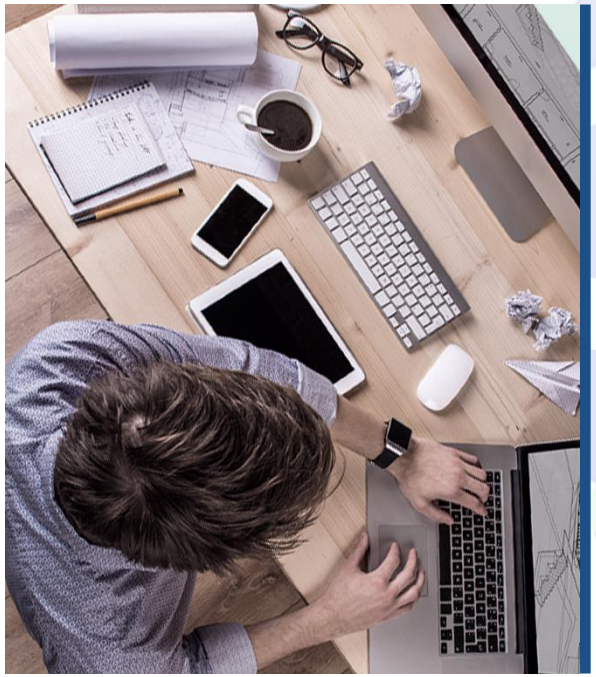
SANGFOR

SANGFOR_NGAF_V8.0.6_Professional

Dekripsi



1. Pengenalan
2. Mendekripsi data ke server internal
3. Mendekripsi data ke internet
4. HSTS

1. Pengenalan

SANGFOR
深信服科技

Latar Belakang

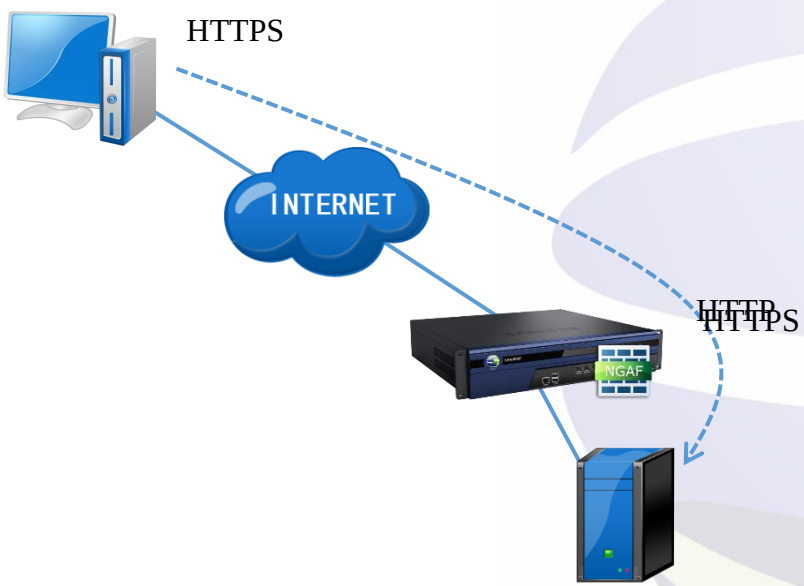
Informasi yang Anda kirim ke Internet diteruskan dari komputer ke komputer untuk sampai ke server tujuan. Komputer apa pun di antara Anda dan server dapat melihat detail pribadi Anda, dan informasi sensitif lainnya jika tidak dienkripsi dengan certificate SSL. Ketika certificate SSL digunakan, informasi menjadi tidak dapat dibaca oleh semua orang kecuali untuk server tempat Anda mengirim informasi. Ini melindunginya dari peretas dan pencuri identitas.

Akibatnya, meningkatnya adopsi protokol SSL untuk mengenkripsi komunikasi Internet menyediakan penjahat cyber dengan lebih banyak cara untuk menghindari deteksi. Sangfor NGAF dapat memeriksa traffic HTTPS dengan bertindak sebagai penengah.

Skenario

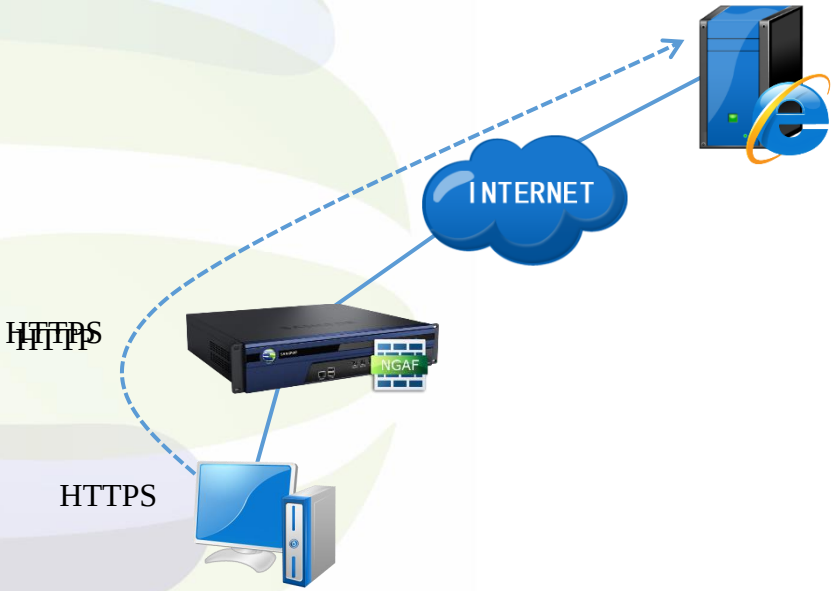
Ada dua skenario dekripsi SSL.

1. Dekripsi data ke server internal dari Internet.



Klien mengakses server HTTPS dalam dengan inspeksi dekripsi untuk melindungi dari dalam server.

2. Dekripso data ke Internet dari LAN



Klien mengakses server HTTPS eksternal dengan inspeksi dekripsi untuk melindungi host internal.

