



SANGFOR



IAM

Network Audit Troubleshooting Guide

Version 12.0.18



Change Log

Date	Change Description
April 2, 2019	Version 12.0.18 document release.

CONTENT

Chapter 1 Background	1
Chapter 2 Unable to audit network behavior	1
1 Check the multi-function serial number first	1
2 Troubleshoot if the recognition behavior is incorrect	1
3 Check Database	1
4 Check audit policy	2
Chapter 3 Unable to audit network content	2
1 Check the multi-function serial number first	2
2 Check Audit Policy	3
3 Check if the mailbox uses SSL protocol	3
4 Query mail	4
Chapter 4 others	4
1 Check global exclusion related addresses	5
1.1 Check if there is an IP address or network segment that excludes the internal network	5
1.2 Check if the domain name or address of the public network is excluded	5
2 Check if the user matches the audit policy	5
3 Check if you have made a custom app or custom URL	6
4 Capture packets in the background to confirm whether the traffic passes through the device in both directions	8
5 Check if the packet has multi-layer protocol encapsulation	8
6 Check if the packet is fragmented	8

Chapter 1 Background

This document is used to troubleshoot auditing without network behavior or content.

Chapter 2 Unable to audit network behavior

1 Check the multi-function serial number first

First check if the Multi-Function License has Activity Audit.



2 Troubleshoot if the recognition behavior is incorrect

In Internet Activities page checks the specific online behavior and whether there is a behavior recognition error.

Internet Activities								
Auto Refresh: 5 second(s) Filter								
Filter: Group (/) Objects: Search term Email IM chats Forum & Microblogging Outgoing File Website Browsing Action: Reject Log Alert								
No.	Time Oc...	Username	Group	IP Address	App Category	Applicati...	Action	Details
1	49.5 min...	192.168.19.4	/default	192.168.19.4	Visit Web Site	IT Indus...	Log	URL: 202.96.137.75
2	50 minut...	192.168.19.4	/default	192.168.19.4	Visit Web Site	IT Indus...	Log	URL: 202.96.137.75
3	50 minut...	192.168.19.4	/default	192.168.19.4	Visit Web Site	IT Indus...	Log	URL: 202.96.137.75
4	50 minut...	192.168.19.4	/default	192.168.19.4	Visit Web Site	IT Indus...	Log	URL: 202.96.137.75
5	50 minut...	192.168.19.4	/default	192.168.19.4	Visit Web Site	IT Indus...	Log	URL: 202.96.137.75
6	50 minut...	192.168.19.4	/default	192.168.19.4	Visit Web Site	IT Indus...	Log	URL: www.sinfors.com.cn

3 Check Database

Check if the Database is updated to the latest, If not the latest, please update to the latest.

Auto Update							
<input checked="" type="checkbox"/> Enable <input type="checkbox"/> Disable Update Server Refresh							
<input type="checkbox"/>	No.	Database	Current Version	Latest Version	Update Service Expire...	Auto Up...	Operation
<input type="checkbox"/>	1	Engine Zero	2018-11-05	2018-11-05	2020-01-25	✓	
<input type="checkbox"/>	2	URL Database	2019-03-05 09:00:00	2019-03-05	2020-01-24	✓	
<input type="checkbox"/>	3	System patch	SP_LFD SP_fsu SP_u...	SP_Vpnppp_AC12.0.16	Never expire	✓	
<input type="checkbox"/>	4	Application Signature Datab...	2019-03-05 12:34:56	2019-03-05	2020-01-24	✓	
<input type="checkbox"/>	5	Audit Rule Database	2019-02-26	2019-02-26	2020-01-24	✓	

4 Check audit policy

Check if there is an audit policy, and whether Schedule and Object are configured correctly.

