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

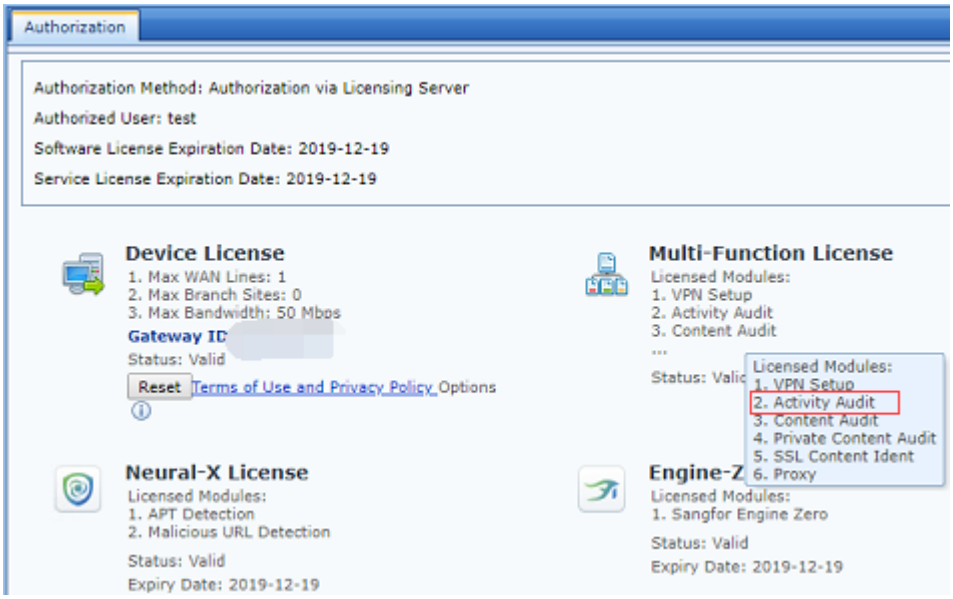
Chapter 1 Background

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

Chapter 2 Unable to audit network behavior

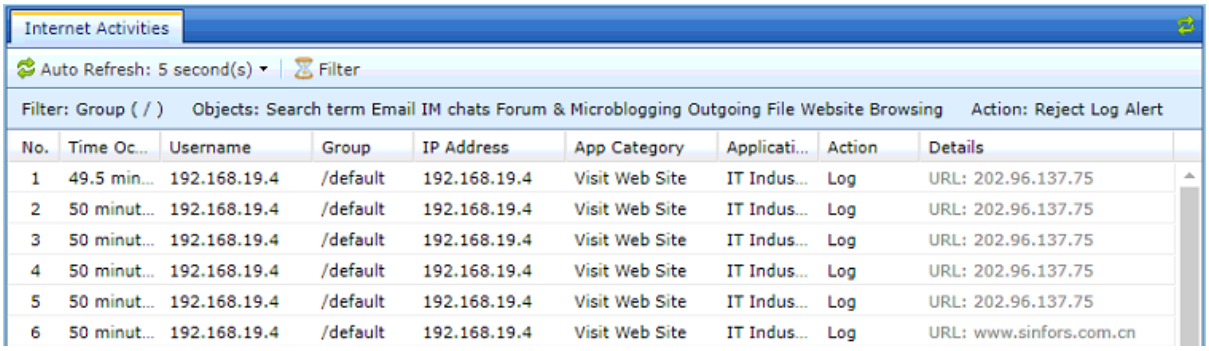
1 Check the multi-function serial number first

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



2 Troubleshoot if the recognition behavior is incorrect

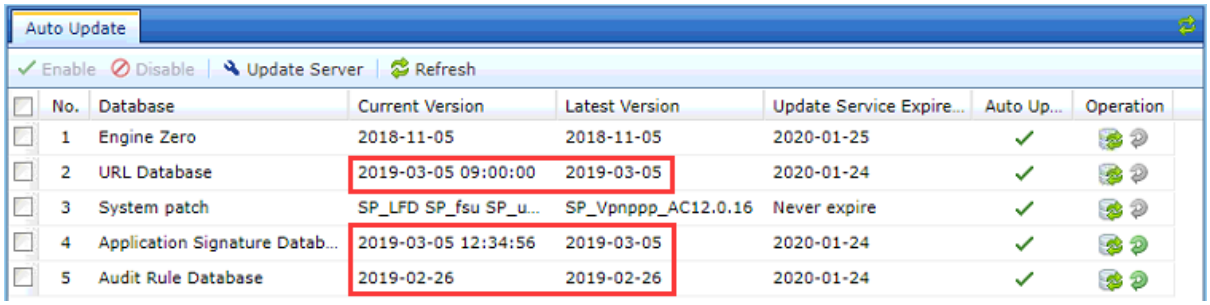
In Internet Activities page checks the specific online behavior and whether there is a behavior recognition error.



