YOUR SECURITY GUARD TO THE FUTURE

NGAF FIREWALL PLATFORM

Sangfor Technologies Co., Ltd.
www.sangfor.com
Table of Content

- **Security Trend**
  - New Business, New Challenges
  - Difficulties of O&M for Network Security
  - New Security Model

- SANGFOR Security Concept
- NGAF – Your Security Guard to the Future
Cyber Risks: The Growing Threat

- Hacking of Hong Kong's VTech may prove worst cybersecurity breach of 2015 in Asia!

- LinkedIn Lost 167 Million Account Credentials in Data Breach!

- Megabreach: 55 million voters' details leaked in Philippines!

- About 40 attacks reported in last two months (2016), but one security firm says it detected 24,000 cases of Locky ransomware hacking attempts in March alone!

Source 3: http://fortune.com/2016/05/18/linkedin-data-breach-email-password/
Source 4: http://www.theregister.co.uk/2016/04/07/philippine_voter_data_breach/
New World, New IT

Internet of Things

Estimated **200 billion objects** in 2020!

Source 2: IDC & Gartner
Source 3: RightScale’s Market Survey

BYOD

- Mobile Worker Population **1.3 million** in 2015
- Tablets forecasted to reach **468 million** in 2017
- Smartphones forecasted to reach **2.1 billion** in 2017

Cloud

93% of organizations are running applications or experimenting with infrastructure-as-a-service
• “By 2020, a third of successful attacks experienced by enterprises will be on their shadow IT resources.”
Source: Predicts 2016: Threat and Vulnerability Management, Gartner.

• If you really want to protect your network, you really have to know your network. You have to know the devices, the security technologies, and the things inside it.
Source: RSA Conference, Rob Joyce, NSA TAO Chief, Usenix Enigma 2016

Not even Superman is able to see through Networks to find threats!
What will happen without Real-Time Detection and Timely Response?

Average number of reported alerts received per week is 16,937 and only about 4% of them could be investigated.

Average 200 Days to detected Security breach and 80 Days to Contain it.

Average of 1.27 million US$ annually in time wasted

Source 1: Ponemon Institute study
Source 2: Ponemon Institute study
Source 3: Windows
Difficulties of O&M for Network Security

In average, an enterprise receives 16,937 alerts per week* !

*Source: Ponemon Institute Study of 630 enterprises

Without intelligent & automatic reporting tools, IT team has to read each report

IT team has to identify real & effective threats amongst thousands of alerts

After identifying the threat, due to lack of knowledge, IT team will waste time to find the right solution

Cost Calculation (Cost per Employee)

Time wasted per day: 4 hours
Average pay per day: US$ 60
Average wasted money per day: US$ 30
Average wasted money per month: US$ 600
Average wasted money per year: US$ 7200

Not including the risk of employees missing important threats and related cost + reputation damage !
Gartner estimates that 75% of attacks now take place at the application layer!

“90% of sites are vulnerable to application attacks”.

“Application security is no longer a choice”.

“Gartner continually hears from clients that are seeing a 90% firewall CPU utilization after they enabled Web or email antivirus on the same platform. This impacts the user experience, with noticeably increased latency and reduced throughput.”

Source 1: Watchfire
Source 2: OWASP
Source 3: Gartner, NGFW & UTM 2015 Report
Traditional Security Model is Outdated!

- No Visibility of Users, Traffic and IT Assets!
- No Real-Time Detection, No Post-Event Detection, Slow Response!
- Difficulties of O&M for Network Security, Time Wasted!
- Low Performance for L7 Application Layer Security!
Self-Adaptive Security Architecture

- Security is **more than just Defend**.
- Real-Time Detection at all phases to provide Real-time **Visibility**.
- **Fast Response and Automation** is the key to reduce Risks.

