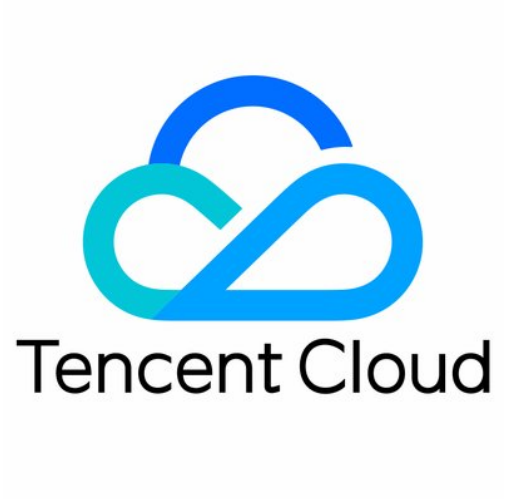
Tencent Cloud Firewall

Product Introduction

Product Documentation



Contents

Product Introduction
Overview

Last updated：2024-01-24 15:41:48

What is Cloud Firewall?

Tencent Cloud Firewall (CFW) is a SaaS firewall based on the public cloud environment that provides network perimeter protection and addresses security and management needs for unified access control and log audit. In addition to the features of traditional firewalls, CFW supports multi-tenancy and elastic scaling and is an essential network security infrastructure for cloud migration.

Features

Cloud Firewall overview

Cloud Firewall offers centralized network access control. You can view the information of Cloud Firewall clearly on the console overview page, which includes the following modules:
Asset protection overview: Displays the number of assets in the public and private networks, exposed ports, and security events, and offers vulnerability intelligence for reference.
Firewall status monitoring: Displays the peak bandwidth of the edge and NAT firewalls within the past 7 days.
Traffic statistics: Displays the volume of inbound traffic, outbound traffic, and total traffic within the past 24 hours to 6 months.
Security policy configuration: Displays the number of access control rules configured for edge, NAT, and inter-VPC firewalls, their remaining quota, and security policies for intrusion prevention.
Log storage statistics: Displays the total log storage capacity, used storage, and remaining storage.

Cloud Firewall toggles

Edge firewall: The system automatically identifies the public IP addresses and the associated instances and assets of a cloud tenant, and allows you to manage access control by public IP. Cloud Firewall supports public BGP IP addresses (IPs provided by CMCC, CUCC, or CTCC are not supported). It offers a public IP address list (asset list) for you to view all of the existing inbound or outbound rules of each public IP, and allows you to manage them using the access control module.
Inter-VPC firewall: The system automatically identifies the number of VPCs in the cloud tenant private network along with their connection status and mode, and visualizes them using a VPC topology. A uniform toggle needs to be enabled when you use the inter-VPC firewall for the first time. After the toggle is enabled, a sub-firewall is automatically

configured for each pair of connected VPCs. You can manually enable or disable a sub-firewall, and configure access control rules for each pair of VPCs.

NAT firewall: A virtual firewall that works similarly as a NAT gateway. In addition to network address translation capabilities, it also offers security audit features such as access control and logs.

After you enable and create a NAT Firewall instance, the system automatically identifies the subnets of the VPCs in the selected region. You only need to enable the firewall for your subnets to route your traffic from the subnets to the NAT firewall. You can configure the access control list for the NAT firewall to filter and control traffic.

Asset management

Asset Management allows you to view and manage the data and information of each asset. It helps you better understand the current asset status, manage your assets, and predict and prevent security events by showing the top 5 core assets and risky assets and the detailed information of all your public network assets, private network assets, and VPCs.

Alert management

Alert Management allows you to view the alerts when your assets are under attack. After you configure all the necessary security policies in the access control, intrusion defense, and security baseline modules, you are kept informed of the alerts from Cloud Firewall, which is helpful for security operations and maintenance.

Traffic monitoring

Traffic Monitoring visually displays external access statistics, outgoing request analysis, and inter-VPC activities based on outbound, inbound, and inter-VPC traffic.

Access control

Access control rules are a collection of security policies, which are defined in the 5-tuple format and are listed in a list. For any data flows that pass through the edge firewall, Cloud Firewall matches them with the 5-tuple information according to rule priorities. If a data flow is matched, the operation specified in the rule is performed on the data flow, which can help tenants control access to public IP addresses. Besides, logging is used for security operations, maintenance and audit. With the traditional 5-tuple configuration model, enterprise security groups can be easily managed and used for protection between subnets of a VPC, VPCs, and direct connections of hybrid clouds.

