you do not allow all in-out traffic. Instead, allow only outbound access traffic to necessary public IP addresses or domain names, and **block** all the other in-out traffic.

1. Allow outbound access traffic from necessary applications or ports.

On the **Access Control** page, click the **In-Out Traffic** tab. Add an access policy. Set the source to `0.0.0.0/0` or a specific IP address. You can also set the source to the default address book **ANY** (`0.0.0.0/0`) or a specific IP address. Set the destination to the domain name or IP address that needs to be accessed or a specific IP address. Set the protocol to **ANY** or a specific protocol based on business requirements. Set the action to **Allow**.

2. **Block** all the other in-out traffic.

On the Access Control page, click the In-Out Traffic tab. Add an access policy. Set the source to 0.0.0.0/0 or the default address book **ANY** (0.0.0.0/0). Set both the destination and protocol to **ANY**. Set the action to **Block**.

Enable Cloud Firewall protection and the interception mode for intrusion prevention

After subscribing to the Cloud Firewall service, you can click **Protect All** on the **Firewall Switch** page and click **Interception Mode** on the **Intrusion Prevention** page. In this way, you can fully protect the security of your assets.

2. Best practices to defend against worms from C&C servers

Worms are a major threat to services in the cloud. Worms exploit server vulnerabilities to spread over networks and carry out malicious operations on compromised servers. Worm attacks pose serious threats to the assets and business of users. Cloud Firewall provides layered defense against the attack chains of worms and can detect and intercept a variety of worms. Cloud Firewall also dynamically updates and expands its capabilities to detect and intercept new worms based on threat intelligence from the cloud.

Impact of worms

The following issues may occur due to worm attacks:

- **Service interruption:** Worms may carry out malicious operations, such as modifying configurations or terminating services, on compromised servers. This may cause risks, such as server breakdown or service interruption.
- **Information theft:** Worms that aim to steal information compress data on compromised servers and send the compressed data to attackers. This may cause data breaches and resource abuse.
- **Regulatory control:** When worms spread over a network, worms send a large number of packets. This may trigger regulatory control on IP addresses, which results in service interruption. For example, IP addresses may be blocked.
- **Economic or data loss:** Ransomware worms encrypt files on compromised servers for ransom, which can cause economic or data loss.

Solution provided by Cloud Firewall

Cloud Firewall provides layered defense against the attack chains of worms and can detect and intercept a variety of worms. Cloud Firewall also dynamically updates and expands its capabilities to detect and intercept new worms based on threat intelligence from the cloud.

The following list describes common worms:

- **DDG:** spreads by exploiting Redis vulnerabilities and by launching brute-force attacks. This worm uses the computing resources on compromised servers to mine cryptocurrency.
- **WannaCry:** spreads by exploiting Windows system vulnerabilities and compromises servers for ransom.
- **BillGates:** spreads by exploiting application vulnerabilities and by launching brute-force attacks. This worm builds a botnet of compromised servers to launch DDoS attacks.

Case: DDG worm

DDG is an active worm that spreads by exploiting Redis vulnerabilities and by launching brute-force attacks. Compromised servers are added to a botnet to mine cryptocurrency.

Impact scope of DDG

- Servers that use weak SSH passwords
- Redis or other database servers for which specific vulnerabilities exist

Major impact of DDG

- **Service interruption:** DDG mines cryptocurrency on compromised servers, during which a large number

of computing resources on the servers are occupied. This may affect service availability or cause service interruption.

- **Regulatory control:** When DDG spreads over a network, DDG sends a large number of packets. This may trigger regulatory control on IP addresses, which results in service interruption. For example, IP addresses may be blocked.

Defense against the DDG attack chain

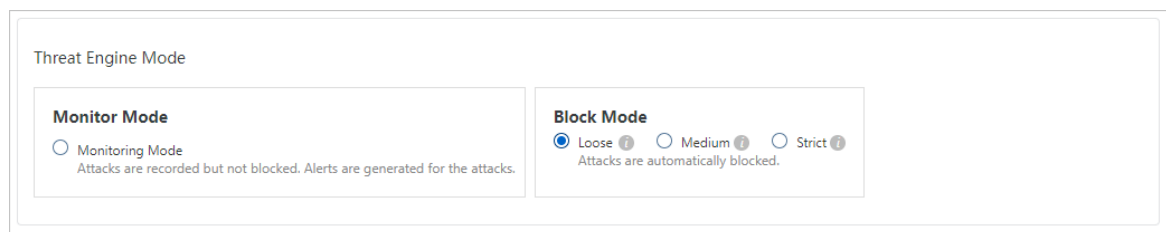
Cloud Firewall detects and defends against the DDG attack chain in real time. This way, worms are blocked and are prevented from spreading.

Cloud Firewall provides the following intrusion prevention features:

- **Whitelist:** Cloud Firewall trusts the source and destination IP addresses that you specify in the whitelist and does not block the traffic of these IP addresses.
- **Threat intelligence:** Cloud Firewall scans your servers for threat intelligence and blocks malicious behavior from C&C servers based on the threat intelligence.
- **Basic protection:** Cloud Firewall detects malware and intercepts the requests sent to or received from C&C servers or backdoors.
- **Virtual patching:** Cloud Firewall provides virtual patches to defend your services against popular high-risk application vulnerabilities in real time.

Procedure

1. Log on to the [Cloud Firewall console](#).
2. In the left-side navigation pane, choose **Intrusion Prevention > Prevention Configuration**.
3. In the **Threat Engine Mode** section of the **Prevention Configuration** page, select **Loose** for **Block Mode**.



4. In the **Advanced Settings** section, click **Whitelist**. In the dialog box that appears, add trusted source IP addresses, destination IP addresses, or address books of both inbound and outbound traffic to a specific whitelist.

5. In the **Threat Intelligence** section, turn on **Threat Intelligence**.

6. In the **Basic Protection** section, turn on **Basic Policies**.

7. In the **Virtual Patches** section, turn on **Patches**.

For more information about how to configure intrusion prevention features, see [防护配置](#).

3. Best practices for database security defense

The intrusion prevention feature of Cloud Firewall can defend against intrusions into common databases.

Requirements for database security defense

A database is a system for an enterprise to manage and store data resources. A database stores large amounts of valuable and sensitive data. As a result, databases become the primary target of attacks. Database security is vital to normal business operations and the growth of enterprises.

Databases may face the following major security threats:

- Brute-force attacks

Brute-force attacks directly cause databases to be compromised.

- Database application vulnerabilities

For example, Common Vulnerabilities and Exposures (CVE) of databases may cause denial-of-service (DoS) attacks to database applications, malicious command execution, or data breaches.

- Malicious command execution and file reading or writing

For example, attackers call high-risk stored procedures or functions, which may cause malicious command execution and file reading or writing.

- Data theft and breaches

Attackers sell stolen data or defraud others, which results in economic loss.

Solution provided by Cloud Firewall

The intrusion prevention feature of Cloud Firewall can defend against intrusions into the following types of databases:

- MySQL
- Microsoft SQL Server
- Redis
- PostgreSQL
- Memcache
- MongoDB
- Oracle

How to use Cloud Firewall to prevent intrusions to databases

The Alibaba Cloud security team continuously tracks and studies database intrusions and their preventive measures, and has accumulated rich experience in intrusion prevention. The prevention rules formulated based on the experience greatly enhance the database security defense of Cloud Firewall.

To ensure the normal running of a database, Cloud Firewall provides multi-point prevention against all the risks that the database faces.

- Brute-force attacks

Threat intelligence: The threat intelligence feature of Cloud Firewall can detect network-wide attacks and block scans or intrusions in advance.

- Database application vulnerabilities

Virtual patching: The virtual patching feature of Cloud Firewall prevents the high-risk application vulnerabilities of databases.

- Malicious command execution and file reading or writing

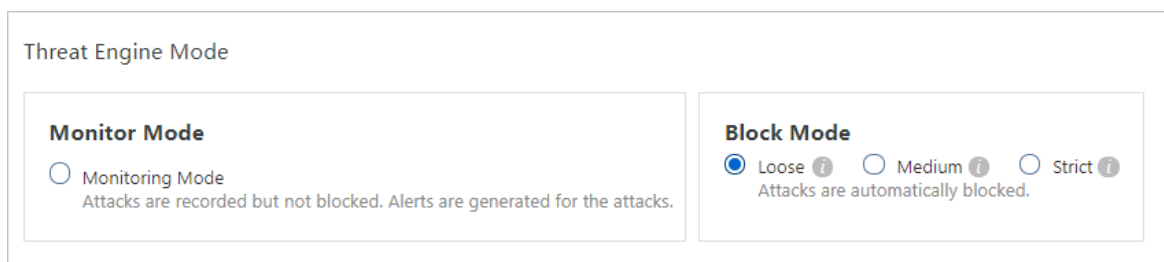
Basic protection: The basic protection feature of Cloud Firewall blocks malicious operations in real time. The operations include system file operations, webshell writing, and the call of stored procedures or user-defined functions (UDFs).

- Data theft and breaches

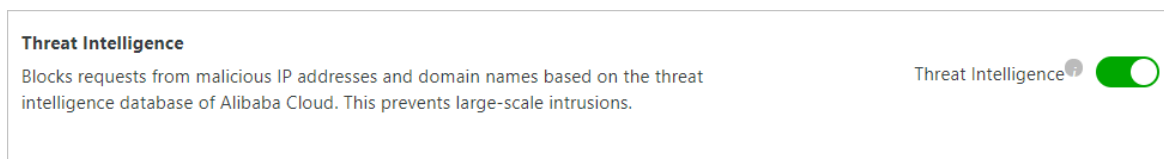
High-risk SQL blocking: The basic protection feature of Cloud Firewall blocks data breach operations in real time to prevent data from being stolen.

