SANGFOR

IAM

DNS Proxy Configuration Guide

Version 12.0.41

Change Log

Date	Change Description
Jan 9, 2020	Version 12.0.41 document release.

CONTENT

Chapter 1 Overview

The IAM is equipped with the function of a DNS proxy, which can replace DNS requests. Implement the requirement of "limiting illegal DNS requests" or forcibly redirecting certain domain names to your own server.

Chapter 2 Solution Advantages

IAM supports DNS proxy function. Users can set DNS proxy scope according to the end user group, website type, domain name, and target DNS address. It supports redirecting to a specified DNS server, redirecting a specified line, resolving fixed IP, and discarding. the way.

When multiple Internet links are deployed in the network, intranet users fill in the DNS server of one of the operators when they go online, so most users are assigned to the same link, making the link always In a busy state, the access speed of users accessed by this link decreases, while the other link is idle. The imbalance of link utilization causes waste of Internet resources on the one hand, and the user's access speed cannot be guaranteed on the other.

Through the DNS transparent proxy technology, no matter which operator's DNS server address is entered by the intranet user, the DNS request will be forwarded through the Sangfor Internet behavior management device, and a suitable DNS server will be found and returned to the intranet computer. The load algorithm can distribute traffic to different links according to the set link utilization policy.

In this case, the traffic of the two links in the user's network will be the same as the manager expects from beginning to end, ensuring the utilization of each link.

Chapter 3 Scenario

Redirect to DNS server: Redirect the original DNS server to the configured DNS server IP

Resolve to IP address: directly resolve the domain name to the specified IP

Drop DNS packet: directly drop DNS request packets

Forward to specified line: redirect to the specified exit

Note:

1. In the Forward to specified line strategy, network ports are displayed in routing mode and virtual lines are displayed in bridge mode.

2. In the Forward to specified line policy, you cannot select a line that is not configured with dns.

Chapter 4 Configuration Method

4.1 Redirect to DNS server

4.1.1 Test Conditions

Prepare an IAM device for deployment in routing or bridge mode

4.1.2 Expected result

Access the specified domain name, forcibly redirect to the specified DNS server for resolution.

4.1.3 Configuration Steps

4.1.3.1 Description of requirements

Forcibly redirect user A's DNS request for domain name www.baidu.com to DNS server 114.114.114.114 to resolve

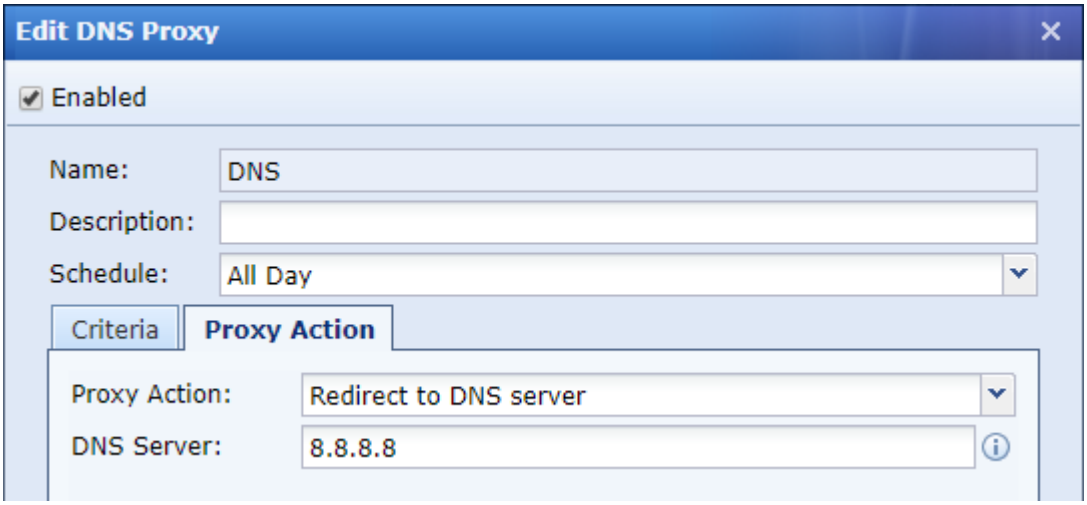
4.1.3.2 Configuration

1. Configure DNS Policy-Proxy Conditions

Select user "A", define the domain name "www.baidu.com", and test that the DNS configured on the user's computer is the target DNS address "3.3.3.3"

2. Configure DNS Policy-Proxy Action

Select " Redirect to DNS server" as proxy policy, and fill in the DNS address you want to use to resolve

