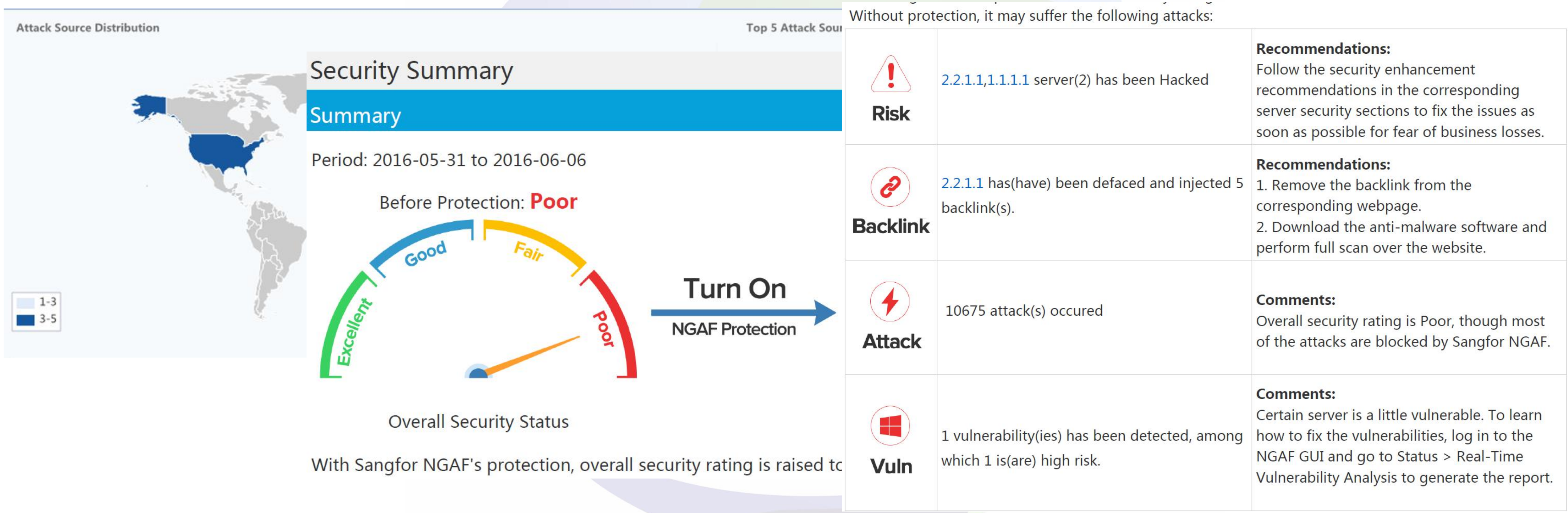
SANGFOR

Sangfor NGAF v8.0.6 Associate

Report Center

NGAF Report Center

NGAF Report Center provides a list of comprehensive logs on network security incidents and security events in the form of reports to convey to users the current Internet security status and recommended solutions to various risks detected.



Security Summary

Summary

Period: 2016-05-31 to 2016-06-06

Before Protection: Poor

Overall Security Status

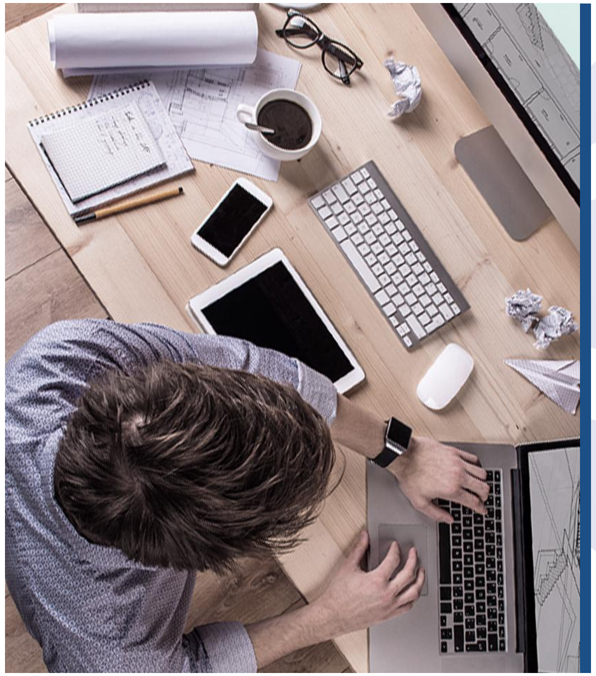
With Sangfor NGAF's protection, overall security rating is raised tc

Turn On

NGAF Protection

Without protection, it may suffer the following attacks:

Risk	2.2.1.1,1.1.1.1 server(2) has been Hacked	**Recommendations:** Follow the security enhancement recommendations in the corresponding server security sections to fix the issues as soon as possible for fear of business losses.
Backlink	2.2.1.1 has(have) been defaced and injected 5 backlink(s).	**Recommendations:** 1. Remove the backlink from the corresponding webpage. 2. Download the anti-malware software and perform full scan over the website.
Attack	10675 attack(s) occured	**Comments:** Overall security rating is Poor, though most of the attacks are blocked by Sangfor NGAF.
Vuln	1 vulnerability(ies) has been detected, among which 1 is(are) high risk.	**Comments:** Certain server is a little vulnerable. To learn how to fix the vulnerabilities, log in to the NGAF GUI and go to Status > Real-Time Vulnerability Analysis to generate the report.