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

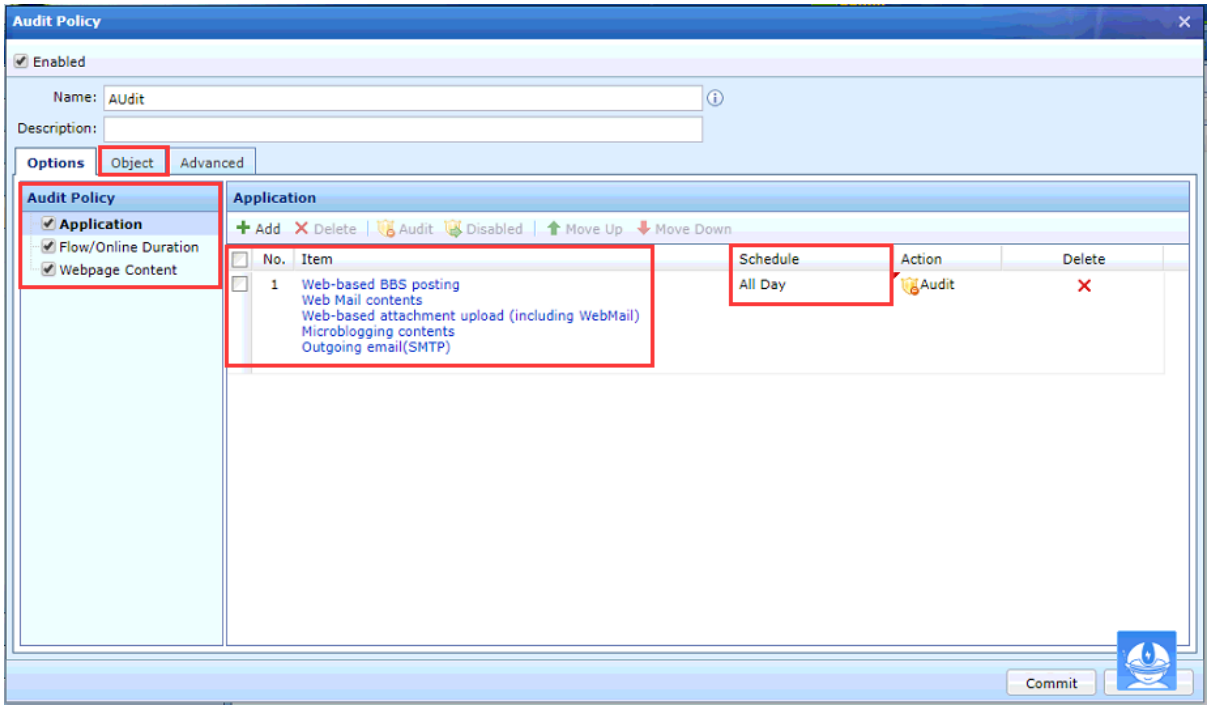
3 Check Database

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