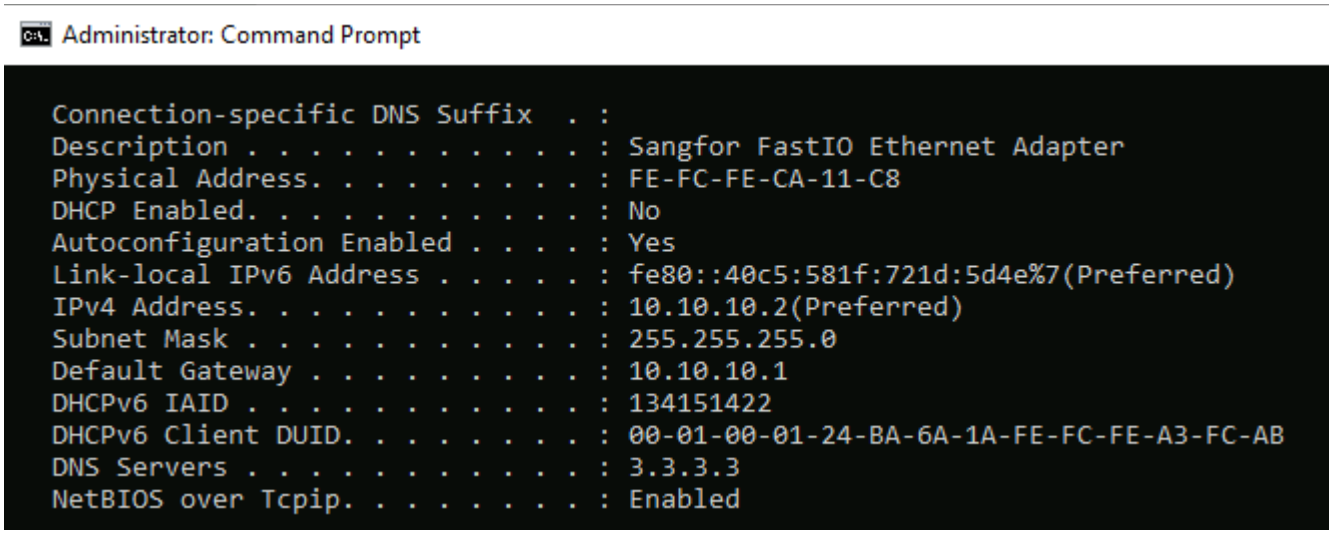


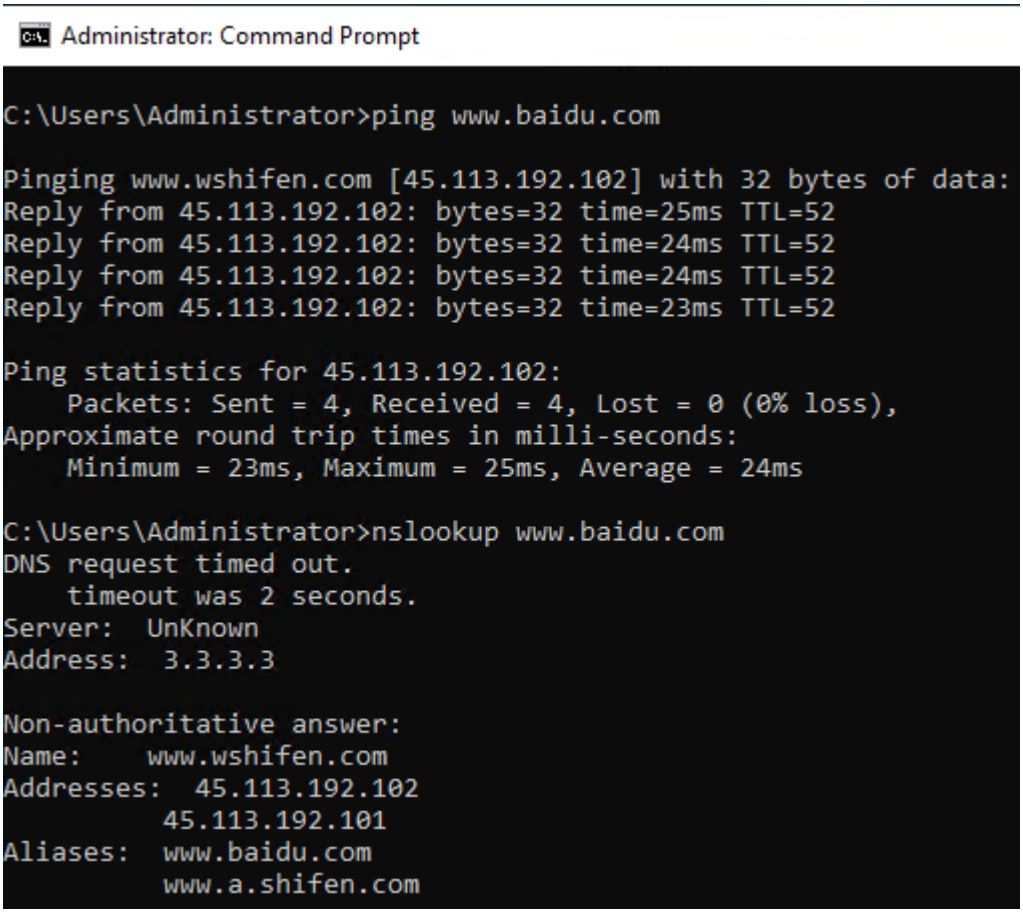
4.1.3.3 Effect presentation

The target dns is configured with a non-effective DNS; the test computer is configured with a non-effective DNS.

