SANGFOR

IAM

Proxy troubleshooting guide

Version 12.0.18

Change Log

Date	Change Description
April 29, 2019	Version 12.0.18 document release.

CONTENT

1 Data interaction process in Proxy scenario

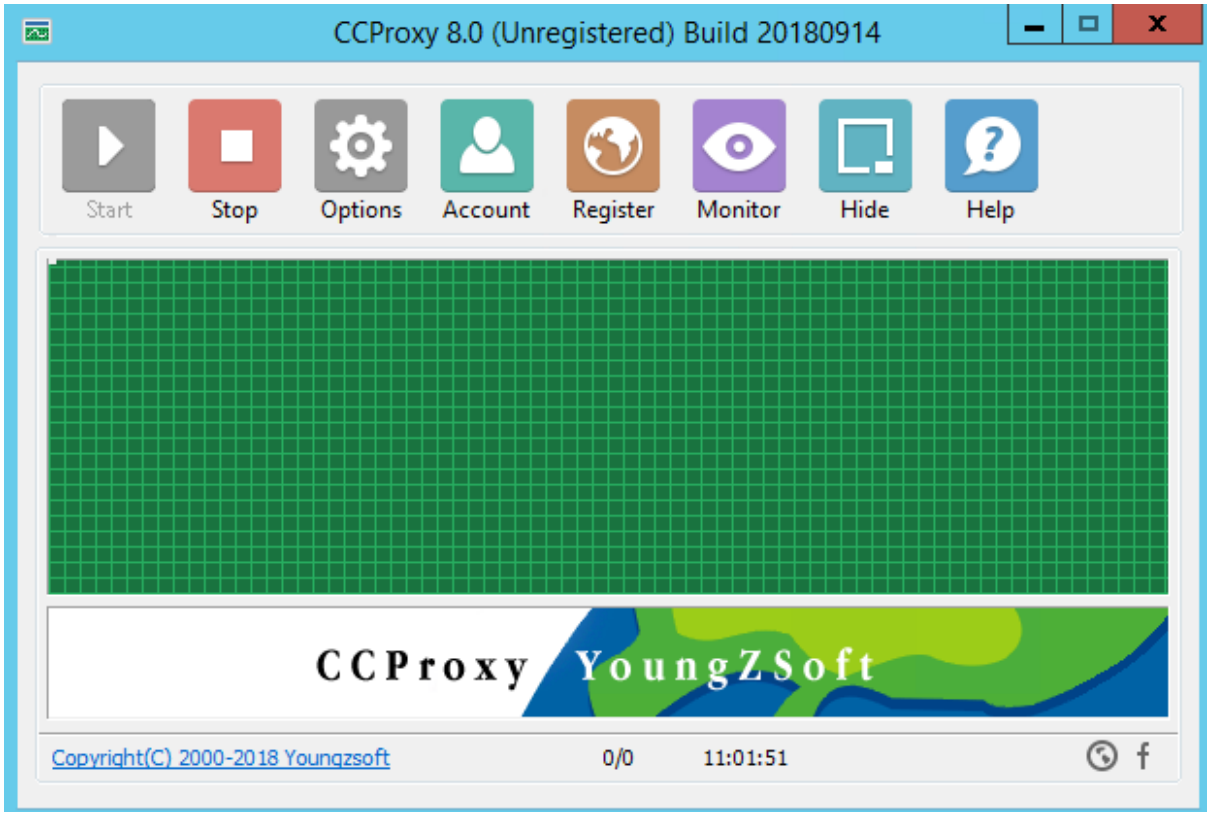
- PC and IAM establish a connection through the proxy port
- PC sends a GET request to IAM
- IAM sends a DNS request packet to get the IP of the website.
- IAM and website IP establish a connection
- IAM sends a GET request
- Website Server IP returns website data to IAM
- IAM will reply the data to the PC
- Disconnect