Procedure

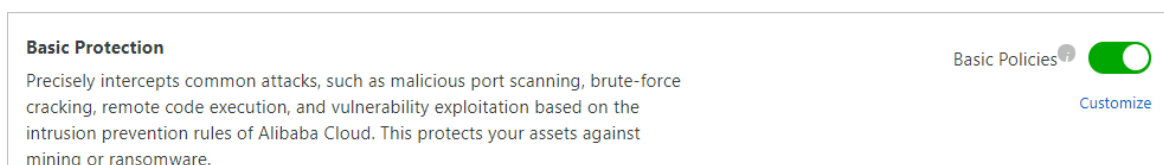
1. Log on to the [Cloud Firewall console](#).
2. In the left-side navigation pane, choose **Intrusion Prevention > Prevention Configuration**.
3. On the **Prevention Configuration** page, select **Loose** for Block Mode in the **Threat Engine Mode** section.



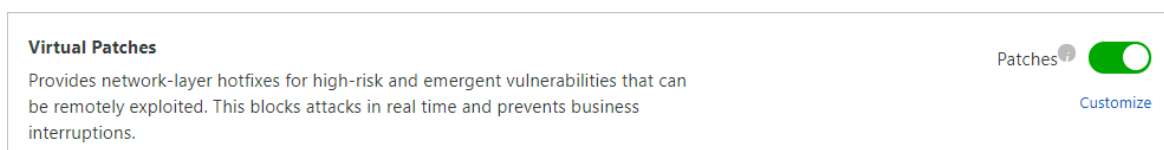
4. Turn on **Threat Intelligence** in the **Threat Intelligence** module of the Advanced Settings section.



5. Turn on **Basic Policies** in the **Basic Protection** module of the Advanced Settings section.



6. Turn on **Patches** in the **Virtual Patches** module of the Advanced Settings section.



4. Best practices for system security defense

System security is a key factor to maintain the secure and stable running of services. As the network offensive and defensive confrontation heats up, more and more attack forms emerge, such as large-scale automated attacks, worms, ransomware, mining programs, and Advanced Persistent Threats (APTs). This brings great challenges to system security.

An automatically installed system has the following security flaws, which makes it vulnerable to intrusions:

- Improper system configurations
 - Unnecessary ports opened: Some opened services and applications are unnecessary, which increases the attack surface.
 - Weak passwords: They are vulnerable to brute-force attacks, which causes intrusions into systems.
 - Improper policy configurations: System security policies are weak or not configured.
- System vulnerabilities or necessary patches not installed
 - Command execution vulnerability: This type of vulnerability can be exploited to execute arbitrary commands, which causes intrusions into systems.
 - DoS vulnerability: The system under DoS attacks rejects normal service requests, which results in service interruptions.
 - Data breach vulnerability: Sensitive or confidential data is breached.

Case: RCE vulnerability in Samba

Samba is the software that implements the Server Message Block (SMB) protocol on Linux and UNIX operating systems. It allows computers to share resources such as files and printers with each other.

A remote code execution (RCE) vulnerability is detected in Samba. This vulnerability allows a client to upload a specific library file to a writable shared directory on a server, which causes the server to load and execute the library file.

CVE: CVE-2017-7494

Impact scope:

- Linux or UNIX operating system on which Samba is installed
- Samba versions: 4.6.4, 4.5.10, and 4.4.14.

Major impact:

- Command execution: Servers are compromised and data is breached due to remote code execution.
- Service interruption: A worm, named SambaCry, can exploit this vulnerability and spread. This worm mines cryptocurrency on compromised servers, which occupies a large number of computing resources on the servers. This may affect service availability or cause service interruptions.

Case: RCE vulnerability in an SMB server

The SMB server is a server protocol component that is automatically installed on Windows operating systems. An RCE vulnerability is detected on the SMB server. This vulnerability allows an attacker to send specially crafted packets to the SMBv1 server and remotely execute code.

CVE: CVE-2017-0143

Impact scope:

- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 Gold
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2008 R2 SP1
- Microsoft Windows Server 2008 SP2

Major impact:

- Command execution: Servers are compromised and data is breached due to remote code execution.
- Data loss: Worms, such as WannaCry, can exploit this vulnerability and spread. These worms encrypt files on compromised servers and cause data breaches.

How to use Cloud Firewall to prevent intrusions into systems

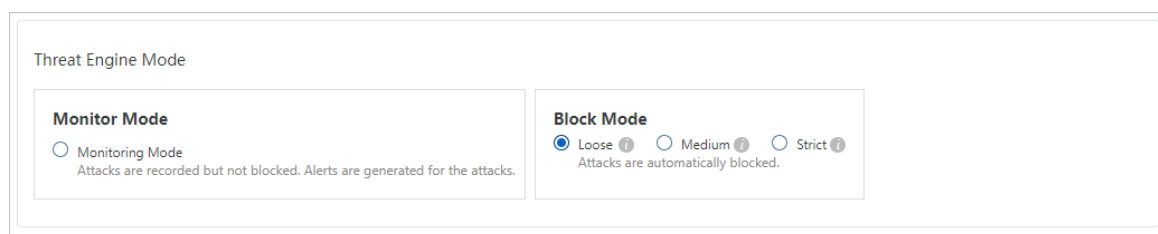
The Alibaba Cloud security team continuously tracks and studies system vulnerabilities and their preventive measures, and has accumulated rich experience in intrusion prevention. The prevention rules formulated based on the experience greatly enhance the system security defense of Cloud Firewall.

To ensure that the system can run as expected, Cloud Firewall provides multi-point prevention against all the risks that the system encounters.

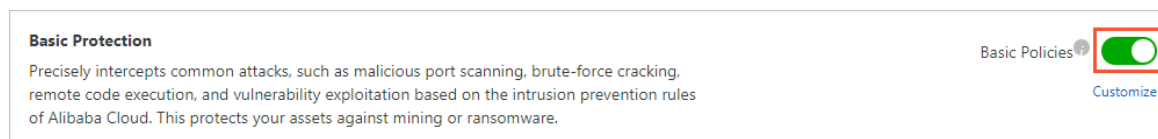
- **Brute-force attacks:** The threat intelligence feature of Cloud Firewall can detect network-wide attacks and block scans or intrusions in advance.
- **System vulnerabilities:** Cloud Firewall prevents high-risk vulnerabilities of operating systems.
- **Other attacks:** The basic protection feature of Cloud Firewall detects other system attacks, such as a reverse shell and system file breach, and blocks them in real time.

Procedure

1. Log on to the .
2. In the left-side navigation pane, choose **Intrusion Prevention > Prevention Configuration**.
3. In the **Threat Engine Mode** section of the **Prevention Configuration** page, select an option for **Block Mode**.



4. In the **Basic Protection** section of the **Prevention Configuration** page, turn on **Basic Policies**.




5. In the **Virtual Patches** section of the **Prevention Configuration** page, turn on **Patches**.

Virtual Patches

Provides network-layer hotfixes for high-risk and emergent vulnerabilities that can be remotely exploited. This blocks attacks in real time and prevents business interruptions.

Patches




[Customize](#)

5. Configure the access control policy that only allow access to a certain port of outbound to inbound traffic

The outbound-inbound traffic and inbound-outbound traffic of Alibaba cloud firewall refer to Internet-oriented traffic, known as north-south traffic. You can customize the access control policy for north-south traffic via Alibaba cloud firewall access control feature, to precisely control the access traffic and to protect your network security.

Context

For example, an ECS (host) IP address is 10.1.1.1, and the EIP is 200.2.2.2, you shall set that only the TCP 80 port of the host can be accessed by outbound to inbound traffic.


 **Note** Elastic IP Address (EIP) is a public IP address resource that can be independently purchased and owned. For more information of EIP, refer to [What is an EIP?](#).

Steps

Access control of outbound-inbound traffic and inbound-outbound traffic allows simplified configuration process of customized IP address book. It can effectively reduce the number of policies and improve configuration efficiency.

1. On Alibaba cloud firewall console, position to **Outbound-inbound traffic** tab in **Access control** tab.
2. Configure the TCP 80 port of host that allows to be accessed by outboard-inbound traffic.
 - In the new outbound-inbound policy, select **IP** for **Origin type**, and enter `0.0.0.0/0` for **Access origin**.
 - For **Destination type**, select **IP**. Enter `200.2.2.2/32` as **Destination**.
 - For **Protocol type**, select **TCP**.
 - For **Destination port**, enter `80/80`.
 - For **Application**, select **ANY**.
 - For **Action**, select **Release**.
 - Enter **description**. We recommend that you enter a description of the policy and its purpose.
3. Configure the outbound-inbound access control policy that rejects all external traffic to the host.
 - In the new outbound-inbound policy, for **Origin type**, select **IP**, and for **Access origin** enter `0.0.0.0/0`.
 - For **Destination type**, select **IP**. Enter `0.0.0.0/0` as **Destination**.
 - For **Protocol type**, select **ANY**.
 - For **Destination port**, enter `0/0` to refer to all ports.
 - For **Application**, select **ANY**.

- For **Action**, select **Reject**.
 - Enter **description**. A description of the policy and its objective are recommended here.
4. Once the policy configuration is complete, confirm the first **Release port 80** Policy priority is higher than the Second Configuration **Reject all traffic** of policy.

 **Note** To adjust priority of the policy, refer to [Change the priority of an access control policy](#).

What to do next

Once the access control policy configuration is complete, you can use the number of hits in **Access control** page to observe the condition of hits. In **Traffic log** page, you can view hits done by the policy.

Log Audit

Event Logs

Traffic Logs

Operation Logs

Access Control / Source: 47.254.213.49/32 / Destination: China Region... / Description: region_test / Policy Action: Deny

Show Advanced Search | List Configuration

Internet Firewall

Source IP

Enter a keyword.

Destination IP

Enter a keyword.