Source: Gartner
Table of Content

- Security Trend

- **SANGFOR Security Concept**
  - Security Visibility
  - Real-Time Detection, Rapid Response
  - Simple Security for O&M
  - L7 Security High Performance

- NGAF – Your Security Guard to the Future
SANGFOR Security Concept

Security Visibility
- Key Elements Visibility
- Intelligent Analyzing
- Management Visibility

Rapid Response
- Real-time Detection
  - Pre&Post-event detection
  - Business risks detection
- Rapid Response
  - Automatic policy enforcement
  - Solution synergy and Correlation
  - Security expertise as a service

Simplified Security
- Easy Deployment
  - Configuration wizard
- Simple O&M
  - Intuitive security reporting
  - Presented as security event
  - Convergence

L7 High-Performance
- Hardware and software architecture
- Efficient algorithm
Visibility is the Foundation

Many Invisible Security Risk in the Network

Users

- Normal users
- Lurked hackers
- Illegal users
- Normal users

Not only IP/Port/Signature Visibility, but also Users, Behaviors, Assets and their Correlation!

Behaviors

- Normal traffic
- New attack/abnormal traffic
- 0-day attack
- Attack using the new vuln.
- Attack in the normal traffic

- Normal traffic
- Info. stealing/abnormal behavior
- Traffic to C&C server
- Access to new domain
- Non-compliance information leakage
- DNS get packet

Assets

- ERP
- Website
- OA
- Supply Chain System
- Backdoor

Traffic through the Firewall are not all Safe!
Broader Visibility and Correlation Analysis

- More accurate defense and detection
- More efficient security O&M and risk management

Effective Analysis and Presentation

Broader Visibility

User Visibility
- ID
- End-points
- Access mode
- Location

Behavior Visibility
- Packet
- Traffic Log
- App
- Content

Business Visibility
- Location
- System Info
- Vuln.
- Data

Risk Positioning
Analysis of Data
Graphical Display

Behavior Visibility
User Visibility
Business Visibility
Real-Time Attack Detection Process

**Pre-Event Detection**
- Reconnoiter
- Port scan
- Vuln. scan
- Social Engineering
- Web attack
- App vuln. attack
- System vuln.
- Cache flushing
- 0-day
- Privilege escalation
- Get Permissions
- Script Modification

**Post-Event Detection**
- Web shell
- Malicious software
- Zombie Trojans
- Back door
- Crack Hash
- RDP
- Exploit
- Remote control
- Springboard attack
- Multi-hop attack
- Data Leak
- Data Destruction
- Clear traces

**Actions on Objectives**

**Weaponization**

**Delivery**

**Exploitation**

**Installation**

**Command and Control**

**Reconnaissance**
Rapid Response: Minimize the loss of security risk, reduce the risk of information assets theft!
Simple Security Operation

**Simplified Security**

**Easy Deployment**
- Configuration wizard
- Straightforward policy layout

**Simple O&M**
- Intuitive security reporting
- Presented as security event

**Convergence**

- Using wizard to make security deployment simply
- Policy layout: Easily to add rules to the system
- Before system online, check security real time, make sure the system has no vuln., no virus, etc.
- Present vuln. and risks by graphic.
- Security event push, automatic detect, automatic update DB, security advice.
- FW+IPS+AV+WAF integrated
L7 Security High Performance

• **Detection**: Signature, Behavior, Data Analyzing, Machine Learning & Modeling.

• **Software**: Parallel Processing & One-Time Detection.

• **Engine**: High-Performance Patented REGEX Engine.

• **Hardware**: Rich Compute Power.
Table of Content

- Security Trend
- SANGFOR Security Concept
- NGAF – Your Security Guard to the Future
### Key Elements Visibility

<table>
<thead>
<tr>
<th>No.</th>
<th>Target Server</th>
<th>Attack Type</th>
<th>Attack Count</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### LAN Server Groups

<table>
<thead>
<tr>
<th>Group</th>
<th>User Status</th>
<th>IP/Username</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default group</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom groups</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auto Identified Servers</td>
<td>1 users</td>
<td></td>
</tr>
</tbody>
</table>

### Abnormal Traffic

<table>
<thead>
<tr>
<th>No.</th>
<th>Host IP</th>
<th>Username</th>
<th>Group</th>
<th>Attack Count</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>200.200.9</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>33.0.80</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note:** The table and diagram illustrate the visibility of key elements in network security monitoring, showing detailed information about online users, server groups, and abnormal traffic.
Attack Status Visibility

C&C Communication
Host is infected with malware and controlled by hacker.

