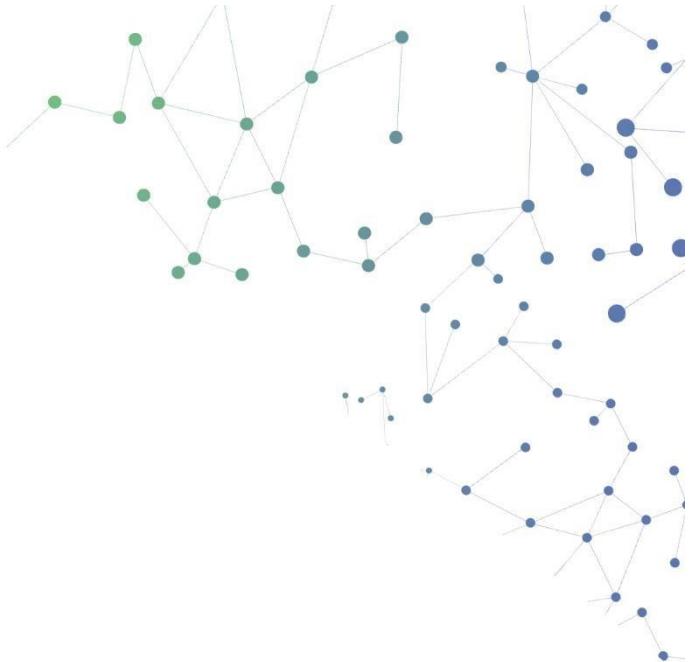


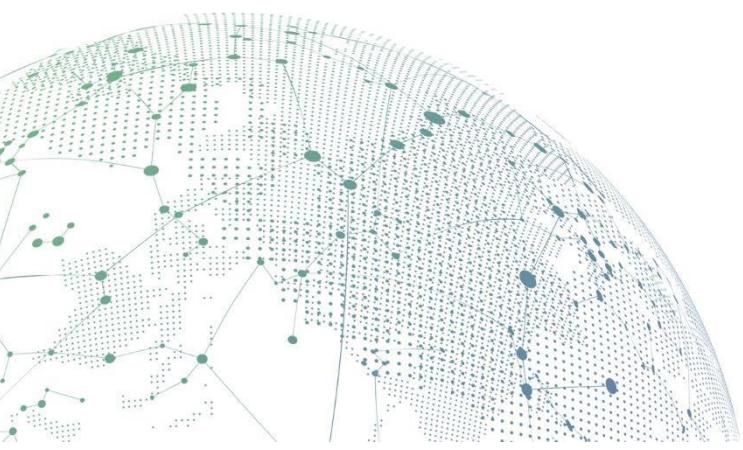


SANGFOR



Praktik Terbaik Keamanan Endpoint untuk Skenario Panduan Implementasi Kebijakan Keamanan Endpoi nt Secure untuk Server

Versi 3.2.22



Catatan Perubahan

Tanggal	Deskripsi Perubahan
16 Mar 2021	Dokumen diterbikan
17 Mei 2021	Dokumen diperbaharui

DAFTAR ISI

Bagian 1 Skenario	1
Bagian 2 Gambaran	1
Bagian 3 Mengidentifikasi Resiko Keamanan Sebuah Server	1
3.1 Pemeriksaan Keamanan & Integritas	1
3.1.1 Pemeriksaan Keamanan & Integritas	1
3.1.2 Mengatasi Kendala	1
3.2 Pemeriksaan Kerentanan System	3
3.2.1 Pemeriksaan Kerentanan	3
3.2.2 Mengatasi Kendala	3
3.3 Memindai Virus.....	4
3.3.1 Memindai Virus Virus	4
Bagian Panduan Implementasi Keamanan Server	4
4.1 Basic Policy.....	4
4.2 Anti Virus	4
4.3 Realtime Protection.....	5
4.4 Trust Files	7
4.5 Vulnerability Fix	7
4.6 Micro-Segmentation Policy	8
4.7 Alarm Policy	11

Bagian 1 Skenario

Bagian 2 Gambaran

Dokument ini sesuai dengan Endpoint Secure sebagai panduan untuk implementasi Endpoint Secure security policy dengan tujuan untuk melindungi keamanan server.

