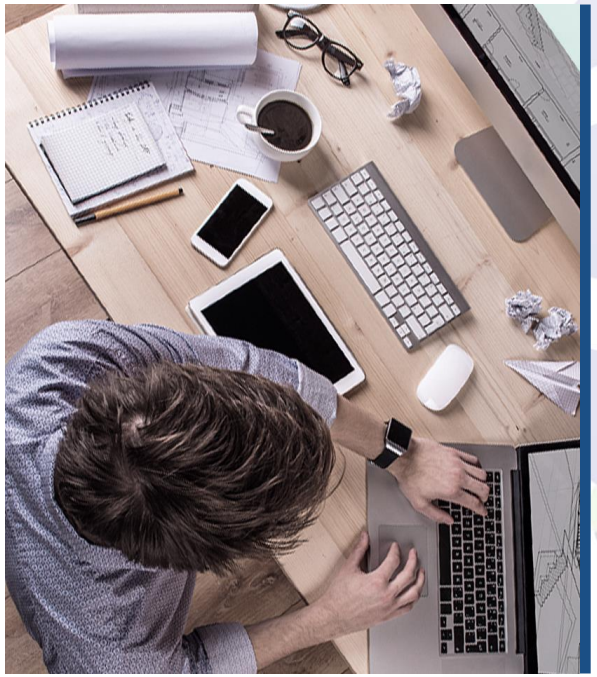
SANGFOR

SANGFOR_NGAF_V8.0.6_Professional

Security Assistant



1. Analisis Kerentanan RT
2. Peringatan Ancaman
3. Analisis Resiko
4. Web Scanner

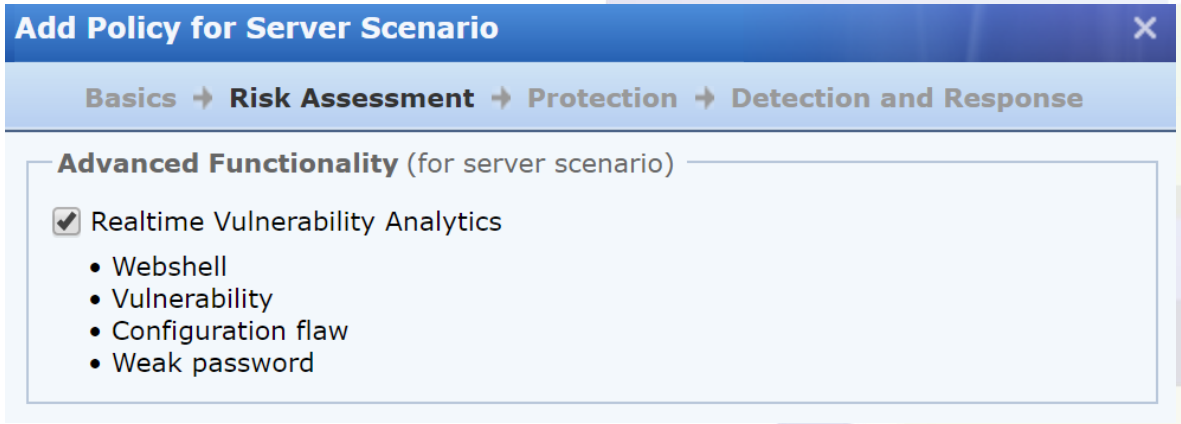
1. Analisis Kerentanan RT

SANGFOR
深信服科技

Analisis Kerentanan RT

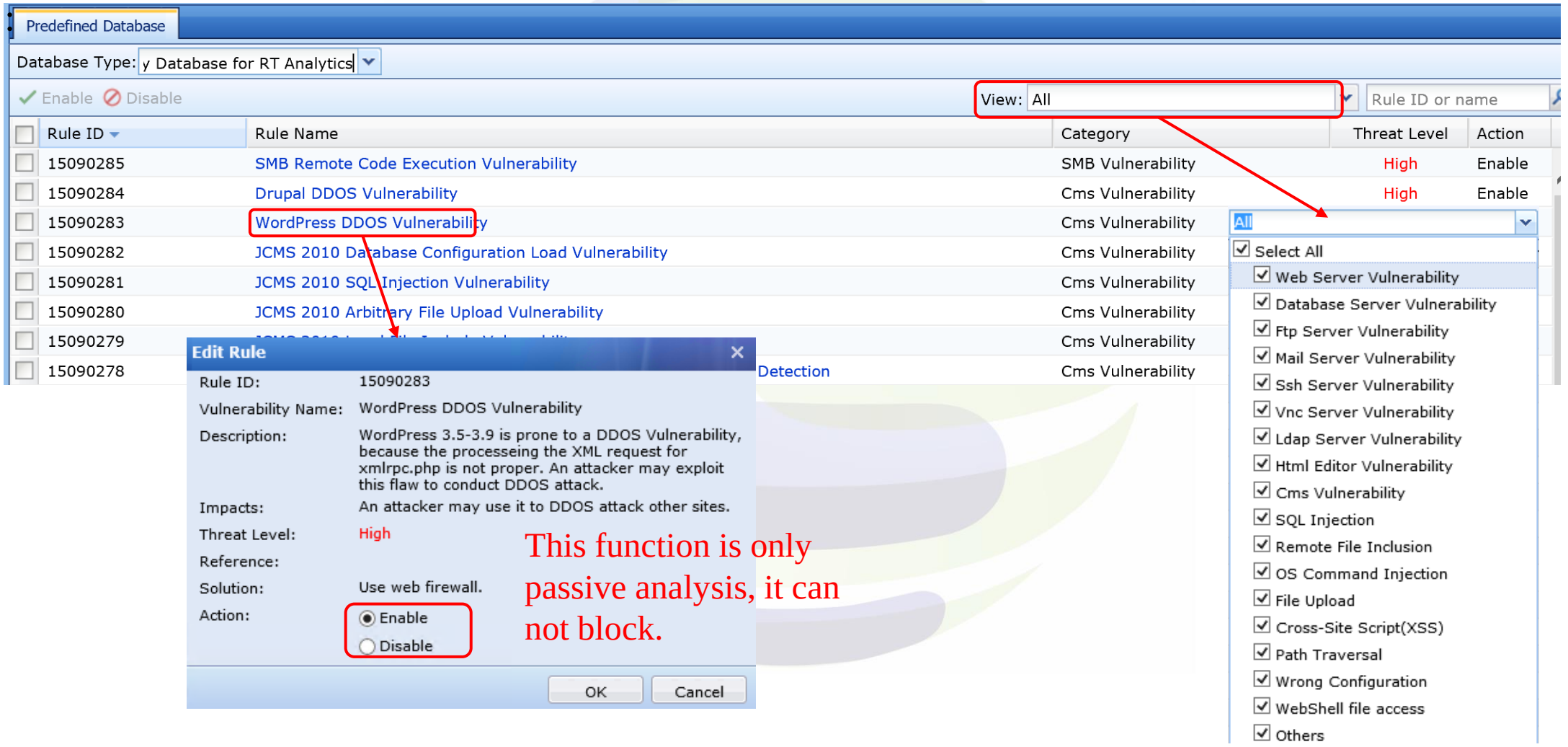
RT Vulnerability Analytics adalah pemindai kerentanan pasif. Data yang melalui perangkat atau bypass akan dicerminkan untuk menganalisis deteksi real-time masalah security di jaringan pelanggan. Proses ini tidak akan mengganggu proses penerusan data di perangkat, tidak akan mengirim paket reset, dan tidak akan mempengaruhi kinerja. Laporan informasi kerentanan akan diproduksi setelah pemindaian selesai.

