

# **Panduan Konfigurasi Sangfor NGAF DNS Proxy dan DNS Transparent Proxy**

<b>Produk Versi</b>	8.0.35
<b>Documen Versi</b>	01
<b>Dirilis pada</b>	Juni. 07, 2021



## Catatan Perubahan

Tanggal	Deskripsi Perubahan
Juni. 07, 2021	Ini adalah rilis pertama dokumen ini.

# Daftar Isi

Catatan Perubahan .....	1
1 Pengantar .....	1
1.1 Singkatan dan Konvensi .....	1
1.2 Umpan Balik .....	1
2 DNS Proxy.....	1
2.1 Skenario .....	1
2.2 Langkah Konfigurasi .....	1
3 DNS Transparent Proxy.....	2
3.1 Skenario .....	2
3.2 Langkah Konfigurasi .....	3
4 Tindakan Pencegahan .....	5

# 1 Pengantar

## 1.1 Singkatan dan Konvensi

NGAF dalam artikel ini mengacu pada perangkat SANGFOR NGAF.

## 1.2 Umpan Balik

Jika Anda menemukan pertanyaan tentang dokumen ini, jangan ragu untuk memberi kami umpan balik, email: [tech.support@sangfor.com](mailto:tech.support@sangfor.com).

# 2 DNS Proxy

## 2.1 Skenario

DNS proxy terutama dikonfigurasi pada perangkat gateway, dan gateway mengirim permintaan DNS ke domain name server sebagai gantinya dari intranet host . Hal ini terutama digunakan dalam kasus bahwa terkadang DNS server address tidak dapat dikonfigurasi di intranet network atau pengguna tidak jelas tentang DNS server address, dan DNS address secara langsung diisi sebagai gateway address untuk kenyamanan pengguna.

Lingkungan pengujian ditunjukkan seperti di bawah ini:



## 2.2 Langkah Konfigurasi

**Step 1.** Login ke NGAF web console, pergi ke **Networks > DNS > DNS Servers**. Enable DNS proxy option seperti yang ditunjukkan pada gambar di bawah ini.

## DNS Servers

---

### DNS Server

Both automatic update and DNS proxy require a valid DNS server to be specified.

Preferred DNS:

8.8.8.8

Alternate DNS:

8.8.4.4

### DNS Proxy

Once enabled, the local DNS server can direct to this device, which sends DNS requests on behalf of internal hosts. Make sure this device can resolve DNS requests.

DNS Proxy ⓘ:



Enable



Disable

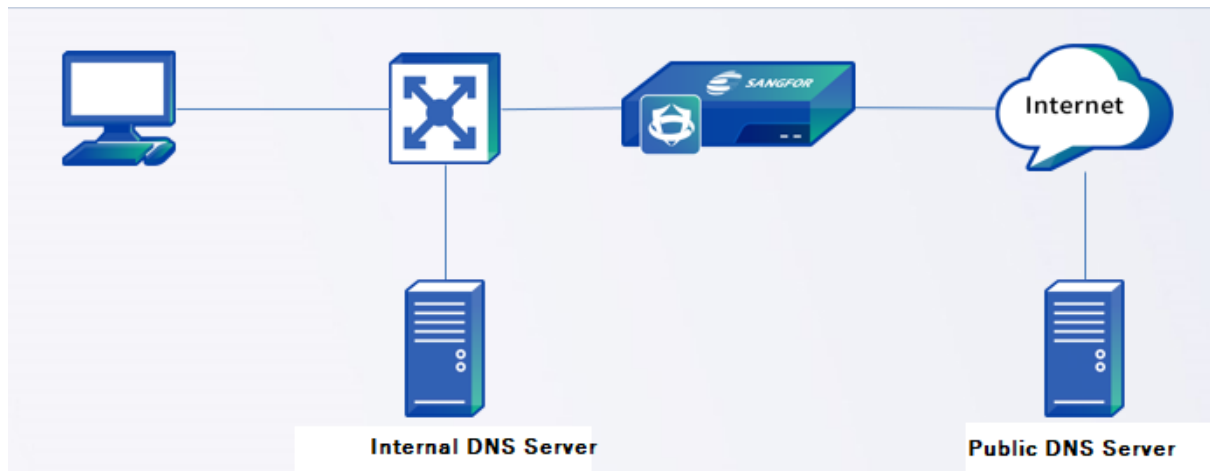
Save

## 3 DNS Transparent Proxy

### 3.1 Skenario

DNS transparent proxy dikonfigurasi pada perangkat gateway, dan gateway mencegat DNS dari intranet host dan kemudian mengirimkan permintaan DNS ke domain name server sendiri yang dikonfigurasi, yang memiliki dua skenario utama berikut.

