

Alibaba Cloud Cloud Firewall

Best Practices

Issue: 20190815

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 due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall 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 the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. 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 bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, 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 content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, 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 the Alibaba Cloud website, product programs, or content 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 contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information 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.
	This warning information 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 restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus, page names, and other UI elements.	Click OK.
<code>Courier font</code>	It is used for commands.	Run the <code>cd / d C :/ windows</code> command to enter the Windows system folder.
<i>Italics</i>	It is used for parameters and variables.	<code>bae log list --instanceid Instance_ID</code>
[] or [a b]	It indicates that it is an optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>

Style	Description	Example
<code>{}</code> or <code>{a b}</code>	It indicates that it is a required value, and only one item can be selected.	<code>swich {stand slave}</code>

Contents

Legal disclaimer.....	I
Generic conventions.....	I
1 Best practices for defending against CNC worms.....	1
2 Best practices for database security defense.....	5
3 Best practices for system security defense.....	9
4 Best practices for access control policy configuration.....	13
5 Best practices for defense against unauthorized access to MongoDB.....	20

1 Best practices for defending against CNC worms

Worms are a major threat to current businesses on the cloud. They exploit server vulnerabilities to spread over the network and do various malicious operations on infected servers. This poses serious threats to the assets and businesses of users. Cloud Firewall provides layered defense against the attack chains of worms, and can detect and intercept a variety of worms and their variants. Additionally, Cloud Firewall can update and expand its capability in real time based on threats on the cloud. This enables Cloud Firewall to detect and intercept the latest worms.

Harms of worms

Worms mainly cause the following harm:

- **Business interruption:** Worms may modify configurations or stop services on infected servers, causing risks such as server breakdown and business interruption.
- **Information stealing:** Worms for stealing information compress data on infected servers and send the compressed data back to attackers. This may cause serious information leakage or resource abuse.
- **Blocking by regulators:** Worms send a large number of packets when they spread. When the number of packets sent from an IP address exceeds the threshold, a regulator may block this IP address. This directly causes business interruption.
- **Monetary or data losses:** Ransomware worms encrypt files on infected servers for ransom, causing monetary or data losses.

Cloud Firewall solution

Cloud Firewall provides layered defense against the attack chains of worms, and can detect and intercept a variety of worms and their variants. Additionally, Cloud Firewall can update and expand its capability in real time based on threats on the cloud. This enables Cloud Firewall to detect and intercept the latest worms.

Typical worms include:

- **DDG:** spreads by exploiting Redis vulnerabilities and through brute-force attacks, and uses the computing resources on infected servers for mining cryptocurrency.
- **WannaCry:** spreads by exploiting the EternalBlue vulnerability of the Windows operating system and infects servers for ransom.

- **BillGates:** spreads by exploiting application vulnerabilities and through brute-force attacks, and builds a zombie network of infected servers for DDoS attacks.

Typical case: DDG worm

DDG is an active worm that spreads by exploiting Redis vulnerabilities and through brute-force attacks. Infected servers are added to a zombie network for mining cryptocurrency.

Impact scope of the DDG

- Servers that use weak SSH passwords
- Redis or other database servers with vulnerabilities

Major harm of the DDG

- **Business interruption:** The DDG mines cryptocurrency on infected servers, which occupies a large amount of computing resources on the servers. This may affect service availability and cause business interruption.
- **Blocking by regulators:** The DDG sends a large number of packets when it spreads. When the number of packets sent from an IP address exceeds the threshold, a regulator may block this IP address.

Defense against the DDG attack chain

Cloud Firewall provides real-time detection and defense against the DDG attack chain to block both the attack and spreading chains of the worm.

Cloud Firewall provides the following intrusion prevention features:

- **Threat Intelligence:** Cloud Firewall scans for and detects threat intelligence, and blocks malicious behavior from command-and-control servers in advance based on received threat intelligence.
- **Basic Protection:** Cloud Firewall detects malware and intercepts communication with command-and-control servers or backdoors.
- **Virtual Patches:** Cloud Firewall provides virtual patches to defend against exploits of popular high-risk vulnerabilities in real time.

Procedure

1. Log on to the [Cloud Firewall console](#).
2. In the console, choose Security Policies > Intrusion Prevention. The Intrusion Prevention page is displayed.

