ສຳນັກງານໃຫຍ່

ເລກທີ: 3393 /ທຄຕລ...2025.....
ນະຄອນຫຼວງວຽງຈັນ, ວັນທີ:.....03 NOV 2025.....

ໜັງສືແຈ້ງເຊີນ

ເຖິງ : ບັນດາບໍລິສັດ ຫ້າງຮ້ານຕົວແທນຈຳໜ່າຍເຄື່ອງໄອທີ ໃນນະຄອນຫຼວງວຽງຈັນ.

ເລື່ອງ: ແຈ້ງເຊີນເຂົ້າຮ່ວມຍື່ນຊອງປະມູນລາຄາເຄື່ອງໄອທີ ອຸປະກອນເຄືອຂ່າຍ.

ທະນາຄານການຄ້າຕ່າງປະເທດລາວ ມະຫາຊົນ ຂໍແຈ້ງມາຍັງບັນດາບໍລິສັດ ແລະ ຫ້າງຮ້ານຕົວແທນຈຳໜ່າຍ ເຄື່ອງໄອທີ ຊາບວ່າ ທຄຕລ ມີຄວາມຕ້ອງການເຄື່ອງໄອທີ ອຸປະກອນເຄືອຂ່າຍ ເພື່ອນຳໃຊ້ເຂົ້າໃນວຽກງານວິຊາ ສະເພາະຂອງ ທະນາຄານ, ຈຶ່ງໄດ້ແຈ້ງເຊີນມາຍັງທ່ານເພື່ອຍື່ນຊອງເຂົ້າຮ່ວມປະມູນລາຄາ ດັ່ງມີລາຍລະອຽດຂ້າງລຸ່ມນີ້:

No.	List	Model	Quantity
1	Core Switch (Spine)	CE16804	2
2	Router	NetEngine 8000E F1A	4
3	Firewall	USG6656F	2
4	Switch Fix 48 port 25/10G	CE6885-48YS8CQ	14
5	Switch Fix 48 port 1G Base-T	CE5855-48T4XS	6
6	Security Management Platform	SecoManager	1
	Support Implementation, Migration, Training and Warranty (MA & License) for 03 Years, ພ້ອມທັງເຝິກອົບຮົມໃນການນຳໃຊ້ງານໃຫ້ພະນັກງານ ທຄຕລ ຕາມມາດຕະຖານສາກົນ (STANDARD ACADEMY COURSE)		

Equipment specification details

Table 1-1 Core Switch (Spine) Parameter Requirements (02 Units)

Specification	Requirement
Brand	Huawei
Model	CE16804
Hardware specifications	Number of service slots ≥ 4
	Switching fabric support N+1 redundancy for all line card
	Fan tray redundancy design. The number of slots in the fan tray must be greater than or equal to 3.
	A single PSU supports dual inputs and hybrid power supply of AC and HVDC.
	The MPU and SFU are separated from each other. The forwarding performance of the entire system is not affected when the MPU is faulty or replaced.
	The device supports the VOQ capability
	Supports cell switching, inter-board forwarding without packet loss
	Strict front-to-rear airflow.
Performance	Switching capacity not less than 43Tbps
	Packet forwarding rate not less than 11280Mpps
Port Configuration Requirements	- Slot: 1x(36-port 40GE interface card (L-J, QSFP+)) - Slot:1x(48-port 25GE interface card (L-J, SFP28)(CM))
Layer 2 Features	The switch supports access, trunk, and hybrid modes.
	Inter-chassis link bundling technologies such as M-LAG, vPC are supported.
	Dynamic MAC address entries, static MAC address entries, and blackhole MAC address entries
Layer 3 Functions	IPv4 dynamic routing protocols such as RIP, OSPF, IS-IS, and BGP
	IPv6 dynamic routing protocols such as RIPng, OSPFv3, IS-ISv6, and BGP4+

	BFD for OSPF, BGP, IS-IS, and static routes
	IPv6 ND and PMTU discovery
QoS	Queue scheduling modes such as PQ, DRR, and PQ+DRR
	Congestion avoidance mechanisms such as WRED and tail drop
	Broadcast storm suppression
	Traffic shaping
Reliability	Switches support hardware-based BFD at the interval of 3.3ms.
	VRRP, VRRP load sharing, and BFD for VRRP
DC features	VXLAN and BGP EVPN
	VXLAN over IPv6 and IPv6 VXLAN over IPv4 are supported.
Security	MACsec is supported.
	Microsegmentation (IPv4 and IPv6) is supported.
	BPDU guard
	Defense against DoS attacks, ARP attacks, and ICMP attacks
	Bindings of IP addresses, MAC addresses, interface numbers, and VLAN IDs
	Port isolation
	AAA, RADIUS, and TACACS authentication
Multicast	Broadcast, multicast, and unknown unicast storm suppression
	VXLAN ARP broadcast suppression is supported
	IGMP snooping
	IGMP snooping proxy
	Protocols such as IGMP, PIM-SM, and MSDP
Configuration and maintenance	Telemetry
	ERSPAN enhancement is supported.
	IFIT is supported.
	Visualization of packet event packet loss and ultra-long delay is supported.
	VXLAN OAM: VXLAN ping and VXLAN tracert
	SNMPv1/v2/v3, Telnet, RMON, and SSH
	Configuration rollback is supported.
	Network-wide path detection is supported.
	Cached microburst status statistics is supported.
	The switch can be managed by the current DC controller to perform unified SDN configuration deployment and service orchestration. .
	Boot Read-Only Memory (BootROM) upgrade and remote online upgrade
	ZTP technology that allows the configuration to be automatically delivered
Network traffic analyzer	NetStream should be supported.

