



Cloud Firewall

Product Documentation





Contents

Cloud Firewall 3

- Product Introduction 3
 - Cloud Firewall Overview 3
 - Advantages 7
 - Scenarios 9
 - Key Concepts 10
 - Use Cases 14
 - Cloud Firewall Networking Planning 16
- Purchase Guide 18
 - Billing Overview 18
 - Renewal Instructions 20
 - Resource deletion Upon Expiration 21
 - Purchase Instructions 22
- Operation Guide 23
 - CVM Creation 23
 - Custom Routing Mode Configuration Guide 24
 - Firewall Toggle 26
 - Inter-VPC Firewall Toggles 26
 - Feature Description 26
 - Operation Guide 28
 - Creating Inter-VPC Firewall Instances 30
 - Performance Metrics 35
 - NAT Firewall Toggle 36
 - Creating a NAT Firewall Instance 36
 - Performance Metrics 38
 - Feature Description 39
 - Operation Guide 41
 - Asset Center 43
 - Traffic Center 44
- Access Control 45
 - Inter-VPC Firewall Rules 45
 - Special Use Cases 49
 - NAT Firewall Rules 52
- Intrusion Prevention 56
- Cloud Log Service 61
- Log Analysis 63
- General Settings 64
- Notification Settings 65
- Common Tools 66
 - Address Templates 66
 - Policy Backup and Rollback 70
 - Task Scheduler 73
 - Packet Capture Tool 77
 - Simulation Test 80
- Troubleshooting 84
 - Solution for False Alarms and False Positives 84

Product Introduction

Cloud Firewall Overview

What is Converge Cloud Firewall (CFW)?

Converge Cloud Firewall (CFW) is a SaaS firewall built for the public cloud environment that provides network perimeter protection and addresses security and management needs such as unified access control and log auditing.

In addition to the capabilities of traditional firewalls, CCFW supports multi-tenancy, elastic scaling, and serves as a core network security infrastructure for organizations undergoing cloud migration.

Features Overview

1. Cloud Firewall Overview

Cloud Firewall offers centralized network access control. The console overview page provides a clear visualization of key modules:

- Asset Protection Overview – Displays asset counts in public and private networks, exposed ports, and security events, including vulnerability intelligence.
- Firewall Status Monitoring – Shows peak bandwidth for edge and NAT firewalls within the last 7 days.
- Traffic Statistics – Monitors inbound, outbound, and total traffic for time periods ranging from 24 hours to 6 months.
- Security Policy Configuration – Displays counts of access control rules for edge, NAT, and inter-VPC firewalls, along with remaining quota and intrusion prevention policies.
- Log Storage Statistics – Shows total, used, and remaining log storage capacity.

2. Cloud Firewall Toggles

- Edge Firewall: Automatically identifies public IP addresses and associated instances, allowing you to manage access control by public IP. Supports public BGP IPs (IPs from CMCC, CUCC, or CTCC are not supported).



You can view all inbound and outbound rules for each public IP and manage them through the Access Control module.

- **Inter-VPC Firewall:** Automatically detects all VPCs in your private network, visualizing them through a VPC topology.

Once the feature toggle is enabled:

- A sub-firewall is created automatically for each connected VPC pair.
- You can enable/disable sub-firewalls and configure access control rules for each.

- **NAT Firewall:** A virtual firewall that operates similarly to a NAT gateway, providing network address translation and security audit features (access control + logs).

After creation:

- The system identifies the subnets of selected VPCs.
- You can enable firewalls for subnets to route traffic through the NAT firewall.
- Configure access control lists (ACLs) to filter and manage traffic.

3. Asset Management

Asset Management enables you to view and manage detailed data for all assets — helping identify top 5 core and risky assets, as well as full visibility over public, private, and VPC-based assets.

It supports proactive monitoring to prevent potential security threats.

4. Alert Management

Alert Management keeps you informed when your assets are under attack.

After configuring rules under Access Control, Intrusion Defense, and Security Baseline, CCFW continuously notifies you of critical alerts for Security Operations & Maintenance (SecOps).

5. Traffic Monitoring

Traffic Monitoring provides visualized data on:

- External access statistics
- Outgoing request analysis



- Inter-VPC activity

This helps identify anomalies and optimize network flow security.

6. Access Control

Access Control rules are defined using a 5-tuple model (protocol, source IP, destination IP, source port, destination port).

These rules:

- Are applied according to priority for each data flow passing through the edge firewall.
- Allow administrators to control access to public IPs.
- Provide logging for auditing, troubleshooting, and compliance.

This structure supports cross-subnet, VPC-to-VPC, and hybrid cloud protection scenarios.

7. Intrusion Defense

Intrusion Defense] automatically detects unknown risks beyond standard access control rules.

It monitors north-south traffic for public IPs and applies intrusion defense rules to protect against CVM vulnerabilities and Internet-based attacks.

8. Security Baseline

Security Baseline uses long-term traffic analysis to build a trusted access list (IP or domain).

Administrators can adjust this baseline by adding/removing entities based on:

- Security scores
- Detected events
- Traffic patterns

This ensures ongoing adaptive security optimization.

9. Log Audit

Log Audit records rule hit data for the last 7 days and provides:

- Traffic rule matching history
- Searchable logs for fast troubleshooting



- Operation history for up to 30 days

This enables efficient auditing, reduces O&M effort, and improves security governance.

10. Log Analysis

Log Analysis stores and processes traffic logs for 6 months, supporting:

- Search-based queries (e.g., by user, resource, or action)
- Report generation
- Advanced analytics

Ideal for trend identification and compliance reviews.

11. Address Template

Address Template simplifies batch IP management.

You can:

- Create templates for IPs or domain names
- Add multiple entries
- Reuse templates in Access Control Rules

This improves administrative efficiency and rule consistency.

Note:

Converge Cloud Firewall unifies protection for both public and private network traffic, combining visibility, control, and compliance for all connected resources within the Converge Cloud ecosystem.

Advantages

Easy to Enable and Deploy

Based on SDN, CFW offers a public cloud SaaS firewall with simple policy configuration and no hardware deployment costs.

It can automatically identify cloud assets and allows you to enable or disable firewalls with one click.

Stable, Reliable, and Scalable

With a primary-secondary disaster recovery system and SaaS features, CFW provides high stability and reliability.

It supports easy scaling for:

- Bandwidth
- Assets
- Storage

allowing your network protection to grow effortlessly with your cloud infrastructure.

Centralized Management for High Efficiency

CFW offers a centralized access control plane for managing access and ensuring security isolation across networks and VPCs.

Network Perimeter Access Control

- Block or observe malicious traffic.
- Prevent attacks from malicious sources on cloud assets based on access control rules configured for public IP addresses.

Inter-VPC Access Control

- Control access between VPCs.
- Ensure security isolation through inter-VPC access control rules.



Enterprise Security Group

- Simplify security group configuration using the 5-tuple configuration model.
- Easily build a cloud demilitarized zone (DMZ) with blocked request logs.
- Protect traffic between subnets, VPCs, and hybrid cloud connections.

By following the rule configuration model of traditional firewalls, CFW is easy to learn and use for security operations and maintenance specialists.

Log Storage and Audit

Rule Hit Log

When an access control rule is matched and applied, CFW records the 5-tuple information of the matched traffic and rule.

This helps with:

- Security operations and maintenance (SecOps)
- Quick troubleshooting during network issues or failures

User Operation Log

Records user operations on CFW, including:

- Account logins
- Firewall toggle operations
- Add/Delete/Edit actions on rules

These logs improve management efficiency, accountability, and cost transparency.

Note:

CFW's SDN-based design makes it simple to deploy, highly scalable, and ideal for enterprise-grade network visibility and control.

Scenarios

Outbound Access Control

For outbound connections, if you need to block access to a specified external address or domain name from CVMs, you can configure outbound access control rules for the public IP address to meet your security requirements.

Inbound Access Control

For inbound connections, if you need to block access to CVMs from a specified external address, you can configure inbound access control rules for the public IP address to meet your security requirements.

Hit Log Audit

If you need to audit the hits of CFW's access control rules, or trace the applied rules in case of failure, CFW's rule hit log audit feature helps you perform rapid log audits and troubleshooting, improving efficiency in security operations and maintenance while reducing costs.

Operation Log Audit

To manage CFW operations, you can use CFW's user operation logs to obtain the time, content, and account information of any CFW operation.

This provides visibility and accountability for all firewall configuration changes and activities.

Note:

Access control and audit features in CFW ensure full visibility over both inbound and outbound traffic, enabling precise policy enforcement and faster issue resolution.

Key Concepts

Network Perimeter

The network perimeter is the boundary between the Internet and Converge Cloud's internal network. The network perimeter traffic, also known as north-south traffic, is the traffic generated during communication between cloud assets and the Internet.

North-south traffic is the traffic between public IP addresses and can be divided into the following:

- Outbound traffic: The traffic generated when cloud assets communicate with the Internet through the bound public IP address.
- Inbound traffic: The traffic generated when the Internet communicates with the cloud assets.

Edge Firewall

The edge firewall is a firewall for clusters that monitors north-south traffic.

It defends the boundary between the assets associated with your Elastic IP (EIP) and the Internet.

The edge firewall offers:

- Access control
- Log audit
- Built-in intrusion defense module
- Default cluster deployment

It is out-of-the-box and easy to scale without complex network configurations or image installation.

Virtual Private Cloud (VPC)

A Virtual Private Cloud (VPC) is a custom and logically isolated network space on Converge Cloud. Similar to a traditional network running in a local data center, your VPC hosts your cloud resources including CVM, CLB, and CDB.

A VPC offers you:

- EIP: Used to access the Internet.
- Peering Connection: Supports communication between VPCs.

[View Peering Connection Documentation](#)

Cloud VPC connection can be achieved using Peering Connection , and the traffic between two VPCs is called east-west traffic.

[View Virtual Private Cloud Documentation](#)

Inter-VPC Firewall

The Inter-VPC Firewall is a distributed firewall that monitors east-west traffic between VPCs. It defends the boundary between two VPCs.

The Inter-VPC Firewall is deployed between two VPCs connected through Peering Connection and offers:

- Access control
- Topology visualization
- Log audit
- Exclusive resource configuration

It is out-of-the-box without complex routing configurations or image installation.

Access Control

Access control is a collection of traffic filtering rules.

An access control list (ACL) contains all the rules for the same type of traffic.

Each access control rule is composed of the rule body and description.

Rule Body

Defines the following:

- Access source: The address of the source (usually an IP address).
- Access destination: The address of the destination (IP address or domain name).
- Destination port: The destination port of the communication.
- Protocol: The network protocol used for the communication.
- Policy: The action to perform for matching traffic.

Policy Types

- Allow: Allows access and records traffic logs (no rule hit logs).
- Observe: Allows access and records both traffic and rule hit logs.
- Block: Denies access and records rule hit logs (no traffic logs).

Rule Description

Describes the purpose of this access control rule.

Note:

A reasonable and standard rule description makes the rule more readable, while reducing maintenance costs and improving efficiency.

Rule Priorities

The priority indicates a rule's position in the list, where 1 is the highest priority.

For any data flows that go through the firewall, Converge Cloud Firewall (CFW) matches them from top to bottom:

1. If a data flow matches a rule, matching stops and the policy is applied.
2. If a data flow does not match the current rule, it moves to the next.
3. If it does not match any rule, it is allowed by default.

Priority values are integers from 1 to n, where 1 is the top and n is the lowest.

Rules of Priority

- Continuity: Priorities must be consecutive integers.
- Uniqueness: No duplicate priorities allowed.

When adding or editing rules:

- Adding a new rule sets its priority to $n+1$.
- Inserting a rule shifts subsequent priorities by +1.
- Editing a rule's priority automatically reorders the list.

Intrusion Defense



Intrusion Defense monitors network transmission and detects suspicious activities.

When a suspicious event is detected, the system can send alerts or take proactive measures.

CFW integrates Converge Cloud's threat intelligence, basic protection, and virtual patching capabilities.

By performing real-time monitoring, statistics, and analysis on network perimeter traffic, CFW can detect:

- Intrusions
- Malicious outgoing requests
- Unknown risks

It provides real-time protection and alerts across Philippine regions.

Logs

Rule Hit Logs

Records the rule hits to assist in security audits.

The rule matching logs display the 5-tuple information of all allowed, observed, or blocked data flows.

