



NGAF

Monitor status NGAF via SNMP

Versi 7.4



Perubahan Catatan

Tanggal	Deskripsi Perubahan
10 March, 2021	Rilis Dokumen Versi 1.0.

Daftar Isi

Bab 1 Pengantar.....	1
1.1 Singkatan dan Konvensi.....	1
1.2 Umpan Balik.....	1
Bab 2 Pengarahan Fungsi.....	1
Bab 3 Skenario.....	1
Bab 4 Persyaratan.....	1
Bab 5 Konfigurasi Mind Map.....	1
Bab 6 Langkah Konfigurasi dan Tangkapan Layar.....	1
6.1 Mengatur opsi Jaringan Tingkat Lanjut.....	1
6.2 Aktifkan Zone SNMP.....	3
Bab 7 Tindakan Pencegahan.....	4

Bab 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.

Bab 2 Pengarahan Fungsi

NGAF menyediakan informasi status pengoperasian, sehingga pelanggan dapat dengan mudah memantau status *real-time*.

Bab 3 Skenario

Dengan menggunakan protokol SNMP di perangkat lunak/perangkat manajemen jaringan pihak ketiga untuk mengelola dan memantau informasi terkait perangkat Sangfor, seperti status antarmuka, aliran data dalam antarmuka, routing dan sebagainya. Ini menyediakan platform terpadu bagi pelanggan untuk mengelola, menjaga dan memantau jaringan.

Bab 4 Persyaratan

Buat daftar persyaratan untuk konfigurasi ini, misalnya:

1. Satu perangkat NGAF.
2. Perangkat lunak manajemen jaringan pihak ketiga (mendukung perangkat lunak pemantauan SNMP)

Bab 5 Konfigurasi Mind Map

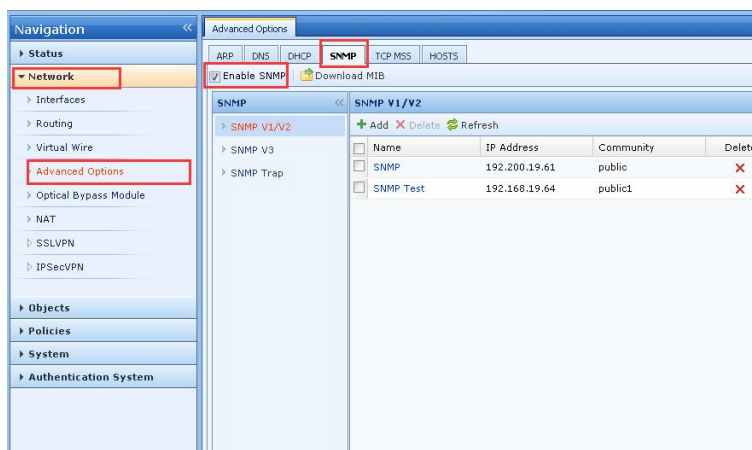
1. Mengatur opsi jaringan tingkat lanjut.
2. Pilih zona di mana SNMP diterapkan.

Bab 6 Langkah Konfigurasi dan Tangkapan Layar

6.1 Mengatur opsi Jaringan Tingkat Lanjut

1. *Enable SNMP*: di bawah [*Navigation*] – [*Network*] – [*Advanced Option*], klik [*SNMP*] di sisi kanan untuk masuk ke halaman edit. Centang [*Enable SNMP*] seperti yang ditampilkan dalam gambar di

bawah:



2. Jika dukungan perangkat lunak manajemen jaringan pihak ketiga protokol SNMP V1/V2 , click [SNMP V1/V2] – [Add], seperti yang ditampilkan dalam gambar di bawah ini:



[Name]: Diberikan sebuah nama semauanya untuk manajemen jaringan host/server.

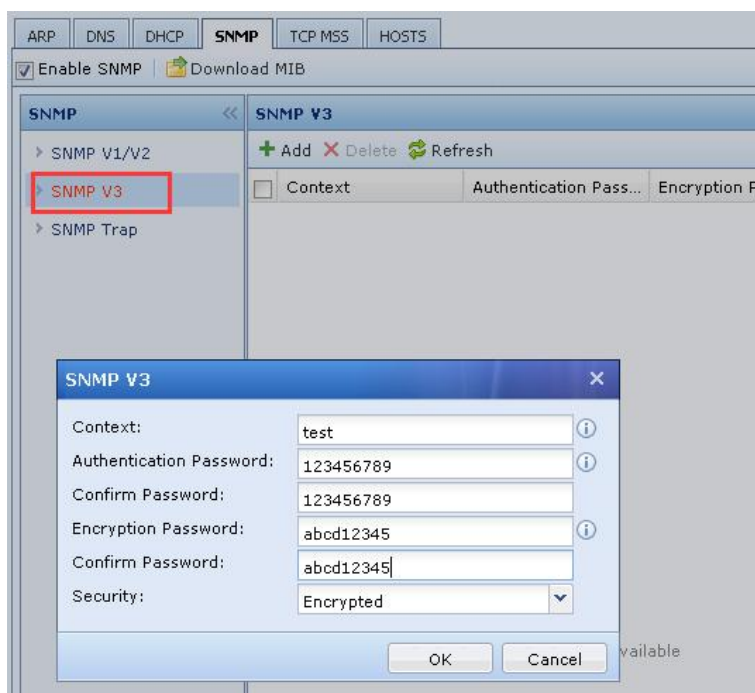
[Address Type]: Jenis host manajemen. Bisa jadi “IP address” atau “Subnet”.