Test computer using nslookup to detect www.baidu.com was unsuccessful, but the ping test was successful

Pinged before, use ipconfig/flushdns to clear the cache





4.2 Resolve to IP address

4.2.1 Test Conditions

Prepare an IAM device for deployment in routing or bridge mode

4.2.2 Expected result

Forcibly resolves the name to the specified IP when accessing the specified domain name.

4.2.3 Configuration Steps

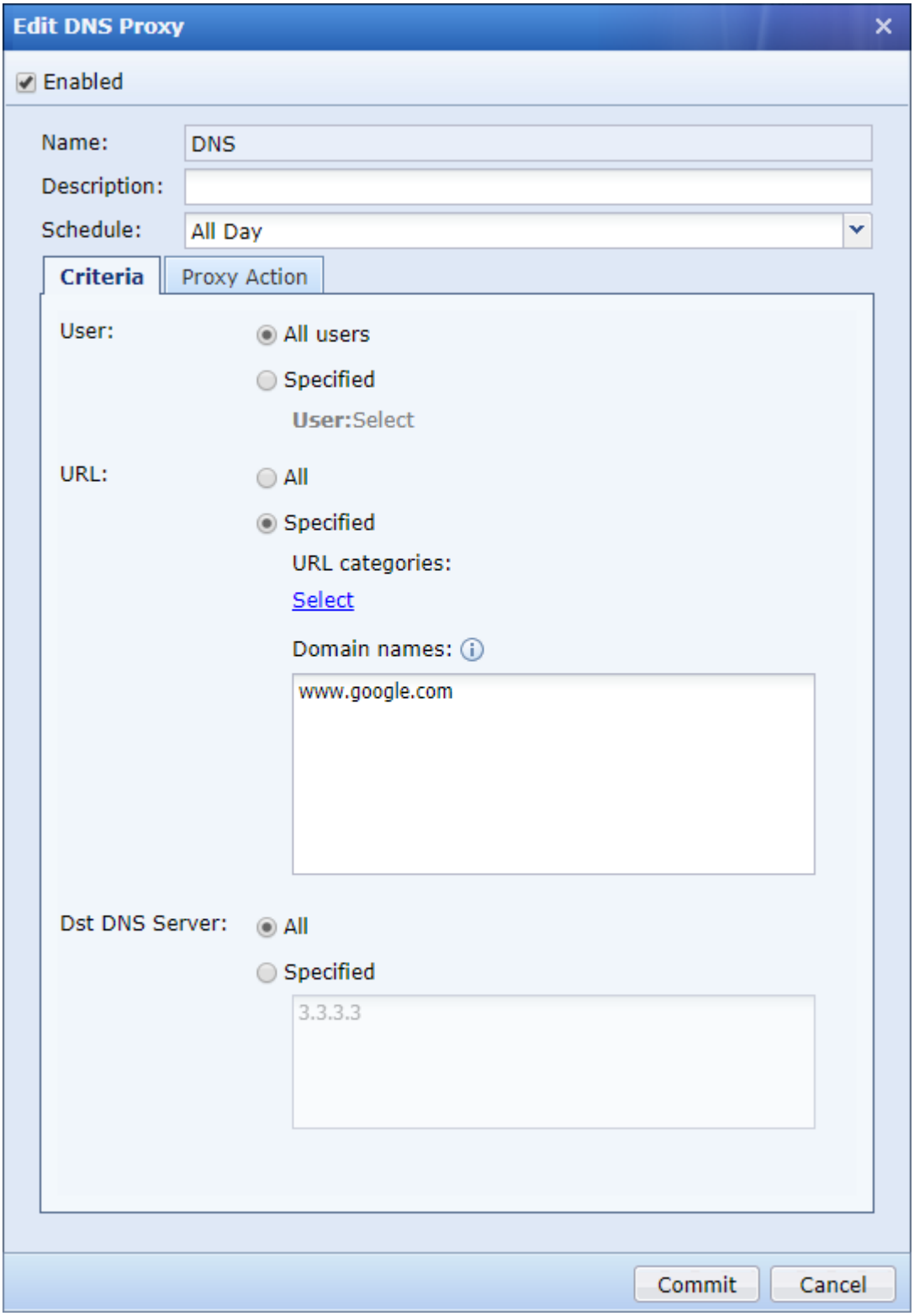
4.2.3.1 Description of requirements

Forcibly resolve DNS requests for users accessing the domain name www.google.com to 6.7.8.9

