

3. Monitor



SANGFOR
深信服科技

Monitor



Logs : Web App Protection, Intrusion Prevention, Botnet, Website Browsing, Email Protection

a1 Protection Logs

Filter | Export Logs | Refresh

Filter: Time (2020-12-01 00:00 - 2020-12-31 23:59) | Type (Web App Firewall) | Src Zone (All) | Source Address (All) | Dst Zone (All) | Destination (All) | Threat Level (Severe, High, Medium, Low)

No.	Time	Type	Attack Type	Src IP	Src IP Location	Dst IP/URL
1	2020-12-29 22:51:36	Web App Firewall	SQL injection	192.200.19.4	U.A.E	172.16.10.110
2	2020-12-29 22:50:25	Web App Firewall	SQL injection	192.200.19.4	U.A.E	172.16.10.110
3	2020-12-29 22:49:22	Web App Firewall	SQL injection	192.200.19.4	U.A.E	172.16.10.110
4	2020-12-29 22:41:36	Web App Firewall	SQL injection	192.200.19.4	U.A.E	172.16.10.110
5	2020-12-24 00:00:04	Web App Firewall	XSS attack	202.0.0.68	Australia	192.168.254.59
6	2020-12-24 00:00:04	Web App Firewall	XSS attack	202.0.0.141	Australia	192.168.254.18
7	2020-12-24 00:00:04	Web App Firewall	XSS attack	202.0.0.221	Australia	192.168.254.17
8	2020-12-24 00:00:04	Web App Firewall	XSS attack	202.0.1.105	Australia	192.168.254.37
9	2020-12-24 00:00:04	Web App Firewall	XSS attack	202.0.0.157	Australia	192.168.254.63
10	2020-12-24 00:00:04	Web App Firewall	XSS attack	202.0.0.28	Australia	192.168.254.69
11	2020-12-24 00:00:04	Web App Firewall	XSS attack	202.0.1.16	Australia	192.168.254.48
12	2020-12-24 00:00:04	Web App Firewall	XSS attack	202.0.1.64	Australia	192.168.254.5
13	2020-12-24 00:00:04	Web App Firewall	XSS attack	202.0.1.46	Australia	192.168.254.8
14	2020-12-24 00:00:04	Web App Firewall	XSS attack	202.0.0.197	Australia	192.168.254.80
15	2020-12-24 00:00:04	Web App Firewall	XSS attack	202.0.1.50	Australia	192.168.254.47
16	2020-12-24 00:00:04	Web App Firewall	XSS attack	202.0.0.142	Australia	192.168.254.89
17	2020-12-24 00:00:04	Web App Firewall	XSS attack	202.0.0.143	Australia	192.168.254.17
18	2020-12-30 00:00:02	Anti-DDoS/DDoS	ICMPv6 flooding attack	202.0.0.28	Australia	192.168.254.181

Exclude
Page: 1 Previous Next

Source

Src Zone: WAN

Src IP: 192.200.19.4

Src IP Location: U.A.E

Src Port: 62446

XFF IP: -

Destination

Dst Zone: LAN

Dst IP: 172.16.10.110

Dst IP Location: -

Dst Port: 80

Basics
Data Packet

TU Tt 01 10

INCLUDE ENCODING TYPE: URL
 REQUEST:
 GET /dashboard/?id=and 1=1 HTTP/1.1
 Host: 192.200.19.55
 Connection: keep-alive
 Upgrade-Insecure-Requests: 1
 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.664.66 Safari/537.36 Edg/87.0.664.66
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
 Accept-Encoding: gzip, deflate
 Accept-Language: en-US,en;q=0.9
 Cookie: _ga=GA1.4.1621054562.1607929421; indexCssModule=true; dependsModule=true; languageModule=true; commonModule=true; PHPSESSID=hqt03e9hmako183arpkcmnon4

Highlighted area shows the potential attack content

Monitor



Logs :

Application Control Logs that enables users to view the logs generated in Access Control > Application Control P

Monitor

Application Control Logs | User Login/Logout Logs | SSL VPN Logs

Q Filter | **Export Logs** | Refresh

Filter: Period (2020-12-29 00:00 -) | Src IP/User (All) | Dst zone (All) | Dst IP (All) | Service/application (All) | Action (Allow, Deny, Deny)

Matched Policy | Action | Operation | ...

