

# **IAM**

## **Panduan Konfigurasi DNS Proxy**

**Versi 12.0.41**

## Catatan Perubahan

Tanggal	Deskripsi Perubahan
Januari 9, 2020	Rilis Dokumen Versi 12.0.41.

# Daftar Isi

Bab 1 Ringkasan .....	1
Bab 2 Keunggulan Solusi .....	1
Bab 3 Skenario .....	1
Bab 4 Metode Konfigurasi .....	1
4.1 Redirect to DNS server .....	1
4.1.1 Tes Kondisi.....	1
4.1.2 Hasil yang diharapkan .....	1
4.1.3 Langkah Konfigurasi .....	2
4.1.3.1 Deskripsi Persyaratan.....	2
4.1.3.2 Konfigurasi .....	2
4.1.3.3 Efek Presentasi .....	4
4.2 Resolve to IP address .....	5
4.2.1 Tes Kondisi.....	5
4.2.2 Hasil yang diharapkan .....	5
4.2.3 Langkah Konfigurasi .....	5
4.2.3.1 Deskripsi Persyaratan.....	5
4.2.3.2 Konfigurasi .....	5
4.2.3.3 Efek Presentasi .....	7
4.3 Drop DNS packet .....	7
4.3.1 Tes Kondisi.....	7
4.3.2 Hasil yang diharapkan .....	7
4.3.3 Langkah Konfigurasi .....	7
4.3.3.1 Deskripsi Persyaratan.....	7
4.3.3.2 Konfigurasi .....	7
4.3.3.3 Efek Presentasi .....	9
4.4 Forward to specified line .....	9
4.4.1 Tes Kondisi.....	9
4.4.2 Hasil yang diharapkan .....	9
4.4.3 Langkah Konfigurasi .....	9
4.4.3.1 Deskripsi Persyaratan.....	9
4.4.3.2 Konfigurasi .....	10
4.4.3.2 Efek Presentasi .....	12
Bab 5 Tindakan Pencegahan.....	12

## Bab 1 Ringkasan

IAM dilengkapi dengan fungsi dari DNS proxy, yang dapat menggantikan permintaan DNS. Menerapkan persyaratan dari "limiting illegal DNS requests" atau secara paksa meneruskan domain name tertentu ke server Anda sendiri.

## Bab 2 Keunggulan Solusi

IAM mendukung fungsi DNS proxy. Pengguna dapat mengatur DNS proxy sesuai dengan user group akhir, website type, domain name, dan target DNS address. Ini mendukung pengalihan ke DNS server tertentu, meneruskan line yang ditentukan, menyelesaikan IP tetap, dan mengabaikan. Jalan.

Ketika multiple Internet links disebarkan di network, pengguna intranet mengisi DNS server dari salah satu operator ketika mereka online, jadi kebanyakan pengguna ditugaskan ke link yang sama, membuat link selalu dalam keadaan sibuk, akses kecepatan pengguna diakses melalui link ini menurun, sementara link lainnya tidak aktif. Ketidakseimbangan pemanfaatan link menyebabkan pemborosan sumber daya internet di satu sisi, dan kecepatan akses pengguna tidak dapat dijamin di sisi lain.

Melalui DNS transparent proxy technology, tidak peduli operator mana alamat DNS server dimasukkan oleh pengguna intranet, permintaan DNS akan diteruskan melalui perilaku Sangfor Internet perangkat manajemen, dan DNS server yang cocok akan ditemukan dan dikembalikan ke intranet komputer. Load algorithm dapat mendistribusikan traffic ke link yang berbeda sesuai dengan kebijakan pemanfaatan link yang ditetapkan.

Dalam hal ini, traffic dari dua link di network pengguna akan sama seperti yang diharapkan manajer dari awal hingga akhir, memastikan pemanfaatan dari setiap link.