4 Check audit policy

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



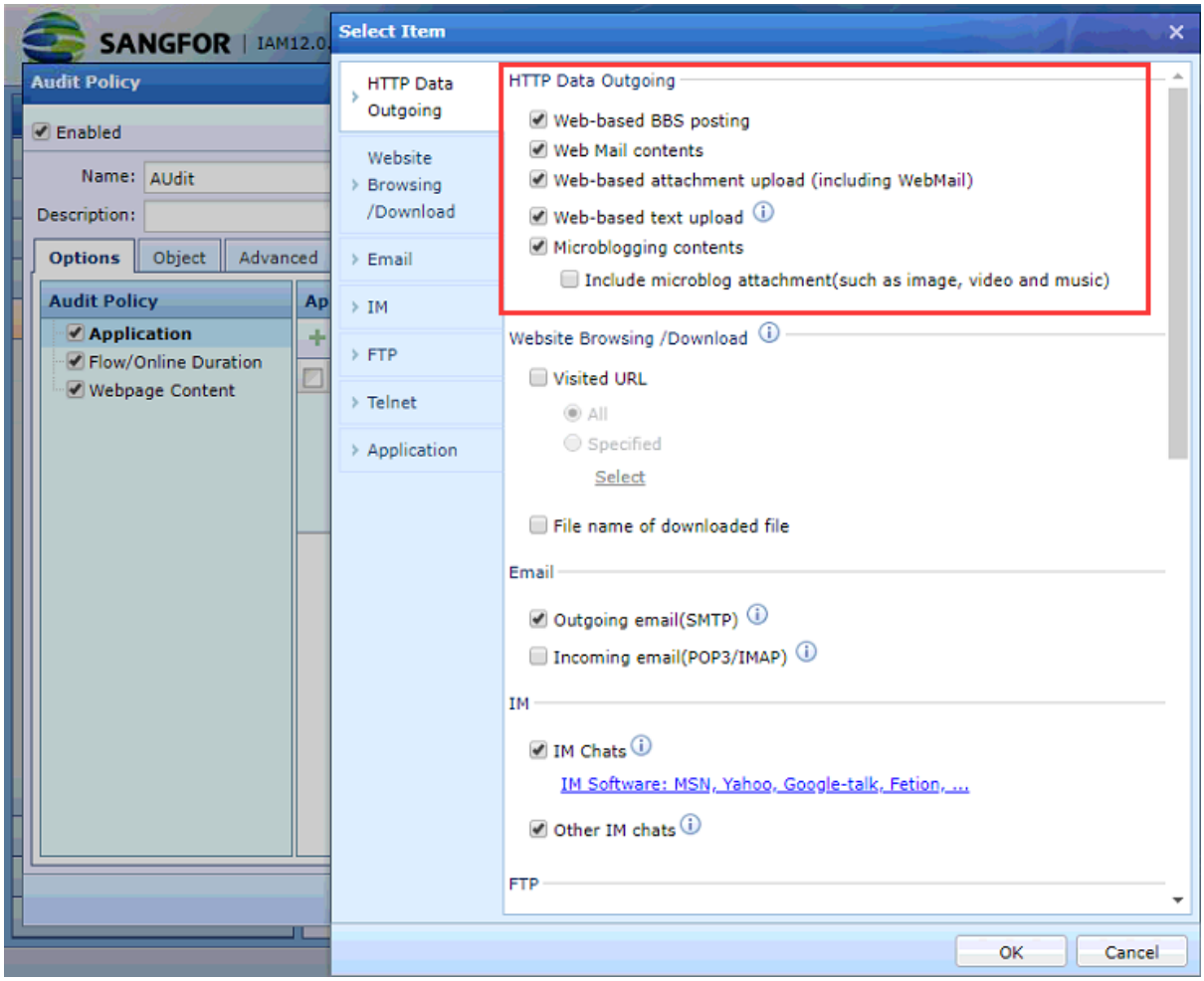
Chapter 3 Unable to audit network content