Ini mendeteksi hal-hal berikut:



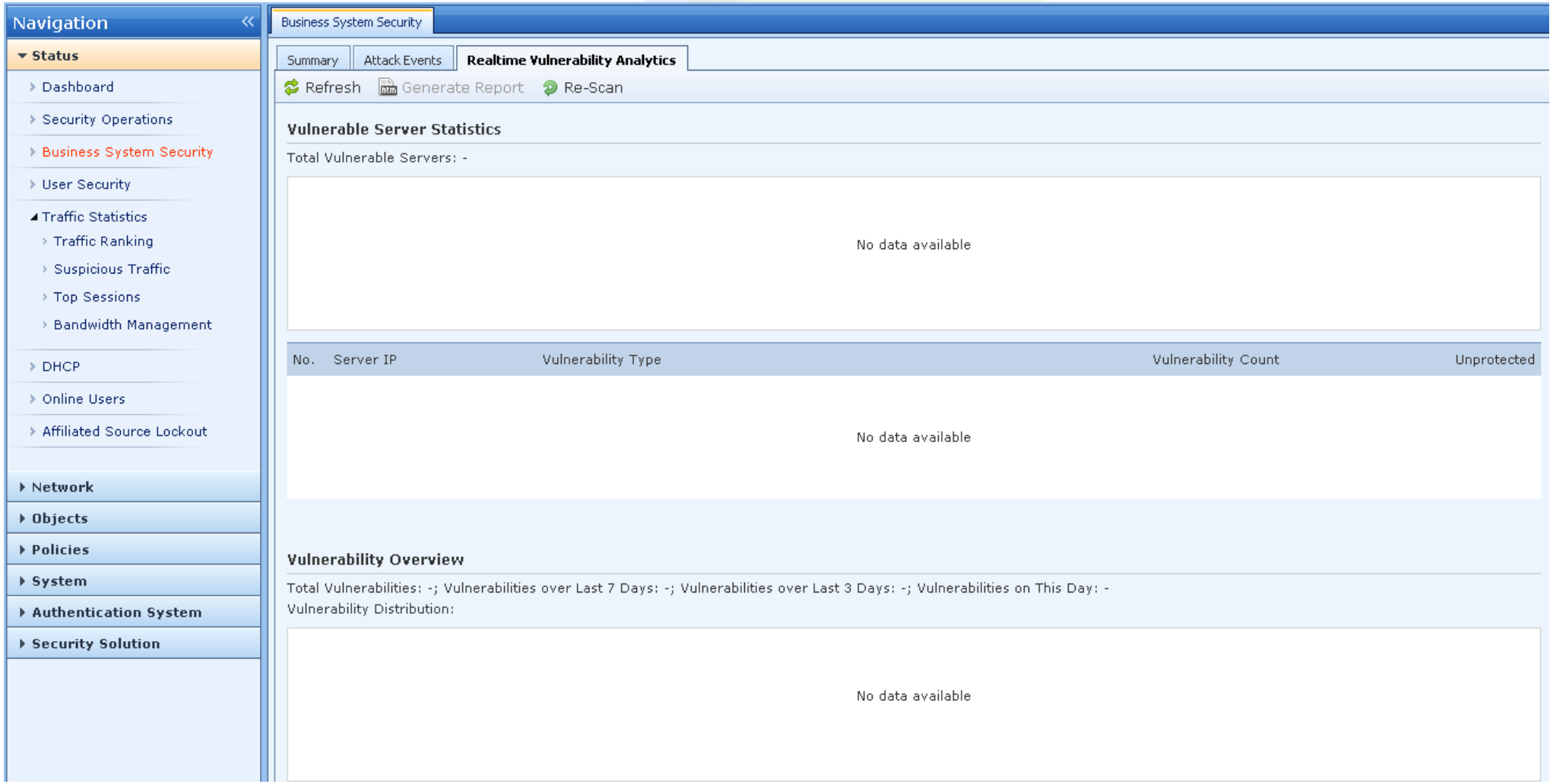
Analisis Kerentanan RT

Screenshot di bawah ini menunjukkan database Analisis Kerentanan RT



Analisis Kerentanan RT

Screenshot memperlihatkan contoh Laporan Analisis Kerentanan RT:



Analisis Kerentanan RT

Laporan Analisis Kerentanan RT

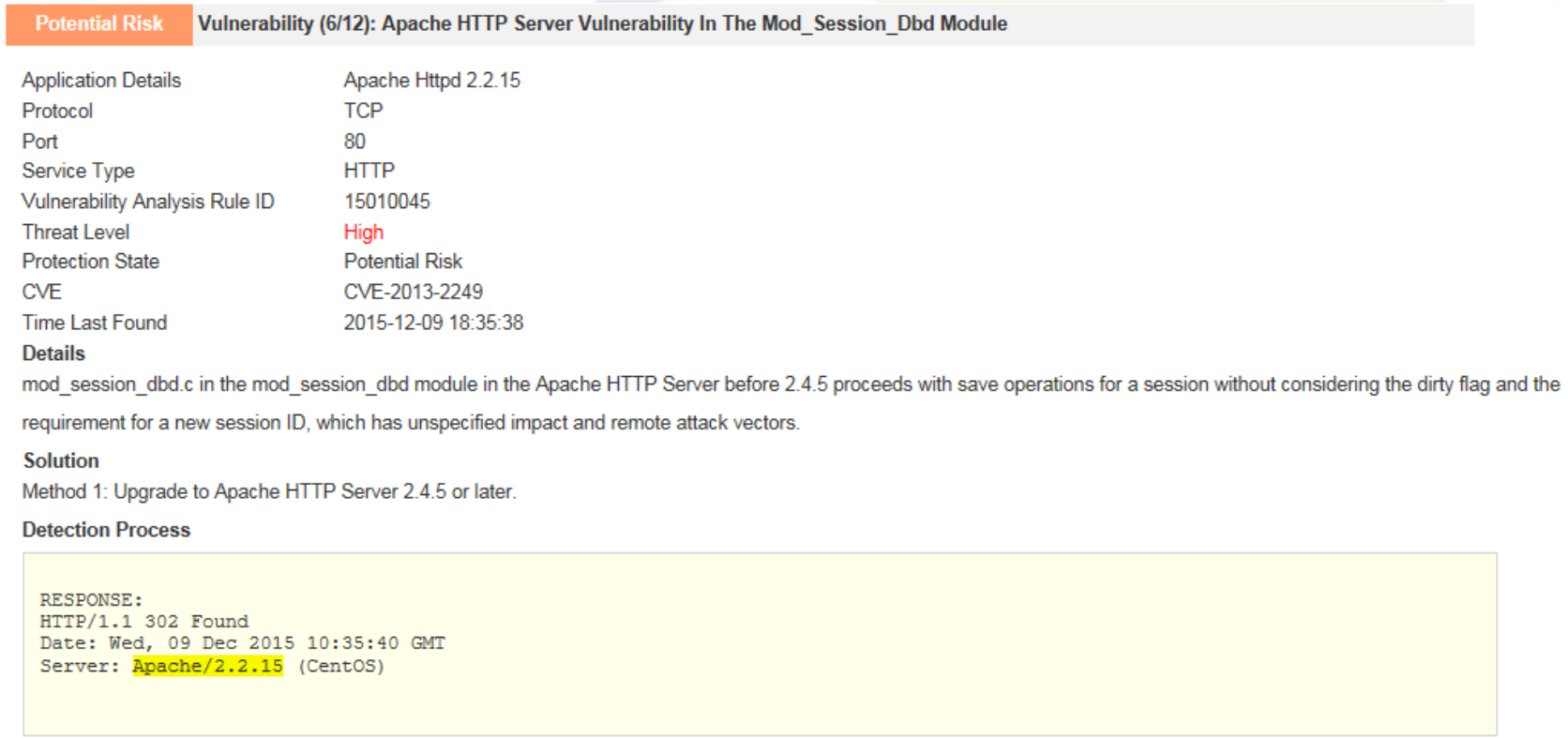
RT Vulnerability Analytics akan membandingkan konfigurasi IPS / WAF saat ini dan menunjukkan bahwa kerentanan telah dilindungi, atau potensi risiko yang terdeteksi AF sebagai tidak terlindungi.