Dokumen ini terdiri dari dua bagian:

Mengidentifikasi resiko keamanan server dan mengimplementasikan security policy pada server. Mengidentifikasikan resiko keamanan server dapat memandu pengguna bagaimana cara mengidentifikasi resiko keamanan klien lebih awal, membuat pengguna mewaspadai resiko keamanan server dan dampaknya terhadap server, dan memandu pengguna untuk menangani resiko keamanan saat mengimplementasikan keamanan server. Security policy nya merujuk kepada policy mana yang seharusnya diatur oleh Endpoint Secure dan bagaimana untuk mengatur security untuk memastikan keamanan dari server.

Bagian 3 Mengidentifikasi Resiko Keamanan Server

Mengidentifikasi resiko keamanan pada server merupakan cara untuk memandu pengguna untuk mengidentifikasikan resiko keamanan klien lebih awal, membuat pengguna menyadari resiko keamanan dan dampaknya terhadap server, dan memandu pengguna untuk menangani resiko keamanan. Bagian ini dapat memandu pengguna untuk mengidentifikasikan resiko keamanan lebih awal dan cara untuk menangani nya dengan tiga cara: pemeriksaan awal, pemeriksaan kerentanan, dan penghapusan virus. Ingat jika semakin banyak server, direkomendasikan untuk memilih 1 atau 2 server untuk memandu pengguna bagaimana cara mengidentifikasi resiko keamanan dan bagaimana cara untuk menangani mereka.

3.1 Pemeriksaan Keamanan & Integritas

Pemeriksaan keamanan & Integritas adalah proses pemeriksaan yang wajib untuk sistem windows dan linux sesuai dengan persyaratan keamanan yang diwajibkan, untuk membantu menemukan terminal yang tidak sesuai dan item yang tidak sesuai di intranet, dan memberikan saran perbaikan.

3.1.1 Pemeriksaan Keamanan & Integritas

Pergilah ke Detection-> Security & Integrity Check, Lakukan pemeriksaan dasar pada server.

The screenshot shows the Sangfor Endpoint Secure software interface. The top navigation bar includes 'Home', 'Endpoints', 'Micro-Segmentation', 'Detection' (which is highlighted in red), 'Response', 'Logs', and 'System'. On the far right, there are user icons for 'admin' and other users. The main content area has a red header with the text 'away from the previous check' and '1 endpoint(s) failed to pass the check'. Below this, a large button says 'Start Now'. At the bottom, there is a table with the following data:

No.	Endpoint	IP Address	Group	OS	Last Scanned	Task Status	Result
1	Windows2	20.10.0.8	Ungrouped Endpoints	Windows 7 Ultimate Servic...	2024-02-27 15:11:44	Check completed.	Failed
2	Server1	20.10.0.10	Ungrouped Endpoints	Windows Server 2012 R2 St...	2021-03-15 16:08:00	Task was sent.	-
3	Windows1	20.10.0.3	Ungrouped Endpoints	Windows 7 Ultimate Servic...	2020-11-23 15:02:14	Check completed.	Failed
4	DESKTOP-EIOOA94	192.168.1.3	Ungrouped Endpoints	Windows 10 Pro x64	2020-08-28 15:56:13	Check completed.	Failed

3.1.2 Menangani Ketidaksesuaian

Memperkuat item yang tidak sesuai pada pemeriksaan keamanan sistem menghasilkan menurut dokumen pengaturan keamanan disediakan oleh Endpoint Secure, seperti ditunjukan figur berikut:

The screenshot shows a summary of security requirements. 18 out of 31 requirements are not met. Key sections include:

- Account policy:**
 - 1.Password**: Minimum password length: >= 8 characters (red), Minimum password age: >= 2 days (red), Maximum password age: <= 90 days (green), Password history remembered: >= 5 (green).
 - 2.Account**: Account lockout counter: >= 15 minutes (green), Account lockout duration: >= 15 minutes (green), Account lockout threshold: <= 10 (red).
 - 3.Auto-login**: Auto-Login account (green).
- Application control policy:**
 - 1.Local user accounts**: Accounts without passwords (green), Accounts with weak passwords (green), Guest accounts (green).