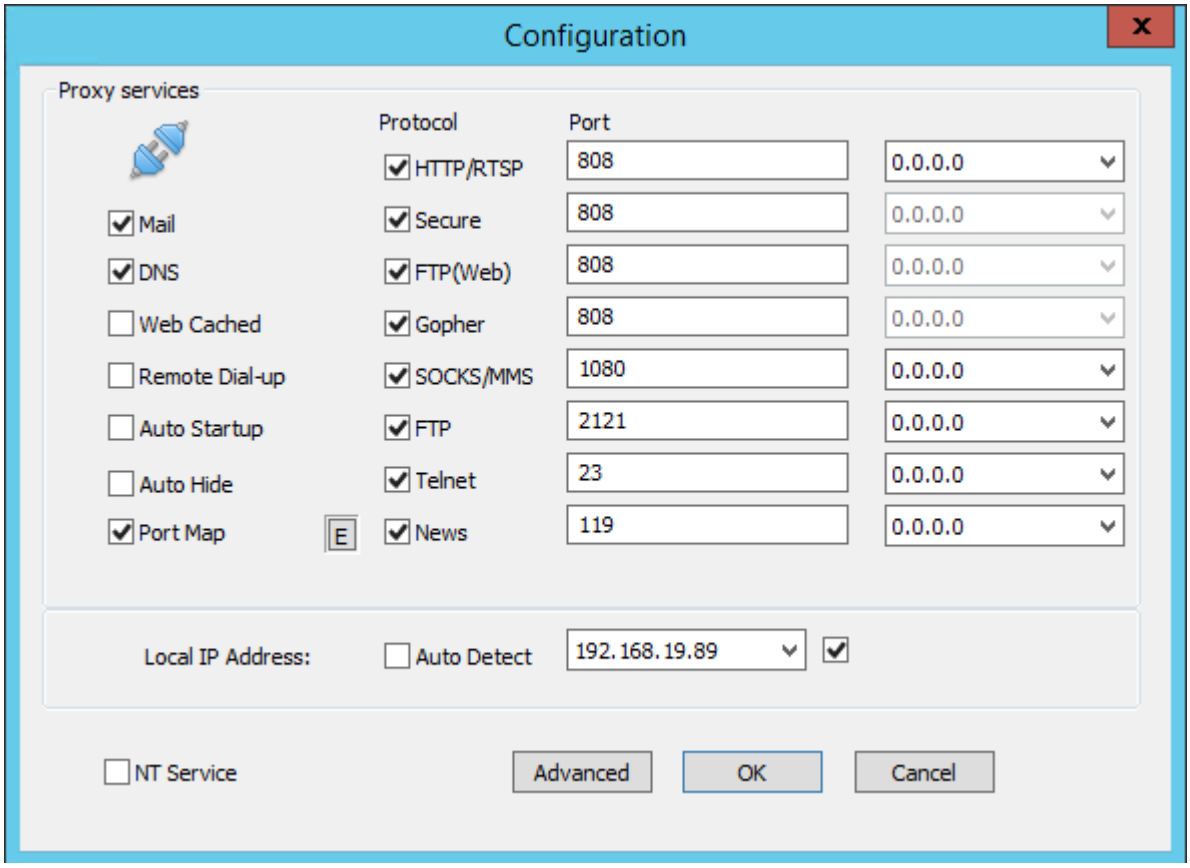
2 Troubleshooting when you can't open the website

2.1 Confirm whether this website supports proxy environment

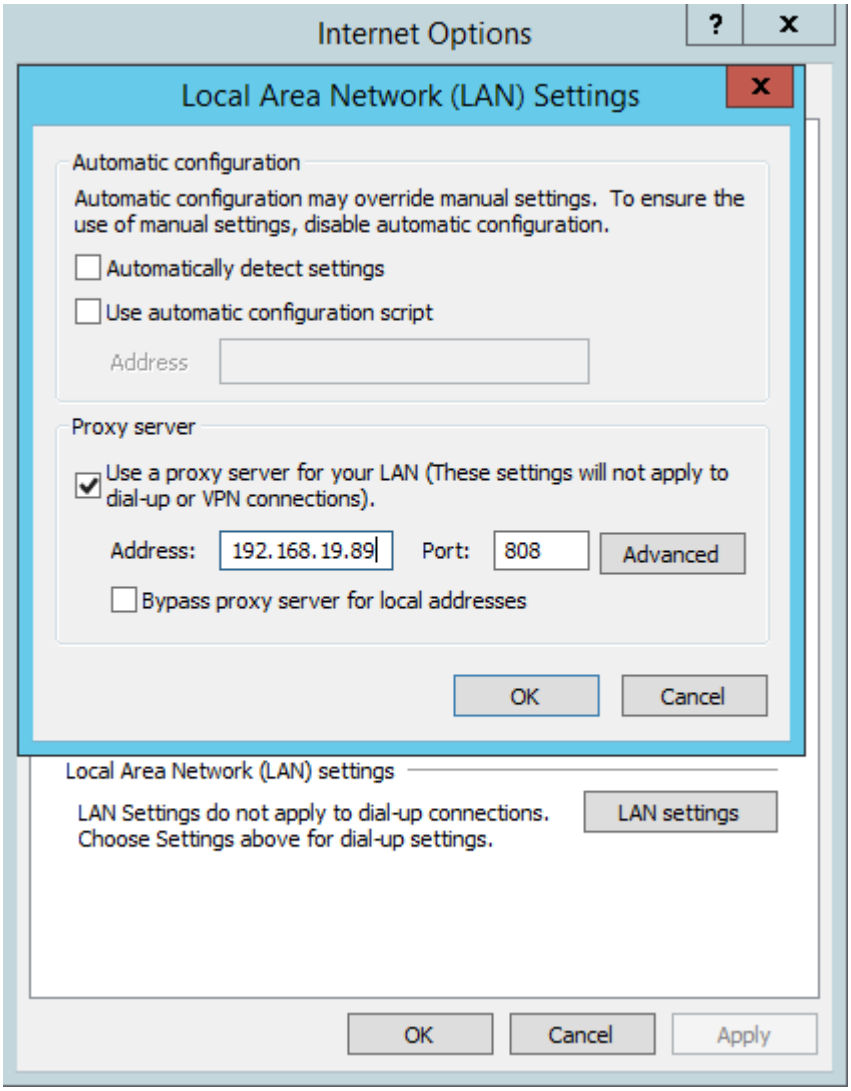
- Install a **ccproxy** on a PC1 that does not go through an IAM proxy, so that PC1 acts as a Proxy Server. Then prepare another test computer PC2, set PC1 as a proxy such in PC1 web browser's proxy settings, and open the website. This method is used to test whether the website supports proxy access. If this is not possible, the website itself does not support proxy so it has no related with IAM.