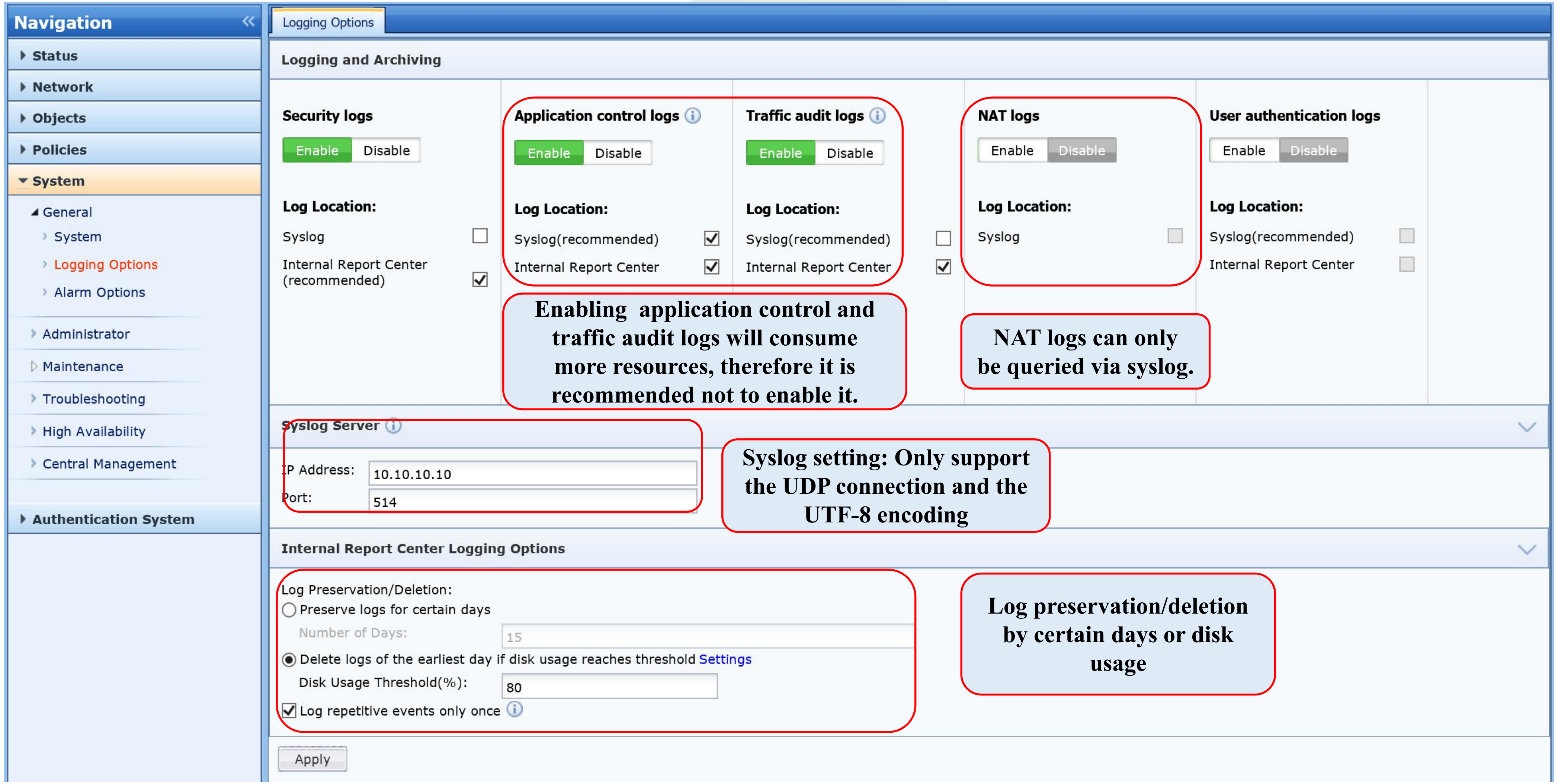
1 Logging Option

2 Syslog

3 Internal Report Center

1. Logging Option

Logging Options



Logging and Archiving

Security logs
[✓ Enable] Disable

Log Location:
Syslog □
Internal Report Center (recommended) ☑

Application control logs
[✓ Enable] Disable

Log Location:
Syslog(recommended) ☑
Internal Report Center ☑

Traffic audit logs
[✓ Enable] Disable

Log Location:
Syslog(recommended) □
Internal Report Center ☑

NAT logs
Enable [✓ Disable]

Log Location:
Syslog □

User authentication logs
Enable [✓ Disable]

Log Location:
Syslog(recommended) □
Internal Report Center □

Enabling application control and traffic audit logs will consume more resources, therefore it is recommended not to enable it.

NAT logs can only be queried via syslog.

Syslog Server

IP Address: 10.10.10.10
Port: 514

Syslog setting: Only support the UDP connection and the UTF-8 encoding

Internal Report Center Logging Options

Log Preservation/Deletion:
○ Preserve logs for certain days
Number of Days: 15
● Delete logs of the earliest day if disk usage reaches threshold Settings
Disk Usage Threshold(%): 80
☑ Log repetitive events only once