The screenshot shows the Control Panel interface. The steps to open Local Security Policy are outlined:

- Open Control Panel and click Administrative Tools > Local Security Policy

The Control Panel window shows:

- Left sidebar: Account Policy, Password, Account Lockout Policy, Auto-login, Access Control Policy, Security Audit Policy, History Information Protection, Intrusion Prevention, Malicious Code Prevention.
- Right pane: **Password** section with requirements: Minimum password length: >= 8 characters, Minimum password age: >= 2 days, Maximum password age: <= 90 days, Password history remembered: >= 5.
- Bottom section: **Security Enhancement - Steps:**
- File list at the bottom: Local Security Policy (selected, highlighted in red), Component Services, Computer Management, Data Sources (ODBC), Event Viewer, Performance Monitor, Print Management, Services.

Pemeriksaan Kerentanan Sistem

Menolong pengguna mengidentifikasi kerentanan resiko tinggi di server dan menyediakan saran perbaikan.

3.1.3 Pemeriksaan Kerentanan

Pergilah ke Detection-> Vulnerability Scan path, Check servers for vulnerabilities.

The screenshot shows the Sangfor Endpoint Secure interface under the 'Detection' tab. In the 'Scan Task' section, there are two entries: 'Sending task...' (Completed, 03-15 16:10) and 'Completed' (Completed, 03-02 11:33). The table below lists endpoints: No. 1, Task Status Completed, Endpoint Status Online, Endpoint Server1, Group Ungrouped Endpoints, IP Address 20.10.0.10, OS Windows Server 2012 ...

3.1.4 Menangani Ketidaksesuaian

Memperbaiki kerentanan yang belum diperbaiki pada hasil pemeriksaan, seperti ditunjukkan

The screenshot shows the 'Patch' tab for 'Server1'. A red box highlights the 'Patch' button. The table lists 141 entries of vulnerabilities, with the first six highlighted as High severity. The columns include No., Severity, Patch Type, Patch Name, Patch ID, Date Released, and Status. A 'Patch' button is visible at the bottom right of the table.

dibawah:

Perlu diketahui setelah mengklik "Patch", direkomendasikan tidak mencentang "Force endpoint to restart after this operation" untuk pengingkatan hanya dapat mendapatkan efek setelah merestart komputer, seperti ditunjukkan dibawah:

The screenshot shows a confirmation dialog box titled 'Confirm'. It asks if the user is sure they want to patch the 10 selected vulnerabilities. It notes that this operation is applicable to unpatched vulnerabilities and that 2 Vulnerability vulnerability patches will take effect after endpoint restarts. There is a checkbox for 'Force endpoint to restart after this operation'. The 'OK' button is highlighted.

3.2 Memindai Virus

Lakukan investigasi penuh pada server, temukan dan tangani file ancaman lebih awal.

3.2.1 Memindai Virus

Organisasi atau departemen dengan lingkungan bisnis yang sama akan mempromosikan implementasi menjadi beberapa ide berikut.

Temukan test komputer: Temukan komputer dalam lingkungan bisnis yang sama untuk diinstall Endpoint Secure client test untuk percobaan . Sebuah percobaan Analisa dan hasilnya : Analisa file ancaman yang ditemukan oleh komputer test. Jika ditemukan

kesalahan penilaian, tambahkan ke witelist.

Jika yakin bahwa itu bukan salah penilaian, hubungi Sangfor Engineer untuk mengurusnya.

Memastikan kemampuan bisnis. Pastikan dan coba komputer bisnis untuk memastikan bisnis dapat digunakan secara normal.

Lakukan instalasi di komputer lainnya: komputer test dipastikan dan bisnis tidak terpengaruh, lalu itu akan dilakukan ke komputer lain di lingkungan yang sama untuk menginstall dan membuang ancaman.