Table 1-2 Router Parameter Requirements (4 Units)

Specification	Requirement
Brand	Huawei
Model	NetEngine 8000E F1A
Hardware Architecture	The proposed router should support switching capacity ≥ 2.4Tbps.
	The proposed router must support at least 8(eight) 100GE, besides this, the router must also support 48 (forty-eight) 10GE ports
	The proposed equipment must support height(U) no more than 1U
	The proposed router should support 100GE/50GE/40GE/25GE/ 10GE/GE interface.
	The 100G interfaces should support QSFP28 optical module and should support adjustable to 40G and 50G.
	The proposed router should support 100G 80km optical module;
	The proposed router should support redundancy for power and fans.
	In order to ensure product quality, maintainability and versatility, the routers proposed should have a footprint in the global market share of at least the top 3 in the previous years (2020, 2021, 2022).

	The proposed equipment should support NP chipset instead of the ASIC architecture to support new features in future by software upgrade only;
Port Configuration requirement	8*40GE+10*10GE+28*GE,2*AC Power,Port-side Intake
Route & MPLS Feature	The proposed router should support RIP, OSPF, IS-IS, BGP, support RIPng, OSPFv3, IS-ISv6.
	The proposed router should support static routes, multicast static routes.
	The proposed router should support IPv4/IPv6 Dual Stack.
	The proposed equipment must support FIBv4/v6 at least 4M/2M
	The proposed equipment must support RIB v4/v6 at least 10M/5M
	The proposed router should support routing policy.
	The proposed router should support MD5 authentication.
	The proposed router should support OSPF-LDP, IS-IS LDP synchronization.
	The proposed router should support BGP route reflector.
	The proposed router should support non-stop routing.
	The proposed router should support multicast protocols such as: IGMPv2, PIM-SM, MSDP, MBGP, IGMPv3.
	The proposed router should support IGMP snooping.
	The proposed router should support anycast RP and Reverse Path Forwarding.
	The Ethernet and trunk interfaces of the proposed router should support multicast protocols.
	The proposed router should support multicast routing policies.
	The proposed router should support MPLS LDP and MPLS RSVP-TE.
	The proposed router should support LDP and TE FRR, support complete the FRR switching within 200ms.
	The proposed router should support SR-TE and SR-BE.
	The proposed router should support SRv6.
	The proposed router should support SRv6 Policy, support EVPN over SRv6 policy; should provide the configuration examples in the official product document to prove it.
	The proposed router should support SRv6 Policy traffic statistics, should provide the official product document to prove it;
	The proposed router should support IPv6 TI-LFA FRR, should provide the official product document to prove it;
	The proposed router should support SRv6 BE, support EVPN over SRv6 BE; should provide the configuration examples in the official product document to prove it.
	The proposed router should support SR-TE, SR Policy and Class-based tunnel selection (CBTS).
	The proposed router should support load balancing in unequal cost multiple path mode.
	The proposed router should support Inter-AS VPN (Option A, B, or C).
	The proposed router should support dual-stack VPN.
	The proposed router should support EVPN and PBB EVPN.
Switch Features	Ethernet interfaces of the proposed router should support VLAN and VPLS services.
	The proposed router should support MAC address limit function.
	The proposed equipment must support MAC address at least 1M
	The proposed router should support VxLAN.
	The proposed router should support EVPN as the VXLAN control plane, and support MAC address learning by EVPN.
	The proposed router should support Eth-Trunk interfaces and BFD for eth-trunk to detect the eth-trunk interface status.
	The proposed router should support ethernet clock synchronization and G.8275.1.
	The proposed router should support traffic suppression include multicast, broadcast, and unknown unicast traffic.
	The proposed router should support Y.1731 and Y.1731 Eth-LCK, Eth-Test, and Eth-SLM.
	The proposed router should support Flexible Ethernet (FlexEth).
QoS scalability	The proposed router should support 5 level H-QOS.
	The proposed router should support PQ, WFQ and LPQ.
	The proposed equipment must support ACLv4 at least 32k
	The proposed equipment must support ACLv4 at least 16k
	The proposed equipment must support at least 128k queues.