No.	Vulnerability Type	Threat Level	Server Domain/IP	Total Vulnerabilities	Protection State
1	Wrong Configuration	Medium	192.200.19.200(69) 192.200.19.201(4) 192.200.19.231(1)	74	unprotected
2	Weak Password	High	192.200.19.200(32) 192.200.19.221(1) 192.200.19.199(1) 192.200.19.201(1) 192.200.19.220(1)	36	unprotected
3	Apache Httpd Vulnerability	High	192.200.19.200(16) 192.200.19.199(12)	28	unprotected
4	SQL Injection	High	192.200.19.200(15)	15	unprotected
5	Sendmail Vulnerability	High	192.200.19.200(12)	12	unprotected

Analisis Kerentanan RT

RT Vulnerability Analytics Report

Laporan akan memberikan rincian untuk setiap kerentanan yang terdeteksi, termasuk solusi dan proses deteksi. Laporan tidak termasuk kerentanan angka yang ditemukan. Hanya waktu terakhir ditemukan akan diperbarui.



Potential Risk **Vulnerability (6/12): Apache HTTP Server Vulnerability In The Mod_Session_Dbd Module**

Application Details	Apache Httpd 2.2.15
Protocol	TCP
Port	80
Service Type	HTTP
Vulnerability Analysis Rule ID	15010045
Threat Level	High
Protection State	Potential Risk
CVE	CVE-2013-2249
Time Last Found	2015-12-09 18:35:38

Details

mod_session_dbd.c in the mod_session_dbd module in the Apache HTTP Server before 2.4.5 proceeds with save operations for a session without considering the dirty flag and the requirement for a new session ID, which has unspecified impact and remote attack vectors.

Solution

Method 1: Upgrade to Apache HTTP Server 2.4.5 or later.

Detection Process

```
RESPONSE:
HTTP/1.1 302 Found
Date: Wed, 09 Dec 2015 10:35:40 GMT
Server: Apache/2.2.15 (CentOS)
```

Analisis Kerentanan RT

Catatan:

1. RT Vulnerability Scanner bergantung pada hasil identifikasi aplikasi. Oleh karena itu, disarankan untuk memiliki lisensi database identifikasi aplikasi yang valid.

2. RT Vulnerability Scanner hanya mendukung protokol TCP dan tidak mendukung analisis protokol UDP, seperti DNS dan layanan lainnya.

Identifikasi dukungan FTP dan HTTP untuk port apa pun namun layanan lain hanya mendukung port standar, seperti SSH, MySQL, dan layanan lainnya.

4. Setiap policy independen satu sama lain. Jika grup IP server tumpang tindih, kerentanan identik akan ditemukan berulang dalam daftar.

2. Peringatan Ancaman

SANGFOR
深信服科技

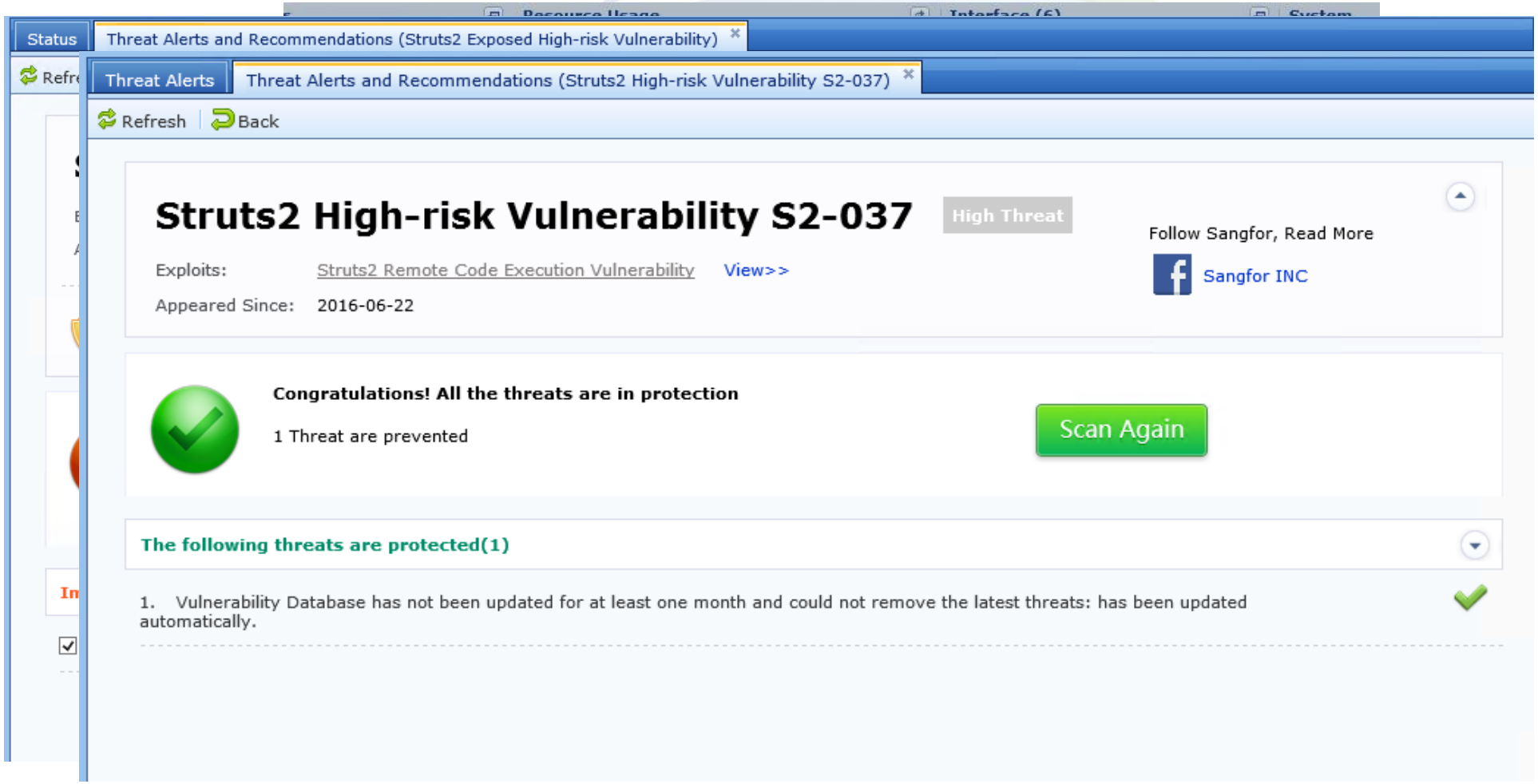
Threat Alerts

Peringatan Ancaman akan memberi tahu tentang peristiwa security yang mengkhawatirkan dalam setiap insiden security yang terjadi di industri dalam waktu 48 jam setelah wabah untuk memberikan deteksi kerentanan 0 Hari lengkap dan memberikan program proteksi yang memungkinkan pengguna untuk fokus pada bisnis mereka, tanpa mengenai ancaman dan kerentanan setiap saat. Pengguna juga dapat belajar tentang situasi security baru-baru ini melalui Threat Intelligence Center.

