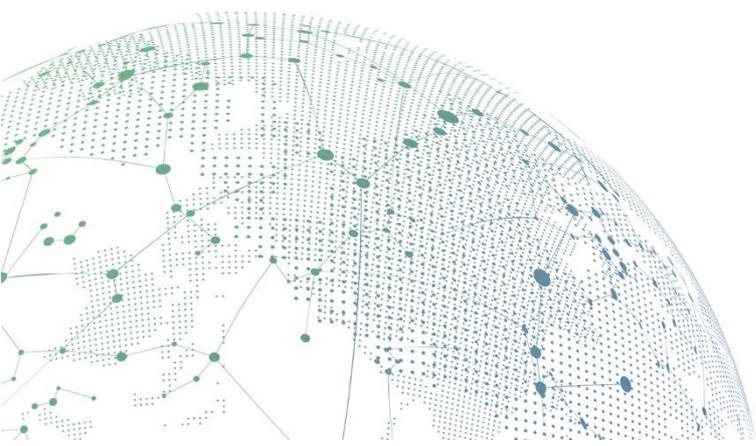


IAM

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.....	1
2 Troubleshooting when you can't open the website.....	1
2.1 Confirm whether this website supports proxy environment	1
2.2 Other troubleshooting.....	3
3 Troubleshooting for slow website access.....	7
3.1 Confirm the details of the problem.....	7
3.2 Confirm whether there is a high latency in the network	8
3.3 Other troubleshooting.....	9

1 Data interaction process in Proxy scenario

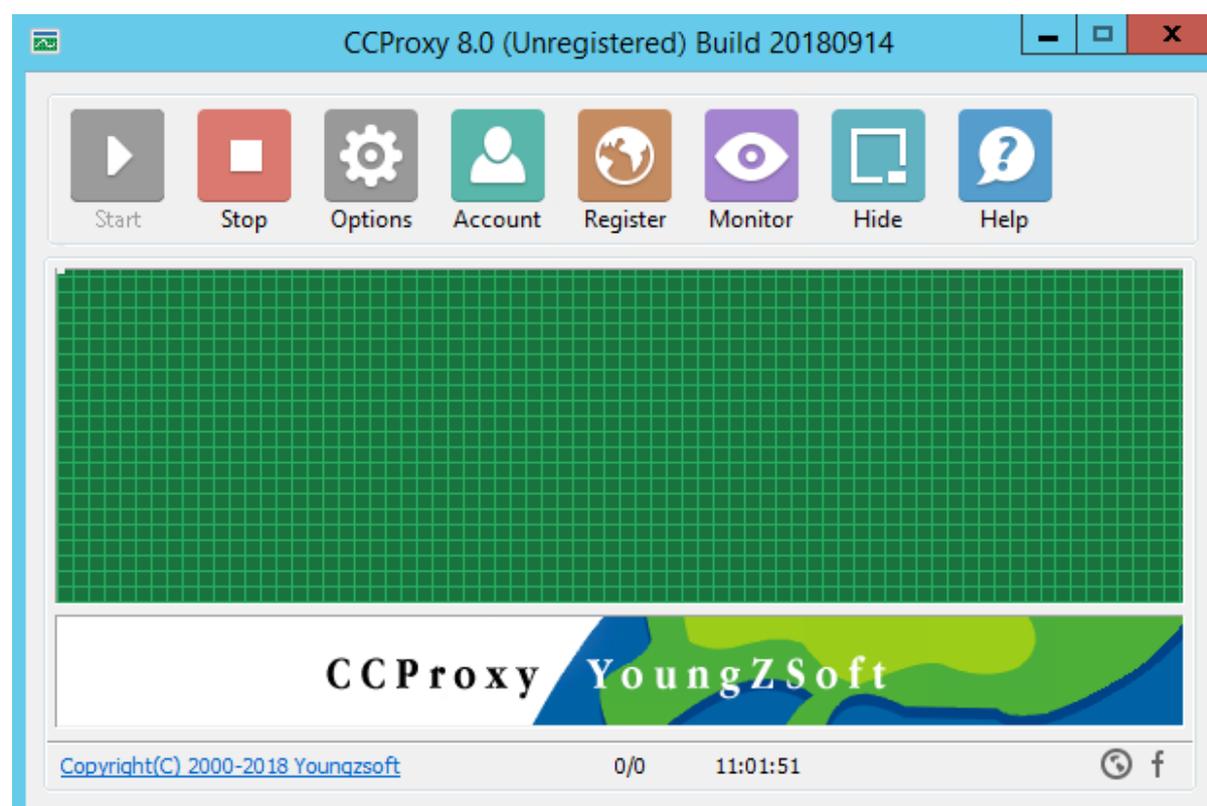
- PC and IAM establish a connection through the proxy port
- PC sends a GET request to IAM
- IAM sends a DNS request packet to get the IP of the website.
- IAM and website IP establish a connection
- IAM sends a GET request
- Website Server IP returns website data to IAM
- IAM will reply the data to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