High Availability Feature	The proposed router should support hardware BFD. BFD detect package send period should within 5ms.
	The proposed equipment must support BFD for VRRP, OSPF, ISIS, BGP, LDP, TE, SR, VRRPv6, OSPFv3, ISISv6, BGP4+,SRv6,PW
	The proposed router should support Remote-LFA.
	The proposed router should support VRRP.
	The proposed router should support Ethernet in the First Mile and connectivity Fault Management.
	The proposed equipment must support RFC2544 as a sender and reflector;
	The proposed equipment must support Y.1564 as a sender and reflector;
	The proposed equipment should support IFIT (in-situ Flow Information Telemetry) for in-service detection, smart flow selection and real-time monitoring, which follow the standard "draft-song-opsawg-IFIT-framework-05"
Security	The proposed router should support IPSec
	The proposed router should support IPv4/IPv6 URPF.
	The proposed router should support traffic statistics that discarded by URPF.
	The proposed router should support ARP attack defense.
	The proposed equipment must support BGP Flow Specification and BGP IPv6 Flow Specification
	The proposed router should support BMP (BGP Monitoring Protocol).

Table 1-3 Firewall Requirement (02 Unit)

Specification	Requirement
Brand	Huawei
Model	**USG6656F**
Performance of the entire system	Firewall throughput ≥ 50Gbit/s; maximum number of concurrent connections ≥ 20 million; number of new connections per second ≥ 500,000
	SD-WAN throughput ≥ 50Gbit/s
	Small-packet throughput decreases by no more than 20% compared with large-packet throughput.
	IPS throughput ≥ 25Gbit/s
	IPsec VPN throughput ≥ 30Gbit/s
	SSL VPN throughput ≥ 3Gbit/s
	The number of IPsec VPN tunnels is greater than or equal to 20,000, and the number of concurrent SSL VPN users is greater than or equal to 10,000.
	Firewall forwarding delay ≤ 18μs
	Supports the virtual firewall system. Multiple independent logical devices can be divided on a physical device. Each virtual system is equivalent to a real device. It has its own interface, address set, user/group, routing entry, and policy. It can be configured and managed by the system administrator. It is not a Virtual Routing Forwarding (VRF). Number of virtual firewalls ≥ 2048
Chassis and Port	100G optical ports≥2; 40G optical ports≥2; 25G optical ports≥4; 10G optical ports≥10; gigabit combo port≥8
	Supports two 10GE optical bypass links.
	≥ 2 expansion slots
	USB 3.0 support (photo of the device is provided)
	Standard rack-mounted 1U appliance (Provide the link to the official website, product documentation description on the official website, and stamp the official seal of the manufacturer or the special bidding seal.)
	Two power supplies are configured. Four fans in 3+1 redundancy mode
Port Configuration requirement	2*QSFP28 + 2*QSFP+ + 4*SFP28 + 10*SFP+ + 8GE combo,2 AC power.
Policy management	Supports the configuration of security policy rules based on the source IP address, destination IP address, MAC address, service type, application type, security zone, and time range.
	IPv4 and IPv6 addresses can be configured in a security policy. (Provide function screenshots)
	When the security policy is blocked, the device can send feedback packets to quickly disconnect the connection. For example, the device can send reset packets for TCP packets and ICMP unreachable packets for UDP and ICMP packets. (Provide function screenshots)
Routing function	Supports routing protocols such as static routing, policy-based routing, RIP, OSPF, BGP, and IS-IS.
	Supports SRv6, SRv6 TE policy, and EVPN L3VPN over SRv6 TE policy. (Provide function screenshots)