## Bab 3 Skenario

**Redirect to DNS server:** Redirect original DNS server ke DNS server IP yang dikonfigurasi

**Resolve to IP address:** Langsung menyelesaikan domain name ke IP yang ditentukan

**Drop DNS packet:** Langsung drop paket permintaan DNS

**Forward to specified line:** redirect ke exit yang ditentukan

**Catatan:**

1. Dalam Forward untuk strategi line yang ditentukan, network ports ditampilkan dalam routing mode dan virtual line ditampilkan di bridge mode.
2. Dalam Forward untuk line policy yang ditentukan, Anda tidak dapat memilih line yang tidak dikonfigurasi dengan dns.

## Bab 4 Metode Konfigurasi

### 4.1 Redirect to DNS server

#### 4.1.1 Kondisi Pengujian

Siapkan perangkat IAM untuk diterapkan dalam routing atau bridge mode

#### 4.1.2 Hasil yang diharapkan

Akses domain name yang ditentukan, paksakan redirect ke DNS server yang ditentukan untuk resolusi.

### **4.1.3 Langkah Konfigurasi**

#### **4.1.3.1 Deskripsi Persyaratan**

Secara paksa mengarahkan permintaan DNS pengguna A untuk domain name `www.baidu.com` ke DNS server `114.114.114.114` untuk diselesaikan.

#### **4.1.3.2 Konfigurasi**

1. Konfigurasi kondisi DNS Policy-Proxy

Pilih pengguna "A", tentukan domain name "`www.baidu.com`", dan tes bahwa DNS yang dikonfigurasi di komputer pengguna adalah target DNS address "`3.3.3.3`"

**Add DNS Proxy**

☒ Enabled

Name:

Description:

Schedule:

**Criteria** | Proxy Action

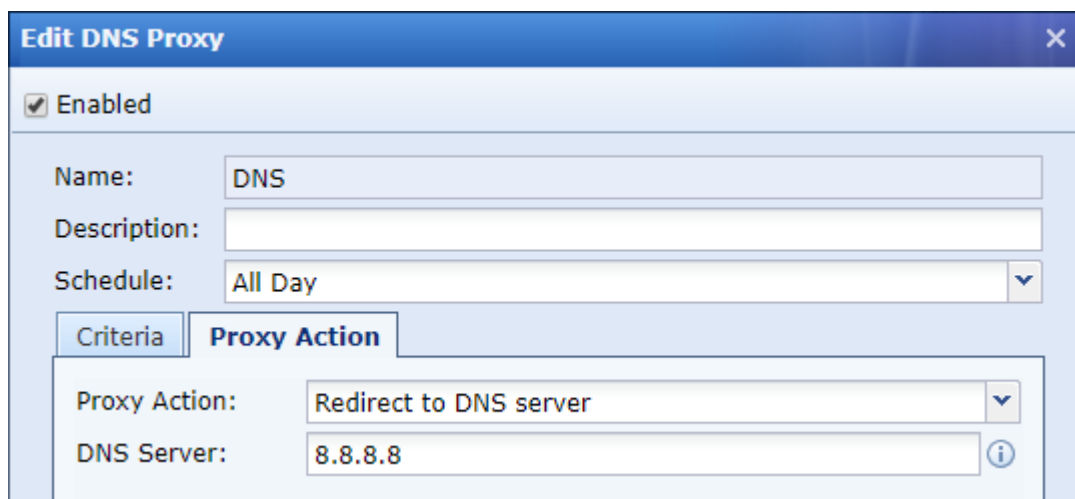
User: ☐ All users  
☒ Specified  
User:a

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

Dst DNS Server: ☐ All  
☒ Specified

## 2. Konfigurasi Tindakan DNS Policy-Proxy

Pilih "Redirect to DNS server" sebagai proxy policy, dan isi DNS address yang ingin Anda gunakan untuk menyelesaikan.



### 4.1.3.3 Efek Presentasi

Target dns dikonfigurasi dengan non-effective DNS; tes komputer di konfigurasi dengan non-effective DNS.

Tes komputer menggunakan nslookup untuk mendeteksi www.baidu.com tidak berhasil, tetapi tes ping berhasil.