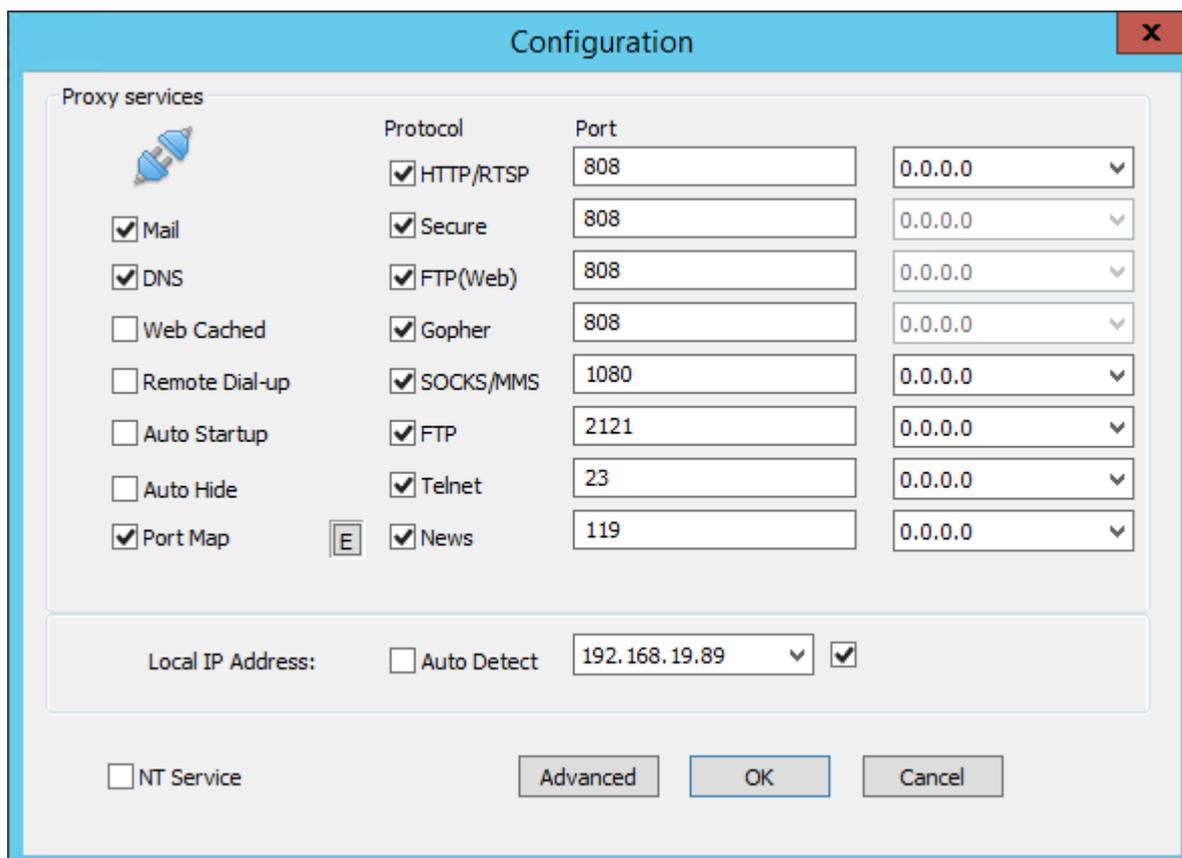
2 Troubleshooting when you can't open the website