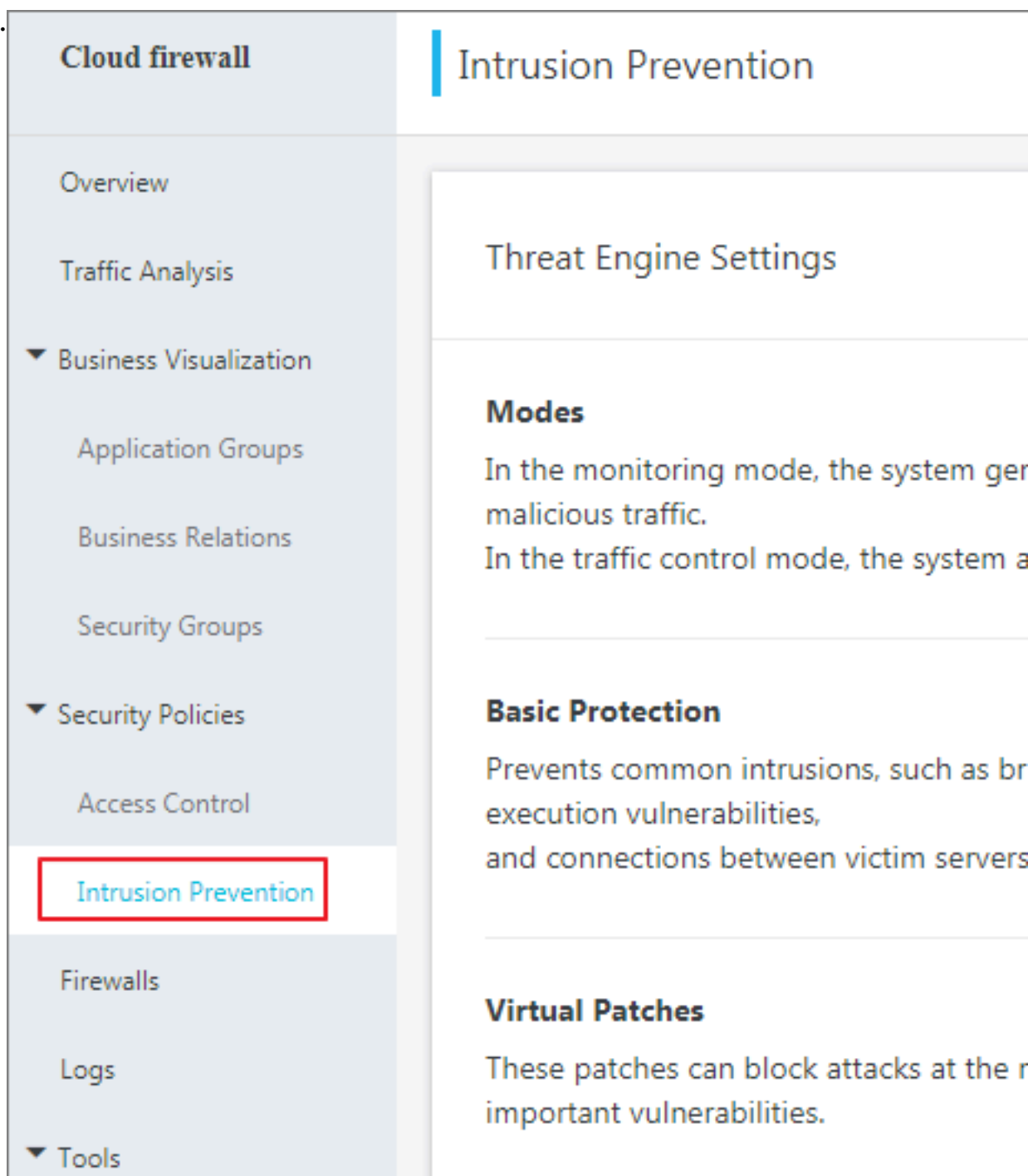
3. Select Traffic Control Mode.

The screenshot shows the 'Cloud firewall' console with the 'Intrusion Prevention' tab selected. The left sidebar contains a menu with 'Intrusion Prevention' highlighted. The main content area shows 'Threat Engine Settings' with three sections: 'Modes', 'Basic Protection', and 'Virtual Patches'. In the 'Modes' section, 'Traffic Control Mode' is selected (indicated by a blue dot and a red box). In the 'Basic Protection' section, 'Basic Policies' and 'Threat Intelligence' are both turned on (indicated by green toggle switches). In the 'Virtual Patches' section, 'Patches' is turned on (indicated by a green toggle switch).

4. In the Basic Protection area, turn on the Basic Policies and Threat Intelligence switches.

This screenshot is similar to the previous one, but it highlights the 'Basic Policies' and 'Threat Intelligence' toggle switches in the 'Basic Protection' section, which are now turned on (indicated by green toggle switches and a red box). The 'Traffic Control Mode' remains selected in the 'Modes' section.

5. In the Virtual Patches area, turn on the Patches switch.



2 Best practices for database security defense

The Intrusion Prevention feature of Cloud Firewall can defend against common database intrusions.

Database security defense requirements

A database is a system for managing and storing data resources in an enterprise. The database stores a lot of valuable and sensitive information, so it is often the primary target of hackers. Database security is vital to normal business operations and enterprise development.

A database faces the following main security threats:

- Brute-force attack

Upon successful brute-force attacks, the database is directly compromised.

- Database application vulnerabilities

For example, database CVE vulnerabilities may cause DoS attacks to database applications, malicious command execution, and information leakage.

- Malicious command execution and file reading or writing

For example, attackers can execute malicious commands and read or write files by calling high-risk stored procedures or functions.

- Information stealing and illegal export of database

Attackers sell stolen data or defraud other people, causing business losses.

Cloud Firewall solution

The Intrusion Prevention feature of Cloud Firewall can defend most databases against intrusions. The databases include:

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

How to use Cloud Firewall for database intrusion prevention

The Alibaba Cloud Security team is continuously tracking and studying database vulnerabilities and their preventive measures, and has accumulated rich experience in attack defense. The defense rules formulated based on this experience greatly enhance the database security defense capability of Cloud Firewall.

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

- Brute-force attack

Threat intelligence: The threat intelligence feature of Cloud Firewall can detect attack threats on the Internet and block scanning or intrusion behavior in advance.