Application Control Logs | User Login/Logout Logs | **SSL VPN Logs**

Q Filter | **Export Logs** | Refresh

Filter: Period (2020-12-29 00:00 -)

No.	Username	Time	Behavior	IP Address	Description	Operation
1	User1	2020-12-29 12:27:43	Log out	192.168.19.71		View
2	User1	2020-12-29 11:57:29	Assign virtual IP	192.168.19.71		View
3	User1	2020-12-29 11:57:24	Log in	192.168.19.71		View
4	User1	2020-12-29 11:46:47	Log out	192.168.19.71		View
5	User1	2020-12-29 11:45:44	Log in	192.168.19.71		View

No.1

Username: User1

Time: 2020-12-29 12:27:43

Behavior: Log out

IP Address: 192.168.19.71

Description: Log out successfully!

Allow all | Allow | [View](#)

Allow all | Allow | [View](#)

Allow all | Allow | [View](#)

Total: 743 < 1 > Entries Per Page 50

Monitor



Logs :

Admin Operation Logs enables users to view the logs generated throughout the process whereby a user logs in to the system.

Monitor

Logs

- Security Logs
- Access Logs
- System Logs**
- Sessions
- Statistics
- Report
- Settings

Admin Operation Logs | System Security Logs | Local ACL Logs

Filter: Period (2020-12-29 00:00 - 2020-12-29 23:59) | Account Type (All) | Management Method (All) | Object (All) | Description (-)

Export logs

No.	Admin	Account Type	Management Method	Host IP	Object	Operation	Time	Description	Details	...
No.1	admin	LOCAL	webui	192.200.19.4	Export security report	Export report	2020-12-29 22:44:51	Export report as PDF successfully.	View	
							2020-12-29 14:48:40	Turn on global packet passthrough/analysis ...	View	
							2020-12-29 14:42:02	IPv4 routesGet resultsSuccess	View	
							2020-12-29 14:41:31	IPv4 routesGet resultsSuccess	View	
							2020-12-29 14:40:43	Translate IPv4 addresses to IPv4 addresses...	View	
							2020-12-29 14:38:43	Translate IPv4 addresses to IPv4 addresses...	View	
							2020-12-29 14:38:07	admin(local) 192.200.19.4 logged in success...	View	