1 Check the multi-function serial number first

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

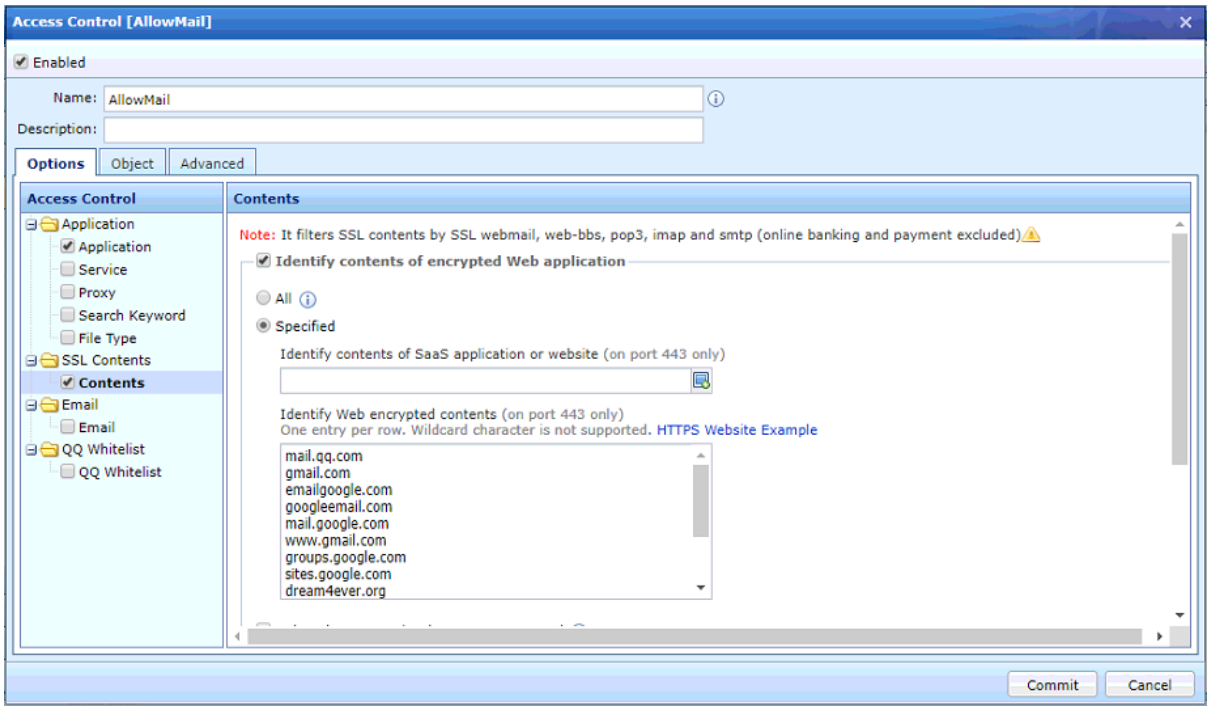
2 Check Audit Policy

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



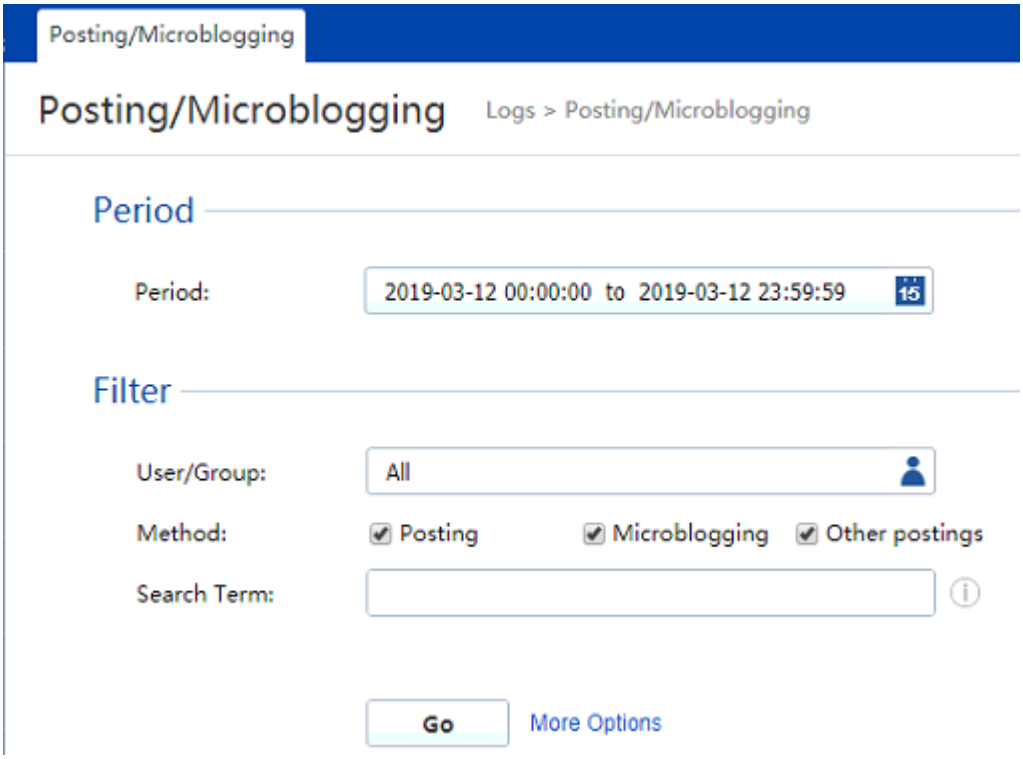
3 Check if the mailbox uses SSL protocol