4.2.3.2 Configuration

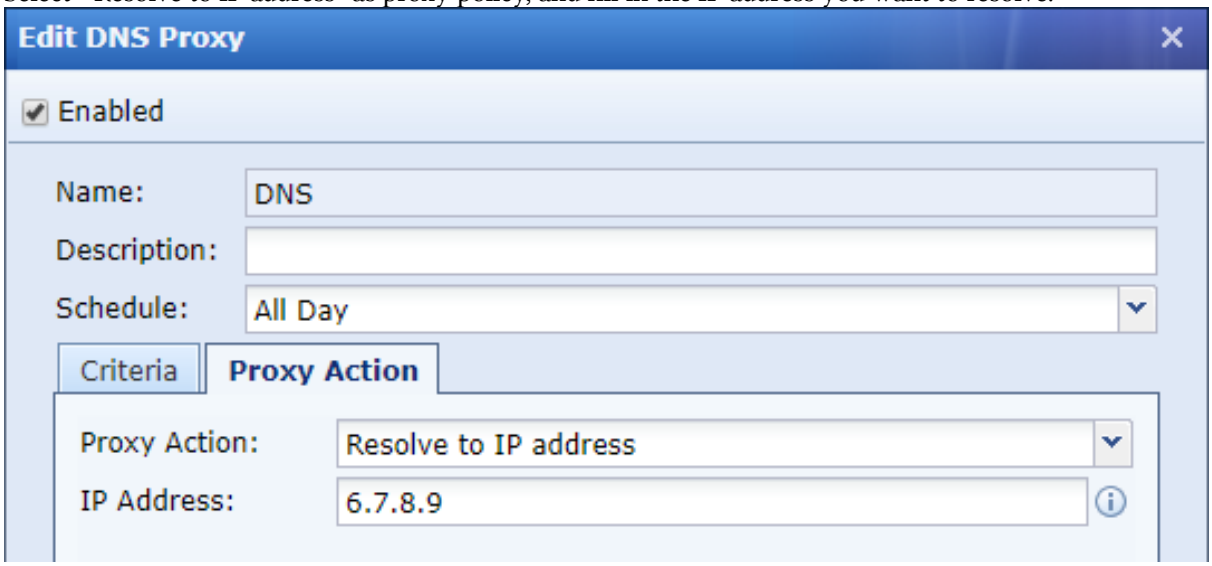
1. Configure DNS Policy-Proxy Criteria

For all users, define the access domain name "www.google.com" and test that the DNS configured on the user's computer is the target DNS address "all":



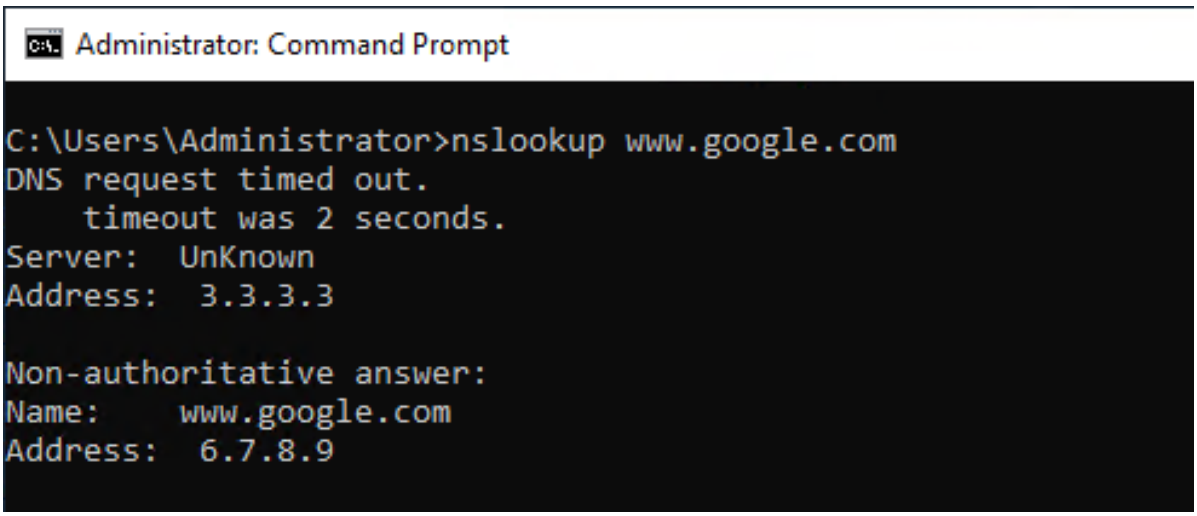
2. Configure DNS Policy-Proxy Action

Select " Resolve to IP address" as proxy policy, and fill in the IP address you want to resolve.



4.2.3.3 Effect presentation

Using nslookup on the test computer, you can see that the target domain name www.google.com is resolved to 6.7.8.9



4.3 Drop DNS packet

4.3.1 Test Conditions

Prepare an IAM device for deployment in routing or bridge mode

4.3.2 Expected result

When a user accesses a specified domain name, IAM discards DNS request packets.