Audit Policy

☒ Enabled

Name: ⓘ

Description:

Options **Object** Advanced

Audit Policy

- ☒ Application
- ☒ Flow/Online Duration
- ☒ Webpage Content

Application

+ Add - Delete | Audit Disabled | ↑ Move Up ↓ Move Down

<input type="checkbox"/>	No.	Item	Schedule	Action	Delete
<input type="checkbox"/>	1	Web-based BBS posting Web Mail contents Web-based attachment upload (including WebMail) Microblogging contents Outgoing email(SMTP)	All Day	Audit	✗

Commit

Chapter 3 Unable to audit network content

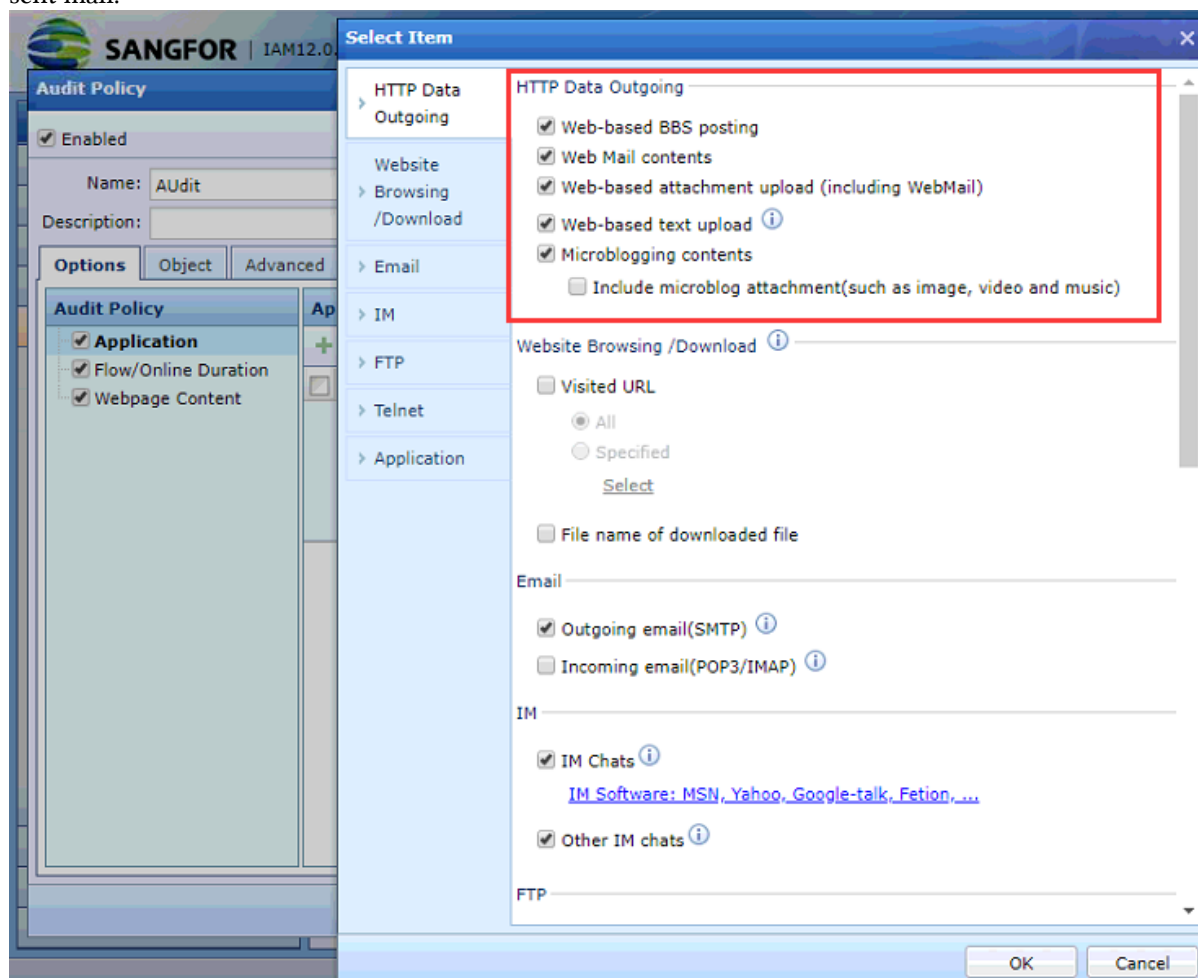
1 Check the multi-function serial number first

First check if the Multi-Function License has Content Audit.



