DPtech Intelligent Self-Security Network Switch

Hangzhou DPtech Technologies Co., Ltd.

Product Overview

In the Internet age, information systems have become the most important infrastructure for enterprises and play an increasingly important role in enterprises. New technologies such as the Internet and cloud computing have helped enterprises to improve their efficiency but also bring new problems. The core business systems and important data are carried and transmitted through the network, which will inevitably cause network and information security issues. How to achieve both efficiency and security is what all enterprises concern about, and network security will become the next hot spot in enterprise information construction.

For the traditional network construction, the enterprise intranet and the Internet are independent of each other, so there is no security risk. Therefore, in the process of information security construction, enterprises concern more about threats from the Internet and network boundaries, ignoring the security construction of intranets. In fact, the primary threat to enterprise information security often comes from intranet attacks and viruses, and intranet security has become a weak link in the entire network. On May 22, 2017, WannaCry ransomware broke out in the world and spread rapidly on the intranet, causing a large number of enterprises with infected intranet servers come to a standstill. Although these companies purchase and deploy a large number of information security devices, they are still stretched in the face of endless intranet attacks. The ransomware is the representative of the intranet threat under the new situation. Its large-scale outbreak just shows that intranet security is a blind spot in today's enterprise information construction. So, it is imperative to build a secure intranet.

The traditional intranet is a shared network. Terminal access is uncontrolled, which provides great convenience for the spread of viruses and attacks. Once an intranet security incident occurs, it is impossible to locate and control the attack source in the first time, and extremely difficult to trace back afterward. At the same time, traditional intranet terminals often adopt client authentication. However, the types of terminals and operating systems are constantly enriched. Client authentication is inconvenient for users, difficult for administrators to maintain, and has poor compatibility. So, it cannot be effectively deployed.

For the status quo of intranet security, DPtech has launched DPtech Self-Security Campus Network Solution, which aims to solve intranet security problems through lightweight deployment. DPtech self-security switches series products, together with self-security controllers and self-security management platforms, can provide features such as clientless authentication, user precise positioning, virus and attack control, user behavior backtracking. Linked from the security switch and the self-security controller and the self-security management platform, the user-based network strategy is followed and automatically deployed based on the SDN architecture, enabling easy access for users and easy operation and maintenance by network administrators.

DPtech self-security campus network solution is designed for campus and office network applications. It can be widely used in enterprises, governments, health care, education, etc. Under the new situation of intranet security threats, the lightweight deployment model is adopted to achieve intranet security access and secure operation and maintenance.

Product Features

Clientless authentication, no sense roaming

The DPtech self-security campus network solution supports clientless authentication for intranet terminals. After the device is authenticated for the first time, secondary access uses no sense authentication. User authentication information can be roamed throughout the network for easy access.

"Black & White List" traffic management model.

The DPtech self-security campus network solution can be used to shape and control the intranet traffic. The white list traffic model is deployed for the intranet horizontal traffic. By default, all traffic is blocked, and only traffic that accesses printers and shared resource groups is allowed to pass, effectively suppressing intranet virus propagation; The blacklist traffic model is deployed for the vertical traffic of the intranet. It is heavily deployed on the three levels: behavior, services and threats, so as to control intranet threats like abnormal access and attacks.

Deploy progressive security policies on demand

DPtech's self-security campus network solution can be targeted at the intranet vertical traffic and deploy the triple strategy of behavior, services, and threats：The behavior policy is for all access users. The security switch detects user behavior and freezes the user once an illegal operation is found；After the user passes the authentication, the business policy is associated with the user identity, location, status, etc., ensuring that only users with specific permissions can access specific service resources to prevent unauthorized access；At the same time, threat strategies can be deployed for deep threats and high-level attacks to achieve internal network heavy arming.

The whole network strategy is linked, and the threat is kept outside of the network

The DPtech self-security switch and the self-security controller can be linked to the self-security management platform to implement the dynamic delivery of the entire network policy. The access layer automatically executes the policies issued by the management platform and drive the threats outside of the network.

Intranet user sense and network backtracking

The DPtech self-security campus network solution intelligently senses users, monitors intranet user behavior, automatically generates logs for abnormal behaviors and user access, and helps administrators fully grasp user intranet behavior.