4.3.3 Configuration Steps

4.3.3.1 Description of requirements

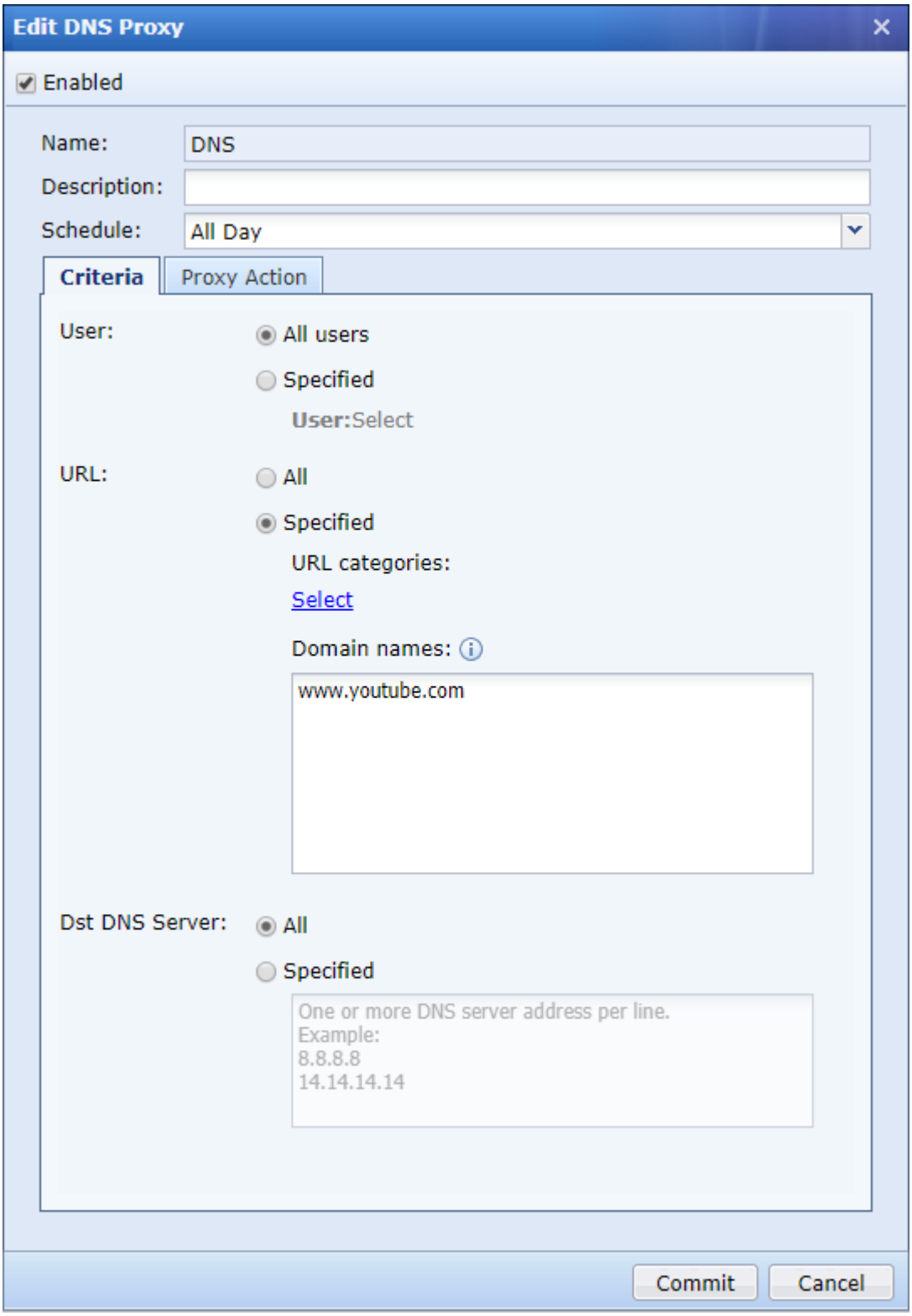
IAM forcibly drops DNS request packets when users visit www.youtube.com

4.3.3.2 Configuration

1. Configure DNS Policy-Proxy Criteria

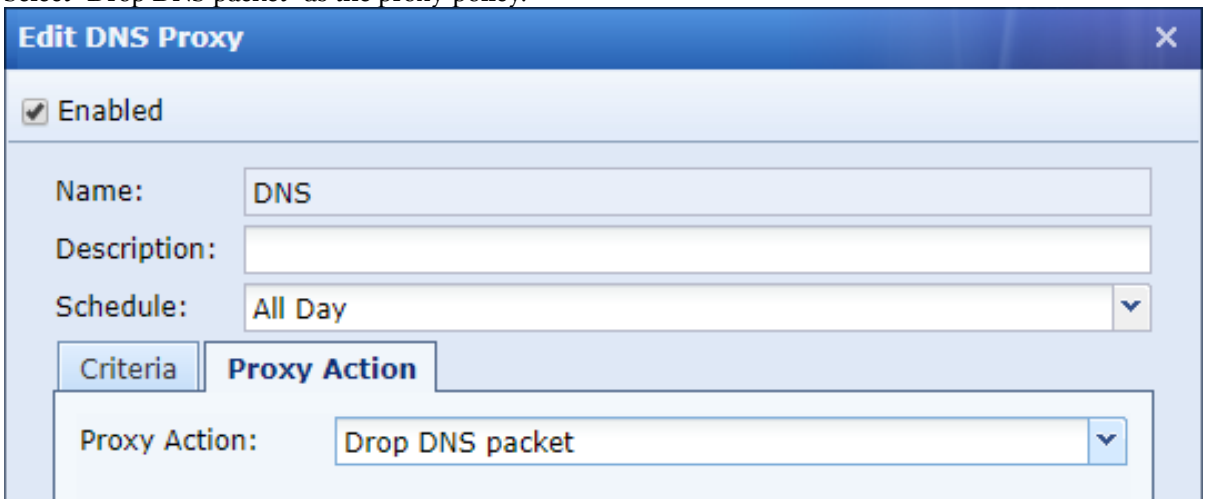
For all users, define the access domain name "www.youtube.com" and test that the DNS configured on

the user's computer is the target DNS address "all".