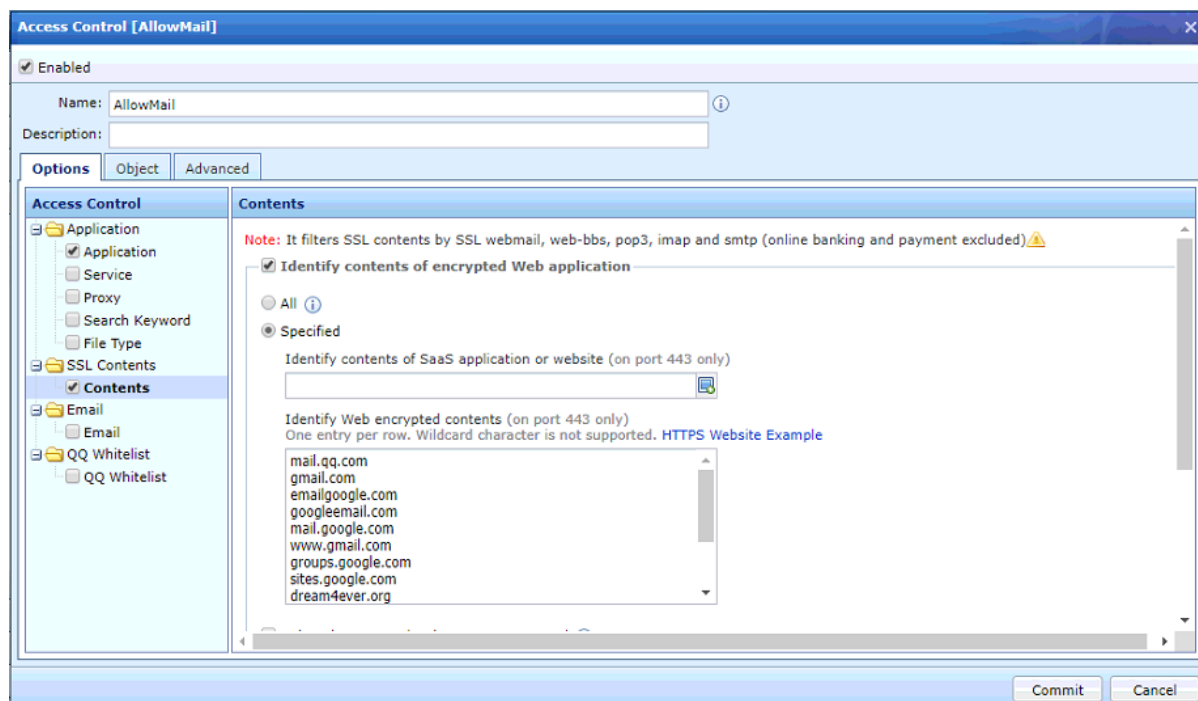
2 Check Audit Policy

Check whether the audit policy has checked the mail content audit, and the web mail can only audit the sent mail.



3 Check if the mailbox uses SSL protocol

If the mailbox is transmitted using the SSL protocol, SSL content recognition is required.



4 Query mail

If you can't find the email content in "Email Incoming/Outgoing", then in "Posting/Microblogging" Look for "Other postings".

Posting/Microblogging Logs > Posting/Microblogging

Period

Period: 2019-03-12 00:00:00 to 2019-03-12 23:59:59

Filter

User/Group: All

Method: ☒ Posting ☒ Microblogging ☒ Other postings

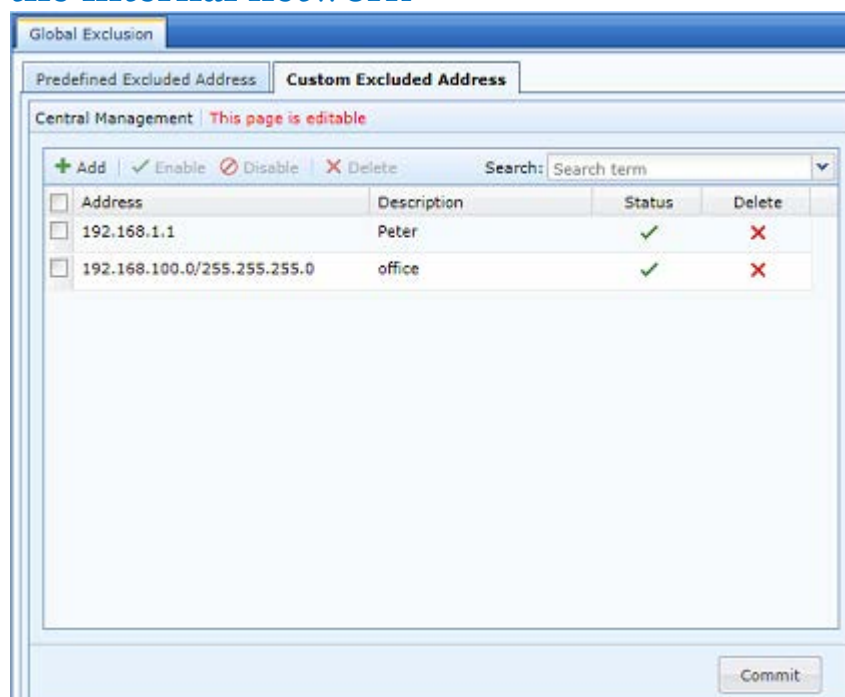
Search Term:

Go [More Options](#)

Chapter 4 others

1 Check global exclusion related addresses

1.1 Check if there is an IP address or network segment that excludes the internal network

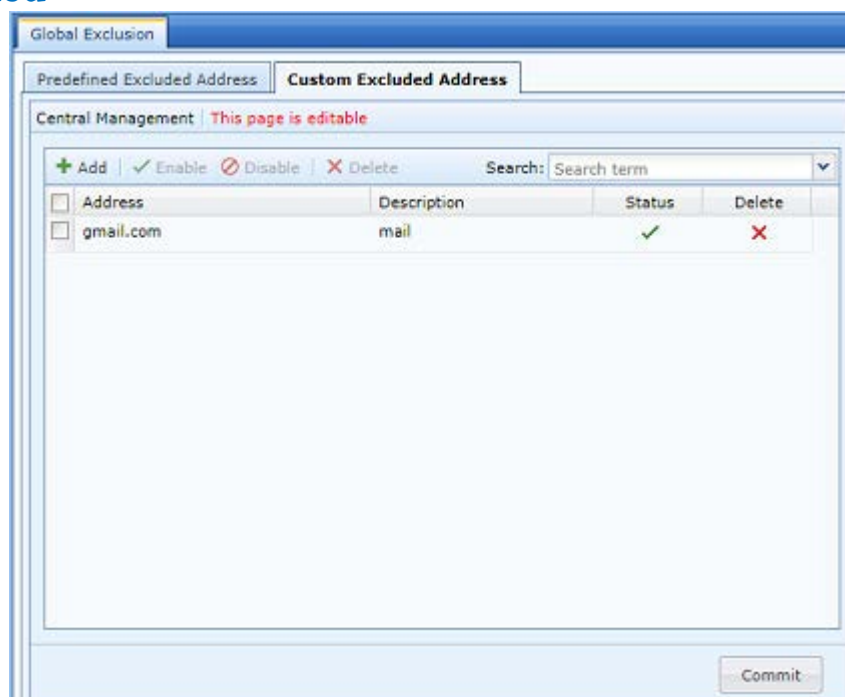


The screenshot shows the 'Global Exclusion' window with the 'Custom Excluded Address' tab selected. The 'Central Management' section indicates 'This page is editable'. Below this, there are buttons for '+ Add', '✓ Enable', '✗ Disable', and '✗ Delete', along with a search bar labeled 'Search: Search term'. A table lists excluded addresses with columns for 'Address', 'Description', 'Status', and 'Delete'.

Address	Description	Status	Delete
<input type="checkbox"/> 192.168.1.1	Peter	✓	✗
<input type="checkbox"/> 192.168.100.0/255.255.255.0	office	✓	✗

A 'Commit' button is located at the bottom right of the window.