2. Mendekripsi data ke server internal

SANGFOR
深信服科技

Mendekripsi data ke server internal dari Internet

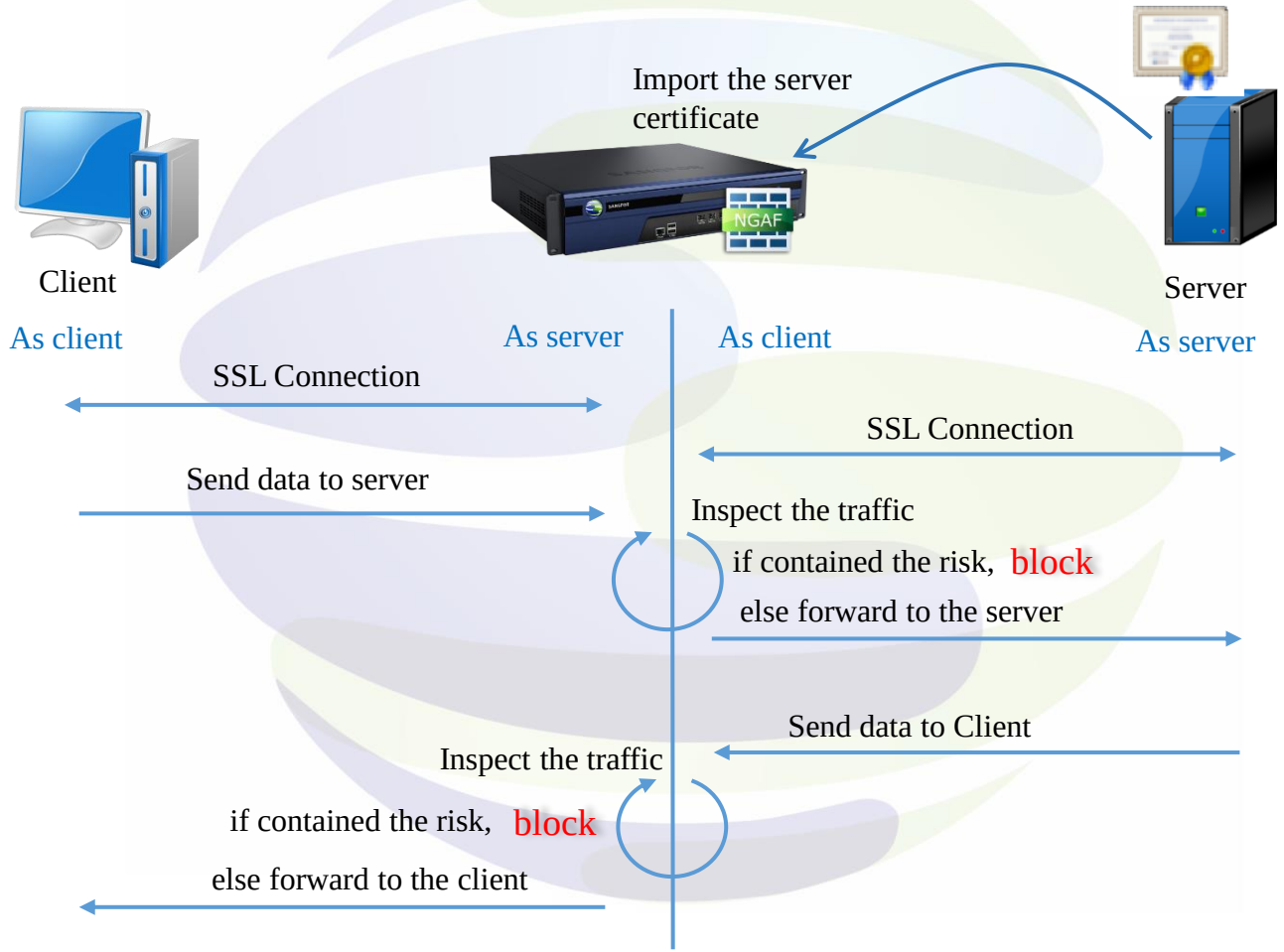
Teori

Handshake klien dengan NGAF pada awalnya, setelah handshake berhasil, NGAF memulai koneksi SSL dengan real server (NGAF adalah klien). Ketika handshake berhasil, NGAF menerima dan mendekripsi data yang dikirim klien, data yang didekripsi akan dikirim ke WAF dan fungsi lain untuk diperiksa. Jika ditemukan serangan, mereka memblokir, jika tidak meneruskan data ke server. Ini adalah cara yang sama untuk menangani data yang me-reply dari server.

Tetapi certificate NGAF tidak ada pada list **Trusted Root Certification Authorizes**, kita harus meng-impor certificate server ke NGAF.

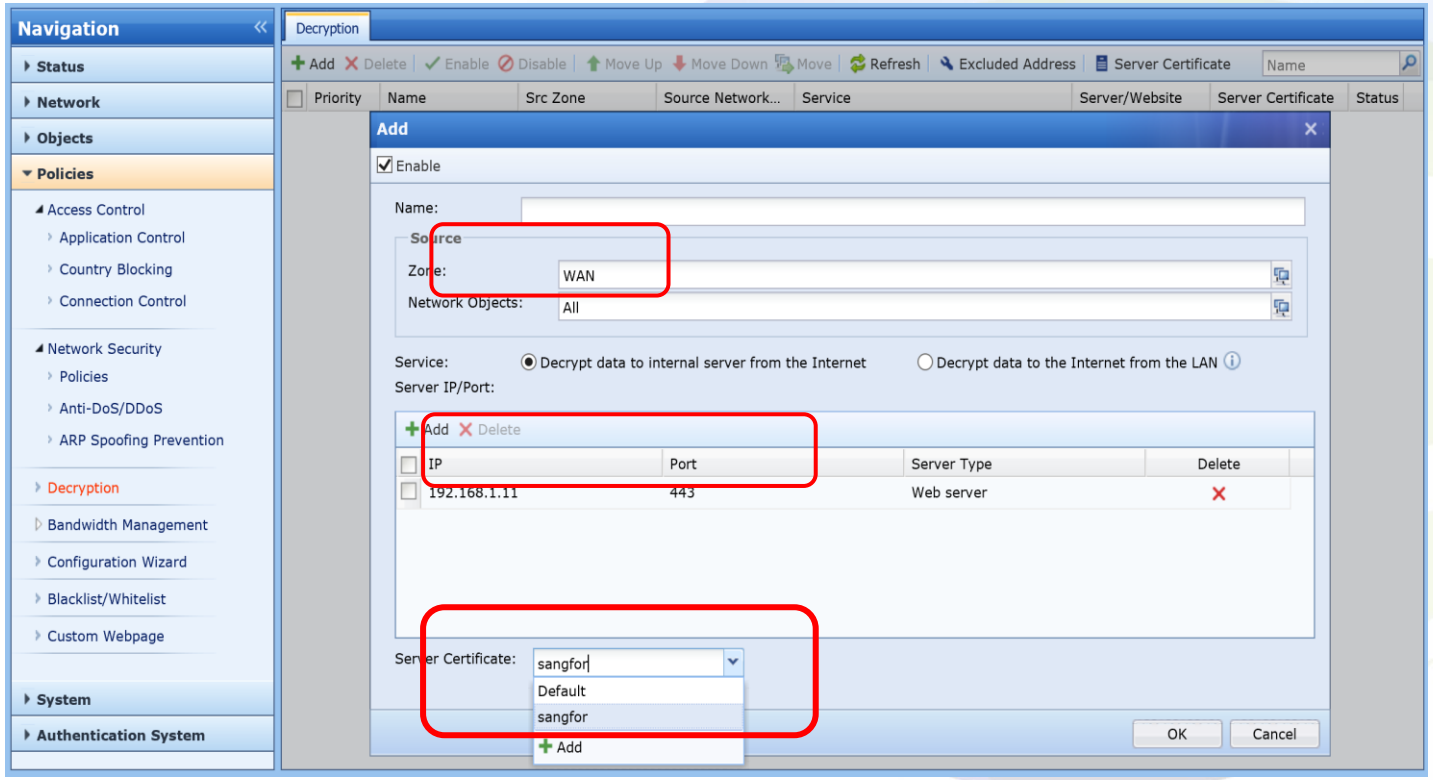
Mendekripsi data ke server internal dari Internet

Teori



Mendekripsi data ke server internal

Server scenario perlu mengisi source zone, source IP group, server IP dan port, serta menambahkan certificate server, default dengan certificate **Default**.

