

Poradnik konfiguracji urządzenia Sophos XG Series firewall

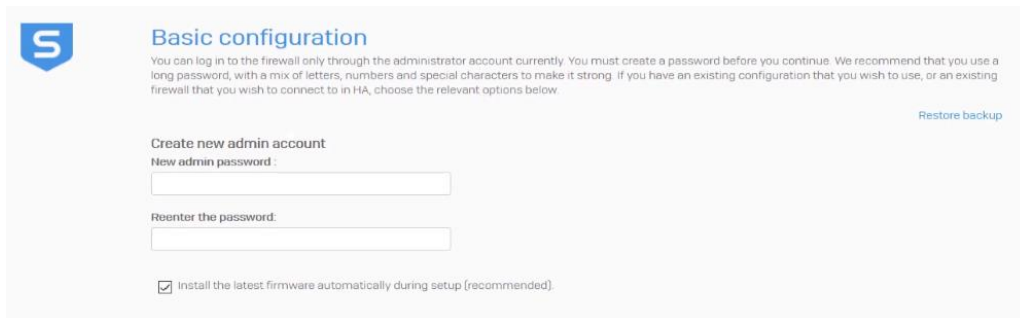
Spis treści

Wstępna konfiguracja.....	2
Dodawanie użytkowników i grup.....	6
Tworzenie grupy.....	6
Tworzenie użytkownika	7
Zmiana portu konsoli.....	8
Konfiguracja VPN	8
Konfiguracja email	14
SMTP route and scan.....	14
POP-IMAP scan	16
Blokowanie aplikacji.....	17
Filtr stron internetowych	18
Konfiguracja Firewalla	19
Aktualizacje	22
Kopia zapasowa i przywracanie.....	22
Raportowanie	23

Wstępna konfiguracja

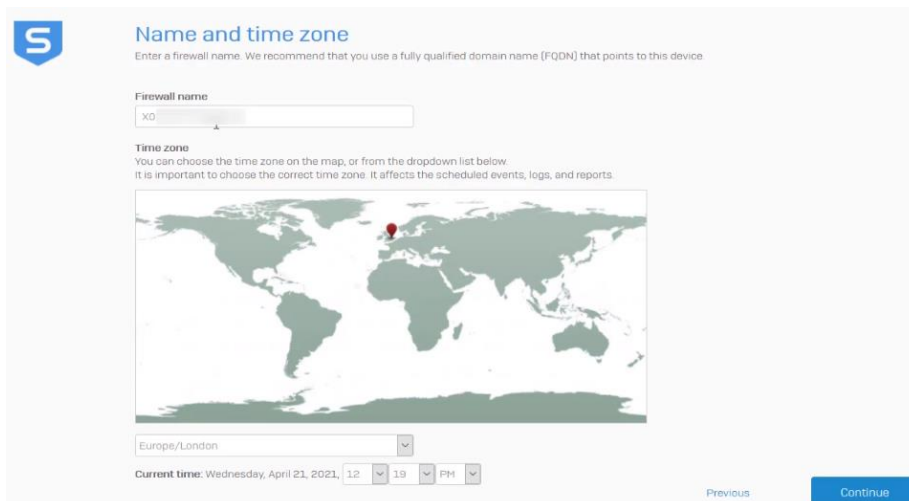
Aby skonfigurować urządzenie musimy podłączyć je przez port LAN do komputera, a następnie przejść na adres: <https://172.16.16.16:4444>.

Pierwszym krokiem jest utworzenie silnego hasła dla konta administratora oraz wyrażenie zgody na pobranie najnowszego oprogramowania do urządzenia.



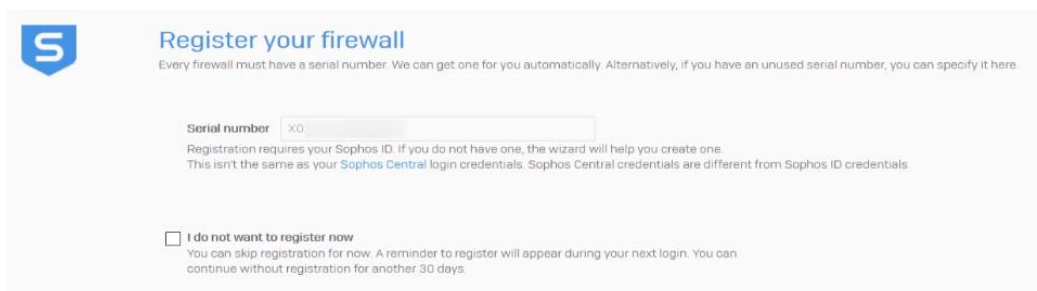
The screenshot shows the 'Basic configuration' screen. It features a blue 'S' logo in the top left. The main heading is 'Basic configuration'. Below the heading, there is a paragraph of text explaining that a password must be created before continuing. To the right of this text is a 'Restore backup' link. The form contains two input fields: 'New admin password' and 'Reenter the password'. Below these fields is a checkbox labeled 'Install the latest firmware automatically during setup (recommended)'. The background is a light gray.

Następnie musimy wybrać nazwę urządzenia oraz strefę czasową.



The screenshot shows the 'Name and time zone' screen. It features a blue 'S' logo in the top left. The main heading is 'Name and time zone'. Below the heading, there is a paragraph of text explaining that a fully qualified domain name (FQDN) is recommended. The form contains a text input field for 'Firewall name' with the placeholder 'XO.'. Below this is a 'Time zone' section with a paragraph of text explaining that the time zone can be chosen on a map or from a dropdown list. A world map is displayed with a red pin over Europe. Below the map is a dropdown menu showing 'Europe/London'. At the bottom, there is a 'Current time' field showing 'Wednesday, April 21, 2021, 12:19 PM'. There are 'Previous' and 'Continue' buttons at the bottom right. The background is a light gray.

Możemy zarejestrować nasze urządzenie od razu lub zrobić to później.