- Database application vulnerabilities

Virtual patches: The virtual patches feature of Cloud Firewall provides intrusion prevention against high-risk vulnerabilities of databases.

- Malicious command execution and file reading or writing

Basic protection: The basic protection feature of Cloud Firewall can block malicious operations in real time, including system file operations, Webshell writing, and stored procedure or user defined function (UDF) invocation.

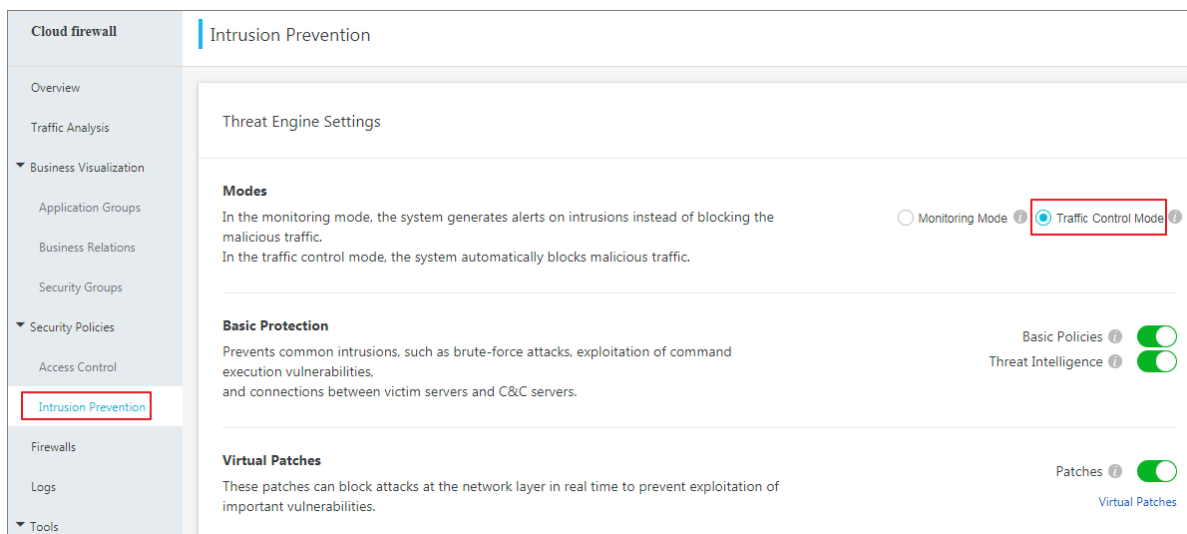
- Information stealing and illegal export of database

High-risk SQL blocking: The basic rules feature of Cloud Firewall can block the database export operation in real time to prevent information from being stolen.

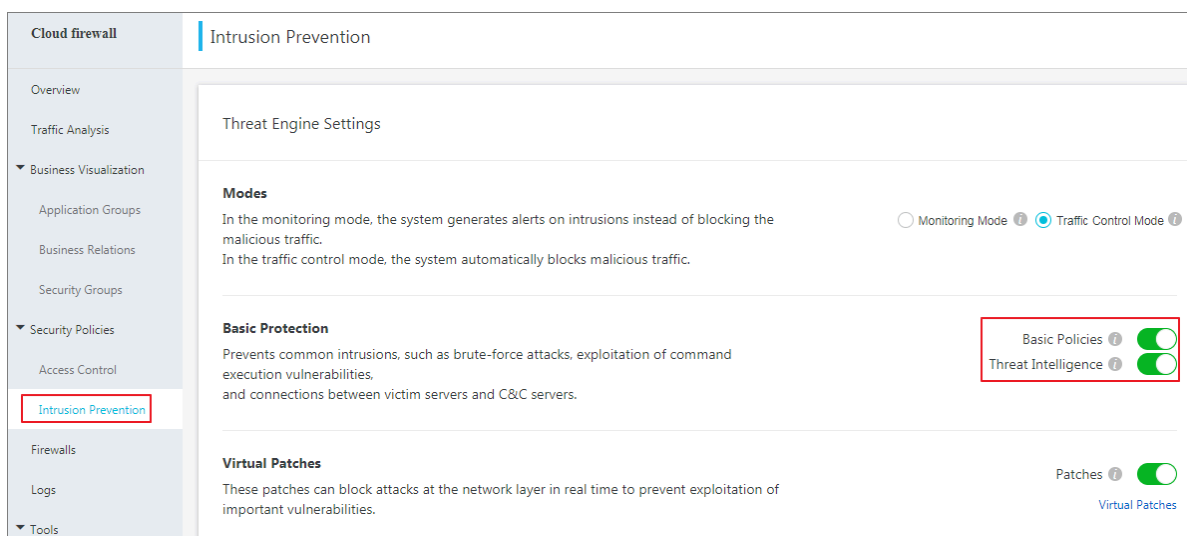
Procedure

1. Log on to the [Cloud Firewall console](#).
2. In the console, choose Security Policies > Intrusion Prevention. The Intrusion Prevention page is displayed.