Application

Sep 10, 2019 09:55 - Sep 17, 2019 09:55

Search


Time	Source IP	Destination IP	Destination Port	Direction	Application	Protocol	Policy Action	Bytes	Packets	Policy Name	Actions
From: Sep 12, 2019, 16:41:57 To: Sep 12, 2019, 16:43:40			80	Outbound	HTTP	TCP	Discard	437 B	4	region_test	Obtain Attack Sample
From: Sep 12, 2019, 16:12:52 To: Sep 12, 2019, 16:12:54			80	Outbound	HTTP	TCP	Monitor	1.22 KB	12	region_test	Obtain Attack Sample

6. Create an outbound access control policy to allow traffic destined only for a domain name

In Cloud Firewall, inbound and outbound traffic is also known as north-south traffic or Internet traffic. You can create custom access control policies in the Cloud Firewall console to control north-south traffic. After you create access control policies, Cloud Firewall implements precise access control to ensure network security.

Background information


Assume that you want to create an outbound access control policy to allow traffic from an Elastic Compute Service (ECS) instance to the domain name `www.aliyundoc.com`. The IP address of the ECS instance is `10.1.X.X` and the elastic IP address (EIP) `47.100.X.X`.

 **Note** An EIP is a public IP address that you can purchase and use as an independent resource. For more information about EIPs, see [What is an EIP?](#).

Procedure

1. Log on to the [Cloud Firewall console](#). On the **Access Control** page, click the **Internet Firewall** tab. On the **Internet Firewall** tab, click the **Outbound Policies** tab.
2. On the **Outbound Policies** tab, click **Create Policy**. In the **Create Outbound Policy** dialog box, create the first outbound access control policy to allow the ECS instance to access only the domain name `www.aliyundoc.com`.
 - Set **Source Type** to **IP** and enter `47.100.X.X/32` for **Source**.
 - Set **Destination Type** to **Domain Name** and enter `www.aliyundoc.com` for **Destination**.
 - Set **Protocol** to **TCP**.
 - Set **Port Type** to **Ports** and enter `0/0` for **Ports**.
 - Set **Application** to **HTTP** or **HTTPS** based on the type of the destination domain name.
 - Set **Policy Action** to **Allow**.
 - Configure **Description**. We recommend that you enter the description and purpose of the policy.
3. On the **Outbound Policies** tab, click **Create Policy**. In the **Create Outbound Policy** dialog box, create the second outbound access control policy to allow Domain Name System (DNS) resolution traffic.
 - Set **Source Type** to **IP** and enter `47.100.X.X/32` for **Source**.
 - Set **Destination Type** to **IP** and enter `0.0.0.0/0` for **Destination**.
 - Set **Protocol** to **UDP**.
 - Set **Port Type** to **Ports** and enter `53/53` for **Ports**.
 - Set **Application** to **ANY**.

- Set **Policy Action** to **Allow**.
 - Configure **Description**. We recommend that you enter the description and purpose of the policy.
4. On the Outbound Policies tab, click **Create Policy**. In the Create Outbound Policy dialog box, create the third outbound access control policy to **deny** traffic from all sources.
- Set **Source Type** to **IP** and enter `0.0.0.0/0` for **Source**.
 - Set **Destination Type** to **IP** and enter `0.0.0.0/0` for **Destination**.
 - Set **Protocol Type** to **ANY**.
 - Set **Port Type** to **Ports** and enter `0/0` for **Ports**.
 - Set **Application** to **ANY**.
 - Set **Policy Action** to **Deny**.
 - Configure **Description**. We recommend that you enter the description and purpose of the policy.
5. After you create the access control policies, make sure that the priorities of the first and the second policies are higher than the priority of the third policy that denies access from all sources.

 **Note** For more information about how to change the priority of an access control policy, see [Change the priority of an access control policy](#).

What to do next

After you create the access control policies, you can view the number of times that access traffic hits the policies on the **Access Control** page. You can also view the access traffic that hits a policy on the **Traffic Logs** tab.

7.Best practices to defend against unauthorized access to a MongoDB database

Unauthorized access to a MongoDB database can result in data leaks, data deletion, or even extortion.

Context

To ensure the security of your business and applications, Cloud Firewall provides a solution to fix the vulnerability of unauthorized access to a MongoDB database.

After MongoDB is installed, an admin database is created. The admin database is empty by default. You cannot view user authentication information in the database.

By default, MongoDB has no requirements for user authentication. If you do not configure parameters when you start MongoDB, user authentication is not required for access to the MongoDB database. As a result, users do not require a password to remotely access the MongoDB database. Then, the users can perform operations on the database by using the default port. These operations include high-risk operations that are performed to insert, delete, modify, or query data.

To address this issue, you must add users to the admin.system.users collection. This way, user authentication is enabled for MongoDB.

Solution

1. Configure access control policies in Cloud Firewall.

i. Configure MongoDB to make sure that MongoDB provides services only for servers on an internal network.

Log on to the Cloud Firewall console and choose **Traffic Analysis > Internet Access**. On the Internet Access page, click the **Open Applications** tab and check whether MongoDB communicates with the Internet. If MongoDB provides services only for servers on an internal network, we recommend that you configure MongoDB to prevent MongoDB from being exposed to the Internet.

Run the following command to bind MongoDB to an IP address to make sure that MongoDB provides services only for servers on an internal network. In this example, bind MongoDB to the internal IP address 192.168.XX.XX.

```
mongod --bind_ip 192.168.XX.XX
```

ii. Allow requests only from trusted source IP addresses.

In the Cloud Firewall console, choose **Access Control > Access Control**. On the Access Control page, click the **Internet Firewall** tab and then click the **Inbound Policies** tab. On the Inbound Policies tab, configure an access control policy to allow requests only from trusted source IP addresses to MongoDB.

- a. On the **Inbound Policies** tab, click **Address Books**. On the **IPv4 Address Books** tab, create an address book and add all trusted source IP addresses to the address book.
- b. On the **Inbound Policies** tab, click **Create Policy**. In the **Create Inbound Policy** dialog box, configure the parameters. Parameter configurations:
 - **Source**: Select the address book that you create.
 - **Destination**: Enter the public IP address of the server on which MongoDB is installed.
 - **Protocol**: Select TCP, which specifies Internet traffic.
 - **Port**: Set this parameter to 0/0, which specifies all ports for the trusted source IP addresses.
 - Configure other parameters as prompted.

iii. Deny all requests from untrusted source IP addresses.

In the Cloud Firewall console, choose **Access Control > Access Control**. On the Access Control page, click the **Internet Firewall** tab and then click the **Inbound Policies** tab. On the Inbound Policies tab, configure an access control policy to deny all requests from untrusted source IP addresses.

On the **Inbound Policies** tab, click **Create Policy**. In the **Create Inbound Policy** dialog box, configure the parameters. Parameter configurations:

- **Source**: Set this parameter to 0.0.0.0/0, which specifies all source IP addresses.
- **Destination**: Enter the public IP address of the server on which MongoDB is installed.
- **Protocol Type**: Select TCP, which specifies Internet traffic.
- **Port**: Set this parameter to 0/0, which specifies all ports for untrusted source IP addresses.
- Configure other parameters as prompted.


2. Enable role-based user authentication.

- i. Log on to MongoDB. Make sure that user authentication is disabled when you run the following command:


```
[mongodbrac3 bin]$ ./mongo 127.0.0.1:27028 (The default port is changed.)
MongoDB shell version: 2.0.1
connecting to: 127.0.0.1:27028/test
```

- ii. Switch to the admin database.

```
> use admin
switched to db admin
```


 **Note** An administrator account can be created only in the admin database.

- iii. Create an administrator account in the admin database. In this example, the username is *supper*, and the password is *supWDxsf67%H*.

 **Note** In MongoDB V3 and later, the `addUser` method is no longer supported. You can run the `db.createUser` command to create a user.

```
> db.addUser("supper", "supWDxsf67%H") or
{ "n" : 0, "connectionId" : 4, "err" : null, "ok" : 1 }
> db.createUser({user:"****",pwd:"*****",roles:["root"]})
{
  "user" : "****",
  "readOnly" : false,
  "pwd" : "*****", "_id"
ObjectId("4f2bc0d357a309043c6947a4")
}
# Store the administrator account in the system.users collection.
> db.getCollectionNames()
[ "system.indexes", "system.users", "system.version" ]
```

The administrator account is stored in the *system.users* collection.

 **Note** The username cannot be a common username. The password must meet the following requirements: The password must be at least eight characters in length and must contain uppercase letters, lowercase letters, digits, and special characters. The password cannot be a common password, such as a birth date, a name, or an ID card number.

- iv. Check whether the administrator account is created.

Run the following command. If 1 is returned, the administrator account is created.

```
> db.auth("supper","supWDxsf67%H")
1
```

- v. Terminate the Mongod process and restart MongoDB.

```
> db.auth("supper","supWDxsf67%H")
> exit
bye
```

- vi. Enable user authentication.

After user authentication is enabled, users who are not logged on to MongoDB cannot perform operations.

```
> mongod --dbpath=/path/mongod --bind_ip=10.0.0.1 --port=27028 --fork=true logpath
=/path/mongod.log --auth&
```

? Note

- Users that are stored in the `admin.system.users` collection have super permissions, but users that are created in other databases do not. Users that are created in the `admin` database can perform operations on data in other databases in MongoDB.
- In MongoDB, a database is created by a superuser. A database can contain multiple users, but a single user can be stored only in one database. Users in different databases can share the same name.
- User1 in a database, such as DB1, cannot access a different database, such as DB2, but can access data created by other users in DB1.
- Users who share the same name in different databases can log on to only one database. For example, if user1 exists in both DB1 and DB2 and logs on to DB1, user1 cannot log on to DB2.
- Users created in the `admin` database have super permissions and can perform operations on data in all databases in MongoDB.
- You can use the `db.auth()` method to authenticate users in a database. If the authentication is successful, a value of 1 is returned. Otherwise, a value of 0 is returned. The `db.auth()` method can authenticate only the users in the database to which the current logon user belongs. The method cannot authenticate users in other databases.