The screenshot shows the 'Register your firewall' screen. It features a blue 'S' logo in the top left. The main heading is 'Register your firewall'. Below the heading, there is a paragraph of text explaining that every firewall must have a serial number. The form contains a text input field for 'Serial number' with the placeholder 'XO.'. Below this is a paragraph of text explaining that registration requires a Sophos ID. At the bottom, there is a checkbox labeled 'I do not want to register now' with a paragraph of text explaining that registration can be skipped for now. The background is a light gray.

Jeśli zarejestrujemy urządzenie to zobaczymy listę usług, które obejmuje nasza licencja.

Basic setup is complete
You have completed the basic setup. The firewall is registered with the following licenses. The wizard will help you set up the basic networking and security features. To configure these manually, click "Skip to finish".

C1701B3TXVRP277

Licensed features

Feature	Status	Expiry
Base firewall	Subscribed	Tue 31 Dec 2999
Network protection	Subscribed	Tue 31 Dec 2999
Web protection	Subscribed	Tue 31 Dec 2999
Email protection	Expired	Sat 20 Jun 2020
Web server protection	Expired	Sat 20 Jun 2020
Sandstorm	Subscribed	Tue 31 Dec 2999
Enhanced support	Subscribed	Tue 31 Dec 2999
Enhanced plus support	Unsubscribed	-

Opt in to the customer experience improvement program. [View Sophos privacy policy](#)

[Add license keys](#)

Wybieramy jakie funkcje będą pełniły porty w naszym urządzeniu oraz jaką rolę będzie pełnił nasz UTM (rolę routera lub mostu). Wybieramy adres dla sieci LAN, maskę, zakresy DHCP i edytujemy połączenie z internetem.

Network configuration (LAN)
Let us set up a protected network. Select the ports to which you will connect the devices you wish to protect. The selected traffic will be permitted among them. You are connected to "Port1" right now.

1 2 3 4 5 6 7 8

■ Connected ■ Enable for LAN ■ Enable for WAN ■ Not configured ○ Fiber port

Choose gateway
This firewall (route mode)

Do you want this firewall to act as the gateway for the protected network (commonly used)? Alternatively, you can use the protected network with it. The firewall delivers the same level of security in both cases. Additionally, it can act as a gateway for other local networks if configured as a gateway.

LAN address and internal client network size
10.10.250.1 /24 (up to 254 client devices)

[Edit internet connection](#)

Enable DHCP
Let the firewall assign IP addresses to your internal devices.

DHCP lease range
10.10.250.100 - 10.10.250.254

Manual configuration
If your service provider has given specific internet configuration settings, enter them here.

Choose a port to configure
Port2

Interface type
Dynamic IP address

IP address

Subnet
/30 (255.255.255.252)

Gateway name
DHCP_Port2_GW

Gateway IP address
128.0.0.1

DNS server 1
127.0.0.1

DNS server 2

Configure upstream proxy settings

Domain name/IPv4 Address

Port

User name

Password

[Reset](#) [Cancel](#) [Apply](#)

Następnym krokiem jest wybranie podstawowej ochrony jaką będzie spełniał nasz firewall.

Network protection
You can configure permissions for users on wired and wireless networks to protect them when they access the internet.

- Protect users from network threats**
Protects users from network intrusion attempts, protects against advanced threats that could be within your network, and blocks network traffic from high-risk applications.
- Protect users from the suspicious and malicious websites**
Protects users from clicking malicious links, and from visiting harmful sites. It does not scan the SSL traffic. [Click here to learn how to scan HTTPS traffic.](#)
- Scan files that were downloaded from the web for malware**
Even reputed sites may contain malicious files. Scan files with Sophos malware detection engine to catch known malware and their variants.
- Send suspicious files to Sophos Sandstorm**
Protects users from undiscovered malware through advanced detection techniques that involve running applications, and viewing documents in a safe sandbox in the cloud, before letting users download files to their computers.

Wybieramy nadawcę oraz odbiorcę powiadomień i naszej kopii zapasowej oraz wybieramy hasło niezbędne do przywrócenia naszego backupu.

Notifications and backups
It is important to have quick access to backups. Enter the details to receive the latest backups and notifications by email.

Email recipient

Email sender

Send weekly configuration backup

Encryption password

Confirm encryption password

Specify an external mail server

Jeśli wszystko się udało zobaczymy podsumowanie naszej konfiguracji.

S

Configuration summary

Please review your choices in the window. Click Finish. This will apply the settings that you have specified, install the latest firmware, and reboot the firewall. It will take approximately five minutes to complete.

Basic settings
Hostname: VB_XG
Time zone: Europe/London

Network settings
Internet connection: DHCP on Port2
Local network: Port1
IP: 172.16.16.16/255.255.255.0
DHCP disabled

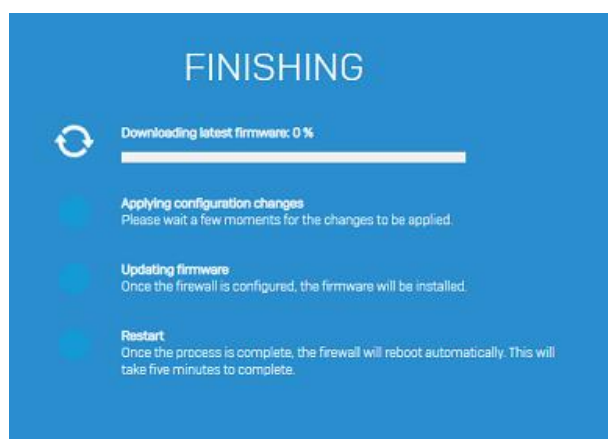
#Default_Network_Policy has been created with:
Scan HTTP: Disable
Detect zero-day threats with Sandstorm: Disable
Web policy: -
Intrusion prevention: -

Created linked NAT rule "#NAT_Default_Network_Policy" with source translated to MASQ.

