

SANGFOR
NGAF



www.sangfor.com

Sangfor NGAF

Internet Gateway Security with Sangfor NGAF



SANGFOR
NGAF
SANGFOR NGAF
SANGFOR NGAF
SANGFOR NGAF
SANGFOR NGAF
SANGFOR NGAF
SANGFOR NGAF
SANGFOR NGAF



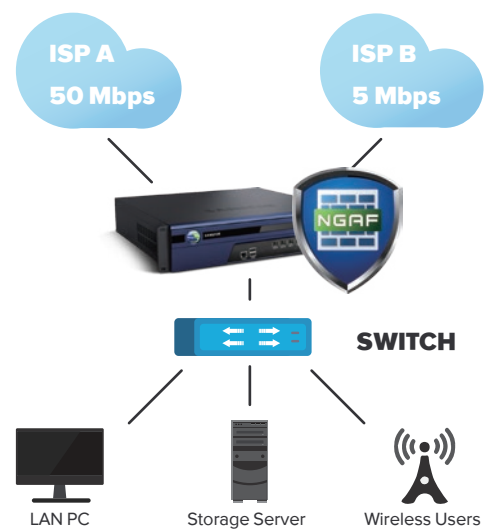
SANGFOR

Gateway Security Risks

For internal network access users, botnets are the most prevalent security problem. Hackers use various intrusion methods including viruses and Trojan worms to control terminals and form Botnets. Information stored in the terminal can be stolen while the terminal is guided to a phishing website and used as an attack bridge to access other resources.

Problems and Challenges Faced by Traditional Internet Gateway

- Office PC users are vulnerable to botnet virus infection, Trojans and worms.
- Legacy security gateways lack appropriate security protection capabilities allowing various ransomware and unidentified threats to easily bypass tradition protection.
- Lack of rapid detection capabilities cause Intranet failure for hosts and don't allow for quick reaction to security issues.
- IT administrators often lack the professional skills necessary to perform effective security operations.



Sangfor NGAF Internet Gateway

Stable Gateway

- Common Access Method
- Basic Routing
- NAT Function
- DHCP Server
- High Availability
- Multi-Line Support
- Load Balance

Secure Gateway

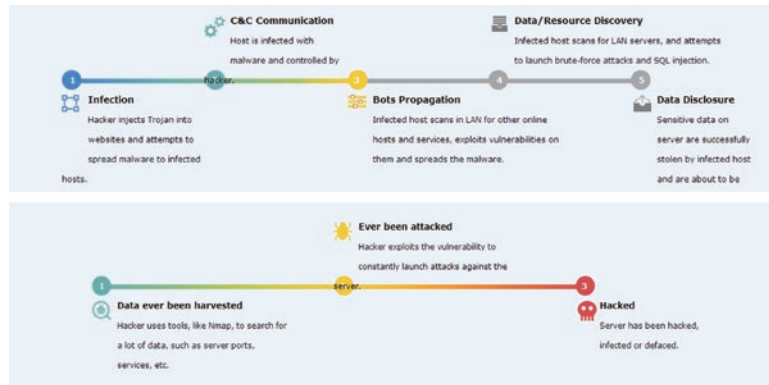
- High Performance Firewall + WAF + IPS
- User, Behavior and IT Asset Visibility
- Risk and Attack Visibility
- Real-Time Detection
- Unknown Threat Detection
- Rapid Response to Threats

Simple Gateway

- Configuration Wizard
- Policy Layout
- Automated Security Operation Guidance
- Business Based Scanning Tool
- Bandwidth Management
- Traffic and User Behavior Control
- Business Based Security Reporting

Real-Time Detection :

Real-time detection of threats at every attack stage allowing rapid response to any risks.



IT administrators are aware of all real-time threats at every stage of the cyber kill chain....



...providing rapid response to any security risks or attacks.

Security Visibility:

Effective Analysis & Presentation: Risk Positioning | Analysis of Data | Graphical Display

Visibility of Assets

- Identify core business system assets (examples: application software, users, devices, and content)

Visibility of Threats & Risks

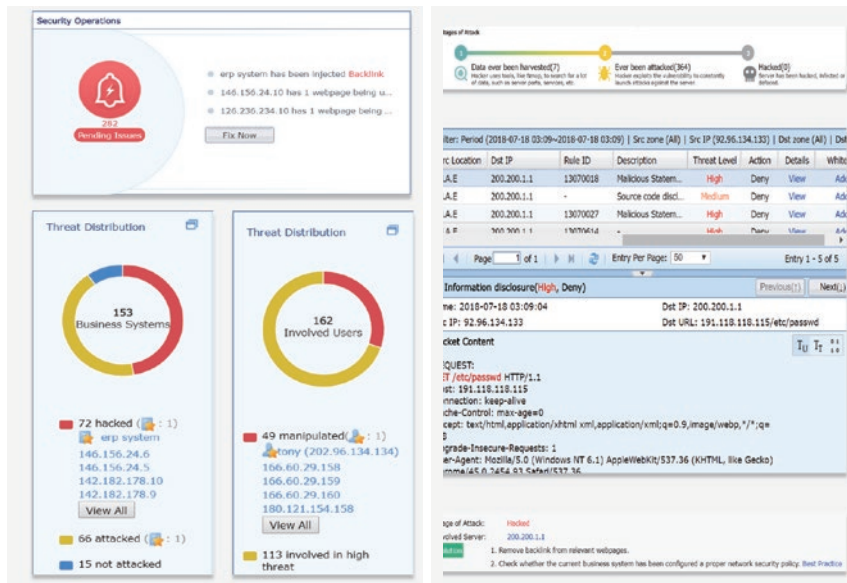
- Identify vulnerabilities and risks to business assets.

Visibility of User Behavior

- Distinguish between common and uncommon user behavior, identify potential risks and respond to threats in real-time.
- Easy distinguish between legitimate users and malicious users accessing services

Simplified Security:

Easy Deployment & Simple Operation



Anti-Virus Engine powered by AI---Sangfor Engine Zero

