NEXT GENERATION APPLICATION FIREWALL

Strengthening the Application-Layer Security of your Network

Current Security Status

- Traditional firewall or UTM are the main security appliance to the whole network including the datacenter.
- Implement the traditional firewall/UTM is the first step of the security construction.
- The security is facing more challenges because the business is becoming opener, the attacks are becoming more complex.
- It need to be strengthened to improve the capability to protect the security of the whole network.

Challenges faced by UTM

UTM is the core security appliance in the network. According to Gartner Research, 75% of the attacks are happening at the application layer, however UTM is weak in term of protection for the application layer attacks because of performance issue.

As mentioned by the RSA, computer security has failed to protect us. The defense-based strategy that’s been in place for many years isn’t working anymore.

New & emerging threats such as 0day attacks, APT, malware, can bypass the traditional security appliance to make the security defense useless.

The border defense provided by UTM & traditional firewall is mainly based on the static signature and only works on the protection from the outside to the inside. However, if the attacks bypass the security appliance, and threats successfully infect the network, it cannot do anything to further protect it.

Complex Business makes it difficult to do Security Management

Businesses are growing at a fast rate but at the same time, are becoming more complex to manage, especially security management. How to know the accurate security status of the whole network? How to immediately detect threats? How to face the challenge lead by the rapid business deployment? How to dispose of the risks simply and effectively?
These are the key problems of the new Security:

- Lack of comprehensive security perspective.
- Organizations do not have enough technical tools and lack of integrated security visibility tools.
- Cannot do a comprehensive security management, organizations can only see a small part of the problem.
- Security management is too complex.
- Businesses are deployed more rapidly, thus there are higher requirement to do the policy management and risk management.
- Security management is too complex to fulfill the business requirement of the security.
- Lack of capability to solve the problem.
- The threats in the network cannot be detected in time.
- Need more professional skills and tools to detect the threat and dispose of it immediately.

Strengthening the Application-Layer Security of your Network

Sangfor application-layer security strengthening solution is the complement of the current network security solution. It’s aimed to remove threats which cannot be done by the traditional firewall or UTM. It greatly reduces the risk produced by a lack of comprehensive security defense and detection.

- **Application-layer security strengthen**
  - Fix the weakness of the border defense, increase the cost & time spent by the hacker.
  - Vulnerabilities protections against web attack, virus, Trojan and botnets.

- **Improve threat detection technology**
  - Provide the detection of threats that bypass the border defense, and present it as a security event.
  - Security event as presented such as attacked host, abnormal behavior, defaced event, black link.

- **Simplified security management**
  - Simplify the security management of the network security team.
  - Easy & convenient tools such as Security reporting, real time threat detection, simple O&M, SECaaS.
Converged Architecture to Fulfill High Security Requirements

SANGFOR NGAF is integrated with NGFW, IPS, AV and WAF. It provides more security protection with bi-direction traffic analyzing in network layer, application layer and content. It can defend against application layer attacks, which have more sources, more power and can do more harm. This architecture will strengthen all layers from L2-L7 security of the entire network.

Powerful & Most Complete APAC Security Database

As an Asian based vendor, Sangfor has one of the strongest and most complete security database for the APAC market. The security database of NGAF is incorporated with the local information of each country, which can best detect and defend against the threats present in Asia. Sangfor NGAF is also a good complement for traditional firewall or UTM coming from Europe/US vendors.
High Compatibility for Integration with Third-Party Firewall

NGAF can be deployed as a second-tier firewall to any other vendor’s. It’s high compatibility makes sure that it can fully cooperate with other brands firewall. With its Asian based security database, application-layer security, and complete security report suite, Sangfor NGAF can be a good complement to the first layer firewall. It’s been already deployed in hundreds of Asian organizations as an extra layer of security.

Visualize Security, Make the Security O&M Simpler!

With Sangfor NGAF’s protection, overall security rating is raised to Excellent. Without protection, it may suffer the following attacks:

- **ImageMagick Exposed High-risk Vulnerability**
  - Exploits: ImageMagick Remote Code Execution Vulnerability
  - Appeared Since: 2016-02-03
  - 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]

- **131 threats need immediate action**
  - Last Occurrence: 2019-11-16 17:00:43

- **Application Server Without Protection**
  - WAF Rule Based Scan (1)
    - 1 IP addresses of 2 servers are allowed in web application protection rule. Potential risk exists!
  - IPM Rule Based Scan (1)
    - No IPM rule is created.

- **Bot List (9)**
  - Infected with Trojan:
    - 192.168.1.100
    - 192.168.1.223
    - 192.168.1.184
    - 192.168.1.194
    - 192.168.1.170
    - More >>
Transform your Network Security with Sangfor NGAF to Protect your Investment

NGAF is a high converged security platform. It can be used as a secure gateway, a traditional firewall, a UTM, a WAF, even as an assessment tool. The user can transform the deployment mode easily.

Our Notable Customers

---

www.sangfor.com
Sangfor Technologies

---

Sangfor NGAF - Next Generation Firewall + WAF
- Full Visibility of the Network Security
- Real-Time Detection & Fast Response
- Simple Operation & Maintenance
- High-Performance Hardware/Software