You can view which rule was applied by clicking a button.

Operation Logs

Operation logs include:

- User login logs – Track all account login activities.
- Toggle operation logs – Record enabling and disabling of firewalls.
- Rule operation logs – Record add, delete, and edit operations on access control rules.

Use Cases

Outbound Access Control

Outbound access control is an inside-out scenario. When you need to block access to an external address or domain name from a CVM instance on the cloud, configure outbound access control rules for all public IP addresses that need to be controlled to meet your security needs.

Inbound Access Control

Inbound access control is an outside-in scenario. When you need to prohibit an external address from initiating access to a CVM instance on the cloud, configure inbound access control rules for all public IP addresses that need to be controlled to meet your security needs.

Hit Log Audit

When you need to audit the hits of the access control rules of CFW or trace the effective rules in case of failure, you can use the rule hit log audit feature of CFW for quick log audit and failure recovery, improving your security Ops efficiency and reducing Ops costs.

Operation Log Audit

When you need to manage the operations of CFW, you can use the user operation log feature of CFW to quickly locate the operation time, operation content, and operation account to meet your management needs.

Industry Compliance Requirements

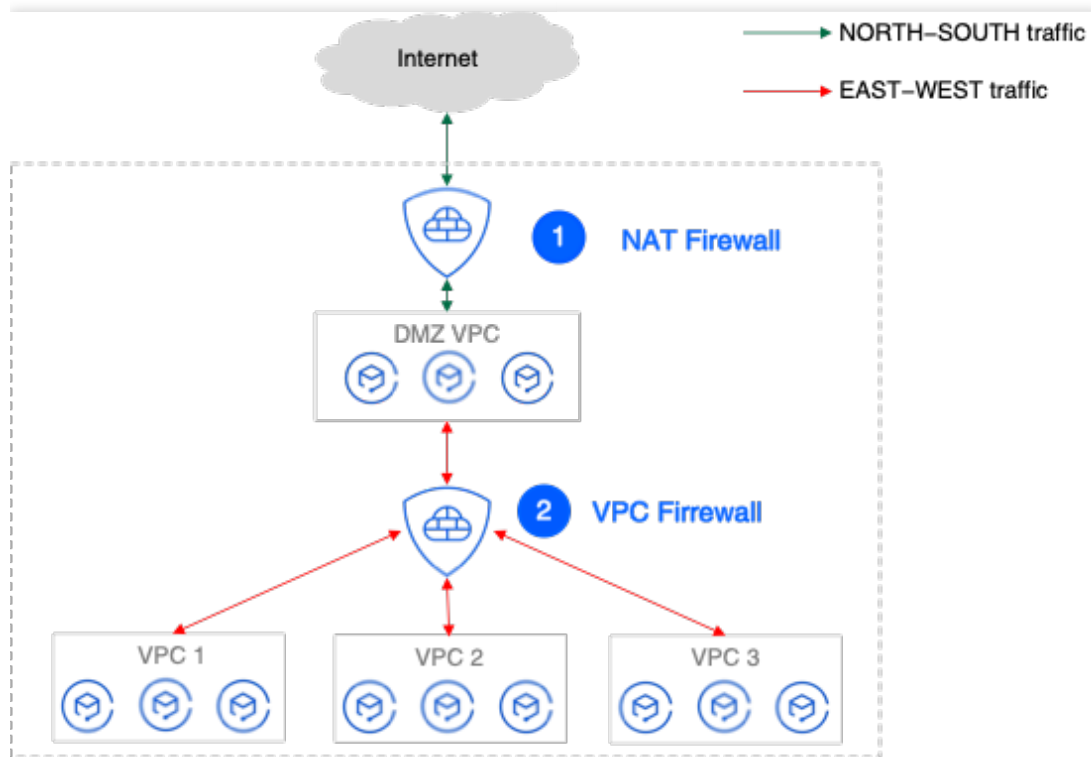
When you are ready to migrate your business to the cloud, you can quickly implement access control and intrusion detection for your business on the cloud by enabling CFW, helping you meet industry compliance requirements and cybersecurity classified protection requirements.



Cloud Firewall Networking Planning

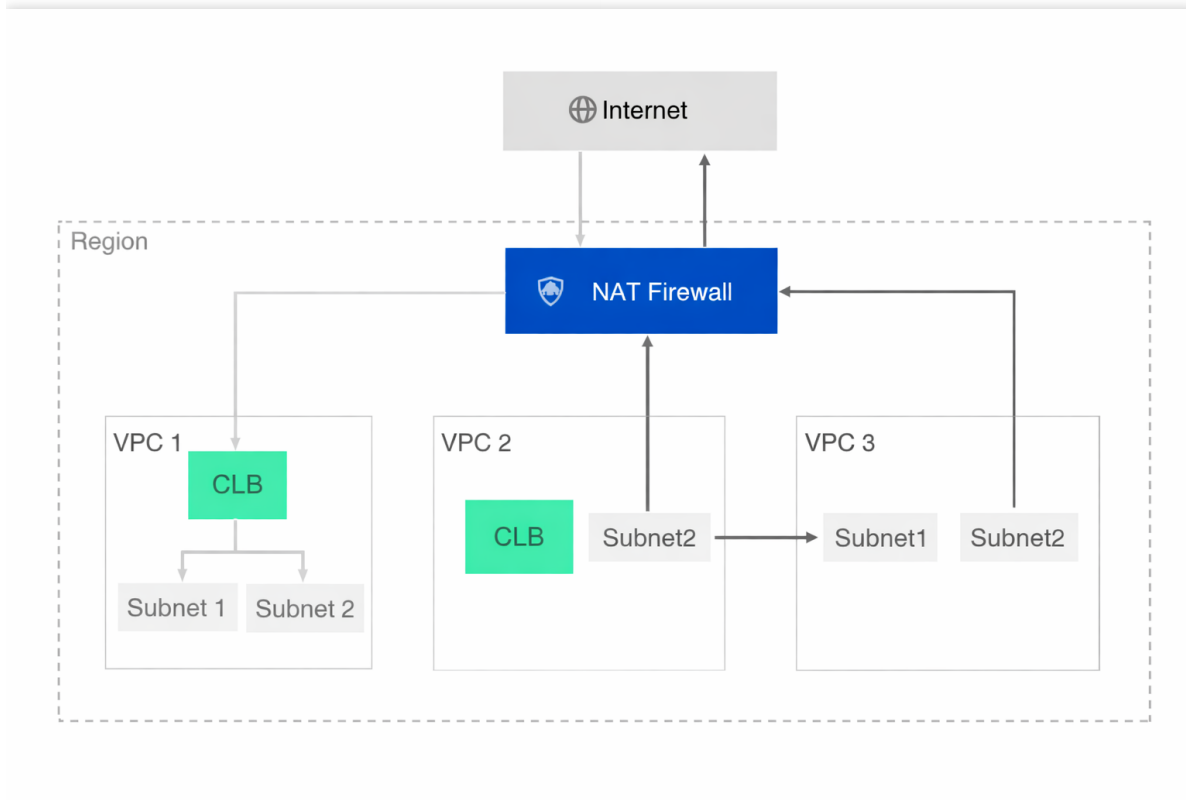
Network Planning Best Practices

CFW supports two types of firewalls: NAT Firewall (NAT CFW) and Inter-VPC Firewall (VPC CFW). The network planning shown in the following figure is for your reference.



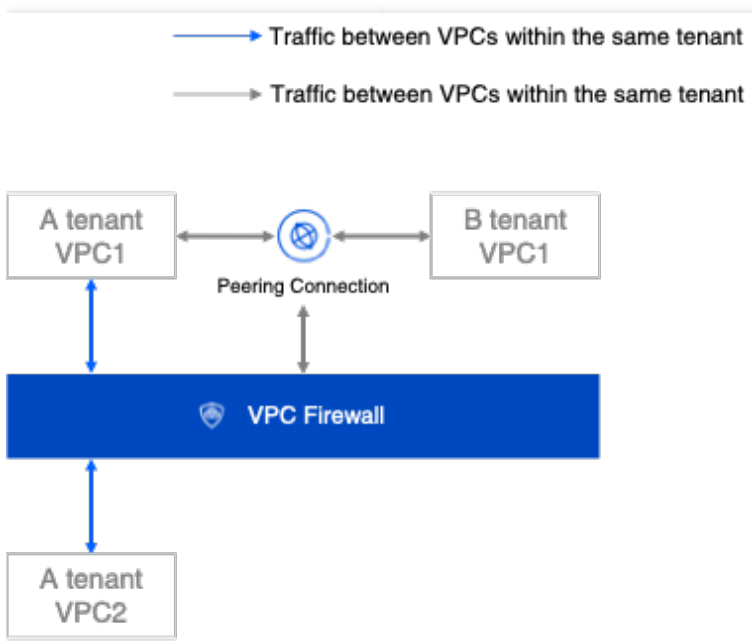
NAT CFW Network Planning Best Practices

NAT CFW is used between the Internet and a VPC.



VPC CFW Network Planning Best Practices

The VPC firewall is used to protect traffic between VPCs, whether they belong to the same tenant or different tenants.





Purchase Guide

Billing Overview

Converge Cloud Firewall Editions

Converge Cloud Firewall (CFW) offers different editions designed to meet the security and performance needs of businesses of all sizes. Each edition provides varying levels of protection, scalability, and management features depending on your network requirements and asset scale.

Editions Overview

Edition	Elastic Scaling	Billing Mode	Internet Access Control	Inter-VPC Firewall	Enterprise Security Group	Threat Intelligence	Intrusion Prevention (IPS)	Traffic Visualization
Enterprise	Fully Supported	Monthly Subscription	Supported	Supported (Expandable)	Supported	Supported	Supported	Supported

- Note:
- All Converge Cloud Firewall editions operate under a monthly subscription model. There are no hourly or pay-as-you-go billing options.
 - Edition downgrades are not available after purchase.
 - Enterprise security groups are available across all editions. Any changes to this feature will be communicated in advance and will not affect existing subscriptions.

Key Feature Highlights

Elastic Scaling

Higher editions of Converge Cloud Firewall support elastic performance scaling, allowing you to dynamically adjust firewall capacity based on asset load and network traffic.

Internet Access Control

Control and monitor both inbound and outbound Internet traffic. Create policies that protect cloud resources from malicious IPs, domains, or suspicious traffic patterns.

Inter-VPC Firewall

Business and Enterprise editions support inter-VPC traffic isolation, allowing you to create security boundaries between Virtual Private Clouds for better compliance and protection.

Threat Intelligence

Integrate global and regional threat intelligence to automatically detect and block malicious outbound or inbound traffic, improving cloud



security posture.

Intrusion Prevention System (IPS)

An intelligent intrusion detection and prevention mechanism that continuously monitors and blocks exploits, attacks, and abnormal behaviors within the network.

Traffic Visualization

Gain complete visibility of your network's traffic, rule hit rates, and access logs. Visual analytics make it easier to monitor performance and detect anomalies.

Access Methods

You can manage Converge Cloud Firewall through the official console:

Cloud Firewall Console — Log in to the [Converge Cloud Firewall Console](#) to configure rules, monitor logs, and manage security policies.

Note:

All configurations, scaling, and management functions are hosted within Converge Cloud's data centers located in the Philippines, ensuring full data residency and compliance with local regulations.

Renewal Instructions

Cloud Firewall Renewal and Expiration Policy

Cloud Firewall resources will be destroyed 14 days after expiration (for details, please refer to the Cloud Firewall Overdue Payment Instructions - Purchase Guide - Documentation Center - Converge Cloud). To ensure the service operates smoothly and normally, it is important for you to pay attention to the expiration date of the Cloud Firewall package and renew it before it expires. We recommend setting the Cloud Firewall to automatically renew upon expiration. Alternatively, you can manually renew the resources on the Cloud Firewall Renewal page.

Note:

During the product arrears period (i.e., within 14 days after the product expires and before the system recovers resources), the Cloud Firewall will not charge for retaining resources. If you renew during the product arrears period, your package's available duration will be calculated from the product's expiration time, rather than from the time you renew. If you wish to recalculate the available duration of the package, please destroy the resources and repurchase the Cloud Firewall package.

Resource deletion Upon Expiration

Note:

If you are a customer of a Converge Cloud partner, the rules regarding resources when there are overdue payments are subject to the agreement between you and the partner.