Intrusion defense

According to the protection mode, Cloud Firewall automatically identifies the unknown risks beyond access control rules, monitors the north-south traffic of public IP addresses based on intrusion defense rules, and prevents CVM vulnerabilities from being exposed to the Internet.

Security baseline

By observing the traffic statistics within a specific period of time, Cloud Firewall generates a basic IP address or domain name access list. You can add or delete IP addresses or domain names based on the security scores, associated security events, and network access statistics to form a security baseline.

Log audit

Cloud Firewall logs and stores rule hit records for the past 7 days. Security O&M specialists can view the matched network traffic and rules for log audit. When failure like a network connection error occurs, you can search the log for a quick fix. You can also view the operation history for the past 30 days to improve the working efficiency of enterprise and network security administrators and reduce management costs.

Log analysis

Log Analysis allows you to view the details of all the traffic logs stored in Cloud Firewall for the past 6 months based on login account, query logs with search statements, and use reporting and analysis services.

Address template

Address Template allows you to batch manage IP addresses more easily. You can create a template for IP addresses or domain names, add multiple IP addresses or domain names to it, and then match the template with access control rules.

Advantages

Last updated：2024-01-24 15:41:48

Easy to enable and deploy

Based on SDN, Cloud Firewall 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 your firewalls with one click.

Stable, reliable, and scale at ease

With a primary-secondary disaster recovery system and SaaS features, Cloud Firewall boasts high stability and reliability, and supports easy bandwidth, asset, and storage scaling.

Centralized management for high efficiency

Cloud Firewall offers users a centralized access control plane for access control and security isolation on traffic between networks and VPCs.
Network perimeter access control: Block or observe malicious traffic and prevent attacks from malicious sources on cloud assets based on the access control rules configured for public IP addresses.
Inter-VPC access control: Control access between VPCs with inter-VPC rules for inter-VPC security isolation.
Enterprise security group: Facilitate management of security group configuration with the 5-tuple configuration model and build a cloud demilitarized zone (DMZ) easily with blocked request logs and protection between subnets in a VPC, VPCs, and direct connections of hybrid clouds.
By following the rule configuration model of traditional firewalls, Cloud Firewall is easy to learn and use for security O&M specialists in the actual scenarios.

Log storage and audit

Rule hit log: When an access control rule is matched and applied, Cloud Firewall will record the 5-tuple information of the matched traffic and rule to help you with security operations and maintenance. If any failure occurs, you can use the logs to fix it quickly.
User operation log: Records user operations on Cloud Firewall, including account login operations, Cloud Firewall toggle operations, and the add, delete, and edit operations on rules to help with management efficiency and costs.

Scenarios

Last updated：2024-01-24 15:41:48

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 can help you with rapid log audit and troubleshooting, improving your efficiency in security operations and maintenance at a lower cost.

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.