Ping sebelumnya, gunakan ipconfig/flushdns untuk clear 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 Tes Kondisi

Siapkan perangkat IAM untuk diterapkan dalam routing atau bridge mode

### 4.2.2 Hasil yang diharapkan

Secara paksa menyelesaikan name ke IP yang ditentukan ketika mengakses domain name yang ditentukan.

### 4.2.3 Langkah Konfigurasi

#### 4.2.3.1 Deskripsi Persyaratan

Menyelesaikan permintaan DNS secara paksa untuk pengguna yang mengakses domain name `www.google.com` ke `6.7.8.9`

#### 4.2.3.2 Konfigurasi

1. Konfigurasi Kriteria DNS Policy-Proxy

Untuk semua pengguna, definisikan akses domain name "`www.google.com`" dan tes bahwa DNS dikonfigurasi pada komputer pengguna adalah target DNS address "`all`":



**Edit DNS Proxy**

☒ Enabled

Name:

Description:

Schedule:

**Criteria** | Proxy Action

User: ☒ All users  
☐ Specified  
User:

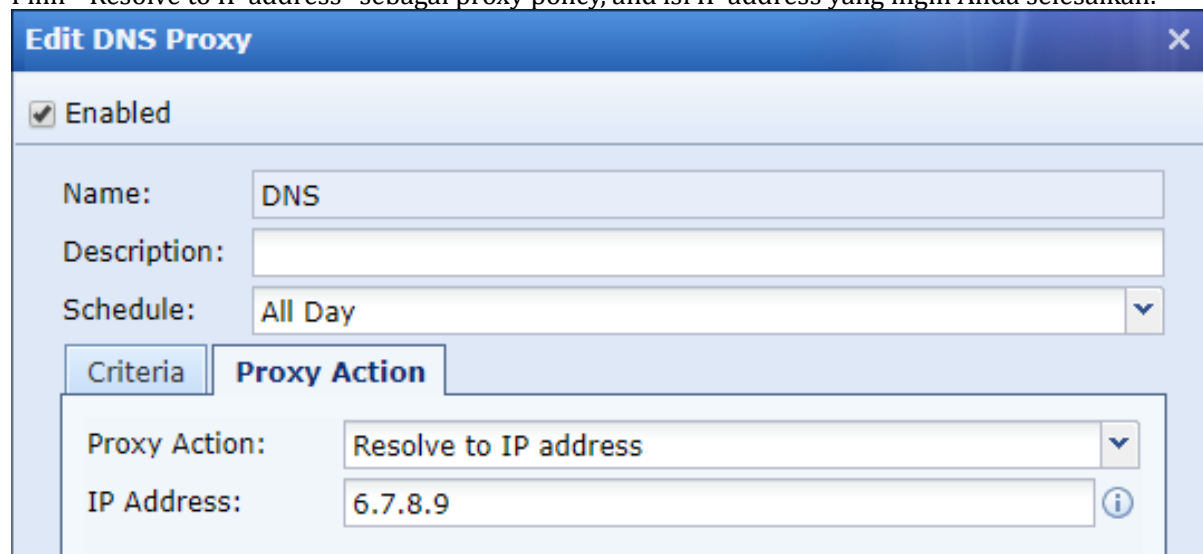
URL: ☐ All  
☒ Specified  
URL categories: [Select](#)