Peringatan Ancaman mencakup langkah-langkah berikut:

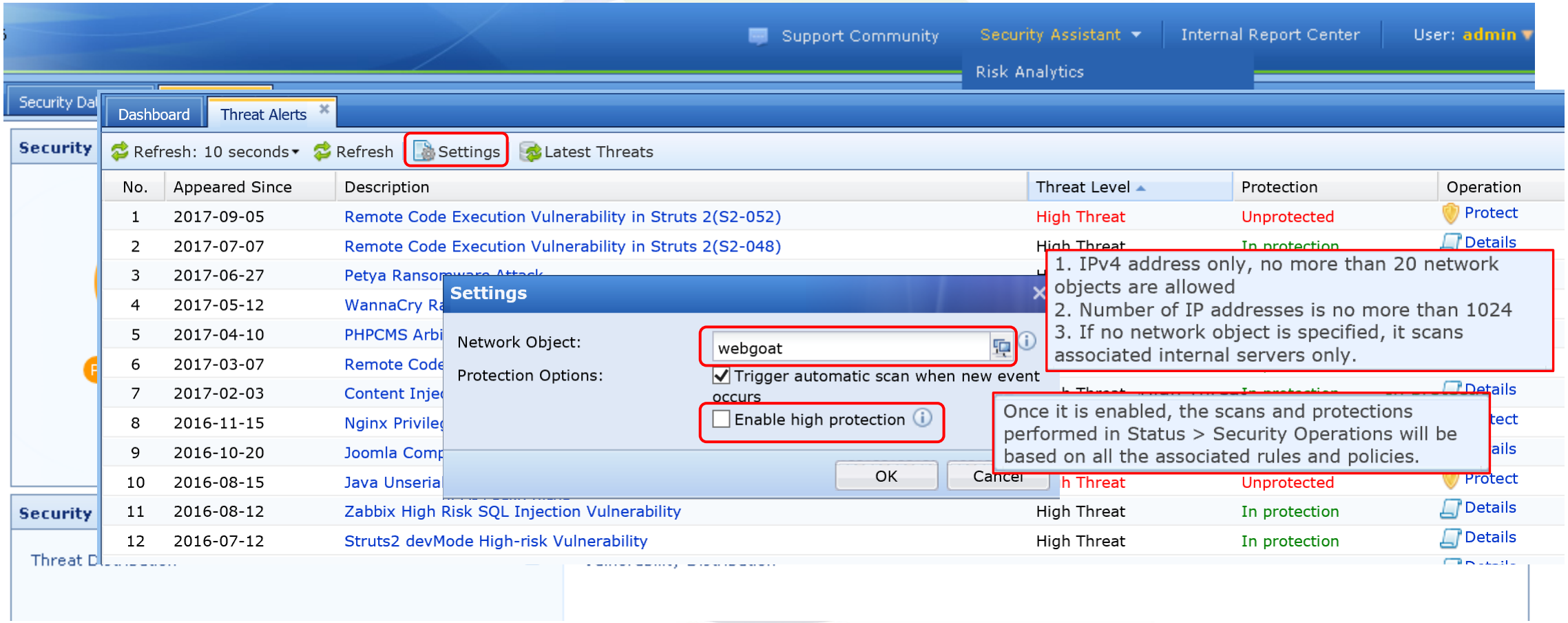
Threat Alerts

Ketika Sangfor mendeteksi peristiwa yang mengkhawatirkan, itu akan muncul informasi security dalam login pertama hari itu.



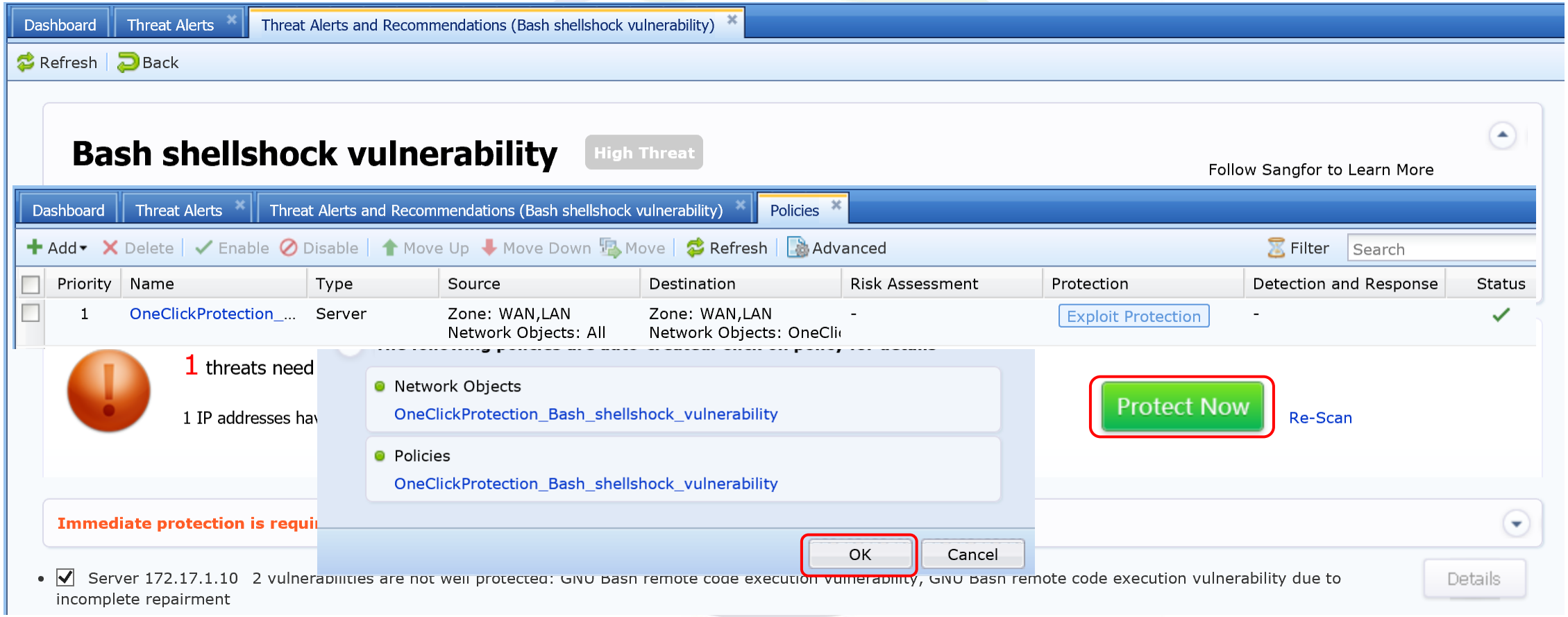
Threat Alerts

Pengaturan



Threat Alerts

Satu klik me-generate policy secara otomatis .



Threat Alerts

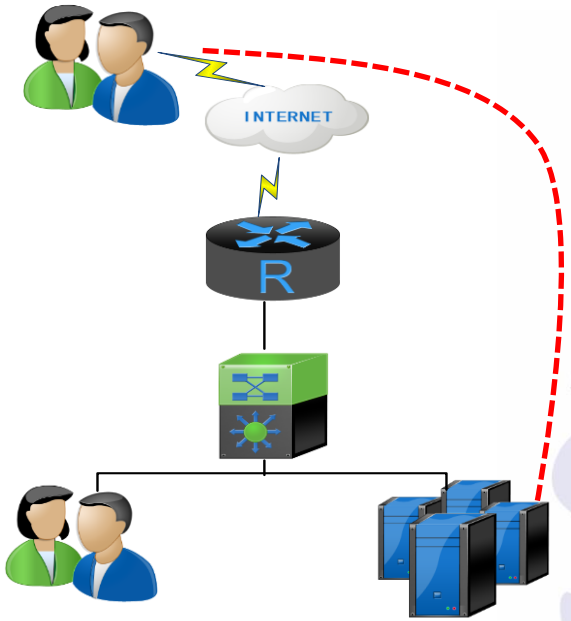
Catatan:

- Perangkat perlu mengakses jaringan secara normal untuk memperbarui peristiwa security.
- Pemindaian ancaman harus memastikan NGAF dapat dijangkau ke server intranet.
- Proteksi hotspot security event menghasilkan security policy dengan tindakan sebagai penolakan.
- Jika [Objek Jaringan] tidak dikonfigurasi, sistem akan memeriksa server yang ditemukan secara otomatis.