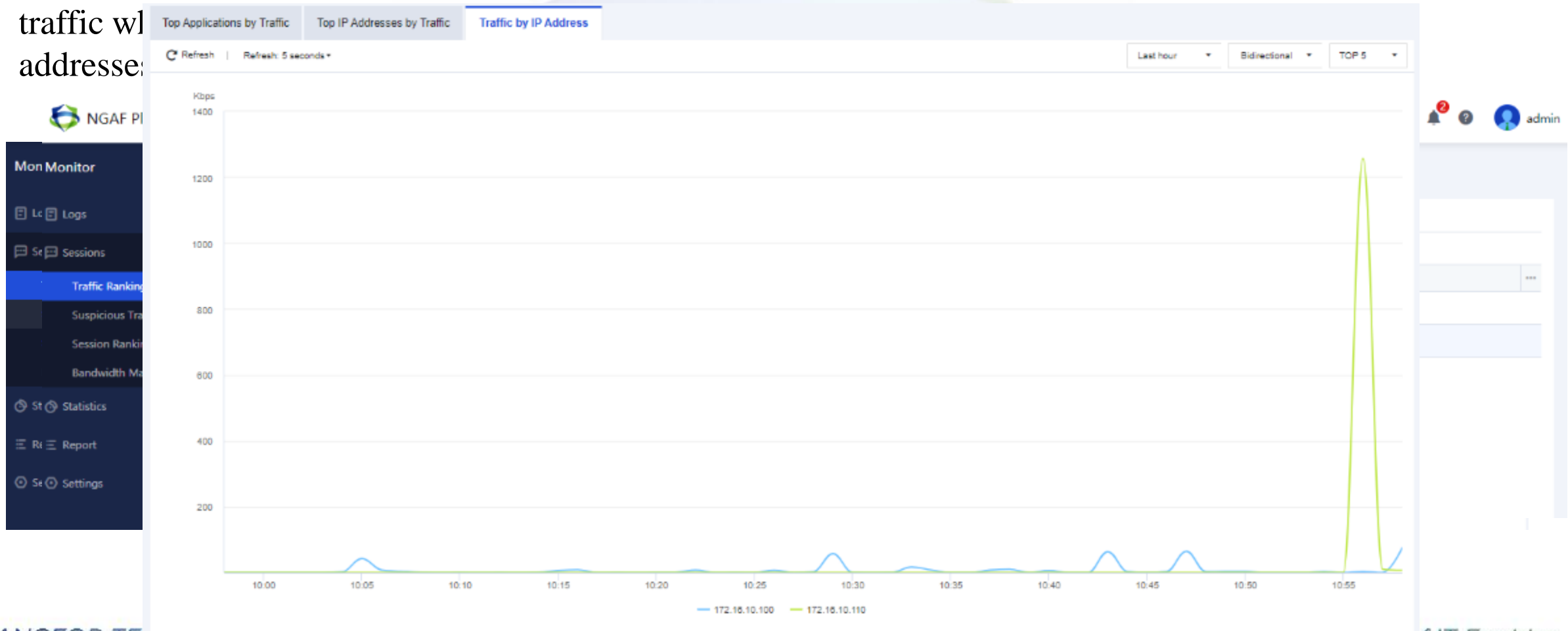
Total: 33 | Entries Per Page: 50

Monitor



Sessions:

Traffic ranking enables users to collect statistics on the Internet access traffic of intranet users by application, IP address, etc. There are 4 modules which allow users to check for different traffic with different IP addresses:



Monitor



Sessions:

In **suspicious traffic** it enables users to check about the LAN hosts and server that have suspicious outgoing traffic.

Suspicious Traffic

Protection Logs

Filter

Export Logs

Refresh

IP, domain

Filter: Time (2021-07-11 18:52 - 2021-07-11 18:53) | Type (Botnet) | Src Zone (All) | Src Address (IP: 192.168.1.110) | Dst Zone (All) | Dst Address (192.200.19.20) | Threat Level (Severe, High, Medium, Low, Info)..|

No.	Time	Type	Attack Type	Src Address	Src IP Location	Dst Address	Dst IP Location	Threat Level	Action	Operation	...
1	2021-07-11 18:52:08	Botnet	Abnormal Conn...	192.168.1.110	-	192.200.19.20	U.A.E	Low	Allow	View	More ▾

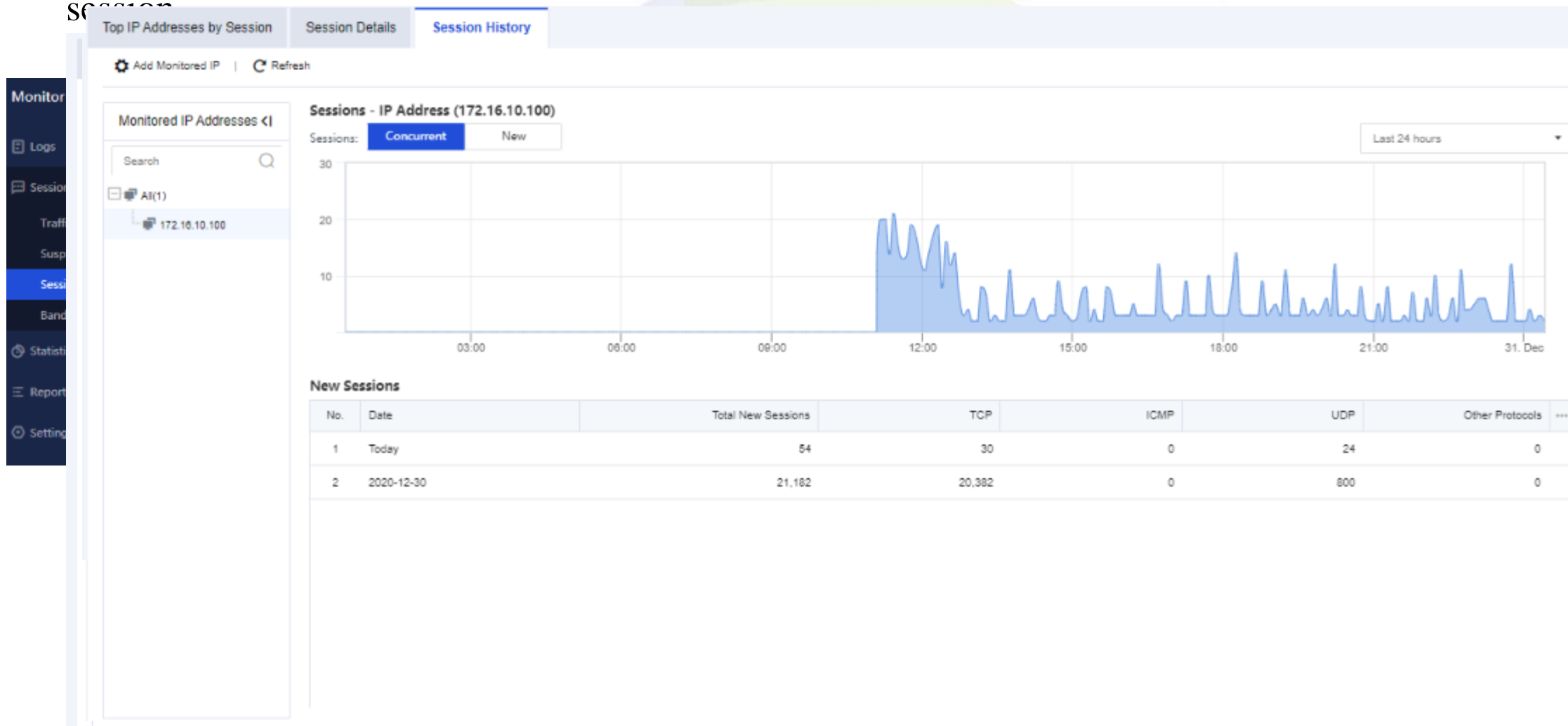
Suspicious Traffic on IP Address (192.168.1.110)

No.	Time	Type	Description	Src IP	Dst IP	Threat Level	Details	...
1	2021-07-11 18:52:08	Reverse on SSH port	Reverse connection is established by SSH p...	192.168.1.110	192.200.19.20	Low	View	
2	2021-07-11 18:54:22	ICMP anomaly	Size of ICMP packet is more than 64Byte.	192.168.1.110	192.168.19.15	Info	View	

Monitor



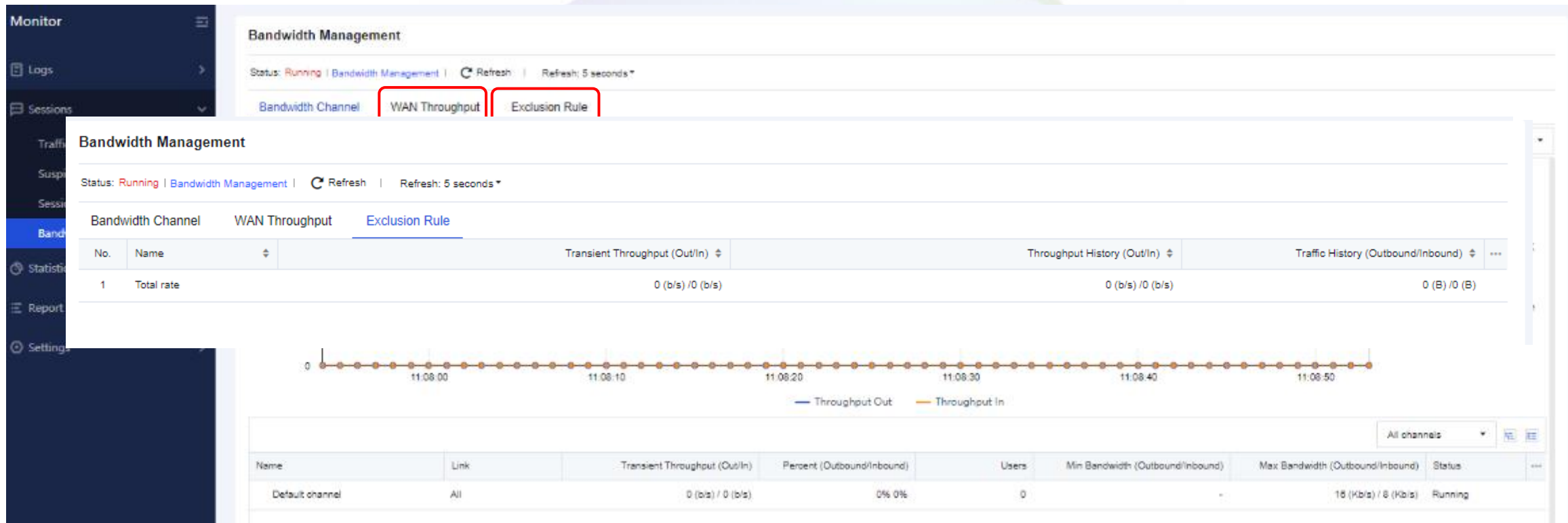
Sessions: Session Ranking allow user to check the IP addresses which has the highest number of session



Monitor



Sessions: Bandwidth Management allows user to check the bandwidth management policy



Monitor



Statistics: Application enables users to collect statistics on the times intranet users access an application on the Internet.

Monitor

Logs

Session

Statistics

Application

Traffic

Report

Setting

Application

Application

Application

Filter

Export as Excel File

Send Report by Email

Filter: Period (2020-12-27 - 2021-01-02)

Export logs

Statistics (App Name)

Show (Top 10)

Statistics by App Name

Statistics

This Week

App Name

TOP 10

App Name	Behaviors	Outbound Traffic	Inbound Traffic
SSL	12	0 KB	0 KB
HTTP_GET	7	0 KB	0 KB
SSH	4	0 KB	0 KB
Total	20	0 KB	0 KB

HTTP_GET

Monitor



Statistics: Traffic enables users to collect statistics on the Internet access traffic of intranet users by application, IP address, etc.

A screenshot of the SANGFOR web interface for monitoring traffic. The left sidebar is dark blue with white text for navigation: Monitor, Logs (with a dropdown arrow), Security Logs, Access Logs, System Logs, Sessions (with a dropdown arrow), Traffic Ranking, Suspicious Traffic, Session Ranking, Bandwidth Management, Statistics (with a dropdown arrow), Application, Traffic (highlighted in blue with a dropdown arrow), Report (with a right arrow), and Settings (with a right arrow). The main content area is titled "Traffic" and contains a "Filter" section. The "Filter" section includes a "Time Period" dropdown set to "Specified" with date pickers for "2020-12-27" and "2021-01-02". Below this are two rows of radio buttons: "Statistics" with options "App Category" (selected), "App Name", "Group", and "IP/User"; and "Rank By" with options "Bidirectional Traffic" (selected), "Outbound Traffic", and "Inbound Traffic". An "Expand" link with a dropdown arrow is below the radio buttons. At the bottom of the filter section is a blue "Search" button and a checkbox for "Open in new tab". The main content area below the filter is currently empty.

Monitor

Report: Security Report page enables users to customize reports based on security.

Monitor

Logs

Security Logs

Access Logs

System Logs

Sessions

Traffic Ranking

Suspicious Traffic

Session Ranking

Bandwidth Management

Statistics

Application

Traffic

Report

Security Report

Report Subscription

Settings

Security Report

Filter

Time Period:

Server:

Host:

Report Contents

Overall Security (t)

Server Security (fi)

Host Security (for)

Security Rating St

Advanced

Generate Report

1 Security Summary

1.1 Summary

Period: 2020-12-25 to 2020-12-30

Pre-Protection: **Medium**

Post-Protection: **Excellent**




Turn On
NGAF Protection

Overall Security Status

Overall Security Status After Protection

With protection, overall security rating is raised to Excellent **Excellent**

If no security policy is enabled, the following attacks may occur:

 Risk	172.16.10.110 server(1) has been Ever been attacked.	Recommendation: Follow the security enhancement recommendations in the corresponding server security sections to fix the issues as soon as possible.
 Attack	4 attack(s) occurred.	Conclusion: Overall security rating is Fair, since most of the attacks are blocked by Sangfor NGAF.
 Vuln	No vulnerability has been detected.	Conclusion: None

Monitor



Report: Report Subscription page can be generated on schedule.

