SANGFOR

Security Report

Period: 2025-11-26 to 2025-12-20

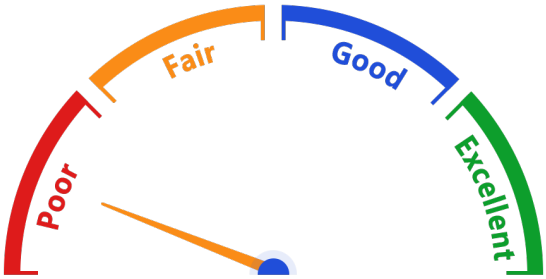
Generated At:	2025-12-20 11:37:47
Application Server Domain/IP:	All
User:	All

1 Security Summary

1.1 Summary

Period: 2025-11-26 to 2025-12-20

Pre-Protection: Poor

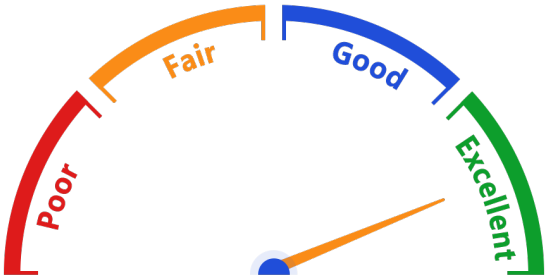


Security Status Without Policies

Turn On

NGAF Protection

Post-Protection: Excellent



Current Security Status

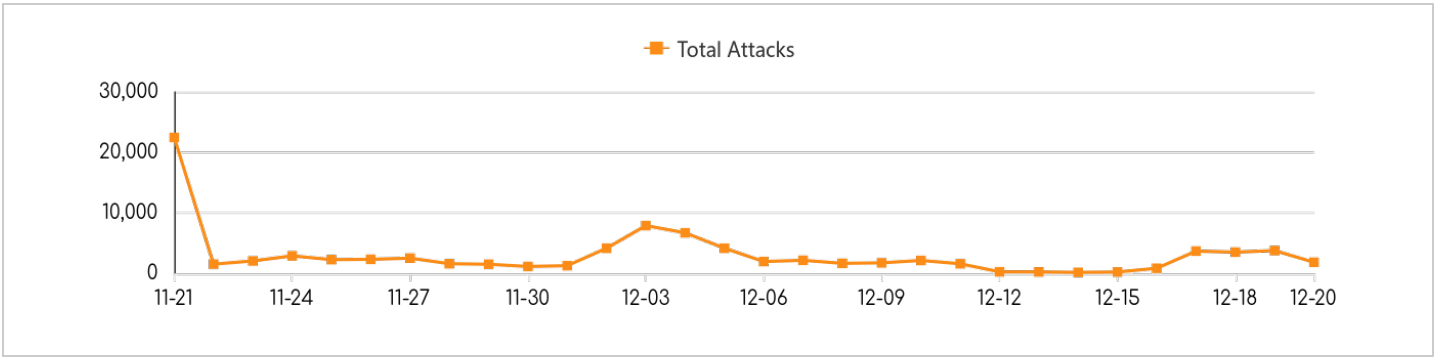
With policies configured, overall security rating can be raised to Excellent

Without security policies enabled, the following attacks cannot be blocked or detected by Network Secure Firewall:

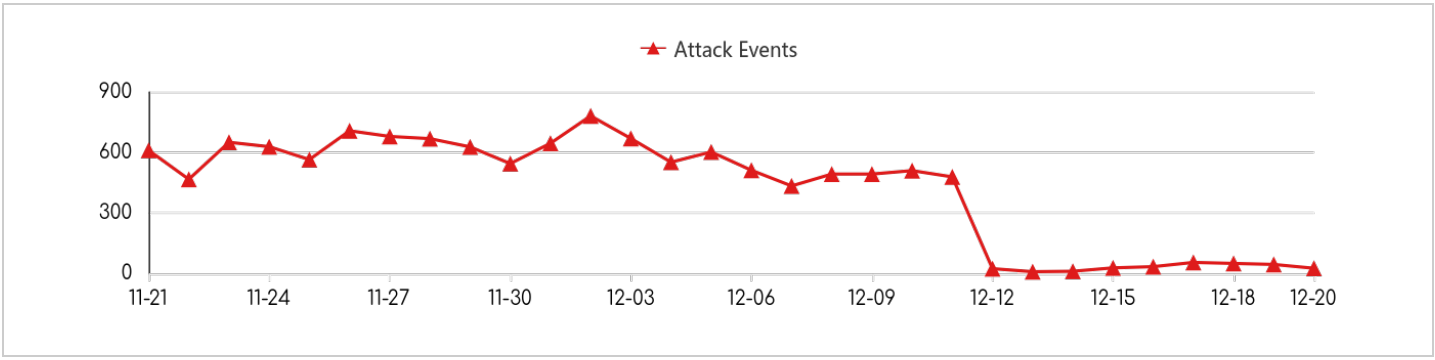
Risk	10.98.0.50,10.98.0.55, 10.0.0.252 server(6) has been Compromised. 10.172.168.13,10.130.11.172, 10.101.1.80 host(82) has been Infected	**Recommendation:** Follow the security enhancement recommendations in the corresponding server security or endpoint security sections to fix the issues as soon as possible.
Attack	58777 attack(s) occurred.	**Conclusion:** Overall security rating is Poor, though most of the attacks are blocked by Sangfor Network Secure Firewall.
Vuln	No vulnerability has been detected.	**Conclusion:** None

1.2 Trends

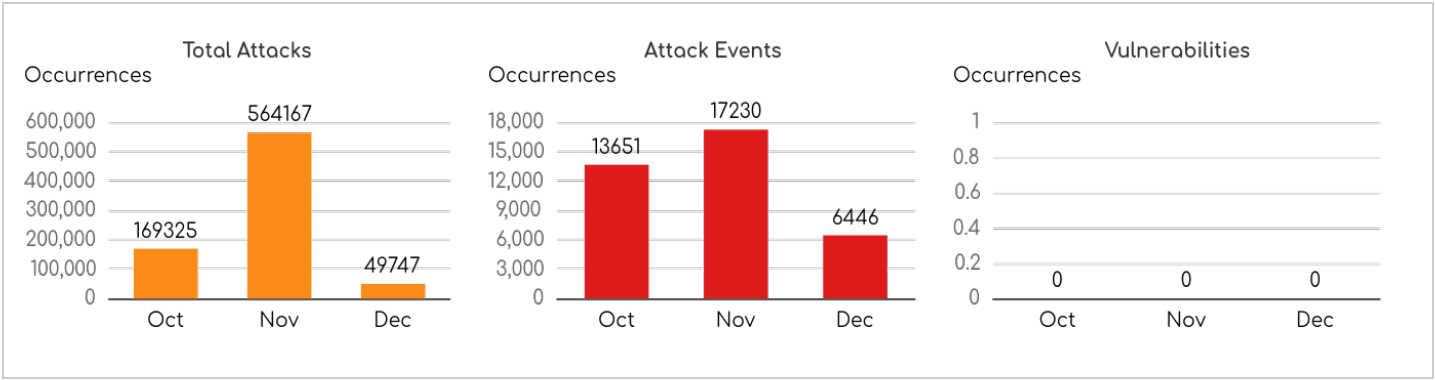
Total Attacks: Indicates the total number of attacks against protected zones. More attacks indicate poorer network security.



Attack Events: Indicates the major attack events extracted and categorized based on a variety of security logs and attack chain analysis techniques. The more attack events there are, the more likely targeted endpoints in protected zones will be compromised. More attack events indicate poorer network security.



Attack Trends



As the number of total attacks increases, network security level goes down accordingly. More attack events indicate more frequent attacks targeting specific servers. Likewise, the more vulnerabilities there are, the more vulnerable the server, and the more likely intrusion may occur.

Failed to render report. Please try again later.

1.3 Vulnerability Distribution

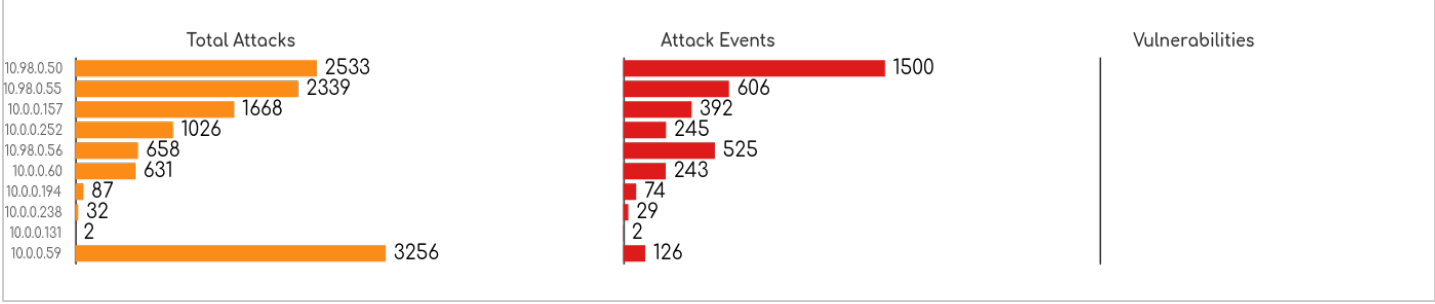
No data available

1.4 Application Server Security

The following are the top attacked servers:

No.	Status	Target Server	Business Asset	Severity	Last Detected	Attack Count
1	Pending	10.98.0.50	-	Compromised(5)	2025-12-20 10:29:31	2533
2	Pending	10.98.0.55	-	Compromised(5)	2025-12-20 05:29:03	2339
3	Pending	10.0.0.157	-	Attacked(4)	2025-12-18 16:53:57	1668
4	Pending	10.0.0.252	-	Compromised(5)	2025-12-16 04:01:43	1026
5	Pending	10.98.0.56	-	Attacked(4)	2025-12-19 15:59:20	658
6	Pending	10.0.0.60	-	Attacked(4)	2025-12-20 09:16:43	631
7	Pending	10.0.0.194	-	Attacked(4)	2025-12-10 00:22:25	87
8	Pending	10.0.0.238	-	Compromised(5)	2025-12-12 14:41:42	32
9	Pending	10.0.0.131	-	Attacked(4)	2025-12-06 00:54:41	2
10	Pending	10.0.0.59	-	Attacked(3)	2025-12-19 12:58:29	3256
11	Pending	10.0.0.240	-	Attacked(3)	2025-12-20 06:56:14	1905
12	Pending	10.172.168.11	-	Attacked(3)	2025-12-20 02:17:04	1778
13	Pending	10.172.168.15	-	Compromised(5)	2025-12-19 14:02:00	1346
14	Pending	10.0.0.115	-	Attacked(3)	2025-12-20 07:29:51	1274
15	Pending	10.0.0.155	-	Attacked(3)	2025-12-20 03:24:23	1155
16	Pending	10.0.0.164	-	Attacked(3)	2025-12-20 03:27:24	1052
17	Pending	10.0.0.73	-	Attacked(3)	2025-12-18 08:57:58	873
18	Pending	10.98.0.58	-	Attacked(3)	2025-12-11 13:59:31	780
19	Pending	10.98.0.53	-	Compromised(5)	2025-12-19 16:34:31	779
20	Pending	10.0.0.217	-	Attacked(3)	2025-12-18 13:16:36	747

Server Risk Distribution



Attack Events

The following are the major attack events categorized and extracted after analysis of security logs, with the help of attack chain analysis techniques.

- Compromised (server has been infected with Trojan or tampered with)
- Bot controlled (host or server has become a Zombie)
- Attacked (server has been attacked, but no data proves that the attack was successful)

No.	Security Event	Details
1	Compromised	No data available
2	Bot Controlled	6 server/host(s) has become zombie, among which are 10.98.0.50,10.98.0.55,10.0.0.252
3	Ever been attacked	1) 10.98.0.50 has suffered 2533 attack(s), which fall into the following major types: Brute-force attack, Web Vulnerability, System Vulnerability, Database Vulnerability, IoT Vuln Exploit. Attack sources: 363 occurrence(s) from 123.143.114.188 (South Korea), 115 occurrence(s) from 79.124.40.174 (Bulgaria), 110 occurrence(s) from 198.23.185.210 (United States) 2) 10.98.0.55 has suffered 2339 attack(s), which fall into the following major types: Brute-force attack, Mail Vulnerability, System Vulnerability, Web Vulnerability, Database Vulnerability. Attack sources: 1097 occurrence(s) from 47.90.162.76 (United States), 115 occurrence(s) from 79.124.40.174 (Bulgaria), 110 occurrence(s) from 198.23.185.210 (United States) 3) 10.0.0.157 has suffered 1668 attack(s), which fall into the following major types: Brute-force attack, Web Vulnerability, System Vulnerability, IoT Vuln Exploit, Scan Vulnerability. Attack sources: 426 occurrence(s) from 123.143.114.188 (South Korea), 420 occurrence(s) from 185.194.178.56 (France), 104 occurrence(s) from 198.23.185.210 (United States)

Attack Sources

The following are the attack sources that have launched the most attacks against the server. We are recommended to log in to the Network Secure Firewall manager and blacklist those attack sources in SOC > Blacklist/Whitelist > Blacklist.

No.	IP Address	Attack Type	Attack Count	Source Location
1	47.90.162.76	Web Vulnerability(15006) System Vulnerability(903) IoT Vuln Exploit(854) Database Vulnerability(70) Mail Vulnerability(28)	16861	United States
2	123.143.114.188	Web Vulnerability(3070)	3070	South Korea

No.	IP Address	Attack Type	Attack Count	Source Location
3	192.159.99.95	Web Vulnerability(1797) IoT Vuln Exploit(679) System Vulnerability(289)	2765	United States
4	18.142.219.158	Web Vulnerability(1188) System Vulnerability(36) IoT Vuln Exploit(28) Database Vulnerability(4)	1256	Singapore
5	79.124.40.174	Web Vulnerability(714) IoT Vuln Exploit(228)	942	Bulgaria
6	185.194.178.56	System Vulnerability(840)	840	France
7	193.34.213.150	Web Vulnerability(648)	648	Poland
8	198.23.185.210	System Vulnerability(538)	538	United States
9	157.15.40.91	Web Vulnerability(498)	498	Indonesia
10	103.179.173.163	Web Vulnerability(471)	471	Viet Nam
11	165.22.53.159	Web Vulnerability(428)	428	Singapore
12	198.23.185.117	System Vulnerability(366)	366	United States
13	47.79.123.30	Web Vulnerability(321) System Vulnerability(18) IoT Vuln Exploit(8) Database Vulnerability(2)	349	Singapore
14	198.143.149.250	System Vulnerability(341)	341	United States
15	141.98.11.189	Web Vulnerability(292)	292	Lithuania
16	185.243.5.134	System Vulnerability(280)	280	United States
17	141.98.82.26	IoT Vuln Exploit(174)	174	Panama
18	72.167.44.205	Web Vulnerability(170)	170	United States
19	147.182.166.6	Web Vulnerability(152)	152	United States
20	194.213.3.8	System Vulnerability(139)	139	United Kingdom

Overseas Attack Sources

The following are the overseas attack sources that have launched the most attacks against the server. We are recommended to log in to the Network Secure Firewall manager and blacklist those attack sources in SOC > Blacklist/Whitelist > Blacklist

No.	IP Address	Attack Type	Attack Count	Source Location
No data available				

1.5 User Security

Bots

The following are the most severe bot-infected hosts:

No.	Status	Infected Host	Zone	Severity	Last Detected	Detections
1	Pending	10.172.168.13	-	Compromised(8)	2025-12-20 11:31:01	12064
2	Pending	10.130.11.172	-	Compromised(8)	2025-12-12 13:24:38	49
3	Pending	10.101.1.80	-	Compromised(8)	2025-12-02 15:54:21	48
4	Pending	10.106.1.218	-	Compromised(8)	2025-11-27 16:18:33	40
5	Pending	10.106.1.197	-	Compromised(8)	2025-12-02 15:52:16	37
6	Pending	10.130.4.22	-	Compromised(8)	2025-11-28 09:28:36	37
7	Pending	10.130.6.251	-	Compromised(8)	2025-12-17 15:17:57	36
8	Pending	10.130.3.108	-	Compromised(8)	2025-12-03 14:14:47	34
9	Pending	10.130.2.50	-	Compromised(8)	2025-12-02 15:48:19	30
10	Pending	10.101.0.171	-	Compromised(8)	2025-12-11 14:36:55	25
11	Pending	10.106.1.136	-	Compromised(8)	2025-12-08 15:20:19	22
12	Pending	10.102.0.174	-	Compromised(8)	2025-12-19 13:24:36	20
13	Pending	10.111.0.191	-	Compromised(8)	2025-12-18 08:16:23	20
14	Pending	10.106.0.138	-	Compromised(8)	2025-12-09 14:05:11	17
15	Pending	10.106.1.135	-	Compromised(8)	2025-11-26 15:28:21	17
16	Pending	10.106.0.168	-	Compromised(8)	2025-12-18 13:55:27	17
17	Pending	10.130.11.74	-	Compromised(8)	2025-12-17 11:04:16	15
18	Pending	10.102.6.134	-	Compromised(8)	2025-12-17 15:30:42	15
19	Pending	10.130.1.140	-	Compromised(8)	2025-12-17 13:24:01	10
20	Pending	10.120.1.176	-	Compromised(8)	2025-11-27 15:39:47	10

Download anti-malware software to scan for and remove malware on the infected host. (Download anti-malware software: http://sec.sangfor.com/apt)

Malicious Files

The following are the top malicious files involved in 0-Day vulnerability exploits detected based on sandbox technology.

No.	File MD5	Virus Name	Severity	Infected Host	Infected Hosts	Last Detected
No data available						

Malicious Website Database

The following are the top malicious websites involved in 0-Day vulnerability exploits detected based on sandbox technology.

No.	URL	Category	Host IP	Hosts	Detections	Last Detected
No data available						

1.6 Overall Security Enhancement Recommendations

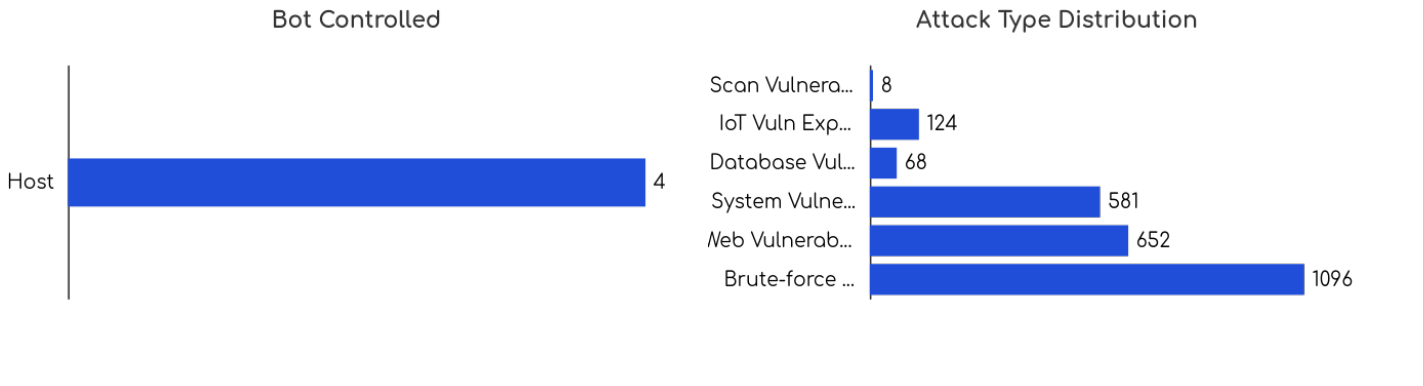
1. Deal with and fix security issues by following the recommendations in SOC > Security Operations of Network Secure Firewall manager.
2. Log in to the Network Secure Firewall manager and go to SOC > Business Asset Security > Passive Vulnerability Scan to generate the Full Report and follow the recommendations to fix the existing vulnerabilities.
3. To prevent subsequent attacks from the above sources, log in to the Network Secure Firewall manager and blacklist the above IP addresses in SOC > Blacklist/Whitelist > Blacklist.
4. Follow the security enhancement recommendations in server and host security to fix security issues.

2 Server Security

2.1 10.98.0.50 Security Details (To be Fixed)

10.98.0.50 Overall security rating: Compromised

10.98.0.50 is controlled by an attacker and has suffered 2533 attack(s)



2.1.1 Attack Events

Category	Bot controlled
Summary	10.98.0.50 has been controlled remotely by an attacker and become a zombie.
Details	2025-12-07 11:28:36 Through the cloud-based engine, it is detected that the internal host (10.98.0.50) is trying to communicate with the malicious IP address (162.216.149.27:53640).. (1 occurrence(s)) 2025-12-07 10:59:55 Through the cloud-based engine, it is detected that the internal host (10.98.0.50) is trying to communicate with the malicious IP address (185.196.9.18:63915).. (1 occurrence(s)) 2025-12-07 10:11:55 Through the cloud-based engine, it is detected that the internal host (10.98.0.50) is trying to communicate with the malicious IP address (185.196.9.18:58464).. (1 occurrence(s))

2.1.2 Vulnerabilities

No data available

2.1.3 Attack Sources

The following are the major sources launched attacks against 10.98.0.50, 2533 attacks in total. You are recommended to blacklist in SOC > Blacklist/Whitelist > Blacklist.

No.	Attack Source	Attack Type	Source Location	Attack Count
1	123.143.114.188	Web Vulnerability(363)	South Korea	363

No.	Attack Source	Attack Type	Source Location	Attack Count
2	79.124.40.174	Web Vulnerability(87) IoT Vuln Exploit(28)	Bulgaria	115
3	198.23.185.210	System Vulnerability(110)	United States	110
4	192.159.99.95	Web Vulnerability(70) IoT Vuln Exploit(18) System Vulnerability(8)	United States	96
5	198.23.185.117	System Vulnerability(73)	United States	73

2.1.4 Security Enhancement Recommendations

The server has been attacked. Follow the recommendations below to enhance security.

1. Status

- Add a corresponding policy to protect the server and then click on the flag icon to change Action status (to Action has been taken) in SOC > Business Asset Security > Summary.

2. Bot Controlled

- Download anti-malware software to scan for and remove malware on the infected host. (Download anti-malware software: http://sec.sangfor.com/apt)

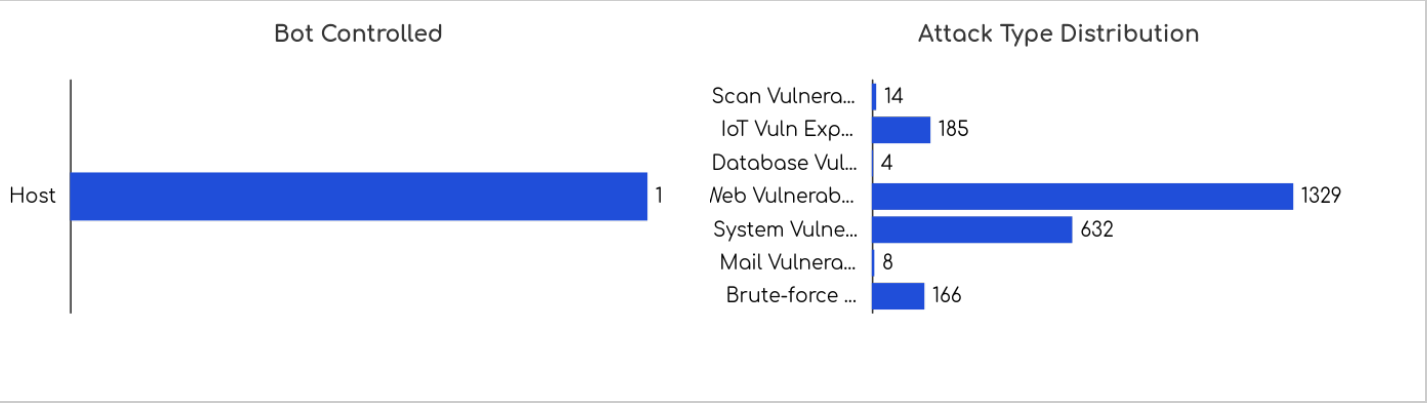
3. Blacklist Attacker IP

- To prevent subsequent attacks from the above sources, log in to the Network Secure Firewall manager and blacklist above IP addresses in SOC > Blacklist/Whitelist > Blacklist.

2.2 10.98.0.55 Security Details (To be Fixed)

10.98.0.55 Overall security rating: Compromised

10.98.0.55 is controlled by an attacker and has suffered 2339 attack(s)



2.2.1 Attack Events

Category	Bot controlled
Summary	10.98.0.55 has been controlled remotely by an attacker and become a zombie.

Details	2025-12-02 05:39:23 Through the cloud-based engine, it is detected that the internal host (10.98.0.55) is trying to communicate with the malicious IP address (195.211.96.85:50595).. (1 occurrence(s))

2.2.2 Vulnerabilities

No data available

2.2.3 Attack Sources

The following are the major sources launched attacks against 10.98.0.55, 2339 attacks in total. You are recommended to blacklist in SOC > Blacklist/Whitelist > Blacklist.

No.	Attack Source	Attack Type	Source Location	Attack Count
1	47.90.162.76	Web Vulnerability(979) IoT Vuln Exploit(66) System Vulnerability(42) Mail Vulnerability(8) Database Vulnerability(2)	United States	1097
2	79.124.40.174	Web Vulnerability(87) IoT Vuln Exploit(28)	Bulgaria	115
3	198.23.185.210	System Vulnerability(110)	United States	110
4	103.179.173.163	Web Vulnerability(77)	Viet Nam	77
5	198.23.185.117	System Vulnerability(76)	United States	76

2.2.4 Security Enhancement Recommendations

The server has been attacked. Follow the recommendations below to enhance security.

1. Status

- Add a corresponding policy to protect the server and then click on the flag icon to change Action status (to Action has been taken) in SOC > Business Asset Security > Summary.

2. Bot Controlled

- Download anti-malware software to scan for and remove malware on the infected host. (Download anti-malware software: http://sec.sangfor.com/apt)

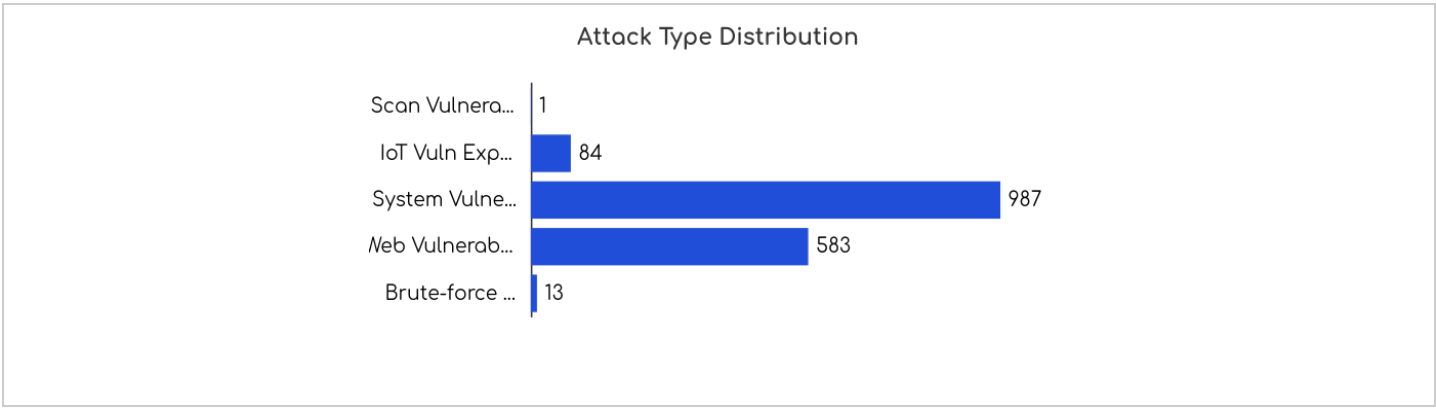
3. Blacklist Attacker IP

- To prevent subsequent attacks from the above sources, log in to the Network Secure Firewall manager and blacklist above IP addresses in SOC > Blacklist/Whitelist > Blacklist.

2.3 10.0.0.157 Security Details (To be Fixed)

10.0.0.157 Overall security rating: Attacked

10.0.0.157 suffered 1668 attack(s)



2.3.1 Attack Events

Category	Ever been attacked
Summary	10.0.0.157 has been attacked by 185.194.178.56(France, 420 occurrences), System Vulnerability (420)
Details	Start Time: 2025-12-07 12:59:59 End Time: 2025-12-07 13:21:00 More logs are available in Monitor > Logs > Security Logs > Web Application, Intrusion Prevention, Website Browsing > Email Protection in Network Secure Firewall GUI.

Category	Ever been attacked
Summary	10.0.0.157 has been attacked by 198.23.185.210(United States, 60 occurrences), System Vulnerability (60)
Details	Start Time: 2025-11-26 00:34:09 End Time: 2025-11-26 20:24:17 More logs are available in Monitor > Logs > Security Logs > Web Application, Intrusion Prevention, Website Browsing > Email Protection in Network Secure Firewall GUI.

Category	Ever been attacked
Summary	10.0.0.157 has been attacked by 123.143.114.188(South Korea, 48 occurrences), Web Vulnerability (48)
Details	Start Time: 2025-12-02 05:38:23 End Time: 2025-12-02 19:53:25 More logs are available in Monitor > Logs > Security Logs > Web Application, Intrusion Prevention, Website Browsing > Email Protection in Network Secure Firewall GUI.

2.3.2 Vulnerabilities

No data available

2.3.3 Attack Sources

The following are the major sources launched attacks against 10.0.0.157, 1668 attacks in total. You are recommended to blacklist in SOC > Blacklist/Whitelist > Blacklist.

No.	Attack Source	Attack Type	Source Location	Attack Count
1	123.143.114.188	Web Vulnerability(426)	South Korea	426
2	185.194.178.56	System Vulnerability(420)	France	420
3	198.23.185.210	System Vulnerability(104)	United States	104
4	192.159.99.95	Web Vulnerability(52) IoT Vuln Exploit(18) System Vulnerability(7)	United States	77
5	198.23.185.117	System Vulnerability(72)	United States	72

2.3.4 Security Enhancement Recommendations

The server has been attacked. Follow the recommendations below to enhance security.

1. Status

- Add a corresponding policy to protect the server and then click on the flag icon to change Action status (to Action has been taken) in SOC > Business Asset Security > Summary.

2. Attacked

- All the attacks against the server have been blocked by Sangfor Network Secure Firewall and vulnerabilities have been fixed. No more action is required.

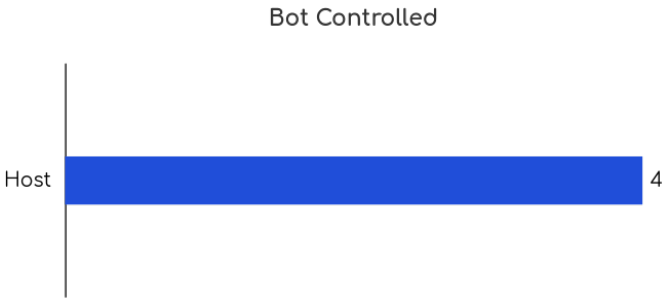
3. Blacklist Attacker IP

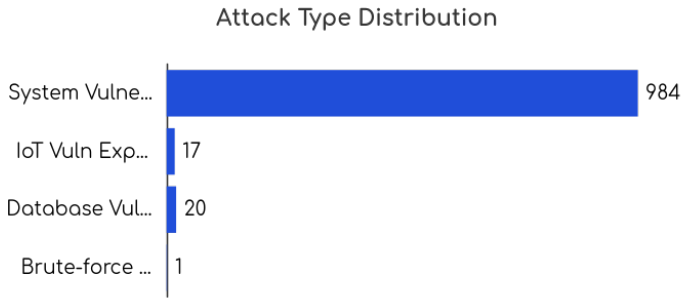
- To prevent subsequent attacks from the above sources, log in to the Network Secure Firewall manager and blacklist above IP addresses in SOC > Blacklist/Whitelist > Blacklist.

2.4 10.0.0.252 Security Details (To be Fixed)

10.0.0.252 Overall security rating: Compromised

10.0.0.252 is controlled by an attacker and has suffered 1026 attack(s)





2.4.1 Attack Events

Category	Bot controlled
Summary	10.0.0.252 has been controlled remotely by an attacker and become a zombie.
Details	2025-12-05 09:36:42 Through the cloud-based engine, it is detected that the internal host (10.0.0.252) is trying to communicate with the malicious IP address (124.226.212.169:46944).. (2 occurrence(s))

2.4.2 Vulnerabilities

No data available

2.4.3 Attack Sources

The following are the major sources launched attacks against 10.0.0.252, 1026 attacks in total. You are recommended to blacklist in SOC > Blacklist/Whitelist > Blacklist.

No.	Attack Source	Attack Type	Source Location	Attack Count
1	185.194.178.56	System Vulnerability(420)	France	420
2	198.23.185.210	System Vulnerability(103)	United States	103
3	198.23.185.117	System Vulnerability(71)	United States	71
4	198.143.149.250	System Vulnerability(68)	United States	68
5	185.243.5.134	System Vulnerability(56)	United States	56

2.4.4 Security Enhancement Recommendations

The server has been attacked. Follow the recommendations below to enhance security.

1. Status

- Add a corresponding policy to protect the server and then click on the flag icon to change Action status (to Action has been taken) in SOC > Business Asset Security > Summary.

2. Bot Controlled

- Download anti-malware software to scan for and remove malware on the infected host. (Download anti-

Failed to render report. Please try again later.

malware software: http://sec.sangfor.com/apt)

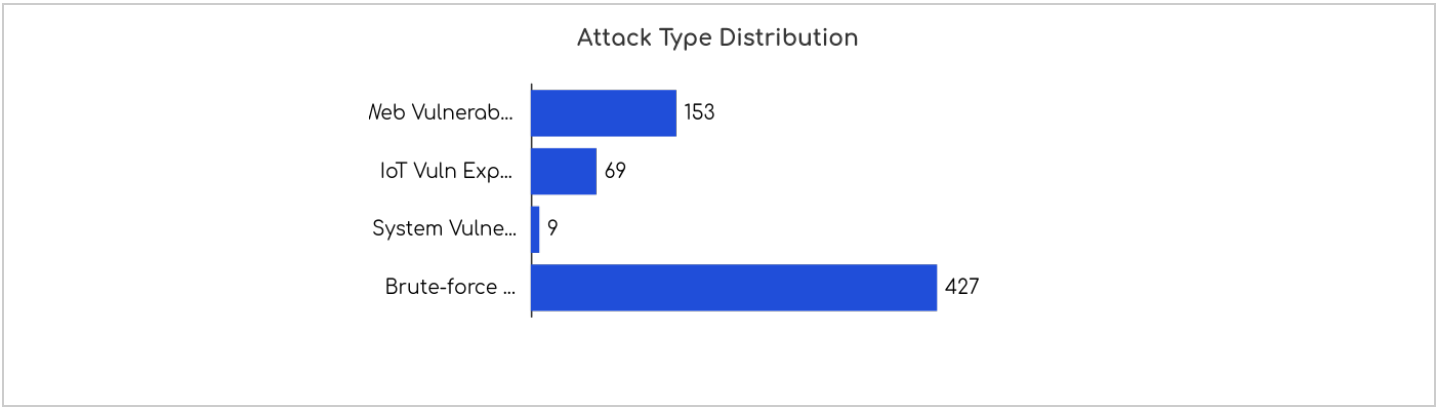
3. Blacklist Attacker IP

- To prevent subsequent attacks from the above sources, log in to the Network Secure Firewall manager and blacklist above IP addresses in SOC > Blacklist/Whitelist > Blacklist.

2.5 10.98.0.56 Security Details (To be Fixed)

10.98.0.56 Overall security rating: Attacked

10.98.0.56 suffered 658 attack(s)



2.5.1 Attack Events

Category	Ever been attacked
Summary	10.98.0.56 has been attacked by 192.159.99.95(United States, 40 occurrences), Web Vulnerability (49), System Vulnerability (8)
Details	Start Time: 2025-12-05 12:09:18 End Time: 2025-12-05 19:34:31 More logs are available in Monitor > Logs > Security Logs > Web Application, Intrusion Prevention, Website Browsing > Email Protection in Network Secure Firewall GUI.

Category	Ever been attacked
Summary	10.98.0.56 has been attacked by 192.159.99.95(United States, 21 occurrences)
Details	Start Time: 2025-11-29 06:35:32 End Time: 2025-11-29 13:36:18 More logs are available in Monitor > Logs > Security Logs > Web Application, Intrusion Prevention, Website Browsing > Email Protection in Network Secure Firewall GUI.

Category	Ever been attacked

Failed to render report. Please try again later.

Summary	10.98.0.56 has been attacked by 192.159.99.95(United States, 20 occurrences), IoT Vuln Exploit (24)
Details	Start Time: 2025-11-28 21:52:05 End Time: 2025-11-28 21:52:14 More logs are available in Monitor > Logs > Security Logs > Web Application, Intrusion Prevention, Website Browsing > Email Protection in Network Secure Firewall GUI.

2.5.2 Vulnerabilities

No data available

2.5.3 Attack Sources

The following are the major sources launched attacks against 10.98.0.56, 658 attacks in total. You are recommended to blacklist in SOC > Blacklist/Whitelist > Blacklist.

No.	Attack Source	Attack Type	Source Location	Attack Count
1	192.159.99.95	Web Vulnerability(54) IoT Vuln Exploit(24) System Vulnerability(9)	United States	87
2	79.124.40.174	Web Vulnerability(41) IoT Vuln Exploit(14)	Bulgaria	55
3	193.34.213.150	Web Vulnerability(8)	Poland	8
4	141.98.82.26	IoT Vuln Exploit(3)	Panama	3
5	72.167.44.205	Web Vulnerability(3)	United States	3

2.5.4 Security Enhancement Recommendations

The server has been attacked. Follow the recommendations below to enhance security.

1. Status

- Add a corresponding policy to protect the server and then click on the flag icon to change Action status (to Action has been taken) in SOC > Business Asset Security > Summary.

2. Attacked

- All the attacks against the server have been blocked by Sangfor Network Secure Firewall and vulnerabilities have been fixed. No more action is required.

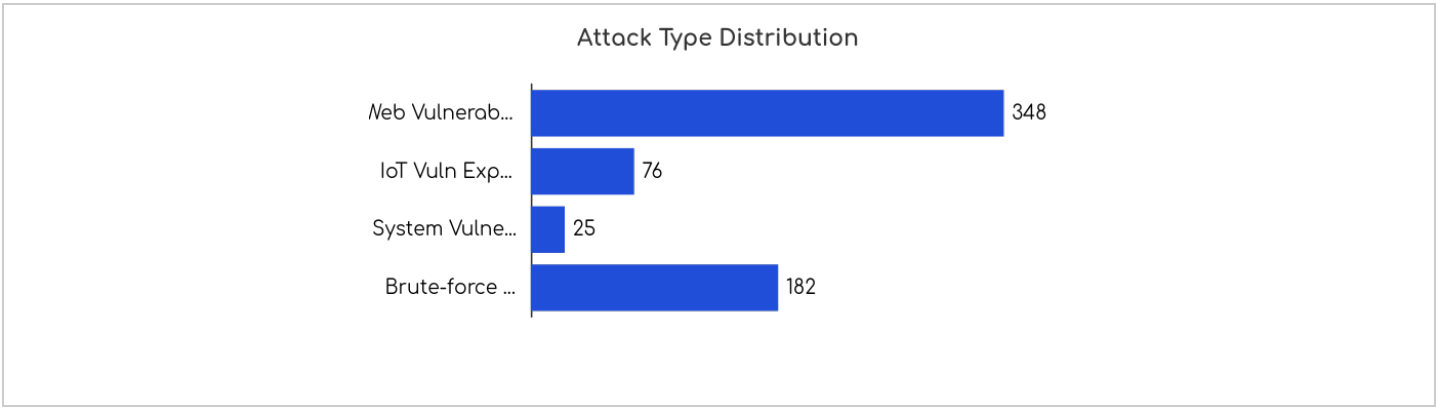
3. Blacklist Attacker IP

- To prevent subsequent attacks from the above sources, log in to the Network Secure Firewall manager and blacklist above IP addresses in SOC > Blacklist/Whitelist > Blacklist.

2.6 10.0.0.60 Security Details (To be Fixed)

10.0.0.60 Overall security rating: Attacked

10.0.0.60 suffered 631 attack(s)



2.6.1 Attack Events

Category	Ever been attacked
Summary	10.0.0.60 has been attacked by 47.90.162.76(United States, 109 occurrences), Web Vulnerability (201), System Vulnerability (18)
Details	Start Time: 2025-12-03 01:43:30 End Time: 2025-12-03 20:08:57 More logs are available in Monitor > Logs > Security Logs > Web Application, Intrusion Prevention, Website Browsing > Email Protection in Network Secure Firewall GUI.

Category	Ever been attacked
Summary	10.0.0.60 has been attacked by 47.90.162.76(United States, 69 occurrences), IoT Vuln Exploit (5)
Details	Start Time: 2025-12-04 00:56:06 End Time: 2025-12-04 23:30:49 More logs are available in Monitor > Logs > Security Logs > Web Application, Intrusion Prevention, Website Browsing > Email Protection in Network Secure Firewall GUI.

Category	Ever been attacked
Summary	10.0.0.60 has been attacked by 47.90.162.76(United States, 46 occurrences)

Failed to render report. Please try again later.

Details	Start Time: 2025-12-02 17:56:11 End Time: 2025-12-02 18:48:26 More logs are available in Monitor > Logs > Security Logs > Web Application, Intrusion Prevention, Website Browsing > Email Protection in Network Secure Firewall GUI.

2.6.2 Vulnerabilities

No data available

2.6.3 Attack Sources

The following are the major sources launched attacks against 10.0.0.60, 631 attacks in total. You are recommended to blacklist in SOC > Blacklist/Whitelist > Blacklist.

No.	Attack Source	Attack Type	Source Location	Attack Count
1	47.90.162.76	Web Vulnerability(247) System Vulnerability(18) IoT Vuln Exploit(11)	United States	276
2	192.159.99.95	Web Vulnerability(42) IoT Vuln Exploit(18) System Vulnerability(7)	United States	67
3	38.45.91.139	IoT Vuln Exploit(20) Web Vulnerability(8)	United States	28
4	101.126.41.218	Brute-force attack(17)	China	17
5	165.154.119.41	Brute-force attack(13)	Thailand	13

2.6.4 Security Enhancement Recommendations

The server has been attacked. Follow the recommendations below to enhance security.

1. Status

- Add a corresponding policy to protect the server and then click on the flag icon to change Action status (to Action has been taken) in SOC > Business Asset Security > Summary.

2. Attacked

- All the attacks against the server have been blocked by Sangfor Network Secure Firewall and vulnerabilities have been fixed. No more action is required.

3. Blacklist Attacker IP

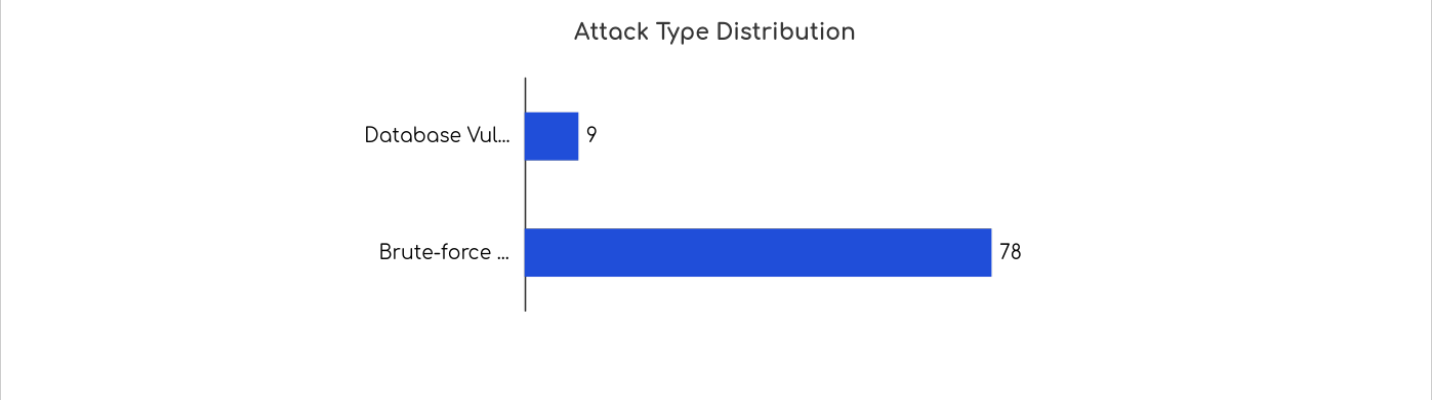
- To prevent subsequent attacks from the above sources, log in to the Network Secure Firewall manager and blacklist above IP addresses in SOC > Blacklist/Whitelist > Blacklist.

2.7 10.0.0.194 Security Details (To be Fixed)

Failed to render report. Please try again later.

10.0.0.194 Overall security rating: Attacked

10.0.0.194 suffered 87 attack(s)



2.7.1 Attack Events

Category	Ever been attacked
Summary	10.0.0.194 has been attacked by 180.101.183.205(China, 2 occurrences), Brute-force attack (2)
Details	Start Time: 2025-11-26 08:56:24 End Time: 2025-11-26 12:55:51 More logs are available in Monitor > Logs > Security Logs > Web Application, Intrusion Prevention, Website Browsing > Email Protection in Network Secure Firewall GUI.

Category	Ever been attacked
Summary	10.0.0.194 has been attacked by 147.45.45.79(Germany, 2 occurrences)
Details	Start Time: 2025-12-02 08:55:31 End Time: 2025-12-02 12:56:14 More logs are available in Monitor > Logs > Security Logs > Web Application, Intrusion Prevention, Website Browsing > Email Protection in Network Secure Firewall GUI.

Category	Ever been attacked
Summary	10.0.0.194 has been attacked by 147.45.45.79(Germany, 2 occurrences), Brute-force attack (4)

Failed to render report. Please try again later.

Details	Start Time: 2025-11-29 08:55:15 End Time: 2025-11-29 12:55:12 More logs are available in Monitor > Logs > Security Logs > Web Application, Intrusion Prevention, Website Browsing > Email Protection in Network Secure Firewall GUI.

2.7.2 Vulnerabilities

No data available

2.7.3 Attack Sources

The following are the major sources launched attacks against 10.0.0.194, 87 attacks in total. You are recommended to blacklist in SOC > Blacklist/Whitelist > Blacklist.

No.	Attack Source	Attack Type	Source Location	Attack Count
1	49.0.82.159	Brute-force attack(5)	Thailand	5
2	27.223.106.194	Brute-force attack(5)	China	5
3	147.45.45.79	Brute-force attack(5)	Germany	5
4	178.166.47.25	Brute-force attack(4)	Portugal	4
5	185.16.38.78	Brute-force attack(4)	Poland	4

2.7.4 Security Enhancement Recommendations

The server has been attacked. Follow the recommendations below to enhance security.

1. Status

- Add a corresponding policy to protect the server and then click on the flag icon to change Action status (to Action has been taken) in SOC > Business Asset Security > Summary.

2. Attacked

- All the attacks against the server have been blocked by Sangfor Network Secure Firewall and vulnerabilities have been fixed. No more action is required.

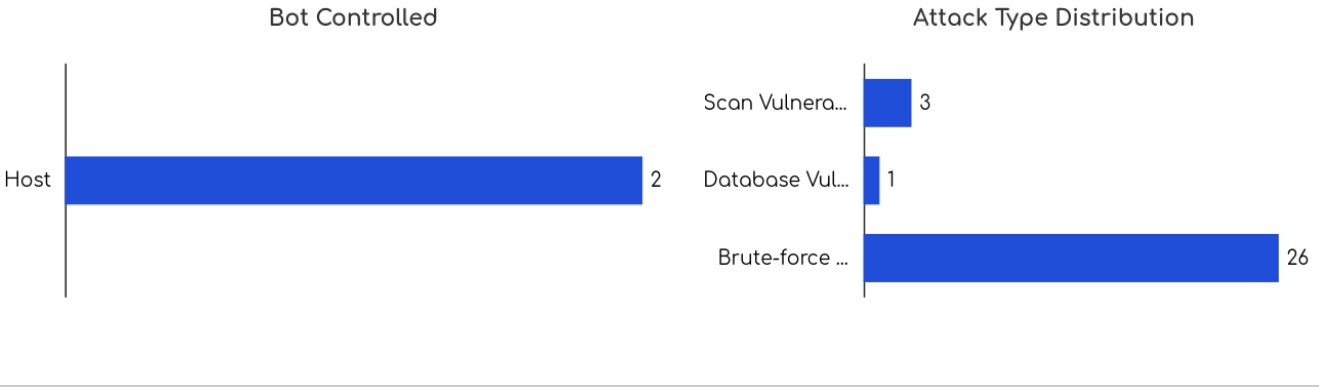
3. Blacklist Attacker IP

- To prevent subsequent attacks from the above sources, log in to the Network Secure Firewall manager and blacklist above IP addresses in SOC > Blacklist/Whitelist > Blacklist.

2.8 10.0.0.238 Security Details (To be Fixed)

10.0.0.238 Overall security rating: Compromised

10.0.0.238 is controlled by an attacker and has suffered 32 attack(s)



2.8.1 Attack Events

Category	Bot controlled
Summary	10.0.0.238 has been controlled remotely by an attacker and become a zombie.
Details	2025-12-01 13:06:32 Through the cloud-based engine, it is detected that the internal host (10.0.0.238) is trying to communicate with the malicious IP address (219.144.86.169:5670).. (1 occurrence(s)) 2025-12-01 12:56:12 Through the cloud-based engine, it is detected that the internal host (10.0.0.238) is trying to communicate with the malicious IP address (219.144.86.169:22038).. (1 occurrence(s))

2.8.2 Vulnerabilities

No data available

2.8.3 Attack Sources

The following are the major sources launched attacks against 10.0.0.238, 32 attacks in total. You are recommended to blacklist in SOC > Blacklist/Whitelist > Blacklist.

No.	Attack Source	Attack Type	Source Location	Attack Count
1	221.8.39.77	Brute-force attack(3)	China	3
2	36.108.170.78	Brute-force attack(2)	China	2
3	154.201.70.217	Brute-force attack(2)	Hong Kong, China	2
4	36.163.6.115	Brute-force attack(1)	China	1
5	111.43.41.40	Brute-force attack(1)	China	1

2.8.4 Security Enhancement Recommendations

The server has been attacked. Follow the recommendations below to enhance security.

1. Status

- Add a corresponding policy to protect the server and then click on the flag icon to change Action status

(to Action has been taken) in SOC > Business Asset Security > Summary.

2. Bot Controlled

- Download anti-malware software to scan for and remove malware on the infected host. (Download anti-malware software: http://sec.sangfor.com/apt)

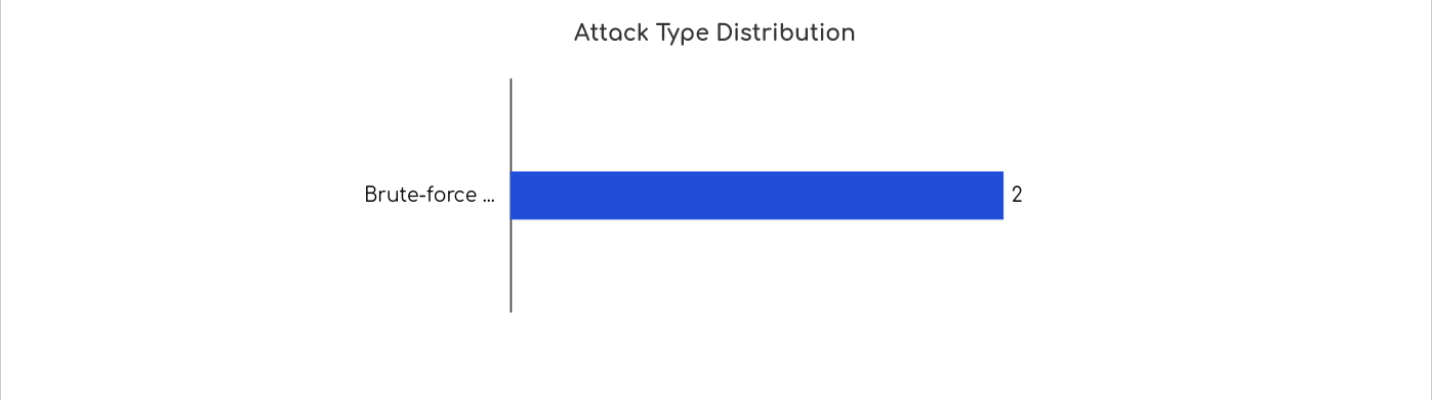
3. Blacklist Attacker IP

- To prevent subsequent attacks from the above sources, log in to the Network Secure Firewall manager and blacklist above IP addresses in SOC > Blacklist/Whitelist > Blacklist.

2.9 10.0.0.131 Security Details (To be Fixed)

10.0.0.131 Overall security rating: Attacked

10.0.0.131 suffered 2 attack(s)



2.9.1 Attack Events

Category	Ever been attacked
Summary	10.0.0.131 has been attacked by 88.218.64.124(Russia, 1 occurrences), Brute-force attack (1)
Details	Start Time: 2025-12-06 00:54:41 End Time: 2025-12-06 00:54:41 More logs are available in Monitor > Logs > Security Logs > Web Application, Intrusion Prevention, Website Browsing > Email Protection in Network Secure Firewall GUI.

Category	Ever been attacked
Summary	10.0.0.131 has been attacked by 143.198.225.197(United States, 1 occurrences), Brute-force attack (1)

Failed to render report. Please try again later.

Details	Start Time: 2025-11-26 20:55:58 End Time: 2025-11-26 20:55:58 More logs are available in Monitor > Logs > Security Logs > Web Application, Intrusion Prevention, Website Browsing > Email Protection in Network Secure Firewall GUI.

2.9.2 Vulnerabilities

No data available

2.9.3 Attack Sources

The following are the major sources launched attacks against 10.0.0.131, 2 attacks in total. You are recommended to blacklist in SOC > Blacklist/Whitelist > Blacklist.

No.	Attack Source	Attack Type	Source Location	Attack Count
1	88.218.64.124	Brute-force attack(1)	Russia	1
2	143.198.225.197	Brute-force attack(1)	United States	1

2.9.4 Security Enhancement Recommendations

The server has been attacked. Follow the recommendations below to enhance security.

1. Status

- Add a corresponding policy to protect the server and then click on the flag icon to change Action status (to Action has been taken) in SOC > Business Asset Security > Summary.

2. Attacked

- All the attacks against the server have been blocked by Sangfor Network Secure Firewall and vulnerabilities have been fixed. No more action is required.

3. Blacklist Attacker IP

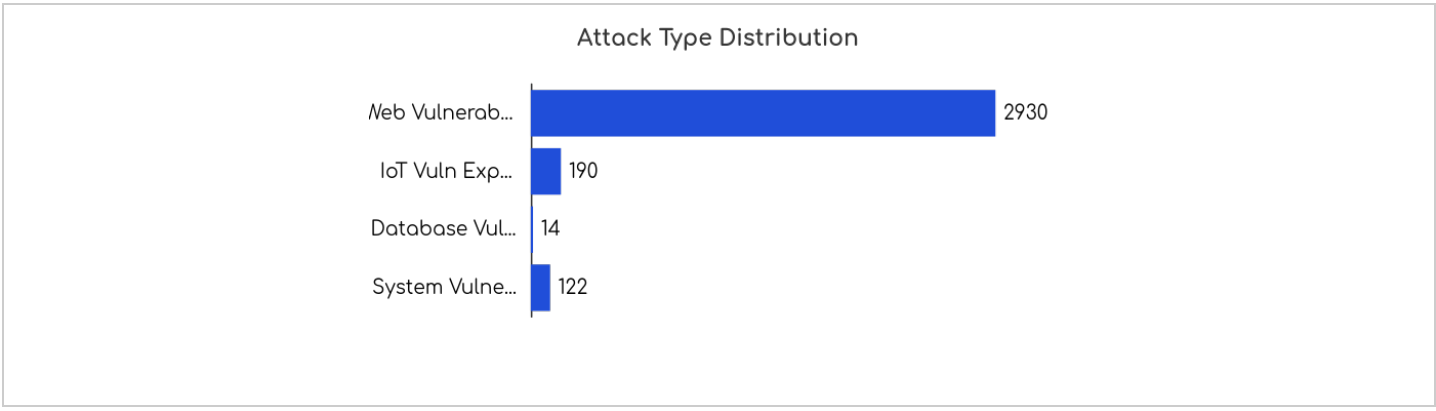
- To prevent subsequent attacks from the above sources, log in to the Network Secure Firewall manager and blacklist above IP addresses in SOC > Blacklist/Whitelist > Blacklist.

2.10 10.0.0.59 Security Details (To be Fixed)

10.0.0.59 Overall security rating: Attacked

10.0.0.59 suffered 3256 attack(s)

Failed to render report. Please try again later.



2.10.1 Attack Events

Category	Ever been attacked
Summary	10.0.0.59 has been attacked by 47.90.162.76(United States, 963 occurrences), System Vulnerability (117), IoT Vuln Exploit (71)
Details	Start Time: 2025-12-03 00:17:20 End Time: 2025-12-03 23:04:17 More logs are available in Monitor > Logs > Security Logs > Web Application, Intrusion Prevention, Website Browsing > Email Protection in Network Secure Firewall GUI.

Category	Ever been attacked
Summary	10.0.0.59 has been attacked by 47.90.162.76(United States, 872 occurrences)
Details	Start Time: 2025-12-04 00:14:24 End Time: 2025-12-04 23:57:40 More logs are available in Monitor > Logs > Security Logs > Web Application, Intrusion Prevention, Website Browsing > Email Protection in Network Secure Firewall GUI.

Category	Ever been attacked
Summary	10.0.0.59 has been attacked by 47.90.162.76(United States, 514 occurrences), Web Vulnerability (2147)
Details	Start Time: 2025-12-02 17:19:20 End Time: 2025-12-02 22:29:44 More logs are available in Monitor > Logs > Security Logs > Web Application, Intrusion Prevention, Website Browsing > Email Protection in Network Secure Firewall GUI.

2.10.2 Vulnerabilities

Failed to render report. Please try again later.

No data available

2.10.3 Attack Sources

The following are the major sources launched attacks against 10.0.0.59, 3256 attacks in total. You are recommended to blacklist in SOC > Blacklist/Whitelist > Blacklist.

No.	Attack Source	Attack Type	Source Location	Attack Count
1	47.90.162.76	Web Vulnerability(2627) IoT Vuln Exploit(145) System Vulnerability(117) Database Vulnerability(14)	United States	2903
2	147.182.166.6	Web Vulnerability(52)	United States	52
3	165.22.53.159	Web Vulnerability(47)	Singapore	47
4	192.159.99.95	Web Vulnerability(30) IoT Vuln Exploit(12) System Vulnerability(5)	United States	47
5	165.22.110.221	Web Vulnerability(28)	Singapore	28

2.10.4 Security Enhancement Recommendations

The server has been attacked. Follow the recommendations below to enhance security.

1. Status

- Add a corresponding policy to protect the server and then click on the flag icon to change Action status (to Action has been taken) in SOC > Business Asset Security > Summary.

2. Attacked

- All the attacks against the server have been blocked by Sangfor Network Secure Firewall and vulnerabilities have been fixed. No more action is required.

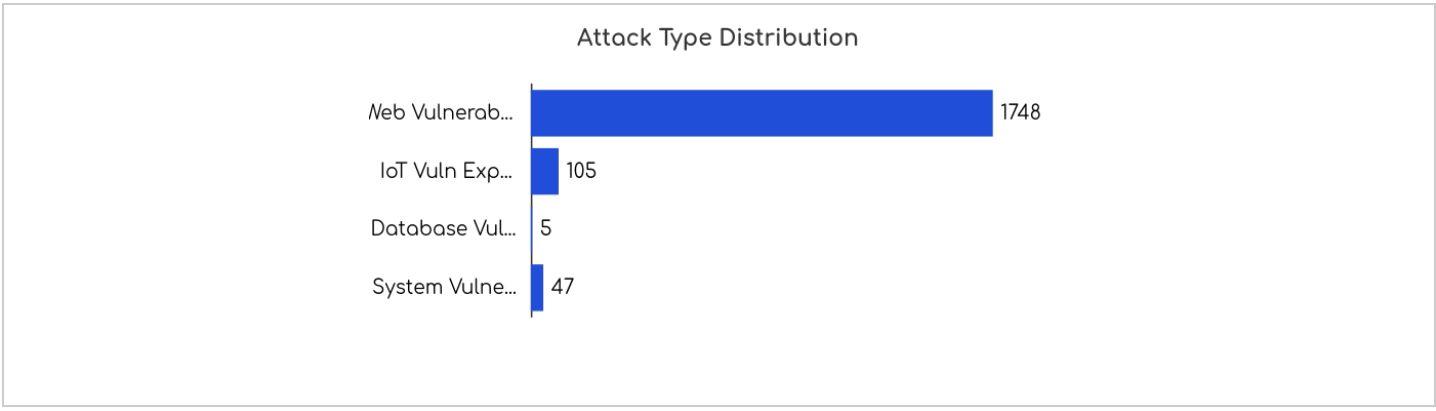
3. Blacklist Attacker IP

- To prevent subsequent attacks from the above sources, log in to the Network Secure Firewall manager and blacklist above IP addresses in SOC > Blacklist/Whitelist > Blacklist.

2.11 10.0.0.240 Security Details (To be Fixed)

10.0.0.240 Overall security rating: Attacked

10.0.0.240 suffered 1905 attack(s)



2.11.1 Attack Events

Category	Ever been attacked
Summary	10.0.0.240 has been attacked by 18.142.219.158(Singapore, 321 occurrences), Web Vulnerability (287), System Vulnerability (18), IoT Vuln Exploit (14)
Details	Start Time: 2025-11-27 17:42:18 End Time: 2025-11-27 22:42:07 More logs are available in Monitor > Logs > Security Logs > Web Application, Intrusion Prevention, Website Browsing > Email Protection in Network Secure Firewall GUI.

Category	Ever been attacked
Summary	10.0.0.240 has been attacked by 47.90.162.76(United States, 161 occurrences), System Vulnerability (18), IoT Vuln Exploit (10)
Details	Start Time: 2025-12-03 01:39:29 End Time: 2025-12-03 23:50:48 More logs are available in Monitor > Logs > Security Logs > Web Application, Intrusion Prevention, Website Browsing > Email Protection in Network Secure Firewall GUI.

Category	Ever been attacked
Summary	10.0.0.240 has been attacked by 47.90.162.76(United States, 131 occurrences), Web Vulnerability (261)
Details	Start Time: 2025-12-04 00:05:27 End Time: 2025-12-04 23:27:02 More logs are available in Monitor > Logs > Security Logs > Web Application, Intrusion Prevention, Website Browsing > Email Protection in Network Secure Firewall GUI.

Failed to render report. Please try again later.

2.11.2 Vulnerabilities

No data available

2.11.3 Attack Sources

The following are the major sources launched attacks against 10.0.0.240, 1905 attacks in total. You are recommended to blacklist in SOC > Blacklist/Whitelist > Blacklist.

No.	Attack Source	Attack Type	Source Location	Attack Count
1	47.90.162.76	Web Vulnerability(439) IoT Vuln Exploit(23) System Vulnerability(18) Database Vulnerability(3)	United States	483
2	123.143.114.188	Web Vulnerability(426)	South Korea	426
3	18.142.219.158	Web Vulnerability(287) System Vulnerability(18) IoT Vuln Exploit(14) Database Vulnerability(2)	Singapore	321
4	103.179.173.163	Web Vulnerability(87)	Viet Nam	87
5	192.159.99.95	Web Vulnerability(44) IoT Vuln Exploit(14) System Vulnerability(6)	United States	64

2.11.4 Security Enhancement Recommendations

The server has been attacked. Follow the recommendations below to enhance security.

1. Status

- Add a corresponding policy to protect the server and then click on the flag icon to change Action status (to Action has been taken) in SOC > Business Asset Security > Summary.

2. Attacked

- All the attacks against the server have been blocked by Sangfor Network Secure Firewall and vulnerabilities have been fixed. No more action is required.

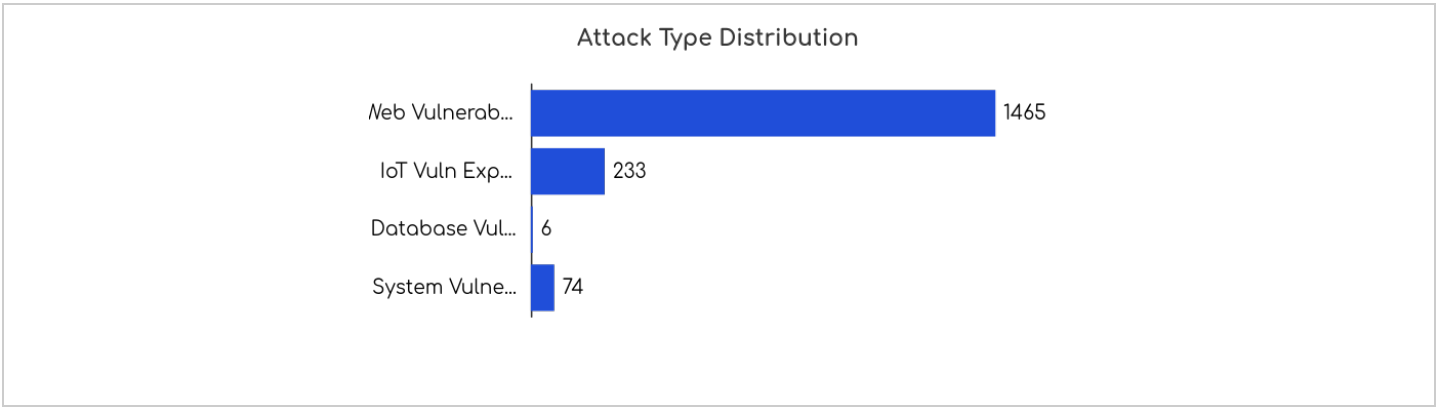
3. Blacklist Attacker IP

- To prevent subsequent attacks from the above sources, log in to the Network Secure Firewall manager and blacklist above IP addresses in SOC > Blacklist/Whitelist > Blacklist.

2.12 10.172.168.11 Security Details (To be Fixed)

10.172.168.11 Overall security rating: Attacked

10.172.168.11 suffered 1778 attack(s)



2.12.1 Attack Events

Category	Ever been attacked
Summary	10.172.168.11 has been attacked by 47.90.162.76(United States, 313 occurrences), System Vulnerability (54)
Details	Start Time: 2025-12-03 00:43:51 End Time: 2025-12-03 21:26:46 More logs are available in Monitor > Logs > Security Logs > Web Application, Intrusion Prevention, Website Browsing > Email Protection in Network Secure Firewall GUI.

Category	Ever been attacked
Summary	10.172.168.11 has been attacked by 47.90.162.76(United States, 253 occurrences), IoT Vuln Exploit (24)
Details	Start Time: 2025-12-04 00:09:50 End Time: 2025-12-04 23:35:44 More logs are available in Monitor > Logs > Security Logs > Web Application, Intrusion Prevention, Website Browsing > Email Protection in Network Secure Firewall GUI.

Category	Ever been attacked
Summary	10.172.168.11 has been attacked by 47.90.162.76(United States, 169 occurrences), Web Vulnerability (651)
Details	Start Time: 2025-12-02 17:15:08 End Time: 2025-12-02 23:50:33 More logs are available in Monitor > Logs > Security Logs > Web Application, Intrusion Prevention, Website Browsing > Email Protection in Network Secure Firewall GUI.

2.12.2 Vulnerabilities

No data available

2.12.3 Attack Sources

The following are the major sources launched attacks against 10.172.168.11, 1778 attacks in total. You are recommended to blacklist in SOC > Blacklist/Whitelist > Blacklist.

No.	Attack Source	Attack Type	Source Location	Attack Count
1	47.90.162.76	Web Vulnerability(766) System Vulnerability(54) IoT Vuln Exploit(42) Database Vulnerability(6)	United States	868
2	192.159.99.95	Web Vulnerability(120) IoT Vuln Exploit(48) System Vulnerability(20)	United States	188
3	79.124.40.174	Web Vulnerability(138) IoT Vuln Exploit(46)	Bulgaria	184
4	103.179.173.163	Web Vulnerability(52)	Viet Nam	52
5	18.142.219.158	Web Vulnerability(46)	Singapore	46

2.12.4 Security Enhancement Recommendations

The server has been attacked. Follow the recommendations below to enhance security.

1. Status

- Add a corresponding policy to protect the server and then click on the flag icon to change Action status (to Action has been taken) in SOC > Business Asset Security > Summary.

2. Attacked

- All the attacks against the server have been blocked by Sangfor Network Secure Firewall and vulnerabilities have been fixed. No more action is required.

3. Blacklist Attacker IP

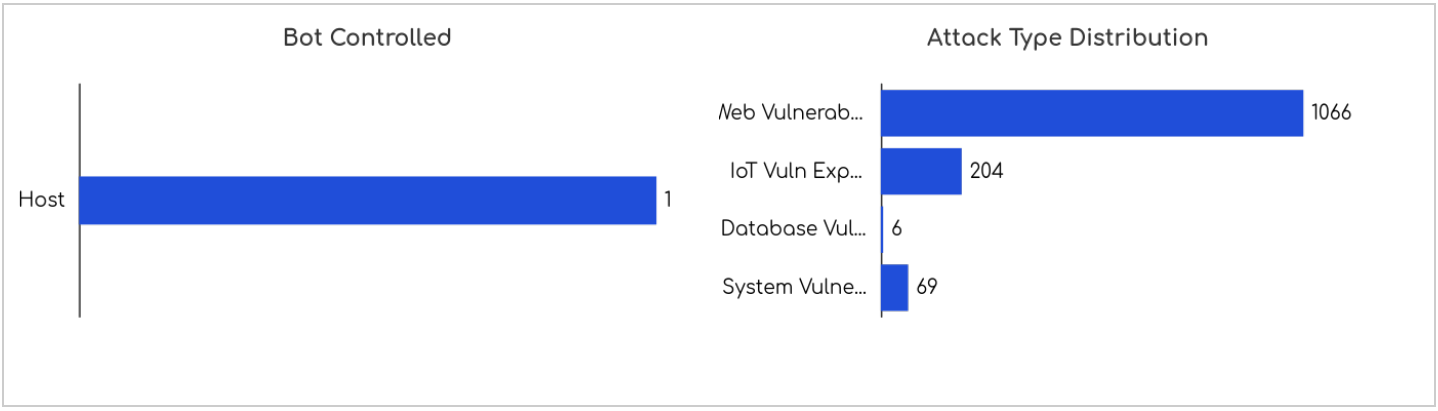
- To prevent subsequent attacks from the above sources, log in to the Network Secure Firewall manager and blacklist above IP addresses in SOC > Blacklist/Whitelist > Blacklist.

2.13 10.172.168.15 Security Details (To be Fixed)

10.172.168.15 Overall security rating: Compromised

10.172.168.15 is controlled by an attacker and has suffered 1346 attack(s)

Failed to render report. Please try again later.



2.13.1 Attack Events

Category	Bot controlled
Summary	10.172.168.15 has been controlled remotely by an attacker and become a zombie.
Details	2025-12-19 23:35:56 Through the cloud-based engine, it is detected that the internal host (10.172.168.15) is trying to communicate with the malicious IP address (176.117.107.94:80).. (1 occurrence(s))

2.13.2 Vulnerabilities

No data available

2.13.3 Attack Sources

The following are the major sources launched attacks against 10.172.168.15, 1346 attacks in total. You are recommended to blacklist in SOC > Blacklist/Whitelist > Blacklist.

No.	Attack Source	Attack Type	Source Location	Attack Count
1	47.90.162.76	Web Vulnerability(261) System Vulnerability(18) IoT Vuln Exploit(14) Database Vulnerability(2)	United States	295
2	18.142.219.158	Web Vulnerability(233) System Vulnerability(18) IoT Vuln Exploit(14) Database Vulnerability(2)	Singapore	267
3	79.124.40.174	Web Vulnerability(126) IoT Vuln Exploit(42)	Bulgaria	168
4	192.159.99.95	Web Vulnerability(90) IoT Vuln Exploit(36) System Vulnerability(15)	United States	141

No.	Attack Source	Attack Type	Source Location	Attack Count
5	146.88.129.134	Web Vulnerability(111) System Vulnerability(18) IoT Vuln Exploit(6) Database Vulnerability(2)	Japan	137

2.13.4 Security Enhancement Recommendations

The server has been attacked. Follow the recommendations below to enhance security.

1. Status

- Add a corresponding policy to protect the server and then click on the flag icon to change Action status (to Action has been taken) in SOC > Business Asset Security > Summary.

2. Bot Controlled

- Download anti-malware software to scan for and remove malware on the infected host. (Download anti-malware software: http://sec.sangfor.com/apt)

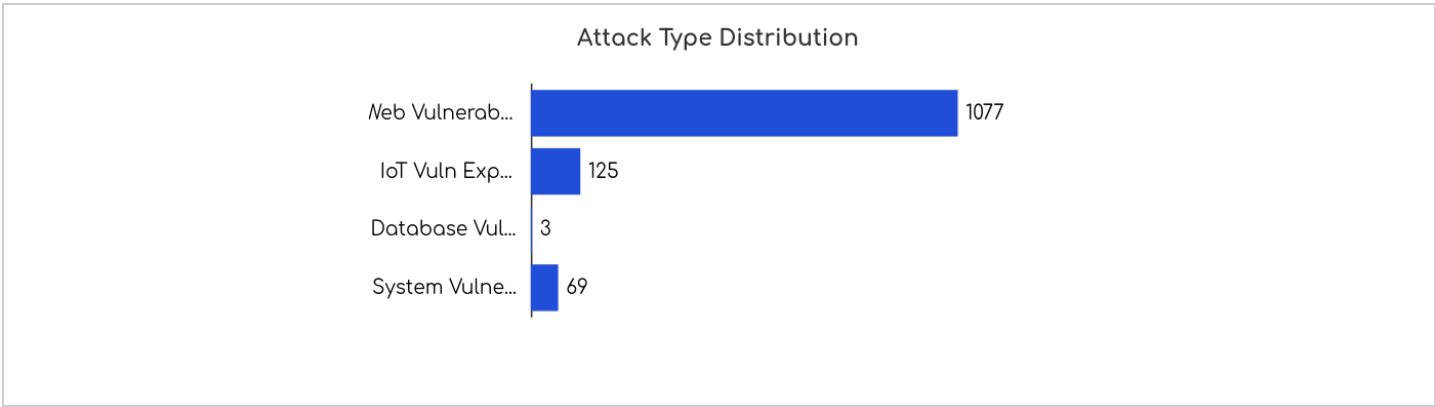
3. Blacklist Attacker IP

- To prevent subsequent attacks from the above sources, log in to the Network Secure Firewall manager and blacklist above IP addresses in SOC > Blacklist/Whitelist > Blacklist.

2.14 10.0.0.115 Security Details (To be Fixed)

10.0.0.115 Overall security rating: Attacked

10.0.0.115 suffered 1274 attack(s)



2.14.1 Attack Events

Category	Ever been attacked
Summary	10.0.0.115 has been attacked by 47.90.162.76(United States, 345 occurrences), System Vulnerability (54), IoT Vuln Exploit (24)

Failed to render report. Please try again later.

Details	Start Time: 2025-12-03 00:21:46 End Time: 2025-12-03 23:59:53 More logs are available in Monitor > Logs > Security Logs > Web Application, Intrusion Prevention, Website Browsing > Email Protection in Network Secure Firewall GUI.

Category	Ever been attacked
Summary	10.0.0.115 has been attacked by 47.90.162.76(United States, 293 occurrences)
Details	Start Time: 2025-12-04 00:38:33 End Time: 2025-12-04 23:27:18 More logs are available in Monitor > Logs > Security Logs > Web Application, Intrusion Prevention, Website Browsing > Email Protection in Network Secure Firewall GUI.

Category	Ever been attacked
Summary	10.0.0.115 has been attacked by 47.90.162.76(United States, 146 occurrences), Web Vulnerability (703)
Details	Start Time: 2025-12-02 17:00:15 End Time: 2025-12-02 20:36:11 More logs are available in Monitor > Logs > Security Logs > Web Application, Intrusion Prevention, Website Browsing > Email Protection in Network Secure Firewall GUI.

2.14.2 Vulnerabilities

No data available

2.14.3 Attack Sources

The following are the major sources launched attacks against 10.0.0.115, 1274 attacks in total. You are recommended to blacklist in SOC > Blacklist/Whitelist > Blacklist.

No.	Attack Source	Attack Type	Source Location	Attack Count
1	47.90.162.76	Web Vulnerability(853) System Vulnerability(54) IoT Vuln Exploit(48) Database Vulnerability(3)	United States	958

No.	Attack Source	Attack Type	Source Location	Attack Count
2	192.159.99.95	Web Vulnerability(90) IoT Vuln Exploit(42) System Vulnerability(15)	United States	147
3	18.142.219.158	Web Vulnerability(40)	Singapore	40
4	147.182.166.6	Web Vulnerability(16)	United States	16
5	193.34.213.150	Web Vulnerability(9)	Poland	9

2.14.4 Security Enhancement Recommendations

The server has been attacked. Follow the recommendations below to enhance security.

1. Status

- Add a corresponding policy to protect the server and then click on the flag icon to change Action status (to Action has been taken) in SOC > Business Asset Security > Summary.

2. Attacked

- All the attacks against the server have been blocked by Sangfor Network Secure Firewall and vulnerabilities have been fixed. No more action is required.

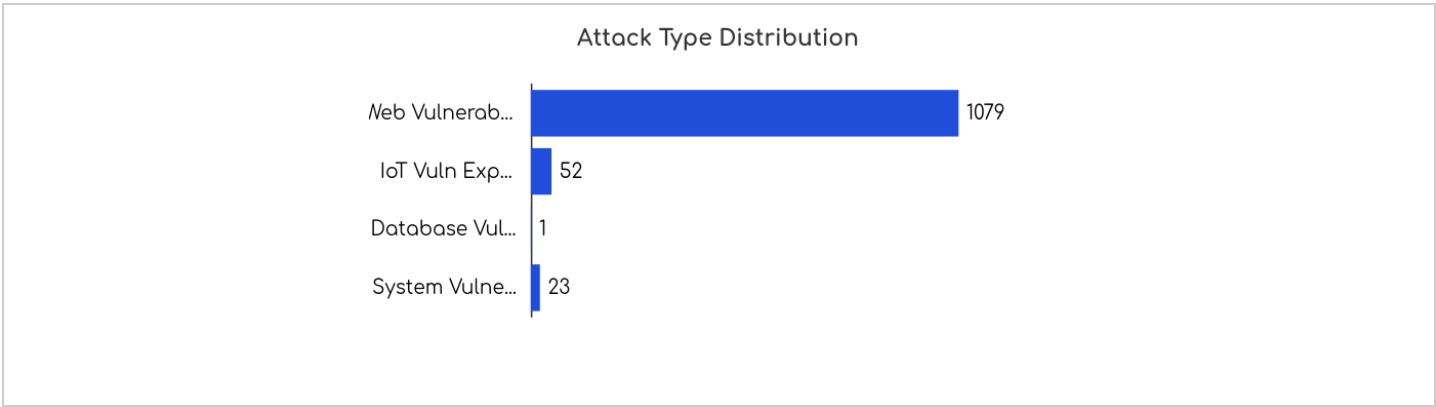
3. Blacklist Attacker IP

- To prevent subsequent attacks from the above sources, log in to the Network Secure Firewall manager and blacklist above IP addresses in SOC > Blacklist/Whitelist > Blacklist.

2.15 10.0.0.155 Security Details (To be Fixed)

10.0.0.155 Overall security rating: Attacked

10.0.0.155 suffered 1155 attack(s)



2.15.1 Attack Events

Category	Ever been attacked
Summary	10.0.0.155 has been attacked by 157.15.40.91(Indonesia, 498 occurrences), Web Vulnerability (498)

Failed to render report. Please try again later.

Details	Start Time: 2025-11-26 10:17:41 End Time: 2025-11-26 15:50:00 More logs are available in Monitor > Logs > Security Logs > Web Application, Intrusion Prevention, Website Browsing > Email Protection in Network Secure Firewall GUI.

Category	Ever been attacked
Summary	10.0.0.155 has been attacked by 47.90.162.76(United States, 103 occurrences), Web Vulnerability (160), System Vulnerability (18), IoT Vuln Exploit (8)
Details	Start Time: 2025-12-03 00:58:38 End Time: 2025-12-03 19:19:14 More logs are available in Monitor > Logs > Security Logs > Web Application, Intrusion Prevention, Website Browsing > Email Protection in Network Secure Firewall GUI.

Category	Ever been attacked
Summary	10.0.0.155 has been attacked by 47.90.162.76(United States, 84 occurrences)
Details	Start Time: 2025-12-04 00:20:36 End Time: 2025-12-04 23:46:35 More logs are available in Monitor > Logs > Security Logs > Web Application, Intrusion Prevention, Website Browsing > Email Protection in Network Secure Firewall GUI.

2.15.2 Vulnerabilities

No data available

2.15.3 Attack Sources

The following are the major sources launched attacks against 10.0.0.155, 1155 attacks in total. You are recommended to blacklist in SOC > Blacklist/Whitelist > Blacklist.

No.	Attack Source	Attack Type	Source Location	Attack Count
1	157.15.40.91	Web Vulnerability(498)	Indonesia	498
2	47.90.162.76	Web Vulnerability(256) System Vulnerability(18) IoT Vuln Exploit(14) Database Vulnerability(1)	United States	289
3	165.22.53.159	Web Vulnerability(52)	Singapore	52

Failed to render report. Please try again later.

No.	Attack Source	Attack Type	Source Location	Attack Count
4	192.159.99.95	Web Vulnerability(30) IoT Vuln Exploit(12) System Vulnerability(5)	United States	47
5	18.142.219.158	Web Vulnerability(38)	Singapore	38

2.15.4 Security Enhancement Recommendations

The server has been attacked. Follow the recommendations below to enhance security.

1. Status

- Add a corresponding policy to protect the server and then click on the flag icon to change Action status (to Action has been taken) in SOC > Business Asset Security > Summary.

2. Attacked

- All the attacks against the server have been blocked by Sangfor Network Secure Firewall and vulnerabilities have been fixed. No more action is required.

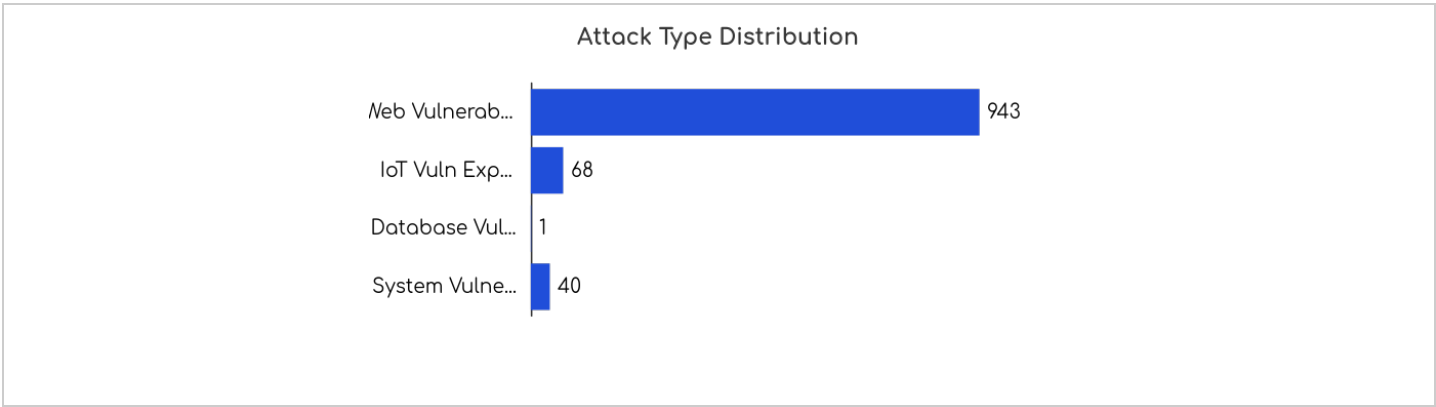
3. Blacklist Attacker IP

- To prevent subsequent attacks from the above sources, log in to the Network Secure Firewall manager and blacklist above IP addresses in SOC > Blacklist/Whitelist > Blacklist.

2.16 10.0.0.164 Security Details (To be Fixed)

10.0.0.164 Overall security rating: Attacked

10.0.0.164 suffered 1052 attack(s)



2.16.1 Attack Events

Category	Ever been attacked
Summary	10.0.0.164 has been attacked by 47.90.162.76(United States, 206 occurrences), Web Vulnerability (388), System Vulnerability (36)

Failed to render report. Please try again later.

Details	Start Time: 2025-12-03 01:07:46 End Time: 2025-12-03 19:29:11 More logs are available in Monitor > Logs > Security Logs > Web Application, Intrusion Prevention, Website Browsing > Email Protection in Network Secure Firewall GUI.

Category	Ever been attacked
Summary	10.0.0.164 has been attacked by 47.90.162.76(United States, 159 occurrences), IoT Vuln Exploit (12)
Details	Start Time: 2025-12-04 00:28:01 End Time: 2025-12-04 23:55:34 More logs are available in Monitor > Logs > Security Logs > Web Application, Intrusion Prevention, Website Browsing > Email Protection in Network Secure Firewall GUI.

Category	Ever been attacked
Summary	10.0.0.164 has been attacked by 47.90.162.76(United States, 72 occurrences)
Details	Start Time: 2025-12-02 17:31:42 End Time: 2025-12-02 22:13:19 More logs are available in Monitor > Logs > Security Logs > Web Application, Intrusion Prevention, Website Browsing > Email Protection in Network Secure Firewall GUI.

2.16.2 Vulnerabilities

No data available

2.16.3 Attack Sources

The following are the major sources launched attacks against 10.0.0.164, 1052 attacks in total. You are recommended to blacklist in SOC > Blacklist/Whitelist > Blacklist.

No.	Attack Source	Attack Type	Source Location	Attack Count
1	47.90.162.76	Web Vulnerability(461) System Vulnerability(36) IoT Vuln Exploit(20) Database Vulnerability(1)	United States	518
2	123.143.114.188	Web Vulnerability(319)	South Korea	319

Failed to render report. Please try again later.

No.	Attack Source	Attack Type	Source Location	Attack Count
3	192.159.99.95	Web Vulnerability(30) IoT Vuln Exploit(11) System Vulnerability(4)	United States	45
4	47.79.123.30	Web Vulnerability(28)	Singapore	28
5	165.22.96.47	Web Vulnerability(26)	Singapore	26

2.16.4 Security Enhancement Recommendations

The server has been attacked. Follow the recommendations below to enhance security.

1. Status

- Add a corresponding policy to protect the server and then click on the flag icon to change Action status (to Action has been taken) in SOC > Business Asset Security > Summary.

2. Attacked

- All the attacks against the server have been blocked by Sangfor Network Secure Firewall and vulnerabilities have been fixed. No more action is required.

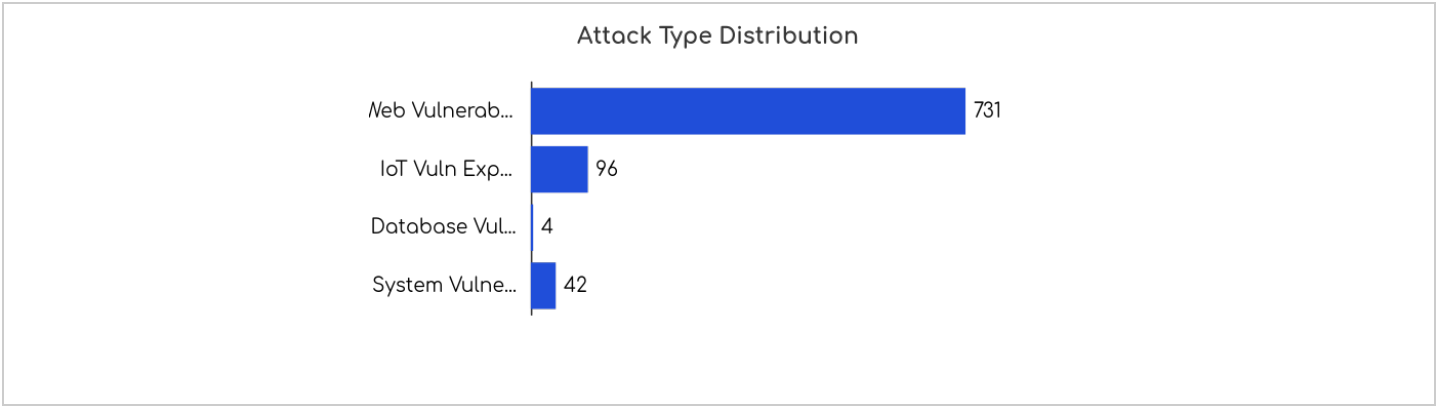
3. Blacklist Attacker IP

- To prevent subsequent attacks from the above sources, log in to the Network Secure Firewall manager and blacklist above IP addresses in SOC > Blacklist/Whitelist > Blacklist.

2.17 10.0.0.73 Security Details (To be Fixed)

10.0.0.73 Overall security rating: Attacked

10.0.0.73 suffered 873 attack(s)



2.17.1 Attack Events

Category	Ever been attacked
Summary	10.0.0.73 has been attacked by 47.90.162.76(United States, 216 occurrences), Web Vulnerability (391), System Vulnerability (36), IoT Vuln Exploit (16)

Details	Start Time: 2025-12-03 00:52:56 End Time: 2025-12-03 20:18:51 More logs are available in Monitor > Logs > Security Logs > Web Application, Intrusion Prevention, Website Browsing > Email Protection in Network Secure Firewall GUI.

Category	Ever been attacked
Summary	10.0.0.73 has been attacked by 47.90.162.76(United States, 159 occurrences)
Details	Start Time: 2025-12-04 00:16:13 End Time: 2025-12-04 23:41:39 More logs are available in Monitor > Logs > Security Logs > Web Application, Intrusion Prevention, Website Browsing > Email Protection in Network Secure Firewall GUI.

Category	Ever been attacked
Summary	10.0.0.73 has been attacked by 47.90.162.76(United States, 72 occurrences)
Details	Start Time: 2025-12-02 17:21:02 End Time: 2025-12-02 19:37:53 More logs are available in Monitor > Logs > Security Logs > Web Application, Intrusion Prevention, Website Browsing > Email Protection in Network Secure Firewall GUI.

2.17.2 Vulnerabilities

No data available

2.17.3 Attack Sources

The following are the major sources launched attacks against 10.0.0.73, 873 attacks in total. You are recommended to blacklist in SOC > Blacklist/Whitelist > Blacklist.

No.	Attack Source	Attack Type	Source Location	Attack Count
1	47.90.162.76	Web Vulnerability(462) System Vulnerability(36) IoT Vuln Exploit(29) Database Vulnerability(4)	United States	531
2	103.179.173.163	Web Vulnerability(59)	Viet Nam	59

No.	Attack Source	Attack Type	Source Location	Attack Count
3	192.159.99.95	Web Vulnerability(36) IoT Vuln Exploit(12) System Vulnerability(6)	United States	54
4	193.34.213.150	Web Vulnerability(18)	Poland	18
5	178.128.0.135	Web Vulnerability(14)	United States	14

2.17.4 Security Enhancement Recommendations

The server has been attacked. Follow the recommendations below to enhance security.

1. Status

- Add a corresponding policy to protect the server and then click on the flag icon to change Action status (to Action has been taken) in SOC > Business Asset Security > Summary.

2. Attacked

- All the attacks against the server have been blocked by Sangfor Network Secure Firewall and vulnerabilities have been fixed. No more action is required.

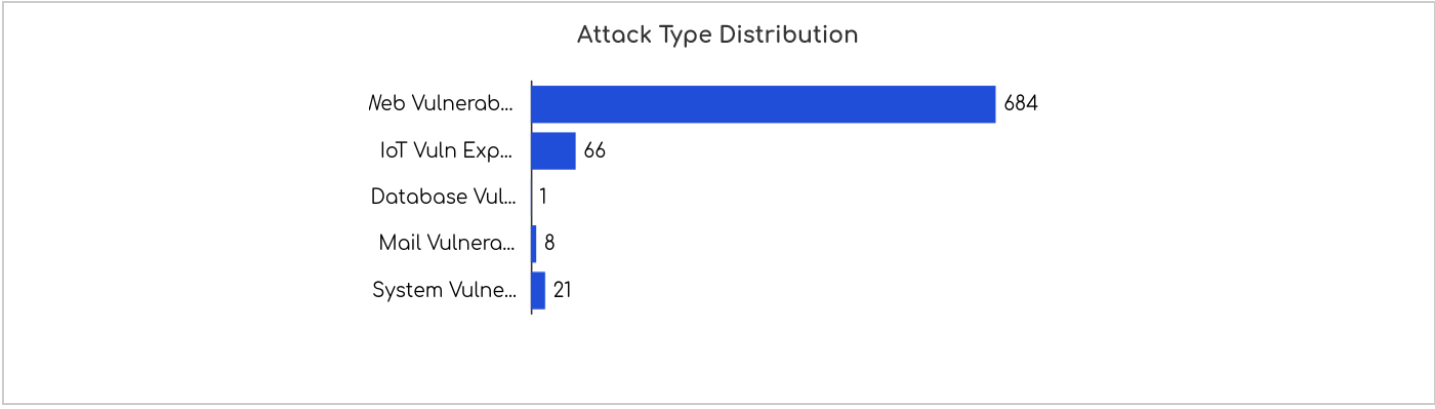
3. Blacklist Attacker IP

- To prevent subsequent attacks from the above sources, log in to the Network Secure Firewall manager and blacklist above IP addresses in SOC > Blacklist/Whitelist > Blacklist.

2.18 10.98.0.58 Security Details (To be Fixed)

10.98.0.58 Overall security rating: Attacked

10.98.0.58 suffered 780 attack(s)



2.18.1 Attack Events

Category	Ever been attacked
Summary	10.98.0.58 has been attacked by 47.90.162.76(United States, 114 occurrences), System Vulnerability (18)

Details	Start Time: 2025-12-03 01:39:38 End Time: 2025-12-03 20:05:48 More logs are available in Monitor > Logs > Security Logs > Web Application, Intrusion Prevention, Website Browsing > Email Protection in Network Secure Firewall GUI.

Category	Ever been attacked
Summary	10.98.0.58 has been attacked by 47.90.162.76(United States, 76 occurrences), IoT Vuln Exploit (6)
Details	Start Time: 2025-12-04 00:52:50 End Time: 2025-12-04 23:27:09 More logs are available in Monitor > Logs > Security Logs > Web Application, Intrusion Prevention, Website Browsing > Email Protection in Network Secure Firewall GUI.

Category	Ever been attacked
Summary	10.98.0.58 has been attacked by 47.90.162.76(United States, 51 occurrences), Web Vulnerability (214)
Details	Start Time: 2025-12-10 11:57:21 End Time: 2025-12-10 23:31:16 More logs are available in Monitor > Logs > Security Logs > Web Application, Intrusion Prevention, Website Browsing > Email Protection in Network Secure Firewall GUI.

2.18.2 Vulnerabilities

No data available

2.18.3 Attack Sources

The following are the major sources launched attacks against 10.98.0.58, 780 attacks in total. You are recommended to blacklist in SOC > Blacklist/Whitelist > Blacklist.

No.	Attack Source	Attack Type	Source Location	Attack Count
1	47.90.162.76	Web Vulnerability(434) IoT Vuln Exploit(28) System Vulnerability(20) Mail Vulnerability(4) Database Vulnerability(1)	United States	487

No.	Attack Source	Attack Type	Source Location	Attack Count
2	51.210.216.192	Web Vulnerability(54) Mail Vulnerability(4)	Switzerland	58
3	79.124.40.174	Web Vulnerability(41) IoT Vuln Exploit(14)	Bulgaria	55
4	123.143.114.188	Web Vulnerability(48)	South Korea	48
5	47.79.123.30	Web Vulnerability(20)	Singapore	20

2.18.4 Security Enhancement Recommendations

The server has been attacked. Follow the recommendations below to enhance security.

1. Status

- Add a corresponding policy to protect the server and then click on the flag icon to change Action status (to Action has been taken) in SOC > Business Asset Security > Summary.

2. Attacked

- All the attacks against the server have been blocked by Sangfor Network Secure Firewall and vulnerabilities have been fixed. No more action is required.

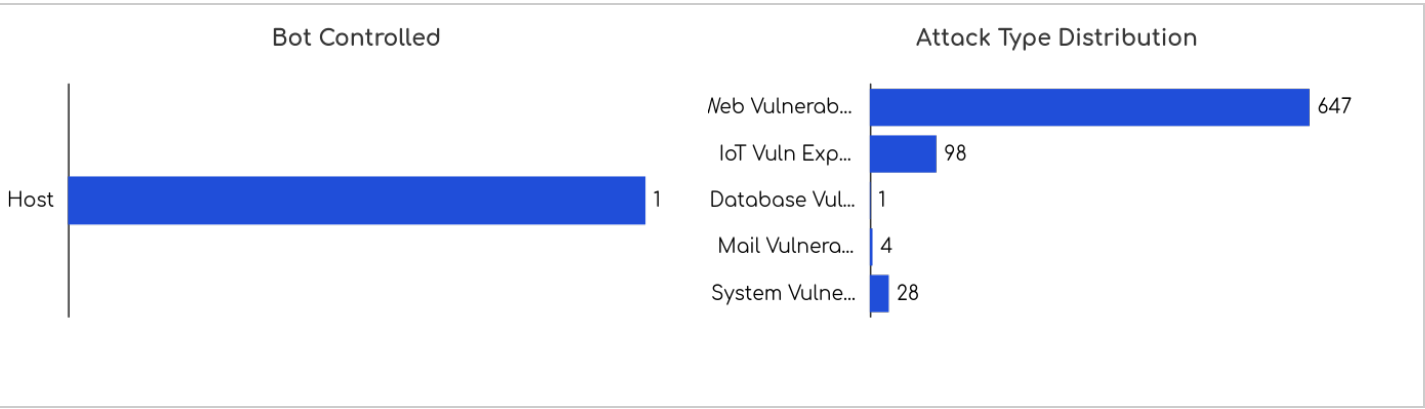
3. Blacklist Attacker IP

- To prevent subsequent attacks from the above sources, log in to the Network Secure Firewall manager and blacklist above IP addresses in SOC > Blacklist/Whitelist > Blacklist.

2.19 10.98.0.53 Security Details (To be Fixed)

10.98.0.53 Overall security rating: Compromised

10.98.0.53 is controlled by an attacker and has suffered 779 attack(s)



2.19.1 Attack Events

Category	Bot controlled
Summary	10.98.0.53 has been controlled remotely by an attacker and become a zombie.

Failed to render report. Please try again later.

Details	2025-11-28 16:53:56 Through the cloud-based engine, it is detected that the internal host (10.98.0.53) is trying to communicate with the malicious IP address (143.20.185.93:41354).. (1 occurrence(s))

2.19.2 Vulnerabilities

No data available

2.19.3 Attack Sources

The following are the major sources launched attacks against 10.98.0.53, 779 attacks in total. You are recommended to blacklist in SOC > Blacklist/Whitelist > Blacklist.

No.	Attack Source	Attack Type	Source Location	Attack Count
1	47.90.162.76	Web Vulnerability(410) IoT Vuln Exploit(26) System Vulnerability(20) Mail Vulnerability(4) Database Vulnerability(1)	United States	461
2	192.159.99.95	Web Vulnerability(46) IoT Vuln Exploit(18) System Vulnerability(8)	United States	72
3	18.142.219.158	Web Vulnerability(40)	Singapore	40
4	79.124.40.174	Web Vulnerability(25)	Bulgaria	25
5	193.34.213.150	Web Vulnerability(18)	Poland	18

2.19.4 Security Enhancement Recommendations

The server has been attacked. Follow the recommendations below to enhance security.

1. Status

- Add a corresponding policy to protect the server and then click on the flag icon to change Action status (to Action has been taken) in SOC > Business Asset Security > Summary.

2. Bot Controlled

- Download anti-malware software to scan for and remove malware on the infected host. (Download anti-malware software: http://sec.sangfor.com/apt)

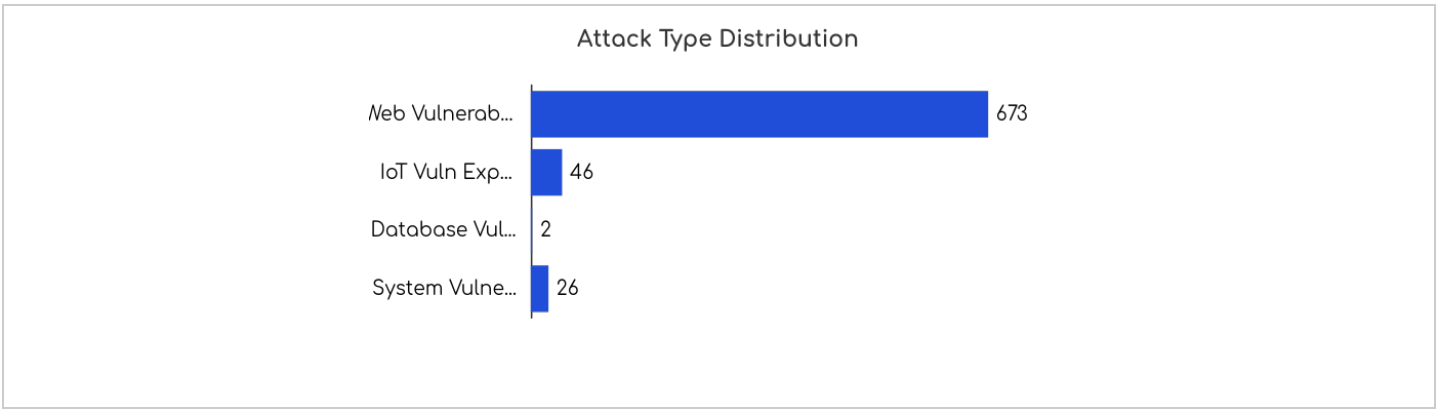
3. Blacklist Attacker IP

- To prevent subsequent attacks from the above sources, log in to the Network Secure Firewall manager and blacklist above IP addresses in SOC > Blacklist/Whitelist > Blacklist.

2.20 10.0.0.217 Security Details (To be Fixed)

10.0.0.217 Overall security rating: Attacked

10.0.0.217 suffered 747 attack(s)



2.20.1 Attack Events

Category	Ever been attacked
Summary	10.0.0.217 has been attacked by 47.90.162.76(United States, 103 occurrences), System Vulnerability (18), IoT Vuln Exploit (8)
Details	Start Time: 2025-12-03 00:58:53 End Time: 2025-12-03 19:19:24 More logs are available in Monitor > Logs > Security Logs > Web Application, Intrusion Prevention, Website Browsing > Email Protection in Network Secure Firewall GUI.

Category	Ever been attacked
Summary	10.0.0.217 has been attacked by 47.90.162.76(United States, 83 occurrences), Web Vulnerability (198)
Details	Start Time: 2025-12-04 00:20:48 End Time: 2025-12-04 23:46:46 More logs are available in Monitor > Logs > Security Logs > Web Application, Intrusion Prevention, Website Browsing > Email Protection in Network Secure Firewall GUI.

Category	Ever been attacked
Summary	10.0.0.217 has been attacked by 47.90.162.76(United States, 40 occurrences)

Failed to render report. Please try again later.

Details	Start Time: 2025-12-02 17:25:13 End Time: 2025-12-02 20:37:41 More logs are available in Monitor > Logs > Security Logs > Web Application, Intrusion Prevention, Website Browsing > Email Protection in Network Secure Firewall GUI.

2.20.2 Vulnerabilities

No data available

2.20.3 Attack Sources

The following are the major sources launched attacks against 10.0.0.217, 747 attacks in total. You are recommended to blacklist in SOC > Blacklist/Whitelist > Blacklist.

No.	Attack Source	Attack Type	Source Location	Attack Count
1	47.90.162.76	Web Vulnerability(239) System Vulnerability(18) IoT Vuln Exploit(14) Database Vulnerability(2)	United States	273
2	123.143.114.188	Web Vulnerability(200)	South Korea	200
3	103.179.173.163	Web Vulnerability(52)	Viet Nam	52
4	18.142.219.158	Web Vulnerability(40)	Singapore	40
5	192.159.99.95	Web Vulnerability(18) IoT Vuln Exploit(6) System Vulnerability(3)	United States	27

2.20.4 Security Enhancement Recommendations

The server has been attacked. Follow the recommendations below to enhance security.

1. Status

- Add a corresponding policy to protect the server and then click on the flag icon to change Action status (to Action has been taken) in SOC > Business Asset Security > Summary.

2. Attacked

- All the attacks against the server have been blocked by Sangfor Network Secure Firewall and vulnerabilities have been fixed. No more action is required.

3. Blacklist Attacker IP

- To prevent subsequent attacks from the above sources, log in to the Network Secure Firewall manager and blacklist above IP addresses in SOC > Blacklist/Whitelist > Blacklist.

Failed to render report. Please try again later.

3 Endpoint Security

3.1 10.172.168.13 Security Details (To be Fixed)

Overall security rating: Compromised

10.172.168.13 has encountered 12064 threat(s), and it is in the stage of C&C Communication. Host is infected with malware and controlled by a hacker.

3.1.1 Threat Details

Event Category	C&C Communication
Details	Host visited C&C communication domain or IP address proved by CNCERT.
Description	2025-12-20 11:31:01 Attempt to parse address of malware C&C server investment1.top (12064 occurrence(s))

3.1.2 Security Enhancement Recommendations

1. Status

- Add a corresponding policy to protect the host according to the threat details and then click on the flag icon to change Action status (to Action has been taken) in SOC > User Security > Summary.

2. Compromised

- The host is infected with malware. Download anti-malware software to scan for and remove malware on the infected hosts. (Download anti-malware software: http://sec.sangfor.com/apt)

3.2 10.130.11.172 Security Details (To be Fixed)

Overall security rating: Compromised

10.130.11.172 has encountered 49 threat(s), and it is in the stage of C&C Communication. Host is infected with malware and controlled by a hacker.

3.2.1 Threat Details

Event Category	C&C Communication
Details	Host visited C&C communication domain or IP address proved by CNCERT.
Description	2025-12-03 12:32:48 Through the pioneered active detection technology, it is detected that the internal host (10.130.11.172) is trying to request for access to the address of the mining pool (195.128.248.23:83).(15 occurrence(s)) 2025-12-03 12:31:30 Through the pioneered active detection technology, it is detected that the internal host (10.130.11.172) is trying to request for access to the address of the mining pool (62.182.85.45:83).(19 occurrence(s))

Event Category	Infection
Details	Host visited link or URL to malware or Trojan, which is proved by sandbox analysis or cncert.
Description	No data available

3.2.2 Security Enhancement Recommendations

1. Status

- Add a corresponding policy to protect the host according to the threat details and then click on the flag icon to change Action status (to Action has been taken) in SOC > User Security > Summary.

2. Compromised

- The host is infected with malware. Download anti-malware software to scan for and remove malware on the infected hosts. (Download anti-malware software: http://sec.sangfor.com/apt)

3.3 10.101.1.80 Security Details (To be Fixed)

Overall security rating: Compromised

10.101.1.80 has encountered 48 threat(s), and it is in the stage of C&C Communication. Host is infected with malware and controlled by a hacker.

3.3.1 Threat Details

Event Category	C&C Communication
Details	Host visited C&C communication domain or IP address proved by CNCERT.

Description	2025-12-02 15:54:21 Through the pioneered active detection technology, it is detected that the internal host (10.101.1.80) is trying to request for access to the address of the mining pool (65.21.18.44:50003).(24 occurrence(s)) 2025-12-02 15:37:47 Through the cloud-based engine, it is detected that the internal host (10.101.1.80) is trying to communicate with the malicious IP address (103.176.197.134:445).(1 occurrence(s)) 2025-12-02 15:37:13 Through the cloud-based engine, it is detected that the internal host (10.101.1.80) is trying to communicate with the malicious IP address (103.176.197.104:445).(2 occurrence(s)) 2025-12-02 14:10:35 Through the cloud-based engine, it is detected that the internal host (10.101.1.80) is trying to communicate with the malicious IP address (103.176.197.131:445).(1 occurrence(s)) 2025-12-02 14:02:19 Through the cloud-based engine, it is detected that the internal host (10.101.1.80) is trying to communicate with the malicious IP address (34.209.195.255:443).(6 occurrence(s))

Event Category	Infection
Details	Host visited link or URL to malware or Trojan, which is proved by sandbox analysis or cncert.
Description	No data available

3.3.2 Security Enhancement Recommendations

1. Status

- Add a corresponding policy to protect the host according to the threat details and then click on the flag icon to change Action status (to Action has been taken) in SOC > User Security > Summary.

2. Compromised

- The host is infected with malware. Download anti-malware software to scan for and remove malware on the infected hosts. (Download anti-malware software: http://sec.sangfor.com/apt)

3.4 10.106.1.218 Security Details (To be Fixed)

Overall security rating: Compromised

10.106.1.218 has encountered 40 threat(s), and it is in the stage of C&C Communication. Host is infected with malware and controlled by a hacker.

3.4.1 Threat Details

Event Category	C&C Communication
Details	Host visited C&C communication domain or IP address proved by CNCERT.
Description	2025-11-27 16:18:33 Through the cloud-based engine, it is detected that the internal host (10.106.1.218) is trying to communicate with the malicious IP address (50.16.27.236:50001).(15 occurrence(s)) 2025-11-27 16:05:17 Through the cloud-based engine, it is detected that the internal host (10.106.1.218) is trying to communicate with the malicious IP address (34.209.195.255:443).(9 occurrence(s)) 2025-11-27 15:23:29 Through the pioneered active detection technology, it is detected that the internal host (10.106.1.218) is trying to request for access to the address of the mining pool (65.21.18.44:50003).(7 occurrence(s)) 2025-11-27 14:53:25 Through the cloud-based engine, it is detected that the internal host (10.106.1.218) is trying to communicate with the malicious IP address (52.27.79.221:443).(7 occurrence(s))

Event Category	Infection
Details	Host visited link or URL to malware or Trojan, which is proved by sandbox analysis or cncert.
Description	No data available

3.4.2 Security Enhancement Recommendations

1. Status

- Add a corresponding policy to protect the host according to the threat details and then click on the flag icon to change Action status (to Action has been taken) in SOC > User Security > Summary.

2. Compromised

- The host is infected with malware. Download anti-malware software to scan for and remove malware on the infected hosts. (Download anti-malware software: http://sec.sangfor.com/apt)

3.5 10.106.1.197 Security Details (To be Fixed)

Overall security rating: Compromised

10.106.1.197 has encountered 37 threat(s), and it is in the stage of C&C Communication. Host is infected with malware and controlled by a hacker.

3.5.1 Threat Details

Event Category	C&C Communication
Details	Host visited C&C communication domain or IP address proved by CNCERT.
Description	2025-12-02 15:52:16 Through the pioneered active detection technology, it is detected that the internal host (10.106.1.197) is trying to request for access to the address of the mining pool (65.21.18.44:50003).(26 occurrence(s)) 2025-12-02 14:37:36 Through the cloud-based engine, it is detected that the internal host (10.106.1.197) is trying to communicate with the malicious IP address (34.209.195.255:443).(9 occurrence(s)) 2025-12-02 14:31:16 Through the cloud-based engine, it is detected that the internal host (10.106.1.197) is trying to communicate with the malicious IP address (39.40.184.118:445).(1 occurrence(s)) 2025-12-02 13:10:26 Through the cloud-based engine, it is detected that the internal host (10.106.1.197) is trying to communicate with the malicious IP address (43.156.36.172:445).(1 occurrence(s))

3.5.2 Security Enhancement Recommendations

1. Status

- Add a corresponding policy to protect the host according to the threat details and then click on the flag icon to change Action status (to Action has been taken) in SOC > User Security > Summary.

2. Compromised

- The host is infected with malware. Download anti-malware software to scan for and remove malware on the infected hosts. (Download anti-malware software: http://sec.sangfor.com/apt)

3.6 10.130.4.22 Security Details (To be Fixed)

Overall security rating: Compromised

10.130.4.22 has encountered 37 threat(s), and it is in the stage of C&C Communication. Host is infected with malware and controlled by a hacker.

3.6.1 Threat Details

Event Category	C&C Communication
Details	Host visited C&C communication domain or IP address proved by CNCERT.

Description	2025-11-28 09:28:36 Through the cloud-based engine, it is detected that the internal host (10.130.4.22) is trying to communicate with the malicious IP address (45.14.233.248:443).(17 occurrence(s)) 2025-11-27 16:05:36 Through the pioneered active detection technology, it is detected that the internal host (10.130.4.22) is trying to request for access to the address of the mining pool (65.21.18.44:50003).(9 occurrence(s)) 2025-11-27 16:04:21 Through the cloud-based engine, it is detected that the internal host (10.130.4.22) is trying to communicate with the malicious IP address (50.16.27.236:50001).(7 occurrence(s)) 2025-11-27 15:27:09 Through the cloud-based engine, it is detected that the internal host (10.130.4.22) is trying to communicate with the malicious IP address (107.189.5.121:9000).(4 occurrence(s))

3.6.2 Security Enhancement Recommendations

1. Status

- Add a corresponding policy to protect the host according to the threat details and then click on the flag icon to change Action status (to Action has been taken) in SOC > User Security > Summary.

2. Compromised

- The host is infected with malware. Download anti-malware software to scan for and remove malware on the infected hosts. (Download anti-malware software: http://sec.sangfor.com/apt)

3.7 10.130.6.251 Security Details (To be Fixed)

Overall security rating: Compromised

10.130.6.251 has encountered 36 threat(s), and it is in the stage of C&C Communication. Host is infected with malware and controlled by a hacker.

3.7.1 Threat Details

Event Category	C&C Communication
Details	Host visited C&C communication domain or IP address proved by CNCERT.

Description	2025-12-17 15:17:57 Through the cloud-based engine, it is detected that the internal host (10.130.6.251) is trying to communicate with the malicious IP address (103.208.230.9:12467).(1 occurrence(s)) 2025-12-17 15:08:27 Through the cloud-based engine, it is detected that the internal host (10.130.6.251) is trying to communicate with the malicious IP address (103.199.123.34:23383).(1 occurrence(s)) 2025-12-17 15:05:50 Through the cloud-based engine, it is detected that the internal host (10.130.6.251) is trying to communicate with the malicious IP address (157.15.67.24:1026).(1 occurrence(s)) 2025-12-17 15:00:45 Through the cloud-based engine, it is detected that the internal host (10.130.6.251) is trying to communicate with the malicious IP address (117.231.149.224:32950).(1 occurrence(s)) 2025-12-17 12:42:09 Through the cloud-based engine, it is detected that the internal host (10.130.6.251) is trying to communicate with the malicious IP address (175.107.0.72:30118).(1 occurrence(s))

3.7.2 Security Enhancement Recommendations

1. Status

- Add a corresponding policy to protect the host according to the threat details and then click on the flag icon to change Action status (to Action has been taken) in SOC > User Security > Summary.

2. Compromised

- The host is infected with malware. Download anti-malware software to scan for and remove malware on the infected hosts. (Download anti-malware software: http://sec.sangfor.com/apt)

3.8 10.130.3.108 Security Details (To be Fixed)

Overall security rating: Compromised

10.130.3.108 has encountered 34 threat(s), and it is in the stage of C&C Communication. Host is infected with malware and controlled by a hacker.

3.8.1 Threat Details

Event Category	C&C Communication
Details	Host visited C&C communication domain or IP address proved by CNCERT.

Description	2025-12-03 14:14:47 Through the pioneered active detection technology, it is detected that the internal host (10.130.3.108) is trying to request for access to the address of the mining pool (47.76.118.67:55530).(23 occurrence(s)) 2025-12-03 13:25:17 Through the cloud-based engine, it is detected that the internal host (10.130.3.108) is trying to communicate with the malicious IP address (85.17.70.38:55530).(2 occurrence(s)) 2025-12-02 16:23:42 Through the cloud-based engine, it is detected that the internal host (10.130.3.108) is trying to communicate with the malicious IP address (3.250.92.156:55531).(1 occurrence(s)) 2025-12-02 10:59:53 Through the pioneered active detection technology, it is detected that the internal host (10.130.3.108) is trying to request for access to the address of the mining pool (47.76.118.67:55531).(6 occurrence(s))

Event Category	Infection
Details	Host visited link or URL to malware or Trojan, which is proved by sandbox analysis or cncert.
Description	No data available

3.8.2 Security Enhancement Recommendations

1. Status

- Add a corresponding policy to protect the host according to the threat details and then click on the flag icon to change Action status (to Action has been taken) in SOC > User Security > Summary.

2. Compromised

- The host is infected with malware. Download anti-malware software to scan for and remove malware on the infected hosts. (Download anti-malware software: http://sec.sangfor.com/apt)

3.9 10.130.2.50 Security Details (To be Fixed)

Overall security rating: Compromised

10.130.2.50 has encountered 30 threat(s), and it is in the stage of C&C Communication. Host is infected with malware and controlled by a hacker.

3.9.1 Threat Details

Event Category	C&C Communication
Details	Host visited C&C communication domain or IP address proved by CNCERT.

Description	2025-12-02 15:48:19 Through the pioneered active detection technology, it is detected that the internal host (10.130.2.50) is trying to request for access to the address of the mining pool (121.127.34.158:853).(11 occurrence(s)) 2025-12-02 15:45:27 Through the pioneered active detection technology, it is detected that the internal host (10.130.2.50) is trying to request for access to the address of the mining pool (196.251.84.115:853).(6 occurrence(s)) 2025-12-02 15:39:53 Through the pioneered active detection technology, it is detected that the internal host (10.130.2.50) is trying to request for access to the address of the mining pool (185.196.11.196:853).(10 occurrence(s)) 2025-12-02 15:00:50 Through the pioneered active detection technology, it is detected that the internal host (10.130.2.50) is trying to request for access to the address of the mining pool (89.208.106.176:853).(1 occurrence(s)) 2025-12-02 13:30:55 Through the pioneered active detection technology, it is detected that the internal host (10.130.2.50) is trying to request for access to the address of the mining pool (151.243.109.31:853).(1 occurrence(s))

3.9.2 Security Enhancement Recommendations

1. Status

- Add a corresponding policy to protect the host according to the threat details and then click on the flag icon to change Action status (to Action has been taken) in SOC > User Security > Summary.

2. Compromised

- The host is infected with malware. Download anti-malware software to scan for and remove malware on the infected hosts. (Download anti-malware software: http://sec.sangfor.com/apt)

3.10 10.101.0.171 Security Details (To be Fixed)

Overall security rating: Compromised

10.101.0.171 has encountered 25 threat(s), and it is in the stage of C&C Communication. Host is infected with malware and controlled by a hacker.

3.10.1 Threat Details

Event Category	C&C Communication
Details	Host visited C&C communication domain or IP address proved by CNCERT.

Description	2025-12-11 14:36:55 Through the cloud-based engine, it is detected that the internal host (10.101.0.171) is trying to communicate with the malicious IP address (182.183.144.118:445).(1 occurrence(s)) 2025-12-11 14:24:24 Through the pioneered active detection technology, it is detected that the internal host (10.101.0.171) is trying to request for access to the address of the mining pool (156.244.1.162:445).(1 occurrence(s)) 2025-12-11 14:23:12 Through the cloud-based engine, it is detected that the internal host (10.101.0.171) is trying to communicate with the malicious IP address (182.183.134.176:445).(3 occurrence(s)) 2025-12-11 12:35:11 Through the cloud-based engine, it is detected that the internal host (10.101.0.171) is trying to communicate with the malicious IP address (154.221.17.44:445).(1 occurrence(s)) 2025-12-11 09:46:23 Attempt to parse address of malware C&C server server2.easywbdesign.com (1 occurrence(s))

3.10.2 Security Enhancement Recommendations

1. Status

- Add a corresponding policy to protect the host according to the threat details and then click on the flag icon to change Action status (to Action has been taken) in SOC > User Security > Summary.

2. Compromised

- The host is infected with malware. Download anti-malware software to scan for and remove malware on the infected hosts. (Download anti-malware software: http://sec.sangfor.com/apt)

3.11 10.106.1.136 Security Details (To be Fixed)

Overall security rating: Compromised

10.106.1.136 has encountered 22 threat(s), and it is in the stage of C&C Communication. Host is infected with malware and controlled by a hacker.

3.11.1 Threat Details

Event Category	C&C Communication
Details	Host visited C&C communication domain or IP address proved by CNCERT.

Description	2025-12-08 15:20:19 Through the pioneered active detection technology, it is detected that the internal host (10.106.1.136) is trying to request for access to the address of the mining pool (137.66.0.147:445).(1 occurrence(s)) 2025-12-08 12:42:25 Through the pioneered active detection technology, it is detected that the internal host (10.106.1.136) is trying to request for access to the address of the mining pool (65.21.18.44:50003).(20 occurrence(s)) 2025-12-08 08:36:13 Through the cloud-based engine, it is detected that the internal host (10.106.1.136) is trying to communicate with the malicious IP address (50.16.27.236:50001).(1 occurrence(s))

3.11.2 Security Enhancement Recommendations

1. Status

- Add a corresponding policy to protect the host according to the threat details and then click on the flag icon to change Action status (to Action has been taken) in SOC > User Security > Summary.

2. Compromised

- The host is infected with malware. Download anti-malware software to scan for and remove malware on the infected hosts. (Download anti-malware software: http://sec.sangfor.com/apt)

3.12 10.102.0.174 Security Details (To be Fixed)

Overall security rating: Compromised

10.102.0.174 has encountered 20 threat(s), and it is in the stage of C&C Communication. Host is infected with malware and controlled by a hacker.

3.12.1 Threat Details

Event Category	C&C Communication
Details	Host visited C&C communication domain or IP address proved by CNCERT.

Description	2025-12-19 13:24:36 Through the pioneered active detection technology, it is detected that the internal host (10.102.0.174) is trying to request for access to the address of the mining pool (137.66.27.247:445).(2 occurrence(s)) 2025-12-19 13:01:50 Through the cloud-based engine, it is detected that the internal host (10.102.0.174) is trying to communicate with the malicious IP address (103.77.214.148:445).(1 occurrence(s)) 2025-12-17 15:53:42 Through the cloud-based engine, it is detected that the internal host (10.102.0.174) is trying to communicate with the malicious IP address (103.162.24.221:445).(2 occurrence(s)) 2025-12-17 10:02:59 Through the pioneered active detection technology, it is detected that the internal host (10.102.0.174) is trying to request for access to the address of the mining pool (38.54.71.116:445).(1 occurrence(s)) 2025-12-16 12:27:27 Through the pioneered active detection technology, it is detected that the internal host (10.102.0.174) is trying to request for access to the address of the mining pool (156.244.1.162:445).(1 occurrence(s))

3.12.2 Security Enhancement Recommendations

1. Status

- Add a corresponding policy to protect the host according to the threat details and then click on the flag icon to change Action status (to Action has been taken) in SOC > User Security > Summary.

2. Compromised

- The host is infected with malware. Download anti-malware software to scan for and remove malware on the infected hosts. (Download anti-malware software: http://sec.sangfor.com/apt)

3.13 10.111.0.191 Security Details (To be Fixed)

Overall security rating: Compromised

10.111.0.191 has encountered 20 threat(s), and it is in the stage of C&C Communication. Host is infected with malware and controlled by a hacker.

3.13.1 Threat Details

Event Category	C&C Communication
Details	Host visited C&C communication domain or IP address proved by CNCERT.

Description	2025-12-18 08:16:23 Through the pioneered active detection technology, it is detected that the internal host (10.111.0.191) is trying to request for access to the address of the mining pool (193.27.90.11:443).(1 occurrence(s)) 2025-12-18 07:30:30 Through the pioneered active detection technology, it is detected that the internal host (10.111.0.191) is trying to request for access to the address of the mining pool (5.252.118.192:53).(4 occurrence(s)) 2025-12-16 14:11:27 Through the pioneered active detection technology, it is detected that the internal host (10.111.0.191) is trying to request for access to the address of the mining pool (185.196.11.196:53).(2 occurrence(s)) 2025-12-16 13:50:42 Through the pioneered active detection technology, it is detected that the internal host (10.111.0.191) is trying to request for access to the address of the mining pool (193.27.90.11:53).(3 occurrence(s)) 2025-12-16 13:49:51 Through the pioneered active detection technology, it is detected that the internal host (10.111.0.191) is trying to request for access to the address of the mining pool (212.224.93.160:53).(3 occurrence(s))

3.13.2 Security Enhancement Recommendations

1. Status

- Add a corresponding policy to protect the host according to the threat details and then click on the flag icon to change Action status (to Action has been taken) in SOC > User Security > Summary.

2. Compromised

- The host is infected with malware. Download anti-malware software to scan for and remove malware on the infected hosts. (Download anti-malware software: http://sec.sangfor.com/apt)

3.14 10.106.0.138 Security Details (To be Fixed)

Overall security rating: Compromised

10.106.0.138 has encountered 17 threat(s), and it is in the stage of C&C Communication. Host is infected with malware and controlled by a hacker.

3.14.1 Threat Details

Event Category	C&C Communication
Details	Host visited C&C communication domain or IP address proved by CNCERT.

Description	2025-12-09 14:05:11 Through the cloud-based engine, it is detected that the internal host (10.106.0.138) is trying to communicate with the malicious IP address (52.27.79.221:443).(10 occurrence(s)) 2025-12-09 13:49:07 Through the pioneered active detection technology, it is detected that the internal host (10.106.0.138) is trying to request for access to the address of the mining pool (65.21.18.44:50003).(6 occurrence(s)) 2025-12-09 10:52:37 Through the cloud-based engine, it is detected that the internal host (10.106.0.138) is trying to communicate with the malicious IP address (182.183.143.166:445).(1 occurrence(s))

3.14.2 Security Enhancement Recommendations

1. Status

- Add a corresponding policy to protect the host according to the threat details and then click on the flag icon to change Action status (to Action has been taken) in SOC > User Security > Summary.

2. Compromised

- The host is infected with malware. Download anti-malware software to scan for and remove malware on the infected hosts. (Download anti-malware software: http://sec.sangfor.com/apt)

3.15 10.106.1.135 Security Details (To be Fixed)

Overall security rating: Compromised

10.106.1.135 has encountered 17 threat(s), and it is in the stage of C&C Communication. Host is infected with malware and controlled by a hacker.

3.15.1 Threat Details

Event Category	C&C Communication
Details	Host visited C&C communication domain or IP address proved by CNCERT.

Description	2025-11-26 15:28:21 Through the cloud-based engine, it is detected that the internal host (10.106.1.135) is trying to communicate with the malicious IP address (34.209.195.255:443).(5 occurrence(s)) 2025-11-26 15:25:00 Through the cloud-based engine, it is detected that the internal host (10.106.1.135) is trying to communicate with the malicious IP address (52.27.79.221:443).(1 occurrence(s)) 2025-11-26 11:24:00 Through the cloud-based engine, it is detected that the internal host (10.106.1.135) is trying to communicate with the malicious IP address (50.16.27.236:50001).(11 occurrence(s))

3.15.2 Security Enhancement Recommendations

1. Status

- Add a corresponding policy to protect the host according to the threat details and then click on the flag icon to change Action status (to Action has been taken) in SOC > User Security > Summary.

2. Compromised

- The host is infected with malware. Download anti-malware software to scan for and remove malware on the infected hosts. (Download anti-malware software: http://sec.sangfor.com/apt)

3.16 10.106.0.168 Security Details (To be Fixed)

Overall security rating: Compromised

10.106.0.168 has encountered 17 threat(s), and it is in the stage of C&C Communication. Host is infected with malware and controlled by a hacker.

3.16.1 Threat Details

Event Category	C&C Communication
Details	Host visited C&C communication domain or IP address proved by CNCERT.

Description	2025-12-18 13:28:40 Through the pioneered active detection technology, it is detected that the internal host (10.106.0.168) is trying to request for access to the address of the mining pool (65.21.18.44:50003).(8 occurrence(s)) 2025-12-18 12:38:18 Through the cloud-based engine, it is detected that the internal host (10.106.0.168) is trying to communicate with the malicious IP address (34.209.195.255:443). (2 occurrence(s)) 2025-12-18 12:27:46 Through the cloud-based engine, it is detected that the internal host (10.106.0.168) is trying to communicate with the malicious IP address (50.16.27.236:50001).(6 occurrence(s))

Event Category	Infection
Details	Host visited link or URL to malware or Trojan, which is proved by sandbox analysis or cncert.
Description	No data available

3.16.2 Security Enhancement Recommendations

1. Status

- Add a corresponding policy to protect the host according to the threat details and then click on the flag icon to change Action status (to Action has been taken) in SOC > User Security > Summary.

2. Compromised

- The host is infected with malware. Download anti-malware software to scan for and remove malware on the infected hosts. (Download anti-malware software: http://sec.sangfor.com/apt)

3.17 10.130.11.74 Security Details (To be Fixed)

Overall security rating: Compromised

10.130.11.74 has encountered 15 threat(s), and it is in the stage of C&C Communication. Host is infected with malware and controlled by a hacker.

3.17.1 Threat Details

Event Category	C&C Communication
Details	Host visited C&C communication domain or IP address proved by CNCERT.
Description	2025-12-17 11:04:16 Attempt to parse address of malware C&C server xmrig.moneroocean.stream (12 occurrence(s))

Event Category	Infection
Details	Host visited link or URL to malware or Trojan, which is proved by sandbox analysis or cncert.
Description	No data available

3.17.2 Security Enhancement Recommendations

1. Status

- Add a corresponding policy to protect the host according to the threat details and then click on the flag icon to change Action status (to Action has been taken) in SOC > User Security > Summary.

2. Compromised

- The host is infected with malware. Download anti-malware software to scan for and remove malware on the infected hosts. (Download anti-malware software: http://sec.sangfor.com/apt)

3.18 10.102.6.134 Security Details (To be Fixed)

Overall security rating: Compromised

10.102.6.134 has encountered 15 threat(s), and it is in the stage of C&C Communication. Host is infected with malware and controlled by a hacker.

3.18.1 Threat Details

Event Category	C&C Communication
Details	Host visited C&C communication domain or IP address proved by CNCERT.

Description	2025-12-17 15:30:42 Through the cloud-based engine, it is detected that the internal host (10.102.6.134) is trying to communicate with the malicious IP address (104.244.73.190:9000). (1 occurrence(s)) 2025-12-17 12:40:32 Through the cloud-based engine, it is detected that the internal host (10.102.6.134) is trying to communicate with the malicious IP address (88.99.31.186:34746).(1 occurrence(s)) 2025-12-16 14:51:50 Through the cloud-based engine, it is detected that the internal host (10.102.6.134) is trying to communicate with the malicious IP address (5.255.102.43:80).(1 occurrence(s)) 2025-12-16 12:04:41 Through the cloud-based engine, it is detected that the internal host (10.102.6.134) is trying to communicate with the malicious IP address (199.195.253.124:9001). (1 occurrence(s)) 2025-12-16 12:00:43 Through the cloud-based engine, it is detected that the internal host (10.102.6.134) is trying to communicate with the malicious IP address (23.142.248.63:666).(1 occurrence(s))

3.18.2 Security Enhancement Recommendations

1. Status

- Add a corresponding policy to protect the host according to the threat details and then click on the flag icon to change Action status (to Action has been taken) in SOC > User Security > Summary.

2. Compromised

- The host is infected with malware. Download anti-malware software to scan for and remove malware on the infected hosts. (Download anti-malware software: http://sec.sangfor.com/apt)

3.19 10.130.1.140 Security Details (To be Fixed)

Overall security rating: Compromised

10.130.1.140 has encountered 10 threat(s), and it is in the stage of C&C Communication. Host is infected with malware and controlled by a hacker.

3.19.1 Threat Details

Event Category	C&C Communication
Details	Host visited C&C communication domain or IP address proved by CNCERT.

Description	2025-12-17 13:24:01 Through the pioneered active detection technology, it is detected that the internal host (10.130.1.140) is trying to request for access to the address of the mining pool (51.79.157.201:5342).(10 occurrence(s))

3.19.2 Security Enhancement Recommendations

1. Status

- Add a corresponding policy to protect the host according to the threat details and then click on the flag icon to change Action status (to Action has been taken) in SOC > User Security > Summary.

2. Compromised

- The host is infected with malware. Download anti-malware software to scan for and remove malware on the infected hosts. (Download anti-malware software: http://sec.sangfor.com/apt)

3.20 10.120.1.176 Security Details (To be Fixed)

Overall security rating: Compromised

10.120.1.176 has encountered 10 threat(s), and it is in the stage of C&C Communication. Host is infected with malware and controlled by a hacker.

3.20.1 Threat Details

Event Category	C&C Communication
Details	Host visited C&C communication domain or IP address proved by CNCERT.
Description	2025-11-27 15:39:47 Through the cloud-based engine, it is detected that the internal host (10.120.1.176) is trying to communicate with the malicious IP address (95.214.234.238:8041). (10 occurrence(s))

3.20.2 Security Enhancement Recommendations

1. Status

- Add a corresponding policy to protect the host according to the threat details and then click on the flag icon to change Action status (to Action has been taken) in SOC > User Security > Summary.

2. Compromised

- The host is infected with malware. Download anti-malware software to scan for and remove malware on the infected hosts. (Download anti-malware software: http://sec.sangfor.com/apt)

4 How To Assess Risks & Impacts

4.1 How To Assess Risks

Server security is based on comprehensive analysis of all the security logs related to the internal servers in protected zones. Server security rating falls into four types: Compromised/Bot controlled, Attacked, Data harvested and Vulnerable. Host security is based on comprehensive analysis of all network security logs related to all the hosts in protected zones, and rating also falls into four types: Compromised, High, Medium and Low. Overall security is assessed according to server and host security, and the rating falls into the following:

Overall Security is rated **Poor** :

- This indicates that severity of at least one server is rated **Compromised** or severity of at least one host is rated **Compromised**

Overall Security is rated **Medium** :

- This indicates that severity of at least one server is rated **Attacked** or severity of at least one host is rated **High**
- This indicates that severity of at least one server is rated **Data Harvested** or severity of at least one host is rated **Medium**

Overall Security is rated **Good** :

- This indicates that severity of at least one server is rated **Vulnerable** or severity of at least one host is rated **Low**

Overall Security is rated **Excellent** :

- This indicates that no server is vulnerable or has been attacked, or no host is likely infected with malware.

4.2 Impacts

4.2.1 Backlink

A backlink is a hidden hyperlink that links from a tampered webpage back to a specific webpage or website, also called inbound link. A hidden backlink is generally used to illegitimately link to another website, or to obtain WebShell of websites with high page rank (PR) or weight in search engine after employing vulnerabilities on the web server. A backlink is no different from an outbound link in nature, with the same purpose of improving page rank, but may cause legal risk if the website is linked to gambling, games, pornography or other illegal content.

Learn More: http://sec.sangfor.com/attacks/4.html

Recommendations:

- Check source code of backlink-injected webpage and remove the injected backlink.
- Download anti-malware software, scan for and remove the backlink injected into the website. (Download Sangfor anti-malware software: http://sec.sangfor.com/apt)

4.2.2 WebShell Backdoor

The attacker exploits a known web server vulnerability and injects WebShell onto the web server to gain remote access and conduct malicious activities.

Learn More: http://sec.sangfor.com/attacks/2.html

Recommendations:

- Download anti-malware software, scan for and remove the potential WebShell or viruses on the server. (Download Sangfor anti-malware software: http://sec.sangfor.com/apt)
- Configure a corresponding web application protection rule and set Action to Deny.

4.2.3 WebShell Upload

The attacker takes advantage of a known web server vulnerability and injects WebShell onto the web server. This allows the attacker to visit the WebShell page, execute system commands and have persistent control of the web server.

Recommendations:

- Download anti-malware software, scan for and remove the potential WebShell or viruses on the server. (Download Sangfor anti-malware software: http://sec.sangfor.com/apt)
- Configure a corresponding web application protection rule and set Action to Deny.

4.2.4 Bot Controlled

Worm, virus or Trojan infected hosts can be controlled remotely by attackers to launch attacks such as DoS and APT attacks, aiming to destroy the network or critical application systems and steal confidential data.

Learn More: http://sec.sangfor.com/attacks/8.html

Recommendations:

- Download anti-malware software to scan for and remove malware on the infected host. (Download Sangfor anti-malware software: http://sec.sangfor.com/apt)

4.2.5 Attacked

The attacker employs advanced techniques to initiate intrusions and attacks against a specific enterprise network, with the purpose of stealing corporate data after long-term planning and operating. Because attackers are very good at hiding, data theft may turn to cyber spying eventually.

- SQL Injection: The attacker exploits a database vulnerability and steals data from it, causing data and account leaks.
- Brute-force Attack: The attacker uses tools to perform brute-force attacks against the servers with password-based authentication enabled.
- XSS Attack: The attacker exploits a vulnerability to execute commands, obtain system running information, create new system user accounts and enable remote access to control the web server.

Learn More: http://sec.sangfor.com/attacks/1.html

Recommendations:

- Configure a corresponding web application protection rule and set Action to Deny.
- Configure a corresponding Intrusion Prevention rule and set action to Deny.

4.2.6 Server Security Ratings

- Stages of Attack

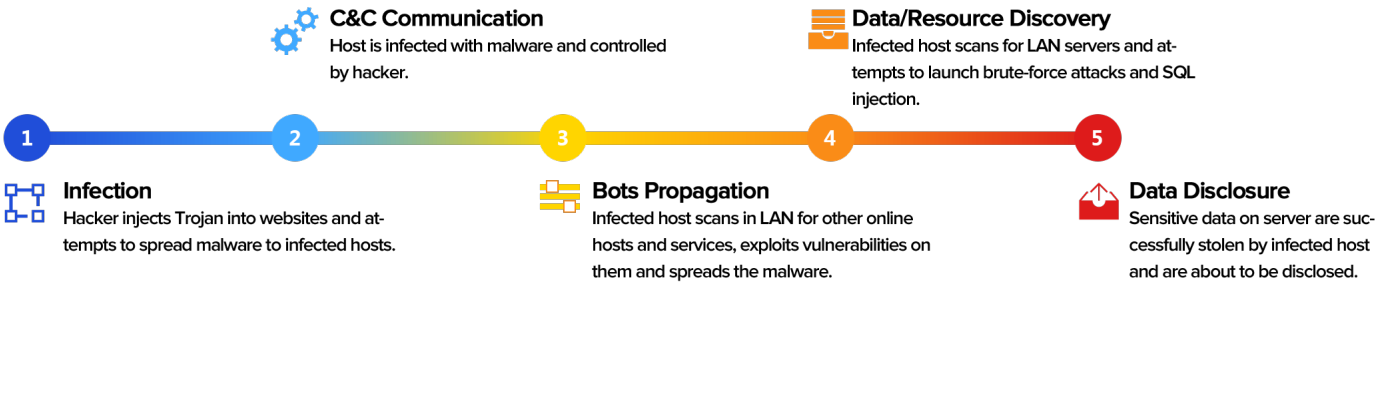
- Severity

No.	Severity	Description	Rating
1	Compromised	Server has been compromised with WebShell or backlink, etc.	5
2	Attacked	It is unknown if the server has been compromised, but log archives show evidence of SQL injection, brute-force login, Webshell upload, etc.	3-4
3	Data harvested	It is unknown if the server has been compromised, but there is evidence that data has been harvested.	2

No.	Severity	Description	Rating
4	Vulnerable	It is unknown if the server has been compromised, but it contains security vulnerabilities.	1

4.2.7 Host Security Ratings

- Stages of Attack



- Severity

No.	Severity	Rating	Description
1	Compromised Host is infected with malware.	10	Host visits malicious URL, domain name or IP address related to known malware, exfiltrates data or may have infected the database server.
		9	Host visits malicious URL, domain name and IP address related to known malware, attempts to spread malicious file to other hosts.
		8	Host visits URL, domain name or IP address related to known malware.

No.	Severity	Rating	Description
2	High Host is very likely infected with malware.	7	Host launches outgoing DDoS attacks or visits suspicious Conficker domain names.
		6	Host sends or receives suspicious packets related to malware, or spreads malicious shellcode.
		5	Host visits DGA-generated domain names, or initiates reverse connection.
3	Medium Host is not acting like an infected host but malware has been downloaded.	4	Host downloads malicious executable files, PDF files or Trojan virus-infected webpage, but has not been infected yet.
		3	Host downloads suspicious files, such as those with unmatching name and extension, but has not been infected yet.
4	Low Host may be infected with malware.	2	Host uses protocols related to malware (such as IRC, HFS, etc.) and visits suspicious domain names or IP addresses related to malware.
		1	Suspicious traffic is detected, such as SSL protocol used on ports other than port 443, but severity is low. Host may visit phishing websites/emails that steal account information.