

STORMSHIELD

NEXT GENERATION FIREWALL PODRĘCZNIK UŻYTKOWNIKA

Stormshield v4 Ostatnia aktualizacja: 2020-01-19 | Opracowanie: DAGMA sp. z o.o.





SPIS TREŚCI

1.	Informacje wstępne	3
2.	Instalacja urządzenia STORMSHIELD UTM	7
3.	Pierwsze podłączenie do urządzenia	9
4.	Podstawowa konfiguracja	15
5.	Tryb pracy urządzenia	24
6.	Konfiguracja interfejsów sieciowych	28
7.	Routing (trasowanie połączeń)	32
8.	Konfiguracja zapory (firewall)	38
9.	Konfiguracja translacji adresów (NAT)	48
10.	System wykrywania i blokowania włamań ASQ (IPS)	53
11.	Konfiguracja Audytu podatności (SEISMO)	59
12.	Autoryzacja użytkowników	61
13.	Wirtualne sieci prywatne (VPN)	82
14.	Konfiguracja proxy HTTP, SMTP, POP3, FTP, SSL	107
15.	Konfiguracja serwera DHCP	114
16.	Klaster wysokiej dostępności (HA)	116
17.	Wsparcie dla protokołu IPv6	121
18.	MONITOROWANIE	123
19.	LOGI	125
20.	STORMSHIELD VISIBILITY CENTER	129
21.	RAPORTY	132
22.	Najczęściej zadawane pytania (FAQ)	134

2





1. Informacje wstępne

Urządzenia STORMSHIELD UTM (Unified Threat Management) integrują w jednej obudowie podstawowe elementy niezbędne do kompletnego zabezpieczenia sieci korporacyjnej. STORMSHIELD UTM to firewall, system wykrywania i blokowania włamań IPS (Intrusion Prevention System), serwer VPN, system antywirusowy, system antyspamowy, system filtrowania dostępu do stron internetowych (filtr URL) oraz system monitorowania bezpieczeństwa sieci.

Ogólnopolskim dystrybutorem rozwiązań STORMSHIELD jest firma DAGMA Sp. z o.o., która świadczy również wsparcie techniczne dla wszystkich klientów, którzy zakupili urządzenia STORMSHIELD UTM w polskim kanale dystrybucyjnym.







Zestawienie najważniejszych parametrów poszczególnych modeli STORMSHIELD UTM:

	SNi40	SN160	SN160W	SN210	SN210W	SN310
Liczba interfejsów 1 Gb	5 0-2***	1+4(switch)	1+4(switch)	2+6(switch)	2+6(switch)	8
WiFi	-	-	802.11 a/b/g/n 2 x SSID	-	802.11 a/b/g/n 2 x SSID	-
Przepustowość FW+IPS [Gbps]	2,9	1	1	1,6	1,6	2,4
Przepustowość antywirus [Gbps]	-	0,26	0,26	0,4	0,4	0,49
Przepustowość IPsec -AES [Gbps]	1,1	0,2	0,2	0,35	0,35	0,6
Liczba jednoczesnych połączeń	500 000	150 000	150 000	200 000	200 000	300 000
Liczba nowych połączeń/sek	20 000	6 000	6 000	15 000	15 000	18 000
VLAN 802.1Q	64	64	64	64	64	64
Tunele IPsec VPN	500	50	50	50	50	100
Portal SSL VPN	75	20	20	20	20	50
Tunele SSL VPN	100	5	5	20	20	20
Dysk twardy	32GB	Karta SD*	Karta SD*	Karta SD*	Karta SD*	Karta SD*

	SN510	SN710	SN910	SN2100	SN3100	SN6100
Liczba interfejsów 1 Gb	12	8–16** 0–8***	8-16** 2-10***	2–26** 0–24 ***	2–26** 0–24***	8–64** 0–64***
Przepustowość FW+IPS [Gbps]	3,3	8	15	35	55	68
Przepustowość antywirus [Gbps]	0,95	2	2,9	7	10	12,5
Przepustowość IPsec -AES [Gbps]	1	2,4	4	8	10	20,5
Liczba jednoczesnych połączeń	500 000	1 000 000	1 500 000	2 500 000	5 000 000	20 000 000
Liczba nowych połączeń/sek	20 000	40 000	60 000	100 000	130 000	146 500
VLAN 802.1Q	256	256	512	1 024	1 024	1 024
Tunele IPsec VPN	500	1 000	1 000	5 000	5 000	10 000
Portal SSL VPN	75	150	300	1 024	1 024	2048
Tunele SSL VPN	100	150	150	400	500	500
Dysk twardy	≥ 250GB	≥ 250GB	≥120GB	≥ 250GB	≥ 250GB	≥ 500GB

* Opcja

** Porty miedziane – 1 Gb / 10 Gb

*** Porty światłowodowe – 1 Gb / 10 Gb / 40 Gb (SN2100, SN3100, SN6100)

Każde urządzenie niezależnie od jego wielkości wyposażone jest w ten sam moduł Firewall oraz Intrusion Prevention System. Urządzenia różnią się liczbą interfejsów oraz parametrami związanymi z wydajnością (przepustowość, liczba połączeń, liczba obsługiwanych kanałów VPN). Urządzenia od SN160 do SN310 mają możliwość podłączenia karty SD, a od modelu SN510 urządzania wyposażone są w dysk twardy.

Doboru urządzenia dokonuje się na podstawie charakterystyki sieci (liczba stacji roboczych, liczba serwerów, liczba nowych / jednoczesnych sesji na sekundę, itp.). W przypadku jakichkolwiek wątpliwości prosimy o kontakt z pomocą techniczną na adres mailowy pomoc@stormshield.pl.

4





Wsparcie Techniczne

W ramach ważnego serwisu użytkownicy rozwiązań STORMSHIELD mają dostęp do wsparcia technicznego w języku polskim. Dział wsparcia technicznego jest dostępny dla Państwa od poniedziałku do piątku w godzinach od 8⁰⁰ do 18⁰⁰ pod numerem telefonu 32 259 11 89. Problemy techniczne można również zgłaszać drogą elektroniczną na adres pomoc@stormshield.pl lub przy użyciu <u>formularza zgłoszeniowego</u> dostępnego na stronie <u>www.stormshield.pl</u>.

Gwarancja na urządzenia

W ramach podstawowej licencji urządzenia STORMSHIELD UTM dostarczone są z podstawowym serwisem gwarancyjnym (STANDARD EXCHANGE). Gwarancja ta określa, iż w przypadku awarii urządzenia zostanie ono wymienione na sprawne w okresie 14 dni roboczych. Istnieje możliwość zakupu specjalnego serwisu zapewniającego wymianę urządzenia na następny dzień roboczy (NEXT BUSINESS DAY/EXPRESS EXCHANGE – tzw. NBD). Co do szczegółów dotyczących tej licencji oraz jej wyceny prosimy o kontakt na adres mailowy kontakt@stormshield.pl lub telefonicznie 32 259 11 00.

Podstawowe funkcje STORMSHIELD UTM:

- Stateful Inspection Firewall,
- Instrusion Prevention System/Intrusion Detection System (IPS/IDS),
- wsparcie protokołów IPv4 i IPv6,
- VPN Server (IPsec VPN, Full SSL VPN, Portal SSL VPN, PPTP VPN),
- uwierzytelnianie i integracja z Microsoft Active Directory lub LDAP,
- kształtowanie pasma (QoS),
- zarządzanie wieloma łączami do Internetu równoważenie obciążenia / brama zapasowa,
- skaner antywirusowy ClamAV (http, pop3, smtp, ftp, ssl),
- moduł antyspam,
- filtrowanie stron WWW (http, https),
- centrum certyfikacji PKI,
- serwer DHCP,
- klient NTP,
- monitorowanie w czasie rzeczywistym,
- logowanie zdarzeń,
- tworzenie raportów TOP10,
- STORMSHIELD Visibility Center system raportowania.