Log preservation/deletion by certain days or disk usage

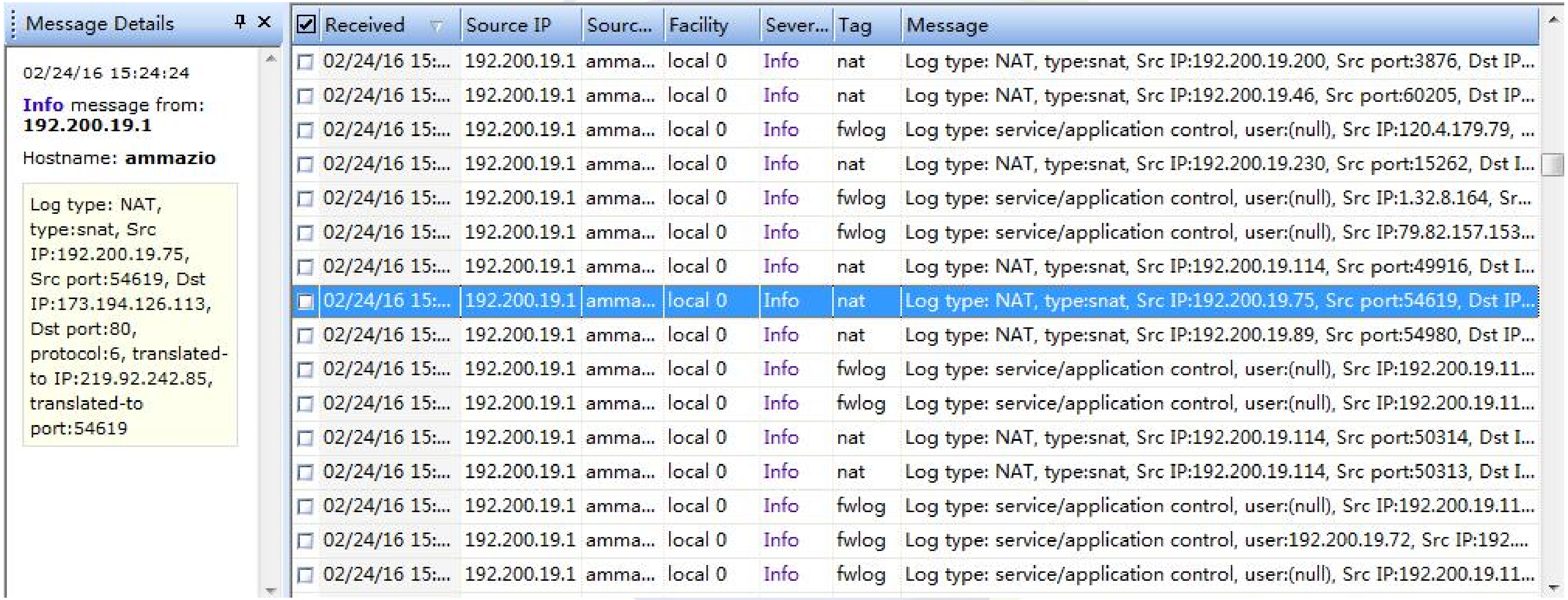
Apply

2. Syslog

SANGFOR
深信服科技

Syslog

Security logs, traffic logs, NAT logs, authentication logs can be sent to syslog server via UDP connection.



Message Details

02/24/16 15:24:24

Info message from:
192.200.19.1

Hostname: **ammazio**

Log type: NAT, type:snat, Src IP:192.200.19.75, Src port:54619, Dst IP:173.194.126.113, Dst port:80, protocol:6, translated-to IP:219.92.242.85, translated-to port:54619

☑	Received	Source IP	Sourc...	Facility	Sever...	Tag	Message
□	02/24/16 15:...	192.200.19.1	amma...	local 0	Info	nat	Log type: NAT, type:snat, Src IP:192.200.19.200, Src port:3876, Dst IP...
□	02/24/16 15:...	192.200.19.1	amma...	local 0	Info	nat	Log type: NAT, type:snat, Src IP:192.200.19.46, Src port:60205, Dst IP...
□	02/24/16 15:...	192.200.19.1	amma...	local 0	Info	fwlog	Log type: service/application control, user:(null), Src IP:120.4.179.79, ...
□	02/24/16 15:...	192.200.19.1	amma...	local 0	Info	nat	Log type: NAT, type:snat, Src IP:192.200.19.230, Src port:15262, Dst I...
□	02/24/16 15:...	192.200.19.1	amma...	local 0	Info	fwlog	Log type: service/application control, user:(null), Src IP:1.32.8.164, Sr...
□	02/24/16 15:...	192.200.19.1	amma...	local 0	Info	fwlog	Log type: service/application control, user:(null), Src IP:79.82.157.153...
□	02/24/16 15:...	192.200.19.1	amma...	local 0	Info	nat	Log type: NAT, type:snat, Src IP:192.200.19.114, Src port:49916, Dst I...
□	02/24/16 15:...	192.200.19.1	amma...	local 0	Info	nat	Log type: NAT, type:snat, Src IP:192.200.19.75, Src port:54619, Dst IP...
□	02/24/16 15:...	192.200.19.1	amma...	local 0	Info	nat	Log type: NAT, type:snat, Src IP:192.200.19.89, Src port:54980, Dst IP...
□	02/24/16 15:...	192.200.19.1	amma...	local 0	Info	fwlog	Log type: service/application control, user:(null), Src IP:192.200.19.11...
□	02/24/16 15:...	192.200.19.1	amma...	local 0	Info	fwlog	Log type: service/application control, user:(null), Src IP:192.200.19.11...
□	02/24/16 15:...	192.200.19.1	amma...	local 0	Info	nat	Log type: NAT, type:snat, Src IP:192.200.19.114, Src port:50314, Dst I...
□	02/24/16 15:...	192.200.19.1	amma...	local 0	Info	nat	Log type: NAT, type:snat, Src IP:192.200.19.114, Src port:50313, Dst I...
□	02/24/16 15:...	192.200.19.1	amma...	local 0	Info	fwlog	Log type: service/application control, user:(null), Src IP:192.200.19.11...
□	02/24/16 15:...	192.200.19.1	amma...	local 0	Info	fwlog	Log type: service/application control, user:192.200.19.72, Src IP:192....
□	02/24/16 15:...	192.200.19.1	amma...	local 0	Info	fwlog	Log type: service/application control, user:(null), Src IP:192.200.19.11...

