Sangfor NGAF

DMZ and Data Center Protection With Sangfor NGAF

www.sangfor.com

SANGFOR

DMZ and Data Center Protection With Sangfor NGAF

01

Data Center Protection Situation

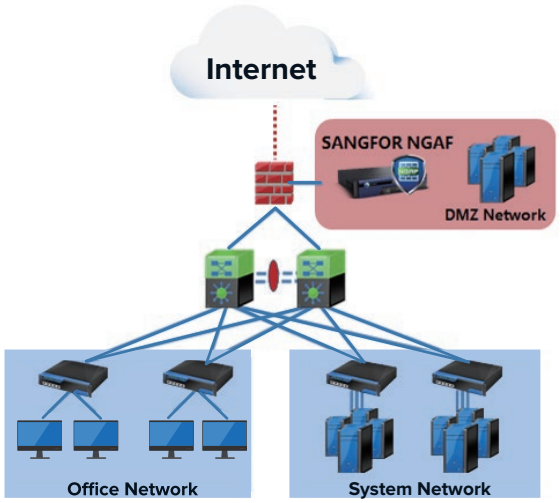
1. Over 70% of network attacks come from the application layer. Although the data center has security domains, there is a short board in the application layer attack protection;

2. Business systems increase and management is complex, lack of a global security perspective to quickly identify and deal with security issues;

3. The security defense system based on static features cannot defend against advanced attacks, resulting in the potential for hidden threats within the data center and impact the normal business.

Problems and Challenges Faced by Traditional Protection

- Customer servers always being exposed to security threats
- Loss of revenue due to business systems down
- Do not have IT expertise to focus and secure the production servers
- Web Defacement Incidents everyday



The Benefit of Data center Secure with NGAF Benefit

Proactive Protection

- Risk assessment
- Web scanner
- Real-time vulnerability analysis

Proactive Protection

- Vulnerability exploits
- Web-based attacks
- Hidden Trojan
- Malware threats,
- APT

Proactive Protection

- Data leakage prevention
- Anti-DDoS
- Anti-defacement

Proactive Protection

- Security Visibility
- Reporting
- Simple O&M with Business Based Interface

Sangfor Secure Data Center Advantages

Business Data Real-Time Protection

- Comprehensive risk assessment
- Leveraging AI technology to defend against unknown and advanced threats

Business Data Real-Time Protection

- Detect and resolve issues associated with webpage tampering, Trojans and information leakage, even if defenses are bypassed

Business Data Real-Time Protection

- Repair any damage done by attack chains with the ability to trace and identify threats

Sangfor Next Generation WAF

Traditional Engine

Signature Based Static Engine

- Traditional engines are unable to detect unknown attacks and exploits and are easy to bypass
- Common false positives in detection of SQL injections
- Outdated detection capabilities and poor performance

Semantic Analysis

Machine Learning

Next Generation WAF Engine: Reduce False Positives by 62.4%

- Identify unknown threats and high-risk vulnerabilities using AI technology
- Automatically learn and model normal business traffic and reduce false positives by 62.4%


SAPIENTIA·ET·VIRTUS
KERANA TUHAN UNTUK MANUSIA
UNIVERSITI TEKNOLOGI MALAYSIA
TEGUH DIRAJA MALAYSIA
สำนักงานประกันสังคม
Social Security Office
MINISTRY OF FOREIGN AFFAIRS
SINGAPORE
KENANGA
AASTOCKS
BNI
MNC
Carrefour
Canon
Shell
AirAsia
Holiday Inn
SNZ