Notifications and backups:
Send weekly configuration backup: Disable
Built-in email server
Email recipient:
Email sender:

Copy to clipboard Send as email Previous **Finish**

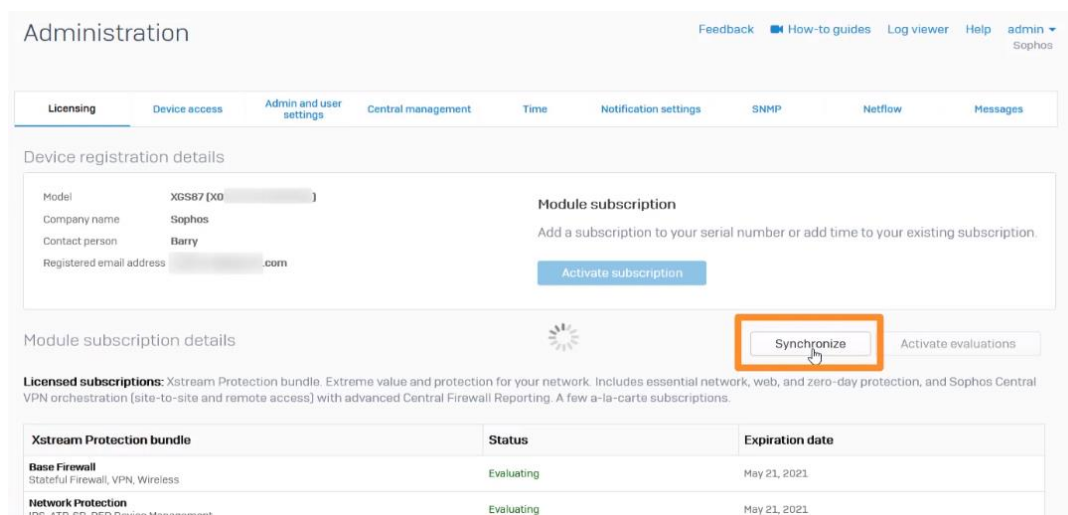
Następnie nasze urządzenie zacznie pobierać najnowsze oprogramowanie w celu aktualizacji.



Po ponownym uruchomieniu się XG firewalla oraz zalogowaniu się na konto administratora, dostaniemy się do interfejsu urządzenia i będziemy mogli utworzyć klucz zabezpieczeń do pamięci masowej.



Ostatnim krokiem wstępnej konfiguracji jest synchronizacja licencji. Przechodzimy do zakładki *Administration* → *Licensing* i wybieramy opcję *Synchronize*.



Dodawanie użytkowników i grup

Tworzenie grupy

Przechodzimy do zakładki *Authentication* → *Groups* → *Add* i wybieramy:

- Nazwę grupy
- Typ grupy
- Limit dostępu do internetu
- Czas dostępu
- oraz opcję związane z VPN

Group name *	<input type="text" value="test group"/>
Description	<input type="text" value="Description"/>
Group type *	<input type="text" value="Normal"/>
<hr/>	
Policies	
Surfing quota *	<input type="text" value="Unlimited Internet Access"/> ⓘ
Access time *	<input type="text" value="Allowed all the time"/> ⓘ
Network traffic	<input type="text" value="None"/> ⓘ
Traffic shaping	<input type="text" value="None"/> ⓘ
Remote access *	<input type="text" value="No policy applied"/> ⓘ
Clientless *	<input type="text" value="No policy applied"/> ⓘ
Quarantine digest *	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
MAC binding	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
L2TP *	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
PPTP *	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
IPsec remote access *	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Login restriction*	<input checked="" type="radio"/> Any node <input type="radio"/> Selected nodes <input type="radio"/> Node range

Tworzenie użytkownika

Przechodzimy do zakładki *Authentication* → *Users* → *Add* i wybieramy:

- Nazwę użytkownika
- Nazwę
- Typ użytkownika
- Hasło
- Email
- Grupę do jakiej ma należeć
- Limit dostępu do internetu
- Czas dostępu
- oraz politykę połączenia SSLVPN

Add user

Username *	<input type="text" value="test"/>
Name *	<input type="text" value="test"/>
Description	<input type="text" value="Description"/>
User type *	<input checked="" type="radio"/> User <input type="radio"/> Administrator
Profile *	<input type="text" value="Profile"/>
Password *	<input type="password" value="....."/> <input type="password" value="....."/>
Email *	<input type="text" value="test@gmail.com"/>

Policies

Group *	<input type="text" value="test group"/>
Surfing quota *	<input type="text" value="Unlimited Internet Access"/> ⓘ
Access time *	<input type="text" value="Allowed all the time"/> ⓘ
Network traffic	<input type="text" value="None"/> ⓘ
Traffic shaping	<input type="text" value="None"/> ⓘ

SSL VPN policy

Remote access *	<input type="text" value="No policy applied"/> ⓘ	⚠ Group's remote access policy applies if you don't select a policy.
Clientless *	<input type="text" value="No policy applied"/> ⓘ	
L2TP *	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	IP address <input type="text"/> ⓘ
PPTP *	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	IP address <input type="text"/> ⓘ
IPsec remote access *	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	IP address <input type="text"/> ⓘ
Quarantine digest *	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Simultaneous logins *	<input checked="" type="checkbox"/> Use global setting <input checked="" type="checkbox"/> Unlimited <input type="text" value=""/> (1-99)	
MAC binding *	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
MAC address list	<input type="text"/>	Use a comma or a new line to separate multiple MAC addresses. Example: 11-11-11-11-11-11, 22-22-22-22-22-22
Login restriction*	<input type="radio"/> Any node <input checked="" type="radio"/> User group node(s) <input type="radio"/> Selected nodes <input type="radio"/> Node range	

Zmiana portu konsoli

Przechodząc do zakładki *Administration* → *Admin and user settings*.

Tutaj możemy zmienić domyślny port łączenia się z interfejsem użytkownika oraz administratora.

Admin console and end-user interaction

Admin console HTTPS port *	<input type="text" value="22137"/>
User portal HTTPS port *	<input type="text" value="942"/>
Certificate *	<input type="text" value="ApplianceCertificate"/> [Selected certificate will be used for My Account, captive portal, SPX registration portal & reply portal]

When redirecting users to the captive portal or other interactive pages:

Use the firewall's configured hostname: SO

Use the IP address of the first internal interface: 192.168.10.1

Use a different hostname:

Konfiguracja VPN

Aby skonfigurować VPN musimy przejść do zakładki *VPN* → *IPsec (remote access)*

W ustawieniach ogólnych wybieramy:

- Dostęp zdalny IPsec: włączony
- Interfejs: *Port sieci WAN*
- Sposób poświadczenia: *klucz lub certyfikat*
- Lokalny i zdany identyfikator
- oraz grupę lub użytkowników, którzy będą mogli logować się przez klienta VPN.