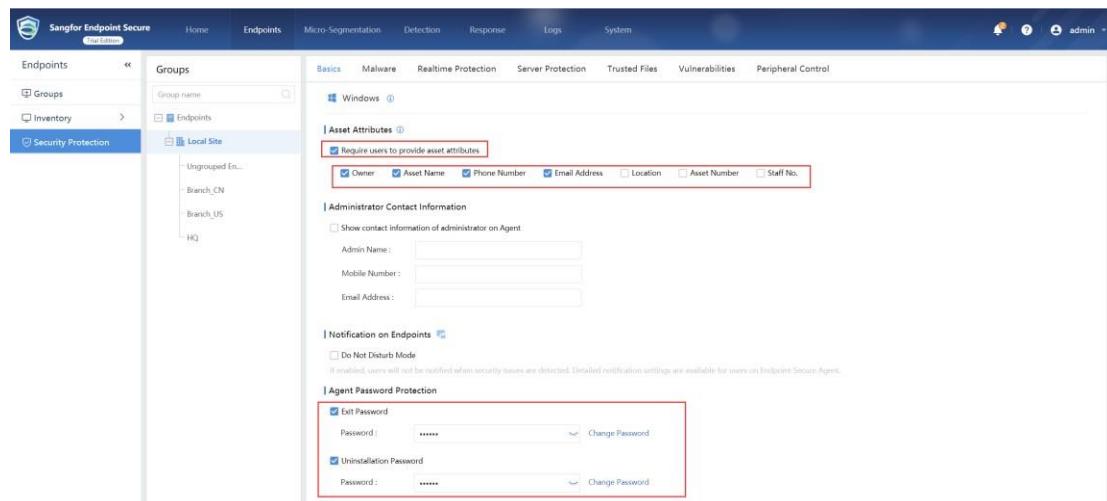
9

Bagian 4 Panduan Implementasi Keamanan Server

Implementasi policy keamanan server merujuk kepada policy mana yang harus dikonfigurasi oleh Endpoint Secure dan bagaimana mengatur policy keamanan dalam rangka menjamin kelanjutan keamanan klien. Policy keamanan server dikonfigurasi dari basic policy, virus detection and killing policy, real-time protection policy, trust list, vulnerability detection dan repair detection, dan alarm policy untuk melindungi keamanan server.

4.1 Basic Policy

Pergi ke Endpoints->Security Protection path, konfigurasi basic policy dari group dimana server berada, mengaktifkan asset information registration, dan set the terminal Exit Password/Uninstallation, seperti figur dibawah ini:



4.2 Anti-Virus

Pergi ke Endpoints->Security Protection path, konfigurasi virus detection dan killing policy pada group dimana server ditempatkan, seperti figur berikut:

The screenshot shows the Sangfor Endpoint Secure interface under the 'Endpoints' tab. In the left sidebar, 'Security Protection' is selected. On the right, the 'Virus Scan' section is active. Under 'Scheduled Scan', the 'Enable scheduled scanning' checkbox is checked. The schedule is set to 'Every day' at 00:00. Task types include 'Quick Scan' and 'High CPU'. Below this, 'Virus Scan' settings show 'Scan Options' like 'Skip files larger than 50 MB' and 'Scan compressed files up to 3 layers deep'. The 'Action' section has 'Standard' selected. Under 'Engine', 'Sangfor Engine Zero' is checked, while 'Gene Analytic Engine', 'Behavioral Analytic Engine', and 'Cloud Based Engine' are unchecked.

[Pemindaian Terjadwal] Aktifkan pemindaian umum otomatis. Direkomendasikan waktu untuk pemeriksaan sebulan sekali, tipe pemindaian adalah quick scanning, dan mode pemindaian adalah balanced.

[Aksi] Simpan konfigurasi default; aksi yang direkomendasikan setelah file ancaman ditemukan adalah "Standard"; Jika mesin pemindai dinyalakan sepenuhnya, itu akan menyerap sumber yang tinggi. Jika CPU dan Memori klien dikonfigurasi dengan 4 cores dan 8GB atau lebih, itu dapat dinyalakan sepenuhnya. Jika anda mengikuti konfigurasi disini, direkomendasikan untuk membuka gene feature engine daripada behaviour analysis engine.

4.3 Realtime Protection

Pergi ke Endpoints->Security Protection path, konfigurasi real-time protection policy dari group dimana server berada, termasuk real-time file monitoring, ransomware protection and

The screenshot shows the Sangfor Endpoint Secure interface under the 'Endpoints' tab. In the left sidebar, 'Security Protection' is selected. On the right, the 'Realtime Protection' section is active. It includes four main detection modules: 'WebShell Detection', 'Brute-Force Attack Detection', 'SMB brute-force attack detection', and 'Ransomware Protection'. Each module has its own configuration options. For example, 'WebShell Detection' has a 'Type' section with 'Realtime' and 'Scheduled' options, and an 'Action' section with 'Fix' or 'No Action - Report Only'. Similar configurations are shown for the other three modules.

advanced threat protection, seperti ditunjukkan oleh figur dibawah, atur real-time protection policy.