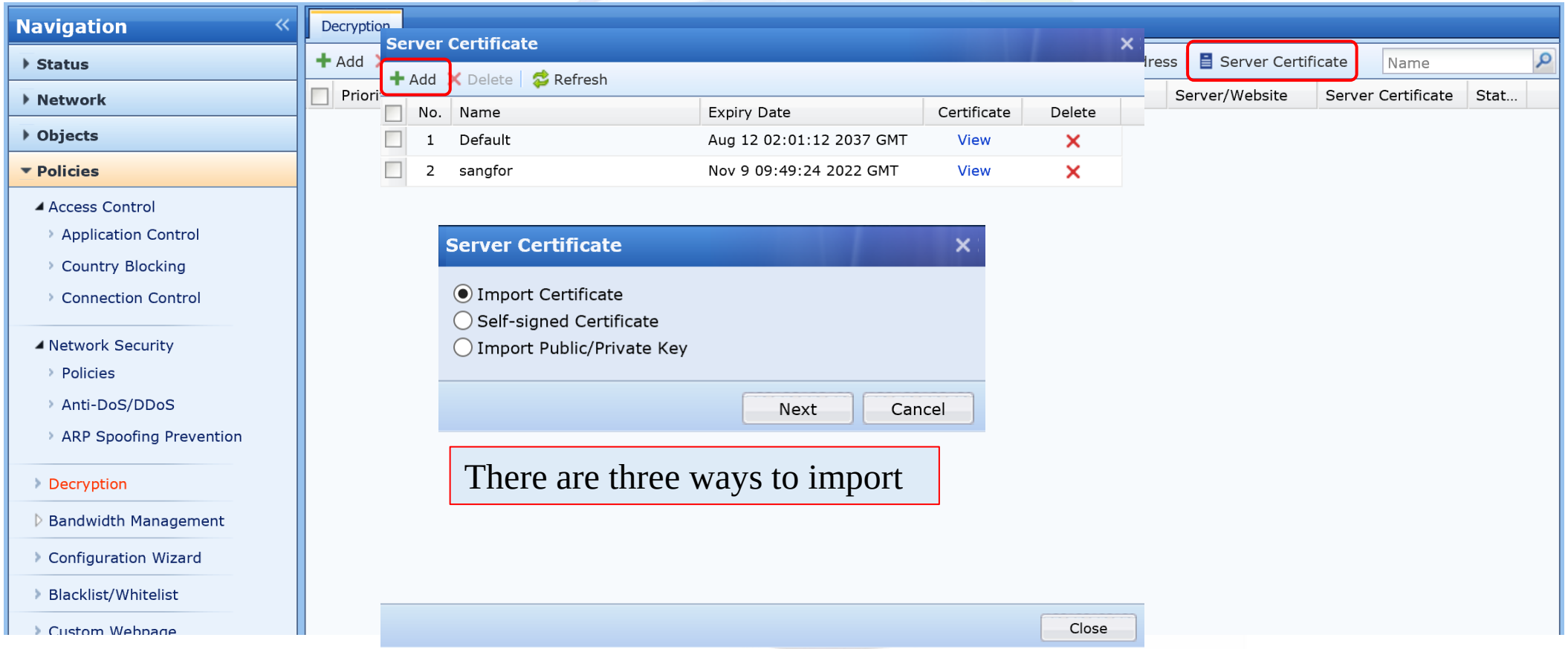


(certificate NGAF tidak ada pada list **Trusted Root Certification Authorizes**, browser akan memunculkan halaman web peringatan. Perlu mengimpor certificate server ke NGAF.)

Pengaturan skenario proteksi server mengharuskan pelanggan untuk menyediakan public key dan private key, dan jika ada password, itu juga perlu disediakan memberikan password (format spesifik akan dijelaskan di bawah)

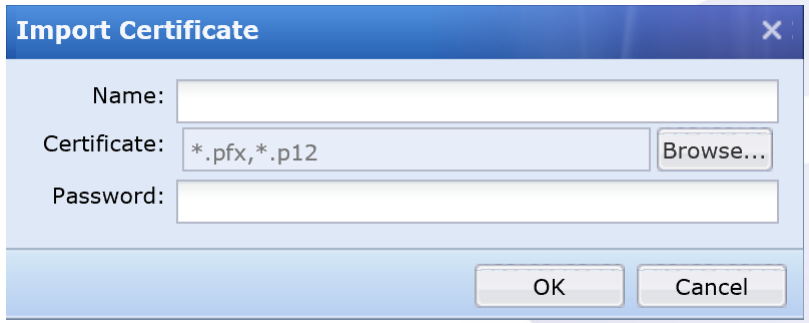
Mendekripsi data ke server internal

Bagaimana cara mengimpor certificate server?



Mendekripsi data ke server internal

1. Import Certificate



.pfx, .p12, Kedua certificate ini adalah kombinasi public key dan private key.
(Ini hanya dapat didekripsi dengan mengimpor public key dan private key)

You can export the certificate from the server as below:

openssl pkcs12 -export -in server.crt -inkey server.key -out server.pfx

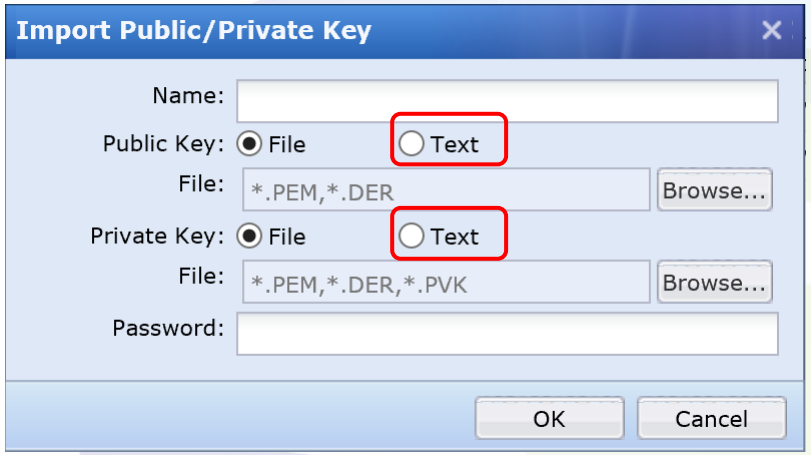
Mendekripsi data ke server internal

2. Self-signed Certificate

Self-signed certificate adalah certificate yang dibuat oleh diri kita sendiri yang bertindak sebagai CA (certificate ini tidak ada pada list **Trusted Root Certification Authorizes**, jadi itu ilegal). Browser akan muncul halaman web peringatan jika sesuai dengan kebijakan yang digunakan certificate ini, jadi umumnya kami tidak menggunakannya.

Mendekripsi data ke server internal

3. Import Public/Private Key



Hal ini dapat diimpor oleh sepasang Public Key dan Private Key.

Format untuk Public Key dapat seperti pem, der, crt;
Format untuk Private Key dapat seperti pem, der, cakey;
Crt dan cakey tidak dapat diimpor secara langsung, dapat menyalin text dan menempelkan text di **Text**.