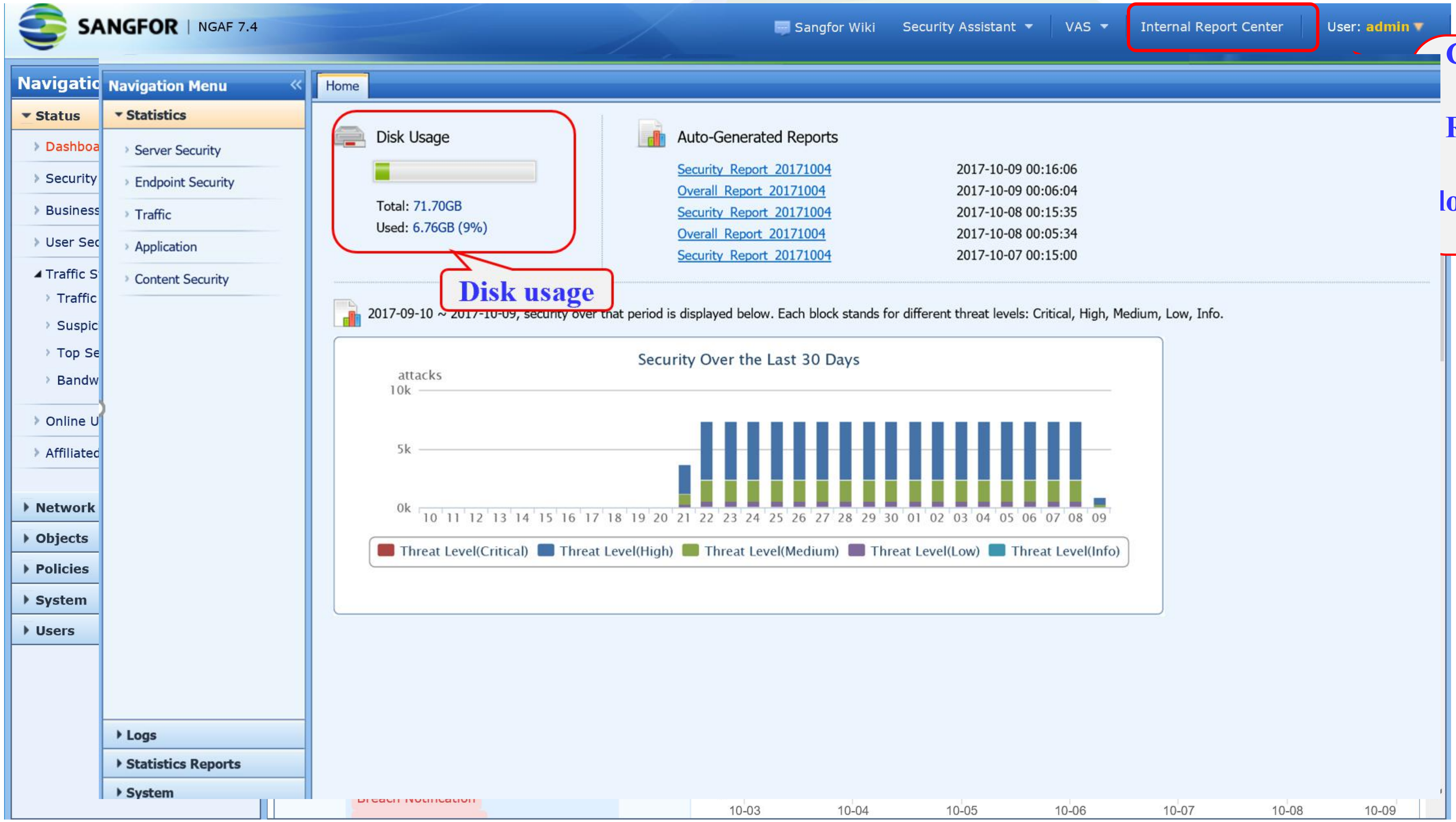
System log are not synchronized to syslog server.

3. Internal Report Center

SANGFOR
深信服科技

Internal Report Center

How to browse into Internal Report Center?



Disk Usage

Total: 71.70GB
Used: 6.76GB (9%)

Auto-Generated Reports

Security_Report_20171004	2017-10-09 00:16:06
Overall_Report_20171004	2017-10-09 00:06:04
Security_Report_20171004	2017-10-08 00:15:35
Overall_Report_20171004	2017-10-08 00:05:34
Security_Report_20171004	2017-10-07 00:15:00

