Secure Web Gateway

NP Series

Product Overview

NP Series is a family of professional web agent appliances for government and enterprise users. It helps customers gain insights into online behavior and risks by providing URL filtering, malicious code detection and filtering, application control, data leakage prevention and other protection capabilities. NP can effectively reduce the risk of Internet use and avoid leakage of confidential information.

Main Functions

Funciton	Description
Internet proxy	• Support mainstream applications, including HTTP, HTTPS , DNS, FTP , SOCK, etc. • Support proxy and reverse proxy to meet different business scenarios.
Authentication proxy	• Support IP-based user identity authentication, session-based proxy authentication, AD authentication, NTLM integration domain authentication, etc.
Control proxy	• Supports access control based on traditional 5-tuple, applications and subdivisions. • Support checking and filtering content based on web pages, uploading and downloading content.
Security detection	• Support virus scanning, malicious URL and threat detection without additional delay.
SSL decryption	• Decryption scanning of designated and unclassified https sites.

Features

In Gartner Magic Quadrant

• Be selected in 2020 Gartner Secure Web Gateways (SWG) Magic Quadrant and Critical Capabilities for Cloud-Based Secure Web Gateways (SWG).

Full Agent Architecture

• Realize complete isolation of internal and external network
• Check and control 100% full traffic

Rich security extension support

• Support application-based raw traffic mirroring

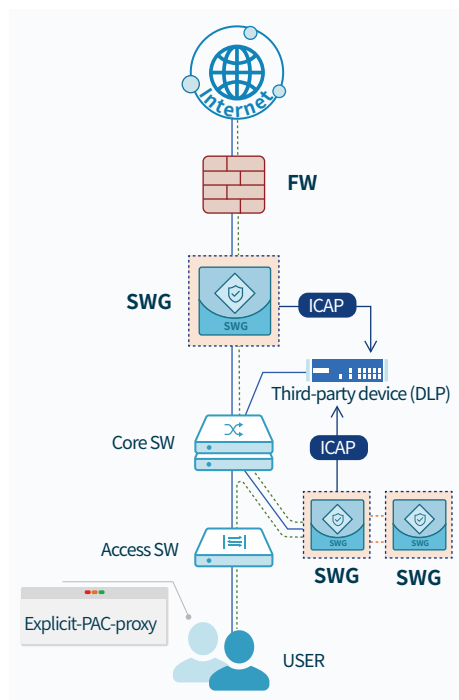• Support the link with other third-party security devices through the ICAP protocol

High-availability Architecture

• Support device redundancy and load balancing without relying on third-party load balancing devices.
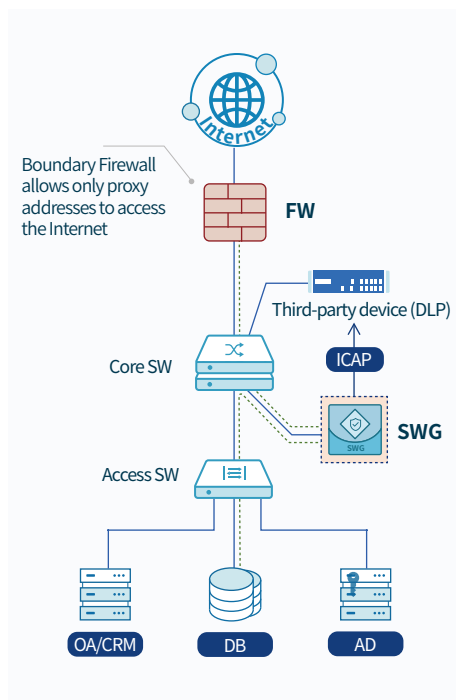
Values

◆ **Prevent and Block Malicious Network Activity**
Block communications associated with spyware, phishing, malwares like Trojan, Spyware and Virus.

◆ **Manage User Network Activity and Promote Employee Productivity**
Provide comprehensive monitoring and analysis to evaluate employee productivity loss due to non-work-related network activities.

◆ **Significantly reduce the management cost of the entire network equipment and improve management efficiency**
Provide visibility of network traffic, composition and trends so as to limit or block the bandwidth-consuming/harmful applications.
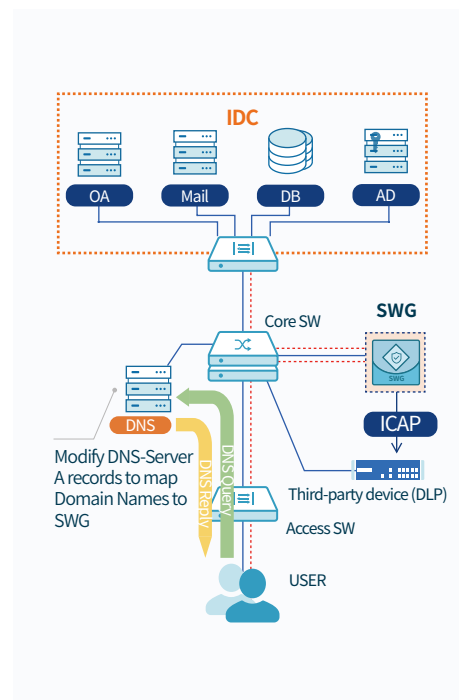
Typical Deployment

Explicit-proxy/Transparent-proxy

Explicit-proxy/Transparent-proxy

Reverse-proxy

Internet Access Control

• Deployment at the entrance of Internet or bypass deployment; all users accessing the Internet via SWG agents;

• Filter out risky traffic and malware for user-initiated internet access;

• Effective protection from web-based threats

Key Application Proxy Access to Internet

• Key application systems access the Internet through agents for upgrading;

• Effective protection from web-based threats

Secure Access to Internal Systems

• Deployed before the internal systems, intranet users accessing internal systems through the reverse-proxy;

• Protect internal system security by strictly checking intranet user access.

Hardware Specifications

Model		NP3010	NP3030	NP5010	NP5030	NP5050	NP7010	NP7030
Performance	Bandwidth	50M	100M	500M	800M	1G	2.5G	5G
	Users suport	400	800	1500	4000	8000	20000	30000
	Concurrent connections	120K			300K	600K	900K	1200K
Hardware Configuration	Interface modules	1MGT+6*10/100/1000M Base			1MGT			
	USB	2						
	RS232 Serial	√						
	Bypass	√						
	Storage	1T					2T	
	W*D*H mm	440*330*44		440*560*89	440*540*88		440*560*88	
	U	1U		2U				

Note: the above contents are for reference only, subject to the actual product