3. In the Mode Selection area, click Interception Mode.



4. In the Basic protection area, turn on the Basic Policies and Threat Intelligence switches.



5. In the Virtual Patches area, turn on the Patches switch.

The screenshot displays the Cloud Firewall console interface. On the left is a navigation sidebar with the following items: 'Cloud firewall' (selected), 'Overview', 'Traffic Analysis', 'Business Visualization' (expanded, showing 'Application Groups', 'Business Relations', and 'Security Groups'), 'Security Policies' (expanded, showing 'Access Control'), 'Intrusion Prevention' (highlighted with a red rectangle), 'Firewalls', 'Logs', and 'Tools'. The main content area is titled 'Intrusion Prevention' and includes a 'Threat Engine Settings' section. Under this section, there are three subsections: 'Modes' (describing monitoring and traffic control modes), 'Basic Protection' (describing prevention of common intrusions), and 'Virtual Patches' (describing patches to block attacks at the network level).

Cloud firewall

- Overview
- Traffic Analysis
- ▼ Business Visualization
 - Application Groups
 - Business Relations
 - Security Groups
- ▼ Security Policies
 - Access Control
- Intrusion Prevention**
- Firewalls
- Logs
- ▼ Tools

Intrusion Prevention

Threat Engine Settings

Modes

In the monitoring mode, the system generates alerts for malicious traffic.

In the traffic control mode, the system automatically blocks malicious traffic.

Basic Protection

Prevents common intrusions, such as buffer overflow, denial of service, and connections between victim servers.

Virtual Patches

These patches can block attacks at the network level for important vulnerabilities.

3 Best practices for system security defense

System security is a key factor in maintaining secure and stable business operations. As the battle between cyberattacks and defense is heating up, more and more attack forms emerge, such as large-scale automated attacks, worms, ransomware, fraudulent cryptocurrency mining, and Advanced Persistent Threats (APTs). This brings great challenges to secure system running.

A system installed with default settings has the following security flaws, making it vulnerable to intrusions:

- The system is not properly configured.
 - Unnecessary open ports: Unnecessary services and applications are opened, and exposed to attacks.
 - Weak passwords: They are vulnerable to brute-force attacks, resulting in easy system intrusions.
 - Improper policy configuration: System security policies are not configured or their strength is weak.
- System vulnerabilities exist or necessary patches are not installed.
 - Command execution vulnerability: This vulnerability allows arbitrary command execution, causing system intrusions.
 - Denial of Service (DoS) vulnerability: The system under DoS attacks rejects normal service requests, resulting in business interruption.
 - Information leakage vulnerability: Sensitive or confidential data is disclosed.

Typical case: remote code execution 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.

The Samba server software was reported to have a remote code execution vulnerability. This vulnerability allows a malicious client to upload a shared library to a writable shared directory, and then cause the server to load and execute the library.

CVE: CVE-2017-7494

Impact scope:

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

Major harm:

- **Command execution:** Servers are breached and information is disclosed due to remote code execution.
- **Business interruption:** A worm, named SambaCry, can spread by exploiting this vulnerability. This worm mines cryptocurrency on infected servers, which occupies a large amount of computing resources on the servers. This may affect service availability and cause business interruption.

Typical case: remote code execution vulnerability in SMB Server

SMB Server is a server protocol component that is installed on the Windows operating system by default. SMB Server was reported to have a remote code execution vulnerability. This vulnerability allows a remote attacker to execute code by sending crafted packets to SMBv1 Server.

CVE: CVE-2017-0143

Impact scope:

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

Major harm

- **Command execution:** Servers are breached and information is disclosed due to remote code execution.
- **Data loss:** Worms, such as WannaCry, can spread by exploiting this vulnerability. Such worms encrypt files on infected servers for ransom and cause information leakage.

How to use Cloud Firewall for system intrusion prevention?

Alibaba Cloud Security team is continuously tracking and studying system vulnerabilities and their preventive measures, and has accumulated rich experience in attack

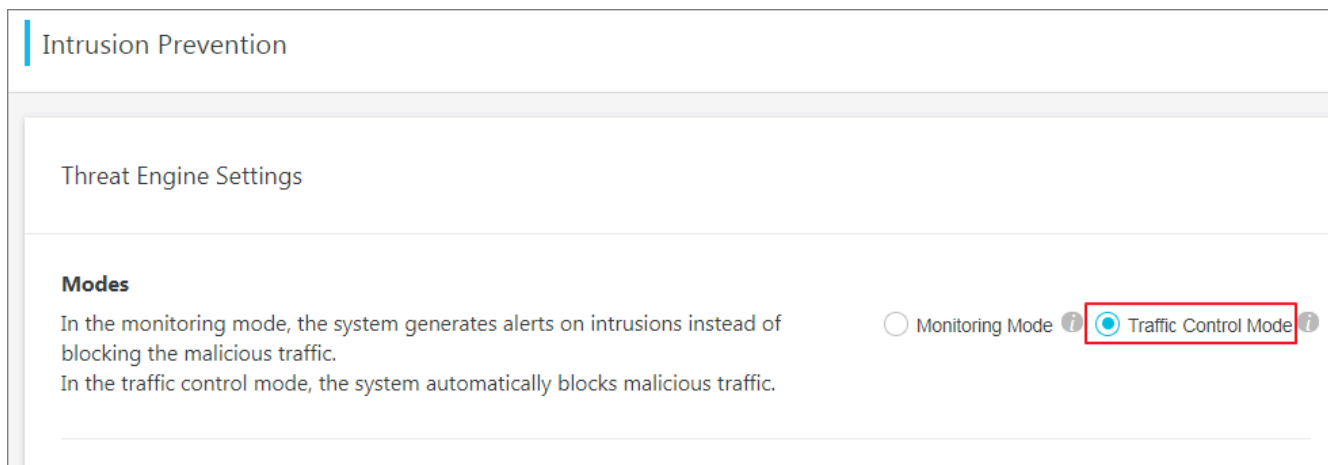
defense. The defense rules formulated based on this experience greatly enhance the system security defense capability of Cloud Firewall.