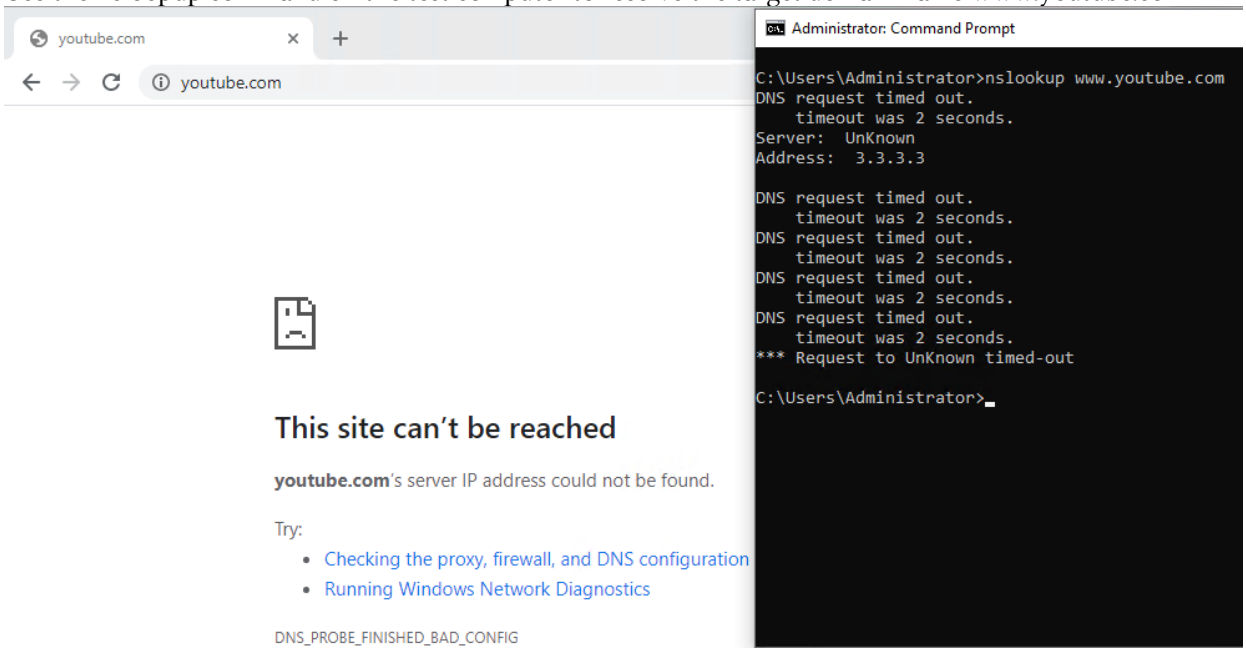
2. Configure DNS Policy-Proxy Action

Select "Drop DNS packet" as the proxy policy.



4.3.3.3 Effect presentation

Use the nsloopup command on the test computer to resolve the target domain name www.youtube.com



4.4 Forward to specified line

4.4.1 Test Conditions

Prepare an IAM device for deployment in routing or bridge mode

Device must be multi-line enabled

The device must be configured with the Policy-Based Routing

4.4.2 Expected result

When a user accesses a specified domain name, IAM forces the traffic to go through the specified line.