	Matching conditions supported by PBR: source/destination IP address, service type, application type, user (group), inbound interface, and DSCP priority
IPV6	Supports the IPv6 protocol stack, IPv6 traversal technology, and IPv6 routing protocol.
	IPv6 over IPv4 tunnels and 6RD tunnels are supported.
Flow control	Traffic control policies can be configured based on application layer protocol including the maximum bandwidth, assured bandwidth, and protocol traffic priority. (Provide functional screenshots and affix the manufacturer's official seal or special bidding seal.)
	Supports HQoS based on bandwidth parent and child policies, implementing hierarchical traffic scheduling and refined traffic control.
NAT	Supports NAT66 and NAT64.
	Supports comprehensive NAT functions and the ALG function for multiple application layer protocol including DN, FTP, H323, MSN, Netbio, PPTP, RSH, RTSP, SIP, and SQLnet.
	Triplet NAT smart-fullcone
	Supports the NAT address reuse technology to implement unlimited port translation for a single public IP address which effectively solves the problem of address shortage. (Provide relevant technical patent certificates)
URL filtering	Supports the URL identification capability and URL identification database. The cloud URL identification database is greater than or equal to 560 million (screenshots are provided for proof).
Protocol Identification	Number of identifiable application layer protocols ≥ 6000 (function screenshots are provided for proof)
Content security	Supports data leakage prevention, identifies, and filters transmitted files and content, and matches the content with ID card, credit card, bank card, and social security card numbers.
	HTTP, FTP, SMTP, POP3, NFS, SMB, IMAP, doc, ppt, xls, docx, pptx, xlsx, html, c, cpp, cxx, h, hpp, java, data filtering detection for the TXT file type
Web Protection	Supports web application protection and HTTP-based management and control. (HTTP request method control, HTTP version detection, HTTP request header control, HTTP request body control, and URL parameter content control), intelligent semantic analysis, anti-leeching detection, and web page anti-tamper functions: fine-grained management and control and threat detection for traffic accessing web application servers
IP reputation	Supports IP reputation filtering to identify malicious IP addresses and defend against attacks such as Botnet, mining, and APT. (Provide functional screenshots)
SSL-encrypted traffic detection	Supports SSL-encrypted traffic detection, decrypts SSL-encrypted traffic, performs content security check on decrypted traffic, and detects and defends against hidden threats in SSL-encrypted traffic.
Centralized management and usability	The firewall can interwork with the sandbox to block unknown APT attacks based on the sandbox detection result. The same file does not need to be repeatedly detected. The firewall can update the malicious file and URL list in the cache based on the sandbox detection result. (Provide function screenshots)
	Supports the packet tracing function. It displays the service process and the cause of packet discarding in a graphical manner. (Provide function screenshots)
	Traffic source tracing is supported. Source and destination IP addresses can be traced for the traffic that causes abnormal CPU usage increase. (Provide function screenshots)
	The device can proactively send interface traffic statistic CPU usage, or memory data to the collector using the telemetry function. (Provide function screenshots)
	Open northbound interface such as RESTCONF and NETCONF, to connect to third-party management platforms. (Provide function screenshots)
Reliability	Supports BFD link detection, association between BFD and VRRP to implement fast active/standby switchover, and association between BFD and OSPF to implement fast active/standby switchover. (Provide function screenshots)
	Dual-system hot backup survival is supported. When all heartbeat ports are unavailable, the device sends Hello packets to the peer device through the available service ports to establish the dual-system state through the service ports. The dual-system state is maintained without switchover.

Table 1-4 Switch Fix port 48 25/10GE (14 Units)

Specification	Requirement
Brand	Huawei
Model	CE6885-48YS8CQ
Hardware Specifications	The height is less than or equal to 1 U, with fixed ports
	The power modules work in 1+1 backup
	Front-to-back and rear-to-front air channels
Performance	Switching capacity ≥ 8Tbps
	Packet forwarding rate ≥ 1200Mpps

Port Support	40/100GE optical ports ≥ 8
	The number of 25/10GE optical ports ≥ 48
Port Configuration requirement	48*25GE SFP28, 8*100GE QSFP28, 2*AC Power Modules, 5*Fans, Port-side Intake
Layer 2 Function	Supports the access, trunk, and hybrid modes
	Supports QinQ
	Supports inter-chassis link bundling technologies such as M-LAG, vPC
	Dynamic, static, and blackhole MAC address entries are supported
Layer 3 Function	Supports IPv4 dynamic routing protocols, such as RIP, OSPF, IS-IS, and BGP
	Supports IPv6 dynamic routing protocols, such as RIPng, OSPFv3, IS-ISv6, and BGP4+
	Supports BFD for OSPF, BGP, IS-IS, and static routes
	IPv6 ND and PMTU discovery
QoS	Supports queue scheduling modes such as PQ, DRR, and PQ+DRR
	Supports traffic classification based on the L2 protocol header, L3 protocol, and L4 protocol
	Supports bidirectional port rate limiting
	Provides the broadcast storm suppression function
	Supports traffic shaping
Reliability	Supports VRRP, VRRP load balancing, and BFD for VRRP
	Bidirectional Forwarding Detection (BFD) with a detection interval of 3.3ms
DC Features	VXLAN and BGP EVPN are supported
	Supports VXLAN over IPv6
	Supports IPv6 VXLAN over IPv4
Security	DoS, ARP, and ICMP attacks can be prevented
	Binding of IP addresses, MAC addresses, ports, and VLANs
	Supports port isolation
	Supports user login authentication, such as RADIUS
Multicast	Multicast traffic suppression
	IGMP Snooping
	Supports IGMP proxy
	Supports IGMP, and PIM-SM
Configuration and maintenance	Supports Telemetry
	Supports ERSPAN enhancement
	Supports VxLAN OAM: VxLAN ping, VxLAN tracert
	Supports SNMP V1, V2, V3, Telnet, RMON, and SSH
	Supports configuration rollback based on the CLI.
	The switch can be managed by the current DC controller to perform unified SDN configuration deployment and service orchestration
	Supports BootROM upgrade and remote online upgrade
	ZTP technology, automatic configuration delivery
	Supports automatic Ansible configuration
Traffic Analysis	NetStream

Table 1-5 Switch Parameter Requirements Fix port 48 1GE (06 Units)

Specification	Requirement
Brand	Huawei
Model	CE5855-48T4XS
Hardware Specifications	The height is less than or equal to 1 U, with fixed ports
	The power modules work in 1+1 backup
Performance	Switching capacity ≥ 176Gbps
	Packet forwarding rate ≥ 125Mpps
Port Support	10 GE optical ports ≥ 4