1.2 Check if the domain name or address of the public network is excluded

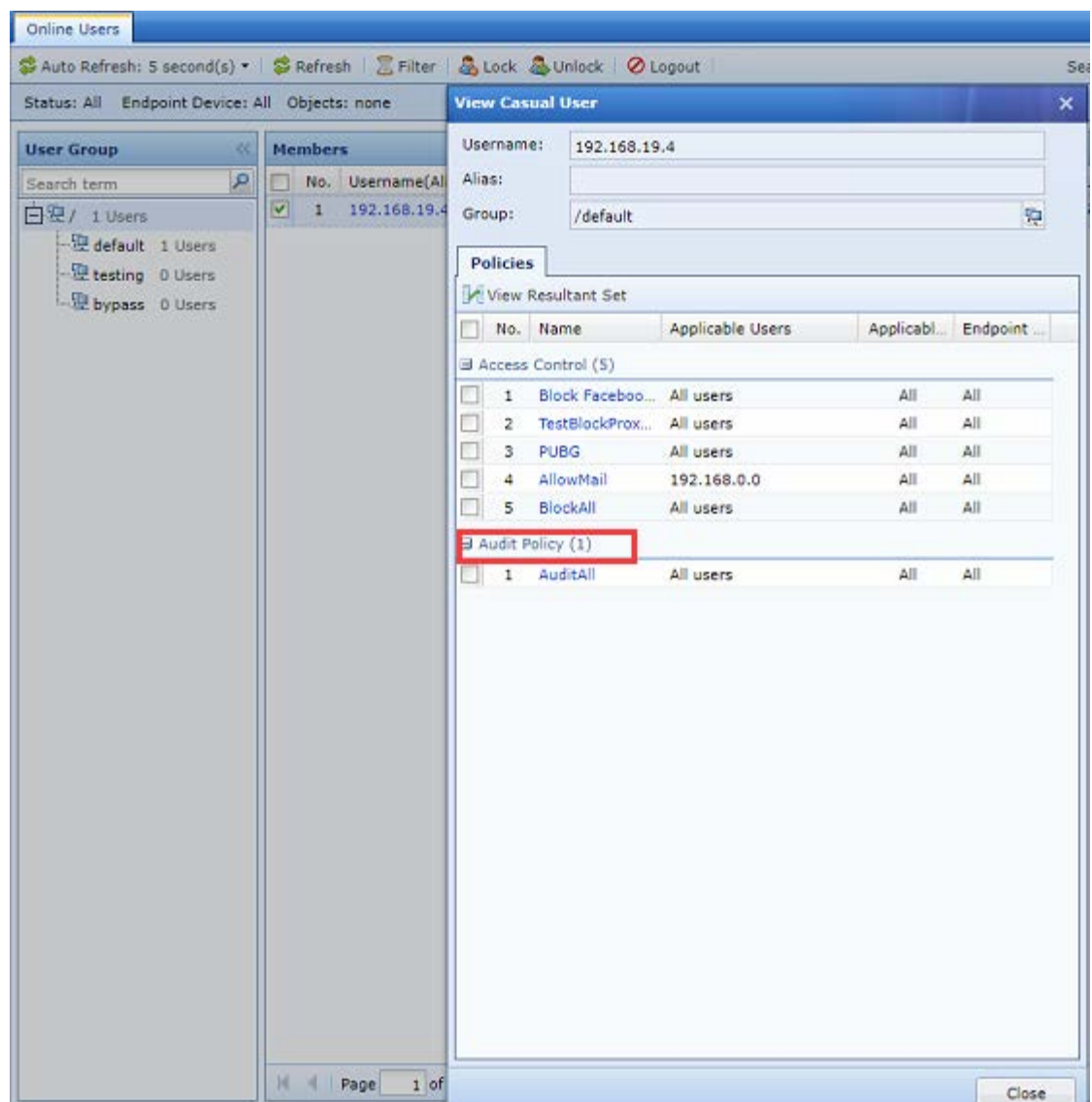


The screenshot shows the 'Global Exclusion' window with the 'Custom Excluded Address' tab selected. The 'Central Management' section indicates 'This page is editable'. Below this, there are buttons for '+ Add', '✓ Enable', '✗ Disable', and '✗ Delete', along with a search bar labeled 'Search: Search term'. A table lists excluded domain names with columns for 'Address', 'Description', 'Status', and 'Delete'.