PC1:




Configuration
Proxy services
Protocol
Port
HTTP/RTSP
808
0.0.0.0
Mail
Secure
808
DNS
FTP(Web)
808
Web Cached
Gopher
808
Remote Dial-up
SOCKS/MMS
1080
0.0.0.0
Auto Startup
FTP
2121
0.0.0.0
Auto Hide
Telnet
23
0.0.0.0
Port Map
E
News
119
0.0.0.0
Local IP Address:
Auto Detect
192.168.19.89
NT Service
Advanced
OK
Cancel

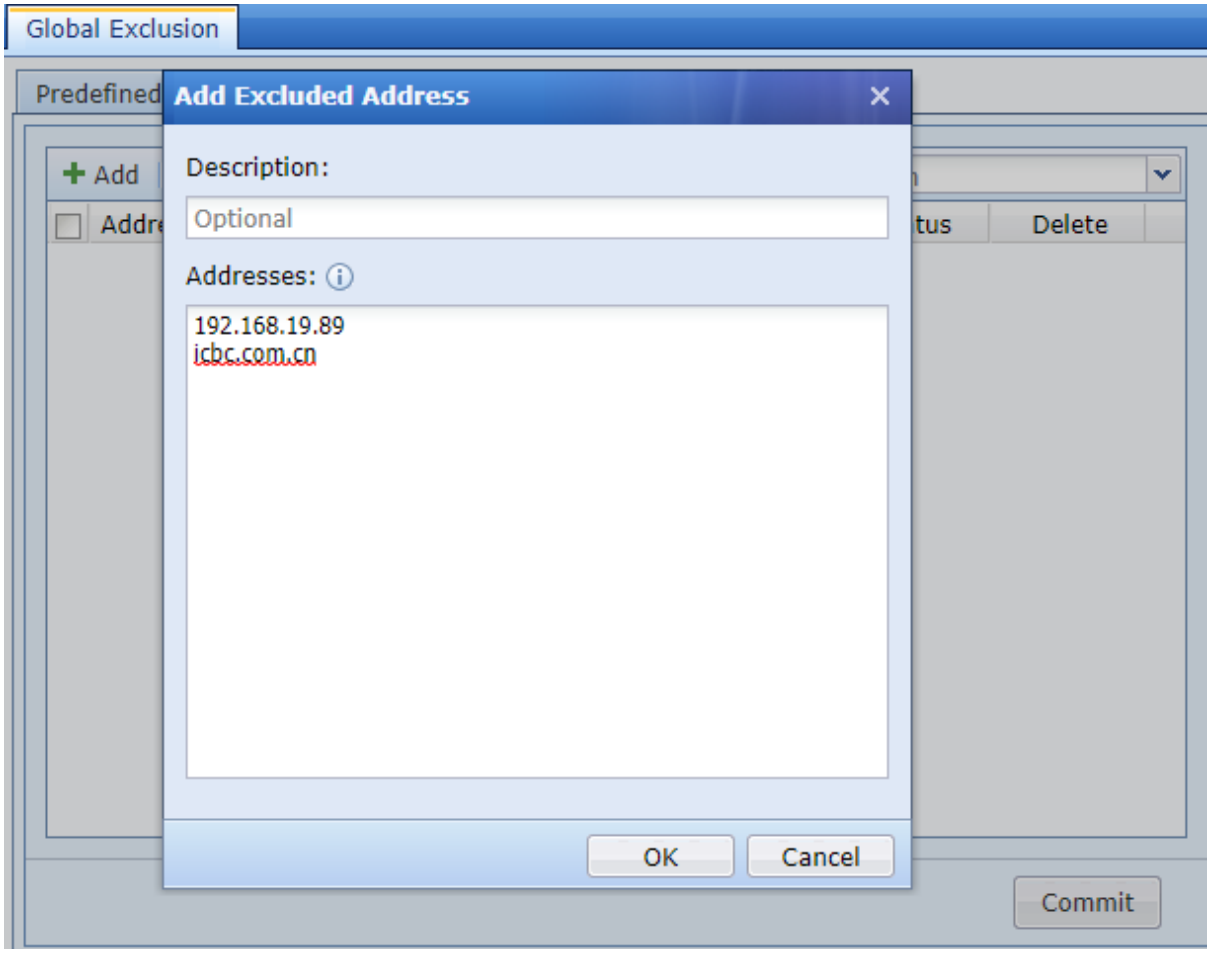
PC2:

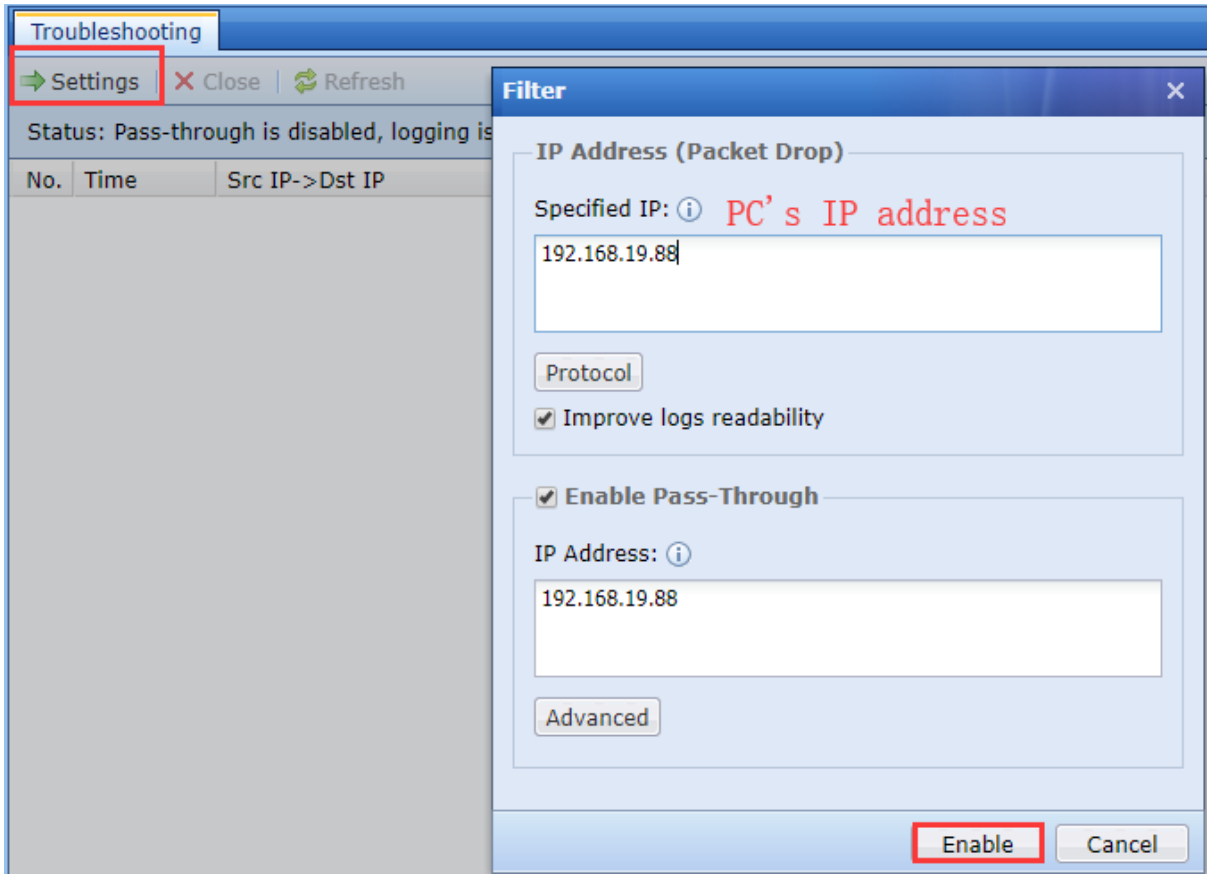


- Some video sites use special protocols when transmitting video data, and the protocol itself does not support proxies.
- Some bank websites use components such as ukey to secure information, while some ukeys do not support agents.