2.1 Confirm whether this website supports proxy environment

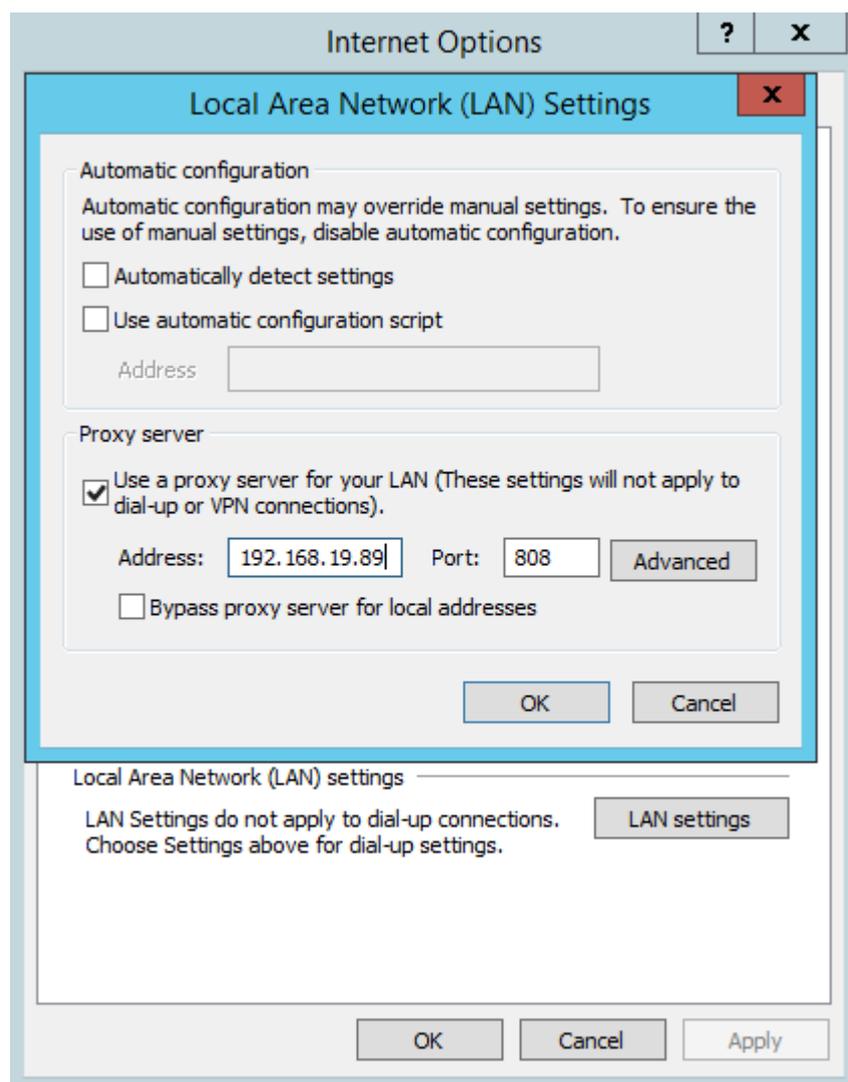
- Install a **ccproxy** on a PC1 that does not go through an IAM proxy, so that PC1 acts as a Proxy Server. Then prepare another test computer PC2, set PC1 as a proxy such in PC1 web browser's proxy settings, and open the website. This method is used to test whether the website supports proxy access.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

PC1:





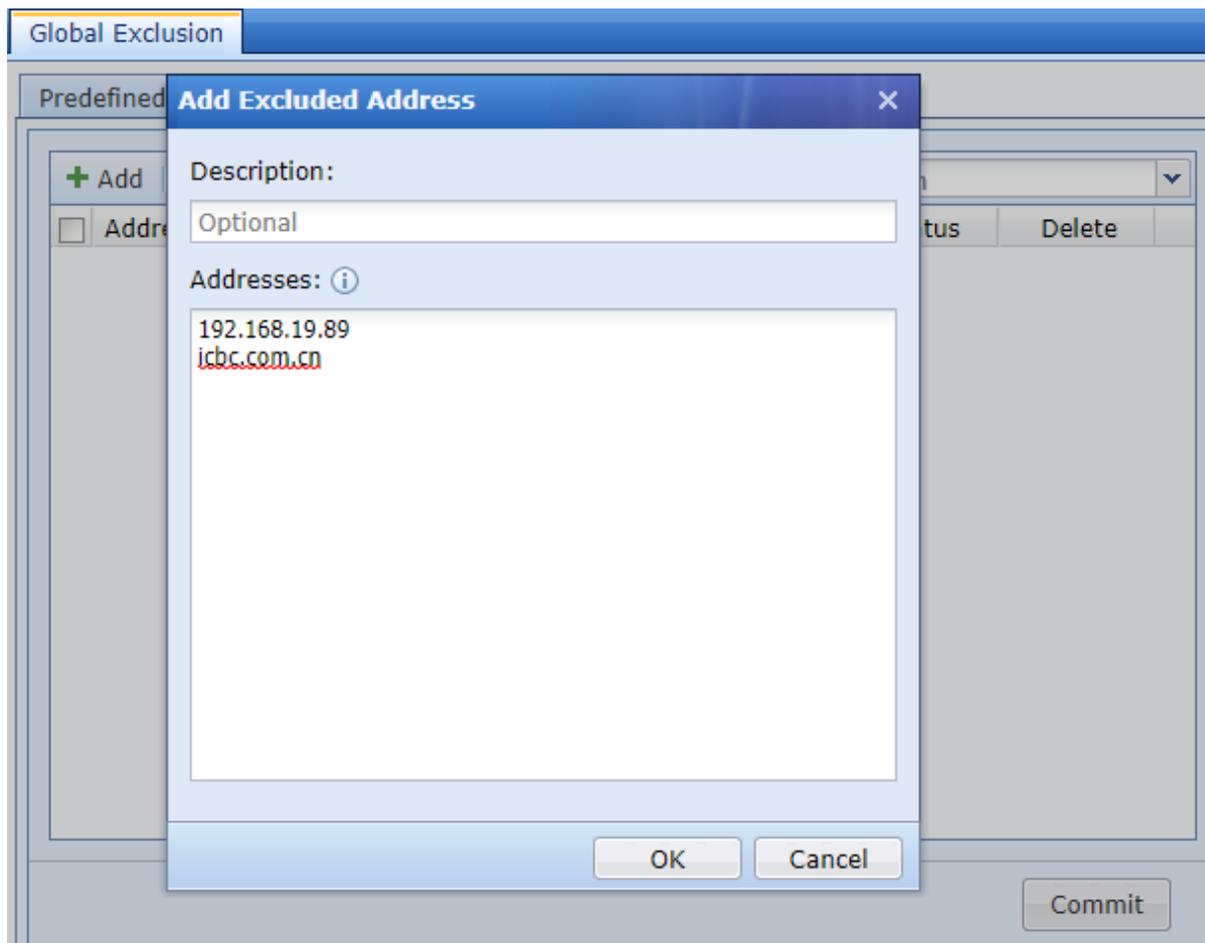
PC2:

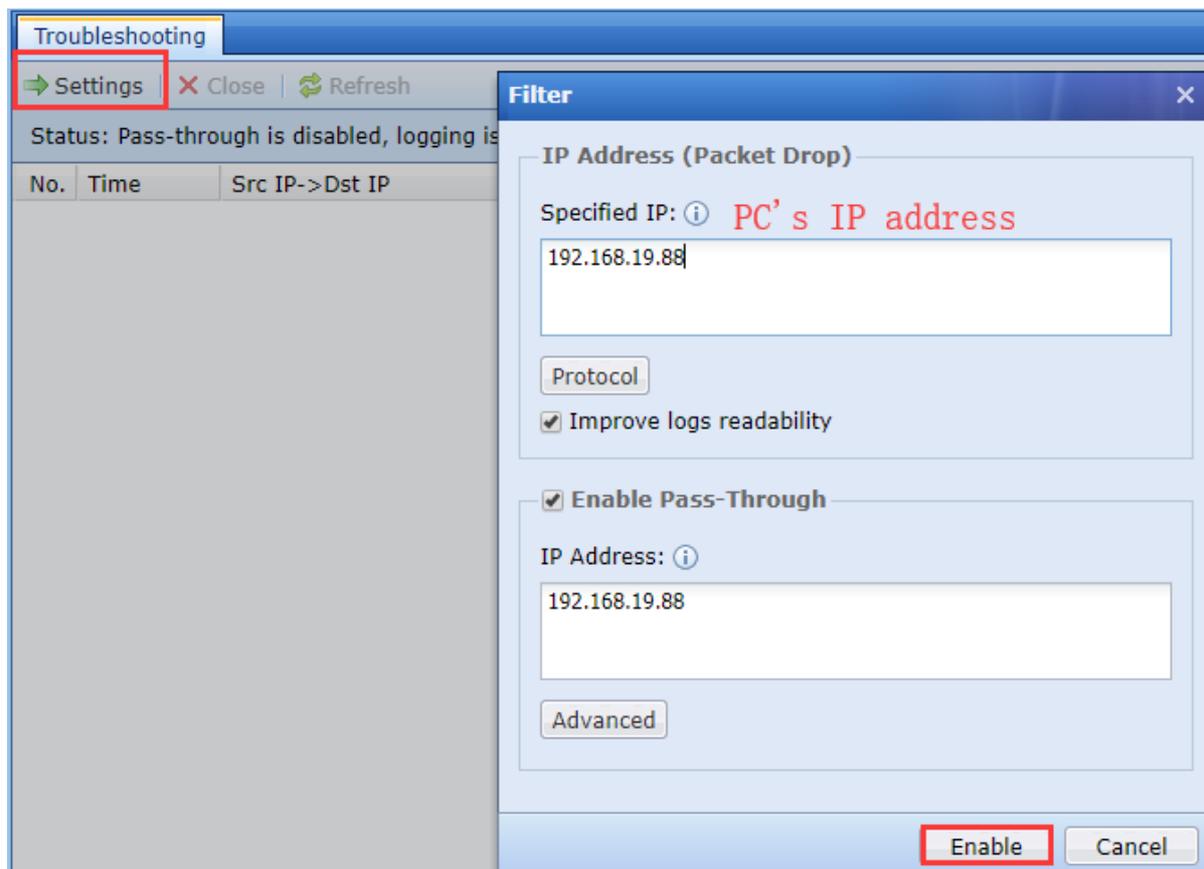


- Some video sites use special protocols when transmitting video data, and the protocol itself does not support proxies.
- Some bank websites use components such as ukey to secure information, while some ukeys do not support agents.

