SANGFOR

IAM

Panduan Konfigurasi Web Single Sign–On

Versi 12.0.18

Perubahan Catatan

Tanggal	Deskripsi Perubahan
Dec 31, 2019	Rilis dokument Versi 12.0.18.

Daftar Isi

Bab 1 Kebutuhan Konten 1
1 Pengenalan Produk 1
2 Skenario Aplikasi 1
3 Syarat Kondisi 1
4 Ide Pembuatan 1
5 Panduan Pembuatan dengan Sceenshot 1
5.1 Kebutuhan dan lingkungan pengujian 1
5.2 Pembuatan Single Sign-On 1
5.3 Konfigurasi kebijakan autentikasi 3
6 Yang harus diperhatikan 3

Bab 1 Kebutuhan Konten

1 Pengenalan Produk

Ketika pengguna masuk dengan menggunakan aplikasi web milik mereka sendiri, pada saat yang sama pengguna akan masuk pada perangkat IAM dengan nama pengguna sesuai dengan aplikasi milik pengguna.

2 Skenario Aplikasi

1. Perangkat IAM berperan sebagai sistem otentikasi pelanggan yang memungkinkan pengguna untuk masuk ke system web mereka sekaligus masuk di perangkat kami sebagai pengguna yang terotentikasi untuk mengakses internet.
2. Klien memiliki sistem otentikasi web sendiri dengan sistem nama pengguna dan kata sandi. Setelah dilakukan otentikasi web, klien tidak perlu masuk kembali pada perangkat kami dengan mengirimkan nama pengguna dan mengidentifikasi identitas pada perangkat kami untuk akses internet.

3 Syarat Kondisi

1. Perangkat IAM dengan versi 12.0.18 atau diatasnya.
2. Sebuah sistem masuk web dengan lalu lintas data yang melewati perangkat kami.

4 Ide Pembuatan

1. Siapkan lingkungan untuk pengujian.
2. Membuat Single Sign-On.
3. Membuat kebijakan autentikasi.

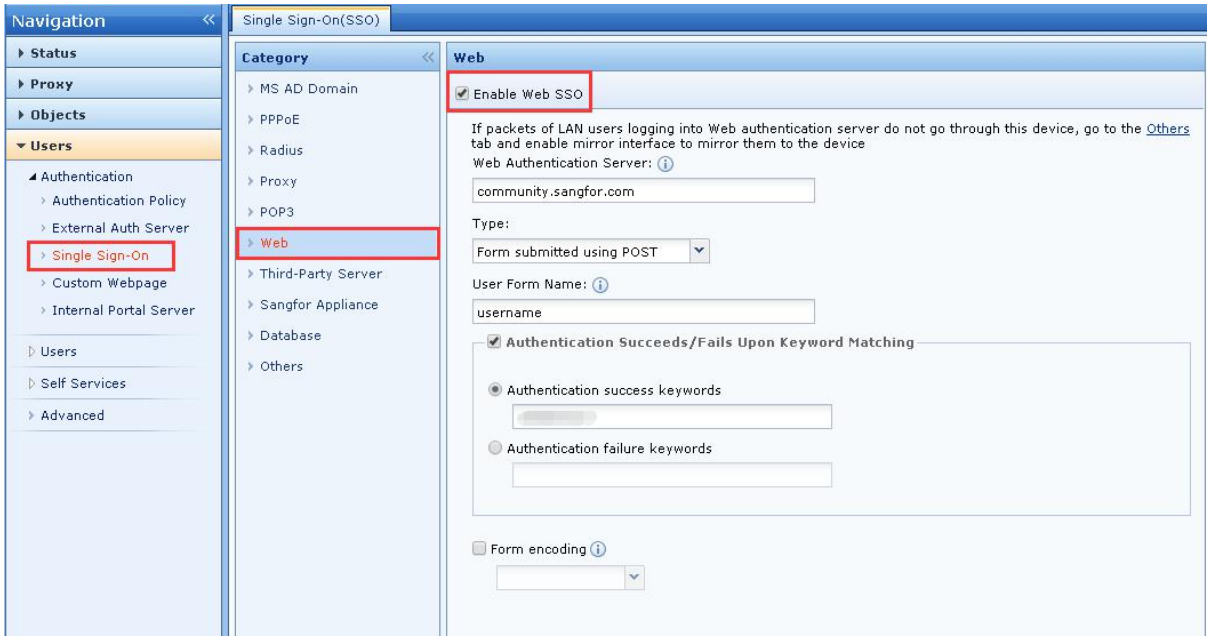
5 Panduan Pembuatan dengan Sceenshot

5.1 Kebutuhan dan lingkungan pengujian

Sebelum mengimplementasikan web single sign-on, kita harus memahami lingkungan jaringan klien yang mana lalu lintas sistem web akan melewati perangkat IAM. Konfigurasikan sistem single sign-on web jika lalu lintas melewati perangkat kami. Jika lalu lintas tidak melewati perangkat kami, kami perlu mengarahkan data yang sesuai ke perangkat kami.