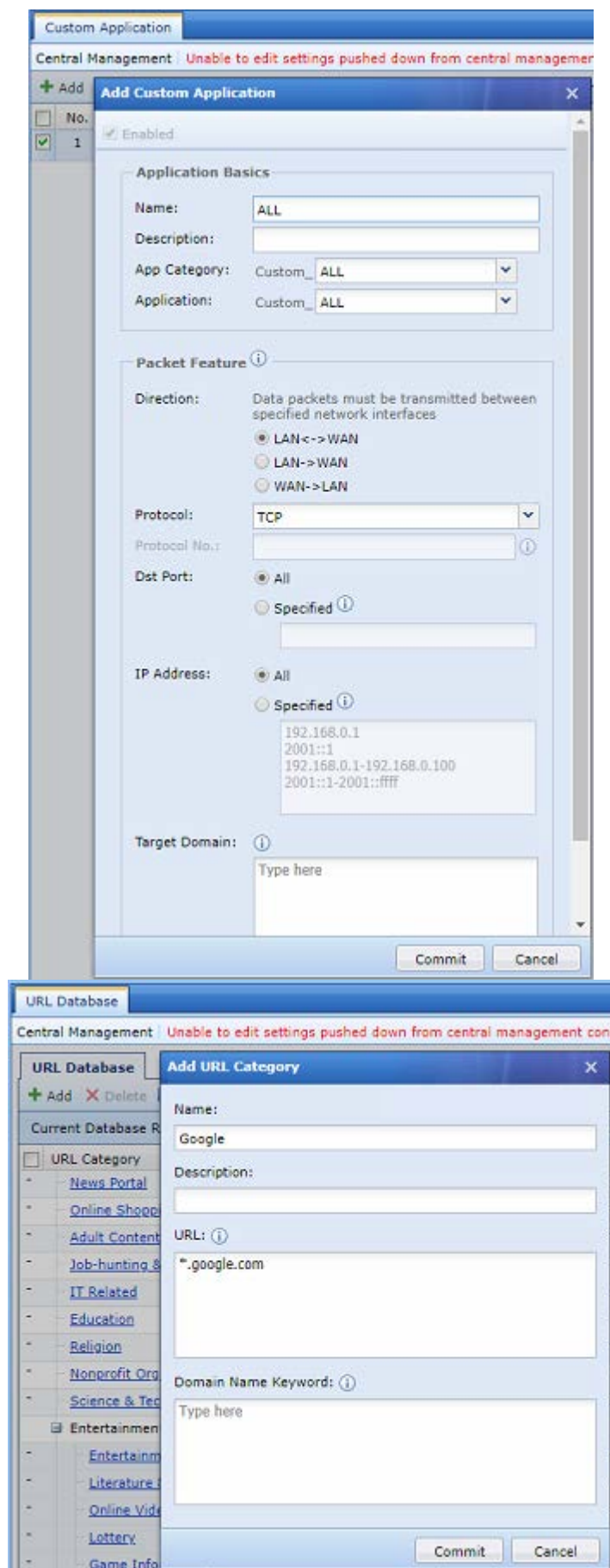
Address	Description	Status	Delete
<input type="checkbox"/> gmail.com	mail	✓	✗

A 'Commit' button is located at the bottom right of the window.

2 Check if the user matches the audit policy



3 Check if you have made a custom app or custom URL



4 Capture packets in the background to confirm whether the traffic passes through the device in both directions

If the packet is not in a two-way pass, it cannot be audited.

No.	Time	Source	Destination	Protocol	Length	Info
3912	6.058747	172.16.248.97	183.3.226.35	TCP	66	53393 → 80 [SYN] Seq=0 Win=17520 Len=0 MSS=1460 WS=256 SACK_PERM=1
3944	6.104048	183.3.226.35	172.16.248.97	TCP	66	80 → 53393 [SYN, ACK] Seq=0 Ack=1 Win=14400 Len=0 MSS=1296 SACK_PERM=1 WS=128
3946	6.104540	172.16.248.97	183.3.226.35	TCP	54	53393 → 80 [ACK] Seq=1 Ack=1 Win=17408 Len=0
3947	6.104840	172.16.248.97	183.3.226.35	HTTP	632	GET / HTTP/1.1
3994	6.117526	183.3.226.35	172.16.248.97	TCP	60	80 → 53393 [ACK] Seq=1 Ack=579 Win=15616 Len=0
3995	6.117528	183.3.226.35	172.16.248.97	HTTP	425	HTTP/1.1 302 Moved Temporarily (text/html)
4021	6.160084	172.16.248.97	183.3.226.35	TCP	54	53393 → 80 [ACK] Seq=579 Ack=372 Win=16896 Len=0

5 Check if the packet has multi-layer protocol encapsulation

If there is a multi-layer protocol package, please open the Protocol Extension.