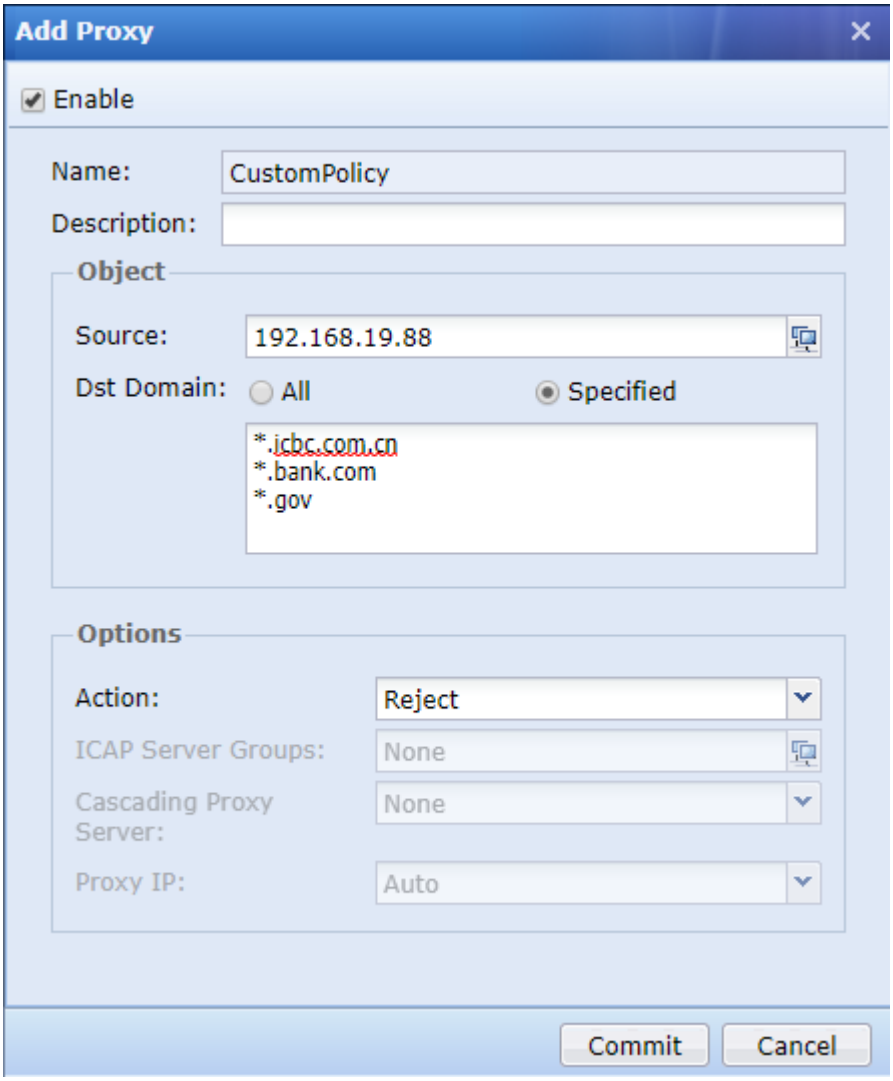
2.2 Other troubleshooting

- Open the **Troubleshooting** for the IP of the PC or add the IP of the PC to the **Global Exclusion**. Check whether the access control policy that causes the website unable to access.

