SANGFOR

IAG

Fungsi RST redireksi autentikasi

Versi 13.0.15

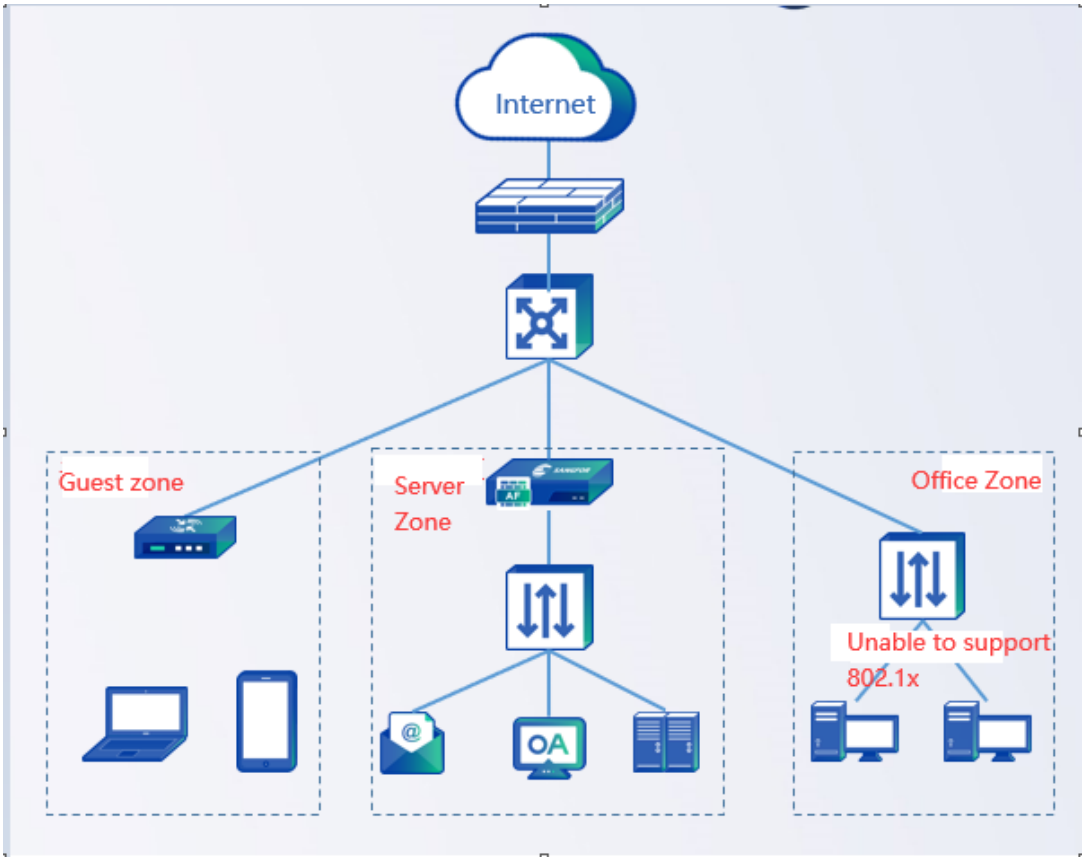
Catatan Perubahan

Tanggal	Deskripsi Perubahan
September 23, 2020	Rilis Versi 13.0.15

Daftar Isi

Bab 1 Latar Belakang

1. Switch tidak mendukung untuk konfigurasi 802.1x autentikasi, dan tidak dapat menggunakan metode level 2 untuk melakukan autentikasi.
2. Akses pengguna ke paket server tidak dapat dikontrol.
3. Akses pengguna ke paket Internet tidak dapat dikontrol.



Bab 2 RST redireksi autentikasi Solusi

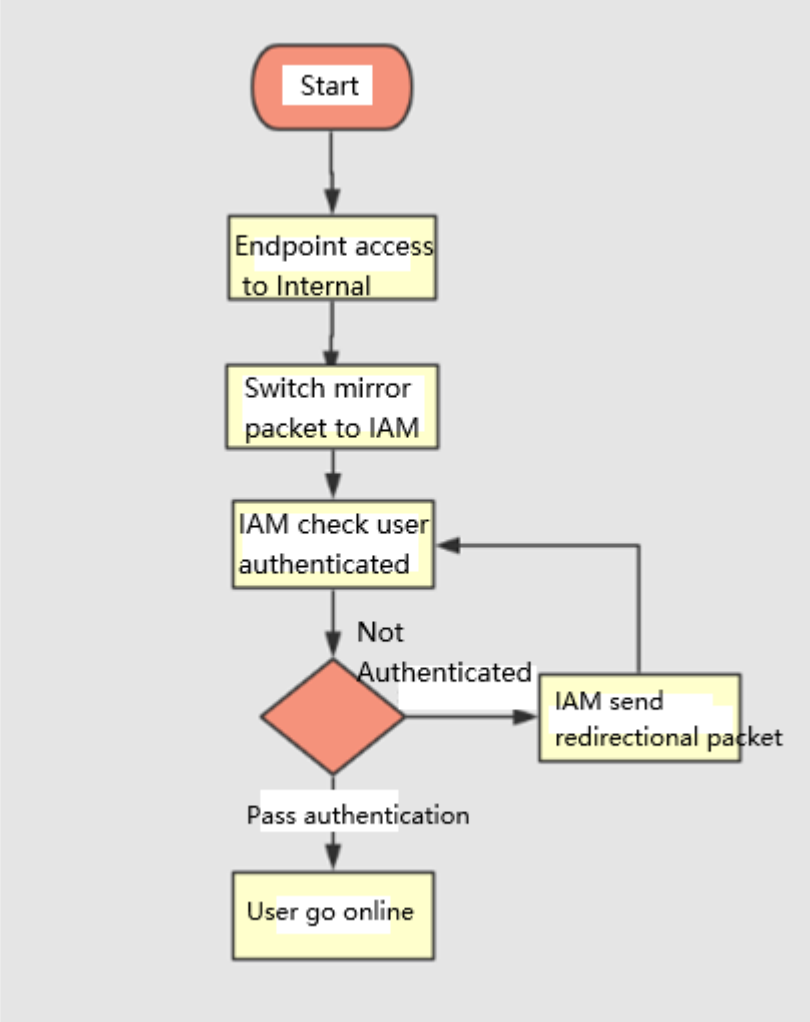
1. IAG diatur sebagai bypass di core switch, ini akan mengatur reset paket menolak permintaan yang tidak diautentikasi; untuk autentikasi yang diperlukan akan mengirim redireksi untuk mengarahkan traffic ke halaman autentikasi.
2. Untuk tidak dapat mengakses bisnis internal sebelum diautentikasi, dan metode ini tidak perlu melalui core switch, solusi ini sederhana, ini hanya diperlukan untuk mirror traffic dari IAG dan switch tidak perlu melakukan konfigurasi.

Bab 2.1 Perbandingan antara RST redireksi authentication dan 802.1x authentication

	Client software	Convenience	Security	Mirror	Proses Autentikasi	Skenario
RST redireksi autentikasi	Tidak dibutuhkan	High	Middle	Yang dibutuhkan	Pengguna mendapatkan IP address, ketika mengakses ke URL tertentu, ini akan dialihkan ke halaman autentikasi portal, setelah itu masukkan username dan password	Layer 3 autentikasi, untuk switch tidak dapat mendukung fungsi 802.1x atau tidak diperlukan untuk docking dengan switch. Perangkat adalah lingkungan 3rd layer dan akses paket akan melalui core switch
802.1x autentikasi	Yang dibutuhkan	Middle	High	Tidak dibutuhkan	Ketika pengguna mengakses layer 2 network yang diperlukan untuk melakukan autentikasi , diperlukan untuk menggunakan klien software untuk melakukan autentikasi, setelah dilakukan autentikasi kemudian dapat mengakses internal resources.	Untuk skenario dimana akses ke network internal secara ketat dikontrol , 802.1x autentikasi digunakan, dan internal network (termasuk Layer 2 network tidak dapat diakses) tidak dapat diakses tanpa autentikasi, artinya, tidak dapat melewati Layer 2 switch.

