



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	1
Chapter 2 Solution Advantages	1
Chapter 3 Scenario	1
Chapter 4 Configuration Method	1
4.1 Redirect to DNS server	1
4.1.1 Test Conditions	1
4.1.2 Expected result	1
4.1.3 Configuration Steps	1
4.1.3.1 Description of requirements	2
4.1.3.2 Configuration	2
4.1.3.3 Effect presentation	3
4.2 Resolve to IP address	4
4.2.1 Test Conditions	4
4.2.2 Expected result	4
4.2.3 Configuration Steps	4
4.2.3.1 Description of requirements	4
4.2.3.2 Configuration	4
4.2.3.3 Effect presentation	6
4.3 Drop DNS packet	6
4.3.1 Test Conditions	6
4.3.2 Expected result	6
4.3.3 Configuration Steps	6
4.3.3.1 Description of requirements	6
4.3.3.2 Configuration	6
4.3.3.3 Effect presentation	8
4.4 Forward to specified line	8
4.4.1 Test Conditions	8
4.4.2 Expected result	8
4.4.3 Configuration Steps	8
4.4.3.1 Description of requirements	8
4.4.3.2 Configuration	9
4.4.3.3 Effect presentation	11
Chapter 5 Precautions	11

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"

Add DNS Proxy

☒ Enabled

Name:

Description:

Schedule:

Criteria | Proxy Action

User: ☐ All users
☒ Specified
User:a

URL: ☐ All
☒ Specified
URL categories:
[Select](#)

Domain names: ⓘ

Dst DNS Server: ☐ All
☒ Specified

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

Edit DNS Proxy

☒ Enabled

Name:

Description:

Schedule:

Criteria **Proxy Action**

Proxy Action:

DNS Server:

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

Administrator: Command Prompt

```

Connection-specific DNS Suffix  . : 
Description . . . . . : Sangfor FastIO Ethernet Adapter
Physical Address. . . . . : FE-FC-FE-CA-11-C8
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::40c5:581f:721d:5d4e%7(Preferred)
IPv4 Address. . . . . : 10.10.10.2(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.10.10.1
DHCPv6 IAID . . . . . : 134151422
DHCPv6 Client DUID. . . . . : 00-01-00-01-24-BA-6A-1A-FE-FC-FE-A3-FC-AB
DNS Servers . . . . . : 3.3.3.3
NetBIOS over Tcpip. . . . . : Enabled

```

```
Administrator: Command Prompt

C:\Users\Administrator>ping www.baidu.com

Pinging www.wshifen.com [45.113.192.102] with 32 bytes of data:
Reply from 45.113.192.102: bytes=32 time=25ms TTL=52
Reply from 45.113.192.102: bytes=32 time=24ms TTL=52
Reply from 45.113.192.102: bytes=32 time=24ms TTL=52
Reply from 45.113.192.102: bytes=32 time=23ms TTL=52

Ping statistics for 45.113.192.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 23ms, Maximum = 25ms, Average = 24ms

C:\Users\Administrator>nslookup www.baidu.com
DNS request timed out.
    timeout was 2 seconds.
Server:    UnKnown
Address:   3.3.3.3

Non-authoritative answer:
Name:      www.wshifen.com
Addresses: 45.113.192.102
           45.113.192.101
Aliases:   www.baidu.com
           www.a.shifen.com
```

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`":

Edit DNS Proxy [X]

☒ Enabled

Name:

Description:

Schedule: ▼

Criteria | Proxy Action

User: ☒ All users
☐ Specified
User: [Select](#)

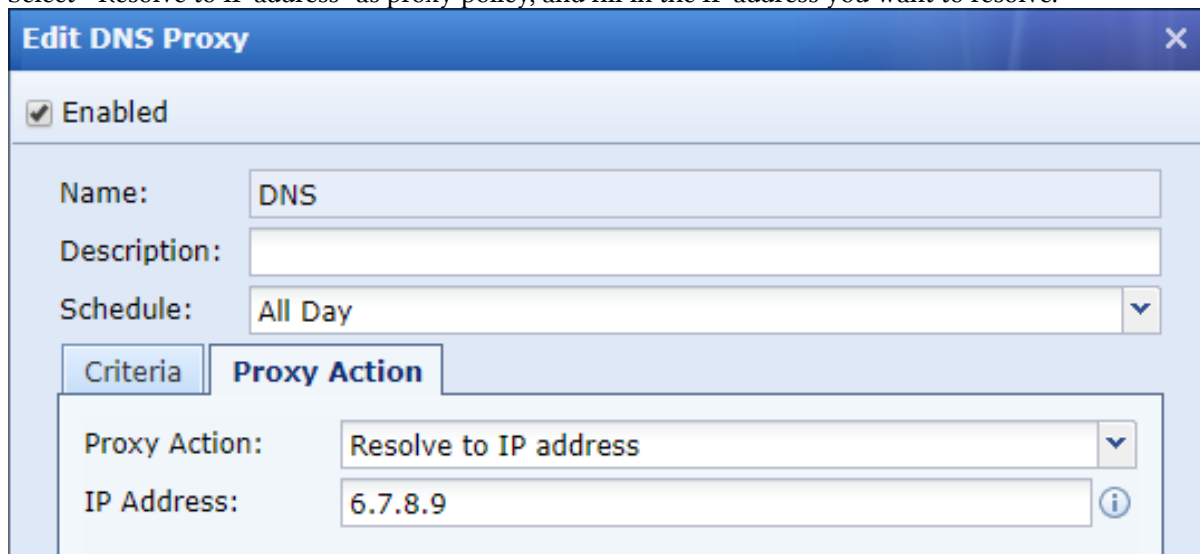
URL: ☐ All
☒ Specified
URL categories: [Select](#)