Wszystkie wymienione wyżej funkcje są dostępne w ramach podstawowej licencji. Funkcje wymagające zakupu rozszerzonej licencji:

- Audyt Podatności pasywny skaner zagrożeń (SEISMO),
- zaawansowany skaner antywirusowy (http, pop3, smtp, ftp, ssl),
- rozszerzone filtrowanie stron WWW (http, https) w chmurze STORMSHIELD,
- Stormshield Breach Fighter sandboxing bazujący na chmurze,
- Obsługa protokołów przemysłowych (BACnet/IP, CIP, EtherNet/IP, IEC-60870-5-104, Modbus, OPC UA, OPC (DA/HDA/AE), PROFINET IO / RT, UMAS, S7 200-300-400)





Szkolenia techniczne

Firma Dagma Sp. z o.o. jest autoryzowanym centrum szkoleniowym dla rozwiązań STORMSHIELD. Wszystkie informacje na temat szkoleń technicznych znajdują się na stronie: <u>https://www.acsdagma.com</u>.







2. Instalacja urządzenia STORMSHIELD UTM

Urządzenia STORMSHIELD UTM dostarczone są w białym kartonie zabezpieczonym taśmą z logo firmy DAGMA. Wewnątrz znajduje się oryginalne opakowanie, na którym widoczna jest naklejka z informacją o modelu i numerze seryjnym urządzenia. Oryginalne opakowanie zabezpieczone jest przed otwarciem przeźroczystą taśmą. W przypadku braku bądź uszkodzenia którejkolwiek z taśm prosimy o kontakt ze sprzedawcą lub firmą DAGMA Sp. z o.o..

Po otrzymaniu urządzenia zalecamy przeprowadzenie następujących czynności:

- 1. weryfikacja zawartości opakowania STORMSHIELD UTM,
- 2. analiza sposobu podłączenia urządzenia do sieci firmowej.

Weryfikacja zawartości opakowania.

W zależności od modelu, zawartość opakowania może być różna. Dla modeli bez dysku twardego (SN160(W), SN210(W), SN310) opakowanie powinno zawierać:

- urządzenie STORMSHIELD UTM etykieta na opakowaniu i etykieta na urządzeniu muszą mieć ten sam numer seryjny. Urządzenie musi posiadać oryginalną nienaruszoną plombę (sticker),
- kabel Ethernet RJ45,
- kabel konsolowy USB A-B lub RS-232 RJ45 (w zależności od modelu),
- kabel zasilający,
- zasilacz 12V/3.33A (SN160, SN160W, SN210, SN210W, SN310),
- quick start guide.









Urządzenie STORMSHIELD UTM można skonfigurować przy wykorzystaniu przeglądarki internetowej za pomocą interfejsu WebGUI lub z poziomu wiersza poleceń (CLI).

Analiza sposobu podłączenia urządzenia do sieci firmowej.

Urządzenie może pracować w trzech trybach (transparentny, router lub mieszany). Domyślnym trybem pracy jest transparentny. W zależności od potrzeb należy wybrać odpowiedni tryb pracy. Różnice pomiędzy tymi trybami pracy zostały opisane w dalszej części instrukcji (sekcja 5 – Tryb pracy). Zachęcamy do zapoznania się z tą sekcją w celu wyboru właściwego trybu pracy urządzenia.







3. Pierwsze podłączenie do urządzenia

Zaleca się aby pierwszego podłączenia do urządzenia dokonać, gdy:

- zweryfikowano zawartość opakowania,
- wybrano sposób podłączenia urządzenia STORMSHIELD UTM do sieci.

\rm Uwaga!

Urządzenie STORMSHIELD UTM można podłączyć do zasilania jedynie przy pomocy zasilacza dostarczonego przez producenta. Jeżeli istnieje podejrzenie, iż zasilacz jest uszkodzony lub widoczne są mechaniczne uszkodzenia wtyku/gniazda zasilacza należy zaniechać podłączenia i zgłosić zaistniałą sytuację na pomoc@stormshield.pl

Uwaga!

Urządzenie STORMSHIELD UTM należy podłączyć do zasilania poprzez listwę zabezpieczająca przed przepięciami lub z wykorzystaniem urządzenia UPS.

Uwaga!

Wyłączenie urządzenia STORMSHIELD UTM z zasilania musi odbywać się zgodnie z zaleceniami producenta. Służy do tego odpowiednia opcja dostępna z konsoli WebGUI w sekcji *Konfiguracja* >*Moduły* > *USTAWIENIA SYSTEMOWE* > *System* > *Konfiguracja* > *System* > *Zatrzymaj* lub polecenie **halt** z linii poleceń.

Podłączenie do urządzenia jest możliwe przy wykorzystaniu:

- przeglądarki WWW (wspierane przeglądarki: Firefox, Chrome, Edge),
- klienta SSH (np. PuTTY),
- portu konsolowego USB lub RS-232 (np. PuTTY),
- klawiatury oraz monitora bezpośrednio podłączonych do urządzenia (wybrane modele).

W domyślnej konfiguracji modyfikację ustawień urządzenia możemy wykonać przy użyciu konsoli WWW (domyślny, zalecany sposób) bądź bezpośrednio korzystając z portu konsolowego (dla użytkowników zaawansowanych). W dalszej konfiguracji można dodatkowo włączyć dostęp SSH.

Konsola WebGUI urządzenia dostępna jest domyślnie pod adresem **https://10.0.0.254/admin** W celu dokonania wstępnej konfiguracji urządzenia zalecamy podłączyć komputer do portu **nr 2**, który domyślnie jest skonfigurowany pod nazwą IN.

Na poniższym rysunku zaznaczono ten port kolorem zielonym:





Komputer podłączony do tego portu otrzyma z serwera DHCP adres IP z zakresu 10.0.0.10-10.0.0.100 z maską 255.0.0.0.

🕕 Uwaga

Jeżeli kabel Ethernet nie zostanie podłączony do prawidłowego portu to nie będzie możliwe podłączenie się do urządzenia poprzez przeglądarkę (WebGUI). Przełączanie się pomiędzy interfejsami urządzenia może uruchomić tzw. Antispoofing Mechanism, który zablokuje cały ruch IP z komputera do urządzenia. Należy wtedy ponownie uruchomić urządzenie. Do ponownego uruchomienia urządzenia z poziomu CLI można użyć polecenia **reboot**.

Widok urządzenia SN510:





- 1. Diody przy interfejsach:
 - lewa stan pracy interfejsu światło ciągłe oznacza połączenie, miganie oznacza transfer danych,
- prawa szybkość interfejsu wyłączona 10Mbps, kolor zielony 100 Mbps, kolor żółty 1Gbps.
- 2. Przycisk przywrócenia konfiguracji do ustawień fabrycznych (brak opisu).
- 3. Port konsoli urządzenia (RJ45 RS-232).
- 4. Diody sygnalizujące stan systemu (od góry):
- urządzenie w trybie online (urządzenie gotowe do pracy), w przypadku konfiguracji klastra HA migająca dioda oznacza urządzenie pasywne,
 - uruchamianie/zatrzymywanie systemu operacyjnego,
 - sygnalizacja stanu zasilania (dioda pomarańczowa).
- 5. Przycisk restartu urządzenia (opis: RESET).

Konsola STORMSHIELD WebGUI

Dostęp do konsoli WebGUI można uzyskać po podaniu loginu i hasła. Konfiguracja pozwala także na autoryzację z wykorzystaniem certyfikatu SSL. Wymaga to jednak wcześniejszej konfiguracji serwera PKI na urządzeniu.

Pozycja *"Opcje"* pozwala zmienić język interfejsu lub zalogować się z uprawnieniami *"tylko do odczytu"*. W domyślnej konfiguracji do konsoli można dostać się przy użyciu następujących poświadczeń:

- użytkownik: admin
- hasło: admin





STORMSHIELD Network Security	
admin Caloguj z wykorzystaniem certyfikatu SSL POŁĄCZENIE Opcje	
Polski 🔹	

Pomyślna autoryzacja na urządzeniu spowoduje wyświetlenie interfejsu urządzenia – WebGUI.

W przypadku firmware 4.x różni się on od wcześniejszych wersji i został podzielony na dwie zakładki – Monitoring oraz Konfiguracja [1]. Po lewej stronie ekranu [2] znajduje się menu z opcjami konfiguracji / monitoringu.

W zakładce Monitoring administratorzy mogą monitorować działanie samego urządzenia, jak i ruch przechodzący przez urządzenie oraz przeglądać zarejestrowane logi.

W zakładce Konfiguracja administratorzy mają możliwość konfiguracji urządzenia.

Zaletą takiego podziału interfejsu jest możliwość przełączania się pomiędzy zakładkami, bez utraty stanu obecnej pracy.