3. Mendekripsi data ke internet

SANGFOR
深信服科技

Mendekripsi data ke Internet dari LAN

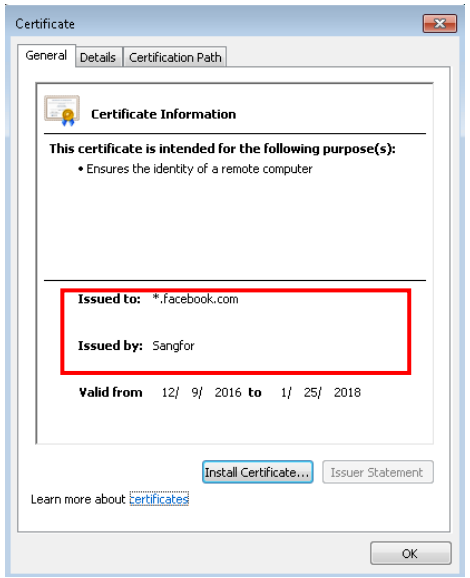
Teori

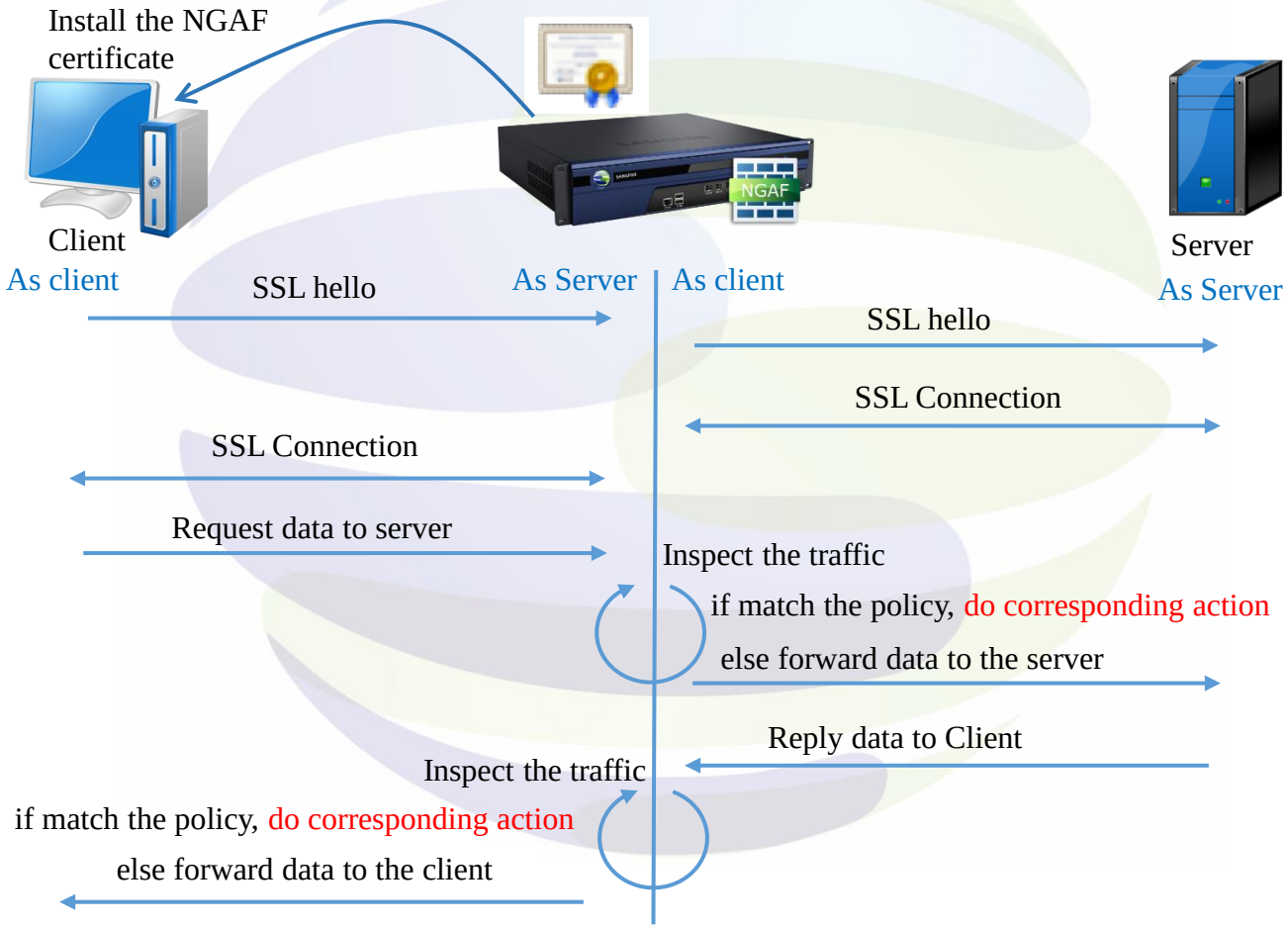
Ketika PC klien memulai permintaan koneksi SSL, perangkat NGAF akan bertindak sebagai server proxy dan mengirim permintaan ke server SSL pada perilaku PC klien, dan setelah koneksi terbentuk, NGAF akan membalas permintaan PC klien.

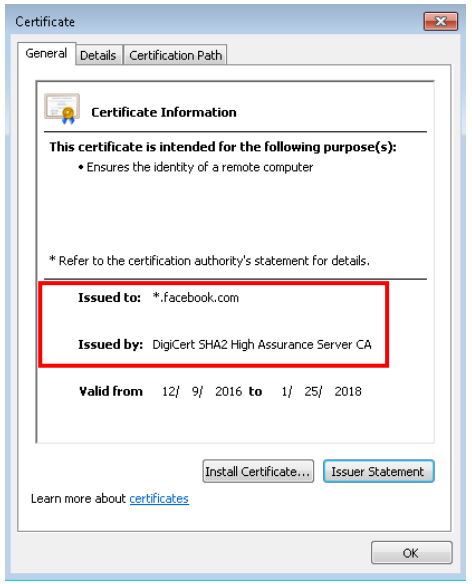
Perangkat NGAF bertindak sebagai server SSL (untuk PC klien) dan sebagai klien (untuk server SSL eksternal). Oleh karena itu, PC klien dan koneksi NGAF dienkripsi menggunakan certificate SSL NGAF tetapi koneksi antara NGAF dan server SSL eksternal menggunakan certificate server SSL untuk mengenkripsi data. Dengan demikian, PC klien akan melihat certificate dikeluarkan oleh NGAF tetapi tidak dari server SSL asli.

Mendekripsi data ke Internet dari LAN

Teori

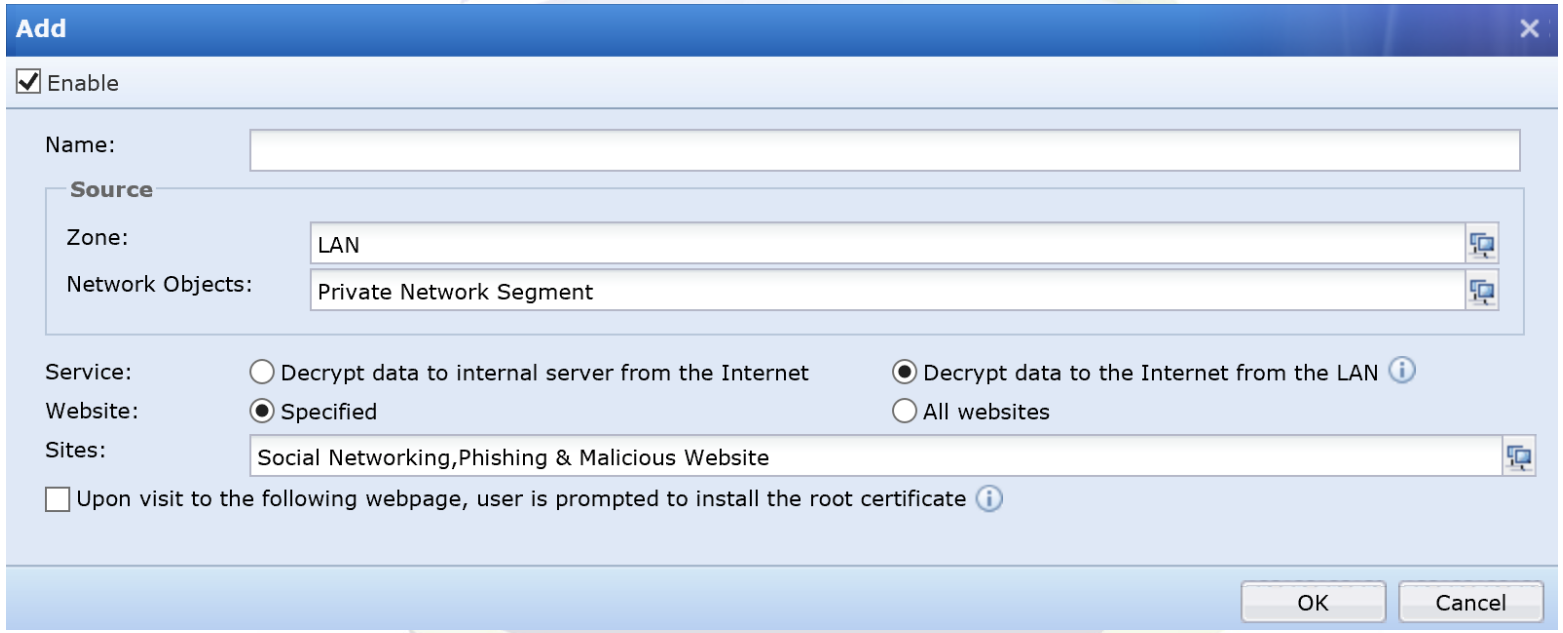






Mendekripsi data ke Internet dari LAN

Skenario perlindungan pengguna perlu mengisi source zone, source IP group, situs web untuk didekripsi.