Smooth network evolution

The DPtech self-security controller supports online deployment and bypass expansion. It can realize “zero-change” expansion in the old network, enabling clientless authentication and policy following for the entire network of users and devices; The DPtech self-security switch can be configured to sense user behavior, access location, and other information, and can link security policies to achieve “overall security”. With the network security upgrade and transformation, it can be deployed with professional security equipment to prevent deep threats and advanced attacks, and help users to smoothly evolve to a secure, manageable, and visualized self-security network.

Product Series

iNAC-Blade-AI

iNAC-Blade-17A

LSW3600-24GTGP-SE

LSW3600-48GTGP-SE

LSW3600-24GT4XGS-SE

LSW3600-48GT4XGS-SE

LSW3600-24GT4GP-PWR-SE

LSW3620-48GT4GP-PWR-SE

LSW3620-24GT4XGS-PWR-SE

LSW3620-48GT4XGS-PWR-SE

Specification

DPtech Intelligent Self-Security Controller Module (iNAC)

Model	iNAC-Blade-AI/17A
Highly reliable design	Supports key hardware redundancy configurations such as main control, power supply, and fan.
Virtualization	Support VSM virtualization and cloud board technology

Access certification	Support Portal, IP, MAC, PPPOE, WeChat, SMS and other access authentication methods Support non-aware authentication and authentication roaming technology
Authority management	Support authority management based on IP, users, and user groups
Traffic control	Whitelist control for horizontal traffic and blacklist control for vertical traffic Support refined traffic control and traffic model analysis and learning
Abnormal control	Supports alarms and blocking of abnormal behavior recognition based on traffic model and behavior model
User traceability	The identity of the entire network is accompanied by the access terminal identification, accurate user location, and user network behavior.
Automatic deployment	Support Openflow1.3 protocol Support automatic network deployment

DPtech Intelligent Self-Security LSW 3600 SE Series Switch

Model	LSW3600-24GT4GP-SE	LSW3600-48GT4GP-SE	LSW3620-24GT4XGS-SE	LSW3620-48GT4XGS-SE
Interface	24*1GE RJ45 +4*1GE SFP	48*1GE RJ45 +4*1GE SFP	24*1GE RJ45 +4*10GE SFP+	48*1GE RJ45 +4*10GE SFP+
Switching Capacity	598Gbps	598Gbps	598Gbps	598Gbps
Packet forwarding rate	216Mpps	252Mpps	222Mpps	252Mpps
IP Routing	Support static routing、RIPv1/v2、OSPF			
User perception	Accurate positioning of access user terminal types and access locations			
Equipment protection	Support automatic discovery and protection of IP cameras, access control, printers, all-in-one devices, etc.			
Intranet attack protection	Supports the positioning and blocking of common network threats such as IP spoofing, ARP spoofing, and ARP flooding. Support the identification and blocking of virus and Trojan propagation behavior Supports internal network attack source host location, alarm, and blocking.			
Fan	No Fan			1
Power consumption (excluding PoE power)	22W	34W	20.6W	39W
Operating temperature	0°C~70°C		-10℃~55℃	
Management	Support RMON Support real-time temperature detection and alarm Support SNMP, CLI, Web network management and self-security management platform unified management			

	Support local and remote output such as system logs, operation logs, and debugging information

Model	LSW3600-24GT4GP-PWR-SE	LSW3600-48GT4GP-PWR-SE	LSW3620-24GT4XGS-PWR-SE	LSW3620-48GT4XGS-PWR-SE
Interface	24*1GE RJ45 +4*1GE SFP	48*1GE RJ45 +4*1GE SFP	24*1GE RJ45 +4*10GE SFP+	48*1GE RJ45 +4*10GE SFP+
Switching Capacity	598Gbps	598Gbps	598Gbps	598Gbps
Packet forwarding rate	216Mpps	252Mpps	216Mpps	252Mpps
IP Routing	Support static routing、RIPv1/v2、OSPF			
User perception	Accurate positioning of access user terminal types and access locations			
Equipment protection	Support automatic discovery and protection of IP cameras, access control, printers, all-in-one devices, etc.			
Intranet attack protection	Supports the positioning and blocking of common network threats such as IP spoofing, ARP spoofing, and ARP flooding. Support the identification and blocking of virus and Trojan propagation behavior Supports internal network attack source host location, alarm, and blocking.			
Fan	2			
PoE supply power	AC input 370W; DC input 740W			
Power consumption (excluding PoE power)	20W	30W	21W	39W
Operating temperature	-10℃~55℃			
Management	Support RMON Support real-time temperature detection and alarm Support SNMP, CLI, Web network management and self-security management platform unified management Support local and remote output such as system logs, operation logs, and debugging information			