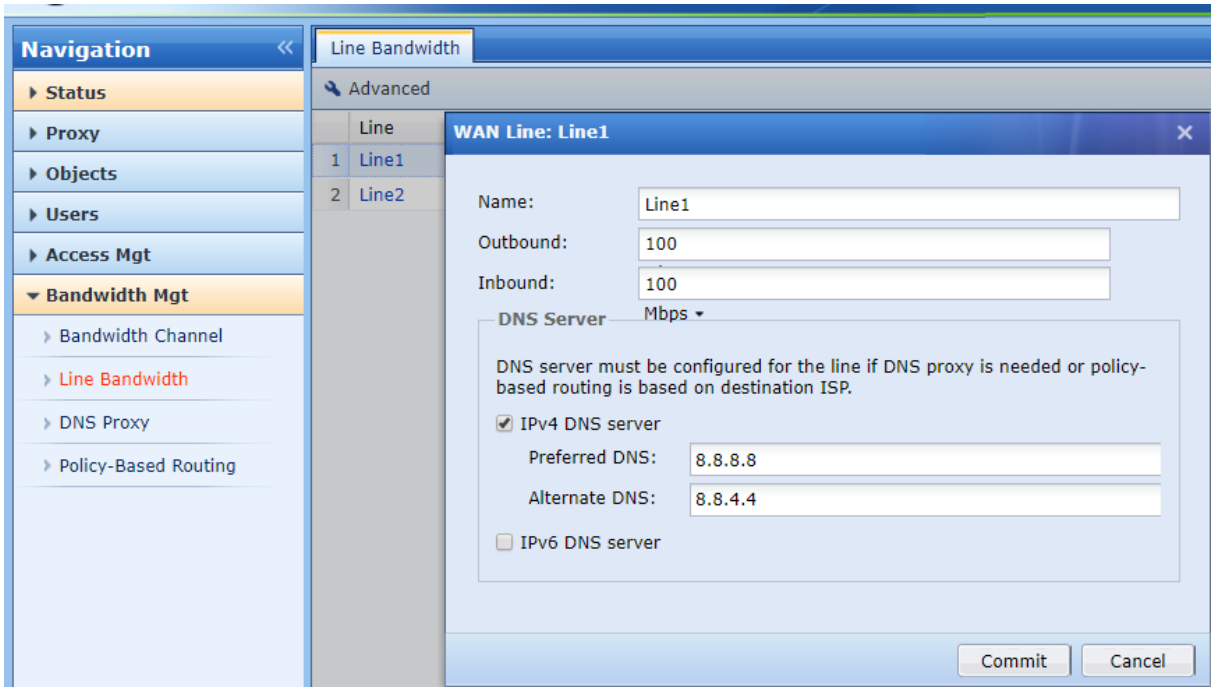
4.4.3 Configuration Steps

4.4.3.1 Description of requirements

The user visits the domain name www.twitter.com, and IAM sends traffic from line 2.

4.4.3.2 Configuration

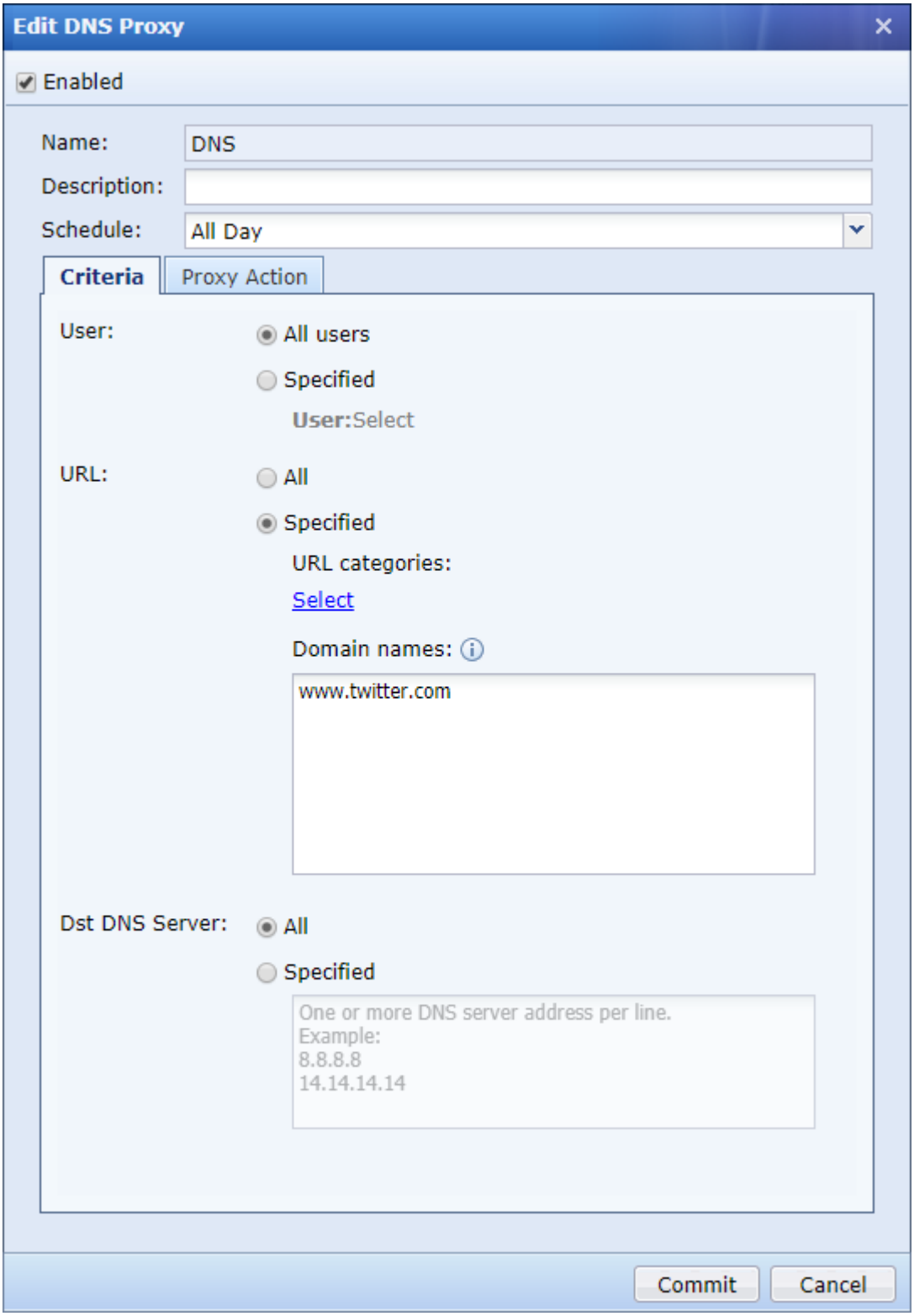
1. Enable DNS server for the line and configure DNS



DNS configuration can be configured in " Deployment", " Line Bandwidth" or " Interfaces".