Check for intrusions

If you are a MongoDB administrator, you can take the following measures to check for intrusions:

- Check whether the MongoDB log is complete. Then, check the IP address of the user who deletes the database and the time when the database was deleted.
- Run the `db.system.users.find()` command to check whether a password is configured for each MongoDB account.
- Run the `db.fs.files.find()` command to check whether other users store files by using GridFS.
- Run the `show log global` command to view log files. Then, check whether other users access the MongoDB database.

8. Best practices to protect bastion hosts

You can use the features of Cloud Firewall to protect your bastion host. The features include access control, intrusion prevention system (IPS), and network traffic analysis. This way, you can manage the public IP addresses that communicate with your bastion host in a centralized manner and protect your bastion host.


Recommended configurations

The following list describes the recommended configurations for Cloud Firewall to protect a bastion host:

1. Configure **inbound** policies for the Internet firewall to allow access to the open ports of a bastion host from the Internet globally or the Internet in specified regions.
2. Configure **outbound** policies for the Internet firewall to allow a bastion host to access the Internet.
3. Enable the Internet firewall for the bastion host so that inbound traffic and outbound traffic of the bastion host all pass through Cloud Firewall.

Procedure


1. Log on to the [Cloud Firewall console](#).
2. In the left-side navigation pane, choose **Access Control > Access Control**.
3. On the **Internet Firewall** tab of the **Access Control** page, configure **inbound policies** to allow access to the open ports of the bastion host from the Internet globally or the Internet in specified regions.
 - i. Click the **Inbound Policies** tab.
 - ii. (Optional) Click **Address Books**. In the dialog box that appears, click the **Port Address Books** tab. Then, click **Create Address Book**.

 **Note** You can add multiple IP addresses or ports to an address book for batch operations, which simplifies your configuration. If you want to open only one port of the bastion host, you do not need to create an address book.

- iii. In **Create Port Address Book**, add the bastion host ports that you want to open.

In this example, ports 60022 (SSH), 63389 (RDP), and 443 (bastion host O&M) need to be opened. You can add ports to a **port address book** based on your business requirements. Separate multiple ports with commas (.). You can add up to 50 ports.

- iv. Create an **inbound** policy to allow access to the specified ports of the bastion host from the Internet.

Parameter	Description
Source Type	Select <i>IP</i> .
Source	To allow all public IP addresses to access the open ports of the bastion host, enter <i>0.0.0.0/0</i> . To allow some public IP addresses to access the open ports of the bastion host, enter the CIDR blocks of these IP addresses.
Destination Type	Select <i>IP</i> .
Destination	Enter the IP address of the bastion host. <div>  Note To view the IP address of the bastion host, log on to the Cloud Firewall console. In the left-side navigation pane, choose Firewall Settings > Firewall Settings. On the Internet Firewall tab, configure Asset Type to search for the IP address of the bastion host. You do not need to log on to the Bastionhost console. </div>
Protocol	Select <i>TCP</i> .
Port Type	To open multiple ports of the bastion host, select Address Book for Port Type and select the address book that you create.
Application	Select ANY .
Policy Action	Select <i>Allow</i> , which indicates that the specified public IP addresses are allowed to access the open ports of the bastion host.
Description	Enter a description for the policy. The description can help you identify the policy.
Priority	Select a priority for the policy. Default value: Lowest . Valid values: <ul style="list-style-type: none"> ▪ Lowest: The policy has the lowest priority. ▪ Highest: The policy has the highest priority.
Enabled	Turn on the switch, which indicates that the policy is enabled.

- v. Create another **inbound** policy to deny access to unopened ports of the bastion host from all public IP addresses.

Ports: Enter *0/0*, which indicates all ports of the bastion host.

Policy Action: Select **Deny**, which indicates that access to the unopened ports of the bastion host from all public IP addresses is denied.

4. Allow the bastion host to access the Internet.

If a bastion host needs to access Alibaba Cloud services over the Internet, an Elastic Compute Service (ECS) instance in a different virtual private cloud (VPC), or a host outside the cloud, you must configure settings to allow the bastion host to access the Internet.

- i. Choose **Access Control > Access Control** and click the **Internet Firewall** tab. Then, click the **Outbound Policies** tab.
 - ii. Click **Create Policy** and configure the parameters.
5. Choose **Firewall Settings > Firewall Settings**. On the **Internet Firewall** tab, find the bastion host for which you want to enable the Internet firewall, and click **Enable Firewall**.

Firewall Settings

Ultimate Edition Cloud Firewall will expire in 8 days at Dec 10, 2021 00:00 AM. [Bandwidth Upgrade](#) [Upgrade](#) [Renew](#) [Auto Renewal](#) [More](#) [Help Documentation](#)

Internet Firewall 1 VPC Firewall

Internet Firewall is not enabled on 1 public IP(s). Please turn them on to prevent threat intrusion. [Enable Firewall](#) [Show](#)

Public IP Unprotected: 1 Protected: 4 Remaining Quota: 401 Increase Quota for Policies	Region Not All IPs Protected: 1 All IPs Protected: 1 View Details	Asset Type Not All IPs Protected: 1 All IPs Protected: 0 View Details
---	---	---

[Enable](#) [Disable](#) [Asset Type](#) [Region](#) [Protection Status](#) [All Accounts](#) [All](#) [Enter an IP address or instance ID](#) [Q](#) [Automatically Enable Firewalls for New Assets](#) [Update Assets](#)

<input type="checkbox"/>	IP	Instance ID/Name	Asset Type	Region	Bound Asset	Default Allow Policy	Firewall Status	Actions
<input type="checkbox"/>	IP: 123.143 UID: 158-2207	i-2-...shnp9 cf-...qa6_0		China (Beijing)		Not Applied Apply	Disabled	Enable Firewall

Note A newly purchased bastion host is synchronized to the Cloud Firewall console within 15 to 30 minutes.

References

- [What is Cloud Firewall?](#)
- [Overview of access control policies](#)
- [Enable or disable the Internet firewall](#)

9. Defend against mining programs

This topic describes how to use Cloud Firewall and Security Center to defend against mining worms from the dimensions of prevention, detection, and damage control. In this topic, a cloud-based environment is used.


Edition limits

- Cloud Firewall:

You must use Cloud Firewall Premium Edition, Enterprise Edition, or Ultimate Edition. Cloud Firewall of these editions can detect and defend against mining worms. If you want to use Cloud Firewall to detect and defend against mining worms, you must purchase Premium Edition, Enterprise Edition, or Ultimate Edition. For more information, see [Purchase Cloud Firewall](#).

- Security Center:

The features supported by Security Center vary based on the editions of Security Center. For more information, see [Features](#).

 **Note** Cloud Firewall provides a 7-day free trial of Premium Edition for users of Free Edition. For more information, see [Apply for a free trial of Cloud Firewall](#).

Characteristics of mining programs

- Mining programs can overclock the CPU, which consumes a large number of CPU resources and affects other applications that run on your server.
- The characteristics of mining programs are similar to the characteristics of computer worms. After a mining program intrudes into your server, the mining program spreads to the servers that are deployed in the same internal network. After the servers are compromised, the mining program achieves persistence on the servers.
- In most cases, mining programs spread to multiple system services and are difficult to remove from the system. Mining programs may repeatedly appear, and system commands may be replaced with malicious scripts. As a result, the system may run malicious scripts such as XOR DDoS. You must remove all trojans and persistent webshells from your server within the execution period of mining programs. This way, mining programs are prevented from appearing in the future.

How do mining worms spread?

The 2018 Cryptocurrency Mining Hijacker Report released by the Alibaba Cloud security team shows that the occurrence of common zero-day vulnerabilities was accompanied by the outbreak of mining worms. Mining worms occupy system resources, which may cause service interruption. Some mining worms, such as Xbash, may also be bundled with ransomware. This type of mining worm can result in economic and data loss for enterprises.

The Alibaba Cloud security team analyzes mining programs and concludes that the mining worms in the cloud exploit the following network vulnerabilities to spread:

- Common vulnerabilities

Mining worms exploited common vulnerabilities in network applications, such as configuration errors, weak passwords, and brute-force attacks by using SSH, Remote Desktop Protocol (RDP), and Telnet, to continuously scan the Internet, launch attacks, and compromise hosts.

- Zero-day and N-day vulnerabilities

Mining worms also exploited zero-day and N-day vulnerabilities to compromise a large number of hosts before the vulnerabilities are fixed.

Solutions to defense against mining worms

Protection phase	Solution	References
Before intrusion	Configure access control policies in the Cloud Firewall console to allow traffic only from authorized addresses.	To allow traffic only from authorized IP addresses, you can create outbound access control policies on the Outbound Policies tab of the Internet Firewall tab. For more information, see Access control policies .
	Enable the block mode in the Threat Engine Mode section in the Cloud Firewall console to block mining activities at the earliest opportunity.	For more information, see Use Cloud Firewall to defend against mining worms .
	Use the intrusion prevention feature of Cloud Firewall to detect and block attack traffic in an efficient manner.	For more information, see Intrusion prevention .
	Use the antivirus feature of Security Center to automatically block common viruses, malicious network connections, and webshell connections. The feature prevents mining activities on Elastic Compute Service (ECS) instances.	For more information, see Overview .
	Handle alerts in the Security Center console. You can check whether mining programs and connection to mining pools exist in ECS instances.	For more information, see View and handle alerts .
	Use the breach awareness feature of Cloud Firewall to detect mining worms.	You can find specific events and addresses that initiated outbound connections in the event list of the Breach Awareness page. For more information, see Use Cloud Firewall to detect mining worms .
	Use the intrusion prevention feature to control the damages of intrusions.	You can block downloads of malicious files by turning on Basic Policies on the Intrusion Prevention page. For more information, see How do I use Cloud Firewall to immediately control the damages of mining worms? .