- Mengatur DNS address yang berubah-ubah untuk kenyamanan pengguna intranet yang tidak mengetahui DNS server address.
- Mengirim permintaan DNS ke DNS server yang ditentukan oleh gateway, yang dapat dikombinasikan dengan policy routing untuk routing dan lain-lain.



## 3.2 Langkah Konfigurasi

**Step 1.** Login ke NGAF web console, pergi ke **Networks > DNS > DNS Transparent Proxy**. Isi **External DNS Server** IP address dan jika ada internal DNS server, isikan IP address di **Local DNS Server**.

### DNS Transparent Proxy

#### External DNS Server

Specify a valid external DNS server IP address to ensure DNS proxy.

Preferred DNS:	<input type="text" value="8.8.8.8"/>
Alternate DNS:	<input type="text" value="Optional"/>

#### Local DNS Server

Specify a valid local DNS server IP address to ensure DNS proxy.

Preferred DNS:	<input type="text" value="192.168.1.110"/>
Alternate DNS:	<input type="text" value="Optional"/>

**Step 2.** **Enable** DNS Transparent Proxy dan isi DNS cache number di **Cached DNS Records**.

### DNS Transparent Proxy

Enable this to support DNS transparent proxy.

DNS Transparent Proxy: ☒ Enable ☐ Disable

Cached DNS Records: 1000

Upload Domain File:

Upload

Select



① Only valid domain can be uploaded.

**Step 3.** Konfigurasi DNAT policy, **Policies > NAT** klik **Add** untuk konfigurasi DNAT policy.

#### Add NAT Policy



##### Basics

Name: DNS Transparent Proxy

Status: ☒ Enabled ☐ Disabled

Description: Optional

Move To: Top



Schedule: All week

##### Original Data Packet

Src Zone: LAN

Src Address: Lan PC

Destination: ☐ IP Address ☒ Network Objects

All

Services: dns-t,dns-u

##### Translated Data Packet

Translate Src IP To: Untranslated

Translate Dst IP To: IP Address

IP Address: 192.168.1.1

Translate Port To: 5354

① To make NAT policy work, please configure local ACL or application control policy.

Allow: ☒ Add ACL policy automatically

☐ Add ACL policy manually

Save and Copy

Save

Cancel

### Original Data Packet

- **Src Zone:** pilih internal zone
- **Src Address:** pilih internal IP address/segment
- **Destination:** pilih Network Objects dan pilih semua
- **Services:** pilih TCP DNS dan UDP DNS service

### Translated Data Packet

- **IP Address:** Isi IP address antarmuka NGAF Lan
- **Translate Port To:** Isi port 5354

## 4 Tindakan Pencegahan

- i. DNS server dari NGAF seharusnya diatur dengan benar untuk memastikan bahwa dapat melakukan resolusi DNS dengan benar.
- ii. DNS proxy dan DNS transparent proxy tidak mendukung di bridge/virtual mengikat lingkungan deployment.
- iii. DNS menggunakan **TCP** Port **53** untuk transfer zona, untuk menjaga koherensi antara DNS database dan the server. **UDP** port **53** digunakan saat klien mengirim kueri ke DNS server.
- iv. DNS proxy yang digunakan adalah **TCP** port **53**, NGAF DNS proxy terbuka semua untuk zona dapat mengakses port ini, seperti NGAF Deployment di network gateway, direkomendasikan konfigurasi aplikasi kontrol atau Local ACL policy untuk menolak memblokir IP address eksternal yang tidak dikenal mengakses port ini.
- v. Diperlukan untuk konfigurasi DNAT policy agar DNS Transparen Proxy untuk bekerja secara normal.
- vi. Port yang digunakan oleh DNS transparent proxy adalah TCP port 5354.
- vii. DNS proxy memerlukan klien untuk mengatur DNS sebagai IP antarmuka NGAF; DNS transparent proxy tidak mengharuskan klien untuk mengatur DNS sebagai IP antarmuka NGAF.
- viii. DNS transparent proxy akan melakukan pencarian intranet untuk permintaan DNS yang ada dalam daftar domain name file yang , dan akan melakukan pencarian extranet bagi permintaan DNS yang tidak ada dalam domain name file yang diunggah.