General settings

IPsec remote access	<input checked="" type="checkbox"/> Enable
Interface *	<input type="text" value="Port2 - 203.0.113.1"/> ⓘ
Authentication type *	<input type="text" value="Digital certificate"/> ⓘ
Local certificate *	<input type="text" value="ApplianceCertificate"/>
Remote certificate *	<input type="text" value="External certificate"/>
Local ID	<input type="text" value="DER ASN1 DN (X.509)"/> <input type="text" value="/C=NA/ST=NA/L=NA/O=NA/OU=NA/CN=Appliance"/>
Remote ID	<input type="text" value="Email"/> <input type="text" value="test@company.com"/>
Allowed users and groups *	<input type="text" value="Open Group"/> ⓘ <input type="text" value="testuser"/> <input type="button" value="Add new item"/>

W sekcji informacje o kliencie wybieramy:

- Nazwę połączenia
- Zakres przypisywanych adresów
- oraz serwery DNS

Client information

Name *	<input type="text" value="TestRemoteAccessVPN"/>
Assign IP from *	<input type="text" value="192.168.1.11"/> - <input type="text" value="192.168.1.254"/>
	<input type="checkbox"/> Allow leasing IP address from RADIUS server for L2TP, PPTP and IPsec remote access i
DNS server 1	<input type="text" value="192.168.1.5"/>
DNS server 2	<input type="text"/>

Należy pamiętać, aby zakres przydzielanych adresów dla klientów VPN był w innej podsieci niż zakres adresów dla sieci LAN.

Przykładowa konfiguracja ustawień zaawansowanych:

Advanced settings

Adds these settings only to the .scx file used with Sophos Connect clients. To apply the changes, send the updated file to users for reimport into the client

Use as default gateway	<input type="checkbox"/> OFF						
Permitted network resources (IPv4) *	<div style="border: 1px solid orange; padding: 5px;"><table><tr><td>LAN_10.1.1.0</td><td>✎ ✖</td></tr><tr><td>DMZ_192.168.2.0</td><td>✎ ✖</td></tr><tr><td colspan="2" style="text-align: center;">Add new item</td></tr></table><ul style="list-style-type: none"><input checked="" type="checkbox"/> Send Security Heartbeat through tunnel<input checked="" type="checkbox"/> Allow users to save username and password<input type="checkbox"/> Prompt users for 2FA token<input type="checkbox"/> Run AD logon script after connecting</div>	LAN_10.1.1.0	✎ ✖	DMZ_192.168.2.0	✎ ✖	Add new item	
LAN_10.1.1.0	✎ ✖						
DMZ_192.168.2.0	✎ ✖						
Add new item							
	<input type="checkbox"/> Connect tunnel automatically						
	<input type="checkbox"/> Assign client DNS suffix						
Hostname or DNS suffix to monitor	<input type="text" value="Enter a hostname or DNS suffix"/>						
DNS suffix	<input type="text" value="Enter a DNS suffix"/>						

Jeśli włączymy opcję *Use as default gateway* połączenie VPN będzie pozwalało na dostęp do wszystkich zasobów (wszystkie sieci LAN, WAN, DMZ). Jeżeli pozostawimy tą opcję wyłączoną będziemy musieli utworzyć nowy element, a następnie dodać sieć w *Permitted network resources (IPv4)*.

Permitted network resources – wybrane zasoby

Use as default Gateway – dostęp do wszystkich zasobów

Jeśli wybierzemy wszystkie interesujące nas opcje klikamy *Apply* i możemy wyeksportować nasze połączenie, a następnie pobrać klienta.



Po ustawieniu VPN musimy dodać go do zapory. Przechodzimy do zakładki *Rules and policies* → *Firewall rules* → *Add firewall rule* → *New firewall rule*.

- Nazwa: VPN to LAN
- Akcja: akceptuj

I następnie wybieramy VPN jako źródło, a LAN jako miejsce docelowe.

The screenshot shows the configuration interface for a firewall rule. It is divided into two main sections: 'Source' and 'Destination and services'.
Source section:
- **Source zones ***: A dropdown menu with 'VPN' selected and an 'Add new item' button below it.
- **Source networks and devices ***: A dropdown menu with 'NET_VPN' selected and an 'Add new item' button below it.
- **During scheduled time**: A dropdown menu with 'All the time' selected and a subtext: 'Select to apply the rule to a specific time period and day of the week.'
Destination and services section:
- **Destination zones ***: A dropdown menu with 'LAN' selected and an 'Add new item' button below it.
- **Destination networks ***: A dropdown menu with 'Any' selected and an 'Add new item' button below it.
- **Services ***: A dropdown menu with 'Any' selected and an 'Add new item' button below it. A subtext below reads: 'Services are traffic types based on a combination of protocols and ports.'

W *Source networks and devices* tworzymy nowy element sieci o adresie sieci VPN.

The screenshot shows the 'Add IP host' configuration form. It has a blue header button labeled 'Add IP host'. The form contains the following fields:
- **Name ***: Text input field containing 'vpn'.
- **IP version ***: Radio buttons for 'IPv4' (selected) and 'IPv6'.
- **Type ***: Radio buttons for 'IP', 'Network' (selected), 'IP range', and 'IP list'.
- **IP address ***: Text input field containing '192.168.5.0'.
- **Subnet**: Dropdown menu with '/24 [255.255.255.0]' selected.
- **IP host group**: A large empty text area with an 'Add new item' button at the bottom.

Analogicznie tworzymy zasadę VPN to WAN z tym wyjątkiem, że miejscem docelowym będzie sieć WAN.

Source
Select the source zones, networks, and devices.
The rule applies to traffic from these sources during the scheduled time period.