You cannot access the console after your subscription expires.

All your protection will be disabled 7 days after your subscription expires.

Traffic protection will be disabled, but your configurations will be retained — you can renew your subscription to restore your configurations.

All your Cloud Firewall resources will be deleted 14 days after expiration.

Your configurations will be permanently deleted and cannot be recovered. In this case, you will need to re-purchase and reconfigure the Cloud Firewall package.

Note:

During the product arrears period (i.e., within 14 days after the product expires and before the system recovers resources), the Cloud Firewall will not charge for retaining resources. If you renew during this period, your package's available duration will be calculated from the product's expiration time, rather than from the time you renew. If you wish to recalculate the available duration of the package, please destroy the resources and repurchase the Cloud Firewall package.



Purchase Instructions

1. Go to the [Cloud Firewall purchase page](#) and select a package according to your demands. You can also customize your billable items, and your fees are automatically calculated.
2. After selection, click "Place Order" and complete the payment.

Operation Guide

CVM Creation

CVM is an automatically scalable computing service. With the strengths of elastic computing, flexible configuration, stability and reliability, simple management, secure network, and comprehensive protection, it realizes cost control and business protection for pain points such as sudden traffic bursts.

Creating a CVM

1. Choose Cloud Computing & Networking > CVM.
2. Click Create.
3. On the CVM page, choose Customize Configuration > 1: Select Region and Instance Type, select the VPC and its corresponding subnet of the CVM under the Network field, and then click Next: Select Image.
4. Select Public Image, select the CentOS-related image, and then click Next: Select Storage and Bandwidth.
5. Modify the default storage and bandwidth settings as needed and click Next: Configure Security and Host.
6. Select it if a security group that allows all ports already exists. If no available security group exists, you can select Create Security Group.
7. Configure the login password of the host and click Next: Confirm Configuration Information.
8. On the Confirm Configuration Information page, view all the configured information. If everything is correct, you can click Activate to complete the creation.

Custom Routing Mode Configuration Guide

Step 1: Creating an Instance in Custom Routing Mode

See [Inter-VPC Firewall Toggle > Creating an Inter-VPC Firewall](#) to create a target instance, where the routing mode is set to custom routing.

Step 2: Configuring a Traffic Steering Route

Check the VPCs at both ends of the peering connection, which are VPC A and VPC B.

1. On the Route Table page, find the route table of VPC A, click the route table ID, and then select the default route table.
2. On the details page, click Add Routing Policy.
3. In the Add Routing Policy pop-up window, add a routing policy with the destination of VPC B IP range and the next hop of a high-availability virtual IP address, and click Create.
4. On the details page, disable the routing toggle for the original peering connection and immediately enable the route you just configured.

Note:

Changing a route may cause a momentary disconnection in the network. It is recommended to perform this operation during off-peak workload hours.

5. On the Route Table page, find the route table of VPC B and select the default route table.
6. Repeat the previous steps to add a firewall route entry.



Step 3: Verifying Whether the Firewall Is Working Properly

See Log Audit to check whether there are traffic logs.

See Log Audit to check whether the intrusion prevention is normal.

Configure inter-VPC rules and check whether they are hit normally.



Firewall Toggle

Inter-VPC Firewall Toggles

Feature Description

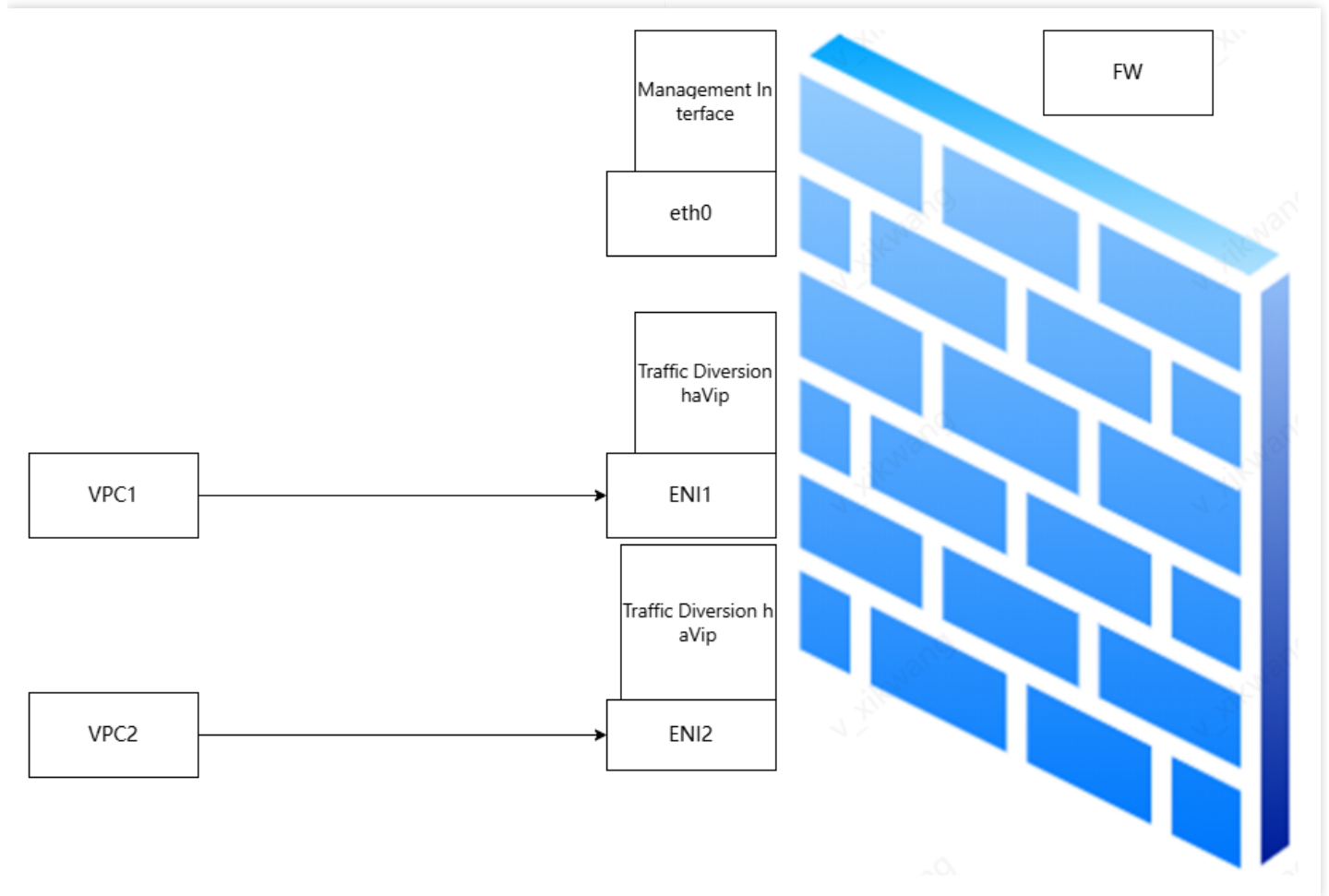
Product Features

Inter-VPC CFW provides traffic control and security protection for private network VPCs and inter-VPC access. It supports cross-region and cross-tenant traffic access control, and offers the IPS feature.

Use Cases of Inter-VPC CFW

Working Mode	Prerequisite	Use Case
Normal mode	A peering connection between VPCs has been established, the route table has been completed, and the VPCs can communicate with each other.	Inter-VPC Firewall can manage inter-VPC access traffic under a single tenant.
Administrator mode	A peering connection between cross-tenant VPCs has been established, the route table has been completed, and cross-tenant VPCs can communicate with each other.	Each tenant is responsible for managing the traffic that other tenants access the VPCs of this tenant, and the administrator mode can be used as the normal mode.
Multi-account mode	A peering connection between cross-tenant VPCs has been established, the route table has been completed, and cross-tenant VPCs can communicate with each other.	CFW needs to be created under multiple accounts across tenants, and traffic passes through two firewalls for access control.

Principles of Traffic Routing for Inter-VPC Firewall



- As shown in the preceding figure, VPC 1 and VPC 2 of the tenant are connected to the firewall. Traffic routing should be implemented first. In this example, a cross-tenant ENI is used to achieve traffic routing. The main implementation principles are as follows:
- FW is an overlay instance of the reserved account.
- Each VPC connected to the inter-VPC firewall will be assigned a firewall subnet, and a cross-tenant ENI will be created for the firewall. This ENI serves as a traffic routing NIC of the VPC and will be assigned a high-availability virtual IP address, to achieve high availability.
- If you switch the next hop route to the high availability virtual IP address of the traffic routing NIC, the traffic will be directed to the firewall.

Operation Guide

Operation Guide

1. Log in to the Converge Cloud Firewall console. In the left sidebar, choose Firewall Toggle > NAT Firewall Toggle to go to the NAT Firewall Toggle page.
2. On the NAT Firewall Toggle page, click Firewall Instance to go to the firewall instance page. Existing instances are displayed as cards in a list. If there is no firewall instance, you can click Create Instance to add instances.
 - The current version only supports a single region.
 - The list of available VPCs displays the information of all VPCs under the current account, and you can select multiple VPCs. If the selected VPCs have been connected to other instances, they will be displayed as grayed and cannot be selected.
3. You can perform other auxiliary operations.
 - Synchronize Assets: On the Network Topology and Firewall Instance tabs under the Inter-VPC Toggles page, click Synchronize Assets to call the backend API promptly to read and synchronize the asset information of the current user again. This can avoid a situation where the user's asset scale is changed within the polling interval of the backend but has not been synchronized.
 - Update Engines: Under the Network Topology or Firewall Instance tab, click Update Engines to immediately update the backend engine. After the update is completed, the Update Engines button becomes gray.
4. On the Firewall Instance tab, click Configure Instance.
5. In the Connect VPC and Public Network IP pop-up window on the right side, click Add Access VPC or Reselect VPC to adjust the VPCs connected to the current firewall instance.
6. On the Port Forwarding tab, create or edit port forwarding rules.
7. On the Egress Binding tab, create or edit egress binding rules.

Network Topology Diagram

Converge Cloud Firewall provides a visual view to help you quickly organize the access relationship between the VPC and the Internet. The network topology diagram illustrates the access relationship

between the Internet and the VPC. Traffic between NATs with the toggle enabled will be routed to the firewall for filtering and protection.

1. Log in to the Converge Cloud Firewall console. In the left sidebar, choose Firewall Toggle > NAT Firewall Toggle to go to the NAT Firewall Toggle page.
2. On the NAT Firewall Toggle page, click Network Topology to go to the Network Topology page.
3. Hover the mouse pointer over a VPC node to view its brief information. You can click a VPC node to view its corresponding information.

Description of Abnormal Scenarios for NAT Firewall

- When you configure a firewall instance, at least one EIP needs to be bound. When there is only one bound EIP left, the unbind button is displayed as gray and unclickable.
- When the firewall toggle is disabled, the system will automatically restore the routing policies of all route tables associated with subnets and the port forwarding rules corresponding to subnets. The traffic of all subnets will be recovered to their original paths and will not pass through NAT Firewall.

Creating Inter-VPC Firewall Instances

A VPC is a user-defined and exclusive network space on the cloud that is logically isolated.

A peering connection is a large-bandwidth and high-quality cloud resource interconnection service that supports multi-VPC and heterogeneous network interconnections. The interconnection of a peering connection does not transmit.

Creating a VPC

1. Choose Cloud Computing & Networking > VPC.
2. Click Create.
3. Enter the VPC name and CIDR block, and the name and CIDR block of the subnet under the VPC, select an availability zone, and then click Create.

Since a peering connection will be established later, it is recommended that the VPC names here be more semantically readable, such as vpc1 and vpc2.

Creating a Peering Connection

1. Choose Peering Connection in the left sidebar.
2. Click Create. In the Create Peering Connection pop-up window, enter the peering connection name and select a region and a VPC.

Here, the selection of the local network and the remote network requires attention, as it will impact the subsequent use of the CFW UDP protocol (the local network corresponds to the client, and the remote network corresponds to the server).

3. After the peering connection is created successfully, a window is displayed. You can go to the Route Table page by clicking Modify Route Table in the pop-up window or through the left sidebar.