	The number of 1GE Electrics ports ≥ 48
Port Configuration requirement	48*GE RJ45, 4*10GE SFP, 2*AC Power Modules, Built-in Fans, Port-side Intake
Layer 2 Function	Supports the access, trunk, and hybrid modes
	Dynamic, static, and blackhole MAC address entries are supported
Layer 3 Function	Supports IPv4 dynamic routing protocols, such as RIP, OSPF, IS-IS, and BGP
	Supports IPv6 dynamic routing protocols, such as RIPng, OSPFv3, IS-ISv6, and BGP4+
	Supports BFD for OSPF, BGP, IS-IS, and static routes
	IPv6 ND and PMTU discovery
QoS	Rate limiting on packets sent and received by an interface
	Packet redirection
	Interface-based traffic policing; two-rate and three-color CAR
	Eight queues on each interface
	DRR, SP, and DRR+SP queue scheduling algorithms
	Re-marking of 802.1p and DSCP priorities for packets
	Packet filtering at Layer 2 to Layer 4, filtering out invalid frames based on the source MAC address, destination MAC address, source IP address, destination IP address, TCP/UDP port number, protocol type, and VLAN ID
	Queue-based rate limiting and traffic shaping on interfaces
	VLAN slicing
Reliability	Smart Link tree topology and Smart Link multi-instance, providing millisecond-level protective switchover
	G.8032 Ethernet Ring Protection Switching (ERPS)
	STP (IEEE 802.1d), RSTP (IEEE 802.1w), and MSTP (IEEE 802.1s)
Security	Hierarchical user management and password protection
	Defense against DoS, ARP, and ICMP attacks
	Binding of the IP address, MAC address, port number, and VLAN ID
	Port isolation, port security, and sticky MAC
	Blackhole MAC address entries
	Limit on the number of learned MAC addresses
Multicast	PIM DM, PIM SM, and PIM SSM
	IGMPv1/v2/v3, IGMPv1/v2/v3 snooping, MLD snooping, and IGMP fast-leave
	Multicast load balancing among member ports of a trunk
	Interface-based multicast traffic statistics
	Multicast VLAN
Configuration and maintenance	Console, Telnet, and SSH terminals
	Network management protocols, such as SNMPv1/v2/v3
	System logs and multi-level alarms

Table 1-6 Security Management Platform of DC (01 Cluster)

Specification	Requirement
Brand	Huawei
Model	SecoManger
Hardware	Per Node: CPU ≥ 2x48Core, 2.6GHz Memory ≥ 6*32G Hard disk ≥ 2*4TB SATA+4*6TB SATA Network Interface ≥ 8*GE+4*10G SFP+ Power Module ≥ 2*900W AC
Security NE Management	Supports centralized management of security NEs, including firewalls, IPSs, and abnormal traffic cleaning devices
	A device in dual-system mode can be abstracted as a logical device on the controller side for management. During policy configuration, you can directly configure the logical device, improving configuration efficiency