No.	Time	Source	Destination	Protocol	Length	Info
9...	20...	100.88.181.209	112.29.150.14	TCP	82	26427 → 80 [SYN] Seq=1008759
9...	20...	112.29.150.14	100.88.181.209	TCP	82	80 → 26427 [SYN, ACK] Seq=25
9...	20...	100.88.181.209	112.29.150.14	TCP	70	26427 → 80 [ACK] Seq=1008759
9...	20...	100.88.181.209	112.29.150.14	HTTP	730	GET / HTTP/1.1
9...	20...	112.29.150.14	100.88.181.209	TCP	70	80 → 26427 [ACK] Seq=2550841

▷	Frame 9506: 730 bytes on wire (5840 bits), 730 bytes captured (5840 bits)
▷	Ethernet II, Src: TendaTec_44:2a:68 (c8:3a:35:44:2a:68), Dst: IETF-VRRP-VRID
▷	802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 3201
▷	802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 2077
▷	PPP-over-Ethernet Session
▷	Point-to-Point Protocol
▷	Internet Protocol Version 4, Src: 100.88.181.209, Dst: 112.29.150.14
▷	Transmission Control Protocol, Src Port: 26427, Dst Port: 80, Seq: 100875927
◀	Hypertext Transfer Protocol
▷	GET / HTTP/1.1\r\n
	Host: www.163.com\r\n

6 Check if the packet is fragmented

If there are packet fragments, please check the network environment.

正在捕获 WLAN

文件(F) 编辑(E) 视图(V) 跟踪(G) 捕获(C) 分析(A) 统计(S) 电话(V) 无线(W) 工具(T) 帮助(H)

ip.addr == 192.168.0.120

No.	Time	Source	Destination	Protocol	Length	Info
14	2.309047	192.168.0.120	192.168.0.104	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=d50a) [Reassembled in #16]
15	2.309070	192.168.0.120	192.168.0.104	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=d50a) [Reassembled in #16]
16	2.309086	192.168.0.120	192.168.0.104	ICMP	88	Echo (ping) reply id=0x0001, seq=34/8704, ttl=64
24	3.311319	192.168.0.120	192.168.0.104	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=d770)
25	3.311367	192.168.0.120	192.168.0.104	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=d770) [Reassembled in #26]
26	3.311392	192.168.0.120	192.168.0.104	ICMP	88	Echo (ping) reply id=0x0001, seq=35/8960, ttl=64
27	4.313811	192.168.0.120	192.168.0.104	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=d7f8) [Reassembled in #29]
28	4.313840	192.168.0.120	192.168.0.104	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=d7f8) [Reassembled in #29]
29	4.313854	192.168.0.120	192.168.0.104	ICMP	88	Echo (ping) reply id=0x0001, seq=36/9216, ttl=64
30	5.316895	192.168.0.120	192.168.0.104	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=da05) [Reassembled in #32]

Source: 192.168.0.120
Destination: 192.168.0.104
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
3 IPv4 Fragments (3013 bytes): #30(1480), #31(1480), #32(53)

[Frame: 30, payload: 0-1479 (1480 bytes)] → 8+1472 1472+1480+53=3003
[Frame: 31, payload: 1480-2959 (1480 bytes)] → 1480
[Frame: 32, payload: 2960-3012 (53 bytes)] → 53

[Fragment count: 3]
[Reassembled IPv4 length: 3013]

0b70 77 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f wabcdefg hijklmno
0b80 70 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 pqrstuvwxyz abcdefgh
0b90 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 ijklmnop qrstuvw
0ba0 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 bcdefghi jklmnopq

Frame (88 bytes) Reassembled IPv4 (3013 bytes)
IPv4 Fragment (ip: fragment), 53 字节 分组: 5050 · 已显示: 12 (0.2%) 配置文件: Default



Copyright © SANGFOR Technologies Inc. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Inc.

SANGFOR is the trademark of SANGFOR Technologies Inc. All other trademarks and trade names mentioned in this document are the property of their respective holders.

Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied. The information in this document is subject to change without notice. To obtain the latest version, contact the international service center of SANGFOR Technologies Inc