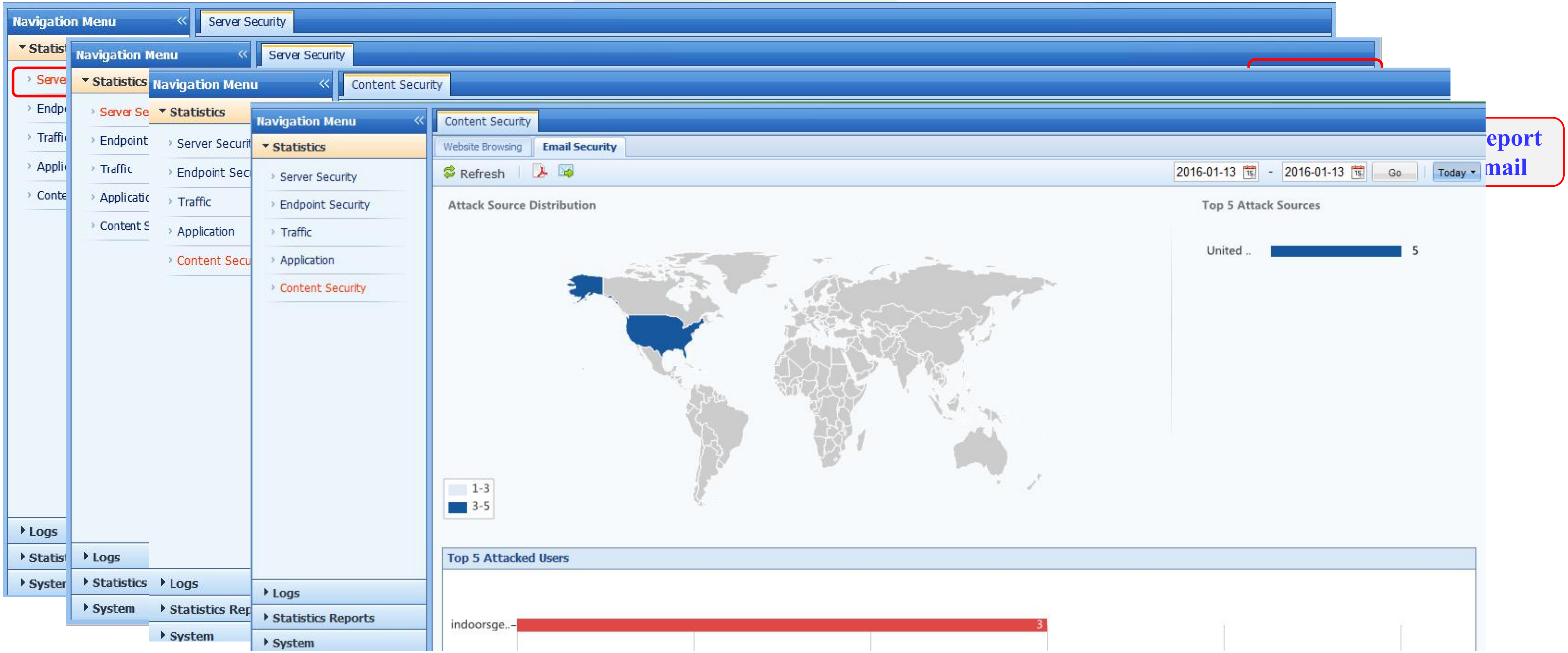
2017-09-10 ~ 2017-10-09, security over that period is displayed below. Each block stands for different threat levels: Critical, High, Medium, Low, Info.

Disk usage

Click here for a quick login to Internal Report Center or surf http://x.x.x.x:85 to login(x.x.x.x represents NGAF IP address)

Internal Report Center

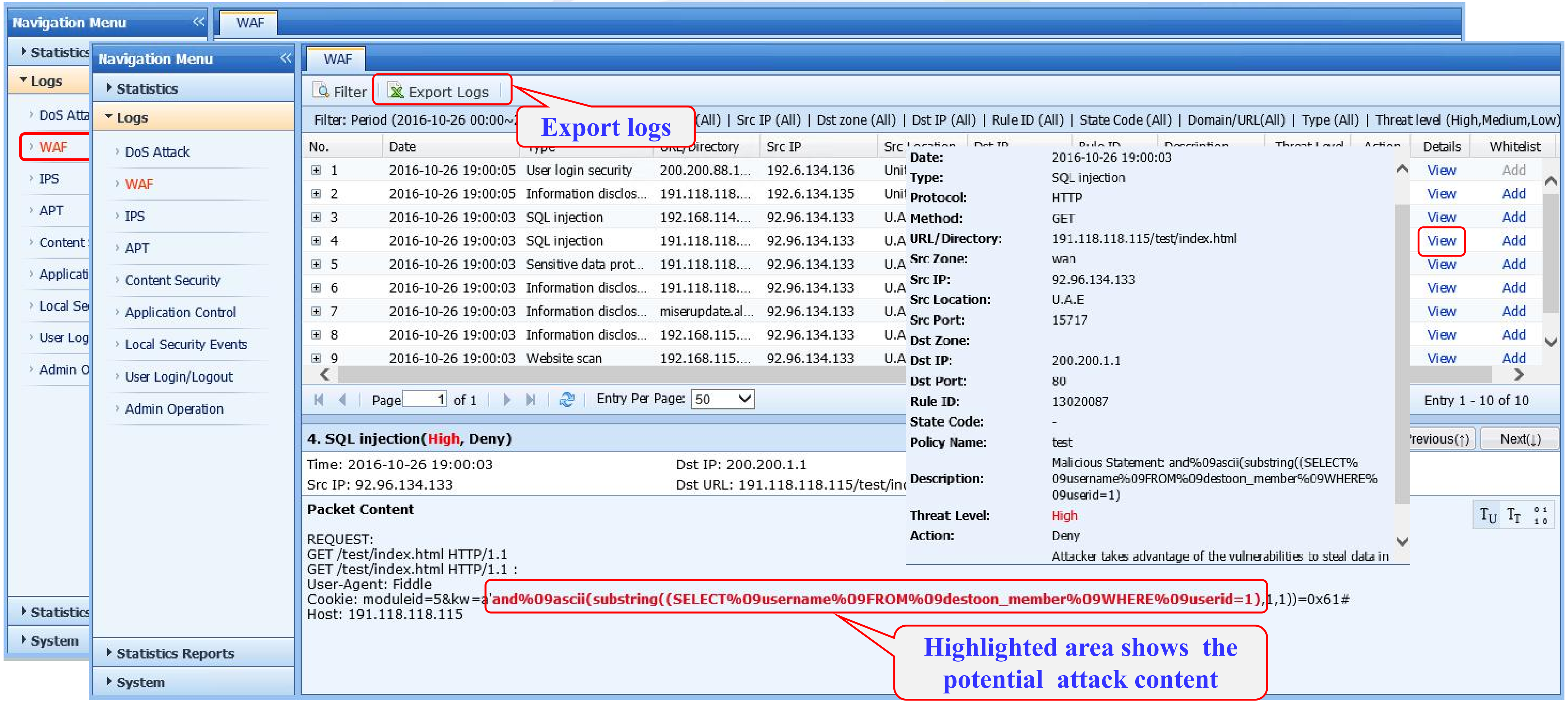
Statistics:



Internal Report Center

Logs: Enable users to view log details.