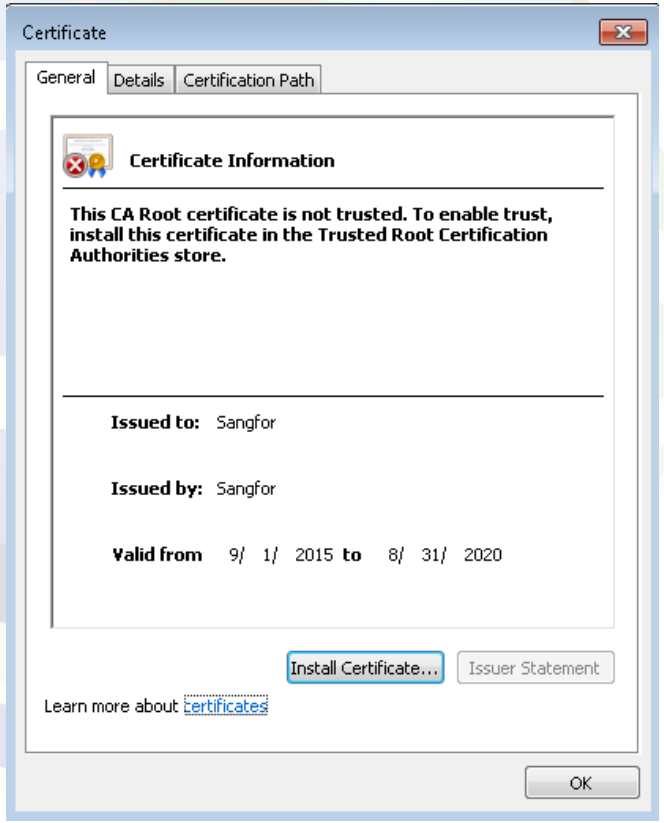
Dibandingkan dengan server protection, tidak ada certificate yang dapat dipilih, tetapi klien perlu menginstal certificate untuk menghilangkan security alert pada browser karena certificate NGAF tidak ada di list **Trusted Root Certification Authorizes.**

Mendekripsi data ke Internet dari LAN

Biasanya tidak lebih dari 1 klien dalam jaringan, Bagaimana mendistribusikan certificate ke semua klien?

Ada tiga cara:

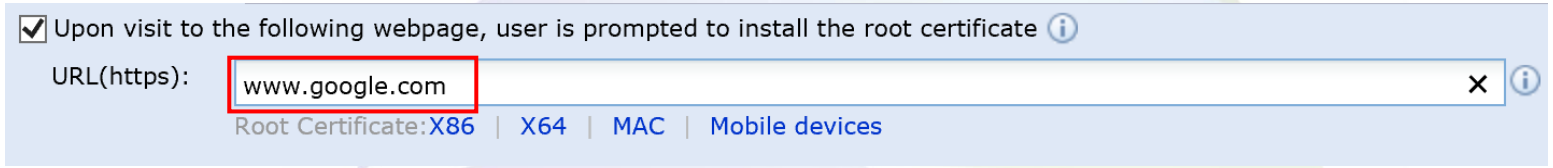
1. Prompt pada web browser
2. AD domain
3. User authentication