Data/Resource Discovery
Infected host scans for LAN servers, and attempts to launch brute-force attacks and SQL injection.

Infection
Hacker injects Trojan into websites and attempts to spread malware to infected hosts.

Bots Propagation
Infected host scans in LAN for other online hosts and services, exploits vulnerabilities on them and spreads the malware.

Data Disclosure
Sensitive data on server are successfully stolen by infected host and are about to be

Ever been attacked
Hacker exploits the vulnerability to constantly launch attacks against the server.

Data ever been harvested
Hacker uses tools, like Nmap, to search for a lot of data, such as server ports, services, etc.

Hacked
Server has been hacked, infected or defaced.
Attack Source Visibility

- Attack Source Distribution
- Top 5 Countries by Attacks: France - 298
- Top 50 Attack Sources:
  1. 2.2.1.1
  2. 3.2.1.2
  3. 4.2.2.3
  4. 5.2.3.4
  5. 6.2.4.5

Status: Security Status
---
Events | Attacks | Attacker Map | Bots | Data Leak | Backlink Injections | Outgoing DoS Attacks

Refresh: Last 7 days
User Traffic Visibility
Risk Visibility

Period: 2016-05-21 to 2016-05-26

Before Protection

Risk

2.2.1.1 server(2) has been Hacked

Recommendations:
Follow the security enhancement recommendations in the corresponding server security sections to fix the issues.

Total Attacks: Indicates the total number of attacks detected by the Sangfor NGAF that are against protected zones. The more the attacks, the worse the network security.

Attack Events: Indicates the major attack events extracted and categorized based on a variety of security logs and attack chain analysis techniques. The more the attack events, the more the attacks.

Vulnerabilities detected in specific protected zone fall into the following major types:

Vulnerability Type Distribution

- Apache Httpd Vulner.: (93.94%)
- IIS Vulnerability: (6.06%)

With Sangfor NGAF's protection, it has been proven to be effective in protecting against attacks.

Without protection, it would be worse.

Period: 04-27 to 04-29

Overall Security

Good

Backlink

2.2.1.1 has been Hacked

Attack

8473 attacks

Vuln

1 vulnerability which 1 is attacker

04-27 04-29
All Risk Real-Time Detection of Attack Process

Detection Technology

- Email AV
- Cloud AV (Multi-engine)
- Cloud sandbox
- Malicious trojan detection
- Attack feature detection
- Malicious link detection (auto)
- Trojan remote control detection
- Abnormal traffic detection
- Anomaly protocol on standard port detection
- LAN attack detection
- Internal scanning behavior detection
- Illegal access detection
- Password cracking behavior detection
- Virus transmission detection
- Real-time vuln. detection
- Web app vuln. detection
- Web attack detection
- Web shell detection
- Data leakage detection
- Backdoor using detection
- Ransomware detection
- Web page tampering detection
- Back link detection

Hundreds of Abnormal Behavior and Threat Detection Technologies
Real-Time Detection of Business System Vulnerabilities

Assets = Business  Threat = Attack  Vulnerability = Loophole

Real-time new vuln. alerts:
- SQL injection
- Cross site script
- …

NGAF
Proactive + Real-Time Scan

Code/system Update

Threats Recognition  Vuln. Recognition  Assets Recognition

Provide Active & Passive Vulnerability Detection, 7*24-hour Vulnerability Monitoring Service
Detection in Sandbox Environment:
- Process creation
- File system modifications
- Registry modification

