# Huawei Qiankun Cloud-network Express

With the continuous digitalization and cloudification of government, enterprise, home, and individual services, networks are playing an increasingly important role in the daily operation. For damage and profit purposes, network attackers employ a range of methods — such as identity spoofing, website Trojan horses, and malware — to initiate network penetration and attacks, disrupting the proper network functioning. Therefore, network security must be protected. The most common method to protect the network security of governments, enterprises, and individuals is through local deployment of multiple security products, such as firewalls, intrusion prevention system (IPS), sandbox, vulnerability scan, and situational awareness. However, due to the lack of professional security personnel, many organizations cannot use these security products to achieve effective security protection. For example, after some security products are rolled out, no one pays attention to security alarms or adjusts security protection policies in a timely manner. As a result, security issues occur frequently.

Conventional security construction solutions of enterprises cannot meet users' diversified security requirements due to drawbacks such as large investment, difficult O&M, and ineffectiveness. To address the issues, Huawei launches the Qiankun Cloud-network Express that uses the innovative cloud-edge integration architecture. In this architecture, the Huawei security cloud platform provides multiple security capabilities and expert O&M capabilities on the cloud. Another important part of this architecture is Huawei Qiankun Shield device, which is deployed as a local protection node. The Qiankun Shield device combines cloud-based intelligent analysis and security expert capabilities to provide cloud-based security services that provide both protection and response.

Innovative Architecture

Huawei Qiankun Cloud-network Express uses the innovative cloud-edge integration architecture. In this architecture, the Huawei Qiankun Shield device is deployed locally to function as a security protection node for performing in-depth security detection on the traffic entering and leaving the network, in addition to providing security detection and blocking capabilities such as IPS, antivirus, and URL filtering.
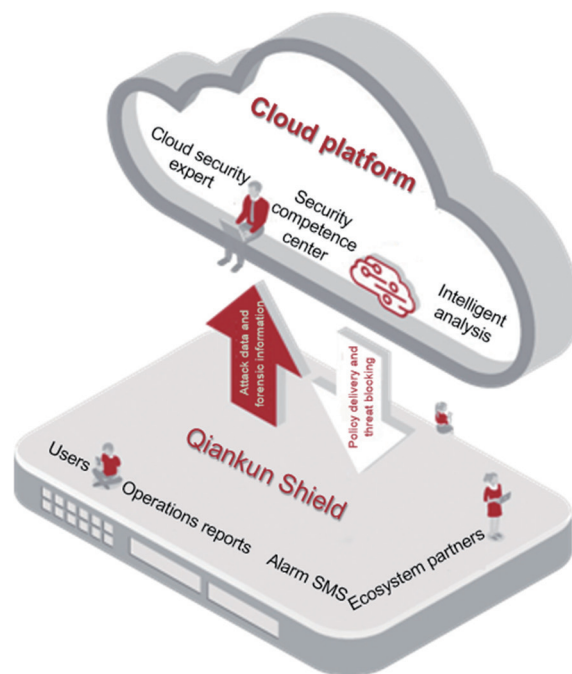
In addition, the Huawei Qiankun Shield device uploads the detected security events and the collected forensic information to Huawei Qiankun CloudService platform. On the cloud, Huawei security operations experts analyze and respond to security events for users based on the intelligent

big data analytics technology and their extensive experience in defending against attacks. After being authorized by users, security operations experts can use blocklist and allowlist policies to block continuous attacks from high-risk attack sources. This helps to drastically reduce local O&M investment for users. They can easily learn about the network security protection status through various means, such as emergency alarm SMS messages and weekly/monthly email reports provided by Huawei Qiankun Cloud-network Express. If local O&M personnel encounter security events that are difficult to handle, they can obtain professional emergency handling guidance from service experts of Managed Security Service Providers (MSSPs) on the cloud, allowing them to swiftly respond to and close emergency security events.

Highlights

Fast service provisioning

ZTP for the local Qiankun Shield devices, real-time provisioning and elastic scaling of cloud-based SaaS services

Fast and continuous upgrade

Real-time upgrade of cloud-edge protection capabilities, and global sharing of any detected threat, implementing immunity in minutes

Fast threat handling

Cloud-edge integration, automated threat handling, real-time perception, resolving threats in seconds

Fast service provisioning
- Huawei Qiankun Shield devices are locally deployed in ZTP mode, involving just three steps.
- The platform provides border protection and response packages that contain a variety of capabilities and services. The packages can be subscribed to on demand and provisioned quickly.
- The service capabilities are continuously enhanced. The security protection evaluation and asset risk assessment capabilities currently support POC tests. The log audit capability, CP compliance service, and endpoint protection and response service are currently being planned.
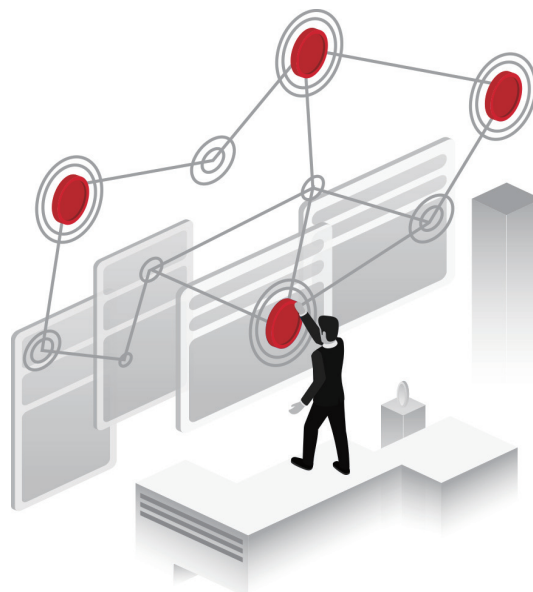
Fast and continuous upgrade

- The platform automatically responds to the latest vulnerabilities and attacks in the industry, and supports global protection once a threat is detected on one node.
- The cloud expert service supports 24/7 online refined operations to resolve difficult problems. Cloud threat intelligence, intelligent technologies, and big data technologies are used to enhance the automatic closed-loop threat handling capability, and real-time upgrade is performed on the cloud and local devices.