Domain names: ⓘ

Dst DNS Server: ☒ All  
☐ Specified

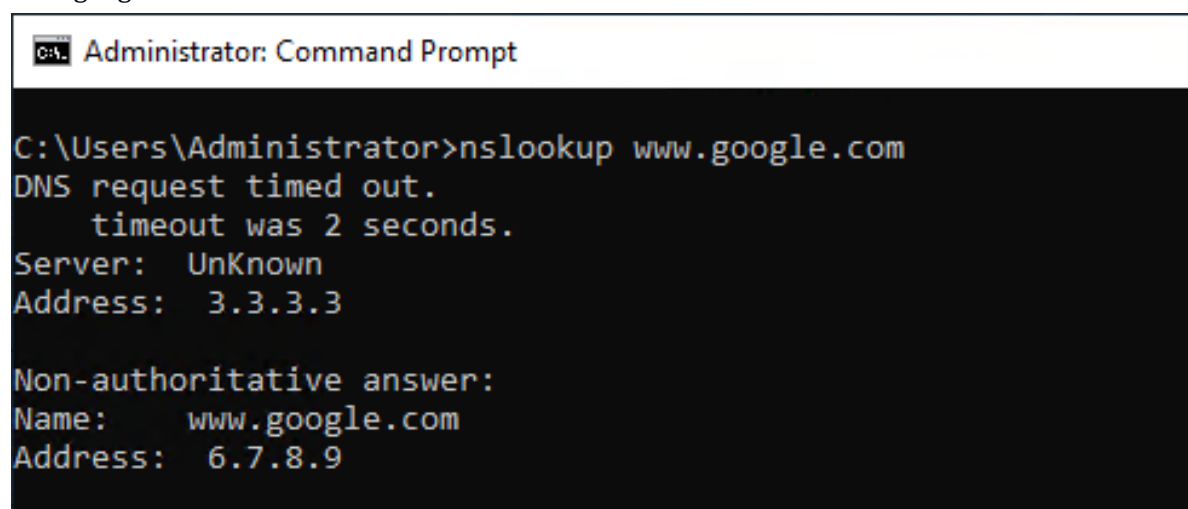
2. Konfigurasi Tindakan DNS Policy-Proxy

Pilih "Resolve to IP address" sebagai proxy policy, and isi IP address yang ingin Anda selesaikan.



#### 4.2.3.3 Efek Presentasi

Menggunakan nslookup pada tes komputer, Anda dapat melihat bahwa target domain name www.google.com telah diselesaikan untuk 6.7.8.9



## 4.3 Drop DNS packet

### 4.3.1 Tes Kondisi

Siapkan perangkat IAM untuk diterapkan dalam routing atau bridge mode

### 4.3.2 Hasil yang diharapkan

Ketika pengguna mengakses domain name tertentu, IAM membuang DNS request packets.

### 4.3.3 Langkah Konfigurasi

#### 4.3.3.1 Deskripsi Persyaratan

IAM secara paksa drops DNS request packets saat pengguna mengunjungi www.youtube.com

#### 4.3.3.2 Konfigurasi

1. Konfigurasi Kriteria DNS Policy-Proxy

Untuk semua pengguna, definisikan akses domain name "www.youtube.com" dan tes bahwa DNS

dikonfigurasi pada komputer pengguna adalah target DNS address "all".

**Edit DNS Proxy**

☒ Enabled

Name:

Description:

Schedule:

**Criteria** Proxy Action

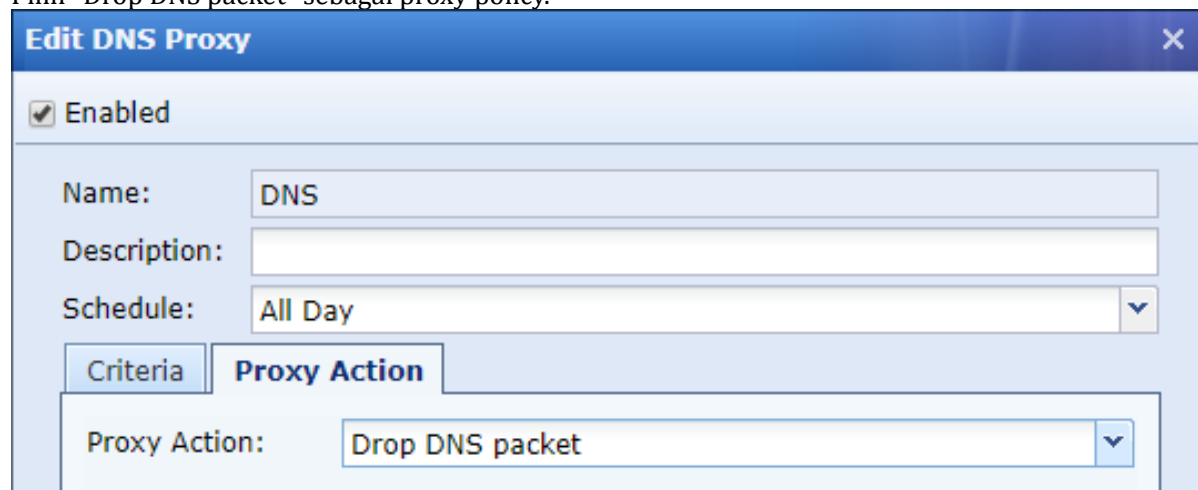
User: ☒ All users  
☐ Specified  
User: Select