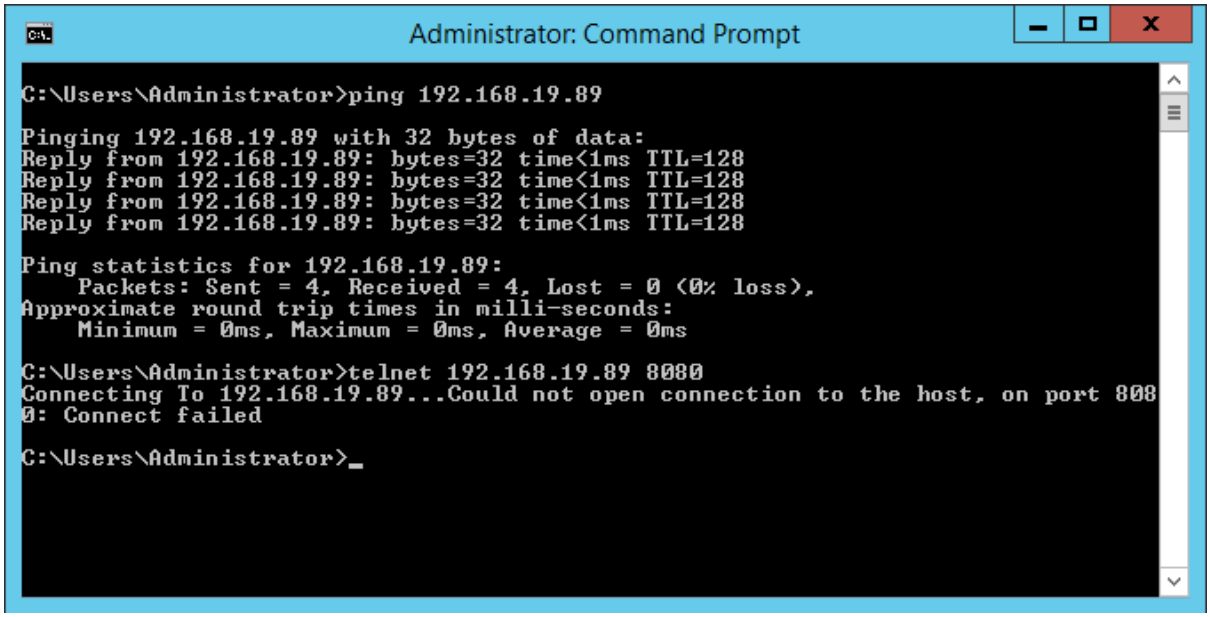

Global Exclusion
Predefined
Add Excluded Address
Description:
Optional
Addresses:
192.168.19.89
icbc.com.cn
OK
Cancel
Add
Delete
Commit



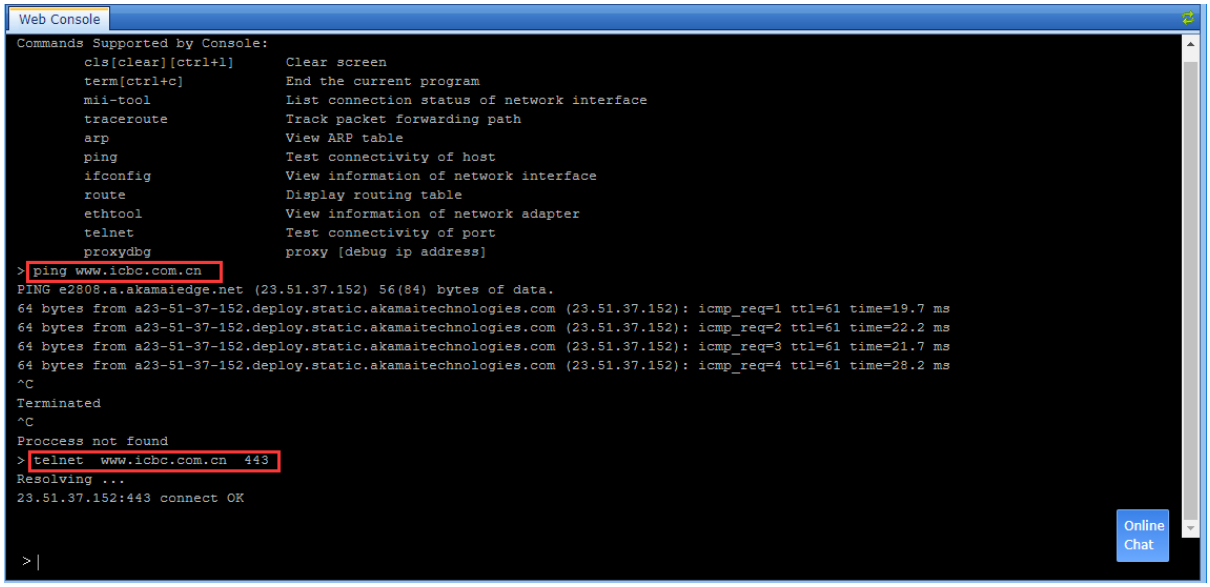
- Check if the proxy policy rejects the action, because **Troubleshooting** and **Global Exclusion** do not work for the proxy policy, so you need to check if the proxy policy itself has a rejection policy.



- Check if the PC and IAM can communicate. You can use **ping** and **telnet** commands to test connectivity.