Source zones *
VPN
Add new item

Source networks and devices *
NET_VPN
Add new item

During scheduled time
All the time
Select to apply the rule to a specific time period and day of the week.

Destination and services
Select the destination zones, networks, devices, and services.
The rule applies to traffic to these destinations.

Destination zones *
WAN
Add new item

Destination networks *
Any
Add new item

Services *
Any
Add new item
Services are traffic types based on a combination of protocols and ports.

Następnym krokiem będzie utworzenie reguł NAT, które będą tłumaczyć adresy z sieci VPN na sieć LAN oraz WAN. Przechodzimy do *Rules and policies* → *NAT rules* → *Add NAT rule* → *New NAT rule*.

- Nazwa: VPN TO LAN
- Źródło: *element sieci VPN*
- Źródło translacji: MASQ
- Interfejs wychodzący: br0 (LAN)

Original source *
NET_VPN
Add new item

Original destination *
Any
Add new item

Original service *
Any
Add new item

Translated source (SNAT)
MASQ

Translated destination (DNAT)
Original

Translated service (PAT)
Original

Interface matching criteria

Inbound interface *
Any
Add new item

Outbound interface *
br0
Add new item

Następnie tworzymy podobną regułę dla połączenia VPN to WAN:

- Nazwa: VPN TO WAN
- Źródło: *element sieci VPN*
- Źródło translacji: MASQ
- Interfejs wychodzący: Port2 (WAN)

Original source *
NET_VPN
Add new item

Original destination *
Any
Add new item

Original service *
Any
Add new item

Translated source (SNAT)
MASQ

Translated destination (DNAT)
Original

Translated service (PAT)
Original

Interface matching criteria

Inbound interface *
Any
Add new item

Outbound interface *
Port2
Add new item

Aby, użytkownik korzystający z VPNa miał dostęp do konsoli urządzenia musimy zmienić ustawienia dostępu do urządzenia. W tym celu przechodzimy do *Administration* → *Devices access*. W wierszu VPN wybieramy interesujące nas ustawienia dostępu.

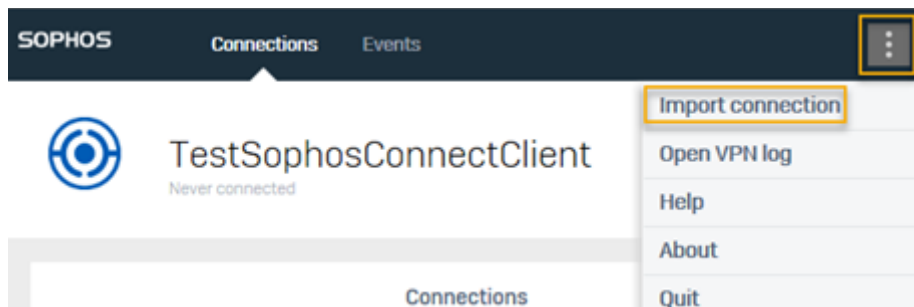
Zone	Admin services		Authentication services				Network services			Other services						
	HTTPS	SSH	AD SSO	Captive portal *	Radius SSO	Client Authentication	Chromebook SSO	Ping/Ping6	DNS	Wireless Protection	SSL VPN	Web proxy	User Portal	Dynamic Routing	SMTP Relay	SNMP
LAN	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
WAN	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
DMZ	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
VPN	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
WiFi	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Po zainstalowaniu klienta musimy wybrać połączenie, aby to zrobić wypakowujemy wcześniej pobrany plik *nazwa.tar*. Po wypakowaniu mamy do wyboru dwa pliki jeden o rozszerzeniu *.scx* i drugi o rozszerzeniu *.tgb*.

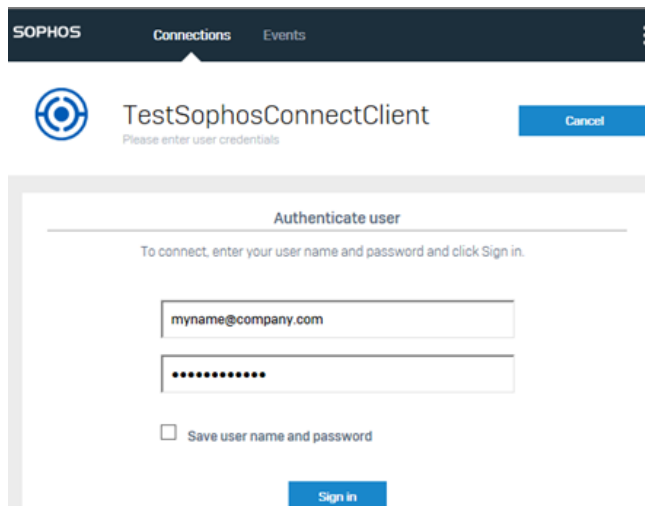
.scx – to plik zawierający ustawienia zaawansowane (zalecany)

.tgb – to plik zawierający jedynie podstawową konfigurację

W kliencie wybieramy opcje: *Import connection*, a następnie wybieramy interesujący nas plik.



Ostatnim krokiem jest zalogowanie się na wybranego użytkownika.



Konfiguracja email

SMTP route and scan

Przechodzimy do zakładki *Email* → *Policies & exceptions* → *Add policy* → *SMTP route and scan*.

SMTP policy

Name *

Domains and routing target

Protected domain *

Add new item

Global action

SPX template

Route by

Dodajemy chronioną domenę.




Add address group

Name *

Description

Group type
 RBL (IPv4) RBL (IPv6) Email address/domain

Type
 Import Manual

Domain *
  
 

Save Cancel

Wybieramy interesujące nas opcje ochrony poczty

Przykładowa konfiguracja:

Spam protection

Check for inbound spam

Use greylisting

Reject based on BATV

Reject based on SPF

Reject based on RBL

Premium RBL Services

Standard RBL Services

Spam action:

Probable spam action:

Prefix subject:

Recipient verification:

Malware protection

Scanning:

Selected antivirus action:

Single scan engine is set to Sophos

Notify sender

Quarantine unscannable content

Detect zero-day threats with Sandstorm

Scanned file size: MB

Maximum 10MB

File protection

Block file types:

MIME white list:

Drop message greater than: KB

Enter 0 for default size restriction of 51200 KB

SMTP zaleca się tylko wtedy, gdy w sieci znajdują się serwer poczty.