Protection phase	Solution	References
During intrusion	Create access control policies in the Cloud Firewall console to deny connections of mining programs.	You can create outbound access control policies to allow traffic from trusted public IP addresses and deny access to addresses of mining pool.
	Use the best practices of Cloud Firewall based on ATT&CK.	Cloud Firewall provides various features for different ATT&CK stages. The features include basic protection, virtual patching, and threat intelligence. You can use the features to harden the security of your network. For more information, see Best practices of Cloud Firewall based on ATT&CK .
After intrusion	Use Security Center to track attacks that are launched by exploiting mining viruses.	For more information, see Use attack source tracing .

Use Cloud Firewall to defend against mining worms

Cloud Firewall detects and blocks malicious inbound and outbound network traffic in the cloud in real time to defend against mining worms.

- Defense against mining worms that exploit common vulnerabilities

Some mining worms launch brute-force attacks by exploiting vulnerabilities such as SSH and RDP vulnerabilities. To defend against these worms, Cloud Firewall provides the basic protection feature. This feature supports common methods to detect brute-force attacks. For example, the feature calculates the threshold for the logon retry attempts and limits the IP addresses from which the number of logon retry attempts exceeds the threshold. The feature also analyzes user access habits and frequency to ensure that normal access requests are allowed and abnormal requests are denied based on behavior models.

This feature takes advantage of the big data capabilities provided by Alibaba Cloud and generates precise defense rules based on the malicious attack samples accumulated in attack and defense by the Alibaba Cloud security team. This way, the feature can protect your assets against other worms that exploit common vulnerabilities, such as write of crontab commands to Redis and UDF-based command execution in databases.

You can enable basic protection to defend against mining worms that exploit common vulnerabilities.

To enable basic protection, perform the following steps:

- i. Log on to the [Cloud Firewall console](#).
- ii. In the left-side navigation pane, choose **Intrusion Prevention > Prevention Configuration**.
- iii. On the **Prevention Configuration** page, turn on the switch for **Threat Intelligence** in the **Threat Intelligence** section.
- iv. On the **Prevention Configuration** page, turn on the switch for **Basic Policies** in the **Basic Protection** section.
- v. In the left-side navigation pane, choose **Intrusion Prevention > Intrusion Prevention** to view the detailed blocking logs in the **Detailed Data** section.

Detailed Data							
All Risk Levels	All Modes	All Attack Types	All Attacked A...	All Directions	All Modules	2021-06-28 14:08:10	2021-07-05 14:08:10
Source IP	Enter a keyword.		Search				
Occurred At	Source IP	Destination IP	Event Name/Attack Type/Direction/Module	Events/Risk Level	Mode	Actions	
Last Time: Jul 5, 2021, 13:59:00 First Time: Jun 28, 2021, 15:00:00	Public: 47 Private: 192.168.1.1	ECS Public IP Public: 94 Lithuania	Mining behavior on the host Mining Behavior Outbound Basic Protection	58378 High	Blocked	View Details	
Last Time: Jul 5, 2021, 13:59:00 First Time: Jun 28, 2021, 15:00:00	Public: 47 Private: 192.168.1.1	ECS Public IP Public: 153 Japan	Mining behavior on the host Mining Behavior Outbound Basic Protection	20744 High	Blocked	View Details	
Last Time: Jul 5, 2021, 13:59:00 First Time: Jun 28, 2021, 15:00:00	Public: 47 Private: 192.168.1.1	ECS Public IP Public: 136 Germany	Mining behavior on the host Mining Behavior Outbound Basic Protection	16941 High	Blocked	View Details	

- Defense against mining worms that exploit zero-day and N-day vulnerabilities

If common zero-day and N-day vulnerabilities are not fixed at the earliest opportunity, these vulnerabilities are likely to be exploited by mining worms. Cloud Firewall analyzes attack traffic by using honeypots deployed across the network and obtains vulnerability intelligence from the Alibaba Cloud Crowdsourced Security Testing platform. This way, Cloud Firewall can promptly detect zero-day and N-day vulnerabilities, obtain the proofs of concept (POCs) and exploits of these vulnerabilities, and generate virtual patches in advance.

You can enable virtual patching to defend against mining worms that exploit zero-day and N-day vulnerabilities.

To enable virtual patching, perform the following steps:

- Log on to the [Cloud Firewall console](#).
- In the left-side navigation pane, choose **Intrusion Prevention > Prevention Configuration**.
- On the **Prevention Configuration** page, turn on the switch for **Patches** in the **Virtual Patches** section.
- Click **Customize** below the switch for **Patches**. In the **Customize Virtual Patches Policies** dialog box, view or manage the virtual patches that are enabled.

Customize Virtual Patches Policies

All IPS Polic...All Risk Lev...All Attack Ty...All VictimsAll Current ...All Rule Gr...Rule IDQ

Restore Default IPS Policies

<input type="checkbox"/>	Rule ID	Policy Name	Update Time	Description	Risk Level	CVE ID	Attack Type	Victim	Rule Group	Default Action	Current Action
<input type="checkbox"/>	20000887	Highly Focused	Apr 30, 2021, 15:36:37	...	Medium	CVE-2020-1938	Command Execution	Apache Tomcat	Loose	Block	Monitor
<input type="checkbox"/>	10000049	Highly Focused	Elasti...	Feb 7, 2021, 19:56:27	...	Medium	CVE-2014-3120	Command Execution	ElasticSearch	Loose	Block
<input type="checkbox"/>	10003030	Highly Focused	Arbit...	Feb 7, 2021, 19:53:42	...	Medium	-	Web Attacks	ThinkPHP	Loose	Block
<input type="checkbox"/>	10003031	Highly Focused	Arbit...	Feb 7, 2021, 20:00:39	...	Medium	-	Web Attacks	ThinkPHP	Loose	Block
<input type="checkbox"/>	10000039	Adobe ColdFusion re...	Apr 30, 2021, 15:26:40	...	Medium	CVE-2017-3066	Command Execution	Adobe ColdFusion	Loose	Block	Block

☐ Selected 0 PoliciesMonitorBlockDisableRestore Default

< Previous1234...18Next >

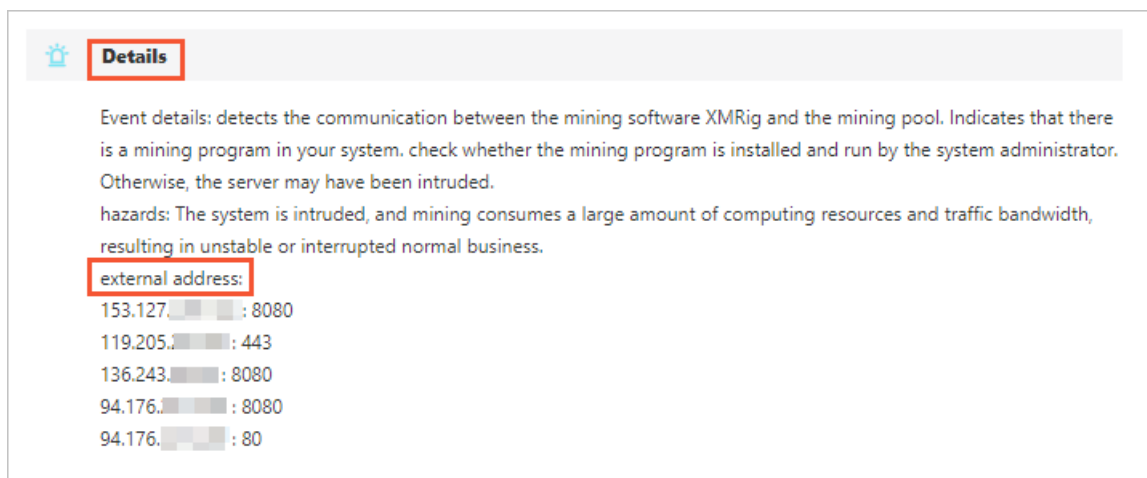
Use Cloud Firewall to detect mining worms

Even if the Internet firewall is enabled to prevent intrusions, hosts may still be vulnerable to mining worms. Mining worms can spread from a development machine to a production network over a VPN. If the system images and Docker images used for O&M are inserted with mining viruses, a large number of hosts may be compromised.

Cloud Firewall uses Network Traffic Analysis (NTA) to provide the breach awareness feature. This feature can detect host intrusion events in a timely and efficient manner. Cloud Firewall uses a powerful threat intelligence network to identify the mining pool addresses of common cryptocurrencies and the common communication protocols of mining pools, and detect the downloads of mining trojans. In addition, Cloud Firewall can identify the mining behavior of hosts in real time and promptly generate alerts.

You can turn on **Auto Blocking** on the **Breach Awareness** page to enable Cloud Firewall to detect mining worms and block the communication between mining trojans and mining pools on the network. To turn on Auto Blocking, perform the following steps:

1. Log on to the [Cloud Firewall console](#).
2. In the left-side navigation pane, choose **Intrusion Prevention > Breach Awareness**.
3. On the **Breach Awareness** page, find an event related to a mining program and click **Details** in the **Actions** column.



You can view the address that initiated outbound connections in the **Details** panel.

4. Log on to the server on which the mining program is detected, find the mining program, and then remove the program.

How do I use Cloud Firewall to immediately control the damages of mining worms?

If a host is compromised by mining worms, Cloud Firewall can use the following methods to prevent the spread of these worms and reduce economic and data loss. The methods are to block malicious file downloads, intercept the communication between command and control (C&C) servers and mining worms, and enable enhanced access control for critical business.