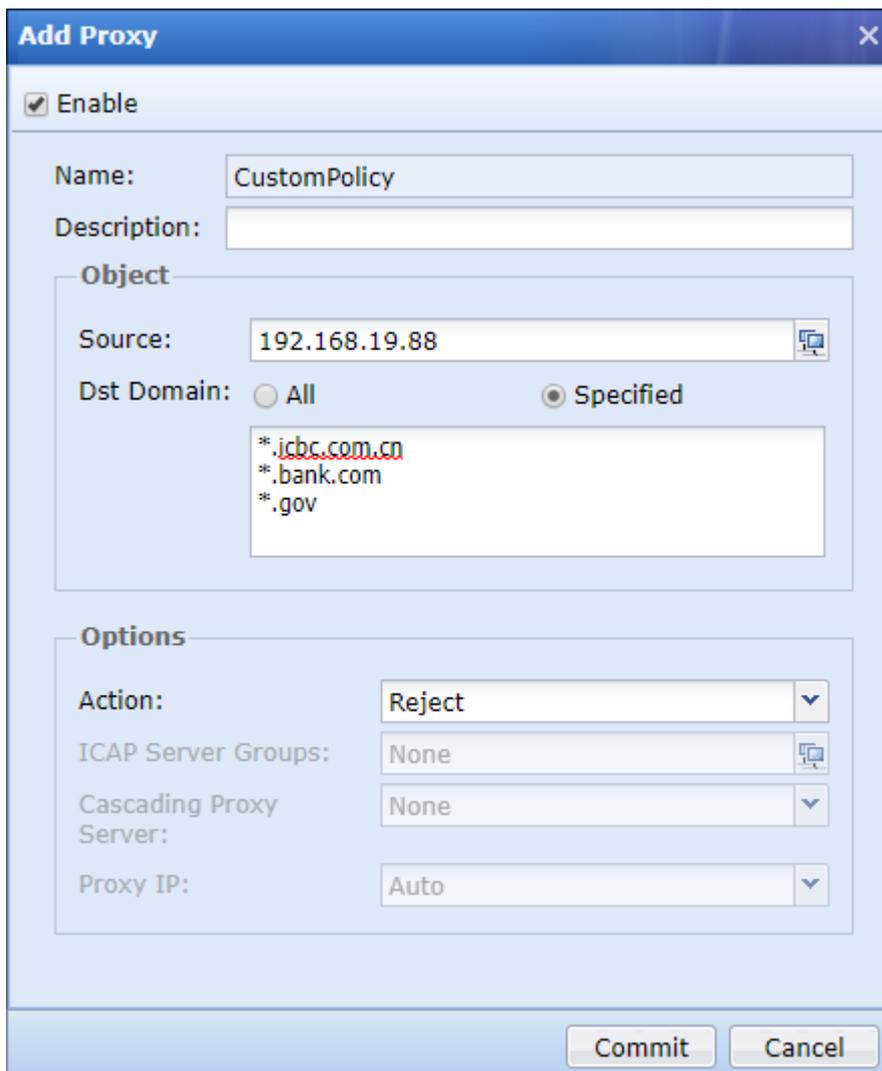
2.2 Other troubleshooting

- 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.





- 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.

```

Administrator: Command Prompt

C:\Users\Administrator>ping 192.168.19.89

Pinging 192.168.19.89 with 32 bytes of data:
Reply from 192.168.19.89: bytes=32 time<1ms TTL=128

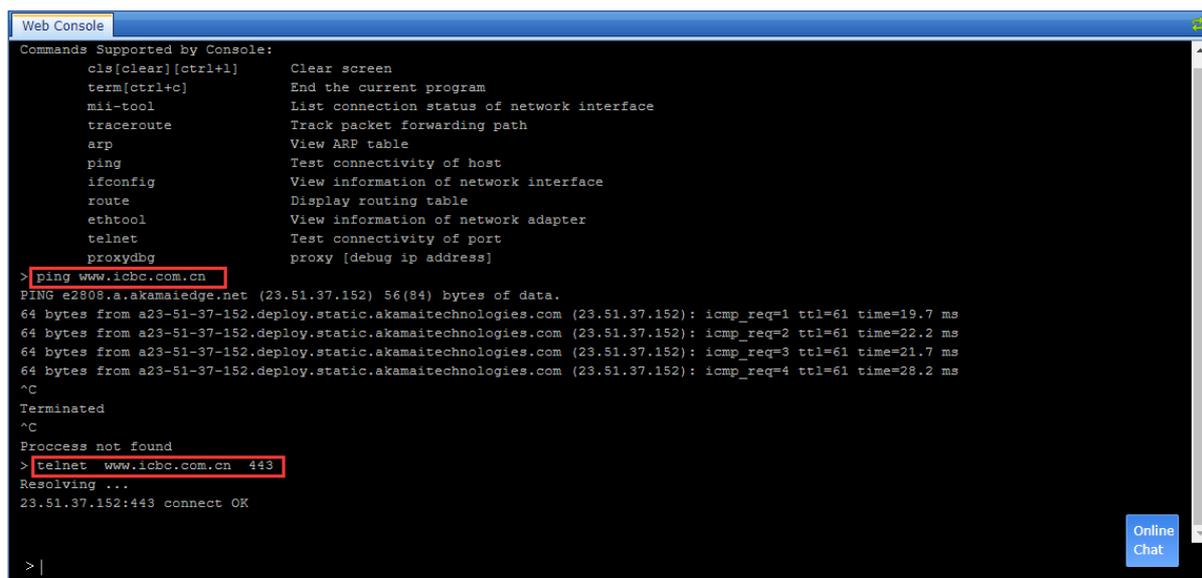
Ping statistics for 192.168.19.89:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>telnet 192.168.19.89 8080
Connecting To 192.168.19.89...Could not open connection to the host, on port 8080
0: Connect failed

C:\Users\Administrator>_