To ensure normal system running, Cloud Firewall provides multi-point defense against all risks that the system faces.

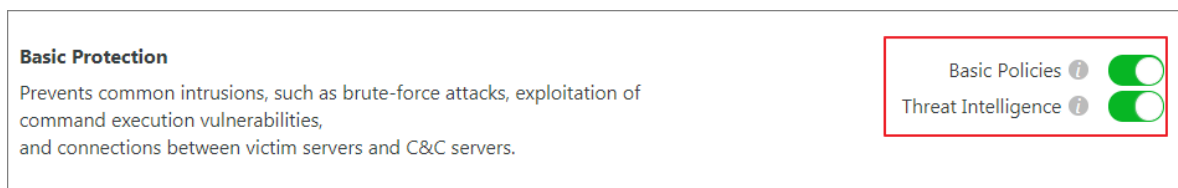
- **Brute-force attack:** The threat intelligence feature of Cloud Firewall can detect attack threats on the Internet and block scanning or intrusion behavior in advance.
- **System vulnerabilities:** Cloud Firewall provides intrusion prevention against high-risk vulnerabilities of operating systems.
- **Other attacks:** The basic rules feature of Cloud Firewall can detect other system attacks, such as a reverse shell and system file leakage, and block them in real time.

Procedure

1. Log on to the [Cloud Firewall console](#).
2. In the console, choose Security Policies > Intrusion Prevention. The Intrusion Prevention page is displayed.
3. In the Modes area, click Traffic Control Mode.





4. In the Basic Protection area, turn on the Basic Policies and Threat Intelligence switches.



5. In the Virtual Patches area, turn on the Patches switch.

Virtual Patches

These patches can block attacks at the network layer in real time to prevent exploitation of important vulnerabilities.

Patches  

[Virtual Patches](#)

Click Virtual Patches to open the virtual patches configuration list. You can enable/disable a certain patch.

Intrusion Prevention

Threat Engine Settings

Modes

In the monitoring mode, blocking the malicious traffic.

In the traffic control mode, blocking the malicious traffic.

Basic Protection

Prevents common intrusion attacks, blocking the malicious traffic and connections between the protected resources.

Virtual Patches

These patches can block attacks at the network layer in real time to prevent exploitation of important vulnerabilities.

Virtual Patches

Level: **All** Status: **All** Patch Name: **Search**

Total Items: 65, Disabled Items: 0

<input type="checkbox"/>	Patch Name	Level	Patch ID	Status	Action
<input type="checkbox"/>	SQL Injection	Medium	0	Enabled	disable
<input type="checkbox"/>	SQL Injection	Medium	0	Enabled	disable
<input type="checkbox"/>	SQL Injection	Medium	0	Enabled	disable
<input type="checkbox"/>	SQL Injection	Medium	0	Enabled	disable
<input type="checkbox"/>	SQL Injection	Medium	0	Enabled	disable

☐ Enable disable

[1](#) [2](#) [3](#) [4](#) ... [13](#) [1/13](#) Go To Page **Go**



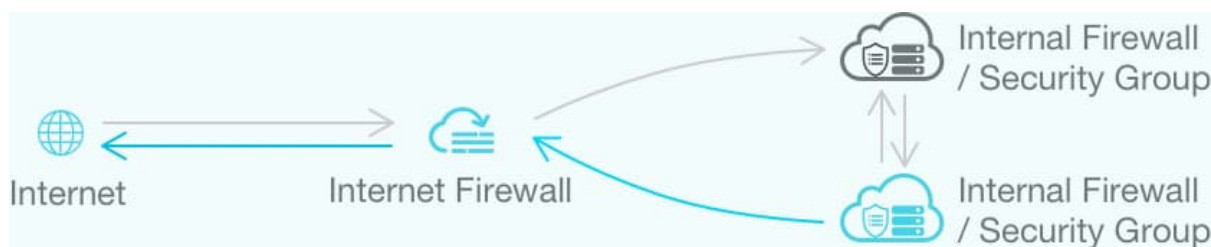
Note:

When the Patches switch is turned on in Virtual Patches module, all the patches on Virtual Patches list will be enabled automatically.

4 Best practices for access control policy configuration

This topic describes the best practice for configuring access control policy.

How network access control works



- **Internet Firewall:**
 - **How it works:** Internet Firewall controls the traffic between internet and cloud assets.
 - **Portal:** Outbound Policies and Inbound Policies in Security Policies > Access Control tab page.
 - **Default Policy:** Both inbound and outbound traffic are allowed to pass through by default.
- **Internal firewall/security group:**
 - **How it works:** A Security Group (also a virtual internal firewall) is deployed on each ECS instance to control the internal network traffic of ECS instances.
 - **Portal:** Security Policies > Access Control > Internal Firewall.