Key Concepts

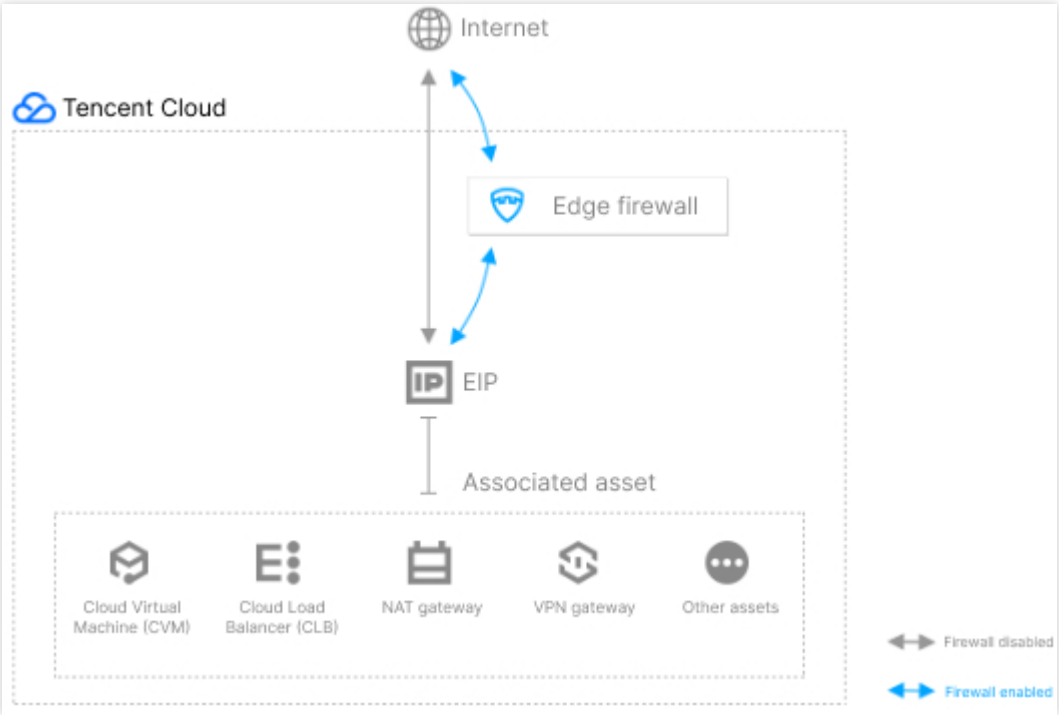
Last updated：2024-01-24 15:41:48

Network perimeter

The network perimeter is the boundary between the Internet and Tencent 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 "outbound traffic" and "inbound traffic" according to the direction.
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 EIP and the Internet, as shown in the image below:



The edge firewall offers access control and log audit. Thanks to its built-in intrusion defense module and default cluster deployment, the firewall is out-of-the-box and easy to scale without complex network configurations and image

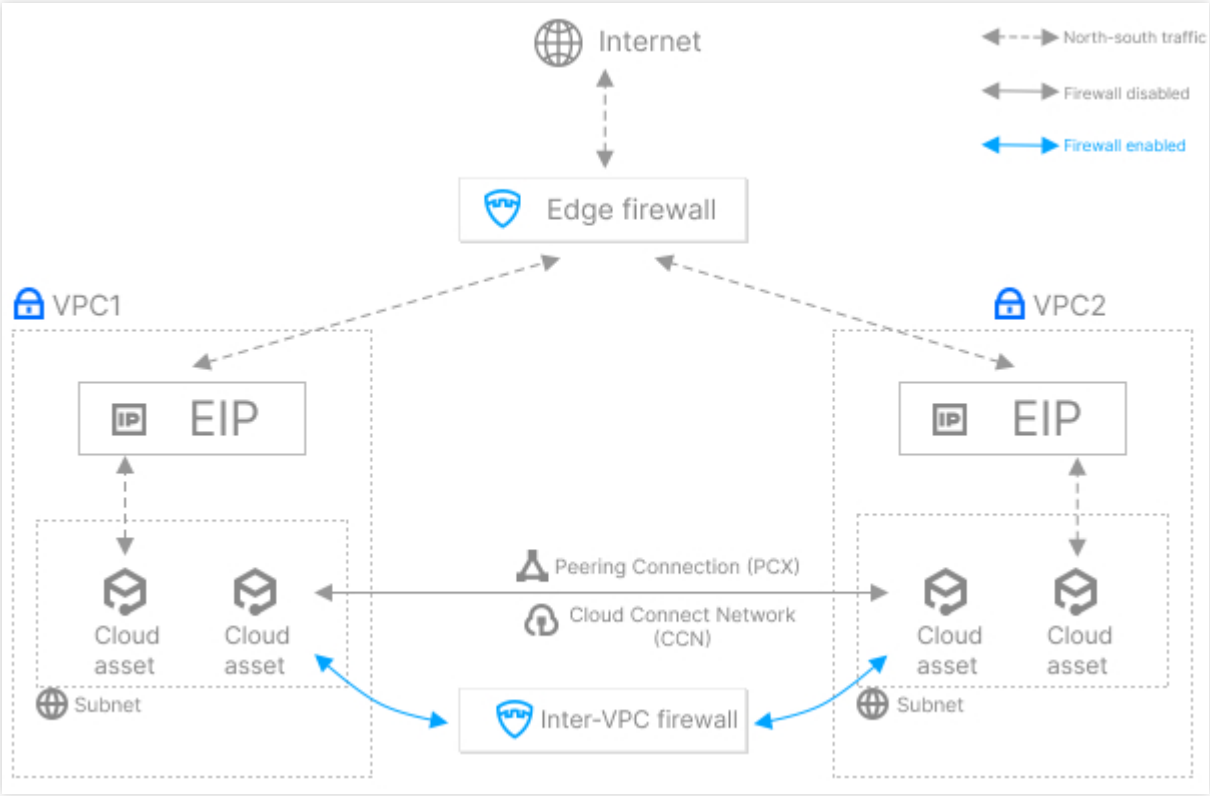
installation.