Domain names: ⓘ

Dst DNS Server: ☒ All
☐ Specified

2. Configure DNS Policy-Proxy Action

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



Edit DNS Proxy

☒ Enabled

Name:

Description:

Schedule:

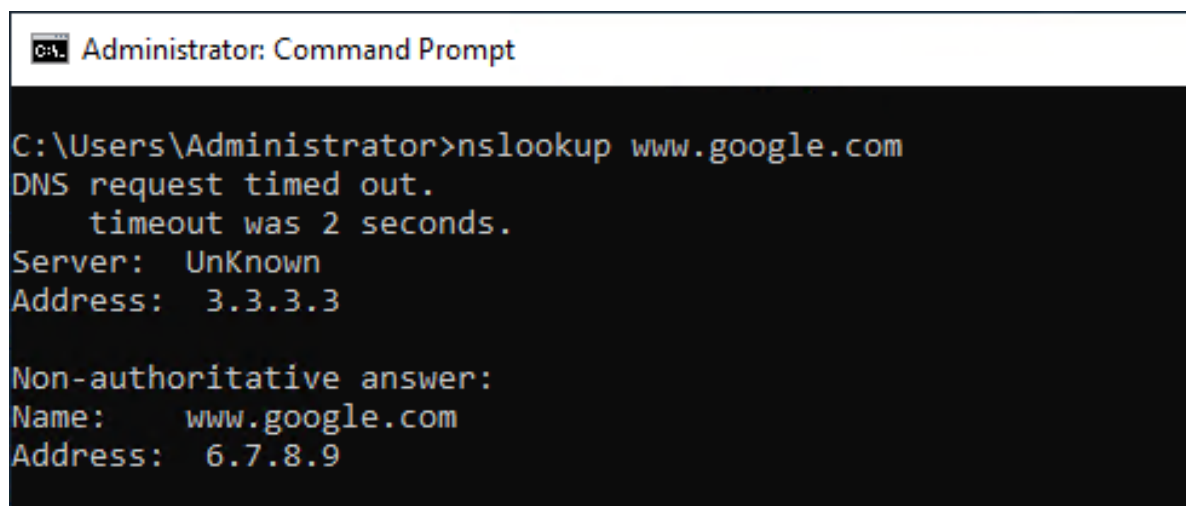
Criteria **Proxy Action**

Proxy Action:

IP Address:

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



```

Administrator: Command Prompt

C:\Users\Administrator>nslookup www.google.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  3.3.3.3

Non-authoritative answer:
Name:     www.google.com
Address:  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".

Edit DNS Proxy

☒ Enabled

Name:

Description:

Schedule:

Criteria **Proxy Action**

User: ☒ All users
☐ Specified
User:Select

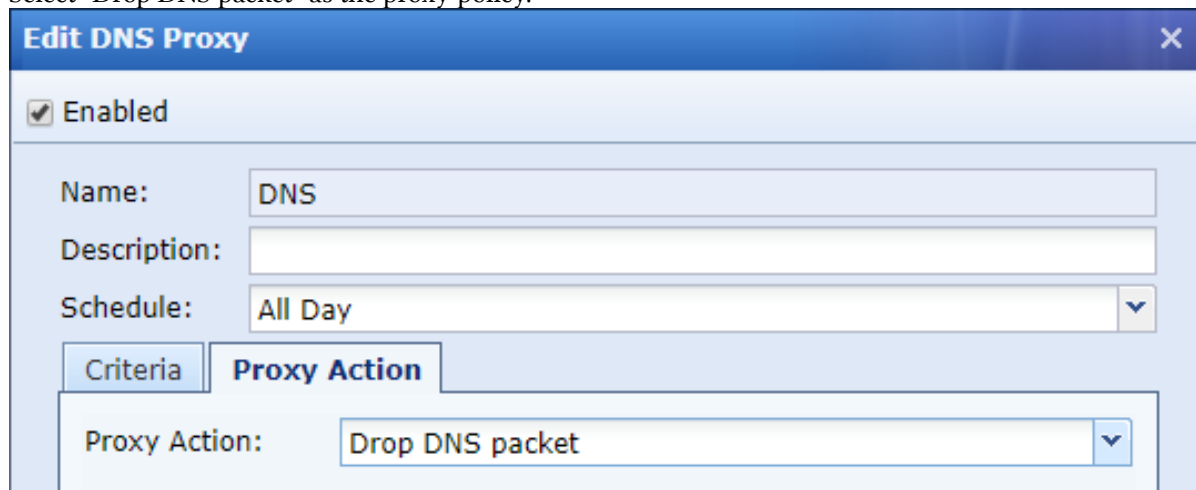
URL: ☐ All
☒ Specified
URL categories:
[Select](#)

Domain names: ⓘ

Dst DNS Server: ☒ All
☐ Specified

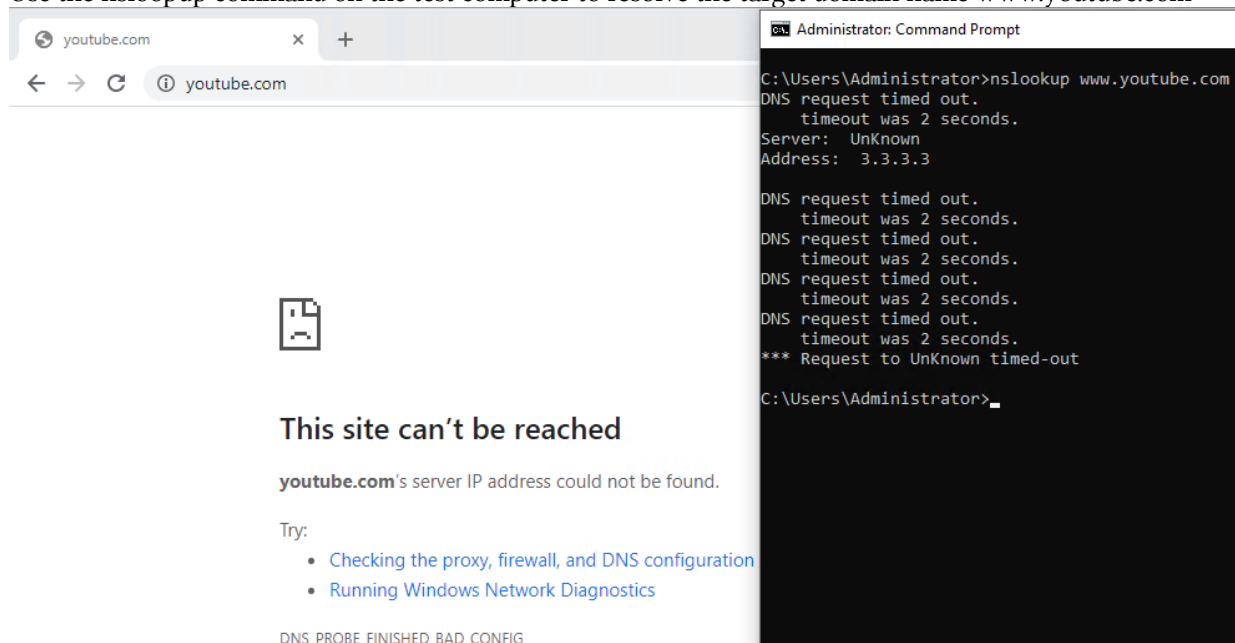
2. Configure DNS Policy-Proxy Action

Select "Drop DNS packet" as the proxy policy.



4.3.3.3 Effect presentation

Use the nslookup 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

The screenshot displays the Sangfor IAM configuration interface. On the left is a 'Navigation' sidebar with a tree view containing: Status, Proxy, Objects, Users, Access Mgt, and Bandwidth Mgt (expanded). Under 'Bandwidth Mgt', the options are: Bandwidth Channel, Line Bandwidth (highlighted in red), DNS Proxy, and Policy-Based Routing. The main area shows the 'Line Bandwidth' configuration for 'Line1'. A table lists two lines: Line1 and Line2. The 'WAN Line: Line1' configuration window is open, showing fields for Name (Line1), Outbound (100), and Inbound (100). Below these is a 'DNS Server' section with a 'Mbps' dropdown. A note states: 'DNS server must be configured for the line if DNS proxy is needed or policy-based routing is based on destination ISP.' There are two checkboxes: 'IPv4 DNS server' (checked) and 'IPv6 DNS server' (unchecked). Under 'IPv4 DNS server', there are fields for 'Preferred DNS' (8.8.8.8) and 'Alternate DNS' (8.8.4.4). At the bottom right of the window are 'Commit' and 'Cancel' buttons.