	Manage devices by group. For example, devices can be managed by area or part. In addition, security policies can be configured based on device groups
	Supports configuration reconciliation between the firewall and the controller. That is, you can compare the configuration delivered by the controller to the device with the current configuration of the device. An alarm is generated after the difference is identified. To eliminate configuration differences, you can overwrite the configuration on the controller side with the device configuration or the configuration on the controller side with the device configuration
	Loading license files to devices in batches
	Loading patch files to devices in batches
	Upgrade and management of the firewall software
	Updates the signature database of devices and periodically updates the signature database by connecting to the Huawei security center platform (isecurity.huawei.com) through the Agile Controller-Campus
	Supports SSO to the corresponding security device management page, simplifying O&M
	Supports batch configuration of system templates (DNS server configuration and remote URL query) based on devices or device groups
	BGP FlowSpec traffic diversion is supported
Security Policy Management	Manages basic objects of firewalls, including security zones, addresses, domain groups, services, time ranges, applications, application groups, URL categories, and NAT address pools. Supports the management of xx million objects
	Provides configuration capabilities of intrusion prevention, antivirus, URL filtering, and APT defense, and associates with security policies to implement security detection on network traffic
	Manages security policies, NAT policies, and bandwidth policies based on firewalls, and supports enabling, disabling, and moving management of policies
	Supports hierarchical security policy management to meet policy requirements in different scenarios. For example, the global top/bottom policy facilitates global policy provisioning. Supports sharing policies, implementing group policy sharing among multiple devices/devices. Local policies are supported to implement special policies for a single device
	Supports security policy change statistics and deployment status statistics
	Provides security policy configuration capabilities for sites and site templates, and allows users to specify specific devices and virtual systems to configure detailed policies, including intrusion prevention, antivirus detection, and URL filtering, to implement automatic deployment of security policies
Security Service Orchestration	A protected network segment refers to the IP address range of assets protected by security devices and is the basis for security service orchestration. It can be manually configured or automatically learned from the network controller (iMaster NCE (Fabric) or network topology
	Supports automatic policy orchestration based on the protected network segment. It automatically finds the security device that carries the policy based on the source and destination IP addresses of the policy and automatically deploys the policy to the device. This not only saves the service configuration time, but also shields the underlying firewall networking, improving O&M efficiency
	Security policies can be managed, controlled, and maintained based on service areas. Users do not need to pay attention to the mapping between devices and services, but only service areas and security services. This effectively simplifies security policy design
	The policy management perspective is changed from IP-to-IP policy management to application-based policy management. The policy management perspective identifies the mutual access relationships between applications on the network. The policy management focuses on applications, effectively reducing the number of IP-based security policies
	Supports secure interconnection between campus branches, security policy configuration in SD-WAN scenarios, and delivers security policies based on the SD-WAN traffic model to the firewalls at the site. Supports protection based on addresses, domain names, protocols, ports, application groups, and time segments. Supports the configuration of IPS, antivirus, and URL filtering content security
VPN management	Supports IPSec policy groups and IPSec device template management, facilitating scenario-based batch configuration of IPSec capabilities and simplifying IPSec deployment. Supports unified IPsec monitoring
	IPSec policy templates are supported, improving IPSec configuration efficiency Supports configuration of IPSec policy templates, including the networking type, IKE parameters, and IPSec parameters. Import and export templates When configuring an IPSec policy group, you can reference a policy template to quickly fill in configuration parameters, improving configuration efficiency
NAT source tracing analysis	Collects IPv4/IPv6 session logs of firewalls and IPv4/IPv6 TLV logs. Collects, stores, and reports session logs of xx million EPS devices per second on a single node. IPv4/IPv6 session logs support MAC/VLAN/IMSI/IMEI/MSISDN/ user-defined information processing, enhancing user source tracing capabilities. Device log management, supporting IPv6 NAT66 session logs; Displays the source and destination IP addresses and source and destination ports after NAT66, and filters logs based on the IP address and port number after NAT66.

	Region configuration is supported, improving log readability. During log display, the source and destination IP addresses can be converted to area information based on area configuration, improving log readability.
cyber security analysis	Collects IPS logs of firewalls through syslog, including logs of zombie, Trojan, and worm threat types, and supports report aggregation and display.
	Antivirus logs of firewalls can be collected through syslog, helping users learn about virus transmission behavior and frequent virus events on the network, learn about the network security status in a timely manner, and support report aggregation and display.
	Collects attack event logs of firewalls, helping users learn about the network security status and take targeted defense measures.
Basic device logs	By collecting policy matching logs of firewalls, you can learn the rankings and details of the matching status of security policies on firewalls. If security policies are frequently hit, you can find out the causes and take targeted measures.
	By collecting firewall traffic logs, you can learn about application traffic statistics in terms of users and application types, so that the traffic limiting policy can be applied to the abnormal traffic in a timely manner on the log source.
	Understand the change operations of firewall devices
	Supports intelligent log search, improving log query and fault locating efficiency. Supports flexible log query conditions, including the time and log information, and supports combination of conditions. Displays the time distribution information of log query results. Displaying details about log query results and flexibly adjusting log display information
Policy optimization	After the policy is deployed, the U2000 performs redundancy analysis on the entire network and eliminates the policy redundancy based on the policy optimization algorithm.
	By defining trustlists, risk rules, and hybrid rules, security compliance checks are performed on security policies, and information such as check results and security levels is automatically fed back to security approval owners. This helps security inspectors focus only on non-compliant policy items and improves approval efficiency. Avoid untimely approval and omission of risk strategies.
	Based on the comprehensive audit report, associate the redundancy analysis, number of hits, and compliance check results to export the comprehensive audit report.
	Supports policy matching analysis and implements security policy convergence. Analyzes the matching information of security policies based on policy matching logs and displays the matching time distribution of policies. Displays the hit information about the source and destination IP addresses, services, and source and destination security zones, including the hit count and hit ratio. Displaying the matching information about policies and 5-tuple groups by device
Intelligent Defense	Receives threat handling requests from the big data security system and delivers threat handling policies. The big data security system detects advanced network threats and delivers threat handling policies to security NEs based on the threat severity and attack mode. The security NEs generate blocking policies based on source and destination IP addresses. Delivers threat handling policies to the network controller. The network controller isolates threatened hosts through the managed TOR switches.
	Learns the network topology from the network controller, determines the mapping between security policies and logical security devices, and diverts tenant traffic to the corresponding logical security devices based on service chain scheduling.
Collaborate with the network controller	After security devices are added to the resource pool, tenants can apply for logical security devices as required. The mapping between logical security devices and physical devices in the resource pool is not required.
	Supports security policies within a VPC, between VPCs, and between VPCs and external networks. End point groups (EPGs) of the network controller can be synchronized to the security controller. Different security policies can be configured based on service differences between EPGs to ensure interworking or isolation between EPGs.
	Enables the SNAT service on a specified logical security device. Tenants can configure the SNAT service based on VPC requirements.
	Enables the EIP service on a specified logical security device. Tenants can configure the EIP service based on VPC requirements.
	Enables the IPSec service on a specified logical security device. Tenants can configure the IPSec service based on VPC requirements.