The screenshot shows the Sangfor Endpoint Secure interface under the 'Realtime Protection' tab for a group named 'Local Site'. The 'Fileless Attack Protection' section is highlighted with a red box. It contains a checkbox for 'Enable suspicious PowerShell script detection' which is checked, and two action options: 'Block script execution' (radio button) and 'No Action - Alert Only' (radio button).

[Realtime File System Protection] Aktifkan small lock icon pada bagian kanan, dan file real-time protection policy akan diterbitkan oleh MGR ke ES agent.

[Protection Level] Direkomendasikan untuk melakukan konfigurasi pada protection level sebagai "Medium"; [File Type] Direkomendasikan untuk memilih semua tipe;

[Scan Options] Direkomendasikan untuk menyimpan konfigurasi default untuk pemindaian file; [Engine] Jika engine pemindaian telah sepenuhnya menyala, itu akan menggunakan sumber tenaga yang besar. Jika CPU dan Memory server telah dikonfigurasi dengan 4 core dan 8GB atau lebih, itu dapat sepenuhnya dinyalakan. Jika konfigurasinya dibawah itu, direkomendasikan untuk menyalakan gene feature engine dibandingkan Sangfor Zero artificial intelligence engine. .

[Action] Aksi default setelah menemukan file yang mencurigakan adalah direkomendasikan untuk di set ke "standard disposal"

[Ransomware Protection] Aktifkan small lock icon pada bagian kanan, dan ransomware protection policy akan dikirimkan dari management terminal ke ES agent.

[Action] Telah ditemukan bahwa rekomendasi konfigurasi untuk ransomware behavior adalah "Fix".

[Fileless Attack Protection] Mengaktifkan small lock icon pada bagian kanan, dan advanced threat protection policy akan diterbitkan dari management end ke ES agent, dan centang "Enable suspicious PowerShell script detection".

[Action] Ketika powershell script yang mencurigakan ditemukan untuk dijalankan, direkomendasikan untuk di set menjadi "Block script execution".

Set Linux server real-time protection policy. Linux server real-time protection policy hanya memiliki webshell detection dan brute force cracking detection, seperti ditunjukkan figur dibawah.

The screenshot shows the Sangfor Endpoint Secure interface under the 'Endpoints' tab. In the left sidebar, 'Security Protection' is selected. On the right, the 'Groups' section is open, showing a group named 'Local Site'. Under 'Basics', the 'Linux' tab is selected. The 'WebShell Detection' section has 'Enable WebShell detection' checked and is set to 'Scheduled' with a frequency of 'Every day' at '00:00'. The 'Brute-Force Attack Detection' section has 'Enable SSH brute-force attack detection' checked, triggered by 'Over 15 login attempts per minute', and the action is set to 'Block for 30 mins'. Buttons for 'Save', 'Restore Defaults', and 'Apply to Subgroups' are at the bottom.

4.4 Trust Files

Pergilah ke Endpoints->Security Protection path, Konfigurasikan whitelist policy pada group dimana server berada, dan tambahkan file dan direktori dimana tidak membutuhkan antivirus dan real-time protection untuk trust list (semacam file business system), seperti ditunjukkan figur berikut:

The screenshot shows the Sangfor Endpoint Secure interface under the 'Endpoints' tab. In the left sidebar, 'Security Protection' is selected. On the right, the 'Groups' section is open, showing a group named 'Windows'. Under 'Basics', the 'Windows' tab is selected. The 'Trusted Files' section contains a 'File/Path Whitelist' input field where 'c:\Program File\Sangfor' is listed. Below it, the 'Excluded IP Addresses from Brute-Force Attack Detection' section is empty. Buttons for 'Save', 'Restore Defaults', and 'Apply to Subgroups' are at the bottom.