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

Dst DNS Server: ☒ All  
☐ Specified

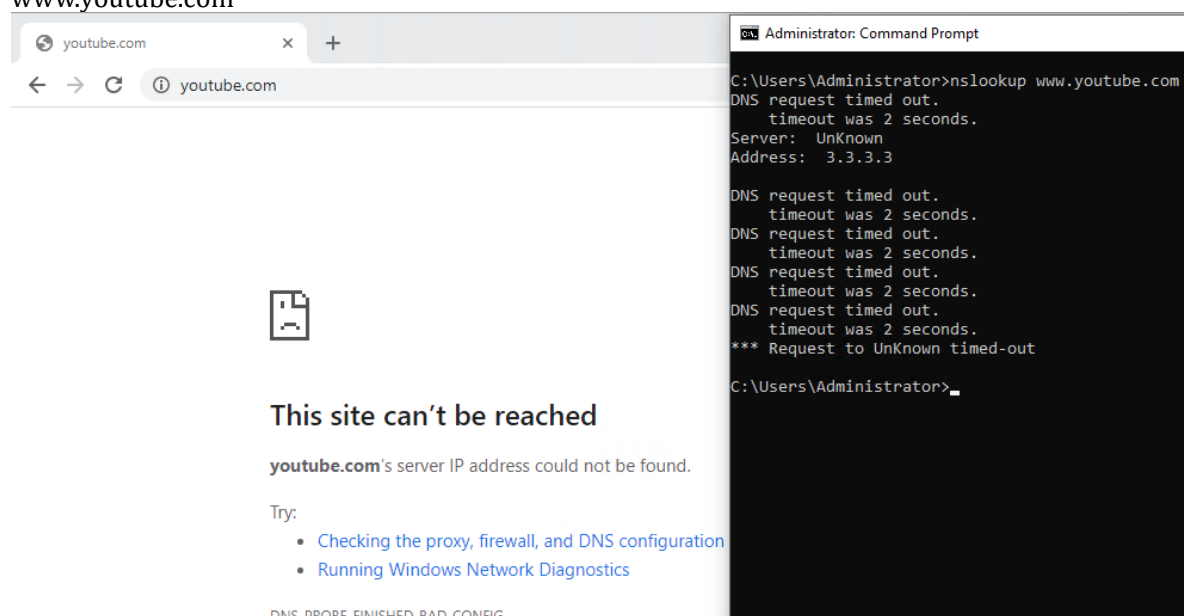
## 2. Konfigurasi Tindakan DNS Policy-Proxy Action

Pilih "Drop DNS packet" sebagai proxy policy.



### 4.3.3.3 Efek Presentasi

Gunakan perintah nslookup pada tes komputer untuk menyelesaikan target domain name [www.youtube.com](http://www.youtube.com)



## 4.4 Forward to specified line

### 4.4.1 Tes Kondisi

Siapkan perangkat IAM untuk diterapkan dalam routing atau bridge mode

Perangkat harus diaktifkan multi-line

Perangkat harus dikonfigurasi dengan Policy-Based Routing

### 4.4.2 Hasil yang diharapkan

Ketika pengguna mengakses domain name tertentu, IAM memaksa traffic untuk pergi melalui line yang ditentukan.