```

- Check if IAM can access the destination website normally.



```
Web Console
Commands Supported by Console:
cls[clear][ctrl+l]      Clear screen
term[ctrl+c]           End the current program
mii-tool               List connection status of network interface
traceroute             Track packet forwarding path
arp                   View ARP table
ping                  Test connectivity of host
ifconfig              View information of network interface
route                 Display routing table
ethtool              View information of network adapter
telnet               Test connectivity of port
proxydbg             proxy [debug ip address]
> ping www.icbc.com.cn
PING e2808.a.akamaiedge.net (23.51.37.152) 56(84) bytes of data.
64 bytes from a23-51-37-152.deploy.static.akamaitechnologies.com (23.51.37.152): icmp_req=1 ttl=61 time=19.7 ms
64 bytes from a23-51-37-152.deploy.static.akamaitechnologies.com (23.51.37.152): icmp_req=2 ttl=61 time=22.2 ms
64 bytes from a23-51-37-152.deploy.static.akamaitechnologies.com (23.51.37.152): icmp_req=3 ttl=61 time=21.7 ms
64 bytes from a23-51-37-152.deploy.static.akamaitechnologies.com (23.51.37.152): icmp_req=4 ttl=61 time=28.2 ms
^C
Terminated
^C
Process not found
> telnet www.icbc.com.cn 443
Resolving ...
23.51.37.152:443 connect OK

> |
```

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.

Add Parent Channel

Enabled

Name:

Channel: /

Options

- > Channel
- > Objects

Channel

Target Line: If not virtual line is created on a line, traffic on that line will not be controlled.

Clone this channel to all other lines

Channel Type

Guaranteed channel

Outbound Bandwidth: Min % Mbps ▾
Max % Mbps ▾

Inbound Bandwidth: Min % Mbps ▾
Max % Mbps ▾

Priority: ▾

Limited channel

Outbound Bandwidth: Max % Mbps ▾

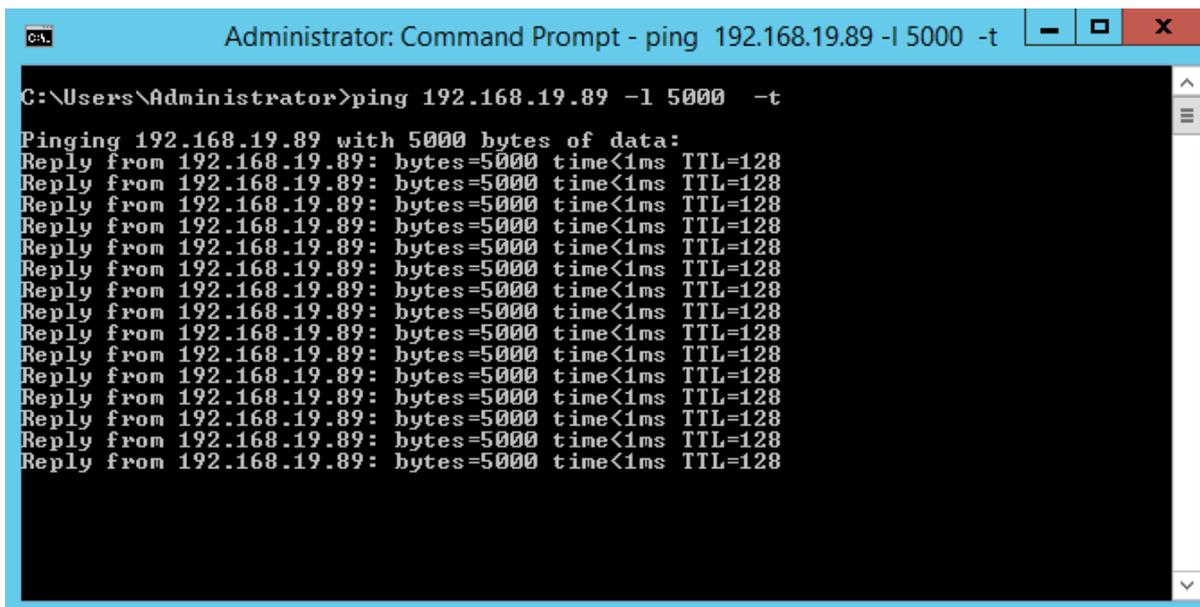
Inbound Bandwidth: Max % Mbps ▾

Priority: ▾

OK Cancel

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.