Ketika “IP address” dipilih, hal ini mengindikasikan bahwa host manajemen adalah perangkat ketika “Subnet” dipilih, ini menunjukkan bahwa host manajemen ada di *subnet*, host yang sesuai *subnet* dapat melewati perangkat SNMP.

[IP Address]: Dapat dikonfigurasi menjadi alamat IP SNMP server atau jangkauan IP. Jika “IP Address” dipilih di [Address Type], kemudian alamat IP server SNMP spesifik harus dimasukkan; jika “Subnet” dipilih di [Address Type], kemudian tentukan ID *subnet*.

[Community]: untuk menentukan string komunitas ketika akses server SNMP ke perangkat di jaringan.

3. Jika perangkat lunak manajemen jaringan pihak ketiga mendukung protokol SNMP V3, klik [SNMP V3] – [Add], beberapa opsi lanjutan perlu dikonfigurasi, seperti yang ditampilkan pada gambar di bawah ini:



[Context]: Username dari SNMPV3

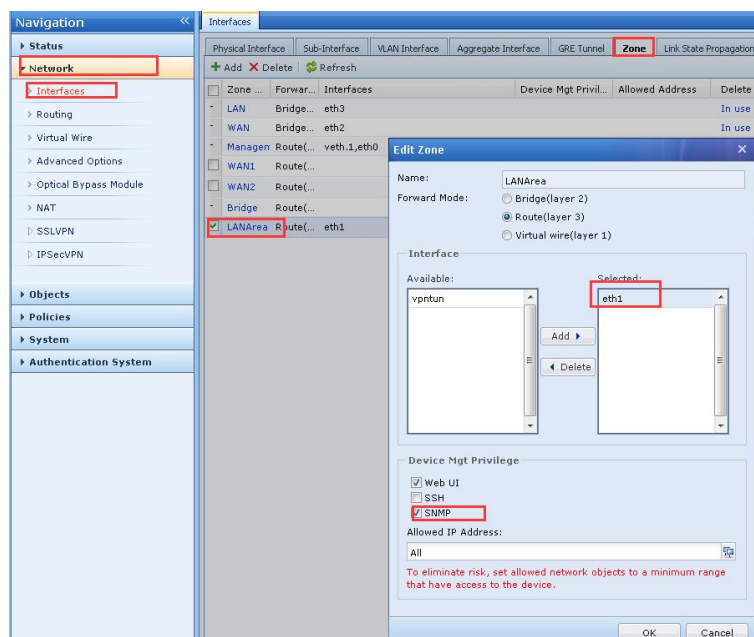
[Authentication Password] dan [Confirm Password]: password spesifik pengguna SNMPV3 yang digunakan untuk tujuan otentikasi. Panjangnya harus lebih panjang dari delapan karakter tanpa ruang kosong.

[Encryption Password] dan [Confirm Password]: password yang digunakan untuk mengenkripsi pesan. Enkripsi password harus lebih dari delapan karakter tanpa spasi kosong.

[Security]: Untuk menentukan apakah mengeksekusi otentikasi SNMP dan enkripsi pesan. Pilihannya adalah [Encrypted] atau [Not Encrypted]. Ketika "Encrypted" dipilih, otentikasi dan enkripsi kedua digunakan dengan langkah pertama untuk mengenkripsi data dan mengotentikasi dengan teknik digest pesan. Jika "Not Encrypted" dipilih, maka otentikasi hanya akan mengambil efek.

6.2 Aktifkan Zone SNMP

Ketika perangkat lunak manajemen jaringan bagian ke tiga berada di salah satu zone yang didefinisikan dalam perangkat NGAF kami, [Network] – [Interfaces] – [Zone], buka zone yang sesuai. Di bawah [Device Mgt Privilege], centang [SNMP]. Pastikan bahwa alamat IP dari pihak ketiga pihak manajemen perangkat lunak/perangkat termasuk dalam daftar [Allowed IP Address], seperti yang ditampilkan pada gambar di bawah ini:



Bab 7 Tindakan Pencegahan

1. Ketika pihak ketiga perangkat lunak manajemen jaringan/perangkat digunakan, semua nilai OID dapat diperoleh dari Sangfor technical support team.
2. Informasi SNMP dikonfigurasi di perangkat lunak manajemen jaringan pihak ketiga/perangkat harus konsisten dengan yang ada di perangkat NGAF, seperti "Community"
3. [SNMP] harus dicentang di zone yang benar yang antarmuka yang sesuai dari pihak ketiga perangkat lunak manajemen jaringan/perangkat.



Hak cipta (c) Sangfor Technologies Inc. Hak cipta dilindungi oleh undang-undang. Dilarang menyebarkan atau memproduksi ulang sebagian dari atau seluruh dokumen ini tanpa persetujuan tertulis dari Sangfor Technologies Inc. SANGFOR adalah merek dagang dari Sangfor Technologies Inc. Semua merek dagang dan nama dagang lain yang disebutkan dalam dokumen ini adalah milik dari pemegangnya masing-masing. Segala upaya telah dilakukan dalam mempersiapkan dokumen ini untuk memastikan keakuratan konten, namun semua pernyataan, informasi, dan rekomendasi dalam dokumen ini bukan merupakan jaminan dalam bentuk apa pun, tersurat maupun tersirat. Informasi dalam dokumen ini dapat berubah tanpa pemberitahuan. Untuk mendapatkan versi terbaru, hubungi pusat layanan internasional SANGFOR Technologies Inc.