Configuring a Route Table

1. On the Route Table page, select the VPCs you created before and configure them. Note that two VPCs need to be configured.
2. Click the blue ID corresponding to a VPC to go to the details page.
3. Click Add Routing Policy and enter the destination (another VPC CIDR), the next hop type (peering connection), and the next hop information. (The previously created peering connection is displayed here by default.) Then, enter the remarks and click Create.
4. After the routing policy is created successfully, the corresponding information is displayed in the list.

5. Perform the preceding steps for another VPC.

Creating Inter-VPC Firewall Instances

Note:

- In normal mode, you need to select a VPC with a connected peering connection under the local account.
- In administrator mode or multi-account mode, you need to select two VPCs with cross-tenant peering connections during the first access.

1. Create an Inter-VPC Firewall. In VPC mode, choose Firewall Toggles > Inter-VPC Toggles in the left sidebar.
2. On the Inter-VPC Toggles page, click Firewall Instance. On the Firewall Instance page, click Create Firewall.

The screenshot displays the 'Firewall toggles' page in the AWS Management Console. At the top, there are tabs for 'Protection object', 'NAT firewalls', and 'VPC boundary switch (legacy)'. Below these, the 'Monitoring' section shows three metrics: 'Firewall bandwidth peak' at 177 bps, 'Single instance peak bandwidth' at 177 bps, and 'Bandwidth usage' at 20 Gbps. A 'Remaining quota: 9.9Gbps' is also shown. At the bottom, there are tabs for 'Network topology', 'Firewall instance', and 'Firewall toggles'. Below the 'Firewall instance' tab, there are buttons for 'Create firewall', 'Update engines', 'Sync assets', 'Sync routes', and a dropdown menu for 'All firewalls'. The 'Create firewall' button is highlighted with a red box.

3. In the Create Inter-VPC Firewall pop-up window, enter an instance name, select Private Network Mode, and then click Next.

Note:

- Instance Name: Indicates the name customized when you create a firewall instance.
- You can configure the firewall instance bandwidth specification and connected networks, and click Next. If the number of instances does not meet your needs, you can click + on the right side to create multiple firewall instances.
- Region: Select the region where the VPC to be protected is located.
- Cross-region disaster recovery: Inter-VPC Firewall supports cross-region disaster recovery. After you check it, the primary and secondary engines are automatically deployed in different AZs.
- Availability Zone: Select an availability zone as needed.
- Instance Bandwidth: An instance supports 200 Mbps to 10 Gbps (up to 6 Gbps is configurable in the

console). To configure a bandwidth greater than the configurable limit, submit a ticket or perform scale-out. If you need more than the maximum bandwidth available, you can create multiple firewall instances. Note that each firewall instance should stay within its throughput limit.

- Inter-VPC Firewall cannot communicate with the basic network. Before connecting to the network, make sure that peering connections have been created between VPCs. If no connection is established between VPCs, the connection does not take effect, and no firewall toggle is displayed.
- An Inter-VPC Firewall instance allows up to 10 VPCs in the same region, and you can create multiple instances in the same region. It is recommended to plan the VPCs to be connected according to regions in advance before creating firewall instances and accessing the network.

4. Click Connected Networks, select VPCs within the region as needed, and then click OK. Note that a VPC can connect to only one firewall instance.

Create inter-VPC firewall

1. The current edition supports 10 VPC(s). To increase the quota, please [Submit a ticket](#).

2. You can deploy different firewall instances for different regions as need. Note that each VPC can only be connected to one firewall instance.

3. Firewall instances are connected by default. But the firewall only allows transfer between VPC connected via Peering Connect.

4. Make sure that the connected VPC is connected to the network through Peering Connection.

Step 1

Step 2

Step 3

Create a firewall instance and connect it to a network instance

	Firewall instance name	Instance region	Remote disast...	Zone	Quota	Connect as an instance
1	cfw-primary - Instance 1	luzon	☐	Random AZ	200 Mbps	Connected networks (0)

Back

Next

Cancel

Select the VPC to connect to

i Each firewall instance can connect up to 10 network instances. Create more firewall instances if you have many network instances.

Select VPCs to associate

Search by instance ID/name, CIDR block

☐	ID/name	IP CIDR	Region
☐	Dedicated firew...	IPv4: 10.199.0.0/24	luzon
☐	test-vpc-01	IPv4: 10.10.0.0/22	luzon
☐	cfw usage--Don'...	IPv4: 9.0.0.0/16 +1	luzon
☐	Dedicated firew...	IPv4: 10.199.16.0/24	luzon

0 of 4 selected

OK

Cancel

5. Configure How to Create the Routing Subnet, Firewall VPC, and Routing Mode, and click Create after checking these settings.

Note:

CFW creates a subnet in the connected VPC to route traffic to the firewall in different ways. Once the routing subnet is created, it cannot be modified.

- Proprietary IP range preferred: CFW automatically selects an idle subnet IP range in the selected VPC. If the VPC has no subnet quota, an extended IP range in the VPC is used.
- Extended IP range preferred: CFW will choose an idle extended IP range reserved by the VPC first. This mode does not consume the VPC's subnet quota. An extended IP range refers to a secondary IP range in a VPC.
- Custom: You can only specify a /24 subnet within the CIDR block of the current VPC, such as



192.168.0.0/24.

6. Enable the firewall toggle. Once the toggle is enabled, the inter-VPC access traffic will be directed to CFW for filtering and forwarding.
7. Choose Security Policies > Access Control > Add Rules to add access control rules.
8. Choose Cloud Log Service > Access Control Logs to view the generated interception or observation log.



Performance Metrics

Performance Metrics for Inter-VPC Firewall Access Quantities

Bandwidth Performance	Machine Specification	Maximum Number of Connected VPCs	Intrusion Prevention
0M~600M	4c8g	10	Not supported.
600M~2048M	8c16g	10	Supported.
2048M~4096M	16c32g	10	Supported.
4096,~6144M	32c64g	10	Supported.
6144M~10240M	64c128g	10	Supported.

NAT Firewall Toggle

Creating a NAT Firewall Instance

Choosing Create Firewall Instance > New Mode

1. Log in to the CFW console. In the left sidebar, choose Firewall Toggle > NAT Firewall Toggle. On the NAT Firewall Toggle page, you can perform operations such as creating instances, synchronizing assets, and viewing and monitoring the bandwidth information based on NAT Firewall. Under NAT Firewall Toggle, you can click Create Instance to add instances.

Warning:

Once a NAT Firewall toggle is enabled, the traffic of the corresponding subnet will pass through the firewall. At that time, access control rules and intrusion prevention will take effect for the firewall, and traffic logs will also be generated.

2. In the Create NAT Firewall pop-up window, you can create a NAT Firewall instance for the current account, configure related fields, select the mode as needed, and then click Next.
3. Under Step 2, select the VPC to be connected to CFW and click Next.
4. Select a traffic routing mode. Three modes are provided: Proprietary IP Range Preferred, Extended IP Range Preferred, and Custom. Then, click Create and wait for the instance creation to complete.

Note:

- CFW will create a /24 subnet in the connected VPC to redirect traffic to the firewall and public network traffic egress. You can select different ways to create subnets.
- Proprietary IP range preferred: CFW automatically selects an idle subnet IP range in the selected VPC. If the VPC has no subnet quota, an extended IP range in the VPC is used.
- Extended IP range preferred: CFW will choose an idle extended IP range reserved by the VPC first. This mode does not consume the VPC's subnet quota.
- Custom: You can only specify a /24 subnet within the CIDR block of the current VPC.

Choosing Create Firewall Instance > Access Mode



1. Choose VPC > NAT Gateway > Create NAT Gateway to configure the VPC to be connected.
2. After the NAT Gateway is created successfully, you can modify the next hop route table of the VPC to point to the NAT Gateway. At this point, the VPC can access the public network through the NAT Gateway, and the gateway ID is recorded.
3. Log in to the CFW console and click Create NAT Firewall. On the Create NAT Firewall page, configure the instance specification, select the access mode, and then click Next.
4. Check the instance ID to be connected to the NAT gateway and click Next.
5. Select a routing mode based on the VPC assignment information of your project and click Create.



Performance Metrics

Performance Metrics Related to NAT Firewall Access Quantities

Mode	**Machine Specification**	**Maximum Number of Connected VPCs**	**Maximum Number of EIPs**	**NAT Gateway**
New mode	Instance with less than 6 million RPS (4 cores and 8 GB)	8	8	/
	Instance with more than 6 million RPS (over 8 cores and 16 GB)	10	8	/
Access mode	Instance with less than 6 million RPS (4 cores and 8 GB)	4	/	4
	Instance with more than 6 million RPS (over 8 cores and 16 GB)	5	/	5



Feature Description

Features

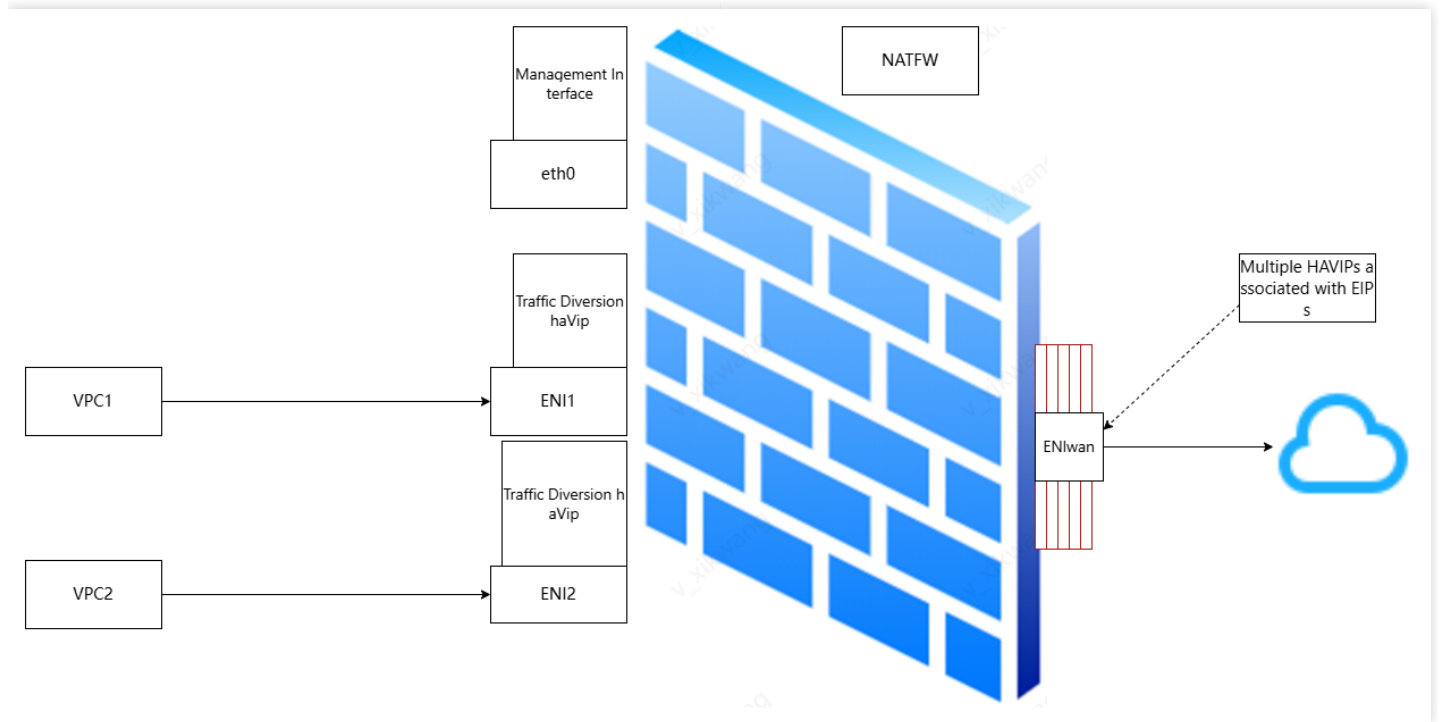
The NAT Firewall toggle supports traffic control and security protection based on private network assets, as well as network traffic forwarding based on SNAT and DNAT.

NAT CFW Use Cases

Working Mode	Prerequisite	Use Case
New mode	The tenant has an EIP that can access the public network.	If there is no NAT gateway in the current region, the new mode allows you to use the built-in NAT features of NAT Firewall to enable specified instances to access the Internet through the firewall.
Access mode	The VPC under the tenant can connect to the Internet through a NAT gateway.	If there is a NAT gateway in the current region or you want to keep the egress IP address of the public network unchanged, the access mode allows for seamless integration of NAT Firewall between the NAT Gateway and CVM instance.