3. Risk Analytics

SANGFOR
深信服科技

Risk Analytics



Server mungkin memiliki masalah berikut:

(1) Port terbuka yang tidak perlu

(2) Kerentanan dari server itu sendiri (untuk sistem operasi server)

(3) Kerentanan dalam software server

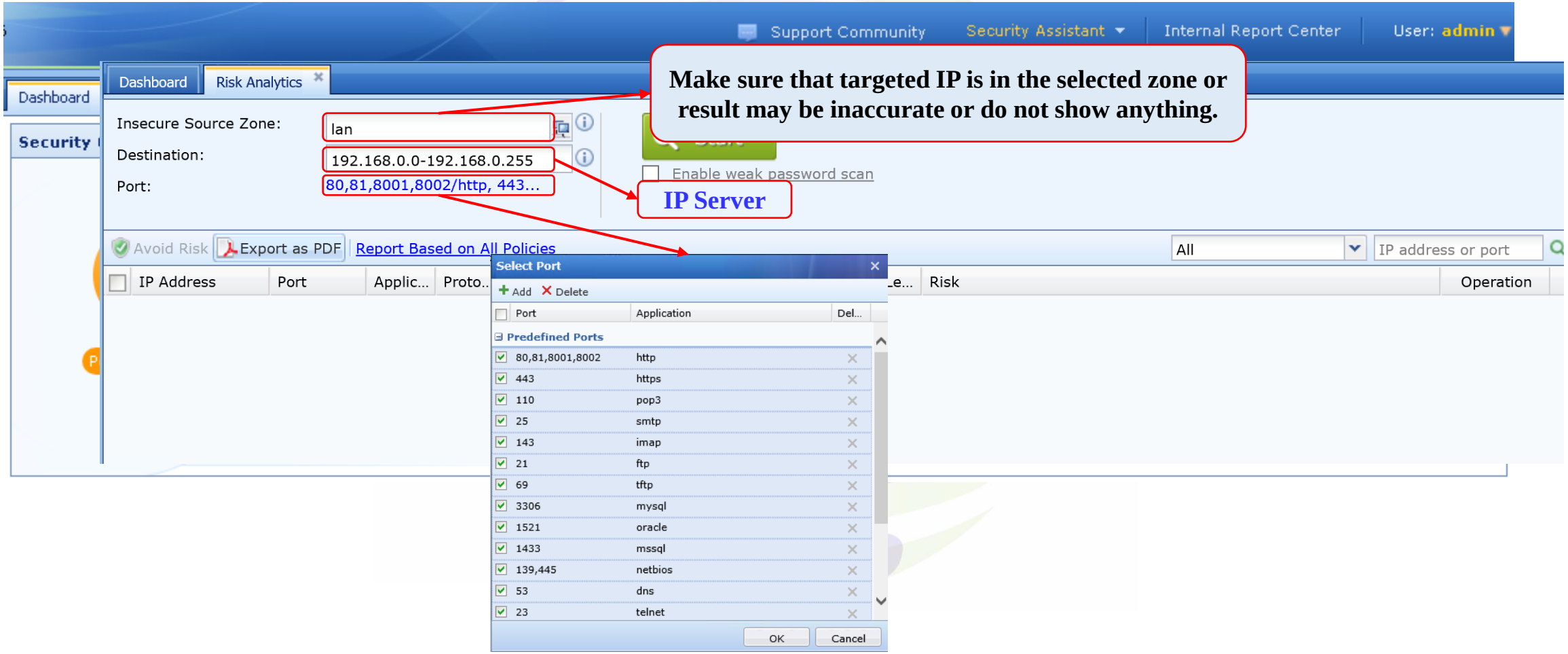
(4) Password lemah yang digunakan dalam login situs web

Analisis risiko mencakup dua aspek:

1. Port scan pada IP yang ditargetkan memungkinkan administrator server untuk memiliki pemahaman yang jelas tentang port terbuka server, layanan, dan kerentanan yang mungkin ada di server, yang memungkinkan administrator untuk menutup port terbuka yang tidak perlu, memblokir kerentanan parah dan meningkatkan security server.
2. Pemindaian password yang lemah pada situs yang ditargetkan digunakan untuk mengatasi ketidakamanan password yang lemah yang diterapkan sebelum akses ke database penting dan rahasia. Pada saat yang sama, analisis risiko dapat dilakukan secara cerdas untuk menghasilkan aturan yang sesuai berdasarkan hasil pemindaian bagi pelanggan untuk menjaga security perangkat.

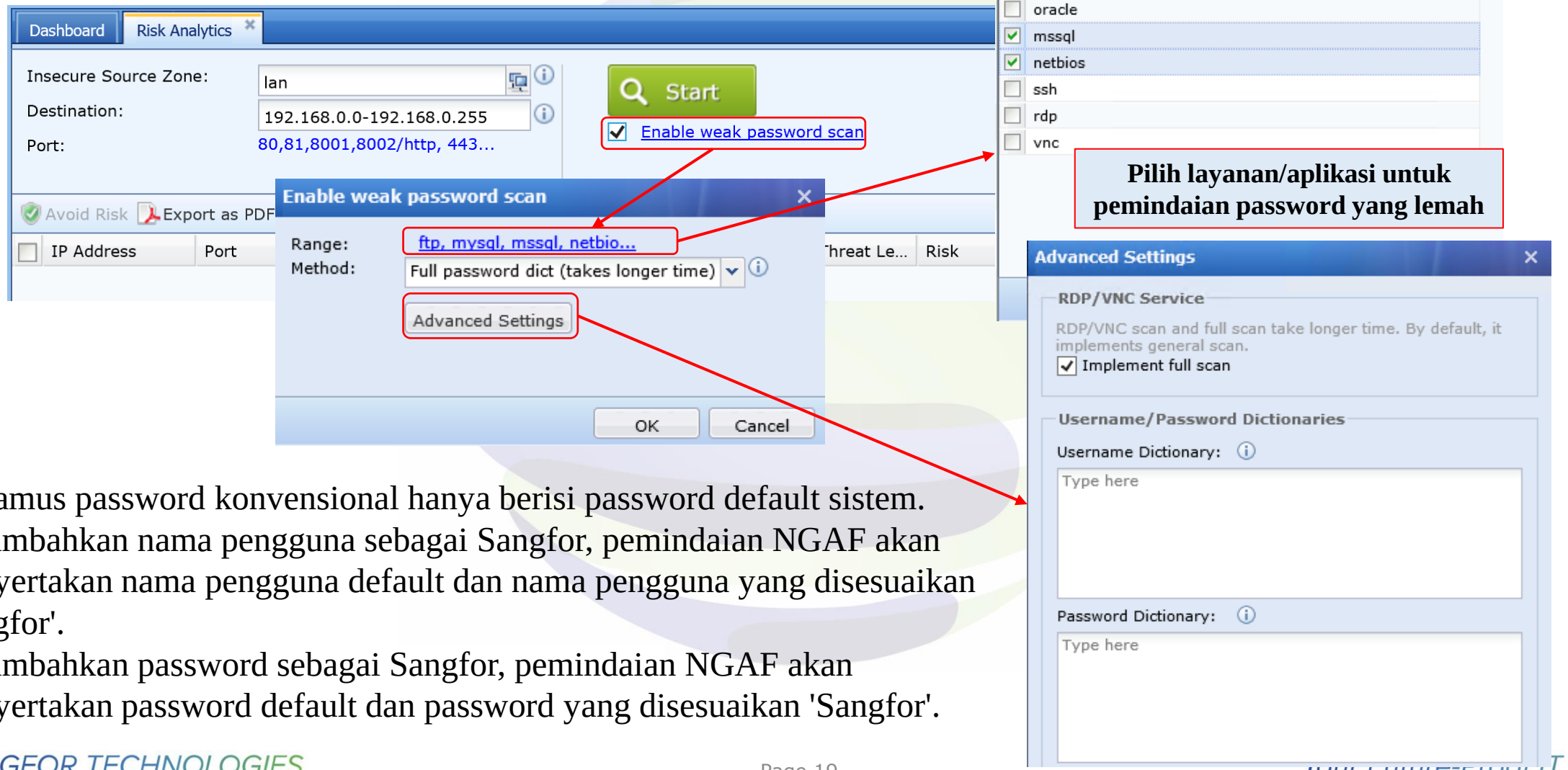
Risk Analytics

Menetapkan kondisi penilaian risiko.