4.5 Vulnerability Fix

Pergilah ke Endpoints->Security Protection path, konfigurasikan vulnerability repair policy pada group dimana server berada, seperti ditunjukkan figur berikut:

The screenshot shows the Sangfor Endpoint Secure interface under the 'Endpoints' tab. In the left sidebar, 'Security Protection' is selected. On the right, the 'Groups' section is open, showing a group named 'Windows'. Under 'Basics', the 'Windows' tab is selected. The 'Scheduled Vulnerability Scan' section has 'Enable scheduled scanning' checked and is set to run 'Every week' on 'Tue' at '00:00' to '03:00'. The 'Action' section has 'No Action - Report Only' selected. The 'Security Patch Downloading Server' section lists servers with their status: 'http://download.windowsupdate.com...' and 'https://upd.sangfor.com.cn/v1/do...' both have 'Up' status. A note at the bottom says 'When security patch is not available on internal server, allow Endpoint Secure Manager to download patch files from above servers. Setting->'.

[Scheduled Vulnerability Scan] Mengaktifkan regular automatic scanning.

[Action] Direkomendasikan untuk mengatur vulnerability scan result menjadi "No Action-Report Only", network administrator akan memperbaiki itu berdasarkan situasi yang sebenarnya.

4.6 Micro-Segmentation Policy

- Micro-isolation adalah dasar dari five-tuples untuk mengontrol inbound dan outbound trafik dari server untuk mencapai tujuan dari melindungi keamanan server. Direkomendasikan bahwa port yang diperlukan dapat dilepaskan dari micro-isolation policy, dan non-essential high-risk ports dapat dilarang untuk meningkatkan keamanan. Konfigurasi sebagai berikut berdasarkan kebutuhan pelanggan, berikut urutan hubungan akses antar pelanggan bisnis, system/IP/role/service dan setiap objek dan persiapan and setiap objek, Dan persiapan dari mengikuti micro-isolation policy, seperti ditunjukkan tabel berikut ini;

Objects	Business System	Business System Name	Endpoint Group	Included Endpoints	
		OA Server	Server Group	OA_WEB	
		Database Server	Server Group	Database Server	
	IP Group	IP Group	IP Range	IP Group Type	
		Office Endpoint	172.16.200.1-172.16.200.254	LAN	
	Services	Services Name	Services Type	Port	Traffic Type
		http	TCP	80	Business
		mysql	tcp	3306	Business
Access Relationship	Access Relationship	Source	Destination	Services	Action
		IP Group: Office Endpoint	Business System: OA Server	http	Allow
		Business System: OA Server	Business System: Database Server	mysql	Allow

2. Berdasarkan isi dari tahap pertama, Isikan business system/IP group/service, dan hubungkan itu ke micro-isolation policy, seperti ditunjukkan pada figur dibawah.

The screenshot shows the Sangfor Endpoint Secure interface under the Micro-Segmentation tab. On the left sidebar, 'Business Systems' is selected. In the main area, there's a table for 'Endpoints' with columns: No., Endpoint, IP Address, Group, and OS. One endpoint, 'Windows3', is listed with IP 20.10.0.9. A modal window titled 'Add Business System' is open, prompting for 'Name:' (Business system name) and 'Endpoint:' (Select). The 'OK' button is highlighted.

The screenshot shows the Sangfor Endpoint Secure interface under the Micro-Segmentation tab. On the left sidebar, 'IP Groups' is selected. In the main area, there's a table for 'IP Groups' with columns: No., Name, IP Address, Type, and Remarks. Three groups are listed: 'auto_187.185.126', 'Default Internal IP Group', and 'Default Public IP Group'. A modal window titled 'Add New IP Group' is open, prompting for 'Name:', 'IP Addresses:', 'Type' (Public or Internal), and 'Remarks'. The 'OK' button is highlighted.

The screenshot shows the Sangfor Endpoint Secure interface under the Micro-Segmentation tab. On the left sidebar, 'Services' is selected. In the main area, there's a table for 'Services' with columns: No., Name, Protocol, Port, Traffic Type, and Remarks. Ten services are listed: Remote, Share, dhcp, mssql, ftp-data, ftp, telnet, smtp, and dns-t. A modal window titled 'Add New Service' is open, prompting for 'Name:', 'Protocol' (TCP and UDP checked), 'Port' (Separate ports or ranges by comma, e.g., 1023 or 1-65535), 'Traffic Type' (Other traffic selected), and 'Remarks' (It is used for world wide web proxy and website browsing). The 'OK' button is highlighted.