NAT Firewall Routing Principles

Assume that VPC 1 and VPC 2 of a tenant need to connect to CFW. Traffic routing should be implemented first. In this example, a cross-tenant ENI is used to achieve traffic routing. The main implementation principles are as follows:



- The NAT Firewall engine is an overlay instance of the reserved account.
- Each VPC connected to the NAT Firewall will be assigned a firewall subnet under the VPC, and a cross-tenant ENI will be created for the firewall. This ENI serves as a traffic routing NIC of the VPC and will be assigned a high availability virtual IP address from the traffic routing subnet, to achieve high availability.
- If you switch the next hop route to the high availability virtual IP address of the traffic routing NIC, the traffic will be directed to the firewall.
- If a cross-tenant egress network port is assigned from one of the VPCs, for example, the ENIWan port in the figure on the left side, all VPC traffic will access the public network through the ENIWan port. To ensure high availability, you can assign a high availability virtual IP address to the ENIWan port. You can also bind the virtual IP address to an EIP to realize public network access.

Note:

Traffic that accesses a VPC passes through the subnet routes of the VPC. Based on the principle that larger subnets have higher priorities, traffic is selected and directed to a NAT Firewall. Then, NAT forwarding is performed to access public networks. In new mode, you can bind the ENIWan port to an EIP. In access mode, you can bind the ENIWan port to a NAT gateway.

Operation Guide

Operation Guide

1. Log in to the CFW console. In the left sidebar, choose Firewall Toggle > NAT Firewall Toggle to go to the NAT Firewall Toggle page.
2. On the NAT Firewall Toggle page, click Firewall Instance to go to the firewall instance page. Existing instances are displayed as cards in a list. If there is no firewall instance, you can click Create Instance to add instances.
 - The current version only supports a single region.
 - The list of available VPCs displays the information of all VPCs under the current account, and you can select multiple VPCs. If the selected VPCs have been connected to other instances, they will be displayed as grayed and cannot be selected.
3. You can perform other auxiliary operations.
 - Synchronize Assets: On the Network Topology and Firewall Instance tabs under the Inter-VPC Toggles page, click Synchronize Assets to call the backend API promptly to read and synchronize the asset information of the current user again. This can avoid a situation where the user's asset scale is changed within the polling interval of the backend but has not been synchronized.
 - Update Engines: Under the Network Topology or Firewall Instance tab, click Update Engines to immediately update the backend engine. After the update is completed, the Update Engines button becomes gray.
4. On the Firewall Instance tab, click Configure Instance.
5. In the Connect VPC and Public Network IP pop-up window on the right side, click Add Access VPC or Reselect VPC to adjust the VPCs connected to the current firewall instance.
6. On the Port Forwarding tab, create or edit port forwarding rules.
7. On the Egress Binding tab, create or edit egress binding rules.

Network Topology Diagram

CFW provides a visual view to help you quickly organize the access relationship between the VPC and the Internet. The network topology diagram illustrates the access relationship between the Internet and the

VPC. Traffic between NATs with the toggle enabled will be routed to the firewall for filtering and protection.

1. Log in to the CFW console. In the left sidebar, choose Firewall Toggle > NAT Firewall Toggle to go to the NAT Firewall Toggle page.
2. On the NAT Firewall Toggle page, click Network Topology to go to the Network Topology page.
3. Hover the mouse pointer over a VPC node to view its brief information. You can click a VPC node to view its corresponding information.

Description of Abnormal Scenarios for NAT Firewall

- When you configure a firewall instance, at least one EIP needs to be bound. When there is only one bound EIP left, the unbind button is displayed as gray and unclickable.
- When the firewall toggle is disabled, the system will automatically restore the routing policies of all route tables associated with subnets and the port forwarding rules corresponding to subnets. The traffic of all subnets will be recovered to their original paths and will not pass through NAT Firewall.

Asset Center

This document describes how to view and manage data and information related to each asset in Asset Center. You can better understand the current status of assets, manage assets, and predict and prevent security incidents by viewing the detailed information on your private network assets, VPCs, and subnets.

Operation Guide

1. Log in to the CFW console. In the left sidebar, click Asset Center to go to the Asset Center page.
2. On the Asset Center page, view server and network asset information and perform related operations. Server assets include both public and private network assets, and network assets include gateways, NICs, VPCs, and subnets.

Server Assets

At the bottom of the Asset Center page, you can click Server Assets to view the details of all server assets under the account, including public and private network assets. You can click the Type button to filter and display information about assets of different types, including asset instance ID/name, IP address, asset type, region, and bandwidth.

Network Assets

At the bottom of the Asset Center page, you can click Network Assets to view detailed information on all network assets under the account. Network assets include four types: gateway, NIC, VPC, and subnet. You can click Type to filter and display assets of different types.

- View the VPC details: In the VPC list, click the ID of the target VPC to jump to the details page of the VPC.
- View additional VPC information: In the Subnet, CVM, or Interconnection VPC column, click the blue field to jump to the corresponding details page.

Traffic Center

The traffic center displays the traffic access between VPCs and contains the Inter-VPC Activities page.

Inter-VPC Activities

You can view the traffic access and protocol distribution between private clouds on the Inter-VPC Activities page.

Operation Steps

1. Log in to the CFW console. In the left sidebar, click Traffic Center and go to the Inter-VPC Activities tab.
2. On the Inter-VPC Activities tab, select a private cloud instance from the filtering box at the top and select a time period.
3. Hover the mouse pointer over the folding line graph for traffic statistics to view the bandwidth rate within a fixed period. You can also hover the mouse pointer over the protocol distribution pie chart on the right side to view the distribution percentage of each protocol.
4. At the bottom of the page, view the specific IP address of Inter-VPC Firewall, and the access destination, access source, access count, and other information on the private cloud. You can also enter the desired access source, access destination, or destination port number in the input box for precise searching.

Access Control

Inter-VPC Firewall Rules

Inter-VPC firewall rules provide multiple Access Control Lists (ACLs), each associated with a pair of connected Virtual Private Clouds (VPCs) and an inter-VPC firewall toggle.

This topic describes how to set up Inter-VPC firewall rules on the Converge Cloud Firewall Console.

Operation Guide

1. Log in to the Converge Cloud Firewall Console.
2. Select Access Control in the left navigation pane, and then select Inter-VPC Firewall Rules.
3. In the upper-left corner of the Inter-VPC Firewall Rules page, you can switch between different inter-VPC ACLs from the drop-down list of Firewall Toggle Name.

Note:

Unlike Edge Firewall and NAT Firewall ACLs, Inter-VPC ACLs have no direction limitations. The local and peer VPCs are equivalent. When configuring rules, you can determine the VPC based on the CIDR block of the access source and destination to differentiate the traffic direction.

Adding Rules

1. On the Inter-VPC Firewall Rules page, click Add Rule.
2. On the Add Rule page, details such as local and peer VPCs and firewall toggle information are pre-filled.
3. Enter the following details:
 - Access Source IP
 - Access Destination IP
 - Destination Port
 - Protocol and Policy
 - Description



Field Descriptions

Field	Description
Priority	Defines rule execution order. Rules with higher priority are processed first. Modifying or deleting priorities adjusts subsequent rules automatically.
Access Source	Must be an IP or subnet in the local or peer VPC's CIDR block. Cannot overlap with the access destination's range. Supports 0.0.0.0/0 as a wildcard.
Access Destination	Must be an IP or subnet in the local or peer VPC's CIDR block. Cannot overlap with the access source's range. Supports 0.0.0.0/0 as a wildcard.
Destination Port	Supports single ports (e.g., 80), ranges (e.g., 80/443), or multiple ports (e.g., 80,443,3389).
Protocol	Supported protocols: TCP, UDP, and ICMP.
Policy	Allow : Permits traffic and records hits and traffic logs. Observe : Permits traffic and records all logs. Block : Denies traffic but records access control logs.
Description	Rule description (up to 50 characters). Supports special markers such as #long connection# .

Wildcard Rules

Refer to Edge Firewall Rules for more information about supported wildcard configurations for IP address ranges.

Caution:

The CIDR blocks of the local and peer VPCs cannot be the same or overlap. Otherwise, the firewall cannot be enabled.

Access source and destination must belong to the CIDR blocks of the local or peer VPC. If both are set to 0.0.0.0/0 , it indicates all VPC addresses.

Rules entered with IPs outside these ranges will not take effect.

Adding Rules in Bulk

Note:

Each rule uses one line. New rules are added to the end of the list by default and have the lowest priority.

Scenario 1: Adding Multiple Rules at Once

1. Click Copy in the action column to duplicate an existing rule.
2. A maximum of 10 rules can be added at a time.
3. Complete all necessary fields.
4. Verify priority order.
5. Click OK to submit.

Scenario 2: Multiple Rules for the Same IP

1. Edit a rule with common field values.
2. Click Copy to duplicate (up to 10 rules).
3. Adjust specific fields and confirm priorities.
4. Click OK to submit.

After adding rules, you can view and manage them in the Rule List.

Importing, Backing Up, and Restoring Rules

- **Import Rules:** Click Import Rule to upload rules from a local file. You can specify an import location, download a template, or export existing rules.
- **Backup Rules:** Click Backup Rules (top-right) to save current Inter-VPC Firewall configurations.
- **Restore Rules:** Click Roll Back beside a backup file to restore previous configurations.

To create a backup:

1. Go to Backup and Rollback Rules.
2. Click Create Backup.
3. Select Inter-VPC Firewall Rule Group, add a description, and click OK.



More Information

For additional guidance:

- [Edge Firewall Rules: Managing inbound and outbound edge traffic.](#)
- [NAT Firewall Rules: Managing NAT-based traffic control.](#)
- [Special Scenarios: Handling advanced or unique network configurations.](#)
- [Inter-VPC Firewall Overview: Understanding cross-VPC access management.](#)

Converge Cloud — Secure and Scalable Network Control for the Philippines

Special Use Cases

This topic describes special scenarios of the Converge Cloud Firewall (CFW) access control feature.

Managing the Execution Priority of Rule Lists

You can manage the execution priority of Edge firewall rules, NAT firewall rules, and Inter-VPC rules. The following takes Edge firewall rules as an example.

Scenario 1: Sorting Rules in the List

1. Log in to the Converge Cloud Firewall console and select Access Control → Edge firewall rules in the left navigation pane.
2. On the Edge firewall rules page, click Sort on the top of the list to enter the modification mode.
3. You can move the positions and priority of rules in batch within the current page and sort the rules by dragging the icons on their left.
4. When you are done, click Save.

Sort Operations:

- If you change the position of any rule when you release the mouse cursor, one sort operation has taken place.
- If you do not change the position of any rule when you release the mouse cursor, no sort operation has taken place.
- After a sort operation takes place, the Cancel button becomes active.
- Click Recover once to return the list to the state before the last sort operation.
- If you click Save, you will see a "Sorted successfully" toast at the top of the page.
- If you click Cancel, the list will return to the initial state and all sort operations will not take effect.

Scenario 2: Modifying a Rule to Move It to a Specified Position

When you need to move a rule within a large range, sorting can be inefficient. Instead, you can use the modification feature. You can modify the execution priority of only one rule at a time.

1. Log in to the Converge Cloud Firewall console and select Access Control → Edge firewall rules in the left navigation pane.
2. On the Edge firewall rules page, find the rule you want to move in the list and determine the new

position.

3. Click **Modify** on the right to enter the rule modification mode.
4. Modify the execution priority to the desired value.

Note:

Execution priority values cannot be repeated and must be continuous. The minimum value is 1, and the maximum value is the total number of rules in the current list.

5. Click **Complete** and check the rule priority.

Note:

When you modify the execution priority of a rule in the list, the positions of all other rules will be automatically adjusted.

Scenario 3: Inserting a Rule to a Specified Position in an Existing List

Converge Cloud Firewall allows you to insert a rule between any two rules, and the inserted rule will be executed based on priority.

For example, if you want to insert a rule between positions 2 and 3:

1. Log in to the Converge Cloud Firewall console and select **Access Control** → **Edge firewall rules** in the left navigation pane.
2. On the **Edge firewall rules** page, find the rule in position 3 and click **Add one above** on the right.
3. The rule modification box will be displayed above the rule in position 3.
4. In the box, enter the fields of the new rule and click **Complete** to insert the rule.