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



4 Query mail

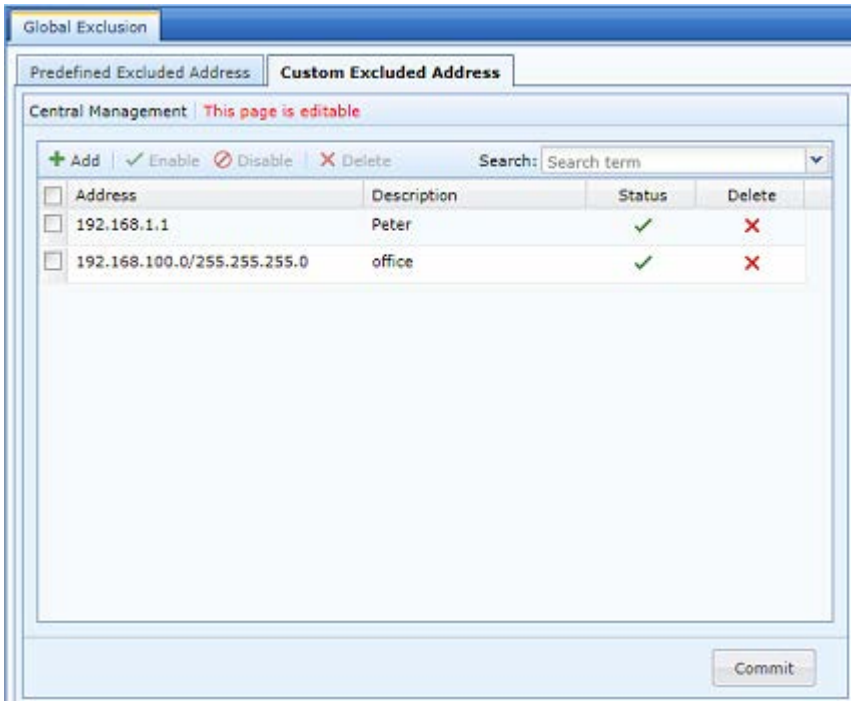
If you can't find the email content in "Email Incoming/Outgoing", then in "Posting/Microblogging" Look for "Other postings".