Przykładowo, jeżeli administrator konfiguruje regułę firewall i w trakcie tej konfiguracji, jeszcze przed jej zapisem, potrzebuje sprawdzić coś w logach urządzenia, wystarczy, że przełączy się do zakładki Monitoring, gdzie sprawdzi potrzebne dane, a następnie powróci do edycji reguły firewall, która będzie w takim stanie jaką ją pozostawił.



Network Security		FIGURACJA EVA1 VMSNSX09C0035A9				😝 admin 👻 🖾 zapis / 🗏 ogra	NICZONY DOS	
★- «	CA DANEL KONTROL NV							
PANEL KONTROLNY	PANEL KONTROENT							
🗐 KONFIGURACJA LOGÓW 🕂	SIEĆ		OCHRONA					Û
			Data 4	Wiadomość	Akcja Prior	ytet Źródło	Cel	
I RAPORTY +	1	2345678	E Active Updat	s undate failed Already r	unning (Clamay) (2)		^	
MONITOROWANIE -			27 12 2019 15	Active Undate: und	(ciantav) (2)	lieki		
Szukaj	_		27.12.2019.15	Active Update: upd	- N	lieki		
			27.12.2019 13	Active opdate: upd	- P	ISKI		
Sprzęt / Klaster HA	WŁAŚCIWOŚCI		E Active Update	e: update failed Already ru	unning (Kaspersky) (1)		
System	Nazwa:	VMSNSX09C0035A9	15:10:53	Active Update: upd	· N	liski		
Interfejsy	Model:	EVA1	E Active Update	e: update failed Already r	unning (Patterns) (7)			
0-0	Model EVA:	EVA1	15:11:14	Active Update: upd	× N	liski		
2005 2	Pojemność pamięci EVA:	1 GiB (Minimalnie 1 GiB - Maksymalnie 2 GiB) 🕕	15:10:53	Active Update: upd	🏩 N	liski		
Hosty	Ilość procesorów w EVA:	CPU 1 (Maksymalnie CPU 1) 💶	27.12.2019 15	Active Update: upd	🏩 N	liski		
Użytkownicy	Numer seryjny:	VMSNSX09C0035A9	27.12.2019 15	Active Update: upd	🗶 N	liski		
Polaczonia	Wersja:	4.0.1	27.12.2019 15	Active Update: upd	🏩 N	liski		
Folgezenia	Czas pracy:	18d 1h 5m 54s	27.12.2019 15	Active Update: upd	🗶 N	liski		
Bramy	Data:	14.01.2020 15:15:30	27.12.2019 14	Active Update: upd	(A) N	liski		
DHCP	Data wygaśnięcia serwisu:	04.07.2020		riotre opuater opua		Haki		
Tunele SSL VPN			Active Update	e: update failed Already ru	unning (Pvm) (2)		> ×	
			STAN URZAD	ZENIA				
Tunele IPSec VPN			o hard ones to	LLINA				
Białe / czarne listy								
				_		610		а.
						3 15		
				LINK HA	ZASILANIE	WENTYLATOR		
	001001			CPU	PAMIĘĆ	DYSK		
						- 🚯 🗸		
		-		RAID	TEMPERATURA	CERTYFIKATY		~

Network Security	MONITORING KONFIGURACJA EV	АТ именехорсоозбар	🕒 admin 🔻	?
*- «	址 USTAWIENIA SYSTEMOWE / KONEIGURA			
🔅 MODUŁY –				
Szukaj	USTAWIENIA OGÓLNE DOSTEP ADMINISTRA	CYJNY USTAWIENIA SIECIOWE		
料 USTAWIENIA SYSTEMOWE	Ustawienia ogólne			î
KONFIGURACJA SIECI	Nazwa urządzenia UTM:	VMSNSX09C0035A9		- 1
S OBIEKTY	Język (logi):	Angielski 👻		
	Układ klawiatury:	Polski 👻		
POLITYKI OCHRONY				- 1
🖉 KONTROLA APLIKACJI	Ustawienia szyfrowania			
🖾 POŁĄCZENIA VPN		Włącz regularne pobieranie listy CRL		- 1
ADMINISTRACJA		Włącz tryb "ANSSI Diffusion Restreinte (DR)"		
				- 1
2	Polityka hasei			
_	Minimalna długość hasła:	8		- 1
	Wymagane typy znaków:	Hasło musi zawierać litery i cyfry 🔹		
				- 1
	Ustawienia czasu - 14.01.2020 15:46:45			- 1
		Tryb ręczny		
		Synchronizuj datę z komputerem - 14.01.2020 15:46:46		
		Klient NTP		
	Strefa czasowa:	Europe/Warsaw 👻		
	LISTA SERWERÓW NTP			~
OBIEKTY		X ANULUJ V ZASTOSUJ		

Pomoc kontekstowa

W prawym górnym rogu interfejsu WebGUI, po kliknięciu na znak zapytania otworzy się dokumentacja opisująca poszczególne elementy i funkcje interfejsu WebGUI.

Pomoc działa w sposób kontekstowy tj. po kliknięciu znaku zapytania otwierana jest dokumentacja do aktywnego modułu konfiguracji urządzenia.

Dokumentacja ta dostępna jest jedynie w języku angielskim i francuskim.











USER MANUAL WELCOME ACCESS PRIVILEGES ACTIVE UPDATE LOGS - AUDIT LOGS ADMINISTRATORS ANTISPAM ANTIVIRUS APPLICATIONS AND PROTECTIONS AUTHENTICATION BLOCK MESSAGES CERTIFICATES AND PKI CLI CONSOLE

CONFIGURATION

"General configuration" tab "Firewall administration" tab "Network settings" tab CONFIGURATION OF MONITORING

DASHBOARD

DHCP

CONFIGURATION

The configuration-administration screen consists of 3 tabs:

- General configuration: definition of the firewall's settings (name, language, keyboard), date and time settings and NTP servers.
- Firewall administration: configuration of access to the firewall's administration interface (listening port, SSH etc.)
- Network settings: Ipv6 activation, configuration of the proxy server and DNS resolution.

"General configuration" tab "Firewall administration" tab "Network settings" tab





4. Podstawowa konfiguracja

Po pierwszym zalogowaniu się do urządzenia należy zweryfikować poprawność licencji. Można to zrobić w menu konfiguracji licencji (KONFIGURACJA > USTAWIENIA SYSTEMOWE > Licencje -> LICENCJA UTM ...)

Network Security	MONITORING KONFIGURACJA EVA1 VMSNSX09CC		● admin → ZAPIS / © OGRANICZONY DOS	?
** « MODUŁY –	料 USTAWIENIA SYSTEMOWE / LICENCJE			
Szukaj 🧩 🦨	INFORMACJE LICENCJA UTM VMSNSX09C0035A9			
11 USTAWIENIA SYSTEMOWE	Szukaj × Sprawdź dostępność nowej licencji Akt	ywuj nową licencję 📔 🧩 🖃 📔		
Konfiguracja urządzenia	Szczegóły licencji - serwisu dla urządzenia 🔺	Status opcji		
Administratorzy	Administracja (3 Elementy)			
Liespeie	SN Global Administration	Dostępne		
Licencje	Realtime Monitor	Dostępne		- 1
System	Event Analyzer	Dostępne		
Aktualizacje	Subskrypcje sygnatur (14 Elementy)			
Klaster HA	AntySPAM	9 Sobota 04 Lipiec 2020		
Management Center	Antywirus	O Sobota 04 Lipiec 2020		
Wieroz polocoń	Gwarancja typu Priviledge	🖉 Brak opcji w serwisle		
Wersz polecen	Przemysłowe	Sobota 04 Lipiec 2020		
KONFIGURACJA SIECI	Przedłużenie licencji/gwarancji nie później niż	Czwartek 31 Grudzień 2037		
S OBIEKTY	Sygnatury	Sobota 04 Lipiec 2020		
	Vaderetro	0 Sobota 04 Lipiec 2020		
POLITYKI OCHRONY	Sandboxing Breach Fighter	Sobota 04 Lipiec 2020		
	Filtr URL	Sobota 04 Lipiec 2020		
V KONTROLA APEIRACJI	Extended Web Control	Sobota 04 Lipiec 2020		
D POŁĄCZENIA VPN	Aktualizacja	9 Sobota 04 Lipiec 2020		
ADMINISTRACJA	Kaspersky	9 Sobota 04 Lipiec 2020		
	Audyt Podatności	0 Sobota 04 Lipiec 2020		
	Gwarancja podstawowa	Sobota 04 Lipiec 2020		
	Opcje dodatkowe (7 Elementy)			
	Tworzenie sygnatur	Dostępne		
	Gwarancja typu Priviledge	Niedostępne		
	Zewnętrzny serwer LDAP	Dostępne		
	Status klastra HA	Master		~
SODIERT				

Wstępną konfigurację można podzielić na następujące etapy:

- konfiguracja ustawień WebGUI,
- ogólne ustawienia dotyczące samego urządzenia,
- konfiguracja/zmiana hasła dla użytkownika admin,
- konfiguracja obiektów,
- konfiguracja interfejsów urządzenia (trybu pracy),
- konfiguracja usługi DHCP,
- ustawienie bramy domyślnej na urządzeniu (routing),
- konfiguracja zapory (firewall),
- konfiguracja translacji adresów (NAT).