We take WAF log for instance:



Export logs

Filter: Period (2016-10-26 00:00~2 … (All) | Src IP (All) | Dst zone (All) | Dst IP (All) | Rule ID (All) | State Code (All) | Domain/URL(All) | Type (All) | Threat level (High,Medium,Low)

No.	Date	Type	URL/Directory	Src IP	Src Location	Details	Whitelist
⊞ 1	2016-10-26 19:00:05	User login security	200.200.88.1...	192.6.134.136	Unit	View	Add
⊞ 2	2016-10-26 19:00:05	Information disclos...	191.118.118....	192.6.134.135	Unit	View	Add
⊞ 3	2016-10-26 19:00:03	SQL injection	192.168.114....	92.96.134.133	U.A	View	Add
⊞ 4	2016-10-26 19:00:03	SQL injection	191.118.118....	92.96.134.133	U.A	View	Add
⊞ 5	2016-10-26 19:00:03	Sensitive data prot...	191.118.118....	92.96.134.133	U.A	View	Add
⊞ 6	2016-10-26 19:00:03	Information disclos...	191.118.118....	92.96.134.133	U.A	View	Add
⊞ 7	2016-10-26 19:00:03	Information disclos...	miserupdate.al...	92.96.134.133	U.A	View	Add
⊞ 8	2016-10-26 19:00:03	Information disclos...	192.168.115....	92.96.134.133	U.A	View	Add
⊞ 9	2016-10-26 19:00:03	Website scan	192.168.115....	92.96.134.133	U.A	View	Add

Page 1 of 1 | Entry Per Page: 50 | Entry 1 - 10 of 10

Date:	2016-10-26 19:00:03
Type:	SQL injection
Protocol:	HTTP
Method:	GET
URL/Directory:	191.118.118.115/test/index.html
Src Zone:	wan
Src IP:	92.96.134.133
Src Location:	U.A.E
Src Port:	15717
Dst Zone:	
Dst IP:	200.200.1.1
Dst Port:	80
Rule ID:	13020087
State Code:	-
Policy Name:	test
Description:	Malicious Statement: and%09ascii(substring((SELECT%09username%09FROM%09destoon_member%09WHERE%09userid=1)
Threat Level:	High
Action:	Deny
	Attacker takes advantage of the vulnerabilities to steal data in

4. SQL injection(High, Deny)

Time: 2016-10-26 19:00:03　Dst IP: 200.200.1.1

Src IP: 92.96.134.133　Dst URL: 191.118.118.115/test/in

Previous(↑)　Next(↓)

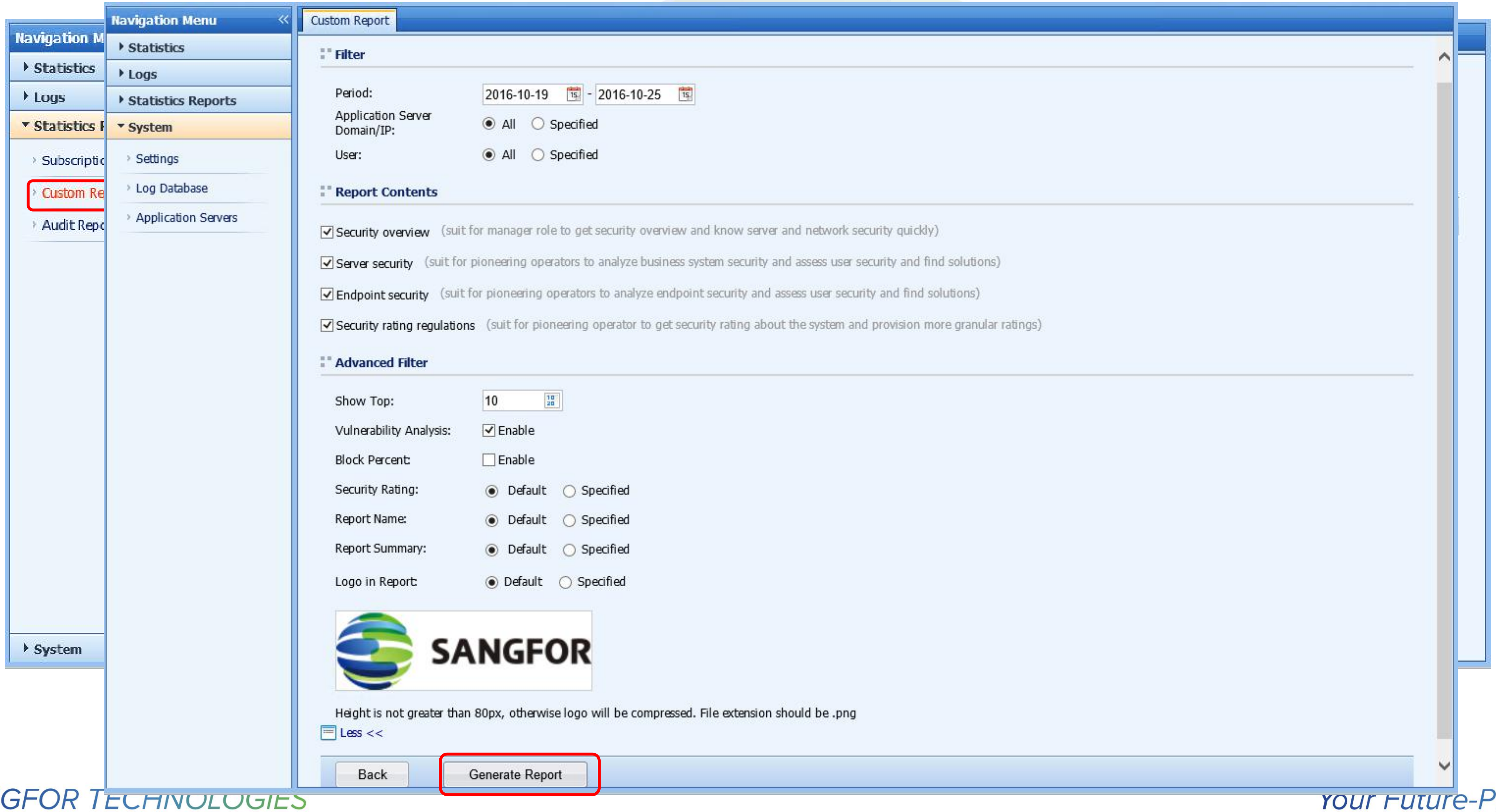
Packet Content

```
REQUEST:
GET /test/index.html HTTP/1.1
GET /test/index.html HTTP/1.1 :
User-Agent: Fiddle
Cookie: moduleid=5&kw=a'and%09ascii(substring((SELECT%09username%09FROM%09destoon_member%09WHERE%09userid=1),1,1))=0x61#
Host: 191.118.118.115
```