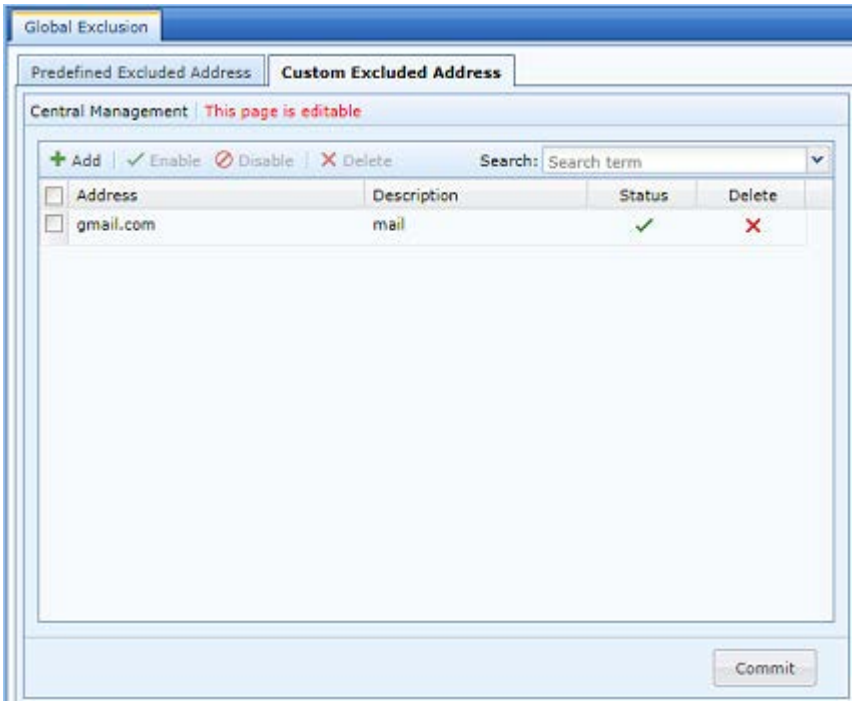
Chapter 4 others

1 Check global exclusion related addresses

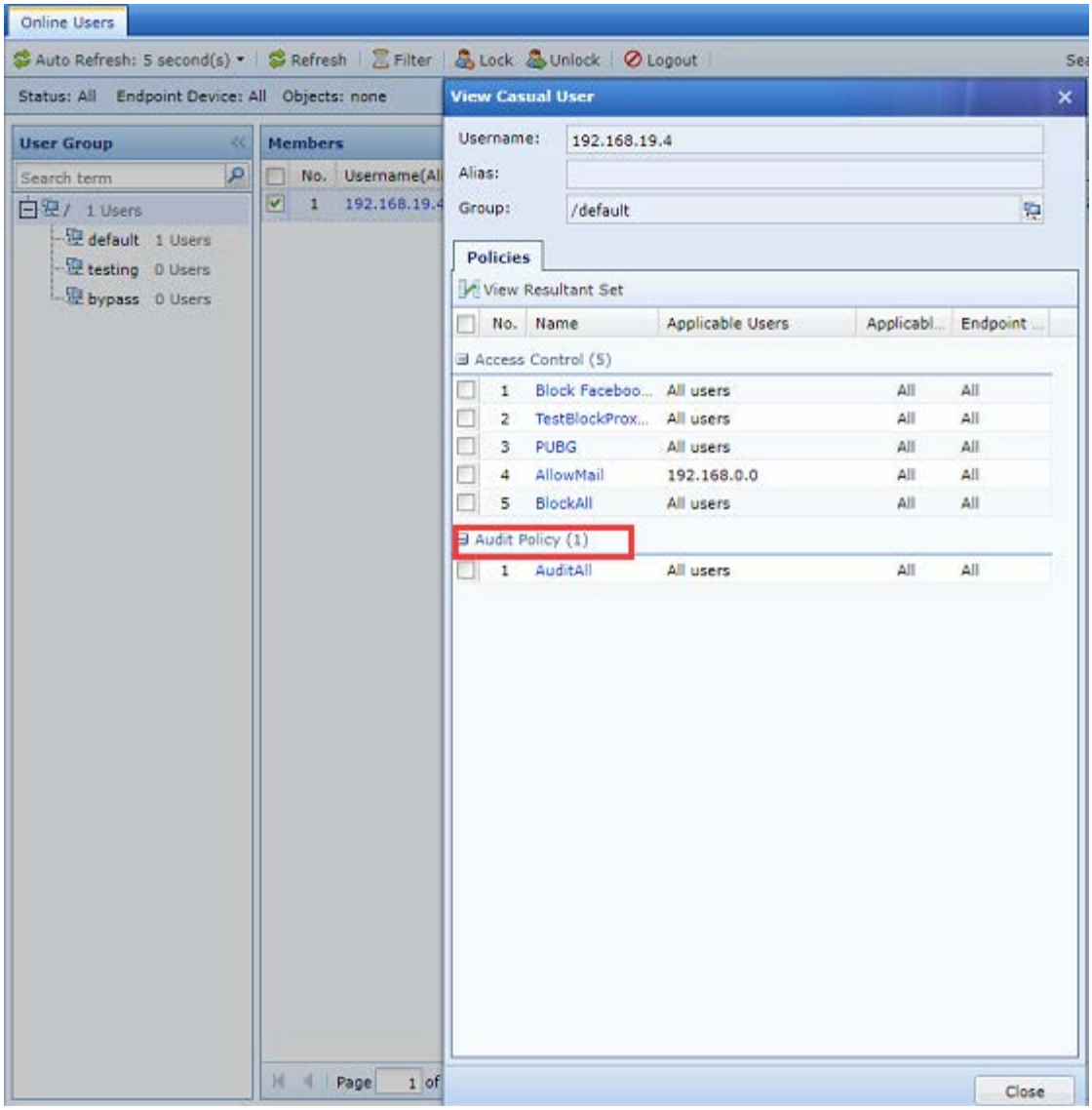
1.1 Check if there is an IP address or network segment that excludes the internal network



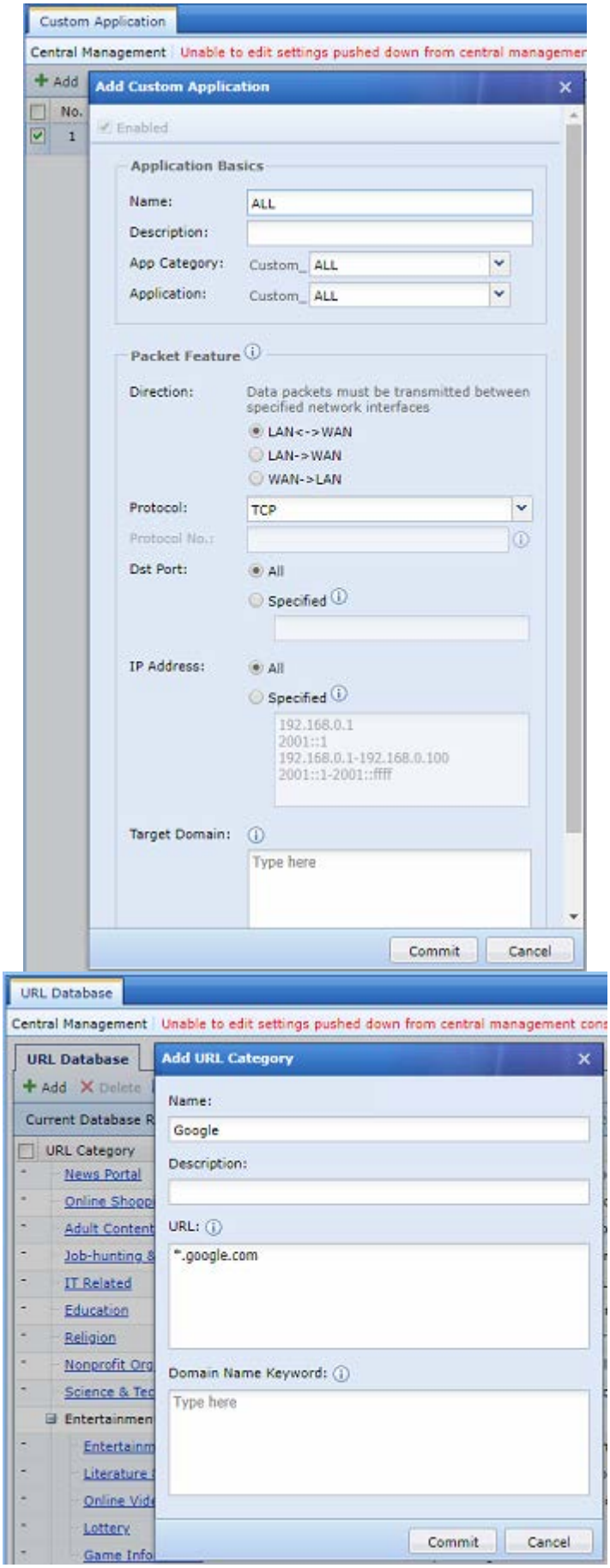
1.2 Check if the domain name or address of the public network is excluded



2 Check if the user matches the audit policy

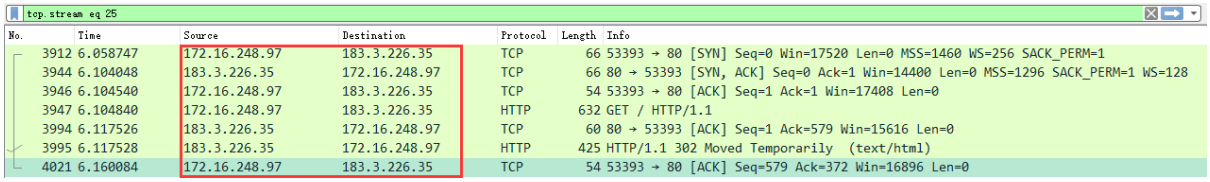


3 Check if you have made a custom app or custom URL


Custom Application
Central Management
Unable to edit settings pushed down from central managemer
Add
No.
1
Add Custom Application
Enabled
Application Basics
Name:
ALL
Description:
App Category:
Custom_
ALL
Application:
Custom_
ALL
Packet Feature
Direction:
Data packets must be transmitted between specified network interfaces
LAN<->WAN
LAN->WAN
WAN->LAN
Protocol:
TCP
Protocol No.:
Dst Port:
All
Specified
IP Address:
All
Specified
192.168.0.1
2001::1
192.168.0.1-192.168.0.100
2001::1-2001::ffff
Target Domain:
Type here
Commit
Cancel
URL Database
Central Management
Unable to edit settings pushed down from central management cons
URL Database
Add
Delete
Current Database R
URL Category
News Portal
Online Shopp
Adult Content
Job-hunting &
IT Related
Education
Religion
Nonprofit Org
Science & Tec
Entertainmen
Entertainm
Literature
Online Vid
Lottery
Game Info
Add URL Category
Name:
Google
Description:
URL:
*.google.com
Domain Name Keyword:
Type here
Commit
Cancel

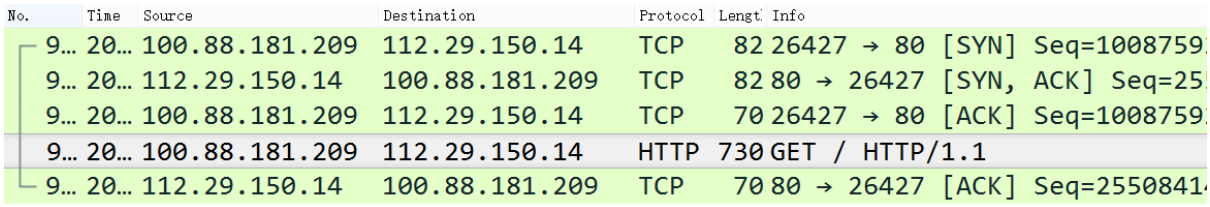
4 Capture packets in the background to confirm whether the traffic passes through the device in both directions