15





Konfiguracja ustawień WebGUI

W pierwszej kolejność należy skonfigurować parametry panelu administracyjnego WebGUI. W tym celu należy użyć przycisku Konfiguracja, który znajduje się w menu dostępnym po kliknięciu nazwy zalogowanego użytkownika w prawym górnym rogu interfejsu WebGUI.

		e admin	•	2
		Obniż uprawni	enia	а
		Uzyskaj upraw	nie	nia do wrażliwych danych (logów)
	×	Konfiguracja		
Į	₽	Wyloguj		

Zmiany w konfiguracji w tej części są aktywowane automatycznie w chwili ustawienia nowej wartości (nie ma potrzeby zatwierdzania zmian).

Przywróć ustawienia domyślne					
Ustawienia uwierzytelnienia					
Maksymalny okres bezczynności :	Zaloguj automatycznie (certyfikat SSL) bez ograniczeń				
Ustawienia interfejsu					
Liczba reguł filtrowania na stronie :	Zawsze wyświetlaj opcje zaawansowane Wyświelt przycisk Zapisz komendy Wczytaj użytkowników/grupy po wybraniu modulu Wczytaj obiekty sieciowe po wybraniu modulu Wyświetl globalne polityki ochrony (Filtering, NAT oraz IPSec VPN) Dodaj domyślne komentarze do reguł Firewall i NAT Automatycznie				
Konfiguracja interfejsu użytkownika					
	Przeszukuj wszystkie właściwości obiektu				
	Wyłącz analizator reguł w czasie rzeczywistym				
	 Niedziela rozpoczyna tydzien Zatwierdź zmiany przed wysłaniem do urządzenia 				
Pliki pomocy i narzędzia administracyj	Pliki pomocy i narzędzia administracyjne (konfiguracja odnośników)				
Podręcznik użytkownika :	http://documentation.stormshield.eu/go				
Opis alarmów i komunikatów :	https://securitykb.stormshield.eu				
Pakiet administracyiny :	http://qui stormshield eu				

Ustawienia uwierzytelnienia

- Zaloguj automatycznie (certyfikat SSL) uruchamia automatyczne logowanie do WebGUI w przypadku, gdy mamy zaimportowany certyfikat SSL użytkownika o uprawnieniach administracyjnych.
- Maksymalny okres bezczynności pozwala określić czas (domyślnie 5 min), po którym nastąpi automatyczne wylogowanie z konsoli w wypadku braku aktywności.

Ustawienia interfejsu

W tej sekcji można zdecydować aby opcje Zaawansowane, które domyślnie są zwinięte, były zawsze rozwinięte i widoczne w oknie konfiguracyjnym.





Zaznaczenie opcji *Wczytaj użytkowników/grupy po wybraniu modułu* oraz *Wczytaj obiekty sieciowe po wybraniu modułu* spowoduje, iż w modułach konfiguracji użytkowników i obiektów sieciowych elementy te zostaną wyświetlone po przejściu do tych sekcji. Gdy opcja ta jest odznaczona użytkownicy bądź obiekty sieciowe będą wczytane dopiero po wybraniu odpowiedniego filtra (np. tylko obiekty typu host). Zaznaczenie opcji *Wyświetl globalne polityki ochrony* spowoduje pojawienie się w konfiguracji Firewall i NAT, IPsec VPN oraz Obiekty sieciowe ustawień globalnych, współdzielonych przez wszystkie urządzenia centralnie zarządzane z wykorzystaniem serwera centralnego zarządzania Stormshield Management Center (SMC).

Dostęp do danych wrażliwych

W celu zapewnienia zgodności z rozporządzeniem GDPR (RODO) dane osobowe takie jak nazwa użytkownika, źródłowy adres IP, źródłowy adres MAC, nazwa hosta źródłowego, domyślnie nie są prezentowane w logach i raportach i są zastąpione słowem *Anonymized*. W celu uzyskania dostępu do tych danych administrator musi kliknąć na opcję *Uzyskaj dostęp do wrażliwych danych (logów)* znajdującą się w menu dostępnym po kliknięciu nazwy zalogowanego użytkownika w prawym górnym rogu interfejsu WebGUI.

Ogólne ustawienia dotyczące samego urządzenia

Ogólnych ustawień urządzenia dokonujemy w sekcji KONFIGURACJA > USTAWIENIA SYSTEMOWE > Konfiguracja urządzenia.

W pierwszej zakładce, **Ustawienia ogólne**, można skonfigurować m.in. nazwę urządzenia, język (kodowanie znaków w logach) i wybrać układ klawiatury. Można tutaj również skonfigurować politykę haseł, czas urządzenia oraz strefę czasową. Alternatywnie można wskazać serwer NTP (serwer czasu), z którym STORMSHIELD UTM będzie synchronizował czas.







Network Security	MONITORING KONFIGURACJA EVA1 VMSNSX09C0035A9
*- «	
🌣 MODUŁY 🚽	
Szukaj 🗶 🖉	USTAWIENIA OGÓLNE DOSTEP ADMINISTRACYJNY USTAWIENIA SIECIOWE
뷰 USTAWIENIA SYSTEMOWE	Ustawienia ogólne
Konfiguracja urządzenia	Nazwa urządzenia UTM: VMSNSX09C0035A9
Administratorzy	Język (logi): 🔹
Licencje	Układ klawiatury: Polski 💌
System	
Aktualizacje	Ustawienia szyfrowania
Klaster HA	Włącz regularne pobieranie listy CRL
Management Center	□ Włącz tryb "ANSSI Diffusion Restreinte (DR)"
Wiersz poleceń	
KONFIGURACJA SIECI	Polityka haseł
S OBIEKTY	Minimalna długość hasła: 8
LŻYTKOWNICY	Wymagane typy znaków: Hasło musi zawierać litery i cyfry 💌
POLITYKI OCHRONY	
🕅 KONTROLA APLIKACJI	Ustawienia czasu - 15.01.2020 11:54:17
DOŁĄCZENIA VPN	Tryb ręczny
I ADMINISTRACJA	Synchronizuj datę z komputerem - 15.01.2020 11:54:18
	Klient NTP
S OBIEKTY	× ANULUJ × ZASTOSUJ

Zakładka **Dostęp administracyjny** pozwala skonfigurować dostęp do urządzenia. Znajdziemy tutaj między innymi możliwość ustawienia portu, na którym będzie działał portal administracyjny (domyślnie jest to port https – 443 TCP), adresu/adresów IP które będą miały dostęp do WebGUI oraz mechanizmu zapobiegania atakom typu *Brute Force*.

W dolnej części okna można włączyć dostęp do urządzenia poprzez konsolę SSH.