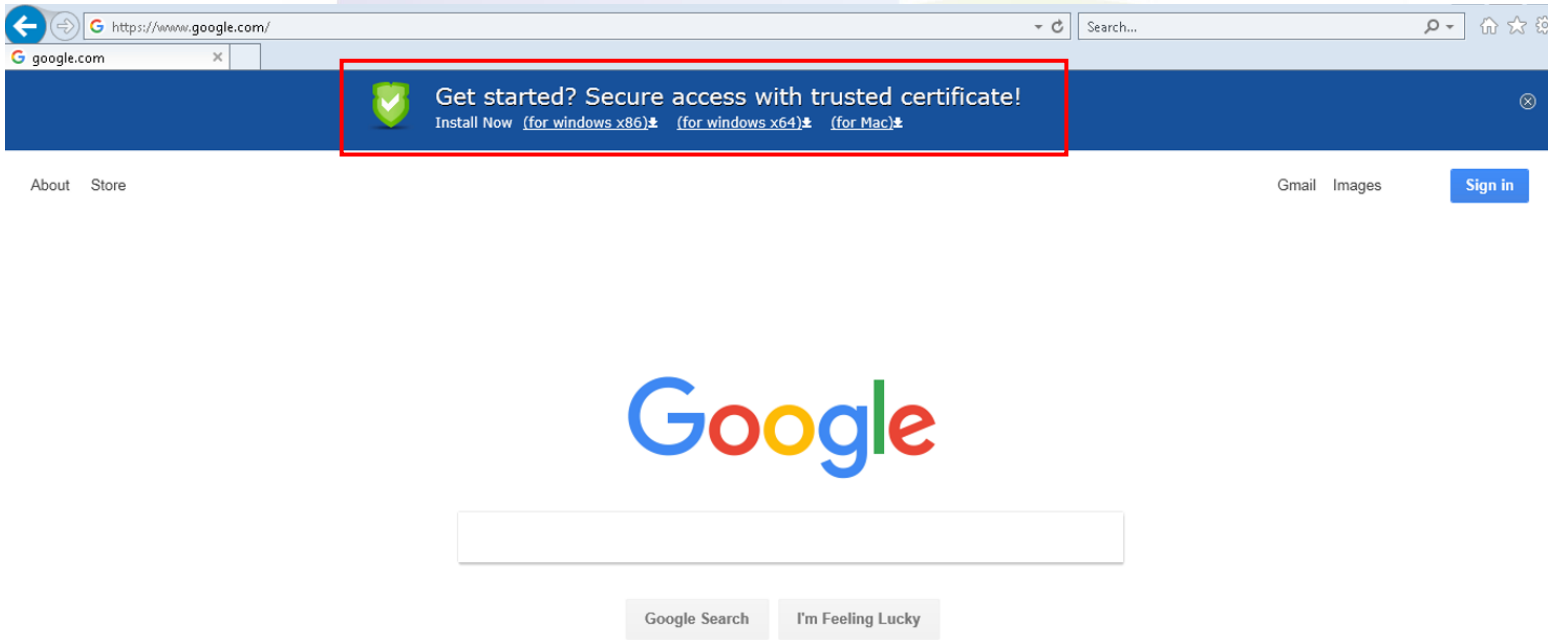
Mendekripsi data ke Internet dari LAN

1. Prompt pada web browser

   Mengatur URL untuk meminta certificate



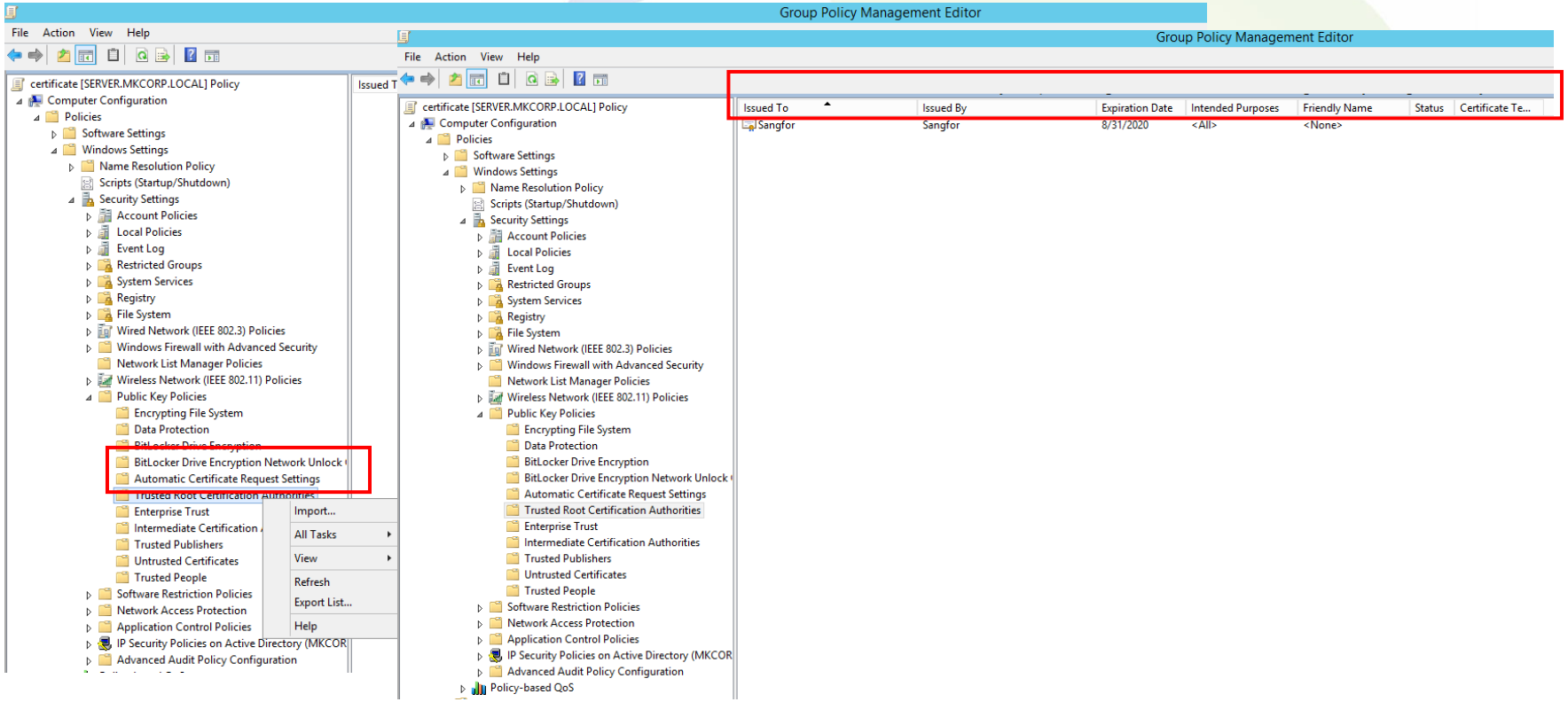
   Klien bisa mendapatkan link download di bagian atas website ketika Anda mengunjunginya.



Mendekripsi data ke Internet dari LAN

2. AD domain

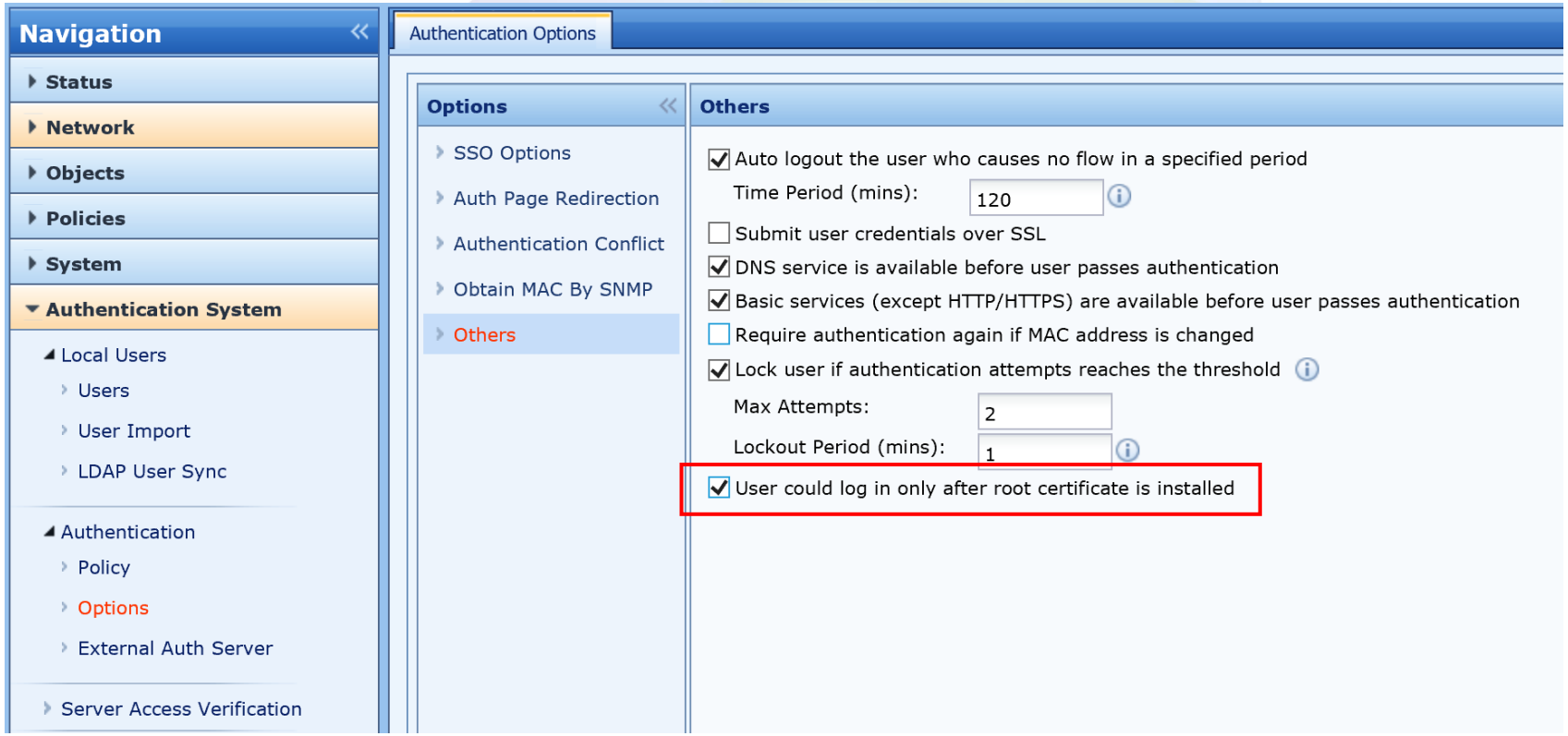
Jika pelanggan memiliki domain, itu adalah cara yang baik untuk mendistribusikan certificate. Tambahkan **Group Policy** untuk mengimpor certificate dari NGAF ke **Trusted Root Certification Authorities**, lau meng-update **Group Policy** untuk semua pengguna domain dengan ‘gpupdate’.