Note:

The inserted rule will take the position of the rule below it, and the execution priority of all rules below it will move down by one position.

Checking if Rules Are Effective

Method 1:

Check the hit counts in the access control list. If there are hits, the rules have taken effect.

**Note:**

If a rule has zero hits, it doesn't necessarily mean it's misconfigured. It may simply have no hits for the time being.

Method 2:

Select Log Auditing → Access Control Logs in the left navigation pane to view access control logs (rule hit logs).

If a rule is included in the log, the rule has taken effect.

Operation Locking

At any one time, only one user is allowed to perform any of the following operations on a single access control list with the same AppID (the firewall ID is used for VPCs):

- Add rule
- Import rule
- Sort
- Modify
- Add one above

When performing operations on a list, you may see a toast message:

"The list is being modified by others. Please wait."

This means another user is currently performing operations on the list.

Note:

Operations are locked for 5 minutes and will be automatically unlocked after that period.

More Information

For more information, please see Access Control in the Converge Cloud documentation.

NAT Firewall Rules

Access control rules can filter specific domain names or filter traffic by geographic location. The NAT firewall has two access control rule lists — Inbound Rules and Outbound Rules.

- Inbound Rules apply to incoming north-south traffic over the edge firewall.
- Outbound Rules apply to outgoing north-south traffic over the edge firewall.

This topic describes operations related to Inbound Rules; operations for Outbound Rules are similar.

Operation Guide

1. Log in to the Converge Cloud Firewall Console.
2. Select Access Control in the left navigation pane, and then select NAT Firewall Rules.
3. On the NAT Firewall Rules page, select a region, and click Inbound Rules.

On the Inbound Rules page, you can:

- Create access control rules for different regions.
- View rule list details (used and total quotas).
- See recent operations and access control logs.

Recent operations include:

- Details – View specific operation details.
- View operation logs – Review detailed action history.

Adding Inbound Rules

1. Click Add Rule on the Inbound Rules page.
2. Configure the rule in the Add Inbound Rule window.

Access Source Type: IP Address, Geographic Location, Cloud Vendor, or Address Template

Access Destination Type: IP Address, Asset Instance, Resource Tag, Address Template, or Asset Group

Select Priority, specify Destination Port, Protocol, and Policy, enter a description, and click OK.

Note:

Access destination type region refers to the region where the cloud instance is located. Access source



type refers to the type of external source when adding an inbound rule.

Field Descriptions

Field	Description
Priority	Determines rule order. Higher priority rules are evaluated first. When modifying a rule's priority, lower ones adjust accordingly.
Access Source	The source of inbound traffic. Supports IP, CIDR block, or geographic location.
Access Destination	The private network asset in the selected region. Supports IP, instance, tag, or group.
Destination Port	Supports single, range, or multiple ports (e.g., 80 , 80/443 , 80,443,3389). Not required for ICMP.
Protocol	Supported inbound: TCP, UDP. Supported outbound: TCP, UDP, ICMP, HTTP, HTTPS, SMTP, SMTPS, DNS, FTP.
Policy	Allow : Permit traffic and record hits (no access control logs). Observe : Permit and log all hits. Block : Deny traffic and log access attempts.
Description	Up to 50 characters. Use # for special flags (e.g., #long connection#).

NAT Firewall Wildcard Rules

Input Field	Example	Description
Access source/destination	0.0.0.0/0	All IPs
Domain name	*	All domains
Domain name	*.aa.com	All subdomains of aa.com
Destination port	-1/-1	All ports
Destination port	0/65535	All ports
Destination port	80,443,3389	Specific ports



Input Field	Example	Description
Destination port	80/443	Range between 80 and 443
Destination port	80/443,3389	Ports 80–443 and 3389

Adding Rules in Bulk

Note:

Each rule occupies one line. New rules are added at the end by default and have the lowest priority.

Scenario 1: Adding Rules in Batch

1. Click Copy in the action column to add multiple rules.
2. Complete all fields.
3. Check priorities.
4. Click OK to submit.

Scenario 2: Multiple Rules for One IP

1. Edit a rule, filling common fields.
2. Click Copy to duplicate it (up to 10 rules).
3. Adjust unique fields and priorities.
4. Click OK to submit.

Importing Rules

Click Import Rule to import from a local file.
You can specify an import location, download templates, or export existing rules.

Backup and Rollback

1. Click Backup Rules (top-right) to save current NAT firewall configurations.
2. Click Roll Back beside a backup to restore previous rules.
3. You can add a description and select NAT Firewall Rules as backup type.

More Information



For additional topics:

- Edge Firewall Rules – Managing inbound/outbound traffic on the edge firewall.
- Inter-VPC Firewall Rules – Managing communication between virtual networks.
- Special Scenarios – Access control in unique environments.
- NAT Firewall Overview – General information and troubleshooting.

Converge Cloud – Philippines' Trusted Cloud Security Platform

Intrusion Prevention

This document describes how to identify unknown risks beyond access control rules, perform intrusion prevention rule detection on the north-south traffic, and prevent vulnerabilities in Cloud Virtual Machine (CVM) from being exposed to the Internet through the intrusion prevention feature.

Operation Guide

Enabling Threat Intelligence

1. After threat intelligence is enabled, CFW forwards protection traffic to the threat intelligence detection and analysis engine to identify unknown risks beyond access control rules.
- Log in to the CFW console. In the left sidebar, select Intrusion Prevention to go to the Intrusion Prevention page.
 - On the Intrusion Prevention page, click the icon next to Threat Intelligence to enable this feature.
 - After threat intelligence is enabled, CFW forwards protection traffic to the threat intelligence detection and analysis engine to identify unknown risks beyond access control rules.
 - External malicious access: CFW monitors and identifies external access to cloud assets from malicious IP addresses and threat samples, such as malicious scans, brute force cracking, mining trojans, ransomware attacks, and remote control.
 - Proactive outgoing access: CFW monitors and identifies proactive outgoing access from cloud assets to external malicious IP addresses or domain names, and determines potential host compromise risks through the comparative analysis of big data provided by threat intelligence.

Enabling Basic Prevention

1. Log in to the CFW console. In the left sidebar, click Intrusion Prevention to go to the Intrusion Prevention page.
2. On the Intrusion Prevention page, find the Basic Prevention module and click View Rules to pop up the Basic Prevention Rules window.
3. In the Basic Prevention Rules pop-up window, view the IPS rule list. You can click any rule ID to view its corresponding description.



4. Click  to enable or disable the rule for NAT and VPC firewalls.

Note:

If the versions of some firewall engines are too early, the prevention rules that rely on later engine versions will not take effect for earlier versions of firewall instances. However, basic prevention rules may still remain effective.

5. In the Current Action column, select the action after a rule is hit. Rule actions take effect only for the assets whose protection mode is the interception mode.

Note:

Custom intrusion prevention rules only take effect for NAT Firewall and VPC boundary firewalls. If the versions of some firewall engines are too early, the custom intrusion prevention rules will not take effect for the corresponding firewalls.

6. For all IPS rules, provide keyword searching, one-click reset, and batch operations.

- Keyword searching: You can query the corresponding rules based on rule attributes, and then configure the toggle status and handling actions.
- One-click reset: You can restore the toggle status of all rules with one click and change a rule action to the default action to make the corresponding rule take effect immediately.
- Batch operations: You can select multiple rules and enable or disable them or change their handling actions in batches.



7. After viewing the rules, click  in the Basic Prevention module to enable this feature.

Note:

After Basic Prevention is disabled, all basic prevention rules no longer take effect. In interception mode, malicious behaviors that hit high-confidence rules are automatically intercepted, and security event alarms are generated when other rules are hit.

Enabling Virtual Patching

1. Log in to the CFW console. In the left sidebar, click Intrusion Prevention to go to the Intrusion Prevention page.
2. On the Intrusion Prevention page, find the Virtual Patching module and click View Rules to pop up the Virtual Patching Rules window.
3. For specific rule operations, see the preceding basic prevention rules.



4. Click  in the Virtual Patching module to enable this feature.

Protection Mode Description

1. Log in to the CFW console. In the left sidebar, click Intrusion Prevention to go to the Intrusion Prevention page.
2. On the Intrusion Prevention page, locate the Protection Mode module to configure the protection mode.
3. Protection modes include the observation mode, interception mode, and strict mode.

Note:

The observation mode is used by default.

- Observation Mode: threat intelligence, basic prevention, and virtual patching are all in detection mode. Only alarms are generated for malicious access or network attack behaviors; connections are not blocked.
- Interception Mode: high-confidence network attacks or malicious access are automatically intercepted. Threat intelligence supports automatic interception of outbound malicious access. Basic prevention supports automatic interception of high-confidence rule alarms. Virtual patching supports automatic interception of traffic detected as vulnerability exploits.
- Strict Mode: threat intelligence (except threat intelligence detection for outbound domain names), basic prevention, and virtual patching are all in global interception mode. Any detected alarms automatically block connections, but false positives may occur. Suitable for critical period guarantees or attack and defense scenarios.

Feature Dynamic Description

1. Log in to the CFW console. In the left sidebar, click Intrusion Prevention to go to the Intrusion Prevention page.
2. On the right side of the Intrusion Prevention page, view the feature dynamics and feature

descriptions:

- Feature Dynamic: view the features of the intrusion prevention module.

Managing the Blocklist (IPS Blocklist) and Allowlist Policy

1. Log in to the CFW console. In the left sidebar, click Intrusion Prevention to go to the Intrusion Prevention page.
2. On the Intrusion Prevention page, view the blocklist and allowlist policy.

Blocklist

Viewing the Blocklist

Click Blocklist to go to the Blocklist tab.

Disabling the Blocklist



In case of emergency, click  to disable the Enable Blocklist switch.

Managing the Effective Time of the Blocklist

When an IP address in the blocklist expires, it is automatically deleted and subsequent access traffic is not blocked. To prevent deletion, click Edit in the Operation column to modify the expiration time.

Note:

For IP addresses in the blocklist, all traffic passing through CFW in the outbound or inbound direction is blocked and recorded in Intrusion Prevention Logs under Log Audit.

Allowlist Policy

Viewing the Allowlist Policy

Click Allowlist Policy to go to the Allowlist Policy tab.

Note:

The IPS feature is bypassed for IP addresses in the allowlist policy.

Managing the Allowlist Policy Effective Time

When an IP address in the allowlist policy expires, it is automatically deleted and subsequent access does



not bypass the IPS feature. To prevent deletion, click Edit in the Operation column to modify the end time and date.

Cloud Log Service

This document describes how to view CFW-related logs.

Viewing Access Control Logs

1. Log in to the CFW console. In the left sidebar, choose CLS > Access Control Logs to go to the Access Control Logs page.
2. On the Access Control Logs page, you can view the rule hit logs generated by CFW based on the access control rules configured on the NAT Firewall and Inter-VPC Firewall pages. On the NAT Firewall page, you can also see two rule hit lists generated based on the inbound and outbound directions, respectively.
3. In the rule hit list, click View in the Operation column on the right side.
4. On the Rule Hit Details page, view the hit details of the current rule.

Note:

- If the rule is deleted after the log generation time, its status is displayed as deleted.
- If the rule is edited after the log generation time, its status is displayed as edited.
- If the rule has not been deleted or edited since the log generation time, its status is displayed as newly added.

5. To further speed up access control log search and filtering, click the magnifier icon on the right side of the access source or destination to view all rule hit information between the two IP addresses.
6. You can manually download logs and filter them based on different conditions. A maximum of 60,000 records can be downloaded each time.

Viewing Intrusion Prevention Logs

1. Log in to the CFW console. In the left sidebar, choose CLS > Intrusion Prevention Logs to go to the Intrusion Prevention Logs page.
2. On the Intrusion Prevention Logs page, view the details of inbound, outbound, and inter-VPC security events in the External Intrusion, Host Compromise, and Horizontal Movement lists, respectively.