Note:

Only Cloud Firewall Enterprise/Flagship edition supports this function. Cloud Firewall Pro users must configure the security groups in ECS console.

- **Default policy:** Only outbound traffic is allowed to pass through by default, and inbound traffic is blocked.

Procedure

1. Tune the configuration of Inbound policies of Internet Firewall.

Priority	Source	Destination	Port/Application/Port	Policy Action	Description	Hits	Actions
1			TCP/SSH60022/60...	Monitor		2	Modify Delete Insert Move
2			TCP/SSH22/22	Deny		0	Modify Delete Insert Move
3			UDP/ANY/165535	Monitor		17	Modify Delete Insert Move
4			UDP/ANY/0	Monitor		0	Modify Delete Insert Move
5			TCP/HTTP8443/443	Monitor		74	Modify Delete Insert Move
6			ICMP/ANY	Allow		0	Modify Delete Insert Move
7			ANY/ANY/21_4-16...	Allow		32	Modify Delete Insert Move

When you perform this task, follow these guidelines:

- Allow all the necessary ports

For ports that must be opened to the Internet, such as HTTP port 80 and HTTPS port 443, set these ports as Allow in Inbound Policies configuration.

- Strictly allow some ports in high risk

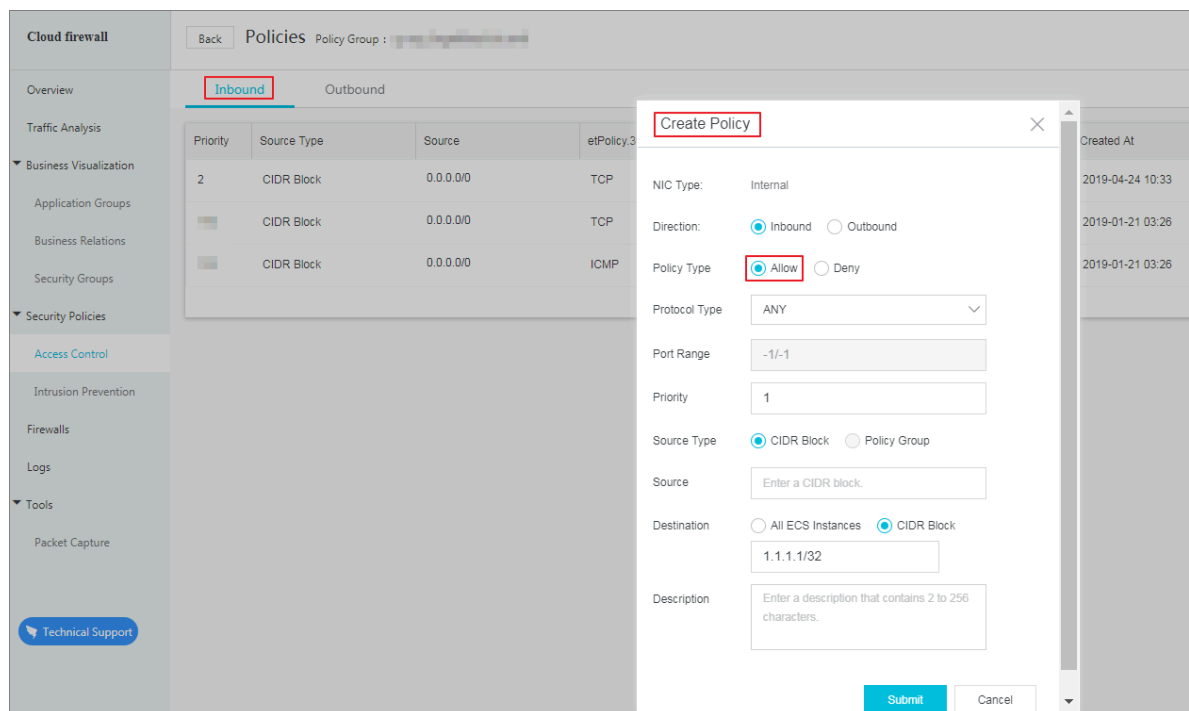
For ports that are used only for operations and maintenance, and ports that may pose high risks, such as SSH port 22 and MySQL port 3306, allow them to communicate with the necessary source IP. You can use the address book function to simplify your configuration.

- Deny the risky ports

For the risky ports, such as SMB port 445, set them as Deny in access control policy configuration.

- Create a policy with both the source and destination set to Any, and then set the policy action to Monitor. After this policy is created, check the access log to make sure that the network traffic is received, and then change the policy action to Deny.

2. Set all the the inbound traffic of Internal Firewall to Allow.



When you perform this task, follow these guidelines:

Go to the Security Policies > Access Control > Internal Firewall tab page, select the policy group that contains all test ECS instances, create a policy to allow the network traffic sent to the test ECS instances from 0.0.0.0./0. By default, the internal firewall and security group forbid all inbound traffic to pass through. Therefore, you must create a policy to allow the inbound traffic to pass through.



Note:

The Security Policies > Access Control > Internal Firewall tab page is only available to Cloud Firewall Enterprise and Flagship editions. Cloud Firewall Advanced users must complete this task in Security Group configuration of ECS console.