POP-IMAP scan

Przechodzimy do zakładki *Email* → *Policies & exceptions* → *Add policy* → *POP-IMAP scan*.

- Nazwa: rule3
- Nadawca: każdy
- Odbiorca: każdy
- Przychodzący email jest: Spamem
- Akcja: Prefix subject
- To: [Spam]:

Email address/domain group

Sender *

Recipient *

Filter criteria

Inbound email is

Source IP/network address

Message size KB

Message header

None

Action

Action To

Analogicznie tworzymy zasadę ochrony przed prawdopodobnym spamem, musimy jedynie wybrać *Probable Spam* w oknie *Inbound email is*.

Inbound email is

Nie musimy tworzyć reguł ochrony przed wirusami, ponieważ takie reguły są już domyślnie utworzone.

Policies Add policy

Name	Sender	Recipient	Details	Action	Manage
antyspam <small>(imap)</small>	Any	hydroserwis	Route email via MX record Spam action: Drop, Probable spam... Dual anti-virus, Action: Drop, Sender... Block file types: None, MIME white...	Accept	
rule4 <small>(pop3/imap)</small>	Any	Any	Mail is identified as spam by inbound anti spam module	Prefix subject To...	
rule3 <small>(pop3/imap)</small>	Any	Any	Mail is identified as probable spam by inbound anti spam mod...	Prefix subject To...	
default-pop-av <small>(pop3/imap)</small>	Any	Any	Single anti-virus (maximum performance)	Accept	
rule2 <small>(pop3/imap)</small>	Any	Any	Mail is identified as probable virus outbreak by inbound ant...	Prefix subject To...	
rule1 <small>(pop3/imap)</small>	Any	Any	Mail is identified as virus outbreak by inbound anti spam mo...	Prefix subject To...	

Blokowanie aplikacji

Aby utworzyć filtr blokowania aplikacji przechodzimy do zakładki *Applications* → *Application filter* → *Add*.

Podajemy nazwę, wybieramy szablon i zapisujemy.

Następnie przy naszym nowo dodanym filtrze wybieramy opcję edytuj i dodaj.

Za pomocą kategorii, ryzyka, charakterystyki, technologii i klasyfikacji możemy wybrać aplikacje, które chcemy zablokować lub odblokować w zależności od tego wybieramy akcje: zezwól lub odmów oraz harmonogram, czyli dni lub godziny w jakich aplikacje będą blokowane.

Add application filter policy rules

Category Risk Characteristics Technology Classification Smart filter Clear filter

Select all Select individual application

<input type="checkbox"/>	Name	Description	Category	Risk	Technology	Characteristics	Classification
<input checked="" type="checkbox"/>	1 & 1 Webmail	1 & 1 Webmail	Web Mail	2 - Low	Browser Based	Cloud Applicatio...	New
<input checked="" type="checkbox"/>	10000ft Plans	10000ft Plans	General Business	1 - Very Low	Browser Based	Cloud Applicatio...	New
<input checked="" type="checkbox"/>	100BA0 P2P	100BA0 P2P	P2P	4 - High	P2P	Excessive Band...	
<input checked="" type="checkbox"/>	101 Network	101 Network	Streaming Media	1 - Very Low	Browser Based	Loss of producti...	
<input checked="" type="checkbox"/>	123RF	123RF	E-commerce	1 - Very Low	Browser Based	Loss of producti...	
<input checked="" type="checkbox"/>	126 Mail	126 Mail	Web Mail	2 - Low	Browser Based	Transfer files, Wi...	

List of matching applications (1 - 50 of 3530)

Action * Allow Deny

Schedule * All the Time

Przykładowa konfiguracja filtru:

- Category = P2P
- Category = Gaming
- Risk = 4-High
- Risk = 5-Very High
- Category = Proxy and Tunnel
- Action: Deny
- Schedule: All the time

Filtr stron internetowych

Przechodzimy do zakładki *Web* → *Policies* → *Add policy*.