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"

Edit DNS Proxy

☒ Enabled

Name:

Description:

Schedule:

Criteria | Proxy Action

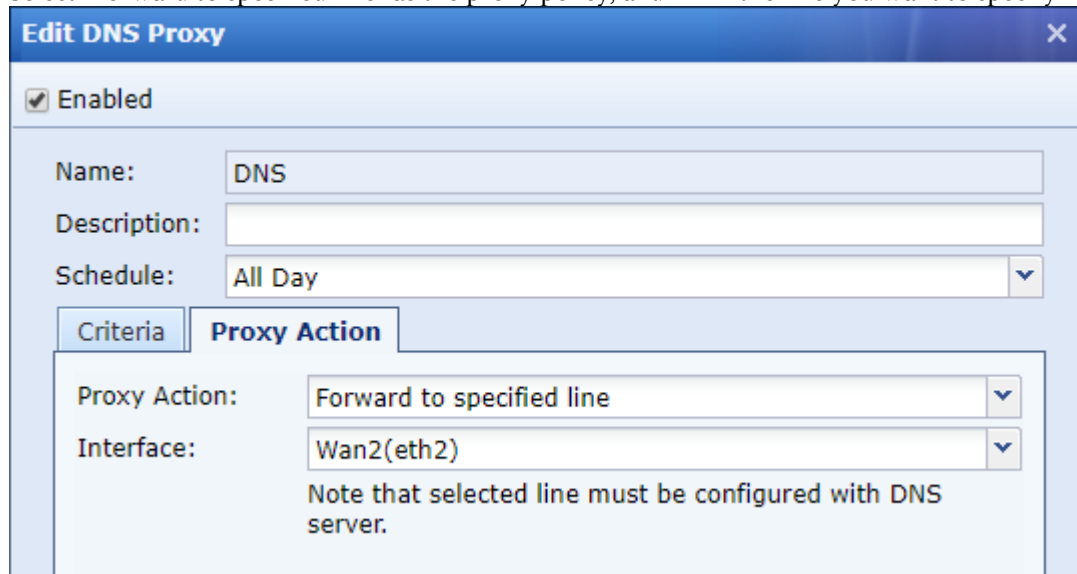
User: ☒ All users
☐ Specified
User:Select

URL: ☐ All
☒ Specified
URL categories:
[Select](#)
Domain names: ⓘ

Dst DNS Server: ☒ All
☐ Specified

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"

DNS Proxy Policy-based Routing Status Connections											
Search by IP Address 10.10.10.2											
No.	Username(Alias)	Group	Source	Line	Policy-based Routing Na...	Global exclusion	Destination	Protocol	App Category	Application	Data Flow
2	10.10.10.2	/	10.10.10.2:50298	Wan2(eth2)	-	No	104.244.42.129:443	TCP	Microblog	Twitter	LAN->WAN
3	10.10.10.2	/	10.10.10.2:50295	Wan2(eth2)	-	No	104.244.42.3:443	TCP	Microblog	Twitter	LAN->WAN
4	10.10.10.2	/	10.10.10.2:50287	Wan2(eth2)	-	No	104.244.42.65:443	TCP	Microblog	Twitter	LAN->WAN
5	10.10.10.2	/	10.10.10.2:50288	Wan2(eth2)	-	No	104.244.42.65:443	TCP	Microblog	Twitter	LAN->WAN
6	10.10.10.2	/	10.10.10.2:50296	Wan2(eth2)	-	No	104.244.42.8:443	TCP	Microblog	Twitter	LAN->WAN
7	10.10.10.2	/	10.10.10.2:50291	Wan2(eth2)	-	No	117.18.237.70:443	TCP	Microblog	Twitter	LAN->WAN
8	10.10.10.2	/	10.10.10.2:50290	Wan2(eth2)	-	No	117.18.237.70:443	TCP	Microblog	Twitter	LAN->WAN
9	10.10.10.2	/	10.10.10.2:50292	Wan2(eth2)	-	No	117.18.237.70:443	TCP	Microblog	Twitter	LAN->WAN
10	10.10.10.2	/	10.10.10.2:50289	Wan2(eth2)	-	No	117.18.237.70:443	TCP	Microblog	Twitter	LAN->WAN
11	10.10.10.2	/	10.10.10.2:50293	Wan2(eth2)	-	No	117.18.237.70:443	TCP	Microblog	Twitter	LAN->WAN
12	10.10.10.2	/	10.10.10.2:50294	Wan2(eth2)	-	No	117.18.237.70:443	TCP	Microblog	Twitter	LAN->WAN

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.



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