Risk Analytics

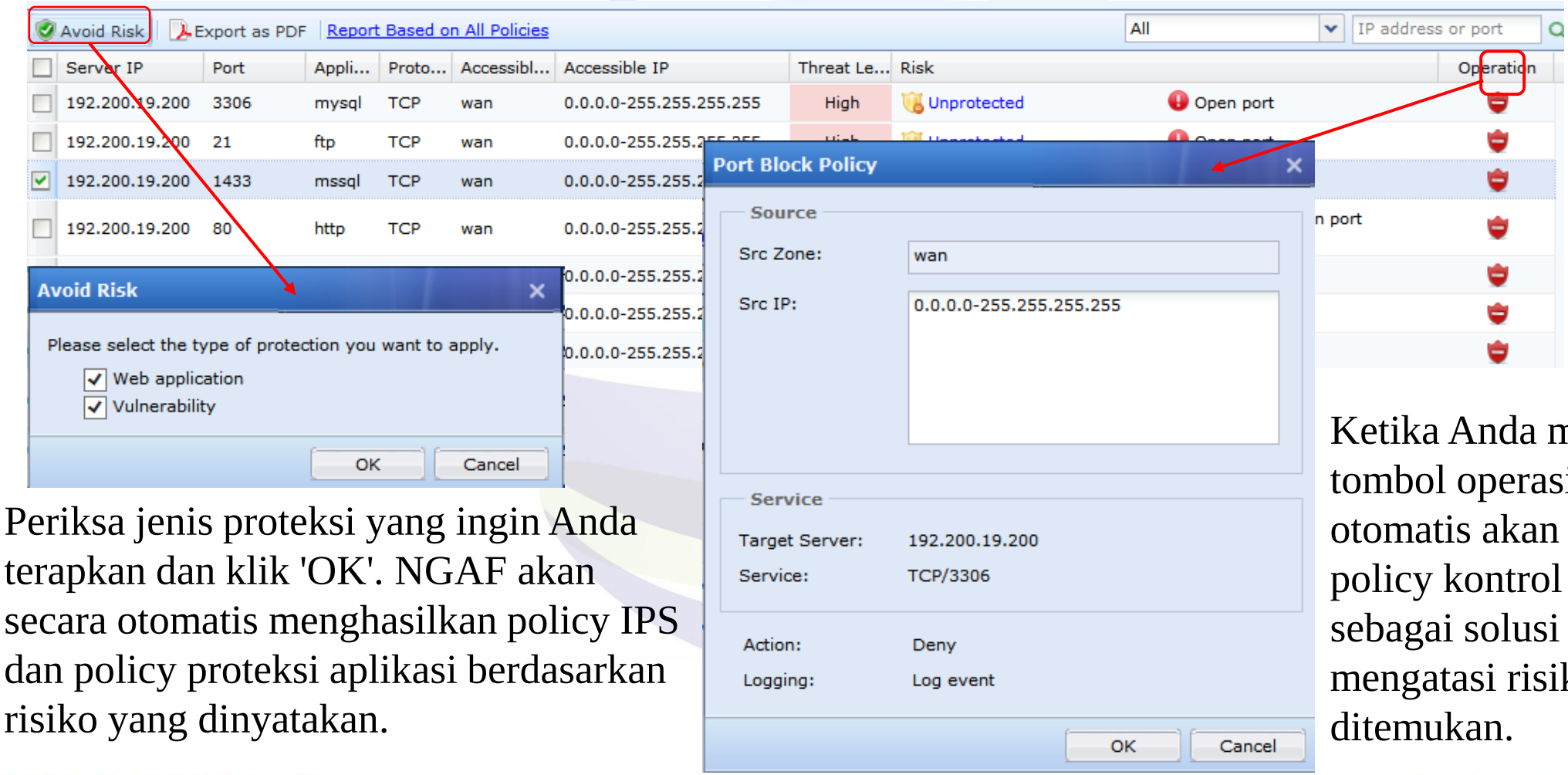
Weak password scan setting



1. Kamus password konvensional hanya berisi password default sistem.
2. Tambahkan nama pengguna sebagai Sangfor, pemindaian NGAF akan menyertakan nama pengguna default dan nama pengguna yang disesuaikan 'Sangfor'.
3. Tambahkan password sebagai Sangfor, pemindaian NGAF akan menyertakan password default dan password yang disesuaikan 'Sangfor'.

Risk Analytics

Atur pemindaian port dan pemindaian password yang lemah, klik mulai pindai, dan itu akan menunjukkan risiko di setiap server

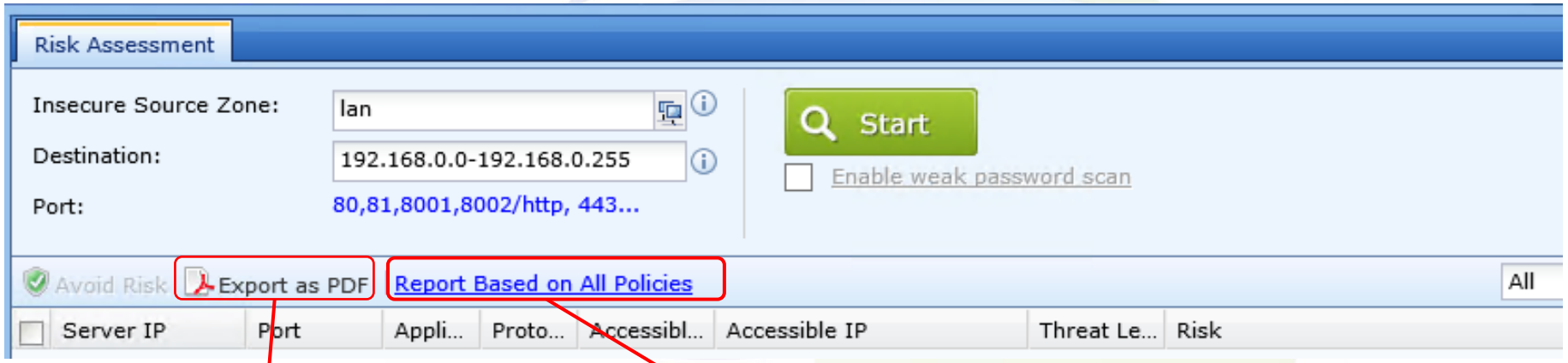


Periksa jenis proteksi yang ingin Anda terapkan dan klik 'OK'. NGAF akan secara otomatis menghasilkan policy IPS dan policy proteksi aplikasi berdasarkan risiko yang dinyatakan.

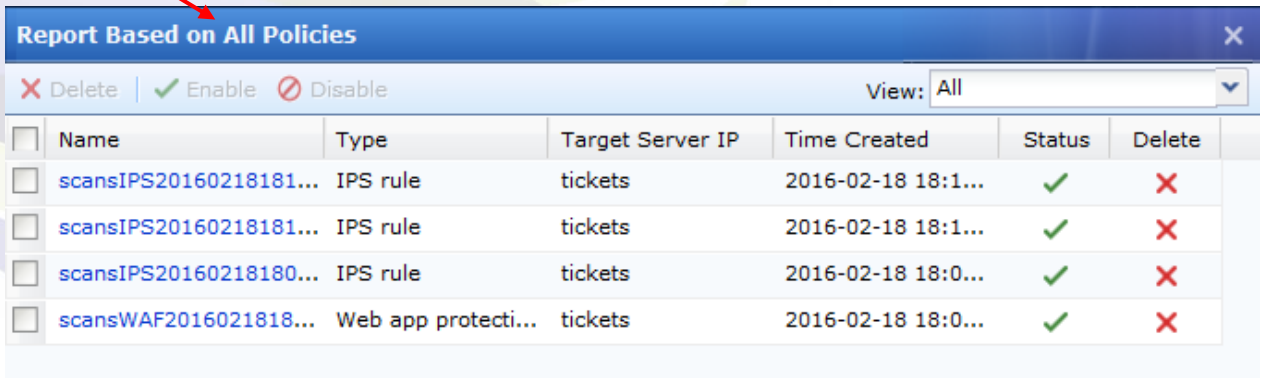
Ketika Anda mengklik tombol operasi, secara otomatis akan menghasilkan policy kontrol aplikasi deny sebagai solusi untuk mengatasi risiko yang ditemukan.