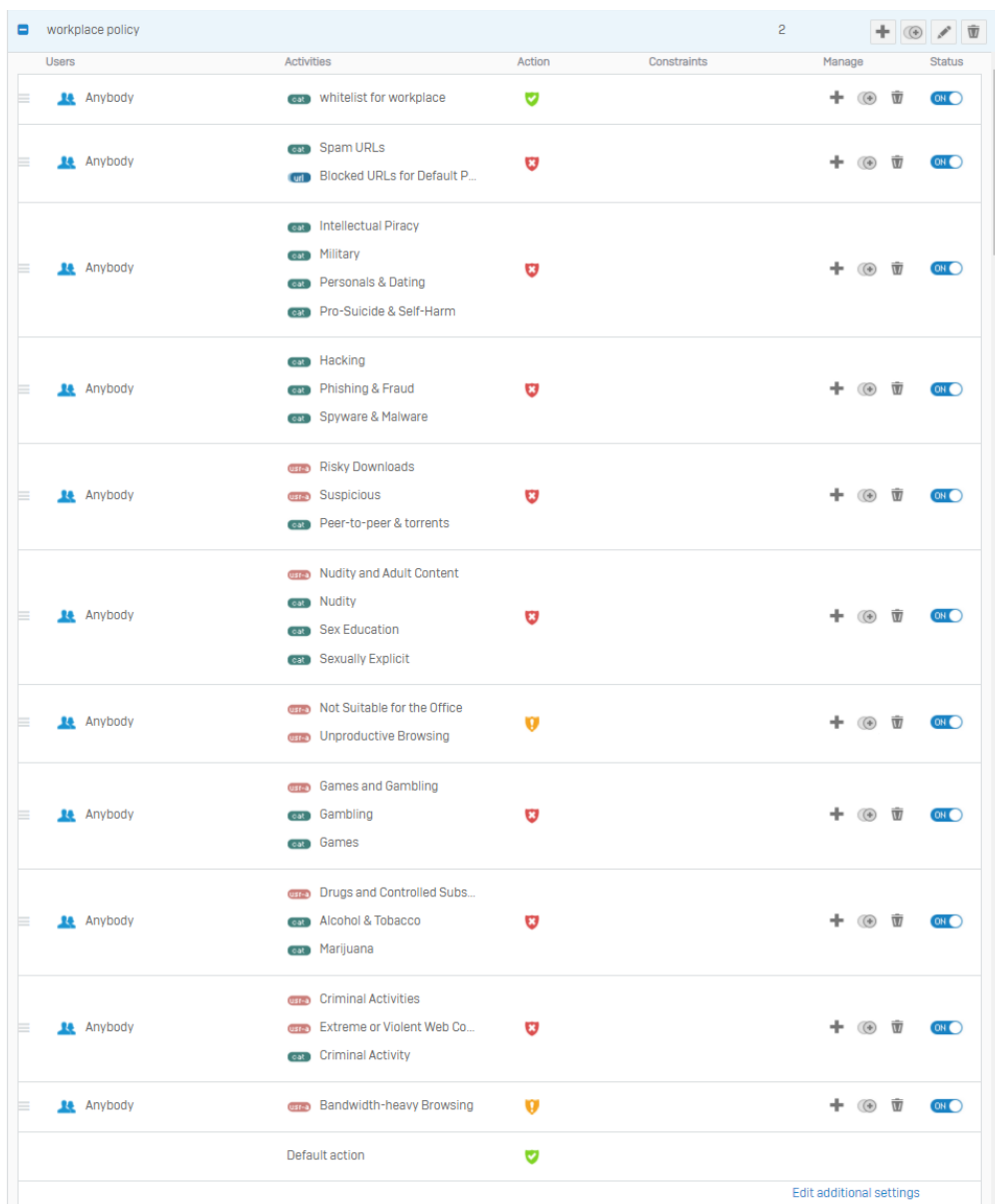
Podajemy nazwę filtru i wybieramy dodaj regułę.

W kolumnie *users* możemy wybrać użytkowników, których będzie dotyczyła reguła.

W kolumnie *Activities*, a następnie *Add new item* wybieramy aktywności, kategorie stron, typy plików i grupy URL, które możemy dodać.

W kolumnie *Action* mamy do wyboru cztery rodzaje akcji, które możemy wykonać w związku z wejściem na wcześniej wybrane przez nas strony. Są to *Zezwól*, *Blokuj*, *Ogranicz*, *Ostrzegaj*.

Przykładowa konfiguracja:



Users	Activities	Action	Constraints	Manage	Status
Anybody	whitelist for workplace	✓		+ ⌂ 🗑	ON
Anybody	Spam URLs Blocked URLs for Default P...	🛑		+ ⌂ 🗑	ON
Anybody	Intellectual Piracy Military Personals & Dating Pro-Suicide & Self-Harm	🛑		+ ⌂ 🗑	ON
Anybody	Hacking Phishing & Fraud Spyware & Malware	🛑		+ ⌂ 🗑	ON
Anybody	Risky Downloads Suspicious Peer-to-peer & torrents	🛑		+ ⌂ 🗑	ON
Anybody	Nudity and Adult Content Nudity Sex Education Sexually Explicit	🛑		+ ⌂ 🗑	ON
Anybody	Not Suitable for the Office Unproductive Browsing	⚠️		+ ⌂ 🗑	ON
Anybody	Games and Gambling Gambling Games	🛑		+ ⌂ 🗑	ON
Anybody	Drugs and Controlled Subs... Alcohol & Tobacco Marijuana	🛑		+ ⌂ 🗑	ON
Anybody	Criminal Activities Extreme or Violent Web Co... Criminal Activity	🛑		+ ⌂ 🗑	ON
Anybody	Bandwidth-heavy Browsing	⚠️		+ ⌂ 🗑	ON
	Default action	✓			

[Edit additional settings](#)

Aby, utworzyć własną grupę stron internetowych musimy przejść do zakładki *Web* → *Categories* → *Add*.

Tutaj podajemy nazwę grupy, wybieramy jak ma być klasyfikowana oraz co najważniejsze możemy podać blokowane domeny lub słowa kluczowe.

The screenshot shows the 'Add Category' configuration window. It contains the following fields and options:

- Name ***: Input field containing 'test'.
- Description**: Empty text area.
- Classification ***: Dropdown menu set to 'Unproductive'.
- Traffic shaping policy**: Dropdown menu set to 'None'.
- Configure category ***: Radio buttons for 'Local' (selected) and 'External URL database'.
- Import domain/keyword**: Two columns for 'Domain' and 'Keyword'. Each has a 'Wybierz plik' button and the text 'Nie wybrano pliku'.
- Domain/keyword ***: Two input fields. The first contains 'instagram.com' and the second contains 'facebook'. Both have a search icon and a '+' button.

Konfiguracja Firewalla

Przechodzimy do zakładki *Rules and policies* → *Firewall rules*.

Pierwszym krokiem będzie usunięcie domyślnych reguł i grup. Aby, to zrobić wybieramy trzykropek obok reguły oraz wybieramy opcję Delete.

Icon	Rule Name	Direction	Zone	Host	Service	Priority	Action	
☰	Traffic to Interna...	in 0 B, out 0 B						
☰	[example] Traffic...	in 0 B, out 0 B	Any zone	Any host	Any service	#4	Drop	
☰	Traffic to WAN	in 0 B, out 0 B	Any zone	Any host	WAN, Any host	Any service	#3	Drop
☰	[example] Traffic...	in 0 B, out 0 B	Any zone	Any host	DMZ, Any host	Any service	#2	Drop
☰	Traffic to DMZ	in 0 B, out 0 B	Any zone	Any host	Any zone, Any host	Any service	#0	Drop
☰	Drop all	in 0 B, out 0 B	Any zone	Any host	Any zone, Any host	Any service	#0	Drop

The context menu for the selected rule includes the following options:

- OFF
- Edit
- Reset data transfer count
- Clone rule above
- Clone rule below
- Add rule above
- Add rule below
- Detach
- Delete

Aby, utworzyć nową regułę wybieramy *Add firewall rule*, a następnie *New firewall rule*.