18



Y //	

4	Network Security	MONITORING KONFIGURACJA	EVA1 умблаховсоозбая					
*	★ • • • • • • • • • • • • • • • • • • •							
Szu		USTAWIENIA OGÓLNE DOSTEP ADMINISTRACYJNY USTAWIENIA SIECIOWE						
141		Dostęp do interfejsu administracyjnego						
	Konfiguracia urządzenia		🕼 Dozwól na uwierzytalnianie użytkownika 'admin' hasłam					
	Administratorzy	Numer portu dla konsoli www:	https					
	Licencje		Konfiguracja certyfikatu SSL					
	System		🗷 Ochrona przed atakiem BruteForce					
	Aktualizacje	Liczba dozwolonych prób uwierzytelnienia:	3					
	Klaster HA	Czas wstrzymania (minuty):	1					
	Management Center	LISTA ADMINISTRACYJNYCH ADRESÓW IP						
	Wiersz poleceń	+ Dodaj X Usun zakres - sieć - host - grupa hostów						
	KONFIGURACJA SIECI	Network_internals						
0))	OBIEKTY							
•	UŻYTKOWNICY							
⇒₽	POLITYKI OCHRONY	Regulamin dostępu do panelu administracyjn	ego					
$\overline{\mathbf{O}}$	KONTROLA APLIKACJI	Regulamin:	•					
•	POŁĄCZENIA VPN		🕁 Usuń regulamin					
(j)	ADMINISTRACJA							
		Ustawienia dostępu SSH						
			🕑 Włącz dostęp SSH 🥹					
		Numer restu dia service COU	Pozwól na dostęp z użyciem hasła					
		Numer portu dia serwera SSH:	S511 V St					

Jeśli STORMSHIELD UTM do komunikacji z Internetem musi łączyć się przez zewnętrzny serwer Proxy, to w zakładce **Ustawienia sieciowe** można skonfigurować dane dostępowe do tego serwera.

Można tutaj również wskazać z jakich serwerów DNS ma korzystać STORMSHIELD UTM przy rozwiązywaniu nazw. Skonfigurowanie tej opcji jest niezbędne do poprawnego pobierania aktualizacji przez urządzenie.

Zakładka ta umożliwia również uruchomienie wsparcia dla protokołu IPv6 tj. filtrowania, analizowania ruchu IPv6 oraz działania usługi dhcpv6.

\rm Uwaga!

Włączenie wsparcia dla IPv6 wymaga restartu urządzenia, ponadto operacji tej nie można cofnąć. Dlatego przed jej uruchomieniem należy koniecznie wykonać backup konfiguracji.







Network Security	MONITORING KONFIGURACJA EVA1 VMSNSX09C0035A9
** « MODUŁY –	밖 USTAWIENIA SYSTEMOWE / KONFIGURACJA URZĄDZENIA
Szukaj 💉 🖉	USTAWIENIA OGÓLNE DOSTEP ADMINISTRACYJNY USTAWIENIA SIECIOWE
뷰 USTAWIENIA SYSTEMOWE	Wsparcie dla IPv6
Konfiguracja urządzenia	WYŁĄCZ
Administratorzy	
Licencje	Ustawienia proxy dla urządzenia
System	WYŁĄCZ
Aktualizacje	
Klaster HA	Ustawienia serwerów DNS dla urządzenia
Management Center	LISTA SERWERÓW DNS
Wiersz poleceń	+ Dodaj 🗙 Usuń
KONFIGURACJA SIECI	Serwery DNS (host)
S OBIEKTY	one.one
	ans I.googie.com
POLITYKI OCHRONY	

Konfiguracja/zmiana hasła dla użytkownika admin

Pierwsze logowanie do urządzenia odbywa się z użyciem konta *admin* i hasłem *admin*. Hasło admin jest hasłem startowym. Należy je zmienić zaraz po pierwszym logowaniu. Można tego dokonać w sekcji KONFIGURACJA > USTAWIENIA SYSTEMOWE > Administratorzy w zakładce Konto Administratora.

Network Security	MONITORING KONFIGURACJA EVA1 vmsnsx09c0035a9	
★ • «	밖 USTAWIENIA SYSTEMOWE / ADMINISTRATORZY	
SZUKAJ · · · · · · · · · · · · · · · · · ·	Uwierzytelnianie	
Konfiguracja urządzenia Administratorzy	Hasło: •••••• Potwierdź hasło: ••••••	
Licencje System	Silne	
Aktualizacje Klaster HA	Klucz prywatny: " Pobierz klucz prywatny	
Management Center Wiersz poleceń	Klucz publiczny: "Pobierz klucz publiczny	

W tej zakładce znajdują się również klucze (prywatny i publiczny), umożliwiające logowanie do urządzenia poprzez SSH bez konieczności podawania hasła.





Uwaga!

Konto admin jest jedynym kontem, które ma możliwość logowania się go usługi SSH.

Konfiguracja obiektów

Obiekty to podstawowy element konfiguracji STORMSHIELD UTM. Obiekt symbolizuje element sieci komputerowej.

Obiekty można podzielić na następujące typy:

- Host (Host) reprezentuje pojedynczy adres IP,
- Nazwa DNS (FQDN) (DNS name (FQDN)) dynamiczny obiekt, który reprezentuje nazwę DNS (FQDN) czyli taką, która może być powiązana z wieloma adresami IP. Obiekty tego typu mogą być użyte jedynie jako adres źródłowy lub docelowy reguł firewall. Nie można ich grupować,
- Sieć (Network) adres IP i maska. Obiekt reprezentuje wszystkie adresy IP we wskazanej sieci,
- Zakres (IP address range) zakres adresów IP wykorzystywany np. w konfiguracji DHCP,
- Router reprezentuje bramy sieciowe dostawców internetowych i relacje w jakich te bramy działają (Load Balancing, Backup Gateways). Obiektu tego typu można użyć zarówno w podstawowej konfiguracji routingu domyślnego jak i w politykach firewall jako routing na podstawie reguł, tzw. Policy Based Routing (PBR),
- Protokół (IP protocol) protokół sieciowy,
- Port (Port) port, na którym nasłuchuje usługa (TCP / UDP/ SCTP),
- Obiekt harmonogramu (Time object) obiekt, który reprezentuje dowolnie zadeklarowany przedział czasu, także w powtarzających się cyklach. Obiekt taki może zostać użyty do aktywacji wybranej reguły firewall wg. wskazanego harmonogramu.

Obiekty odpowiedniego typu można grupować:

- Grupa portów (Port group) grupa obiektów typu port,
- Grupa IP (Group) grupa obiektów, w skład której mogą wchodzić obiekty typu Host, Zakres, Sieć,
- **Grupa lokalizacji (Region group)** grupa obiektów lokalizacji IP, w skład której mogą wchodzić kraje lub kontynenty.

Aby utworzyć nowy obiekt należy przejść do sekcji **KONFIGURACJA > OBIEKTY > Obiekty sieciowe** i kliknąć przycisk **Dodaj**.



Ą	stormshield v4.0.1 Network Security	MONITORING	KONFIGURACJA	VA1 уменехоэсоозбая				😝 admin 👻 🖾 ZAPIS / 🗎 OGRANICZONY DOS	?
*-	«								
∯ N	IODUŁY +	S OBIEKTY/OB	IEKTY SIECIOWE						
S 0	ВІЕКТУ –	Szukaj	× [9	Filtr:Wszystkie 👻 [S] Typ:IPv4 i IPv6 👻					
Szuk		+ Dodaj 🗙 Usu	ní 👁 Sprawdź 🐴 Eksporti	uj ▼ Zaimportuj ▼ 🗚 Zwiń wszystkie	SZCZEC	SÓŁ Y			
SZUK		Typ Używany	Nazwa	Wartość					
Тур	Nazwa	Typ : Nazwa DNS (F	QDN) (1)		Nazwa:		SNS_Support		
•	Internet	Typ : Grupa IP (4)			Opis:				
C	Firewall_out_router		Firewall_all		🖉 Ed	iytuj grupę			
	Firewall_out		Network_internals		Тур	Obiekty w grupie			
Ci i	Firewall_in		rfc5735			support1.stormshie	eld.eu		
	Firewall_dmz1_router		SNS_Support		6	support2.stormshie	ld.eu		
Ci i	Firewall_dmz1	E Typ : Hosty (49)							
	Firewall_dmz2_router								
Ci i	Firewall_dmz2	H Typ : Internet (1)							
l	Firewall_dmz3_router	Typ : Sieć (21)							
	Firewall_dmz3	🗄 Typ : Protokół (29)							
l	Firewall_dmz4_router	Typ : Zakres (1)							
U	Firewall_dmz4	Typ : Port - Zakres	portów (258)						
E G	Firewall_dmz5_router	E Typ : Grupa portów	(15)						
U	Firewall_dm25		(10)						
	Firewall_umzo_router	typ : Harmonogram	1(1)						
U (B	clouduri download ana stor								
6	cloudurl1 one stormshieldes								
6	cloudurl? and stormshieldes								
	cloudurl3-sns stormshieldos								
e R	cloudurl4-sns stormshieldcs								
	cloudurl5-sns.stormshieldcs.				«	< Strona 1	z1 > _ > 4	0	
« <	Strona 1 z1 > > C W	« < Strona	1 z1 > > C	Wyświetlono 1 - 379 z 379		× ANU	LUJ 🗸 KOPI	IUJ 🗸 ZASTOSUJ	

Obiekty można również tworzyć będąc w oknie konfiguracyjnym dowolnego z modułów, jeśli opcja którą chcemy skonfigurować wymaga wskazania obiektu, to poza listą już istniejących obiektów, dostępna jest

również ikona 💁 14, po kliknięciu której otworzy się okno dodawania obiektu odpowiedniego typu.