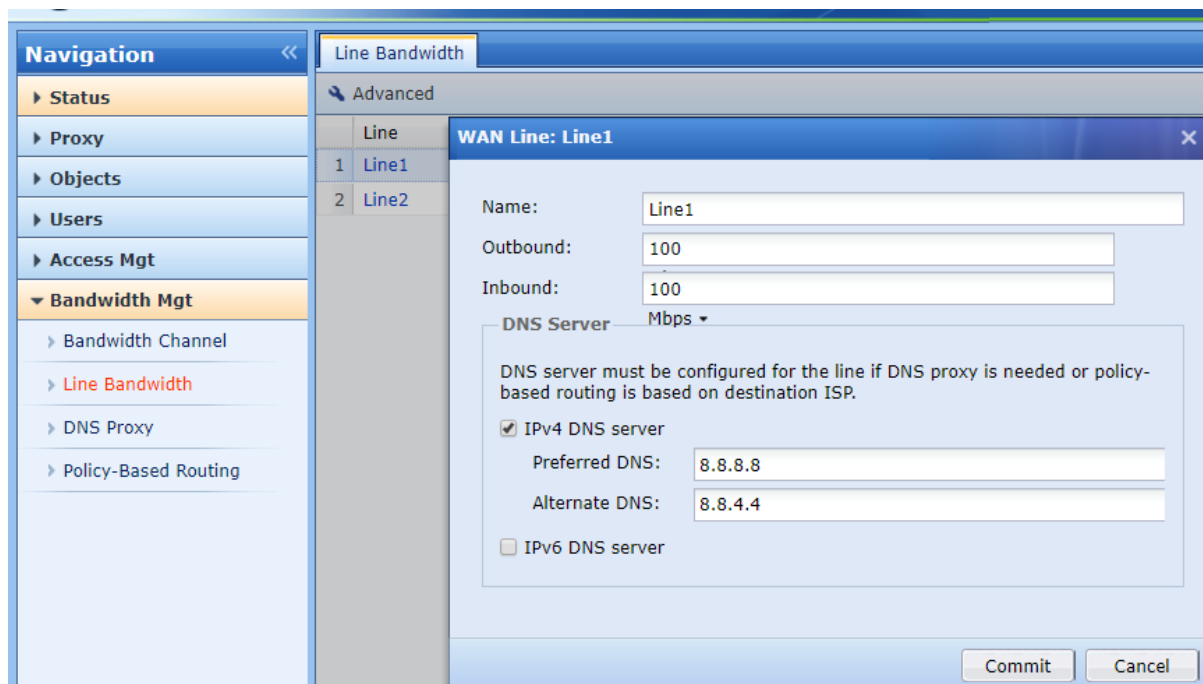
### 4.4.3 Langkah Konfigurasi

#### 4.4.3.1 Deskripsi Persyaratan

Pengguna mengunjungi domain name [www.twitter.com](http://www.twitter.com), dan IAM mengirimkan traffic dari line 2.

### 4.4.3.2 Konfigurasi

#### 1. Aktifkan DNS server untuk line dan konfigurasi DNS



Konfigurasi DNS dapat dikonfigurasi di "Deployment", "Line Bandwidth" atau "Interfaces".