- **ເງື່ອນໄຂຂອງບໍລິສັດ ແລະ ຫ້າງຮ້ານຕົວແທນຈຳໜ່າຍ ທີ່ມີຄວາມຕ້ອງການຍື່ນຊອງປະມູນລາຄາຕ້ອງປະກອບ ເອກະສານໃຫ້ຄົບຖ້ວນດັ່ງລຸ່ມນີ້:**

- **<u>ເອກະສານ ຊອງທີ 1:</u>**

1. ປະກອບເອກະສານໃນນາມນິຕິບຸກຄົນ ທີ່ດຳເນີນທຸລະກິດຈຳໜ່າຍເຄື່ອງອຸປະກອນໄອທີ ຢ່າງໜ້ອຍ 03 ປີ ຂຶ້ນໄປ, ສຳເນົາໃບທະບຽນວິສາຫະກິດ, ໃບຢັ້ງຢືນການເສຍອາກອນປີ 2023-2025 ແລະ *ຕ້ອງເປັນບໍລິສັດ ທີ່ມີໃບ **Manufactural Authorization**, ສາມາດເປີດ **Case & Ticket** ໄດ້.*
2. ຕ້ອງເປັນບໍລິສັດຜູ້ສະໜອງພາຍໃນ ສປປ ລາວ ທີ່ມີໃບຮັບຮອງ ຫຼື ເປັນໂຕແທນຢ່າງເປັນທາງການຂອງ ຜະລິດຕະພັນດັ່ງກ່າວ, ມີທີມງານຊັບພອດທີ່ສາມາດໃຫ້ຄຳປຶກສາ ແລະ ແກ້ໄຂບັນຫາ.
3. ເອກະສານລາຍລະອຽດສະເປັກສິນຄ້າ, ການຮັບປະກັນສິນຄ້າ, ໄລຍະເວລາການຈັດສົ່ງສິນຄ້າ ແລະ ຂໍ້ມູນ ຕ່າງໆ ຕາມ format ທີ່ຕິດຄັດມາພ້ອມນີ້.
4. ເອກະສານຂ້າງເທິງແມ່ນໃຫ້ຍື່ນກ່ອນ ວັນ ພະຫັດ **ວັນທີ 13/11/2025 ເວລາ 11:00 ໂມງ** ໂດຍການສົ່ງ ຟາຍເຂົ້າ E-mail: **procurement@bcel.com.la ແລະ inspect-it@bcel.com.la** ເພື່ອໃຫ້ສຸນໄອ ທີໄດ້ກວດລາຍລະອຽດ, ຂໍ້ມູນທີ່ຈຳເປັນ ແລະ ສະເປັກ.

- **<u>ເອກະສານ ຊອງທີ 2:</u> (ປິດຊອງ)**

1. ໃບສະເໜີລາຄາໃຫ້ລະບຸລາຄາຫົວໜ່ວຍແຕ່ລະລາຍການໃຫ້ລະອຽດ, ແລະ ຕ້ອງລວມມູນຄ່າອາກອນທັງ ໝົດເປັນສະກຸນເງິນກີບໃຫ້ຄົບຖ້ວນ.
2. ຜູ້ສະໜອງຕ້ອງວາງເງິນຄ້ຳປະກັນການປະມູນຕ່ຳສຸດ 10% ຂອງມູນຄ່າທັງໝົດ ໂດຍໜັງສືຄ້ຳປະກັນທີ່ ອອກໂດຍທະນາຄານພາຍໃນ **(ວັນໝົດອາຍຸໜັງສືຄ້ຳປະກັນຕ້ອງເຖິງ ວັນທີ 20/02/2026)** ຫຼື ແຊັກທີ່ວີຊ້າແລ້ວ (ທຄຕລ ບໍ່ຮັບເງິນສົດ), ພາຍຫຼັງປະກາດຜົນ ທຄຕລ ໃຫ້ຜູ້ບໍ່ຊະນະການປະມູນ ຈະສົ່ງ ໜັງສືຄ້ຳປະກັນດັ່ງກ່າວຄືນພາຍໃນ 10 ວັນ.
3. ໃນ **ວັນພະຫັດ ຕອນເຊົ້າ ວັນທີ 20/11/2025 ເວລາ 09:00 ໂມງ** ແມ່ນມື້ເປີດຊອງປະມູນ ສະນັ້ນ , ໃຫ້ຜູ້ສະໜອງທີ່ຜ່ານການຄັດເລືອກຈາກເອກະສານຊອງທີ 1 ມາຍື່ນຊອງລາຄາດ້ວຍຕົນເອງ ຫຼື ສົ່ງຜູ້ຕາງ ໜ້າເຂົ້າຮ່ວມທີ່ຫ້ອງປະຊຸມໃຫຍ່ດອກຄູນ ຊັ້ນ 5 ອາຄານ C.