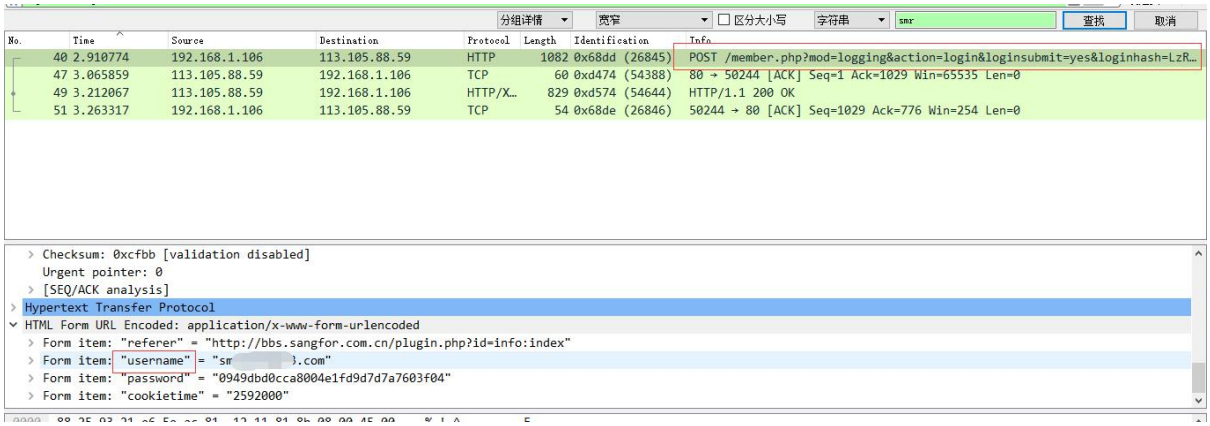
5.2 Pembuatan Single Sign-On

Sistem web single sign-on IAM 11.0 memiliki perubahan besar dibandingkan dengan versi sebelumnya. Selain itu, didukung dengan fungsi POST untuk mengirimkan nama pengguna yang menambahkan fungsi mengambil data pengguna melalui cookie dan parameter URL. IAM akan memilih [Type] yang terkait dengan cara pengguna memasukkan nama pengguna di aplikasi web. Kita dapat menentukan apakah login pengguna berhasil berdasarkan “return value” dari server. IAM tidak dapat mengidentifikasi apakah login berhasil jika tidak ada respon dari server. Diagram di bawah ini adalah konfigurasi Single Sign-On dengan mengirimkan POST sebagai contoh.

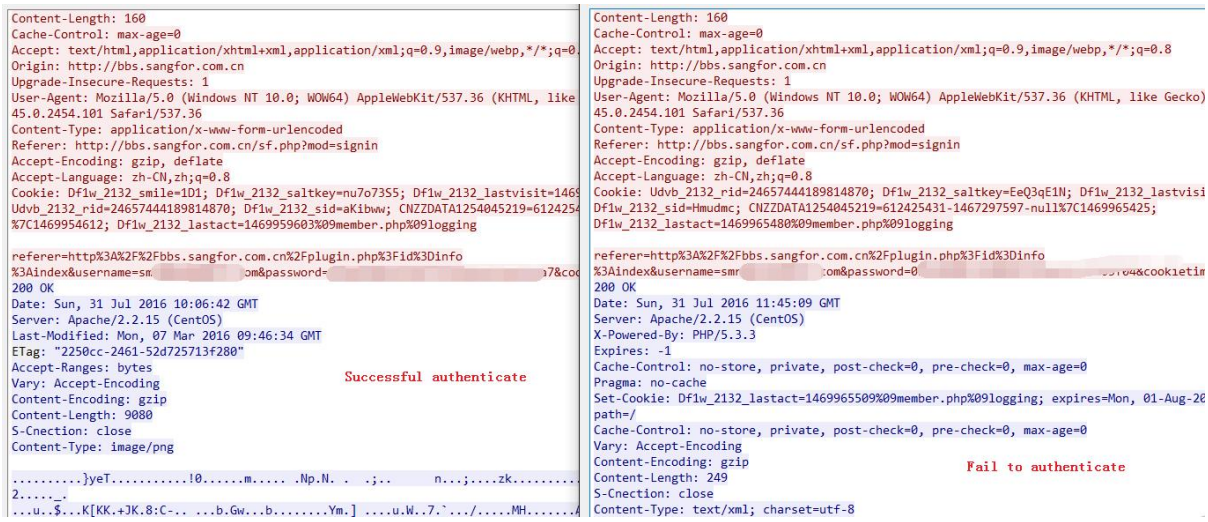


Otentikasi server web diisi dengan nama domain web pengguna atau alamat IP, seperti diagram di atas. Isikan dengan community.sangfor.com, pilih [Type] sesuai form yang dikirimkan menggunakan POST, isikan [User Form Name:] sesuai aslinya nama formulir, Anda dapat mencari admin web untuk memberikan informasi, jika tidak, Anda dapat menggunakan https watch for wireshark untuk menangkap paket lalu lintas guna mengidentifikasi informasi yang diperlukan.