Fast threat handling

- Border protection and response: The cloud-based threat intelligence database and intelligent technologies are used to automatically cope with the latest vulnerabilities and attacks in the industry. In addition, the automatic security orchestration capability and cloud expert security O&M are provided to quickly handle and close attacks. In-depth border security detection is performed to efficiently block attack traffic.
- Real-time awareness: Users can quickly gain insights into the cyber security situation through the weekly and monthly reports, alarm SMS messages, mobile apps, and visualized portal interfaces, helping them process and close threat issues in a timely manner.

Deployment

Huawei Qiankun Cloud-network Express supports convenient cloud-based deployment. The only hardware required on the live network is the Huawei Qiankun Shield device that is locally deployed as a security protection node, enabling service deployment without changing the existing network topology.

The Qiankun Shield device is equipped with a dedicated cloud communication service module. The only configuration required for the Qiankun Shield device is an IP address that has the permission to access the Internet. Then, the Qiankun Shield device can automatically complete trusted authentication with the Huawei Qiankun Cloud-network Express platform, implement encrypted connections, and support rollout of Huawei Qiankun Cloud-network Express within seconds.

Emergency Response

Huawei Qiankun Cloud-network Express shares security expert resources on the cloud and imports expert capabilities into the platform through technical means, thereby providing standardized expert-level security operations services. When a security threat event requiring immediate handling occurs, the emergency response service is provided as needed to ensure the "last mile" processing of security services.

Security Capabilities

Security Cloud Service	Function		Implemented By
Border Protection and Response - Standard Edition	Service awareness	Identifies more over 6000 applications and covers all mainstream application protocols.	Qiankun Shield security protection node
	Web category	Supports a web category database with more than 120 million websites to regulate access behaviors and prevent malicious websites from attacking enterprise networks.	Qiankun Shield security protection node
	IPS	Supports attack detection based on vulnerability and behavior analysis, anti-evasion based on content restoration in context, a maximum of over 12,000 signature databases, automatic update, botnet detection, and application server protection.	Qiankun Shield security protection node
	Defense against botnets, Trojan horses, and worms	Supports precise role identification based on the botnet topology analysis technology, identification of 500+ botnets, and identification of 1000+ worms and Trojan horses.	Qiankun Shield security protection node
	Protecting against malware	Supports multi-level protection technologies, detects multiple types of malicious code carriers, and updates the antivirus database in real time to cover popular high-risk malware.	Qiankun Shield security protection node
	Threat correlation analysis	Supports security event aggregation and correlation model analysis to provide attack determination results and handling suggestions.	Huawei Qiankun CloudService platform
	Blocklist and allowlist	Supports blocklist and allowlist configuration to protect known services and quickly block threat attack sources.	Huawei Qiankun CloudService platform
	Emergency security notification	Supports emergency security notifications via SMS and email, and sends emergency notifications for compromised host events to provide timely response guidance.	Huawei Qiankun CloudService platform

Security Cloud Service	Function		Implemented By
	Periodic security report	Provides security service reports for users by week or month. Security service reports are sent to users' subscription mailboxes by email. The security service reports enable customers to clearly learn about the following information: 1. Security service overview; 2. Threat prevention times and trend; 3. Number and details of compromised hosts; 4. Number and trend of external attack sources; 5. Number and trend of malicious files.	Huawei Qiankun CloudService platform
Border Protection and Response - Value-added Edition (with Capabilities of the Standard Edition)	Automatic blocking of external attack sources	Accurately identifies external high-risk attack sources and automatically blocklists them to prevent subsequent attacks.	Huawei Qiankun CloudService platform
	Advanced threat information service	Supports tens of millions pieces of IP reputation threat intelligence, tens of millions pieces of domain name reputation threat intelligence, and hundreds of millions pieces of file reputation threat intelligence (detected by hash algorithms).	Huawei Qiankun CloudService platform
	Advanced threat correlation analysis	Supports correlation analysis of security events and threat intelligence to implement precise profiling and analysis of threat sources and improve threat blocking accuracy.	Huawei Qiankun CloudService platform
	Visualized application access	Supports statistics collection of application access based on the source IP addresses, access time, and application distribution, and provides statistical analysis reports by week or month.	Huawei Qiankun CloudService platform

Huawei Qiankun Shield Hardware Specifications

Qiankun Shield Model	Eudemon1000E-T1
Fixed ports	10×GE (RJ45) ports +2×GE (SFP) ports
Product type	Desktop
Dimensions (H×W×D)	43.6mm×250mm×210mm
Storage	Optional, supporting SD card (by using an adapter), 64 GB
Power supply	Standard: single power module

Ordering Guide

Product	Model	Description
Eudemon1000E-T1	Eudemon1000E-T1-AC	Eudemon1000E-T1 AC Host
		(10*GE RJ45+2*GE SFP, 1*Adapter)
Basic License		
Border Protection and Response Service	LIC-Eudemon1000E-T1-BPRA-1Y	Border Protection and Response Add-value (Applies to Eudemon1000E-T1), Per Device, 1 Year