Viewing Traffic Logs

1. Log in to the CFW console. In the left sidebar, choose CLS > Traffic Logs to go to the Traffic Logs page.
2. On the Traffic Logs page, view the north-south traffic information generated by the NAT firewall based on outbound and inbound directions, as well as the east-west traffic between VPCs.
3. Query and filter logs by asset instance name. To obtain a comprehensive view of traffic based on assets, click All Assets in the upper left corner of the Traffic Logs page, and select an asset instance name in the search dropdown list to filter logs and query all traffic logs of the asset.
4. To further speed up the retrieval and filtering of logs, click the magnifier button on the right side of the access source or destination to view all traffic information between the two IP addresses.

Viewing Operation Logs

1. Log in to the CFW console. In the left sidebar, choose Log Audit > Operation Logs to go to the Operation Logs page.
2. On the Operation Logs page, view all operations you performed on the security policy page and the firewall toggles page within the current account, as well as their details.

Tag Name	Tag Description
Firewall Switch Logs	Records the firewall switch status and users' operation details on the instance configuration.
Access Control Logs	Records users' operations for adding, editing, and deleting access control rules.
Intrusion Prevention Logs	Records users' operations in the intrusion prevention module.
Login Logs	Records users' account login information.

Log Analysis

Log analysis feature: You can view the detailed traffic logs stored in CFW based on the login account in the past 6 months. In addition, Log Analysis supports log search and query based on search statements, and provides report generation and statistical analysis services. This document describes how to use the log analysis feature.

Operation Steps

1. Log in to the CFW console. In the left sidebar, click Log Analysis to go to the Log Analysis page.
2. To facilitate log retrieval within a specified time range, drag your mouse pointer on the log quantity bar chart in blue to quickly select a time range, and click a bar chart to zoom in on the logs for searching.
 - Restore: Click Restore in the upper right corner of the bar chart. The time selector will show the initial time range (today).
 - If you switch between time options or log types or enter new keywords in the search boxes to search again, the bar chart will show the initial time (today) of the current time selector.
3. The log list displays the field details of each traffic log from top to down based on the Display Fields module. When the Display Fields module only contains source, the log list displays the field details of each traffic log in the order the fields appear in Hide Fields.
 - Show: Hover your mouse pointer over a hidden field and click Show. This field will appear under Display Fields and its details will be displayed in the log list on the right side.
 - Hide: Hover your mouse pointer over a displayed field and click Hide. This field will be deleted from Display Fields and its details will not be displayed in the log list on the right side.



General Settings

This document describes how to set access control rules on the General Settings page.

Operation Guide

1. Log in to the CFW console. In the left sidebar, click General Settings to go to the General Settings page.
2. On the General Settings page, configure related parameters for access control rules.

Configuring Access Control Rules

Each time you add, insert, or import a control rule in the access control rule list, you can set the rule's enabling status, which can be either enabled by default or not enabled by default.



Notification Settings

Subscribing to Message Center

1. Log in to the CFW console, and in the left sidebar, click Notification Settings.
2. On the Notification Settings page, configure the firewall push notifications. If you need to adjust to subscription-based push or enable the Message Center, click Switch in the Message Center Subscription Settings.

Note:

Once the Message Center is enabled, all alarm objects in Notification Settings will become invalid. The actual configuration will follow the Message Center settings.

Configuring Notification Settings

On the Notification Settings page, you can configure common firewall alarms and notifications.

Notification Type	Notification Content	Supported Configuration Item
Bandwidth alarm notification	Three levels of bandwidth alarms are provided. When firewall bandwidth reaches the configured threshold percentage, a notification will be triggered.	It supports tiered alarms by firewall type.
Storage alarm notification	Two levels of storage alarms are provided. When firewall storage reaches the configured threshold percentage, a notification will be triggered.	It supports tiered alarm configuration.
Disaster recovery alarm notification	When your NAT firewall or inter-VPC firewall triggers BYPASS, a notification will be triggered.	-
Automatic task except notification	A notification is sent if anomalies are detected in automatic tasks.	-
System log push notification	When new system logs are generated, notifications are sent according to your configured settings.	It supports triggering notifications by system log event type.

Common Tools

Address Templates

Address templates provide users with a more convenient and efficient way to manage common addresses in batches. Users can create IP address templates, domain name templates, or protocol port templates in the address templates. These templates can be applied to access control rules to facilitate management and Ops. This section describes how to manage addresses in batches by using address templates. Users can also match the existing templates with relevant access control rules for easier management.

Feature Entry

1. Log in to the CFW console. In the left sidebar, click Common Tools.
2. On the Common Tools page, click Go to Configuration under Address Template.



Address template

It provides users with a more convenient and efficient way to manage commonly used addresses in bulk. Users can create IP templates, domain templates, or protocol port templates in the address template. These templates can be applied to access control rules, making management and operations easier.

[Configure now](#)

3. On the Address Templates page, users can create and edit templates. When adding rules on the Access Control page, they can directly invoke the templates to reduce the operation frequency.

Creating a Template

1. On the Address Templates page, click Create Template.
2. In the New Address Template pop-up window, select Template Type:
 - IP Address Template: contains only IP addresses or CIDR blocks. IP address ranges are supported.
 - Domain Template: contains only domain name-type addresses. Wildcard domain names are supported.
 - Protocol Port Template: a combination of protocols and ports, categorized by Layer-4 and Layer-7 protocols. Ports can be a single port, a combination of ports, or a port range.



Create address template

×

Template type

☒ IP address template

☐ Domain name template

☐ Protocol:port template

Name

(Required) Enter a unique name within 20 characters.

IP address

1

Supported Formats: 10.0.0.1, 10.0.1.0/24, 10.0.0.1-10.0.0.100
Manual Input: Use line breaks for each entry. For multiple IP addresses copied from external sources, use commas (,) as separators. Duplicate IP addresses or ranges will be automatically merged.

Description

(Optional) Up to 50 characters

OK

Cancel

3. Enter the address template name, IP address, and description, and click OK to create an address template.

Note:

- When you enter a single address, press Enter to wrap to a new line.
- When you enter multiple addresses at a time, make sure that they are separated by commas before pasting to facilitate system recognition.
- Duplicate addresses will be automatically merged by the backend.
- A single address template allows you to add a maximum of 500 addresses at a time. For details about the filling specifications and content, see the related description in the console.

Editing a Template

After creating an address template, users can view it in the address template list on the left. Users can add, delete, and modify addresses of the corresponding category in the existing template list.

1. On the Address Templates page, click Edit in the operation column on the right of the target address template.
2. In the Edit Address Template pop-up window, select the IP address you want to modify or delete, or search for the IP address you want to modify in the search box to perform the operation. Then, click OK to save the modification.

Note:

Template type cannot be edited. If modification is required, delete the template and create a new template.

Deleting a Template

1. On the Address Templates page, click Delete in the operation column on the right of the target address template.

Note:

- If associated rules exist, go to the Access Control page to delete the associated rules.
- The deletion operation cannot be undone. It is recommended to back up the current template before deletion.

 2. In the Confirm Deletion pop-up window, click ****OK**** to delete the rule.

Using an Address Template

On the Access Control page, click Add Rule or locate the rule to be modified and click Edit on the right, then select to use an address template.

Note:

- Access rules configured with an address template apply to all addresses within the template.
- The number of address templates is limited, so please plan and use them reasonably.

IP Address Template or Domain Name Template

In access control rules, you can select Address Template in Access Source or Access Destination. The dropdown menu will list supported IP address templates or domain name templates that can be configured.

Note:

The selection of template types is related to the protocol. Please fill in according to the prompts of the corresponding access control rule.

Protocol Port Template

In access control rules, you can select Protocol Port Template in Port Protocol Type. The dropdown menu will list supported protocol port templates that can be configured.

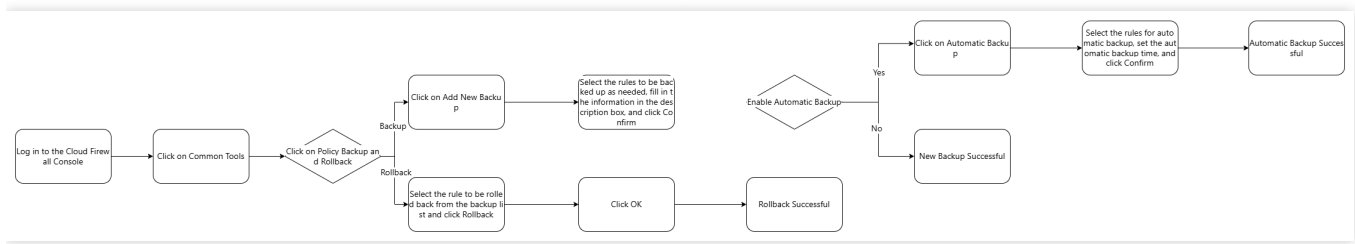
Note:

The selection of template types is related to the configuration format of the source or destination. Please fill in according to the prompts of the corresponding access control rule.

Policy Backup and Rollback

To handle possible misoperations, policy change requirements, or emergency fault recovery scenarios, policy backup and rollback features are provided to ensure your network protection policies remain stable and reliable. With policy backup and rollback, you can quickly undo recent modifications and restore the policy configuration of NAT firewalls or inter-VPC firewalls to a previously saved status.

Flowchart



Policy Backup

1. Log in to the CFW console. In the left sidebar, click Common Tools.
2. On the Common Tools page, click Go to Configuration under Policy Backup and Rollback.



Back up and roll back rules

[Configure now](#)

Provides users with quick backup and rollback of access control rules, blocklists, whitelist policies, address templates, etc.; supports regular automatic backups.

3. On the Policy Backup and Rollback page, click New Backup.

Back up and roll back rules

1. Backup: The current version supports up to 10 backups for each access control rule list. The backup does not differentiate between inbound and outbound rules (i.e., each backup includes both inbound and outbound rules).

2. Rollback: Overwrite the selected backup onto the current list of rules. It is recommended to backup the current rules before performing a rollback.

3. Backups will not be cleared when the product expires or is reclaimed. Therefore, when the number of backups reaches the limit, please delete the earlier backups first. If automatic backup is enabled, we will automatically eliminate the earliest backup files.

Create backup

Auto-backup

All

Search by the description of the rule backup

Backups	Description	Backup time	Policies	Operation
				Roll back Delete

4. Expand the backup list box, and the system will display the list of rules currently available for backup. Select the rules you want and enter a clear description in the Description field.
5. Click OK. The system will immediately initiate the backup process. After completion, a 'Backup successful' prompt confirms that the backup is securely stored.
6. To schedule Automatic Backup, click Automatic Backup, select the rules to enable automatic backup for, and set the appropriate time. Click OK to start the scheduled backup task.

Policy Rollback

Note:

Performing a rollback with a selected policy backup will overwrite the corresponding policy list. Existing policies will be deleted. To ensure data security, it is recommended to back up the current list before rollback.

1. Log in to the CFW console. In the left sidebar, click Common Tools.
2. On the Common Tools page, click Go to Configuration under Policy Backup and Rollback.
3. On the Policy Backup and Rollback page, all backed-up rule resources, descriptions, and backup times are displayed.
4. In the dropdown list box, locate the rules that require rollback and click Rollback.
5. Click OK, and the system will immediately start overwriting the current rule list with the backed-up rules.

Use Cases

Scenario Type	Policy Details
Policy Backup –	Backing up firewall policies periodically retains different stages of network



Scenario Type	Policy Details
Regular backup	protection statuses. Useful for reviewing policy evolution, compliance audits, or comparing policies across periods. For example, during quarterly internal network security reviews, backups show the focus of firewall policy adjustments.
Policy Backup – Before major business changes	Before launching new business systems, expanding network areas, or making large-scale server architecture adjustments, backup ensures policies can be restored if new configurations disrupt access, introduce latency, or create security vulnerabilities. For instance, e-commerce enterprises backing up policies before the "Double 11" festival can quickly restore settings if unexpected issues arise.
Policy Backup – Personnel handover	Backing up policies before team changes reduces delays and risks. Backup policies serve as reference baselines for new team members to ensure consistent and rational policy modifications.
Policy Rollback – After misoperation	If critical rules are accidentally deleted or misconfigured, rollback recovers policies to the correct status, ensuring normal business operations. Example: restoring the previous day's backup after mistakenly deleting active key access rules.
Policy Rollback – After failed policy adjustment test	When testing new firewall policies reveals incompatibilities, high false positives, or performance degradation, rollback restores the stable pre-test configuration to allow further evaluation.
Policy Rollback – After network attack or failure	In the event of malicious tampering or system failure, rollback quickly recovers the previously reliable policy configuration, minimizing losses. Example: restoring the previous day's backup during a midnight DDoS attack that modified firewall rules.