<u>ໝາຍເຫດ:</u>

- ທຄຕລ ຂໍສະຫງວນສິດ ປະຕິເສດຜູ້ສະໜອງທີ່ປະກອບເອກະສານ ບໍ່ຄົບຖ້ວນ ຫຼື ບໍ່ຖືກຕ້ອງຕາມການ ກຳນົດ ຂ້າງເທິງ.

❖ ເງື່ອນໄຂຂອງສັນຍາລະຫວ່າງ ທຄຕລ ແລະ ຜູ້ສະໜອງທີ່ຊະນະການປະມູນ:

1. ຜູ້ທີ່ຊະນະການປະມູນຈະໄດ້ເຊັນສັນຍາກັບ ທຄຕລ ແລະ ຮັບຜິດຊອບຄ່າທຳນຽມໃນການຈົດທະບຽນ ສັນຍາ.
2. ຖ້າຜູ້ຊະນະການປະມູນປະຕິເສດການເຊັນສັນຍາ ແມ່ນຕ້ອງຮັບຜິດຊອບຄ່າເສຍຫາຍໃຫ້ແກ່ ທຄຕລ ໃນ ອັດຕາ 10% ຂອງມູນຄ່າລວມທີ່ສະເໜີປະມູນ.

ການຊຳລະຈະແບ່ງຈ່າຍເປັນ 02 ງວດ ລຸ່ມນີ້:

- **ງວດທີ 1:** ຊຳລະ 90% ຂອງມູນຄ່າ ພາຍໃນ 25 ວັນ ລັດຖະການ, ພາຍຫຼັງໄດ້ຮັບເຄື່ອງຄົບຖ້ວນ ແລະ ກວດກາຄວາມຖືກຕ້ອງຈາກຄະນະກຳມະການຕິດຕາມກວດກາ.
- **ງວດທີ 2:** ຊຳລະ 10% ຂອງມູນຄ່າ ພາຍຫຼັງຄົບກຳນົດການຄ້ຳປະກັນຄຸນະພາບສິນຄ້າ 06 ເດືອນ.

ດັ່ງນັ້ນ, ຈຶ່ງຂອກແຈ້ງເຊີນມາຍັງທ່ານທີ່ມີຄວາມສົນໃຈເຂົ້າຮ່ວມຍື່ນຊອງປະມູນໃນຄັ້ງນີ້.

ຜູ້ອຳນວຍການ

ທະນາຄານ ການຄ້າຕ່າງປະເທດລາວ ມະຫາຊົນ BANQUE POUR LE COMMERCE EXTERIEUR LAO PUBLIC

ນ. ສາຍສະໝອນ ຈັນທະຈັກ

(ຕົວຢ່າງ) ລາຍລະອຽດເອກະສານການປະມູນ (ກະລຸນາຕື່ມຂໍ້ມູນ ແລະ ເຊັນຢັ້ງຢືນ)

- ອີງຕາມໃບແຈ້ງປະມູນ ສະບັບເລກທີ ……/ທຄຕລ, ລົງວັນທີ ……..

ລ/ດ	ຜູ້ສະໜອງ	ເງື່ອນໄຂ									ໝາຍເຫດ
		ໃບທະບຽນວິສາຫະກິດ	ໃບຢັ້ງຢືນການເສຍອາກອນ	ໃບອະນຸຍາດດຳເນີນທຸລະກິດ	ໄລຍະເວລາໃນການດຳເນີນທຸລະກິດ	ຜົນງານຜ່ານມາ (Server ທີ່ເຄີຍສະໜອງໃຫ້ພາກສ່ວນໃດແນ່)	ປະເພດ / ວັດສະດຸ / ຍີ່ຫໍ້ສິນຄ້າ	ປະເທດຜະລິດ	ການຮັບປະກັນສິນຄ້າ	ກຳນົດສົ່ງ (ວັນ)	
1	ບ/ສ……	(ເລກທີ/ລົງວັນທີ)	(ເລກທີ/ລົງວັນທີ)	(ເລກທີ/ລົງວັນທີ)	…. ປີ	(ໃຫ້ລະບຸ)			…. ປີ	……	

ໝາຍເຫດ: ຂໍ້ມູນທີ່ແຈ້ງຂ້າງເທິງນີ້ ເປັນຄວາມຈິງທຸກປະການ, ຖ້າມີຂໍ້ມູນຜິດພາດ ຂ້າພະເຈົ້າຂໍຮັບຜິດຊອບເອງທຸກປະການ.

ນະຄອນຫຼວງວຽງຈັນ, ວັນທີ .....
ຜູ້ອຳນວຍການບໍລິສັດ

ຜູ້ປະສານງານບໍລິສັດ:
ຊື່:
ໂທ: