DPtech LSW5662-SE Series Ethernet Switch

Overview

In traditional network construction, the corporate intranet and the Internet are independent, causing no harm to network security. As a result, enterprises have long been focused on addressing threats from Internet and network borders and paid little attention to the construction of intranet security. However, the types and numbers of intranet terminals are on the rise, making intranet security an integral part and a vulnerable link in the security police of the entire network. On May 22, 2017, a global outbreak of WannaCry ransomware spread rapidly on the intranet. Although a large number of security control and management devices had been deployed on the customer's existing network, a huge number of internal server and terminal were infected and paralyzed, which indicated their poor performance in face of intranet attacks that keep popping up. A typical intranet security threat under new circumstances, the large-scale outbreak of ransomware shows that intranet security has become a blind spot of today's enterprise information construction. Building a secure intranet will become a major trend in network security construction.

Traditional intranet is a shared network, with no access control on terminals or mutual access among terminals. This vulnerability can be easily exploited by hackers to spread viruses and attacks. In case of intranet security incidents, it is impossible to locate and control the source of attack in the first place and extremely difficult to trace back. DPtech LSW5662-SE Series Self-Secure switches provide the network with security protection and exception disposal capabilities by taking advantage of intelligent computing technology. The built-in behavior model and baseline detection provides the Self-Secure switches with immunity to virus transmission, network attacks, and hacker penetration. With automatic policy deployment, self inspection and recovery of ring networks, and baseline detection, it can further extend its security protection to intranet, realizing threat suppression of key nodes of network, operation and maintenance of the entire network, and simplified network management.

Product Features

- **Behavior model detection to enable virus suppression and other threats**
  With its built-in behavior model and traffic baseline, the LSW5662-SE Series can provide timely alerts on abnormal network events, such as virus transmission, IP/MAC spoofing, bots attacks and hacker penetration, and contain such events within one switch.

- **Fast loop blocking to pinpoint exceptions**
  Based on the Technology of industry’ s unique real-time loop detection, the LSW5662-SE Series can spot and block the switch’ s own loop, downlink switch and Hub loop, and pinpoint loop interfaces

and loop vlan through active detection and passive monitoring.

- **Effectively detect breaches to provide clean intranets**

  The LSW5662-SE Series can spot illegal inline behaviors of connected devices (such as small routers) to avoid network security threats and daily operation and maintenance problems caused by private connections, ensuring compliance and reliability of intranet access devices.

- **Automatic deployment of policies to enable convenient operation and maintenance**
- Through real-time interactions of security policies with the Self-Secure management platform, the LSW5662-SE Series enables administrators to distribute threat disposals on a unified management interface, making sure the security policies take effects on a real time basis and simplifying network operation and maintenance.

- **A wide temperature range of 0°C~70°C**

  The LSW5662-SE Series adopts an environment-enhanced design, which provides features such as a wide range of operating temperature (i.e., 0°C~70°C) and pressure, and lightning protection. This helps ensure highly reliable operation in complex electrical environments (e.g., LV well) and air-conditioning free deployment environments.

- **Comprehensive IPv6 features**

  The LSW5662-SE Series Self-Secure switches support IPv4/IPv6 dual stack and IPv6 over IPv4 Tunnel (including manual Tunnel, 6to4 Tunnel, ISATAP Tunnel) as well as IPv6 layer 3 wire-speed forwarding. It can be flexibly deployed on a network with only IPv4 or IPv6, or with both IPv4 and IPv6, thus satisfying the transition requirements from IPv4 to IPv6.

Product Series

LSW5662-28GT4XGS-SE

LSW5662-48GT4XGS-SE

LSW5662-24GP4XGS-SE

LSW5662-48GP4XGS-SE

Function Descriptions

Product Name	LSW5662 -28GT4XGS-SE	LSW5662 -48GT4XGS-SE	LSW5662 -24GP4XGS-SE	LSW5662 -48GP4XGS-SE
Service interface	20 Gigabit electrical interfaces + 8 Gigabit Combo+4 10-Gigabit optical interfaces (SFP+)	48 Gigabit electrical interfaces + 4 10-Gigabit optical interfaces (SFP+)	16 Gigabit optical interfaces + 8 Gigabit Combo + 4 10-Gigabit optical interfaces (SFP+)	48 Gigabit optical interfaces (SFP); 4 10-Gigabit optical interfaces (SFP+)
Switching capacity	758Gbps/7.58Tbps	758Gbps/7.58Tbps	758Gbps/7.58Tbps	758Gbps/7.58Tbps
Packet forwarding rate	342Mpps	372Mpps	342Mpps	372Mpps
Expansion Slots	1 pieces			
Interface Module	2-port 40G optical interface module (QSFP), 8-port 10-Gigabit optical interface module (SFP+), 8-port 10-Gigabit Ethernet interface module, 1-port 40G optical interface module (QSFP), 4-port 10-Gigabit optical interface module (SFP+), 2-port 10-Gigabit optical interface module (SFP+), 8-port Gigabit optical interface module (SFP), 8 port Gigabit electrical interface module, 4 port Gigabit optical interface module (SFP) + 4 port Gigabit electrical interface module			
Protection against intranet attacks	Support locating and blocking of IP spoofing, ARP spoofing, ARP flooding and other common network threats Support identifying and blocking of intranet virus and Trojan horse spreading Support IP scanning, UDP scanning, TCP scanning and other hacking behaviors; Support locating, alerting and blocking of the source host of intranet attacks			
Device protection	Support automatic discovery and protection of IP cameras, entrance control, printers, and all-in-one devices in the network; Support real-time discovery and blocking of TP-Link, D-Link and other small routers			
Loop suppression	Spot and block the switch’s own loop, downlink switch and HUB loop, and pinpoint loop interfaces and loop vlan			
User awareness	Support identification of the type of access terminals and access locations			

Dimension (W*D*H)	440mm*400mm*44 mm			
Power supply	hot-plug, modular dual power supply, support AC/DC			
Power Consumption	70W	61W	90W	108W
Operating environment	0℃ ~ 70℃, 6KV interface lightning protection			
IP routing	Support layer 3 routing of IPv4 and IPv6 Support static routing Support RIPv1/v2, OSPF, BGP, VRRP Support RIPng, OSPFv3, BGP4+ for IPv6, and VRRPv3 Support policy-go-together			
Security features	Support locating and blocking of IP spoofing, ARP spoofing, ARP flooding and other common network threats Support identifying and blocking of intranet virus and Trojan horse spreading; Support locating, alerting and blocking of the source host of intranet attacks Support automatic discovery and protection of IP cameras, entrance control, printers, and all-in-one devices in the network; Support local and centralized authentication based on MAC address Support local and centralized authentication based on 802.1x; Support local and centralized authentication based on Portal Support dynamic ARP detection, one-click ARP binding, authorized ARP, ARP source suppression, ARP source address inspection; Support port isolation, port security Support broadcast storm suppression; Support SSH2.0			
Virtualization	Support VSM virtualization			
Management and Maintenance	Support RMON Support IEEE 1588v2 PTP Support real-time temperature detection and alarm Support SNMP, CLI, Web management, and Unified Management Center (UMC); Support local and remote output of system logs, operation logs, commissioning and debugging information, etc.			

Hangzhou DPtech Technologies Co., Ltd.
Address: 6th Floor, Zhongcai Building, No. 68 Tonghe Road, Binjiang District, Hangzhou City, Zhejiang Province
Postcode: 310051
Official Website: www.dptech.com
Service Hotline: 400-6100-598