- Block malicious file downloads

In most cases, after hosts are compromised by mining worms, the hosts download malicious files. Basic protection is integrated with malicious file detection and dynamically updates the unique characteristics codes and fuzzy hashes of malicious files for common mining worms. After the mining worms intrude into your host, your host may further download updated malicious payloads. In this case, basic protection performs security checks on the files downloaded to your host. The checks include file restoration and characteristics matching. If an attempt to download a malicious file is detected, an alert is generated, and the download is blocked.

<input type="checkbox"/>	Rule ID	Policy Name	更新时间	Description	Risk Level	CVE ID	Attack Type	Victim	规则组	Default Action	Current Action
<input type="checkbox"/>	100030	Activemq malicious fil...	Feb 8, 2021, 13:52:12	...	High	CVE-2016-3088	Command Execution	Apache ActiveMQ	Loose	Block	Block ▼
<input type="checkbox"/>	300000	IRC backdoor commu...	Apr 30, 2021, 15:35:11	...	High	-	Trojan Backdoor	Backdoor	Loose	Block	Block ▼

You can turn on the switch for **Basic Policies** in the Virtual Patches section of the **Prevention Configuration** page to block malicious file downloads.

- Intercept communication between C&C servers and mining worms

After C&C servers are compromised by mining worms, the C&C servers may leak sensitive data or receive malicious instructions from mining worms. In this case, basic protection intercepts the communication between the worms and C&C servers by using the following methods:

- Basic protection dynamically monitors and analyzes the data related to mining worms across the network and the communication traffic of the C&C servers. Then, basic protection dynamically extracts the characteristics of unusual communication traffic and forms a mechanism to identify the communication between the mining worms and C&C servers. This way, basic protection ensures the prompt detection of attacks.
- Basic protection learns historical access information and establishes a model to detect unusual traffic and explore potential mining worm information.
- Basic protection uses big data visualization to map access behavior to all IP addresses and uses machine learning to detect suspicious IP addresses and access domains. In addition, a threat intelligence library for C&C servers is formed based on network-wide attack data. This way, basic protection matches host communication traffic with the information in the library to block malicious traffic between C&C servers and mining worms.

The following figure shows the communication interception records between a C&C server and mining worms. The communication is intercepted by basic protection based on threat intelligence.

<input type="checkbox"/>	Rule ID	Policy Name	更新时间	Description	Risk Level	CVE ID	Attack Type	Victim	规则组	Default Action	Current Action
<input type="checkbox"/>	100031	Acunetix WVS scan	Feb 8, 2021, 13:25:29	...	Medium	-	Scan	Acunetix	Loose	Block	Block ▼
<input type="checkbox"/>	100031	Acunetix WVS scan	Apr 30, 2021, 15:35:38	...	Medium	-	Scan	Acunetix	Loose	Block	Block ▼

You can turn on the switch for **Basic Policies** in the Basic Protection section of the **Prevention Configuration** page to intercept the communication between C&C servers and mining worms.

- Enable enhanced access control for critical business

To ensure critical business, enterprises may need to open services or ports to the Internet. However, Internet-based scans and attacks pose security threats to the assets of enterprises, which makes fine-grained control on external access challenging. Outbound connections that are initiated from an ECS instance, elastic IP address, or internal network are usually valid. In these scenarios, the number of domain names or IP addresses is controllable. Cloud Firewall implements access control on these domain names and IP addresses to prevent mining trojans from being inserted into compromised ECS instances by using suspicious domain names and block communication between trojans and C&C servers.

Cloud Firewall allows you to configure access control rules for source IP addresses and domain names, including wildcard domain names. For critical business, you can configure fine-grained access control policies for outbound connections. For example, you can open critical ports only to specific domain names or IP addresses. Fine-grained access control policies effectively prevent the downloads and spread of mining worms. The policies also prevent mining worms from surviving and eliciting malicious actions.

For example, a total of six IP addresses are used for outbound connections on an internal network, all NTP services are identified as Alibaba Cloud services, and the IP address of the DNS server is 8.8.8.8. In this case, you can configure policies to allow outbound connections only from the six IP addresses based on the security suggestions provided by Cloud Firewall. The policies prevent other outbound connections, such as malicious downloads and outbound C&C connections, without affecting normal business access.

Outbound Domains

Outbound IP Addresses

Assets

Total Outbound IP Addresses: 13,366

IP Addresses Not Covered by Policies: 13,366

Risky IP Addresses: 0

IP Addresses Followed: 1

Ignored: 2

All Products

All Categories

All Intelligence Tags

Destination IP

Search

Destination IP	Applications/Ports	Traffic	Sessions	Category	Address Book	Intelligence Tag	Recommended Operation
8.136	Unknown/8300 2	Request Rate: 169.45 KB Response Rate: 135.93 KB	624	-	1234567890	-	Ignore More
120.25	NTP/123 1	Request Rate: 60.16 KB Response Rate: 57.36 KB	560	Alibaba Cloud Products	1234567890	New	Ignore More
94.176	Unknown/8080 3	Request Rate: 317.33 KB Response Rate: 48.47 KB	528	-	1234567890	-	Ignore More

To configure the policies, perform the following steps: In the left-side navigation pane of the Cloud Firewall console, choose **Access Control > Access Control**. On the Access Control page, click the **Internet Firewall** tab and then the **Outbound Policies** tab. Then, configure policies to allow outbound connections that are initiated only from the authorized IP addresses.

Mining worms spread on a large scale because of the persistence of common application vulnerabilities on the Internet, frequent occurrence of zero-day vulnerabilities, and highly efficient monetization of mining activities. Customers whose workload is deployed on the cloud can transparently access Cloud Firewall to protect their applications against various attacks on the Internet. Cloud Firewall relies on strong cloud computing power to perceive the latest attack threats and connects to a threat intelligence network to provide optimal security protection from mining worms. Cloud Firewall can also be scaled out as your business grows. This way, you can focus more on your business expansion.

10.Import the traffic logs of Cloud Firewall to a third-party system

The traffic logs of Cloud Firewall Premium Edition, Enterprise Edition, and Ultimate Edition can be collected by using Log Service. You can use the log analysis feature of Cloud Firewall to export traffic logs and import the logs to a third-party system.

Cloud Firewall supports the traffic logs of the Internet firewall and virtual private cloud (VPC) firewalls. You can use the log analysis feature of Cloud Firewall to export traffic logs and import the logs to your business system, such as your O&M center.



Note


Prerequisites

The log analysis feature is purchased and enabled. For more information, see [Enable the log analysis feature](#) and [Specifications and pricing for log storage in Cloud Firewall](#).

Export methods

You can use Log Service or the log analysis feature of Cloud Firewall to export logs.

- Export a small amount of log data

Log on to the . In the left-side navigation pane, choose **Log Analysis > Log Analysis**. On the **Log Analysis** page, click the **Logs** tab. On the Logs tab, click the  icon to download a log file. Then, upload the log file to a third-party system.

- Export a large amount of log data

Log on to the [Log Service console](#) and use programming methods to export log data.

For more information about operations in Log Service, see [Use consumer groups to consume log data](#).



Note If Log Service is not activated, Log Service is automatically activated when you enable the log analysis feature of Cloud Firewall.

Specifications and pricing for log storage in Cloud Firewall

The log analysis feature of Cloud Firewall provides scalable log storage. The following table describes the specifications and pricing for log storage.

Log storage duration	Log storage capacity	Monthly bandwidth	Recommended edition	Cloud Firewall instance in mainland China	
				Monthly subscription	15% discount for annual subscription

Log storage duration	Log storage capacity	Monthly bandwidth	Recommended edition	Cloud Firewall instance in mainland China	
				Monthly subscription	15% discount for annual subscription
180 days	1 TB	Up to 10 Mbit/s	Premium Edition	USD 80	USD 861
	5 TB	Up to 50 Mbit/s	Enterprise Edition	USD 400	USD 4,080
	20 TB	Up to 200 Mbit/s	Ultimate Edition	USD 1,600	USD 16,320

For more information about the log storage, see [Manage log storage](#).

11. Block access from regions outside China

If you want to block access to your assets from regions outside China, you can go to the Cloud Firewall console and configure an access control policy. This topic describes how to configure a policy to block access from regions outside China in the Cloud Firewall console.

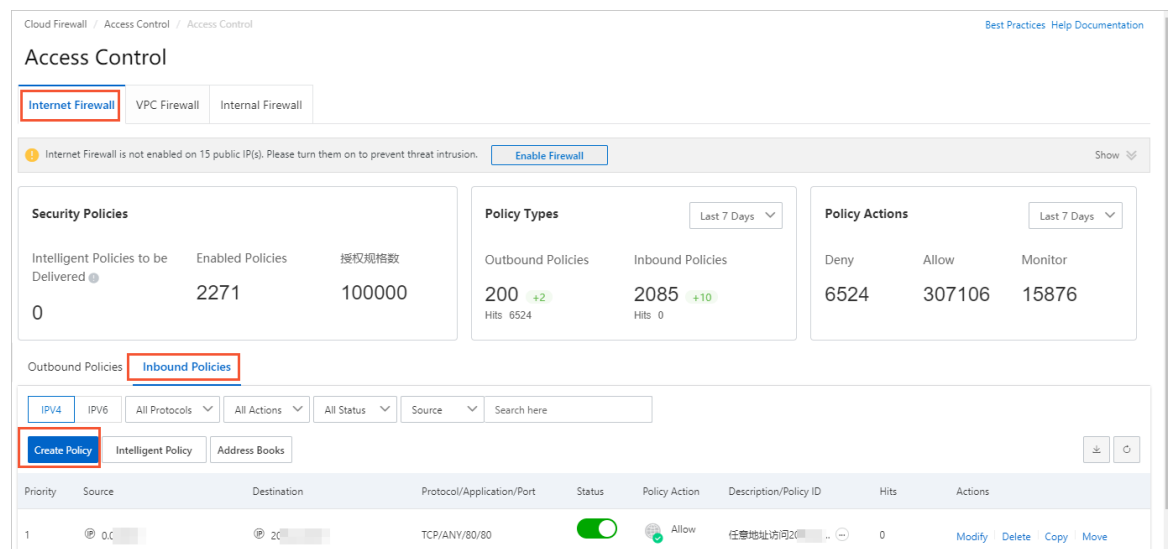
Prerequisites

Context

On the **Internet Firewall** tab, you must create an inbound access control policy. When you create the policy, set **Source Type** to **Region**, select **Regions Outside China**, and then set **Policy Action** to **Deny**.

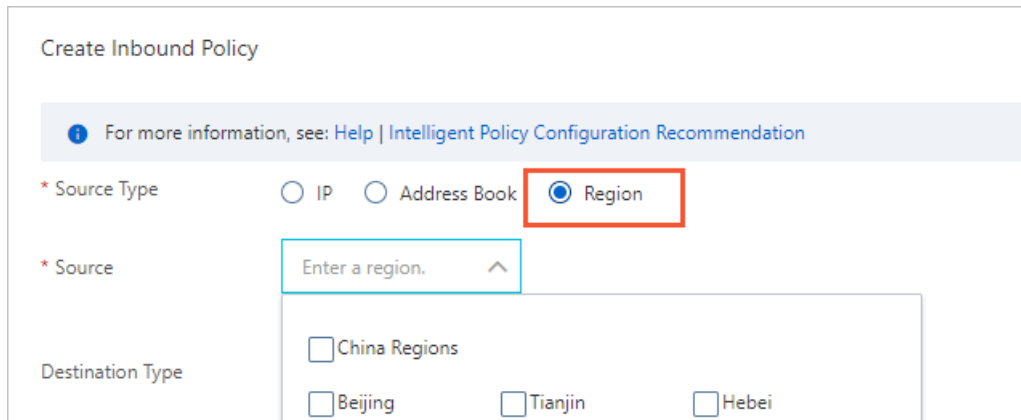
Create an access control policy

1. .
2. In the left-side navigation pane, choose **Access Control > Access Control**.
3. On the **Internet Firewall** tab, click **Inbound Policies**.
4. On the **Inbound Policies** tab, click **Create Policy**.

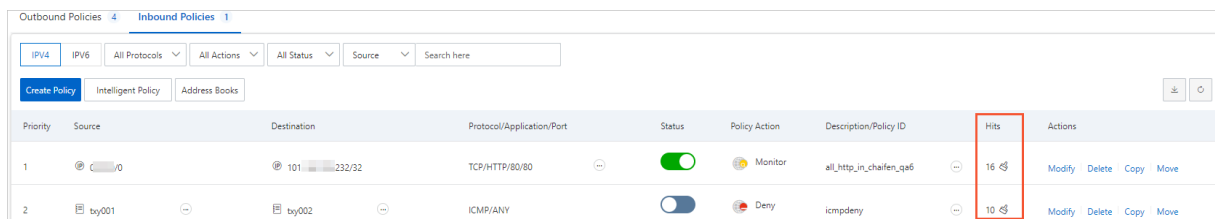


5. In the **Create Inbound Policy** dialog box, configure the parameters and click **Submit**.

Set **Source Type** to **Region**. Then, set **Source** to **Regions Outside China** and **Policy Action** to **Deny**. The following figure provides an example.



In the access control policy list, if the number in the **Hits** column is greater than 0 for an access control policy, access traffic hits the policy. The number in the **Hits** column indicates the number of times that access traffic hits the policy.



Priority	Source	Destination	Protocol/Application/Port	Status	Policy Action	Description/Policy ID	Hits	Actions
1	0	101 232/32	TCP/HTTP/80/80	On	Monitor	all_http_in_chaifen_qa6	16	Modify Delete Copy Move
2	tsy001	tsy002	ICMP/ANY	Off	Deny	icmpdeny	10	Modify Delete Copy Move

You can click the number in the **Hits** column to go to the **Traffic Logs** tab. On the **Traffic Logs** tab, you can view the names of the access control policy that the traffic hits in the **Policy Name** column.

Note This tab displays information about the traffic that was generated in the last seven days. If traffic hit the access control policy seven days ago, no data is displayed.

Modify an access control policy

After an access control policy is created, you can modify the access control policy based on your business requirements.

To modify an access control policy, find the access control policy on the **Inbound Policies** tab and click **Modify** in the **Actions** column. In the **Modify Policy** panel, modify the parameters of the access control policy.

12. Best practices of Cloud Firewall based on ATT&CK

12.1. Disclaimer

The topics provided in **Best practices of Cloud Firewall based on ATT&CK** describe various rules. The rules may be used in business workloads or in illegal operations. By default, the rules of Cloud Firewall are in Disable or Monitor mode to prevent false positives that may occur in different scenarios. You can change the mode of the rules based on your business scenarios to resolve issues. However, the rules may be insufficient in some scenarios. For example, the rule that **forbids the installation of illegal tools** is not equivalent to a rule that **forbids the installation of any illegal tool** or a rule that **allows only the items specified on the Prevention Configuration page**. If you want to use more rules, you can give your feedback by submitting a ticket or communicating with technical support in the specified DingTalk group. After Cloud Firewall engineers evaluate and approve your feedback, the engineers publish rules to meet your requirements.

12.2. Overview

Cloud Firewall provides various features that you can use in different Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) stages. The features include basic protection, virtual patching, and threat intelligence. You can use the features in different scenarios to defend against risks such as vulnerabilities, brute-force attacks, mining activities, and data leaks. If the rules of a feature are disabled regardless of your workloads, scenarios, and internal compliance requirements, the protection capabilities of Cloud Firewall may not be maximized. Therefore, Cloud Firewall sets the rules to the Monitor or Disable mode. You can change the mode of the basic protection rules and virtual patching rules based on your business and security requirements. This way, you can implement the best practices for network defense, service monitoring, and security compliance within your enterprise. The following table describes the common scenarios in which you can use Cloud Firewall features.

Initial access	Execution	Persistence	Defense evasion	Discovery	Command and control
Cloud Firewall allows you to enable supply chain downloading or install a monitoring plug-in to prevent supply chain attacks.	Cloud Firewall allows you to disable script downloading to prevent scripts from performing operations, such as executing scheduled tasks or jobs, on your hosts.	Cloud Firewall allows you to disable script downloading to prevent scripts from performing operations, such as executing scheduled tasks or jobs, on your hosts.	Cloud Firewall allows you to disable script downloading to prevent scripts from performing operations, such as changing the permissions on files or directories, on your hosts.	Cloud Firewall allows you to disable the installation of illegal tools to prevent web service scans.	Cloud Firewall allows you to disable cloud-based remote debugging to prevent attacks that are initiated by using non-application layer protocols.

Initial access	Execution	Persistence	Defense evasion	Discovery	Command and control
N/A	N/A	N/A	Cloud Firewall allows you to disable script downloading to prevent scripts from performing operations, such as hiding files, on your hosts.	Cloud Firewall allows you to disable uninstallation of cloud security software to prevent security software discovery. The cloud security software can be the agent of a cloud security service such as Security Center.	Cloud Firewall allows you to disable proxies to prevent attacks that are initiated by using proxies.
N/A	N/A	N/A	Cloud Firewall allows you to disable script downloading to prevent scripts from performing operations, such as clearing historical records, on your hosts.	Cloud Firewall allows you to disable leaks of critical system information to prevent system information discovery.	Cloud Firewall allows you to disable remote control software to prevent attacks that are initiated by using remote access software.
N/A	N/A	N/A	Cloud Firewall allows you to disable script downloading to prevent scripts from performing operations, such as deleting files, on your hosts.	N/A	Cloud Firewall allows you to disable DNS over HTTPS (DoH) to prevent attacks that are initiated by using tunneling protocols.

Initial access	Execution	Persistence	Defense evasion	Discovery	Command and control
N/A	N/A	N/A	N/A	N/A	Cloud Firewall allows you to disable access to public services to prevent attacks that are initiated by using web services.

Related information

-
- [Disable uninstallation of cloud security software such as the Security Center agent](#)
- [Disable remote control software](#)
- [Disable script downloading](#)
- [Disable proxies](#)
- [Disable leaks of critical system information](#)
- [Disable remote debugging in the cloud](#)
- [Disable information detection](#)
- [Disable DoH](#)
- [Disable access to .onion proxy domain](#)
- [Disclaimer](#)

12.3. Disable the installation of unauthorized tools

In most cases, tools such as Nmap, MassCAN, and Pnsan are used to perform a large number of Internet-based scans, and Netcat is used to listen on ports and establish webshell connections. Cloud Firewall can be used to identify and control the unauthorized installation of the tools.

Impacts

This section describes the impacts of the installation of unauthorized tools.

- Unauthorized operations performed by an employee of an enterprise
After an employee of an enterprise downloads and installs an unauthorized tool, the employee can use the tool to perform asset mapping on the enterprise, disclose the network topology of the enterprise, and perform other unauthorized operations.
- Attacks
After an attacker intrudes into an internal network, the attacker can run the `yum` and `apt-get` commands to install unauthorized tools. The attacker can use the tools to implement lateral movement, insert webshells, and steal data based on the mapping of the network topology.

- Spreading of worms and trojans

After worms or other viruses compromise your host, unauthorized tools are downloaded and installed on the host by using scripts. If the tools are used to perform Internet-based scans, various hosts can be compromised.

Operations in the Cloud Firewall console

If you want to disable the installation of unauthorized tools for your Elastic Compute Service (ECS) instance, you can log on to the , choose **Intrusion Prevention > Prevention Configuration**, and click **Customize** in the Basic Protection section. In the **Customize Basic Protection Policies** dialog box, change the mode of some or all related rules to **Block**. This prevents or minimizes the preceding impacts in an efficient manner.