1. Suspicious Traffic Reporting
2. Sandbox Detection is Performed
3. Generate Security Rules
4.1 Safety Rules Delivered
4.2 Cloud Sync Update

Unknown Threats Detection - Sangfor Cloud Sandbox
Rapid Response to New Threats

ImageMagick Exposed High-risk Vulnerability

Exploits: ImageMagick Remote Code Execution Vulnerability

Appeared Since: 2016-05-03

Update recommendations are as follows. Your device is in protection against the APT attack stated in this event.
Vulnerability Database Updated to 2016-05-06 [New threat can be prevented on 2016-05-05 version]

2 threats need immediate protection

1 IP addresses have been scanned, 2 threats need immediate protection

Protect Now
Add Web Application Protection Rule

**Protection**

- Website-based Attack: **Selected: SQL Injection, XSS Attack**
  - CSRF defense Settings
  - Restrictive URL access Settings
  - Cookie-based attack Settings

- Parameters:
  - Proactive protection Settings
  - Custom parameter protection Settings

- Application Hiding:
  - FTP Settings
  - HTTP Settings

- Password:
  - FTP Weak Password Protection Settings
  - Web-access weak password
  - Web-access cleartext request inspection
  - Defense against brute-force attack Settings

- Privilege:
  - File upload restriction Settings
  - URL access Settings

Save and Add

OK | Cancel
Automated Security Operation Guidance

131 threats need immediate action
Last Occurrence: 2015-10-16 17:00:40

Application Server Without Protection (2)

- WAF Rule Based Scan (1)
  1. IP addresses of 2 servers are allowed in Web application protection rule. Potential risk exists!

- IPS Rule Based Scan (1)
  1. No IPS rule is created.

Bots (96)

- 70.0.0.100: Infected with trojan.
- 202.0.194.223: Infected with trojan.
- 202.0.190.164: Infected with trojan.
- 202.0.197.194: Infected with trojan.
- 202.0.186.170: Infected with trojan.

More >>
Automated Security Operation Guidance

1. 200.200.88.93
1 webpages are injected with hidden link of Gambling.

More >>

Hidden Links(1)

1. IP addresses of 2 servers are Allowed in Web application protection rule. Potential risk exists!

Details

Zone: SSH
Port: HTTP (80)
Solution: 1. Edit the entry to Deny.
2. Edit the entry to unprotected zone.
3. Edit the entry to unprotected port.

IP Address:
70.0.0.100
200.200.88.93

Bots(96)

Impacts:
Worm, virus or Trojan infected hosts are controlled remotely by hackers to launch attacks like DoS attack and APT attack, aiming to destroy user network or critical application system and steal confidential data.

Solution:
1. Download, install and launch "Third-Party Anti-Malware Software" on bot-infected host to remove the bot worm.
2. Check the next week whether the bot worm still exists, for its capability of duplication and infection makes it not easy to be removed completely.

More >>
SANGFOR NGAF Hardware Architecture

- **Intel Quick Path Interconnect**
  - Wide bus bandwidth
  - High computing capacity

- **Multi-Core Level Processing**
  - Up to 2.5GHz
  - Up to 126 cores

- **Hybrid Processing Model**
  - Fragmentated processing
  - One module can use all power
SANGFOR NGAF Software Architecture

One Content Detection Engine

- WAF DB
- IPS DB
- AV DB

Data Forwarding Plane

- One Time Data Replication

Data Replication

- Decapsulation
- Detection
- Regex Engine

1x

Low latency
High throughput
Good flexibility
High performance
New Business Environment Drives New Security Model!

- **Real Time Security Visibility** is the foundation of modern security.

- **Fast response** to security events is crucial.

- Security **operation simplification** becomes part of security requirements.

- **Application layer Security** capability is what new security cares about.
Thank you!

Global Service Center:
+60 12711 7129 (7511)

sales@sangfor.com
marketing@sangfor.com