3. Verify the policies.

Cloud Firewall												
Logs												
Event Log Access Log Operation Log												
Internet boundary ... Source IP <input type="text"/> Enter a source IP: Destination IP <input type="text"/> Enter a keyword: Application <input type="text"/> Show Advanced Search List Configuration												
2019-04-29 16:59 - 2019-04-29 17:59 <input type="button" value="Search"/>												
Time	Source IP	Destination IP	Source Port	Destination Port	Direction	Application	Protocol	Policy Action	Bytes	Packets	Policy Name	
From : 2019-04-29 17:59 To : 2019-04-29 18:01			33148	8080	Inbound	Unknown	TCP	Monitor	274 B	3	海外封禁	
From : 2019-04-29 17:59 To : 2019-04-29 18:01			33222	8080	Inbound	HTTP	TCP	Monitor	544 B	5	海外封禁	
From : 2019-04-29 17:59 To : 2019-04-29 18:01			50656	10001	Outbound	Unknown	TCP	Discard	965 B	4	Mining b...	
From : 2019-04-29 17:59 To : 2019-04-29 18:01			50650	10001	Outbound	Unknown	TCP	Discard	965 B	4	Mining b...	
From : 2019-04-29 17:59 To : 2019-04-29 18:01			61619	9009	Inbound	HTTP	TCP	Monitor	1.98 KB	18	海外封禁	
From : 2019-04-29 17:59 To : 2019-04-29 18:01			57036	13531	Outbound	Unknown	TCP	Discard	704 B	4	Mining b...	
From : 2019-04-29 17:59 To : 2019-04-29 18:00			50638	10001	Outbound	Unknown	TCP	Discard	1.03 KB	5	Mining b...	

Go to Log > Access Log to verify the network traffic that is permitted, denied, and monitored. Based on the access log and the actual test results, verify the policies are executed as expected.

4. Tune the Internet Firewall policies.

Cloud firewall

Access Control

Internet Firewall Internal Firewall

Outbound Policies Inbound Policies

Create Policy Search by source.

Priority	Source
1	10.0.0.0/24
2	10.0.0.0/24
3	10.0.0.0/24
4	10.0.0.0/24
5	10.0.0.0/24
6	10.0.0.0/24
7	10.0.0.0/24

Make sure that the Internet Firewall policies do not have any false positives, and then change the action of the Any-Any policies from Monitor to Deny. Make sure that you understand the risks of this operation before you perform this task.

5. Allow the inbound traffic to pass through the Internal Firewall on all ECS instances.

Policy Group Name	VPC	Source	Template	Related Instance	Created At	Description	Status	Actions
cfw_sg_visible_test_sg_22	China (Shenzhen) /	Security Group Synchronization	-	1	2019-03-20 03:42	-	Published	Configure Policy Publish Modify Delete
cfw_sg_visible_test_sg_21	China (Shenzhen) /	Security Group Synchronization	-	1	2019-03-20 03:42	-	Published	Configure Policy Publish Modify Delete
cfw_sg_visible_test_sg_20	China (Shenzhen) /	Security Group Synchronization	-	1	2019-03-20 03:42	-	Published	Configure Policy Publish Modify Delete
cfw_sg_visible_test_sg_19	China (Shenzhen) /	Security Group Synchronization	-	1	2019-03-20 03:42	-	Published	Configure Policy Publish Modify Delete

When you perform this task, follow these guidelines:

- Go to Security Policies > Access Control > Internal Firewall, add a policy to all policy groups to allow all network traffic sent from 0.0.0.0/0.
- After you complete this task, you no longer need to create a new policy for new ECS instances that join the security groups. However, if you add an ECS instance to a newly created security group, then you must create a default inbound policy in the group to allow all inbound traffic.

6. Verify the availability of all businesses.

Go to Log > Access Log and verify the network traffic that is permitted, denied, and monitored. Based on the access log and the actual test results, verify the policies are executed as expected.

7. Configure Internet Firewall outbound policies.

The screenshot displays the 'Access Control' section of the Cloud Firewall console, specifically the 'Outbound Policies' tab. The interface includes a sidebar with navigation options like Overview, Traffic Analysis, Business Visualization, and Security Policies. The main content area shows a table of outbound policies. The table has columns for Priority, Source, Destination, Port/Application/Port, Policy Action, Description, Hits, and Actions. There are six policies listed, with actions like Deny, Allow, and Monitor. A 'Create Policy' button is visible at the top left of the table area.

Priority	Source	Destination	Port/Application/Port	Policy Action	Description	Hits	Actions
1			TCP/HTTP/80/80	Deny		4	Modify Delete Insert Move
2			TCP/SMTP/25/443	Allow		6	Modify Delete Insert Move
3			TCP/HTTP/80/80	Monitor		0	Modify Delete Insert Move
4			TCP/HTTPS/443	Allow		0	Modify Delete Insert Move
5			TCP/SSH/22/22	Deny		0	Modify Delete Insert Move
6			TCP/HTTP/80/80	Deny		0	Modify Delete Insert Move

When you perform this task, follow these guidelines:

- When you need to establish external connections, you can go to Security Policies > Access Control > Internet Firewall > Outbound Policies tab page to create policies.
- We recommend that you only allow network traffic destined for the specified domain names or IP addresses, such as the end point of an external API.
- By default, all network traffic destined for the Internet are not allowed to pass through the Internet Firewall. You can monitor your businesses a short period of time to make sure that they need external connections before creating a policy.