#### 2. Konfigurasi Kriteria DNS Policy-Proxy

Untuk semua pengguna, definisikan akses domain name "www.twitter.com" dan tes bahwa DNS dikonfigurasi pada komputer pengguna adalah target DNS address "all"

**Edit DNS Proxy** [X]

☒ Enabled

Name:

Description:

Schedule:  ▼

**Criteria** | Proxy Action

User: ☒ All users  
☐ Specified  
 User:Select

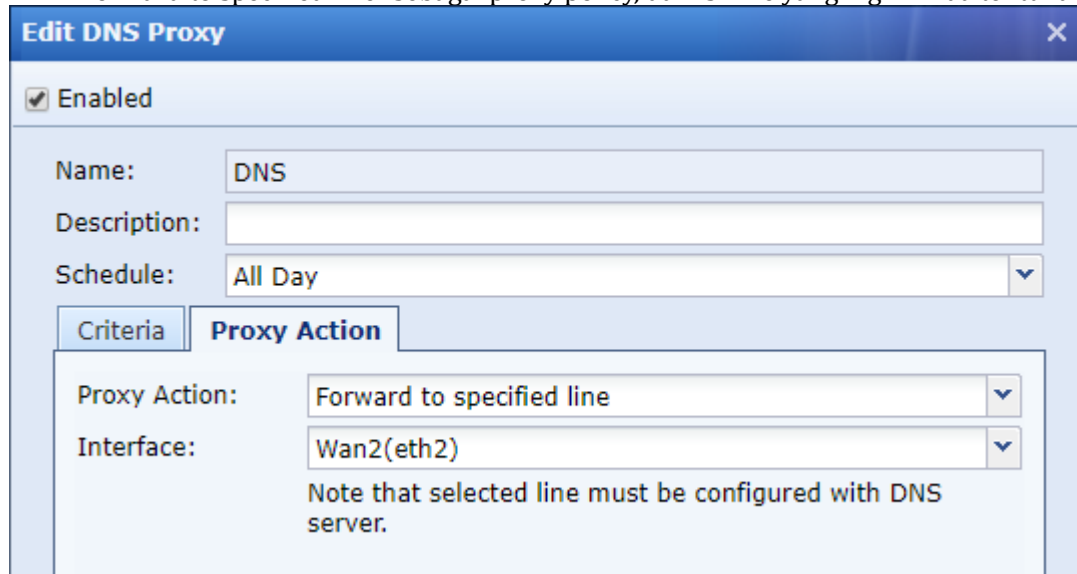
URL: ☐ All  
☒ Specified  
 URL categories:  
[Select](#)  
 Domain names: ⓘ

Dst DNS Server: ☒ All  
☐ Specified

[Commit] [Cancel]

### 3. Konfigurasi Tindakan DNS Policy-Proxy

Pilih "Forward to specified line" sebagai proxy policy, dan isi line yang ingin Anda tentukan



Hanya line yang dikonfigurasi dengan DNS atau DSCP / TOS nilai dapat dipilih. Fungsi ini tidak mengambil efek ketika Policy-Based Routing tidak diaktifkan.

#### 4.4.3.2 Efek Presentasi

Kunjungi target domain name [www.twitter.com](http://www.twitter.com) pada tes komputer, dan periksa perangkat IAM "Traffic Statistics" - "Link Load Status"

DNS Proxy   Policy-based Routing Status   Connections											Total 35 Connections
No.	Username(Alas)	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

## Bab 5 Tindakan Pencegahan

1. Proxy to the intranet DNS server: DNS proxy policy proxy ke intranet DNS server (DNS server ada di DMZ area)

Fenomena:

Proxy ke intranet DNS server gagal (Jika komputer pengguna sendiri memiliki DNS server yang valid dikonfigurasi, maka gunakan DNS server, dan DNS server yang tidak valid akan menyebabkan network terputus)

Solusi:

Konfigurasi firewall memungkinkan traffic dari DMZ-> LAN

2. Apakah fungsi DNS proxy mempunyai efek ketika global exclusion dan pass-through diaktifkan?

Setelah DNS proxy dikonfigurasi dengan "Drop DNS packet" dan domain name ditambahkan ke global exclusion, DNS proxy "Drop DNS packet" policy tidak lagi berlaku;

Setelah pass-through diaktifkan, DNS proxy tidak berlaku.

3. Dalam bridge mode, jika DNS deteksi adalah mengirim paket dari dmz port untuk mendeteksi, Anda perlu memastikan bahwa paket yang dikirim dari dmz port dapat mencapai 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