12.4. Disable uninstallation of cloud security software such as the Security Center agent

Host-based security software such as the Security Center agent is used to monitor the security status of hosts, detect and remove viruses and scripts, and detect execution of malicious commands. If the security software is uninstalled without authorization, the cloud security service can no longer protect hosts.

Impacts

- Unauthorized operations performed by an employee of an enterprise

If an employee of an enterprise wants to perform unauthorized operations, the employee first uninstalls the security software from hosts to prevent the security software from detecting unauthorized operations and generating alerts.

- Attacks

After an attacker intrudes into a cloud-based system, the attacker can uninstall the security software from hosts. This way, alert notifications of intrusions cannot be sent to engineers even if the hosts are attacked.

- Spreading of worms and trojans

After security software is uninstalled from hosts, alert notifications of intrusions cannot be sent even if malware such as worms and trojans is downloaded to implement webshell persistence or steal data.

Operations in the Cloud Firewall console

The rules that you can use to disable uninstallation of the Security Center agent are in **Monitor** mode. If you want to disable uninstallation of the agent in the cloud, you can log on to the , choose **Intrusion Prevention > Prevention Configuration**, and click **Customize** in the Basic Protection section. In the **Customize Basic Protection Policies** dialog box, and change the mode of some or all related rules to **Block**. This prevents or minimizes the preceding impacts in an efficient manner.

12.5. Disable remote control software

O&M engineers use remote control software in routine O&M, such as remote host control, remote desktop connections, remote startups, remote management, and internal network penetration.

Impacts

- Unauthorized operations performed by an employee of an enterprise

After an employee of an enterprise installs remote control software on a remote host, the employee has full permissions on the host without the need to enter the username and password of the host. For example, the employee can steal and delete data on the host.

- Attacks

After an attacker integrates remote control software with a host, the attacker can remotely perform visualized operations on the host by using webshells and has full permissions on the host. For example, the attacker can steal data from the host and insert webshells to the host.

- Spreading of worms and trojans

After remote control software is installed on a host, worms and trojans can insert webshells to the host. This way, worms and trojans have full permissions on the host.

Operations in the Cloud Firewall console

By default, the rules that you can use to disable commonly used remote control software such as TeamViewer and Sunlogin are in **Monitor** mode.

If you want to disable remote control software on your Elastic Compute Service (ECS) instance, you can log on to the , choose **Intrusion Prevention > Prevention Configuration**, and click **Customize** in the **Basic Protection** section. In the **Customize Basic Protection Policies** dialog box, change the mode of some or all related rules to **Block**. This prevents or minimizes the preceding impacts in an efficient manner.

12.6. Disable script downloading

Scripts such as Bash Shell, Python, Perl, and PowerShell scripts can contain a large amount of information. Attackers can use the information to perform common operations on hosts.

Impacts

- Unauthorized operations performed by an employee of an enterprise

The scripts that are remotely downloaded and contain malicious commands can be used to run pre-written commands.

- Attacks

The scripts that are remotely downloaded and contain malicious commands can be used to launch attacks.

- Spreading of worms and trojans

Worms and trojans compromise hosts by using scripts. In most cases, the scripts are written to crontab files for periodic execution. This way, the scripts cannot be permanently deleted from the hosts.

Operations in the Cloud Firewall console

The rules that you can use to disable script downloading are in **Monitor** mode. Downloaded scripts can be used to run commands such as Bash history and useradd on your hosts. If you want to disable script downloading in the cloud, you can log on to the , choose **Intrusion Prevention > Prevention Configuration**, and click **Customize** in the Basic Protection section. In the **Customize Basic Protection Policies** dialog box, change the mode of some or all related rules to **Block**. This prevents or minimizes the preceding impacts in an efficient manner.

12.7. Disable proxies

A proxy is a special network service that allows a client to indirectly connects to another client. A proxy can be used to bypass existing network detection.

Impacts

- Unauthorized operations performed by an employee of an enterprise

Proxies can be used to forward data of an enterprise to evade detection by intrusion prevention rules, access control policies, and threat intelligence rules.

- Attacks

Proxies can be used to forward traffic over internal networks. This way, attackers can detect internal networks and intrude into the internal networks.

- Spreading of worms and trojans

Proxies can be used by worms and trojans to evade detection by intrusion prevention rules, access control policies, and threat intelligence rules.

Operations in the Cloud Firewall console

The rules that you can use to disable operations such as the SOCKS5 proxy-related operations are in **Monitor** mode. If you want to disable SOCKS5 communication in the cloud, you can log on to the , choose **Intrusion Prevention > Prevention Configuration**, and click **Customize** in the Basic Protection section. In the **Customize Basic Protection Policies** dialog box, change the mode of some or all related rules to **Block**. This prevents or minimizes the preceding impacts in an efficient manner.

12.8. Disable leaks of critical system information

Critical information of users is stored in system files such as /etc/passwd and /etc/shadow. The information can be read by running system commands such as `cat` , `head` , and `tail` .

Impacts

- Attacks

Critical system information can be obtained from your server that is under web attacks such as remote command execution. After attackers obtain the information, the attackers can launch attacks such as remote logons and remote control.

- Spreading of worms and trojans

Worms and trojans can obtain critical system information to laterally spread in internal networks.

Operations in the Cloud Firewall console

The rules that you can use to disable leaks of critical system information are in **Monitor** mode. If you want to prevent the leaks of critical system information such as `/etc/passwd` in the cloud, you can log on to the , choose **Intrusion Prevention > Prevention Configuration**, and click **Customize** in the **Basic Protection** section. In the **Customize Basic Protection Policies** dialog box, change the mode of some or all related rules to **Block**. This prevents or minimizes the preceding impacts in an efficient manner.

12.9. Disable remote debugging in the cloud

Cloud-based software and services can be used to perform debugging operations, such as implementing breakpoint debugging and step debugging, and viewing stack information. This is called remote debugging. Protocols such as GDB, Java Debug Wire Protocol (JDWP), Xdebug, and Android Debug Bridge (ADB) can be used to debug scripts, binary files, and system files that are written in different programming languages. The programming languages include C, C++, Java, PHP, and Android.

Impacts

Remote debugging protocols have permissions on remote software and services. This may cause remote command execution.

- Unauthorized operations performed by an employee of an enterprise
Open remote debugging services can be used to remotely run commands and fully control hosts.
- Attacks
After attackers scan the ports that are open to the Internet for remote debugging services on the cloud, the attackers can implement remote command execution. As a result, the attackers have full permissions on your hosts and can perform operations such as trojan insertion and data theft.
- Spreading of worms and trojans
Worms and trojans can spread over remote debugging protocols, which causes threats such as mining activities and ransomware.

Operations in the Cloud Firewall console

The rules that you can use to disable remote debugging in the cloud are in **Monitor** mode. If you want to disable remote debugging in the cloud, you can log on to the , choose **Intrusion Prevention > Prevention Configuration**, and click **Customize** in the **Basic Protection** section. In the **Customize Basic Protection Policies** dialog box, change the mode of some or all related rules to **Block**. This prevents or minimizes the preceding impacts in an efficient manner.

12.10. Disable information detection

Web scanners are used to detect open web services and ports. You can use software such as Nmap, Masscan, and PNScan to detect open ports and open services.

Impacts

- Ports and services exposed

If ports and services are exposed, the information that is collected from the ports and services can be used to launch attacks.

- Attacks

Web scanners can detect the information about services or service configurations. The information can be used to launch attacks.

Operations in the Cloud Firewall console

The rules that you can use to disable information detection are in **Monitor** mode. If you want to disable information detection by using software such as Nmap in the cloud, you can log on to the , choose **Intrusion Prevention > Prevention Configuration**, and click **Customize** in the **Basic Protection** section. In the **Customize Basic Protection Policies** dialog box, change the mode of some or all related rules to **Block**. This prevents or minimizes the preceding impacts in an efficient manner.

12.11. Disable DoH

DNS over HTTPS (DoH) is a safe Domain Name System (DNS) resolution method. If you use DoH, DNS requests are encrypted by using HTTPS. This prevents DNS requests from being monitored or modified.

Impacts

- Unauthorized operations performed by an employee of an enterprise

An employee of an enterprise can access unauthorized domain names by using DoH to bypass detection by access control policies or threat intelligence rules.

- Spreading of worms and trojans

Worms and trojans can query the originating IP addresses of domain names by using DoH. This way, worms and trojans can bypass detection by intrusion prevention rules, access control policies, and threat intelligence rules.

Operations in the Cloud Firewall console

The rules that you can use to disable DoH are in **Monitor** mode. If you want to disable DoH, you can log on to the , choose **Intrusion Prevention > Prevention Configuration**, and click **Customize** in the **Basic Protection** section. In the **Customize Basic Protection Policies** dialog box, change the mode of some or all related rules to **Block**. This prevents or minimizes the preceding impacts in an efficient manner.

12.12. Disable access to .onion proxy domain

The top-level domain .onion is specially used to retrieve addresses in the Tor network. You can use a Tor server on which the required proxy is installed to send specific requests to a .onion website. Then, your operations cannot be tracked.

Impacts

- Unauthorized operations performed by an employee of an enterprise

An employee of an enterprise can visit .onion websites to access Tor servers. This way, the employee can perform malicious operations without being tracked by security engineers.

- Spreading of worms and trojans

Worms and trojans can query the originating IP addresses of domain names by using DoH. This way, worms and trojans can bypass detection by intrusion prevention rules, access control policies, and threat intelligence rules.

Operations in the Cloud Firewall console

The rules that you can use to disable monitoring of the Tor network are in **Monitor** mode. If you want to disable monitoring of the Tor network in the cloud, you can log on to the , choose **Intrusion Prevention > Prevention Configuration**, and click **Customize** in the **Basic Protection** section. In the **Customize Basic Protection Policies** dialog box, change the mode of some or all related rules to **Block**. This prevents or minimizes the preceding impacts in an efficient manner.