5 Best practices for defense against unauthorized access to MongoDB

Unauthorized access to MongoDB could lead to data disclosure or deletion extortion.

To ensure the security of your business and applications, Cloud Firewall provides a solution to fix this vulnerability.

Hazards

By default, a MongoDB database requires no authentication if you do not set any parameters when activating the MongoDB service. Without any passwords, users who have logged on to the service can use the default port to remotely access the database and perform any operations (including high-risk operations such as add, delete, edit, and query) on the database.

Solution

1. Configure an access control policy in Cloud Firewall.

- a. Log on to the Cloud Firewall console. Choose Network Traffic Analysis > Internet Access Activities > Open Applications. On the Open Applications tab, check the public IP address of the MongoDB service. If the MongoDB service provides services only for intranet servers, we recommend that you disable the MongoDB service from being open to the Internet.

Bind the MongoDB service to a specified IP address so that the MongoDB service provides services only for intranet servers. (In this example, the MongoDB instance listens only on the requests sent from intranet IP address 10.0.0.1.)

```
mongod -- bind_ip 10 . 0 . 0 . 1
```

- b. Configure an access control policy for MongoDB in Cloud Firewall to allow only trusted IP addresses to access the MongoDB service.

Log on to the Cloud Firewall console. Choose Security Policy > Access Control > Internet Border Firewall > Internet-to-Intranet. In the dialog box that appears,

configure an access control policy to allow only the MongoDB servers to access the MongoDB service.

A. Add all trusted IP addresses that are allowed to access the MongoDB service to an IP address book.

B. Allow trusted IP addresses to access the MongoDB service.

- **Source:** The address box in which you have configured all trusted IP addresses that are allowed to access the MongoDB service.
- **Destination:** The IP address of the MongoDB service.
- **Protocol Type:** Select TCP, which indicates that this policy applies to access traffic from the Internet.
- **Port:** Set this parameter to 0/0, which indicates that this policy applies to all ports corresponding to trusted IP addresses.

c. Disallow non-trusted IP addresses to access the MongoDB service.

- **Source:** Set this parameter to Any, which indicates that this policy applies to all non-trusted access IP addresses.
- **Destination:** The public IP address of the MongoDB service.
- **Protocol Type:** Select TCP, which indicates that this policy applies to access traffic from the Internet.
- **Port:** Set this parameter to 0/0, which indicates that this policy applies to all ports corresponding to non-trusted IP addresses.

2. Enable role-based logon authentication.

a. Create a user in the admin database.

b. Log on to the database with authentication disabled.

```
[ mongodbrac 3 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
```

c. Switch to the admin database.

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

d. Create an administrator account.



Note:

In MongoDB V3 and later, the addUser method is no longer used. You can run the db.createUser command instead to create users.

```
> db . addUser ( " supper ", " supWDxsf67 % H " ) or
{ " n " : 0 , " connection Id " : 4 , " err " : null , " ok
  " : 1 }
> db . createUser ( { user : "****", pwd : "*****", roles : [ "
  root " ] } )
{
  " user " : "****",
  " readOnly " : false ,
  " pwd " : "*****", " _id "
  ObjectId ( " 4f2bc0d357 a309043c69 47a4 " )
}
# The administra tor account informatio n is in the
  system . users collection .
> db . getCollect ionNames ( )
[ " system . indexes ", " system . users ", " system . version " ]
```



Note:

The account name cannot be a common word. The password must contain at least eight characters, including at least one uppercase letter, one lowercase letter, one number, and one special character. Do not use a common password, such as a birth date, a name, or an ID number.

e. Verify that the user has been created.

```
# Terminate the process and restart the MongoDB
  service .
> db . auth ( " user ", " password " )
> exit
bye
./ mongod -- dbpath = / path / mongod -- bind_ip = 10 . 0 . 0 .
  1 -- port = 27028 -- fork = true logpath = / path / mongod .
  log &
```



Note:

- The admin.system.users collection has the super privilege. It stores the information of users who have higher user privileges than users in other databases. That is, users created in the admin database can perform operations on data in other databases in MongoDB.
- In the MongoDB system, a database is created by a super user. A database may contain multiple users, but a single user may only exist in one database at a time. Users in different databases may share the same name, however.
- User1 in a particular database (such as DB1) cannot access database DB2, but can access data created by other users in DB1.

- Users with the same name in different databases cannot log on to other databases. For example, if both DB1 and DB2 have user1. After user1 logs on to DB1, it cannot log on to DB2.
- Users created in the admin database have the super privilege, and can perform operations on any data object in any database in the MongoDB system.
- You can use the `db . auth ()` method to validate users in the database. If the validation is successful, a value of 1 is returned. Otherwise, a value of 0 is returned. The `db . auth ()` method can only validate the user information in the database to which the user belongs, and cannot validate user information in other databases.

Check for intrusion risks

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

- Check whether the MongoDB log is complete and confirm the source IP address, time, and activity of the request for deleting the database.
- Run the `db . system . users . find ()` command to check whether any MongoDB account has no password.
- Run the `db . fs . files . find ()` command to check whether any file is stored in GridFS.
- Run the `show log global` command to view the log file and check whether other users have accessed MongoDB.