Dengan menangkap paket dari “community.sangfor.com” seperti diagram di bawah ini, kita bisa melihat username dari form name yaitu “Username”

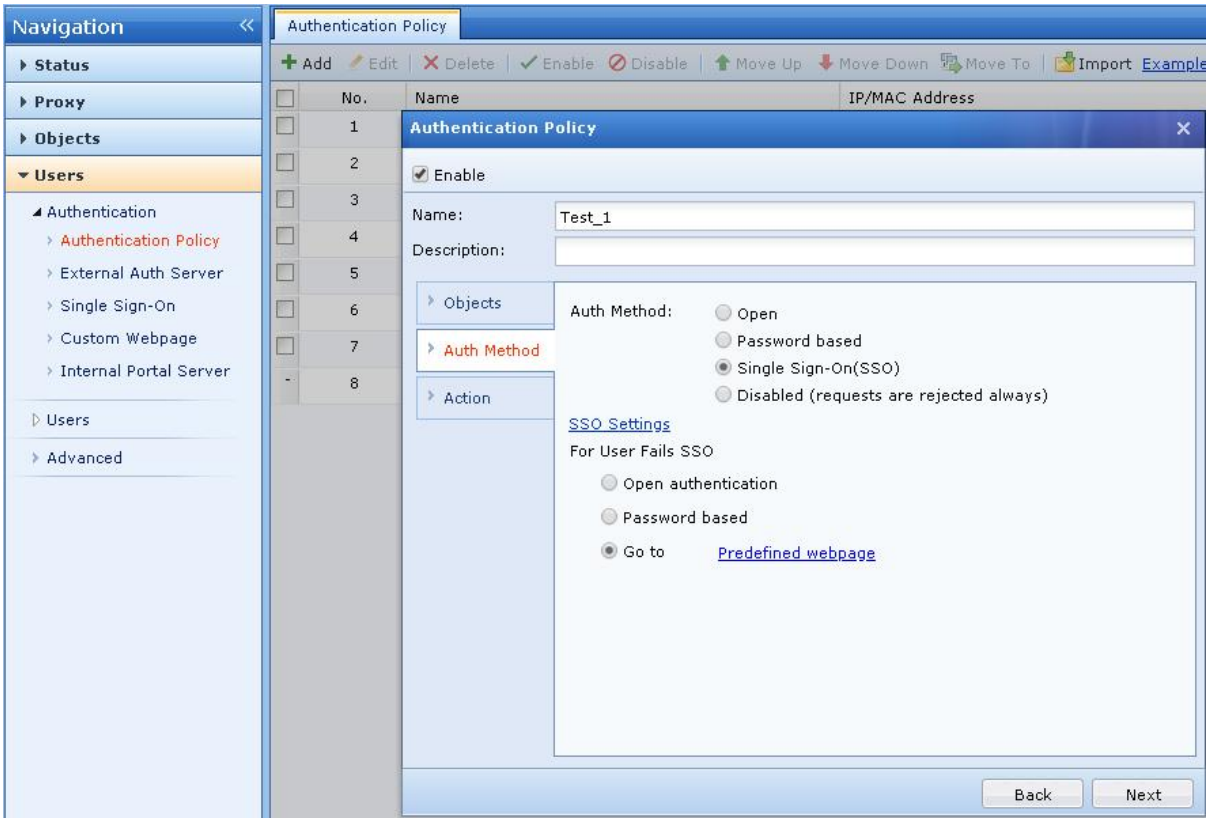


Berikut ini adalah mengaktifkan [Authentication Keyword], di sini Anda dapat memilih kata kunci sukses atau kata kunci gagal. Anda bisa mendapatkan kata kunci dari data yang dikembalikan oleh server web. Seperti diagram dibawah ini adalah paket capture oleh Wireshark dan bandingkan antara otentikasi yang berhasil dan yang gagal untuk otentikasi data yang dikembalikan oleh server.



5.3 Konfigurasi kebijakan autentikasi

Untuk kebijakan otentikasi, pastikan pahami objek otentikasi sebelum mengkonfigurasi kebijakan, pilih [Single Sign-On] sebagai metode otentikasi, untuk pengguna gagal SSO dapat dikonfigurasikan sesuai dengan kebutuhan pelanggan seperti diagram di bawah ini.



6 Yang harus diperhatikan

1. Selama pengujian, jangan masuk dan keluar berulang kali pada alamat IP, ini akan menyebabkan otentikasi SSO gagal.
2. Cara yang kami sebutkan untuk mendapatkan “username” untuk tabel formulir dan kata kunci otentikasi menggunakan http watch dan Wireshark, dari dokumen ini kami tidak menyediakan panduan pengoperasian terkait Wireshark dan Anda dapat mengetahui sendiri metode pengoperasiannya.