Virtual Private Cloud

Virtual Private Cloud (VPC) is a custom and logically isolated network space on Tencent Cloud. Similar to a traditional network running in an IDC, 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. For more information, please see Peering Connection Documentation.
Cloud Connect Network (CCN): Supports communication between VPCs. For more information, please see Cloud Connect Network Documentation.
Cloud VPC connection can be achieved with Peering Connection and CCN, and the traffic between 2 VPCs is called east-west traffic. For more information, please see 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, as shown in the image below:



Inter-VPC firewall is deployed between two VPCs connected through Peering Connection and CCN, and offers access control, topology visualization, log audit, exclusive resource configuration, and other features. Besides, it is out-of-the-box without complex routing configurations and image installation.

Access control

Access control is a collection of traffic filtering rules. An access control list contains all the rules for the same type of traffic. Each access control rule is composed of the rule body and description:

Rule body: Allow or block communication from the port of a specified address to the port of another address over a specific protocol.

Access source: The address of the source, and it is usually an IP address.

Access destination: The address of the destination, and it can be an IP address or a domain name.

Destination port: The destination port of the communication.

Protocol: The network protocol used for the communication.

Policy: For traffic that matches the above 4 conditions specified in a rule, one of the following operations is performed according to the policy of the rule.

Allow: Allows access, and will record traffic logs, but not rule hit logs.

Observe: Allows access, and will record both traffic and rule hit logs.

Block: Denies access, and will record rule hit logs, but not 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 and 1 indicates the top priority. For any data flows that go through the firewall, Cloud Firewall (CFW) matches them with the rules according to the list from top to bottom:

If a data flow matches a rule, matching will stop and the corresponding policy is applied.

If a data flow does not match the current rule, CFW will try to match it with the next rule.

If a data flow does not match any of the rules, it is allowed.

In an access control list, the priority is an integer that ranges from 1 to n, where 1 indicates the highest priority and n is the total number of rules or the lowest priority in the current rule list. Generally, the priority of a general rule with wildcards is set to n.

The priorities conform to the principles of **continuity and uniqueness**.

Continuity: The priorities must be consecutive positive integers. If the total number of rules is n, the maximum priority value is n.

Uniqueness: A rule list cannot contain duplicate priorities.

The following rules ensure the continuity and uniqueness of priorities:

If a new rule is added to the list, its priority is n+1.

If a new rule is inserted into the list, its priority is set to that of the original rule at the position, and the priorities of all the following rules automatically increase by 1.

When you edit a rule, you can move the rule by modifying its priority to that of the rule at the target position within the range of 1 to n. After you enter the new priority, the rule is moved to that position, and the priorities of all the following rules automatically increase by 1.

Intrusion defense

Intrusion defense is designed to monitor network transmission and detect suspicious activities. When a suspicious event is detected, the system will send an alert or take proactive measures. CFW has integrated Tencent Cloud's threat intelligence, basic protection, and virtual patching features. By performing real-time monitoring, statistics, and analysis on your network perimeter traffic, it can help detect intrusion, malicious outgoing requests, and other unknown risks, and offer real-time protection and alerts.

Logs

Rule hit logs: Records the rule hits to help O&M specialists with security audit. The rule matching logs display the 5-tuple information of all the data flows that are allowed, observed, or blocked, and allow you to view the rule applied by clicking a button.
Operation logs: CFW operation logs are divided into user login logs, toggle operation logs, and rule operation logs.
User login logs: Records the login activities of all the accounts of a given user.
Toggle operation logs: Records the enabling and disabling of firewalls.
Rule operation logs: Records users' add, delete, and edit operations on the access control rules.