3. Tetapkan micro-isolation policy. Menurut hubungan akses diurutkan di langkah 1 dan business system/IP group/service ditetapkan pada langkah 2, tetapkan micro-isolation policy, seperti ditunjukan figur dibawah

The screenshot shows the Sangfor Endpoint Secure interface with the 'Micro-Segmentation' tab selected. On the left, a sidebar lists 'Policies', 'Traffic Statistics', 'Business Systems', 'Tags', 'IP Groups', 'Services', and 'Miscellaneous'. The 'Policies' item is highlighted. In the main area, a table titled 'Policies' displays a single row with 'Priority' 1 and 'Name' 'Anti'. A modal window titled 'Add New Policy' is open, prompting for configuration. It includes fields for 'Policy Name' (auto_187.185.126), 'Source' (auto_187.185.126), 'Destination' (Select), 'Services' (Select), and 'Action' (Allow). A note at the top of the modal states: 'This will invalidate firewall rules on associated endpoints.' At the bottom of the modal are 'OK' and 'Cancel' buttons.

4. Aktifkan micro-isolation policy switch dan traffic report, seperti ditunjukan figur dibawah:

The screenshot shows the Sangfor Endpoint Secure interface with the 'Miscellaneous' tab selected. On the left, a sidebar lists 'Policies', 'Traffic Statistics', 'Business Systems', 'Tags', 'IP Groups', 'Services', and 'Miscellaneous', with 'Miscellaneous' highlighted. The main area contains three sections: 'Micro-Segmentation' (with 'ON' checked), 'Report traffic statistics' (with 'ON' checked), and 'Backup and Restore' (with 'Download Configurations' and 'Restore Configurations' buttons). The 'Micro-Segmentation' and 'Report traffic statistics' sections are enclosed in a red box.

5. Periksa efek micro-isolation dan coba konektifitas port server.

4.7 Alarm Policy

Konfigurasi alarm policy untuk memberitahukan kepada administrator tepat waktu ketika ada ancaman terjadi di intranet. Langkah konfigurasinya seperti berikut:

1. Konfigurasi SMTP Server.

The screenshot shows the Sangfor Endpoint Secure interface under the 'System' tab. On the left, a sidebar lists various system settings like Agent Deployment, Update, Correlated Devices, Remote Sites, Administrators, Licensing, and System (with General selected). The main panel displays the 'General' configuration section, specifically the 'SMTP Server' settings. It includes fields for Preferred DNS (8.8.8), Alternate DNS (114.114.114.114), Sender (Endpoint Secure Manager), SMTP Server Address (smtp. [REDACTED].com), SMTP Server Port (25), and SSL checkbox. Below these are fields for Sender Address ([REDACTED]_sangfor@163.com) and Password (*****). A 'Send Test Email' button is present. At the bottom, there's a note about the Sangfor Cloud Security Program with a checked checkbox indicating agreement to its terms.

Klik Send "Send Test Email", jika anda dapat menerima test email seperti ditunjukan figur dibawah, artinya mailbox server telah sukses dikonfigurasi.

The screenshot shows an email client interface with a toolbar at the top containing buttons for Back, Edit and send again, Reply all, Forward, delete, move to, and More. The main area displays an email titled '[Endpoint Secure]Test Mail' from 'Endpoint Secure Manager <[REDACTED]_sangfor@163.com>' to 'sangfor. [REDACTED] <sangfor. [REDACTED]@gmail.com>'. The email was sent on 'March 02, 2021 17:13 (Tuesday)'. Below the email, a yellow bar indicates the 'Sending status: send successfully to' with a link to 'view details'. The bottom of the screen shows the Sangfor Endpoint Secure logo.



Copyright © SANGFOR Technologies Inc. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Inc.

SANGFOR is the trademark of SANGFOR Technologies Inc. All other trademarks and trade names mentioned in this document are the property of their respective holders.

Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied. The information in this document is subject to change without notice. To obtain the latest version, contact the international service center of SANGFOR Technologies Inc