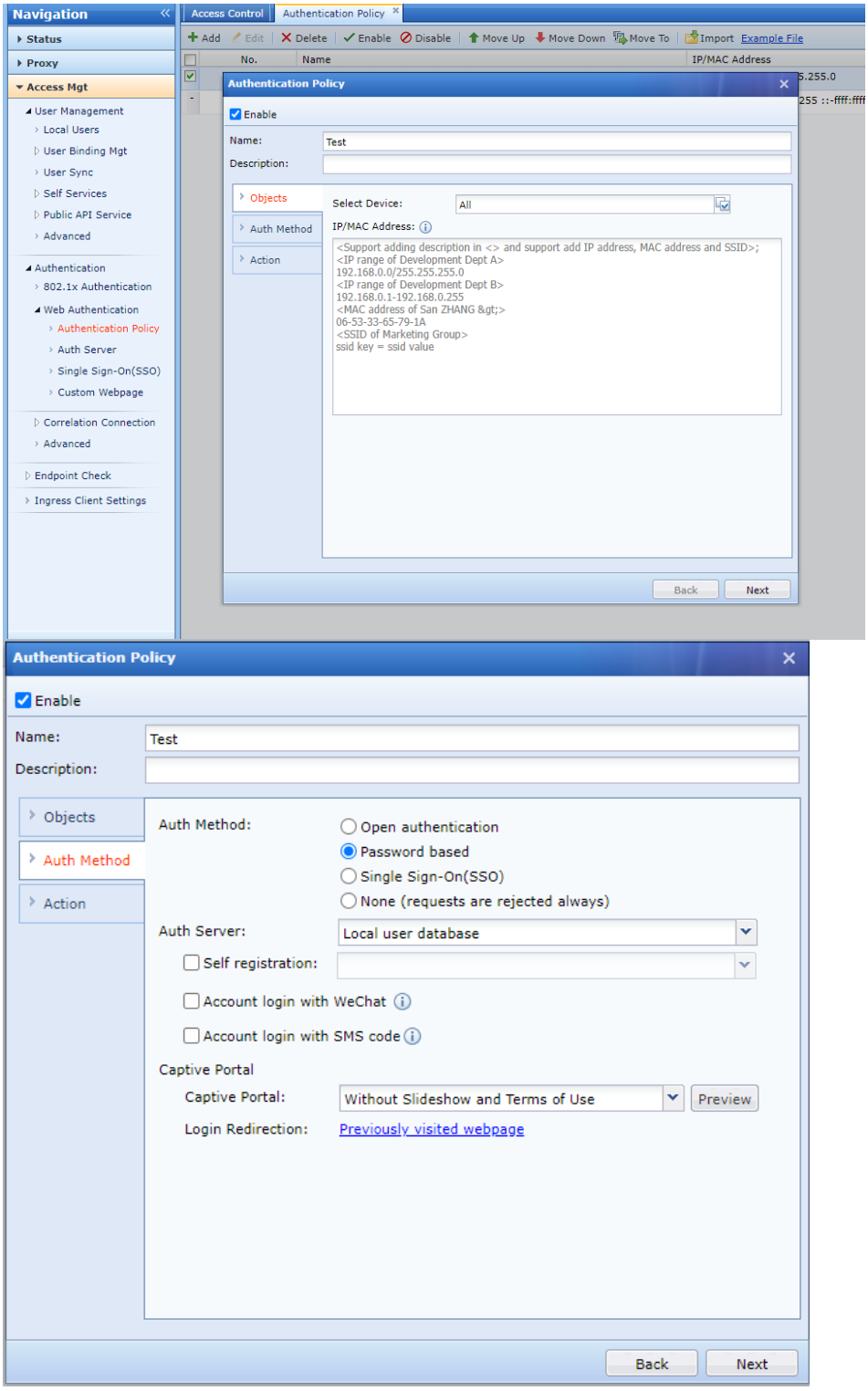
Bab 2.2 Deskripsi Fungsi RST redireksi autentikasi

1. Endpoint access ke bisnis atau data internet melalui switch, switch mirror traffic ke IAG, IAG akan memeriksa endpoint telah diautentikasi atau tidak, jika tidak diautentikasi, ini akan mengirim paket redireksi 302.
2. Ketika endpoint menerima paket redireksi 302, ini akan melakukan autentikasi pada IAG.
3. Setelah endpoint terautentikasi, ini tidak akan mengirim paket redireksi lagi dan mengizinkan traffic, jika autentikasi tidak lewat, ini akan mengirim paket reset untuk menolak akses pengguna ke sumber internal network.
4. Kecuali dari autentikasi, ini juga diperlukan untuk memeriksa endpoint apakah ini memenuhi rule sebelum menyambung ke network, setelah terautentikasi dan memeriksa semua rule, maka mengizinkan untuk mengakses sumber internal network.