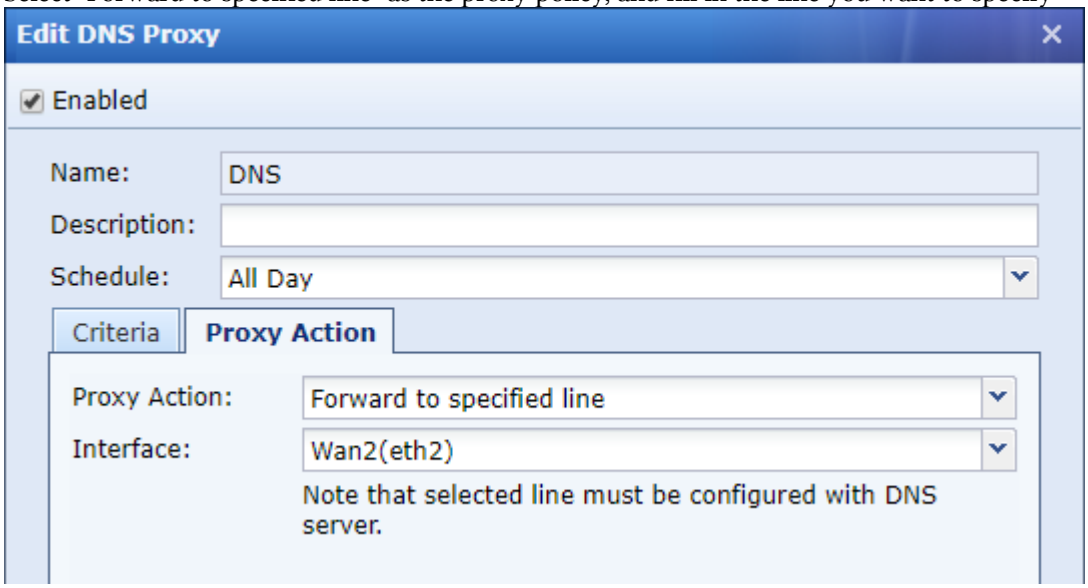
2. Configure DNS Policy-Proxy Criteria

For all users, define the access domain name "www.twitter.com" and test that the DNS configured on the user's computer is the target DNS address "all"



3. Configure DNS Policy-Proxy Action

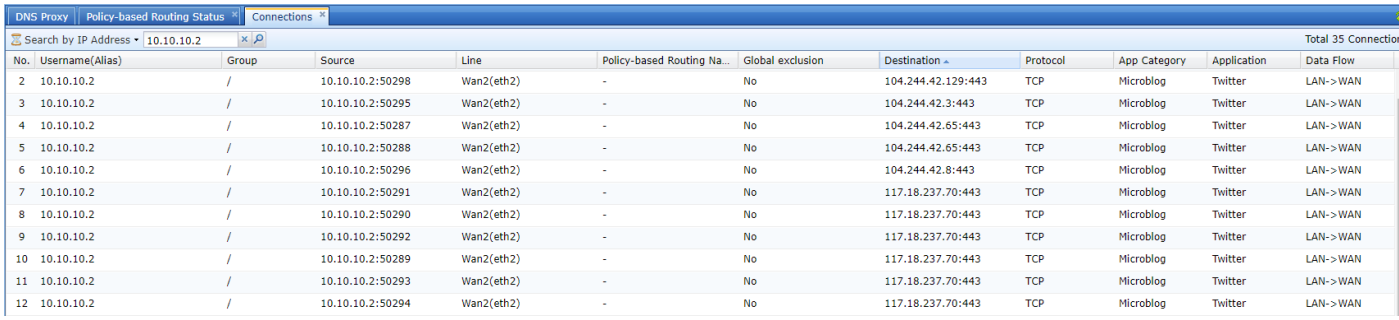
Select "Forward to specified line" as the proxy policy, and fill in the line you want to specify



Only the line configured with DNS or DSCP / TOS value can be selected. This function does not take effect when the Policy-Based Routing is not enabled.

4.4.3.2 Effect presentation

Visit the target domain name www.twitter.com on the test computer, and check on the IAM device "Traffic Statistics"-"Link Load Status"



Chapter 5 Precautions

1. Proxy to the intranet DNS server: DNS proxy policy proxy to the intranet DNS server (DNS server is in the DMZ area)

Phenomenon:

Proxy to the intranet DNS server fails (if the user's own computer has a valid DNS server configured, then use his own DNS server, and the invalid DNS server will cause the network to be disconnected)

Solution:

Firewall configuration allows traffic from DMZ-> LAN

2. Does the DNS proxy function take effect when global exclusion and pass-through are enabled?

After the DNS proxy is configured with "Drop DNS packet" and the domain name is added to the global exclusion, the DNS proxy "Drop DNS packet" policy no longer takes effect;

After the pass-through is enabled, the DNS proxy does not take effect.

3. In the bridge mode, if the DNS detection is to send packets from the dmz port to detect, you need to ensure that the packets sent from the dmz port can reach the exit.