Risk Analytics

Ekspor laporan penilaian risiko, dan melihat aturan yang ditambahkan secara otomatis.



Menghasilkan laporan analisis pemindaian proaktif dalam format PDF



4. Web Scanner

SANGFOR
深信服科技

Web Scanner

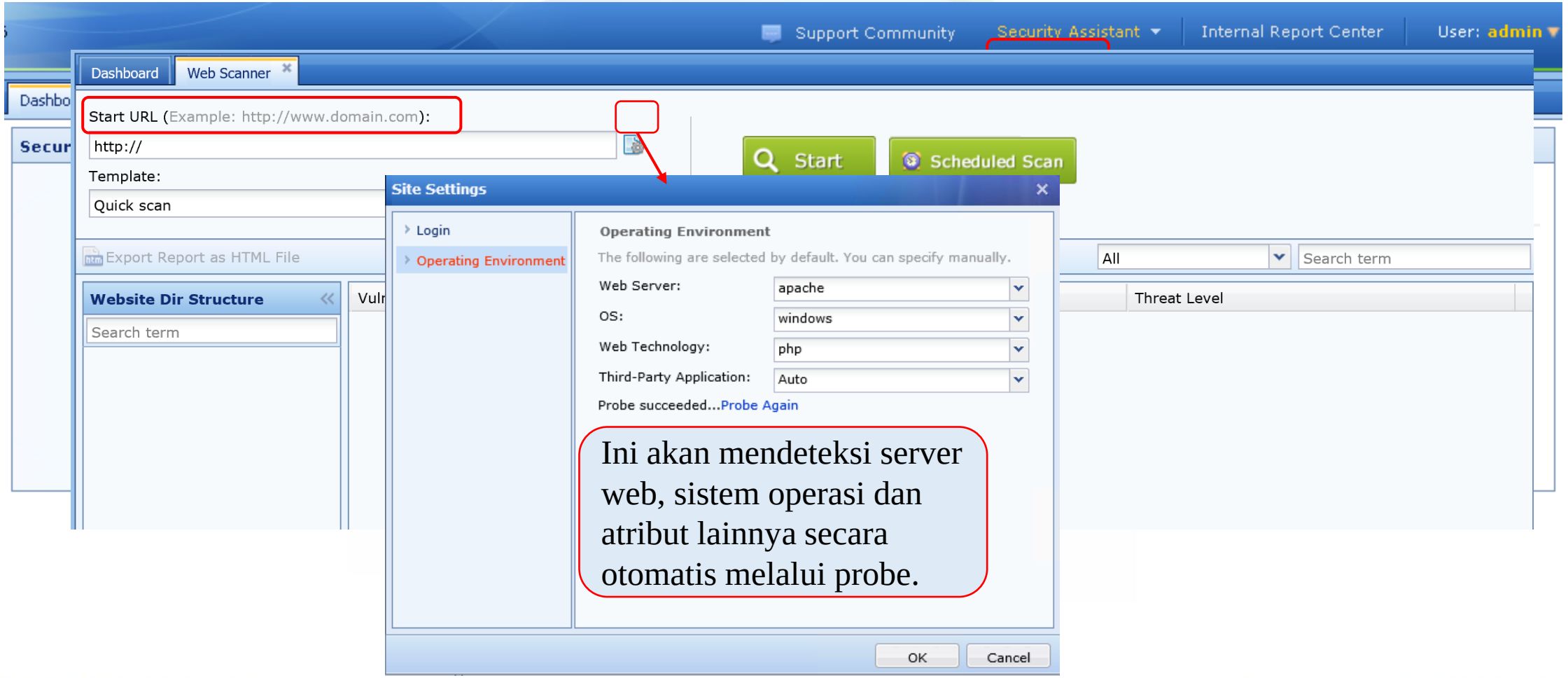
Pemindai web mendukung pemindaian kerentanan berikut:

Injeksi SQL, mengikat injeksi SQL, serangan scripting lintas situs (XSS), serangan skrip lintas situs yang disimpan, injeksi perintah OS, inklusi file lokal, inklusi file jarak jauh, serangan brute force, password lemah, pemalsuan permintaan lintas situs (CSRF), injeksi XPATH, injeksi LDAP, divisi respons, sisi server Termasuk (SSI), pengalihan yang tidak aman, konfigurasi DAV yang tidak aman, metode HTTP yang tidak aman, mengaktifkan WebDAV, memancing iframe, pelacakan lintas situs (XST), pengungkapan informasi phpinfo, konfigurasi PHP yang tidak aman, temukan daftar direktori, temukan direktori tersembunyi.

1. Penting untuk memberi tahu pengguna sebelum memindai: Pemindai Web memiliki risiko merusak data situs, oleh karena itu pemindaian tidak dapat dilakukan secara langsung di server web produksi. Klien harus menyediakan server cermin untuk memindai kerentanan.
2. Jika Anda memindai server produksi secara langsung, Anda perlu mendapatkan persetujuan dan tekanan pelanggan tentang kemungkinan risiko terhadap pelanggan, dan mencadangkan data situs dan kode sumber sebelum melakukan pemindaian untuk memastikan bahwa jika ada masalah, data dapat dipulihkan dari cadangan.