Mendekripsi data ke Internet dari LAN

3. User authentication

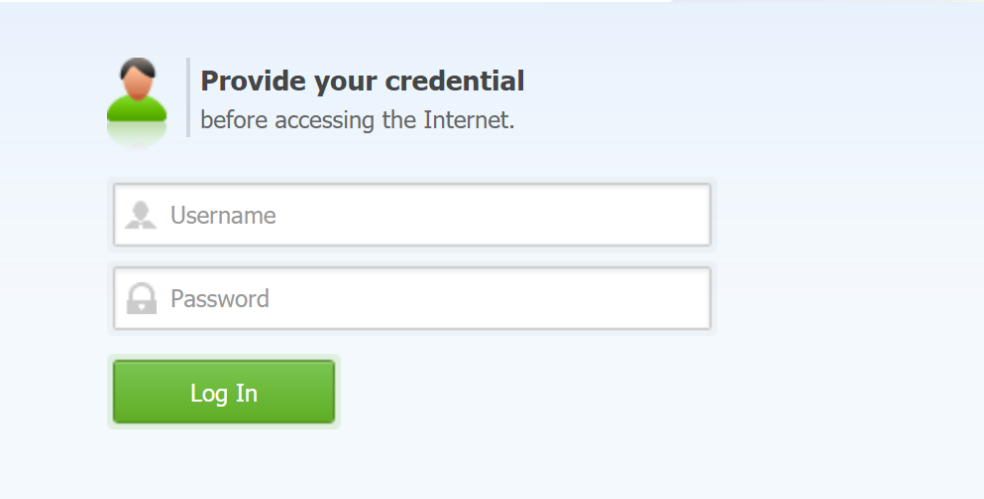
Meng-instal certificate dikombinasikan dengan otentikasi pengguna dengan mengaktifkan opsi berikut, memaksa pengguna untuk menginstal certificate.



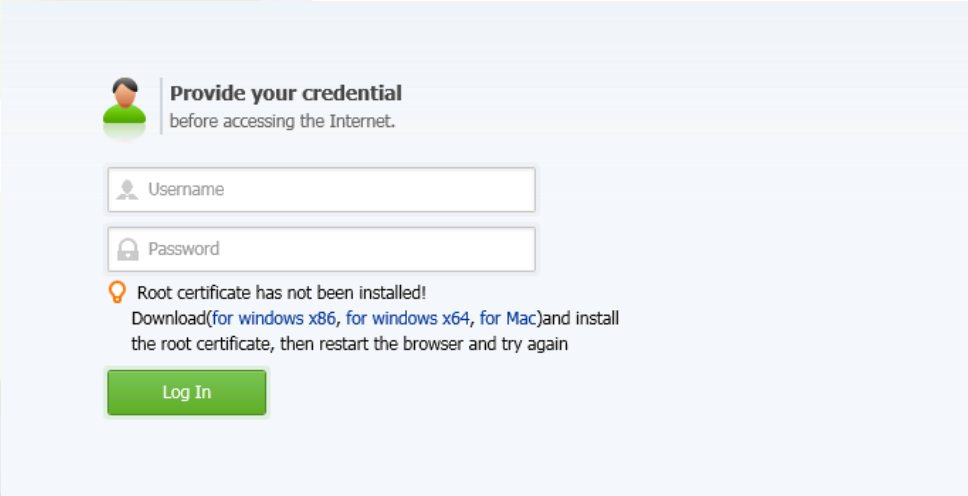
Mendekripsi data ke server internal

Efek dari memaksa untuk menginstal sertifikat.

Tidak Aktifkan



Diaktifkan



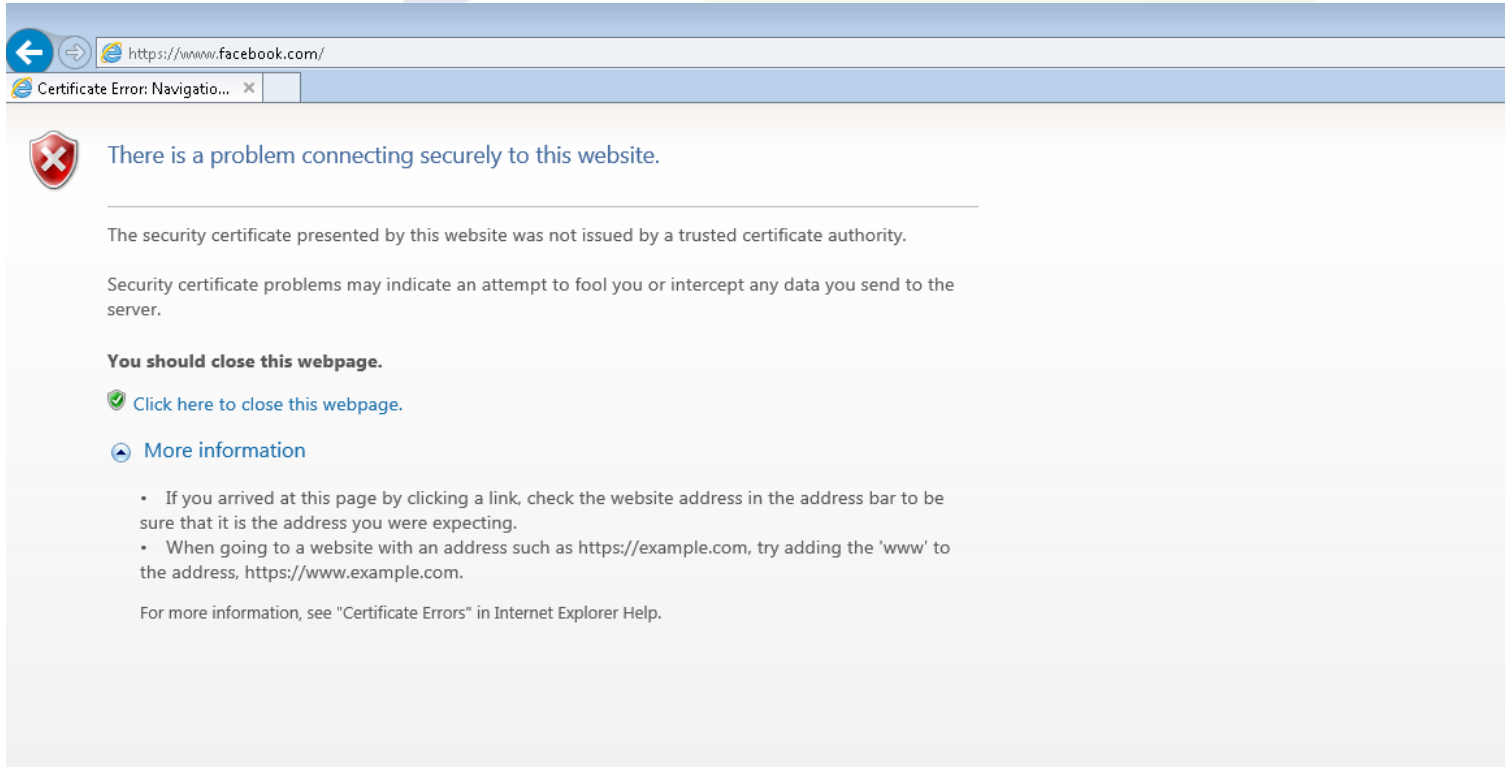
Jika certificate belum diinstal, pengguna tidak dapat memasukkan password.