Tworzenie obiektu typu Host: Obiekt Host reprezentuje powiązanie nazwy z adresem IP (jest to relacja 1:1).

DODAJ OBIEKT		
Host P™ Nazwa DNS (FQDN) P⊟ Sieć Pª Zakres E™ Router B⊞ Grupa IP	Nazwa: Adres IP v4: Adres MAC: Rozwiąż nazwę O Statyczny	stormshield.pl 91.201.154.220 01:23:45:67:89:ab (opcjonalne) Organiczny
 Protokół Port Grupa portów Grupa lokalizacji Obiekt harmonogramu 	Obiekt globalny Opis:	Strona domowa dystrybutora urządzeń Stormshield
	٢	× ZAMKNIJ + UTWÓRZ I POWIEL + UTWÓRZ

NEXT GENERATION FIREWALL PODRĘCZNIK UŻYTKOWNIKA

>





W polu **Nazwa** należy wpisać nazwę pod jaką obiekt będzie widoczny w konfiguracji urządzenia. Może to być nazwa DNS co pozwoli na automatyczne rozwiązywanie nazwy na **Adres IP** w przypadku zaznaczenia opcji **Dynamiczny**. Opcja ta powoduje, że UTM co 5 minut odpytuje serwery DNS o rozwiązanie nazwy obiektu na adres IP. Wybór opcji **Statyczny** powoduje, że powiązanie **Nazwy** i **Adresu IP** jest trwałe i może być zmienione jedynie poprzez edycję obiektu. Do obiektu można również przypisać adresu MAC. Opcja ta jest wykorzystywana w przypadku konfiguracji serwera DHCP i korzystania ze statycznych rezerwacji adresów IP dla komputerów lub do filtrowania ruchu w regułach firewall na podstawie adresu MAC.

\rm 🛛 Uwaga!

Skonfigurowanie pola Adres MAC powoduje stworzenie statycznego wpisu w tablicy ARP urządzenia. Jeśli wartość tego pola będzie inna niż rzeczywisty adres MAC komputera o podanym adresie IP komunikacja z nim nie będzie możliwa.

Konfiguracja pozostałych typów obiektów jest analogiczna jak dla obiektu **Host** z uwzględnieniem charakterystycznych pól dla każdego z tych obiektów.

Uwaga!

STORMSHIELD UTM posiada wstępnie skonfigurowaną pulę obiektów i są to głównie obiekty typu Protokół oraz Port.

Część obiektów jest tworzona na etapie konfiguracji urządzenia i są to np. obiekty reprezentujące adres IP oraz sieć skonfigurowane na interfejsie urządzenia. Nazwy takich obiektów rozpoczynają się od frazy **Firewall_** oraz **Network_**, gdzie po znaku "_" umieszczana jest nazwa interfejsu (np. Firewall_in). Obiekty **Firewall_** oraz **Network_** nie mogą być edytowane, ponadto nie można stworzyć ręcznie obiektu, którego nazwa zaczynałaby się od tych fraz.

🕖 Wskazówka

Informacje o obiektach typu **Host**, **Zakres**, **Sieć**, **Protokół** oraz **Port** przechowywane są w pliku: /usr/Firewall/ConfigFiles/object

Informacje o obiektach typu **Grupa IP** i **Grupa portów** umieszczone są w pliku: /usr/Firewall/ConfigFiles/objectgroup

Informacje o obiektach typu **Router** umieszczone są w pliku: /usr/Firewall/ConfigFiles/router

Synchronizację obiektów dynamicznych można przeprowadzić ręcznie z poziomu wiersza poleceń (SSH lub konsola) używając polecenia: objectsync





5. Tryb pracy urządzenia

Tryb pracy urządzenia STORMSHIELD UTM zależy od roli jaką ma pełnić w sieci. Tryb pracy określa relację pomiędzy interfejsami. Konfiguracja trybu pracy urządzenia odbywa się w sekcji **KONFIGURACJA > KONFIGURACJA SIECI > Interfejsy**.

Urządzenia STORMSHIELD UTM mogą pracować w trzech trybach:

- BRIDGE (transparentny/most),
- ADVANCED (zaawansowany, tryb routera),
- HYBRID (mieszany).

Tryb BRIDGE

Tryb Bridge inaczej jest zwany trybem transparentnym. Jest to tryb, w którym urządzenie jest skonfigurowane domyślnie. W tym trybie wszystkie interfejsy urządzenia należą do tej samej podsieci. Ustawienie adresu IP określone jest na logicznym interfejsie typu BRIDGE, a same interfejsy dziedziczą ten adres. Urządzenie filtruje ruch, który przechodzi pomiędzy interfejsami bez modyfikacji adresów IP (bez translacji NAT).

Schemat topologii:



Przykład konfiguracji:

NEXT GENERATION FIREWALL PODRĘCZNIK UŻYTKOWNIKA



Network Security	MONITORING	KONFIGURAC	JA	EVA1	VMSNSX09C0035A9			
** « * MODUŁY –		A SIECI / INTER	RFEJSY			_	_	
Szukaj	Q Wprowadź filtr	x[≠] x[≉] terfejs	C 4	Edycja ▼ Port ↑	+ Dodaj • × U Typ	Isuń 🔀 Monitor Włączony	Przejdź do monitoringu Adres IPv4	Sprawdź Komentarze
부부 USTAWIENIA SYSTEMOWE	⊡ 📲 bridge				bridge		192.168.0.2/24	
KONFIGURACJA SIECI	i out		_	1	Ethernet, 1 Gb/s			
Interfejsy	in Marcia		*	2	Ethernet, 1 Gb/s Ethernet, 1 Gb/s	🐙 Właczony. Odłacz	onv	
Interfejsy wirtualne	👼 dmz2			4	Ethernet, 1 Gb/s	Włączony, Odłącz	ony	
Routing	👘 dmz3			5	Ethernet, 1 Gb/s	🐙 Włączony, Odłącz	ony	
Routing multicast	m dmz4			6	Ethernet, 1 Gb/s	🐙 Włączony, Odłącz	ony	
Dynamiczny DNS	m dmz5 m dmz6			7	Ethernet, 1 Gb/s Ethernet, 1 Gb/s	📌 Włączony, Odłącz 🐙 Włączony, Odłącz	ony	
Serwer DHCP								
Proxy DNS								

Tryb ADVANCED

Inaczej zwany trybem routera. W tym trybie każdy interfejs ma przypisany adres należący do innej podsieci. Tym samym każdy z interfejsów określa pewną strefę w sieci, stanowi odrębny segment w obrębie firmy. W tym trybie STORMSHIELD UTM pełni rolę routera pomiędzy bezpośrednio podłączonymi do niego sieciami.

Schemat topologii:



Przykład konfiguracji:



Network Security	MONITORING	KONFIGURACJ	A EV/	\1 v	MSNSX09C0035A9			
** «		A SIECI / INTERFI	EJSY					
Szukai	Q Wprowadź filtr	* ** \$	C 🛃 Edy	oja 🔻	+ Dodaj • X	Usuń 🔀 Monitor	Przejdź do monitoringu	Sprawdź
52utuj x ^e <u>x</u> ^e	In	terfejs	Port	1	Тур	Włączony	Adres IPv4	Komentarze
해 USTAWIENIA SYSTEMOWE	im out			1	Ethernet, 1 Gb/s		178.183.0.2/28	
KONFIGURACJA SIECI	in		→	2	Ethernet, 1 Gb/s		192.168.0.1/24	
Interfeiou	👘 DMZ			3	Ethernet, 1 Gb/s		192.168.1.1/24	
interrejsy	👘 dmz2			4	Ethernet, 1 Gb/s	🐙 Włączony, Odłą	czony	
Interfejsy wirtualne	dmz3			5	Ethernet, 1 Gb/s	📈 Wyłączony, Odła	ączony	
Routing	👘 dmz4			6	Ethernet, 1 Gb/s	🚽 Wyłączony, Odła	ączony	
Routing multicast	👘 dmz5			7	Ethernet, 1 Gb/s	🚽 Wyłączony, Odła	ączony	
Dynamiczny DNS	👘 dmz6			8	Ethernet, 1 Gb/s	😾 Wyłączony, Odła	ączony	

Tryb HYBRID

Tryb HYBRID jest to połączenie dwóch poprzednich trybów, przez co nazywany jest również trybem mieszanym. Polega on na takim ustawieniu interfejsów STORMSHIELD UTM, że cześć z nich względem siebie jest w trybie BRIDGE, a część w trybie ADVANCED. Jest to jeden z najczęściej używanych trybów.