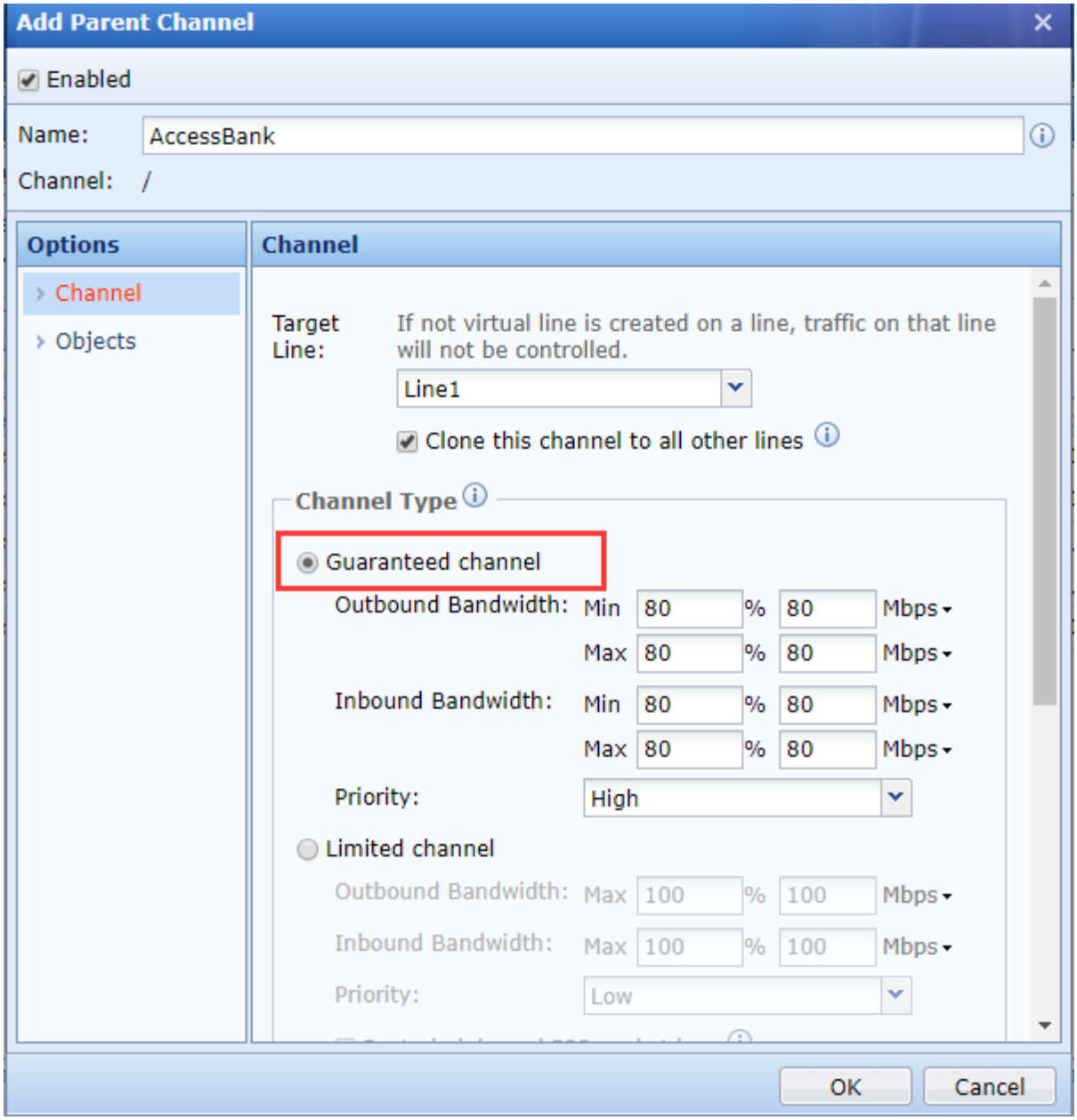
- Check if IAM can access the destination website normally.