No.	Time	Source	Destination	Protocol	Length	Info
653	10:05:54.258576	10.60.110.55	10.60.20.73	TCP	54	51808 → 22345 [ACK] Seq=1 Ack=137 Win=254 Len=0
655	10:05:54.258820	10.60.110.55	10.60.20.73	TCP	54	[TCP Dup ACK 653#1] 51808 → 22345 [ACK] Seq=1 Ack=137 Win=254 Len=0
671	10:05:54.370561	10.60.20.73	10.60.110.66	TCP	66	[TCP Retransmission] 8080 → 61441 [FIN, ACK] Seq=1 Ack=1 Win=8 Len=0 TSval=2388443...
677	10:05:54.458611	10.60.20.73	10.60.110.66	TCP	102	8080 → 50943 [ACK] Seq=1 Ack=1 Win=8 Len=36 TSval=238844040 TSecr=151299349
880	10:05:54.808663	10.60.110.55	10.60.20.73	TCP	55	52632 → 8080 [ACK] Seq=1 Ack=1 Win=256 Len=1
881	10:05:54.808848	10.60.110.55	10.60.20.73	TCP	55	[TCP Keep-Alive] 52632 → 8080 [ACK] Seq=1 Ack=1 Win=256 Len=1
882	10:05:54.809402	10.60.20.73	10.60.110.55	TCP	66	8080 → 52632 [ACK] Seq=1 Ack=2 Win=8 Len=0 SLE=1 SRE=2
914	10:05:54.864723	10.60.20.73	10.60.110.55	TCP	110	8080 → 52592 [PSH, ACK] Seq=1 Ack=1 Win=8 Len=56
915	10:05:54.864920	10.60.20.73	10.60.110.55	TCP	60	8080 → 52592 [FIN, ACK] Seq=57 Ack=1 Win=8 Len=0
916	10:05:54.864986	10.60.110.55	10.60.20.73	TCP	54	52592 → 8080 [ACK] Seq=1 Ack=58 Win=252 Len=0
917	10:05:54.865152	10.60.110.55	10.60.20.73	TCP	54	[TCP Dup ACK 916#1] 52592 → 8080 [ACK] Seq=1 Ack=58 Win=252 Len=0
918	10:05:54.865317	10.60.110.55	10.60.20.73	TCP	54	52592 → 8080 [FIN, ACK] Seq=1 Ack=58 Win=252 Len=0
919	10:05:54.865634	10.60.110.55	10.60.20.73	TCP	54	[TCP Out-Of-Order] 52592 → 8080 [FIN, ACK] Seq=1 Ack=58 Win=252 Len=0
920	10:05:54.866122	10.60.20.73	10.60.110.55	TCP	60	8080 → 52592 [ACK] Seq=58 Ack=2 Win=8 Len=0
950	10:05:54.976681	10.60.110.55	10.60.20.73	TCP	55	52633 → 8080 [ACK] Seq=1 Ack=1 Win=256 Len=1
951	10:05:54.976845	10.60.110.55	10.60.20.73	TCP	55	[TCP Keep-Alive] 52633 → 8080 [ACK] Seq=1 Ack=1 Win=256 Len=1
953	10:05:54.977396	10.60.20.73	10.60.110.55	TCP	66	8080 → 52633 [ACK] Seq=1 Ack=2 Win=8 Len=0 SLE=1 SRE=2
968	10:05:55.063796	10.60.20.73	10.60.110.55	TCP	122	22345 → 51808 [PSH, ACK] Seq=137 Ack=1 Win=8 Len=68
1141	10:05:55.255660	10.60.110.55	10.60.20.73	TCP	54	51808 → 22345 [ACK] Seq=1 Ack=205 Win=253 Len=0
1142	10:05:55.255840	10.60.110.55	10.60.20.73	TCP	54	[TCP Dup ACK 1141#1] 51808 → 22345 [ACK] Seq=1 Ack=205 Win=253 Len=0
1353	10:05:55.560015	10.60.110.55	10.60.20.73	TCP	66	53164 → 4435 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1354	10:05:55.560427	10.60.110.55	10.60.20.73	TCP	66	[TCP Out-Of-Order] 53164 → 4435 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1355	10:05:55.560816	10.60.20.73	10.60.110.55	TCP	66	4435 → 53164 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=8192

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

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