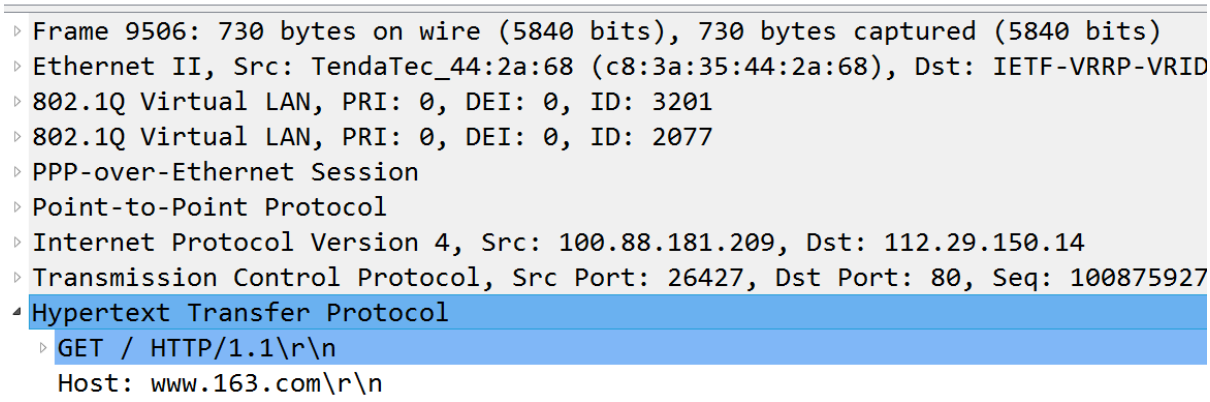
If the packet is not in a two-way pass, it cannot be audited.



5 Check if the packet has multi-layer protocol encapsulation

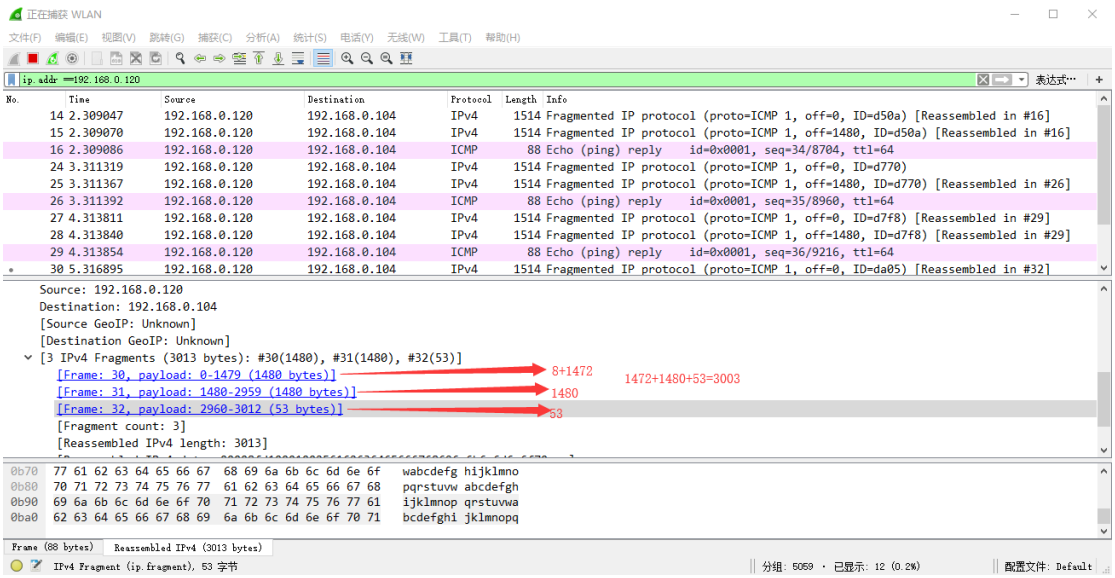
If there is a multi-layer protocol package, please open the Protocol Extension.





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) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 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)]
[Frame: 31, payload: 1480-2959 (1480 bytes)]
[Frame: 32, payload: 2960-3012 (53 bytes)]
[Fragment count: 3]
[Reassembled IPv4 length: 3013]
8+1472
1480
53
1472+1480+53=3003
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 pqrstuvw abcdefgh
0b90 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 ijklmnop qrstuvwa
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: 5059 · 已显示: 12 (0.2%)
配置文件: Default