DPtech Self-Secure Switch Series

Overview

In the Internet era, information systems have become vital infrastructure of enterprises and played a increasingly important part in the operation. The Internet and Cloud computing technologies have greatly improve efficiency for enterprise, while bringing new problems. For example, as core business systems and important data are carried and transmitted through the Internet, network and information security has emerged as a key issue. All enterprises are keen to address the issue of keeping balance between efficiency and security, with network security being the next hot topic for enterprise information system construction. 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 first and foremost information security threat generally comes from attacks and viruses on the intranet, as it has become a vulnerable link in the entire network. On May 22, 2017, the global outbreak of WannaCry ransomware that spread rapidly on the intranet paralyzed a large number of intranet servers. Although these companies had purchased and deployed a large amount of information security equipment, they still failed to do anything effective to cope with intranet attacks that keep popping up. A typical intranet security threat, the large-scale outbreak of ransomware shows that intranet security has become a blind spot of today's enterprise information construction and that it is imperative to build a secure intranet.

Traditional intranet is a shared network, with no access control on 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. Meanwhile, traditional intranet terminals require authentication on clients, but it becomes inconvenient to use client authentication given the diversified types of terminals and operating systems nowadays. What' s more, difficulty in maintenance by administrators and poor compatibility result in ineffective deployments.

In response to the current status of intranet security, DPtech has launched a Self-Secure secure network Solution, aiming to address intranet security issues through lightweight deployment. In combination of Self-Secure controllers and Self-Secure management platform, DPtech' s Self-Secure switches provides users with clientless authentication, precise user location, virus and attack control, and traceability of user behaviors. Through interactions of Self-Secure switch, Self-Secure controller and Self-Secure management platform, and relying on policy follow-up and automatic deployment based on SDN architecture, it will become easier for users to access to intranet and administrators to conduct operation and maintenance.

Designed for secure network and office network, DPtech Self-Secure secure network Solution can be widely adopted in enterprises, governments, health care, education and other industries. In face of intranet security threats under new circumstances, the solution enables Self-Secure intranet access and operation and maintenance with lightweight deployment models.

Product Features

- **Clientless authentication and non-sensing roaming**

  DPtech Self-Secure secure network Solution supports clientless authentication for internal terminals. After the successful authentication for the first time, the device can log to the intranet later with transparent authentication. The authentication information can be roamed throughout the network to realize easy access.

- **Traffic control model combining blacklist and whitelist**

  The DPtech Self-Secure secure network Solution provides intranet traffic shaping and control. A whitelist model is deployed for intranet lateral traffic, blocking all traffic and allowing only service traffic such as access to printer and sharing resource groups to pass through. In this way, it helps effectively control virus spreading in intranet. A blacklist model is deployed for intranet vertical traffic in order to manage and control DDoS and other attacks through defenses against behavior, service and threat.

- **Progressive security policies deployed as needed**

  The DPtech Self-Secure secure network Solution allows policy deployments of vertical traffic control at three levels: behavior, service and threat. Behavior policy is deployed to monitor all access users. Once illegal actions by a user are found, the Self-Secure switch will freeze the user. When the user passes authentication, the service policy will be linked to user identity, location, status and other information, making sure access to certain services is limited to users with certain permissions to avoid unauthorized access. In the meantime, special policies can be deployed to address deep threat and advanced attacks, realizing intensified protection for the intranet.

- **Network-wide policy interaction to prevent any potential threat**

  Through interactions of DPtech Self-Secure switch, Self-Secure controller and Self-Secure management platform, network-wide policies can be dynamically distributed, and the access layer automatically can implement policies from the management platform to prevent any potential threat.

- **Intranet user awareness and network-wide traceability**

  The DPtech Self-Secure secure network Solution is capable of intelligently detecting users and monitoring their online behaviors. It performs auditing and generates logs automatically of any abnormal behavior and access, helping administrators gain an overall understanding of intranet user behaviors.

- **Smooth evolution of the existing network**

  The DPtech Self-Secure controller can be deployed online or side-by-side, realizing zero-modification expansion in the original network, and allowing clientless authentication and policy follow-up of users and devices within the network. DPtech Self-Secure Switch enables awareness of user behaviors, access location and other information. Through interactions with security policies, seamless security is thus made possible. The deployment of professional Network Security devices will facilitate the

upgrade and transformation of network security construction by providing strong defense against deep threats and advanced attacks, and help users to smoothly evolve their networks and build a Self-Secure network that is safe, easy to manage, and visualized.

Product Series

iNAC-Blade-A

iNAC-Blade-AI

iNAC-Blade-17A

LSW3600-24GT4GP-SE

LSW3600-48GT4GP-SE

LSW3600-24GT4GP-PWR-SE

LSW3600-48GT4GP-PWR-SE

LSW3620-24GT4XGS-SE

LSW3620-48GT4XGS-SE

Function Descriptions

Function Descriptions of DPtech Self-Secure Controller

Product Model	iNAC-Blade-A/AI/17A
Highly reliable design	Support key hardware redundancy of master control, power supplies and fans
Virtualization features	Support VSM virtualization and cloud boards
Access authentication	Support Portal, IP, MAC, PPPOE, WeChat, SMS and other authentication modes
Access management	Support permission management based on IP, user and user group
Traffic control	Support whitelisting for lateral traffic and blacklisting for vertical traffic Support granular traffic control and traffic model analysis and learning
Auditing of abnormal traffic	Support alert and blocks based on unified auditing of traffic model and behavior models
User traceability	Network-wide identity follow-up; support detection of access terminal, precise positioning of user location, and network-wide traceability of user behaviors
Automatic deployment	Support Openflow1.3 protocol and network-wide automatic deployment

Function Descriptions of DPtech Self-Secure Switch

Product Model	LSW3600-24GT4GP-SE	LSW3600-48GT4GP-SE	LSW3600-24GT4GP-PWR-SE	LSW3600-48GT4GP-PWR-SE	LSW3620-24GT4XGS-SE	LSW3620-48GT4XGS-SE
Service interface	24 Gigabit RJ45 +4 Gigabit SFP	48 Gigabit RJ45 +4 Gigabit SFP	24 Gigabit RJ45 +4 Gigabit SFP	48 Gigabit RJ45 +4 Gigabit SFP	24 Gigabit RJ45 +4 10-Gigabit SFP+	48 Gigabit RJ45 +4 10-Gigabit SFP+
Switching capacity	598Gbps/ 5.98Tbps	598Gbps/ 5.98Tbps	598Gbps/ 5.98Tbps	598Gbps/ 5.98Tbps	598Gbps/ 5.98Tbps	598Gbps/ 5.98Tbps
Packet forwarding rate	216Mpps	252Mpps	216Mpps	252Mpps	222Mpps	252Mpps
IP routing	Support static routing, RIPv1/v2, OSPF					
User awareness	Support precise identification of the type of access terminals and access locations					
Device protection	Support automatic discovery and protection of IP cameras, entrance control, printers, and all-in-one devices in the network					
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 locating, alerting and blocking of the source host of intranet attacks					
Fan	Fanless		2 pieces		Fanless	1 pieces
PoE external power	- -	- -	AC input 370W DC input 740W	AC input 370W DC input 740W	- -	- -
Operating Temperature	0°C~70°C 6KV interface lightning protection		-10°C~55°C 6KV interface lightning protection			
Management and Maintenance	Support real-time temperature detection and alarm Support SNMP, CLI, Web network management and unified management through Self-Secure management platform Support local and remote output of system logs, operation logs, debugging information					

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