Monitor

Logs

Security Logs

Access

System

Session

Traffic

Suspicious

Session

Bandwidth

Statistics

Application

Traffic

Report

Security Report

Report Subscription

Settings

Report Subscription

+

 Add

🗑

 Delete

✓

 Enable

☐ Report Name

Report History

←

 Back

🗑

 Delete

<input type="checkbox"/>	Report Name	Generated At	User	Operation	...
<input type="checkbox"/>	Security Report_ 20201231	2020-12-31 00:48:28	admin	Export as PDF Email	

1 Security Summary

1.1 Summary

Period: 2020-12-30 to 2020-12-30

Pre-Protection: Excellent

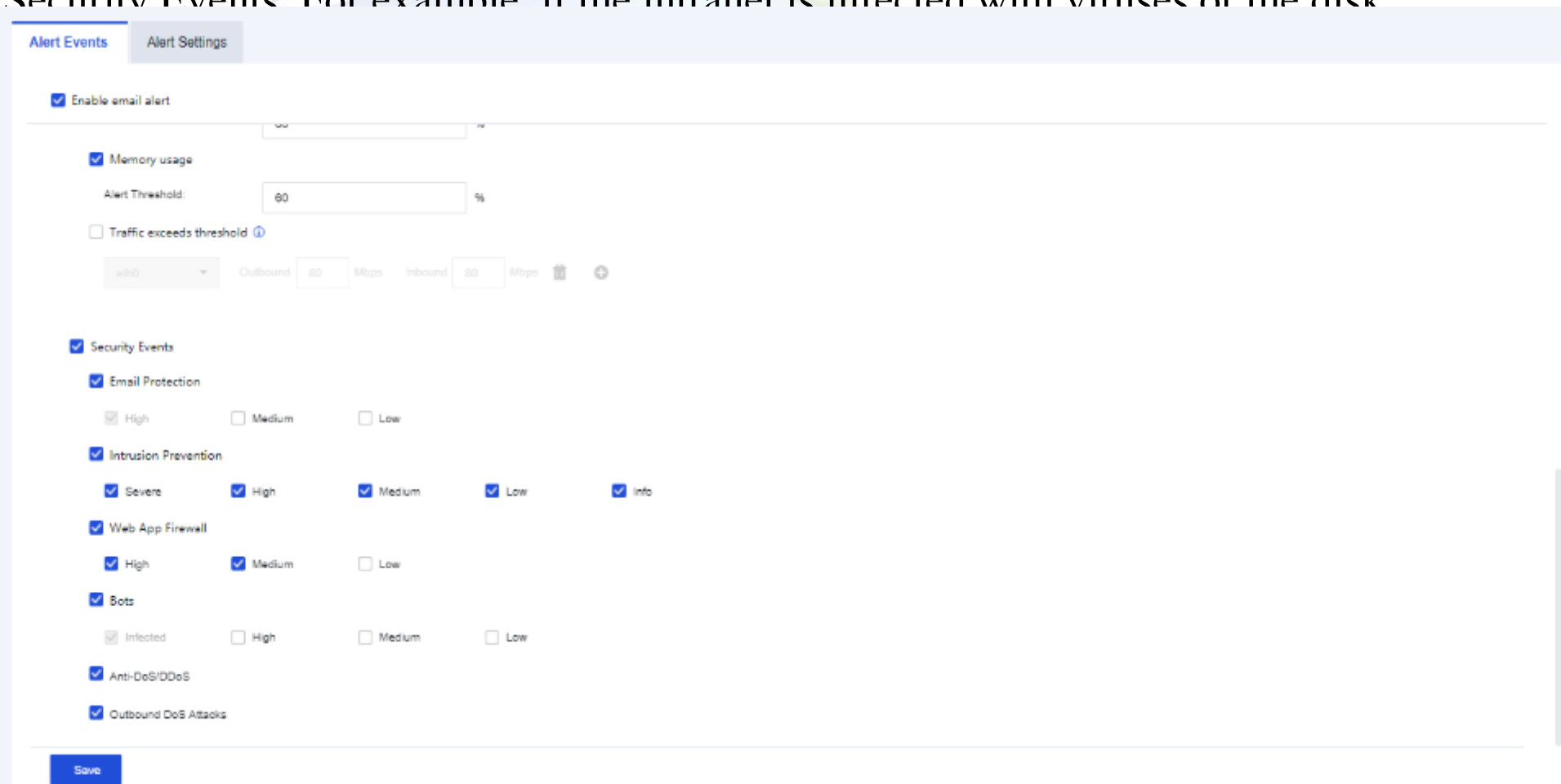
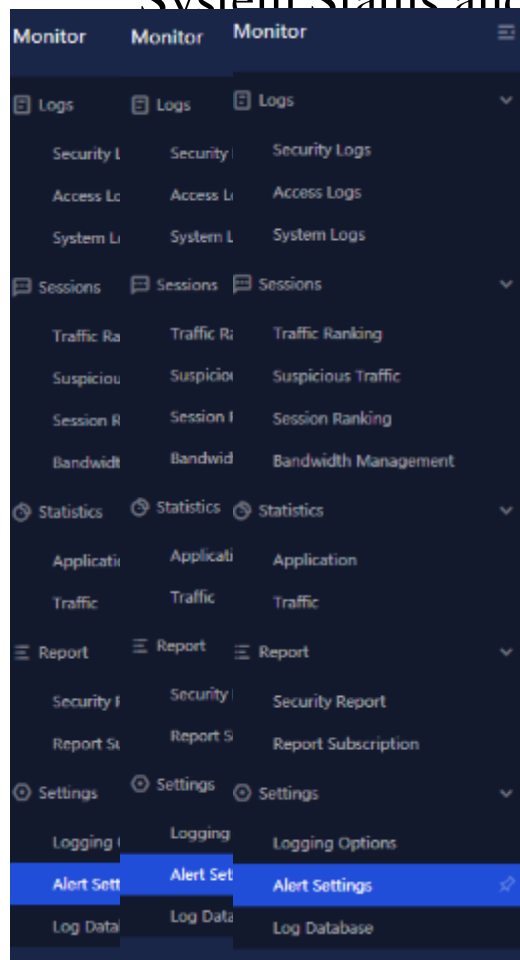
Post-Protection: Excellent

<div><div>Attack</div><div>No attack succeeded.</div></div>	<div><div>Vuln</div><div>No vulnerability has been detected.</div></div>
<div>Conclusion: None</div>	<div>Conclusion: None</div>

Monitor



Settings: Alert Settings enables alarm information to be sent to the administrator's mailbox via email. There are some events which will trigger the alarm which includes Basic, Health Check, Local Logs, System Status and Security Events. For example, if the intranet is infected with viruses or the disk



Monitor



Settings: Log Database page enables users to view the sizes of logs generated over a specified period and refresh the data.

Log Database	
Filter	
Filter: Period (2019-12-31 - 2020-12-31)	
Date	Data Size
2020-12-14	942 KB
2020-12-15	1,765 KB
2020-12-16	3,877 KB
2020-12-17	10,740 KB
2020-12-18	20,774 KB
2020-12-19	34,206 KB
2020-12-20	18,841 KB
2020-12-21	16,200 KB
2020-12-22	7,762 KB
2020-12-23	7,009 KB
2020-12-24	6,205 KB
2020-12-25	5,718 KB
2020-12-26	6,888 KB
2020-12-27	4,833 KB
2020-12-28	2,150 KB
2020-12-29	5,411 KB

Total: 181Entries Per Page50