Highlighted area shows the potential attack content

Internal Report Center

Statistics Report:



Filter

Period: 2016-10-19 - 2016-10-25

Application Server Domain/IP: ● All ○ Specified

User: ● All ○ Specified

Report Contents

☑ Security overview (suit for manager role to get security overview and know server and network security quickly)

☑ Server security (suit for pioneering operators to analyze business system security and assess user security and find solutions)

☑ Endpoint security (suit for pioneering operators to analyze endpoint security and assess user security and find solutions)

☑ Security rating regulations (suit for pioneering operator to get security rating about the system and provision more granular ratings)

Advanced Filter

Show Top: 10

Vulnerability Analysis: ☑ Enable

Block Percent: □ Enable

Security Rating: ● Default ○ Specified

Report Name: ● Default ○ Specified

Report Summary: ● Default ○ Specified

Logo in Report: ● Default ○ Specified

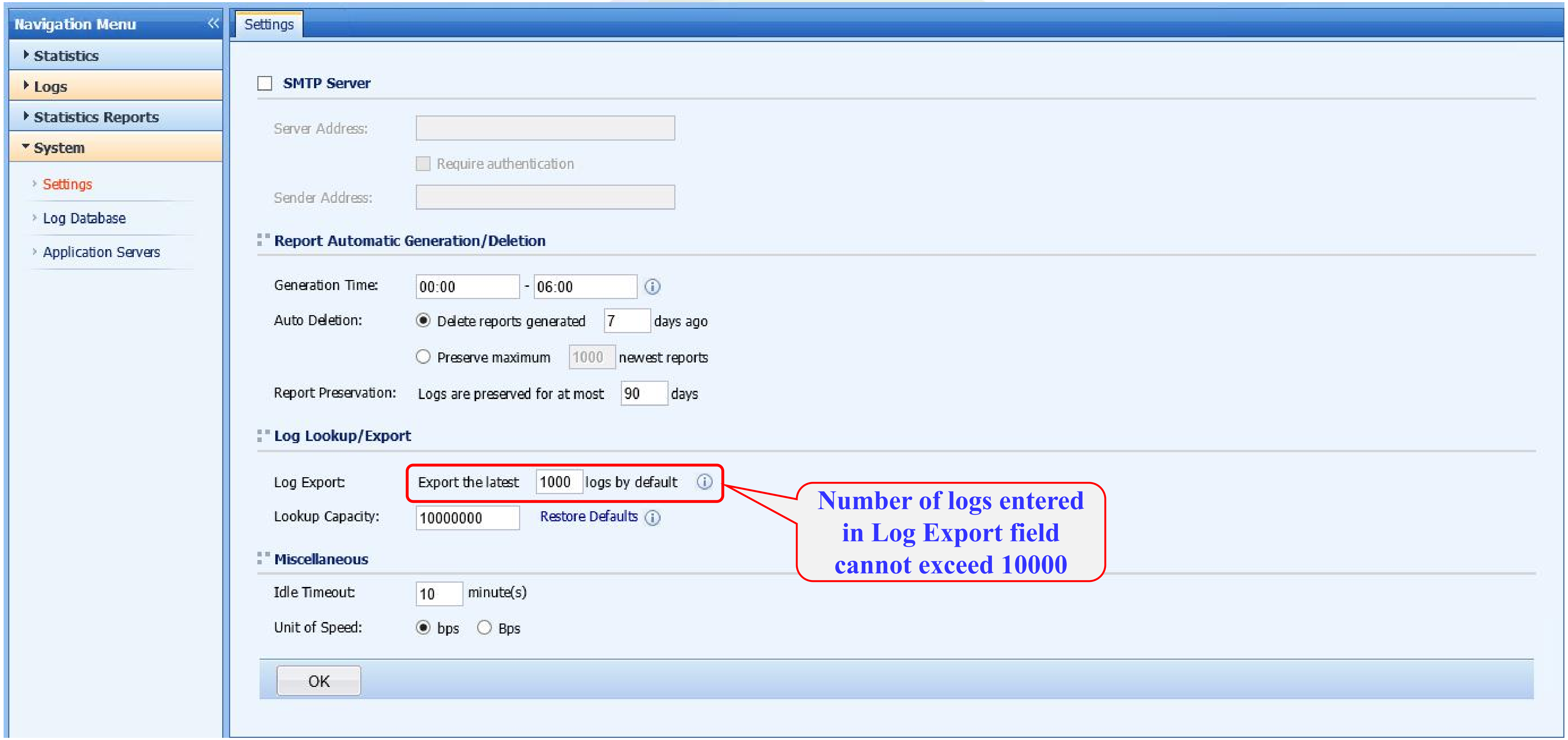
SANGFOR

Height is not greater than 80px, otherwise logo will be compressed. File extension should be .png