Schemat topologii:



Przykład konfiguracji:



A	Network Security	MONITORING	KONFIGURACJA	EVA1	MSNSX09C0035A9			
*	~ «		A SIECI / INTERFEJS	Y				
S71		Q Wprowadź filtr	* * C	🛃 Edycja 👻	+ Dodaj - 🗙 Usu	uń 🔀 Monitor 🛛 🖓 Prz	ejdź do monitoringu	Sprawdź
020	× *	In	terfejs	Port 1	Тур	Włączony	Adres IPv4	Komentarze
	USTAWIENIA SYSTEMOWE	🖃 📲 WAN			bridge		178.183.0.2/28	
	KONFIGURACJA SIECI	im out		1	Ethernet, 1 Gb/s			
		m DMZ		3	Ethernet, 1 Gb/s			
	Interfejsy	in	÷	2	Ethernet, 1 Gb/s		192.168.0.1/24	
	Interfejsy wirtualne	👘 dmz6		8	Ethernet, 1 Gb/s	🕺 Wyłączony, Odłączony		
	Routing	dmz5		7	Ethernet, 1 Gb/s	😾 Wyłączony, Odłączony		
	Pouting multicast	👘 dmz4		6	Ethernet, 1 Gb/s	🗙 Wyłączony, Odłączony		
	Routing multicast	🗂 dmz3		5	Ethernet, 1 Gb/s	Wyłączony, Odłączony		
	Dynamiczny DNS	m dmz2		4	Ethernet, 1 Gb/s	Wyłączony, Odłączony		
	Serwer DHCP							

27





6. Konfiguracja interfejsów sieciowych

Moduł **Interfejsy** umożliwia zarządzanie, dodawanie i usuwanie elementów sieciowych zwanych interfejsami sieciowymi reprezentującymi fizyczne lub wirtualne urządzenia komunikacyjne między różnymi sieciami przechodzącymi przez urządzenie STORMSHIELD UTM.

Na urządzeniu występuje 6 typów interfejsów:

- Interfejs fizyczny fizyczny interfejs zainstalowany na urządzaniu (bezpośrednio lub w postaci modułu rozszerzającego),
- interfejs bridge łączy kilka interfejsów fizycznych lub VLAN w jeden interfejs logiczny (wirtualny).
 Liczba interfejsów bridge zależy od modelu urządzenia (w domyślnej konfiguracji urządzenia wszystkie fizyczne interfejsy należą do tego samego interfejsu bridge),
- **interfejs VLAN** segment sieci podłączony do fizycznego interfejsu. Pakiety takiego segmentu oznaczone są tagiem VLAN ID oraz określonym zakresem adresów. Maksymalna liczba interfejsów VLAN zależy od modelu urządzenia,
- interfejs GRETAP interfejs umożliwiający połączenie dwóch zdalnych sieci na poziomie warstwy 2 (L2) modelu ISO/OSI. W tym celu enkapsuluje ramkę Ethernet w pakiecie IP za pośrednictwem protokołu GRE. Dzięki temu hosty z dwóch zdalnych sieci będą mogły komunikować się tak, jakby należały do tej samej sieci LAN.
- interfejs Modem ten typ interfejsu umożliwia obsługę połączeń między UTM a modemem (ADSL, ISDN, PSTN itp.). Możliwe typy połączeń to: PPPoE, PPP, PPTP i 3G,
- interfejs USB / Ethernet są tworzone i używane w połączeniach zdalnych za pośrednictwem modemu bezpośrednio podłączonego do zapory (port USB).

Konfiguracja interfejsów sieciowych znajduje się w menu KONFIGURACJA > KONFIGURACJA SIECI > Interfejsy. W centralnej części znajduje się lista interfejsów zawierająca podsumowanie ich konfiguracji.

★- «		/ INTEDEE IOV						
🌣 MODUŁY –	NONFIGURACIA SIECI /	/ INTERFEJST						
Szukaj	🔍 Wprowadź filtr	* 2 C 🖉	Edycja 🝷	🕂 Dodaj 👻 🗙 Usuń	🛛 🛛 🔀 Monitor 🛛 🖓 Przej	dź do monitoringu 🗶 Sj	vrawdź	
	Interfejs		Port	Тур	Włączony	Adres IPv4	Adres MAC	Nazwa systemu
밖 USTAWIENIA SYSTEMOWE	⊟ ¤⊑ DMZ			bridge		192.168.20.254/24		
KONFIGURACJA SIECI	📆 dmz2		4	Ethernet, 1 Gb/s	😾 Wyłączony, Odłączony		00:15:5d:c8:9b:0a	hn3
Interfeiou	👘 dmz3		5	Ethernet, 1 Gb/s			00:15:5d:c8:9b:0b	hn4
interiejsy	👘 dmz4		6	Ethernet, 1 Gb/s			00:15:5d:c8:9b:0c	hn5
Interfejsy wirtualne	nt dmz5		7	Ethernet, 1 Gb/s			00:15:5d:c8:9b:11	hn6
Routing	m out		1	Ethernet, 1 Gb/s		172.18.71.42/28 (DHCP)	00:15:5d:c8:9b:07	hn0
Routing multicast	👘 in	+1	2	Ethernet, 1 Gb/s		10.11.11.2/24	00:15:5d:c8:9b:08	hn1
	itan 👘		3	Ethernet, 1 Gb/s		192.168.10.254/24	00:15:5d:c8:9b:09	hn2
Dynamiczny DNS	👼 dmz6		8	Ethernet, 1 Gb/s	🐙 Włączony, Odłączony	192.168.30.254/24	00:15:5d:c8:9b:12	hn7

Poszczególne kolumny tego widoku oznaczają:

• Interfejs – nazwa interfejsu np. out, in, dmz1, ..., mogą tutaj też pojawić się dodatkowe ikony:

23 interfejs przez który aktualnie zalogowany jest administrator,

24 interfejs, który aktualnie jest edytowany,

- Port numer fizycznego interfejsu, dla interfejsów logicznych (VLAN, modem) nr portu nadrzędnego,
- **Typ** typ interfejsu: bridge, Ethernet, VLAN, PPPoE, ..., prędkość portu, vlan id, ...,
- Status status interfejsu: wyłączony, odłączony. Jeśli interfejs jest podłączony i aktywny kolumna będzie pusta,





- Adres IPv4 skonfigurowany adres IPv4 wraz z maską sieciową lub adres pobrany z DHCP jeśli skonfigurowana jest adresacja dynamiczna,
- Adres IPv6 skonfigurowany adres IPv6 wraz z maską sieciową lub adres pobrany z DHCP jeśli skonfigurowana jest adresacja dynamiczna. Ta kolumna pojawia się jedynie po włączeniu na urządzeniu obsługi protokołu IPv6,
- Adres MAC adres MAC interfejsu
- Nazwa systemowa nazwa interfejsu używana przez system operacyjny urządzenia,
- Komentarz pole komentarza.

Przeciągnij i upuść – można używać tej metody do modyfikacji konfiguracji interfejsów np. w celu dodania interfejsu fizycznego do interfejsu typu bridge lub przeniesienia interfejsu typu VLAN do innego interfejsu fizycznego.

Po wejściu w tryb edycji konfiguracji interfejsu (po wybraniu interfejsu dwukrotne kliknięcie lub Edycja w górnym menu) pojawia się ekran konfiguracji interfejsu.