Task Scheduler

Task Scheduler is an Ops tool that provides users with automated instructions and scheduled instructions, allowing orchestration of tasks and achieving automated operations.

Feature Entry

1. Log in to the CFW console. In the left sidebar, click Common Tools.
2. On the Common Tools page, click Go to Configuration under Task Scheduler.



Task scheduler (Beta)

• Limited-time trial

Configure now

Provides users of Enterprise and above editions with automatic command and scheduled command to implement automatic operations.

3. On the Task Scheduler page, users can create and orchestrate automatic tasks to achieve scheduled operations such as enabling/disabling access control rules or ignoring categorized alarms.

Adding an Automatic Task

1. On the Task Scheduler page, click Add Task.
2. In the Create Automatic Task pop-up, enter the task name.

Create automatic task

×

① After the task is created, it will be executed in sequence according to the execution order

Task name *

Enter the task name

Task object

Click to select

Task action ①

Priority ①	Task type ①	Action	Execution time	Status	Operation
No action yet. Please select a task object					

Submit

Cancel

3. Click Click to Select next to the task object and select via Category Selection or Custom Selection, then click OK.
4. Click Add Action to configure task actions. Set temporary or periodic tasks with execution time. Actions

execute sequentially; click Duplicate to add up to 10 actions.

5. Click Submit to view tasks and their status in the task list.

Task scheduler (Beta)

Limited-time trial

You can create up to 100 automated tasks.

Add task

Separate keywords with "|"; press Enter to separate filter tags

Q

↺

Task ID	Task name	Executions	Latest execution	Created time/Edited	Operation
		1			Edit Delete
		1			Edit Delete
		1			Edit Delete

Quickly Adding an Automatic Task

1. Go to Access Control > NAT Boundary Rule.
2. On the NAT Firewall Rules page, click Batch Operations.
3. Select rules to execute automatic tasks, then click Add Automatic Task.
4. In the pop-up, fill in task name, click Add Action, configure parameters, and click Submit.

Editing an Automatic Task

1. Go to Common Tools > Task Scheduler.

Task scheduler (Beta) Limited-time trial

You can create up to 100 automated tasks.

Add task

Separate keywords with "|"; press Enter to separate filter tags

Q

↺

Task ID	Task name	Executions	Latest execution	Created time/Edited	Operation
		1			<a>Edit <a>Delete
		1			<a>Edit <a>Delete
		1			<a>Edit <a>Delete

2. Locate the task to edit and click Edit.

Task ID	Task name	Executions	Latest execution	Created time/Edited	Operation
		1			<a>Edit <a>Delete

3. In the Edit Automatic Task pop-up, modify task name, type, actions, and execution time. Use Duplicate or Delete if needed. Click Submit to save.

Note: If the task object is changed or deleted, the automatic task will no longer execute.

Edit automatic task

After the task is created, it will be executed in sequence according to the execution order

Task name *

Task object

Selected Nat|1ap 1 items Select again

Task action ⓘ

Priority ⓘ	Task type ⓘ	Action	Execution time	Status	Operation
1	One-off task ▾	Disable rule ▾		• Executed	<a>Copy <a>Delete

Submit

Cancel



Deleting a Task

- 1. Go to Common Tools > Task Scheduler.

Task ID	Task name	Executions	Latest execution	Created time/Edited	Operation
		1			Edit Delete

- 2. Locate the task and click Delete.

Task ID	Task name	Executions	Latest execution	Created time/Edited	Operation
		1			Edit Delete

- 3. In the Confirm Deletion pop-up, click OK.

Querying Execution Records

Operation logs of the task-associated object display actions where the operation account is "Automatic Task".



Packet Capture Tool

The Packet Capture Tool allows users to capture network packets for specified IP addresses and ports, and analyze their contents. It helps locate network failures and analyze attack behaviors to identify security risks in network communications.

Feature Entry

- 1. Log in to the CFW console. In the left sidebar, click Common Tools.
- 2. On the Common Tools page, click Go to Configuration under Network Packet Capture Tool.



Packet capture tool

New

[Configure now](#)

Provide tools for Enterprise and above version users to obtain network packets with specified IP and port, and analyze the content of the packets. This helps you locate network faults and analyze attack behavior, thereby identifying security risks in network communication.

- 3. On the Network Packet Capture Tool page, capture traffic from the NAT firewall or inter-VPC firewall and download results for analysis.

Creating a Packet Capture Task

- 1. Click Create Packet Capture Task on the Network Packet Capture Tool page.

Packet capture tool

1. Today, you can create 50 packet capture tasks. After the packet capture is completed, please download the packet capture file in a timely manner. The file is valid for 3 days.

2. Please ensure that the corresponding firewall switch is enabled for your packet capture target; otherwise, the corresponding traffic cannot be captured.

Create task

24 hoursLast 7 days

Separate keywords with "; press Enter to separate filter tags

Task ID/name	Packet capture target	Protocol	Captured time	Packet size	Task status	Operation
		TCP		1KB	Completed	DownloadDelete

Total items: 1

20 / page1 / 1 page

- 2. In the New Packet Capture Task pop-up, configure the parameters and click Start Packet Capture.

Note: Ensure the corresponding firewall switch for your capture object is enabled; otherwise, traffic cannot be captured.



Create task

Task name *

Please enter the task name

Max packet size

Max packet size

Byte ▾

Up to 100 MB.

Interval *

Interval to capture packets

s

Up to 6000 seconds

Protocol

☒ ANY ☐ TCP ☐ UDP ☐ ICMP

IP configuration

☒ Single IP ☐ IP pair

IP *

Enter an IP address, such as 10.10.10.10

Port *

Please enter the port

It can be a single port and all ports (-1).

Location

☒ NAT firewalls ☐ Inter-VPC firewalls

Firewall *

Please select a firewall

▾

Capture now

Cancel

3. After completion, click Download to obtain the packet capture results.

Note: The packet capture file is valid for 3 days; download it promptly.



←

Packet capture tool

1

Today, you can create 50 packet capture tasks. After the packet capture is completed, please download the packet capture file in a timely manner. The file is valid for 3 days.

2

Please ensure that the corresponding firewall switch is enabled for your packet capture target; otherwise, the corresponding traffic cannot be captured.

Create task

24 hours

Last 7 days

Separate keywords with "; press Enter to separate filter tags

Task ID/name	Packet capture target	Protocol ▾	Captured time	Packet size	Task status ▾	Operation
		TCP		1KB	Completed	Download Delete

Total items: 1

20 / page

1 / 1 page

4. Open the downloaded capture file using software like Wireshark for further analysis.



Simulation Test

Choose Common Tools > Simulation Test to configure and monitor network connectivity in real time. The simulation test tool detects access path anomalies promptly, helping improve Ops and network availability.

Entry to Simulation Test

Navigate to Common Tools > Simulation Test.



Simulated test

New

Configure now

We provide a tool for Enterprise Edition and above versions to perform simulated probe tasks on the firewall. This tool allows real-time monitoring and verification of network connectivity, ensuring that the access links are functioning properly and improving network security and stability.

Creating a Simulation Test Task

1. Click Create Simulation Test Task.

← Simulated test

1. Your current version supports up to 50 simulated automatic test tasks.
2. The auto-test task only verifies by sending ICMP messages, and does not support other protocols.
3. The test direction refers to the session direction. Each task supports up to four one-way subtasks at the same time.

Create automated test

Associated firewall instance

Separate keywords with ";", press Enter to separate filter tags

Task ID	Task name	Tested object	Associated firewall instance	Task type	Last tested	Test status	Operation
							Automated testing Details Delete
							⌵ Details Delete
							⌵ Details Delete
							Automated testing Details Delete
							Automated testing Details Delete
							⌵ Details Delete
							Automated testing Details Delete

2. Configure the following parameters:
- Location to be tested
 - Access source and destination of the test request
 - Traffic direction
 - Firewall entry and exit points

- Task type: temporary or periodic

3. Note: Simulation tests can only be initiated in one direction via a firewall instance. The firewall monitors the health of the engine access path by simulating packet sending and receiving, verifying whether traffic flows normally through the firewall engine.

Create automated test

×

1. A simulated test can only be initiated by the firewall instance.

2. Select the scope of the one-way test task and the test object below.

Task name *

Please enter the task name

!

Enter the task name

Test location

☒ NAT firewalls
 ☐ Inter-VPC firewalls

Select the test target

(Required) Enter the private IP

!

(Required) Select a firew...

▼

!

(Required) Public IP

!

Please enter a correct private IP.

Please select a firewall instance

Please enter the public IP address

Retry attempts

5

▼

Task type

☒ One-off task
 ☐ Scheduled task

Execution time

📅

OK

Cancel

Viewing Test Tasks

1. Check the test status in the task list:

- Test Object: displays the status of each subtask in real time
- Test Status: displays the overall health status of the linkage



← Simulated test

1. Your current version supports up to 50 simulated automatic test tasks.
2. The auto-test task only verifies by sending ICMP messages, and does not support other protocols.
3. The test direction refers to the session direction. Each task supports up to four one-way subtasks at the same time.

Create automated test

Associated firewall instance

Separate keywords with "; press Enter to separate filter tags

Q

↺

Task ID	Task name	Tested object	Associated firewall instance	Task type	Last tested	Test status	Operation
		Firewall					Automated testing Details Delete
		Firewall					Details Delete
		Firewall					Details Delete
		1 Firewall					Automated testing Details Delete
		Firewall 1					Automated testing Details Delete
		Firewall					Details Delete
		Firewall					Automated testing Details Delete
		Firewall	li-nat2				Automated testing Details Delete

2. Click a Task ID or the Details button to view detailed information about a task.

DORAVPC

Edit taskQuick testX

Task ID15919Task typeScheduled task(in seconds / Every 5 seconds)

Test sourceTest targetLast testedFirewall instance name

Test resultHealthy

TopologyTest history

```
graph LR; S1[Server 1] -- "Access Firewall: normal" --> F[Firewall [autotest]]; F -- "Access Firewall: normal" --> S2[Server 2];
```

Test source	Test target	Test status	Result
		Healthy	Link is normal.
		Healthy	Link is normal.
		Healthy	Link is normal.
		Healthy	Link is normal.

3. If a test task encounters anomalies, system logs are recorded and exception information is pushed according to your system log push configurations.

Troubleshooting Solution for False Alarms and False Positives

This topic describes how to deal with a large number of firewall false positives or an abnormal drop in traffic caused by improper strategy changes.

Problem

A large number of legitimate requests from certain IPs are blocked due to false positives in intrusion defense, or an abnormal traffic drop occurs because of improper strategy configuration.

Solution

If legitimate requests are blocked by Cloud Firewall, you can:

- Disable the blocking feature temporarily
- Allow requests from the affected IPs
- Submit a support ticket to the Product Security Team for assistance

Steps

Step 1: Disable the Blocking Feature

1. Log in to the Cloud Firewall Console.
2. Click Intrusion Protection System in the left navigation pane.
3. On the Intrusion Defense page, select Observe for the protection mode.
4. Disable the "Enable Blocklist" option above the blocklist.

Step 2: Manual Troubleshooting

1. Log in to the Cloud Firewall Console.

2. Click Alert Management in the left navigation pane to open the Alert Management page.
3. On the Alert Management page, select Blocked Statistics → Inbound.
4. On the Inbound tab, choose Sort by Blocking Statistics to identify falsely blocked IP addresses.
5. Add the falsely blocked IP addresses to the Allowlist using one of the following methods:

Method 1:

Click Allow on the right side of the falsely blocked IP address to add it to the Allowlist (Ignore List) and permit access.

Method 2:

On the Intrusion Defense page, select Ignore List → Add Addresses to add falsely blocked IP addresses in batches.

After these steps, restore the configuration made in Step 1 and monitor whether the traffic volume returns to normal.

Step 3: Submit a Ticket to Report False Positives

If the traffic volume remains abnormal after manual troubleshooting:

1. Go to the Submit Ticket page.
2. Provide your AppID and the falsely blocked IP addresses to the Security Team.
3. The Security Team will review your case and adjust detection rules as necessary.

Note:

After you submit your report, the Security Team will respond within the specified timeframe and fine-tune intrusion defense rules based on the reported false positives.