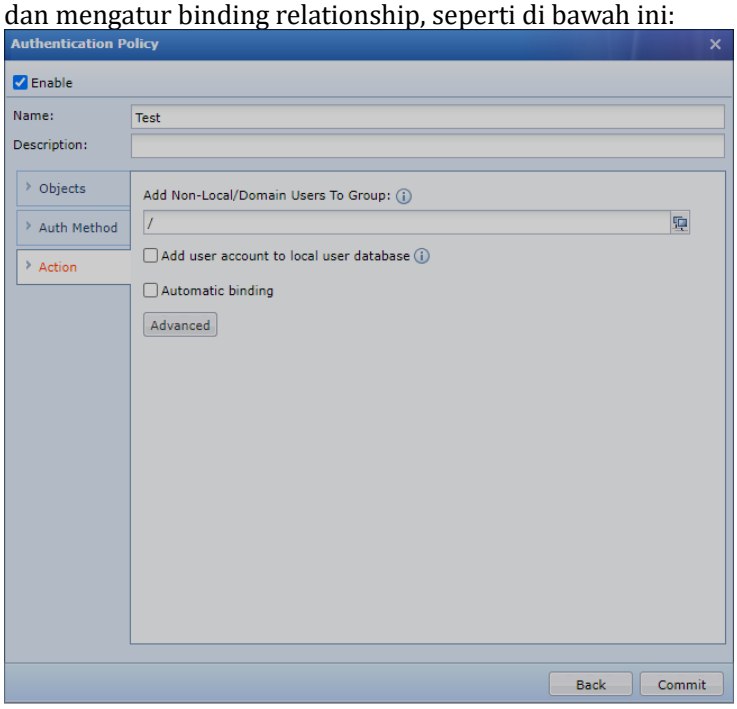


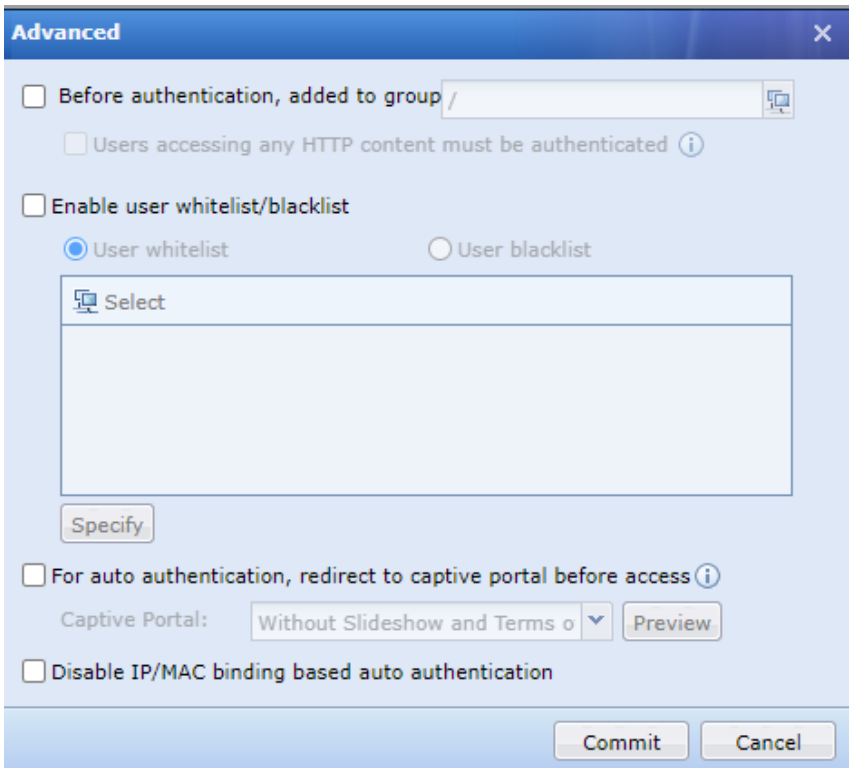
Bab 2.3 Panduan Konfigurasi

1. Switch konfigurasi mirror port dan sambungkan ke mirror port IAG.
2. Konfigurasi baru authentication policy, navigasikan ke Authentication -> Web Authentication -> Authentication policy dan buat baru, Masukkan IP range, authentication method dapat memilih password based, SSO dan None.



3. Action dapat memilih online ke group tertentu, juga dapat Add user into local user group dan mengatur binding relationship, seperti di bawah ini:





Tindakan Pencegahan:

1. RST redireksi hanya mendukung mode bypass deployment.

2. Paket reset hanya dapat mendukung permintaan TCP, permintaan UDP tidak didukung, jika halaman autentikasi tidak dapat mengarahkan ulang diperlukan untuk melakukan penangkapan paket pada IAG untuk memeriksa apakah endpoint telah mengirim paket dan IAG telah mengirim paket RST.

3. Untuk traffic https dapat mengambil efek, tingkat keberhasilan dari redireksi https tergantung pada kecepatan paket balasan dari website, jika paket lebih dari 10mm maka tingkat keberhasilan akan lebih tinggi.