Pierwsza reguła jaką utworzymy będzie odpowiedzialna za ruch z sieci lokalnej do sieci globalnej.

- Nazwa: LAN to WAN
- Akcja: akceptuj
- Reguła grupy: żadna
- Rejestruj ruch zapory: tak

ON Rule status

Rule name *
LAN to WAN

Description
Enter Description

Rule group
None

Action
Accept

Log firewall traffic
Logs traffic, matching this firewall rule, on the appliance (by default) or on the configured syslog server.

Jako źródło wybieramy LAN, a jako miejsce docelowe WAN.

Source
Select the source zones, networks, and devices.
The rule applies to traffic from these sources during the scheduled time period.

Source zones *
LAN
Add new item

Source networks and devices *
Any
Add new item

During scheduled time
All the time
Select to apply the rule to a specific time period and day of the week.

Destination and services
Select the destination zones, networks, devices, and services.
The rule applies to traffic to these destinations.

Destination zones *
WAN
Add new item

Destination networks *
Any
Add new item

Services *
Any
Add new item
Services are traffic types based on a combination of protocols and ports.

Jeśli chcemy, aby dostęp do internetu był tylko dla określonej grupy użytkowników możemy wybrać funkcję *Match known users* i wybrać grupę lub użytkowników.

Match known users

Use web authentication for unknown users

User or groups *
Any
Add new item

Exclude this user activity from data accounting

W sekcji *Security features* wybieramy wcześniej utworzoną politykę stron internetowych lub jedną z domyślnych polityk. Następnie zaznaczamy:

- Blokuj protokół *QUIC*
- Skanuj *HTTP* oraz deszyfrowane *HTTPS*
- Wykrywaj zagrożenia *zero-day* za pomocą *Sandstorm*
- Skanuj *FTP*

Security features

Web filtering

Web policy ⚠

workplace policy

Apply web category-based traffic shaping

Block QUIC protocol

Malware and content scanning

Scan HTTP and decrypted HTTPS

Detect zero-day threats with Sandstorm

Scan FTP for malware

Filtering common web ports

Use web proxy instead of DPI engine

[i DPI engine or web proxy?](#)

Web proxy options

Decrypt HTTPS during web proxy filtering

W *Other security features* wybieramy wcześniej utworzony filtr aplikacji lub jeden z domyślnych filtrów, a w sekcji *IPS* wybieramy *LAN TO WAN*.

Other security features

Identify and control applications (App control)

application filter

Apply application-based traffic shaping policy

Shape traffic

None

DSCP marking

Select DSCP marking

Detect and prevent exploits (IPS)

LAN TO WAN

W sekcji skanowania poczty wybieramy skanowanie: *IMAP*, *IMAPS*, *POP3*, *POP3S*.

Scan email content

Scan IMAP

Scan IMAPS

Scan POP3

Scan POP3S

Scan SMTP

Scan SMTPS

Zaleca się tworzenie osobnej zasady dla każdego ruchu przepływającego z sieci (np. LAN to WAN, VPN to LAN, itd.)

Aktualizacje

Aby, zaktualizować urządzenie do najnowszej wersji musimy przejść do zakładki *Backup and firmware* → *Firmware*, a następnie wybrać opcję *Check for new firmware*.

Latest available firmware

Firmware version	Type	Actions
No records found		

Check for new firmware

Aby, zaktualizować oprogramowanie przechodzimy do *Backup and firmware* → *Pattern updates* i wybieramy opcję *Update pattern now*.

Updates status

Last checked for updates : 15:09:22, May 17 2021

Update pattern now

Kopia zapasowa i przywracanie

Aby, utworzyć kopie zapasową przechodzimy do zakładki *Backup & firmware* → *Import export*.

Wybierając opcję *Export full configuration*, a następnie *Export* pobierzemy kopię zapasową naszej konfiguracji.

Import

Import file *

Wybierz plik Nie wybrano pliku

Import

Export

Export full configuration

Export selective configuration

Export

Aby zaimportować konfigurację wybieramy plik z menu *Wybierz plik*, a następnie potwierdzamy przyciskiem *Import*.

Ustawienia kopii zapasowej możemy zmienić w zakładce *Backup & firmware* → *Backup & restore*.

Backup

Backup mode Local FTP Email

Backup prefix

Email address * Quarantine digest will be sent to the first email address only.

Frequency Never Daily Weekly Monthly

Schedule Date HH MM

Encryption password * ***** [Change Encryption password](#)

Backup restore

Restore configuration Nie wybrano pliku

Encryption password i

Raportowanie

Dostęp do bieżących raportów mamy w zakładce *Reports*, ale jeśli chcemy sporządzić harmonogram raportów musimy przejść do zakładki z której chcemy sporządzić raport (Panel nawigacyjny, Aplikację i strony, Sieć i zagrożenia, VPN, Email). Następnie przechodzimy do *Schedule* i wybieramy:

- Pokaż: wybieramy interesujące nas dane
- Nazwę
- Adres email odbiorcy
- Częstotliwość wysyłania maili
- Okres raportowania
- oraz dzień i godzinę o której będzie wysyłany email

Show:

Name* (Special characters "!", ".", "\" are not allowed)

Description

To email address* (Use comma ";" for multiple mail id's)

Email frequency* Daily Weekly

Report period Previous day Since midnight

Send email at Hour(s)

Sunday Monday Tuesday Wednesday
 Thursday Friday Saturday

Jeśli chcemy usunąć harmonogram raportów przechodzimy do *Show Reports settings* → *Report scheduling*. Tutaj możemy dodawać i usuwać raporty oraz jest również możliwość wysłania maila testowego.

<input type="checkbox"/>	Name	Report group/bookmark	Email frequency	To email address	Last sent time
<input type="checkbox"/>	test	User App Risks & Usage	Daily	test@gmail.com	Not sent

Sporządził:
Dominik Jurczyński