4. HSTS

SANGFOR
深信服科技

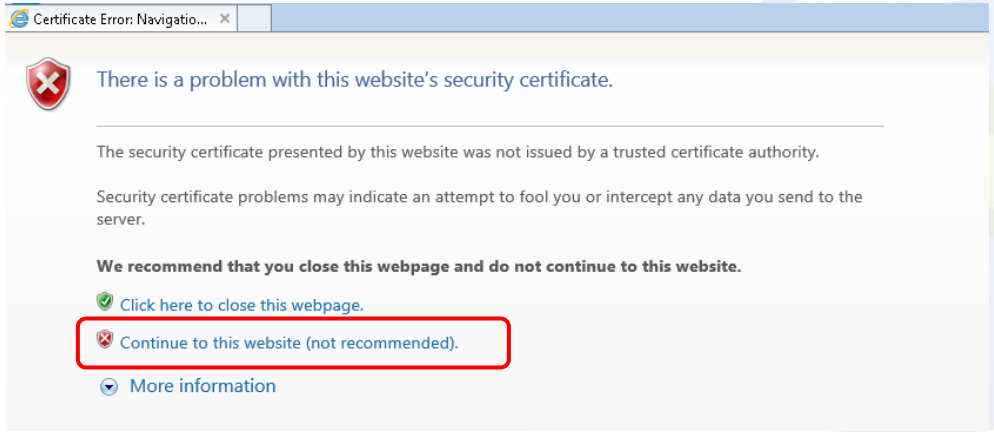
HSTS

HSTS (HTTP Strict Transport Security) Adalah mekanisme web security policy. Ini dapat membantu melindungi situs web dari serangan SSL-stripping man-in-the-middle. Jika keamanan koneksi tidak dapat dipastikan (misalnya certificate TLS server tidak dipercaya), tampilkan pesan kesalahan dan jangan izinkan pengguna mengakses aplikasi web seperti di bawah ini.

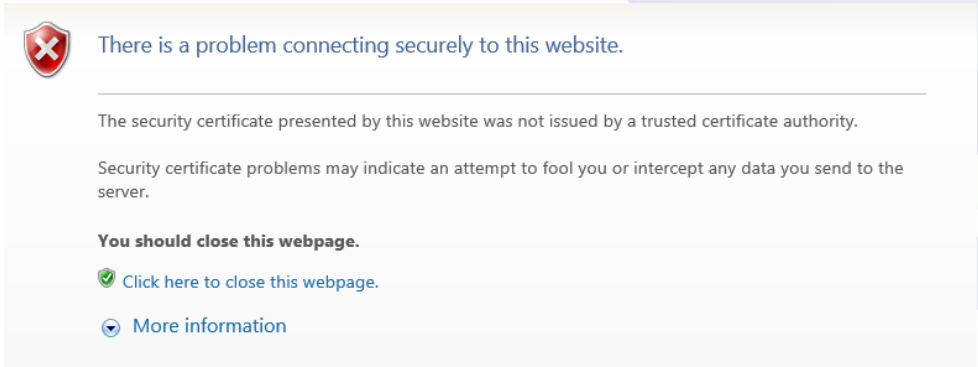


HSTS

Jika hal itu adalah situs web non-HSTS dan klien tidak mengimpor certificate NGAF ke browser, kita dapat mengklik 'Continue to this website(not recommended)' untuk menelusurinya

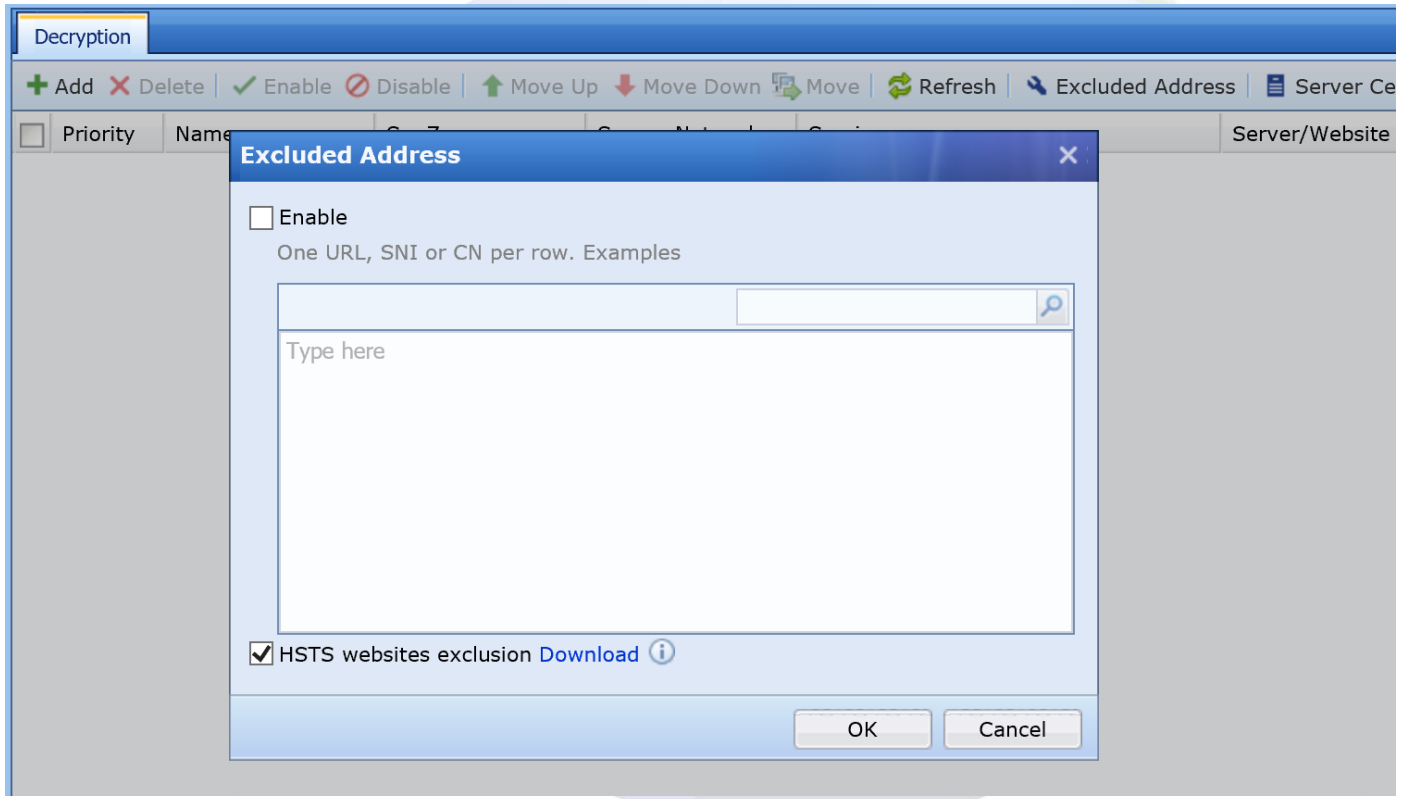


Tetapi jika klien tidak menginstal sertifikat, tidak ada pilihan untuk menelusuri.



HSTS

Ada daftar situs web HSTS bawaan yang dikecualikan dalam NGAF untuk menghindari dekripsi diaktifkan dan certificate tanpa instalasi.



Pemberitahuan: Jika Anda ingin mendekripsi situs web HSTS, certificate harus diinstal di awal.

Dekripsi terverifikasi

Bagaimana cara memeriksa apakah dekripsi berhasil?

Skenario Server

Pengujian serangan untuk trafik HTTPS dan periksa apakah NGAF dapat memblokir dan meng-log nya.

Skenario Internet Access

Periksa apakah ‘**issued by’** certificate situs web HTTPS adalah **Sangfor.**
Pengujian serangan untuk trafik HTTPS dan periksa apakah NGAF dapat memblokir dan meng-log nya.

Terimakasih!

tech.support@sangfor.com
community.sangfor.com

Sangfor Technologies (Kantor Pusat)
Blok A1, Nanshan iPark, No.1001
Jl. Xueyuan, Distrik Nanshan,
Shenzhen, Provinsi Guangdong,
P. R. China (518055)