3 Troubleshooting for slow website access

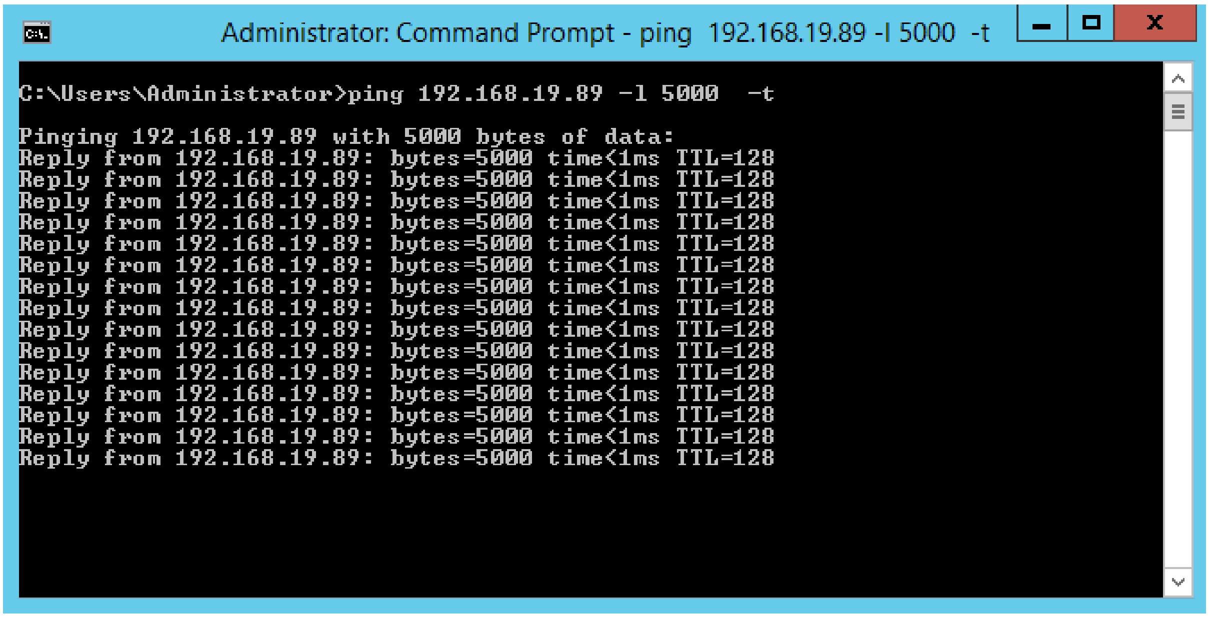
3.1 Confirm the details of the problem

- Confirm that it is slow to access all sites or to visit specific or partial sites.
- Confirm that all PCs are slow to access the website or only a few of PCs.
- Confirm whether it is slow to access the website all the time or at a specific time, such as the peak period of the network.
- If a large number of PCs are slow to access all websites, check if the network bandwidth is sufficient.
- If you are slow to access a few websites, you can first try to configure the policy to guarantee the bandwidth rate.

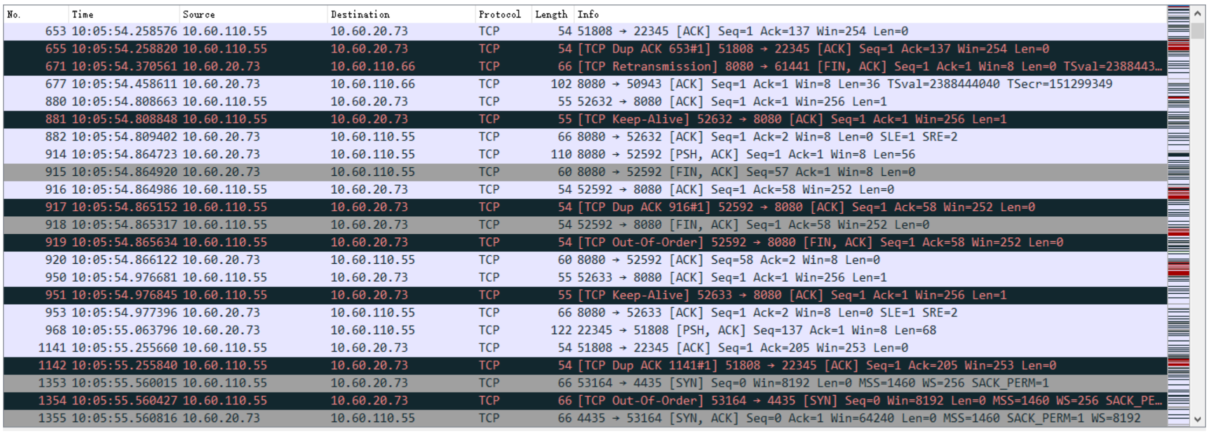


3.2 Confirm whether there is a high latency in the network

- Ping the IAM on the PC to see if there is a delay packet loss. You can specify the size of the ping packet.



- Ping the gateway and website address on the IAM to see if there is a delay packet loss.
- Use **wiresahrk** to capture packets on the PC and check if there are retransmission packets and out-of-order packets in the intranet transmission. If there are a large number of retransmissions and out-of-order packets, there is a problem with the intranet network.



3.3 Other troubleshooting

- Check the network topology. If there are devices such as Firewall between the network egress and IAM, consider whether the devices such as Firewall have restrictions on the number of IAM connections and network speed.
- If there is a firewall or other device between the IAM and the egress device, please give IAM sufficient bandwidth on the device such as Firewall. When the IAM is acting as a proxy, it carries a large amount of user traffic. The Firewall does not limit the IAM network speed but only indicates that IAM can use it freely. However, if other devices use up traffic, IAM still has no traffic to use, so you need to configure a security policy for IAM.
- You can try to change the DNS of IAM, for example, 8.8.8.8.

SANGFOR