Less <<

Internal Report Center

Internal Report Center settings:



☐ SMTP Server

Server Address:

☐ Require authentication

Sender Address:

Report Automatic Generation/Deletion

Generation Time: 00:00 - 06:00 ⓘ

Auto Deletion: ● Delete reports generated 7 days ago

○ Preserve maximum 1000 newest reports

Report Preservation: Logs are preserved for at most 90 days

Log Lookup/Export

Log Export: Export the latest 1000 logs by default ⓘ

Lookup Capacity: 10000000 Restore Defaults ⓘ

Miscellaneous

Idle Timeout: 10 minute(s)

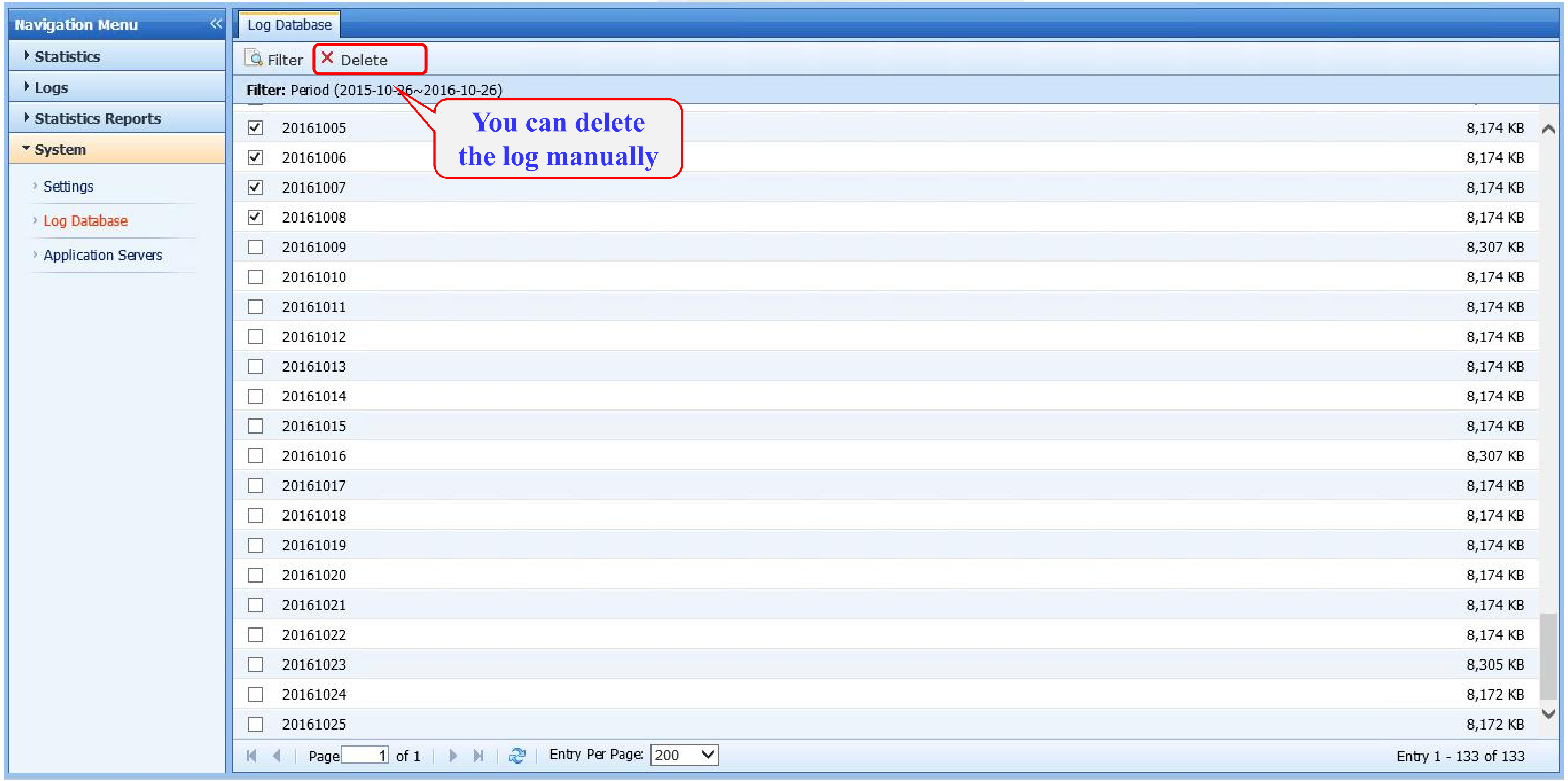
Unit of Speed: ● bps ○ Bps

OK

Number of logs entered in Log Export field cannot exceed 10000

Internal Report Center

Log databases



Filter: Period (2015-10-26~2016-10-26)

You can delete the log manually

☑	20161005	8,174 KB
☑	20161006	8,174 KB
☑	20161007	8,174 KB
☑	20161008	8,174 KB
□	20161009	8,307 KB
□	20161010	8,174 KB
□	20161011	8,174 KB
□	20161012	8,174 KB
□	20161013	8,174 KB
□	20161014	8,174 KB
□	20161015	8,174 KB
□	20161016	8,307 KB
□	20161017	8,174 KB
□	20161018	8,174 KB
□	20161019	8,174 KB
□	20161020	8,174 KB
□	20161021	8,174 KB
□	20161022	8,174 KB
□	20161023	8,305 KB
□	20161024	8,172 KB
□	20161025	8,172 KB

Page 1 of 1 Entry Per Page: 200 Entry 1 - 133 of 133

Thank you !

tech.support@sangfor.com
community.sangfor.com

Sangfor Technologies (Headquarters)
Block A1, Nanshan iPark, No.1001
Xueyuan Road, Nanshan District,
Shenzhen, Guangdong Province,
P. R. China (518055)