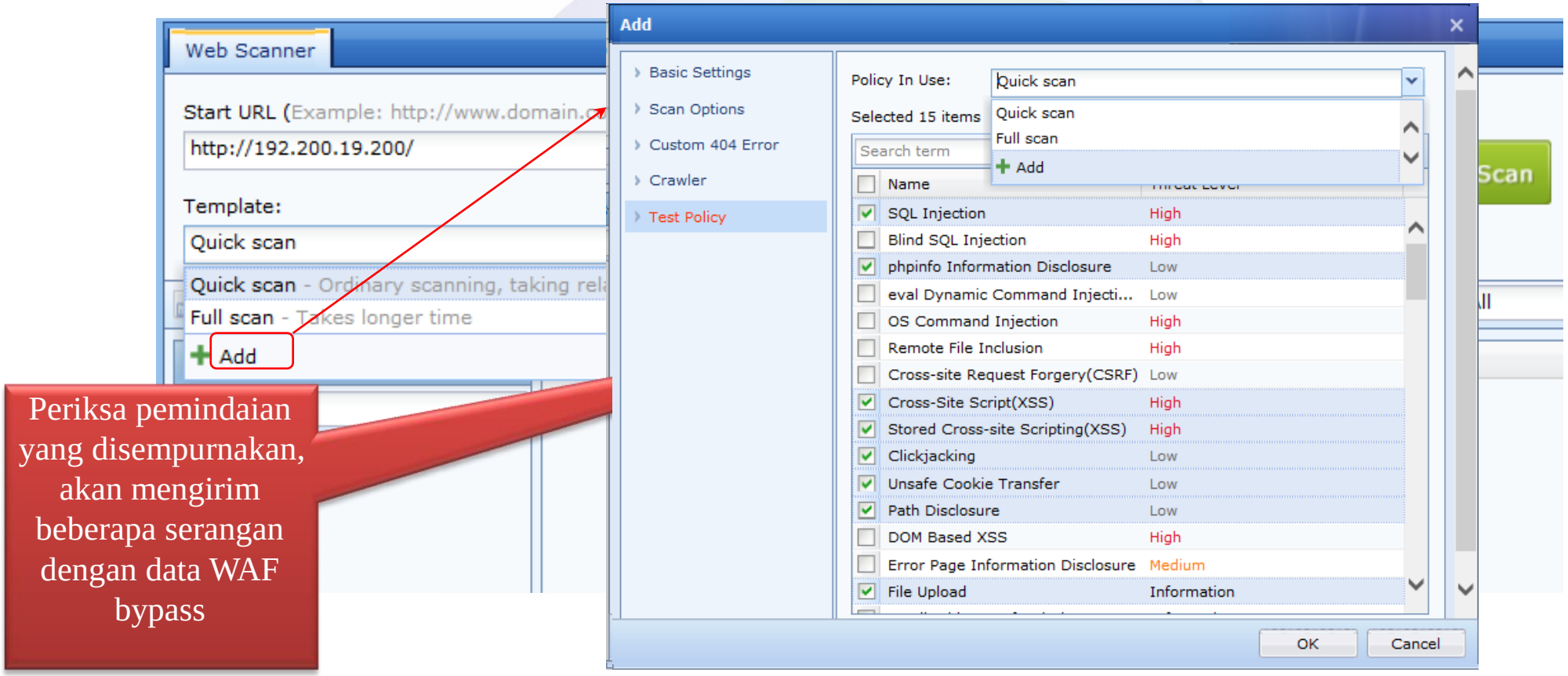
Web Scanner

Isi URL mulai serta templat pemindaian, klik ikon pena di sebelah kanan untuk memasukkan antarmuka pengeditan



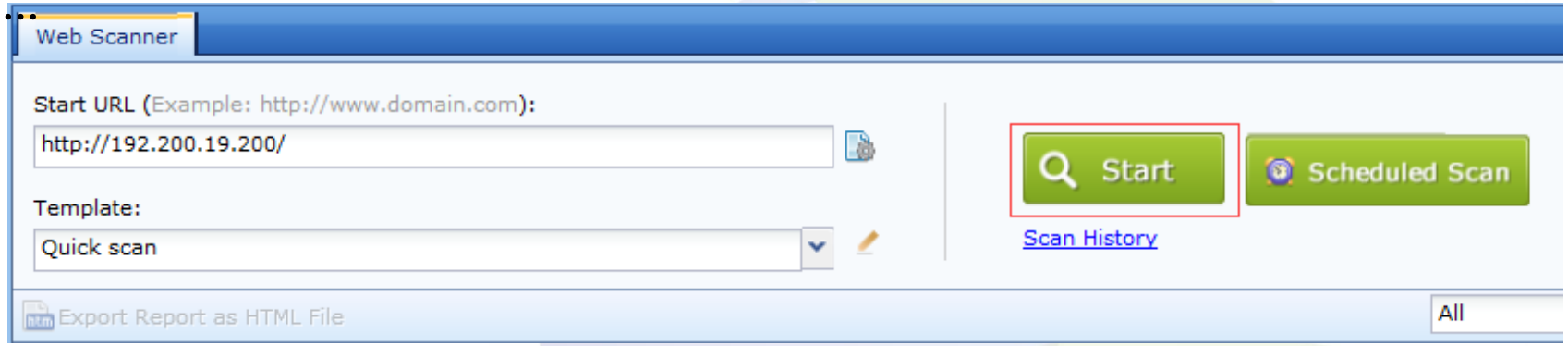
Web Scanner

Template pemindai web bawaan (pemindaian cepat dan pemindaian penuh) tidak dapat diubah. Anda perlu mengklik menu drop-down untuk menambahkan template seperti yang ditunjukkan pada tangkapan layar di bawah ini:

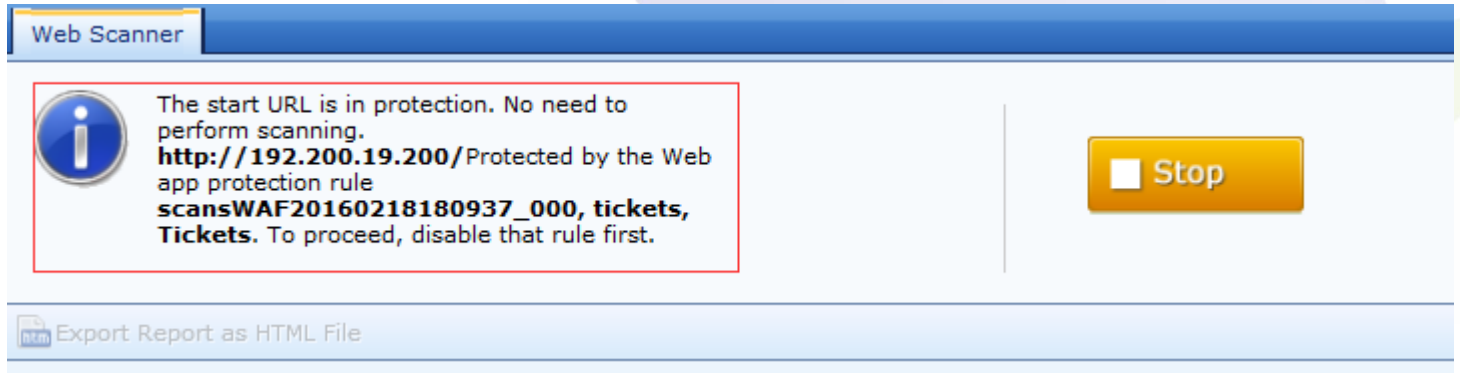


Web Scanner

Periksa pemindaian yang disempurnakan, akan mengirim beberapa serangan dengan data WAF bypass



•Catatan: Jika ada policy WAF untuk melindungi URL yang ditargetkan dan tindakan ditolak, itu akan mendorong "URL awal dalam proteksi. Tidak perlu melakukan pemindaian." Anda harus menonaktifkan atau mengubah tindakan policy WAF yang relevan untuk mengaktifkan pemindaian



Web Scanner

Setelah pemindaian selesai, Anda dapat melihat proses pemindaian, deskripsi, dan solusi kerentanan yang direkomendasikan.

Web Scanner

Setelah pemindaian selesai, Anda dapat mengekspor Laporan Kerentanan Web html.

Web Vulnerability Report

Start Time:2016-02-19 11:27:54

Scanning Duration:1 seconds

Target Site

Start URL:	http://192.200.19.200/
Web Server:	Apache/2.2.11 (Win32) PHP/5.2.8
OS:	windows
Web Language:	Unknown
Third-Party Application:	unknown 0
Login Method:	Not login
URLs Scanned:	0

Overview

Possible Threats:
- Intercept session, get user login credential to get access to site.

Solution(s):
1. Check validity of data on client-side and server-side, and filter special characters.
2. Deploy security appliance that is able to perform Web application protection.

No.	Page	Vulner
1	http://192.200.19.200/	

Vulnerability Content Details

Clickjacking (1)

Description:
Clickjacking is a malicious technique that attacker uses multiple transparent or opaque layers to trick a user into clicking on something different from what the user p

Solution:
Increase or set value of HTTP header option X-Frame-Options to DENY or SAMEORIGIN

Web Scanner

Catatan:

1. Jika ada policy WAF yang dibuat untuk melindungi URL yang ditargetkan dan tindakannya ditolak, itu akan mendorong "URL awal dalam proteksi. Tidak perlu melakukan pemindaian." Anda harus menonaktifkan atau mengubah tindakan policy WAF yang relevan untuk memindai.
2. Ketersediaan tinggi tidak menyinkronkan konfigurasi dalam pemindai web.
3. Untuk memiliki hasil yang lebih akurat pada pemindaian password yang lemah, pengguna harus masuk ke URL yang ditargetkan. Ini tidak melibatkan penyertaan kode otentikasi, dll.
4. Setelah pemindaian selesai, Anda dapat segera mengekspor laporan pemindaian dalam format PDF. Perangkat tidak akan menyimpan laporan. Laporan akan dihapus lagi setiap kali pemindaian baru dimulai.

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)