0 🖉	Edycja 🔹 🕂 Dodaj 👻 Usuń 🔠 N	lonitor 🖓 Przejdź do monitoringu 📔	Sprawdź
	S KONFIGURACJA LAN		
_	OGÔLNE ZAAWANSOWANE		
	Włączony		
	WŁĄCZ		
	Ustawienia podstawowe		
•1	Nazwa:	LAN	
	Komentarze:		
	Ten interfejs jest:	Wewnętrzny (chroniony)	O Zewnętrzny (publiczny)
	Zakres adresów:	 Zakres adresów odziedziczony z bridge 	Oynamiczny / Statyczny
	Adres IPv4:	O Pobierz adres z DHCP	Konfiguracja statyczna
	🕂 Dodaj 🗙 Usuń		
	Adres/ Maska	Opis	
	192.168.10.254/24	sieć LAN	
	192.168.100.254/255.255.255.0		
	192.168.100.250/255.255.255.0		
	• €	Edvcja * + Dodaj * X Usuň (*) KONFIGURACJA LAN OGÓLNE ZAAWANSOWANE Włączony WŁĄCZ Ustawienia podstawowe Ustawienia podstawowe Nazwa: Komentarze: Ten interfejs jest: Zakres adresów Zakres adresów: Adres IPv4: + Dodaj × Usuń Adres/ Maska 192.168.10.254/24 192.168.10.254/25.255.255.0 192.168.100.250/255.255.255.0	 Edycja * + Dodaj * × Usuń P& Monitor C2 Przejdź do monitoringu KONFIGURACJA LAN OGÓLNE ZAAWANSOWANE Włączony Włącz Ustawienia podstawowe Nazwa: LAN Komentarze: Ten interfejs jest: Wewnętrzny (chroniony) Zakres adresów Zakres adresów: Zakres adresów: Zakres adresów: Pobierz adres z DHCP + Dodaj × Usuń Adres / Maska Opis 192.168.10.254/254.255.255.0

Poszczególne pozycje tego widoku oznaczają:

- Włącz / Wyłącz włączenie lub wyłączenie interfejsu
- Nazwa nazwa interfejsu. Na podstawie tej nazwy automatycznie tworzone są obiekty
 Firewall_nazwa i Network_nazwa zawierające odpowiednio adres IP interfejsu i sieci na nim skonfigurowane.
- Komentarz komentarz
- Ten interfejs jest interfejs może być Wewnętrzny (chroniony) lub Zewnętrzny (publiczny).



wewnętrzny (chroniony): chroniony interfejs akceptuje tylko pakiety pochodzące ze znanego zakresu adresów IP, na przykład bezpośrednio połączona sieć lub sieć zdefiniowana przez trasę statyczną. Dodatkowo ochrona obejmuje rejestrację hostów podłączonych do tego interfejsu (chroniąc w ten sposób przed fałszowaniem adresów IP – tzw. IP address spoofing) i pozwala na generowanie domyślnych reguł firewall podczas aktywacji niektórych usługi

urządzenia (na przykład SSH). Chroniony interfejs reprezentowany jest ikoną tarczy 🔍 163,

- zewnętrzny (publiczny): oznacza, że interfejs nie korzysta z zabezpieczeń chronionego interfejsu i dlatego może odbierać pakiety pochodzące z dowolnego zakresu adresów (z wyjątkiem adresów przypisanych do interfejsów wewnętrznych). Ten typ interfejsu służy głównie do połączenia z Internetem.
- Zakres adresów dostępne opcje to: Zakres adresów odziedziczony z bridge lub Dynamiczny / Statyczny
 - Zakres adresów odziedziczony z bridge: wybierając z listy Bridge interfejs typu bridge, interfejs fizyczny zostanie przypisany do interfejsu typy bridge i jednocześnie odziedziczy jego adres IP,
 - Dynamiczny / Statyczny: są tu do wyboru dwie opcje: Pobierz adres z DHCP uruchamia klienta usługi DHCP na danym interfejsie oraz Konfiguracja statyczna, gdzie można ręcznie podać adres IP interfejsu wraz z maską sieciową. Maskę sieciową można zapisać w notacji pełnej np. 255.255.255.0 lub skróconej np. /24. Interfejs może mieć przypisanych kilka adresów IP należących do tej samej lub do różnych podsieci. Jedynym ograniczeniem jest to, że adresacja na poszczególnych interfejsach musi być unikatowa czyli nie można podać tej samej bądź nakładającej się adresacji sieciowej dla kilku interfejsów (z wyjątkiem interfejsów należących do tego samego interfejsu typu bridge). W przypadku dodania więcej niż jednego adresu IP na interfejsie, automatycznie tworzone są obiekty odpowiednio zawierające kolejne adresy IP Firewal_nazwa_1, ..._2, itd. oraz adresację sieci Network_nazwa_1, ..._2, itd.

Dla niektórych typów interfejsów pojawiają się dodatkowe opcje:

- VLAN:
 - Interfejs nadrzędny: interfejs, na którym urządzenie nasłuchuje pakietów oznaczonych tagiem VLAN ID,
 - o ID: nr VLANu tj. tag VLAN ID,
 - **Priorytet CoS**: wskazana wartość CoS (pole Class of Service) zostanie ustawiona dla wszystkich pakietów wysyłanych przez ten VLAN.
- GRETAP:
 - Sieć lokalna obiekt sieciowy odpowiadający interfejsowi typu bridge, do którego należy sieć lokalna, dla której tworzony jest tunel GRETAP.
 - Sieć zdalna obiekt sieciowy odpowiadający adresowi publicznemu zdalnego urządzenia realizującego połączenie GRETAP.
- Modem:
 - o Interfejs nadrzędny: interfejs, na którym podłączony jest modem PPPoE,
 - Adres PPTP: adres serwera PPTP, do którego nawiązywane będzie połączenie PPTP,
 - Użytkownik: nazwa użytkownika wykorzystywana do autentykacji,





- o Hasło: hasło wykorzystywane do autentykacji,
- **Potwierdź**: potwierdzenie poprawności wpisania hasła.
- Interfejs USB / Ethernet ten typ interfejsu tworzony jest automatycznie za każdym razem, gdy modem USB HUAWEI 4G obsługujący funkcję HiLink jest podłączony do urządzenia. Jeśli po podpięciu modemu USB do urządzenia port nie został utworzony, należy skonfigurować profil modemu, aby utworzyć interfejs USB / Ethernet powiązany z danym modemem USB. Możliwe jest zdefiniowanie dwóch profili modemu, ale na urządzeniu można dodać tylko jeden interfejs USB / Ethernet.





7. Routing (trasowanie połączeń)

Routing, czyli określenie drogi przesyłania pakietów można skonfigurować w STORMSHIELD UTM na kilka sposobów. Trasy mogą być zdefiniowane osobno dla IPv4 jak i IPv6.

Kolejność analizy poszczególnych metod trasowania jest następująca:



Trasa powrotna

W przypadku posiadania przynajmniej dwóch lub więcej usługodawców Internetu (ISP) należy skonfigurować w STORMSHIELD UTM tak zwane trasy powrotne. Trasy powrotne pozwolą zdefiniować bramę, przez którą będą musiały przejść pakiety zwrotne, tak aby zagwarantowana była spójność połączeń.

Network Security	ΜΟΝΙΤΟ	ORING	KONFIGURACJA	EVA1	VMSNSX09C0035A9
★ - « MODUŁY – Szukaj	KONFI	GURAC.	IA SIECI / ROUTIN	G JTING DYNAMIC	CZNY IPV4 TRASY POWROTNE
밖 USTAWIENIA SYSTEMO	TRASY PO	NROTNE	+ Doc	laj 🗙 Usuń	Interfeie
Interfejsy Interfejsy wirtualne	Włącz Włącz	BI	RAMA-ISP-1 RAMA-ISP-2		out
Routing Routing multicast					

Konfiguracja jest bardzo prosta i sprowadza się do wskazania właściwej bramy danego ISP, interfejsu, przez który ta brama jest osiągalna oraz włączenia takiej trasy.





Routing na podstawie reguł – Policy Based Routing (PBR)

Jest to typ trasowania połączeń ze względu na adres źródłowy, adres docelowy pakietu, usługę (serwis, port) lub na podstawie zalogowanego użytkownika. Rysunek poniżej prezentuje jedno z możliwych zastosowań:



Na ilustracji zaprezentowano sytuację, w której ruch WWW kierowany jest przez bramę *BRAMA-ISP-1*, natomiast ruch związany z pocztą (smtp, pop3) kierowany jest przez innego usługodawcę – przez *BRAMA-ISP-2*.

Ruch sieciowy można skierować na wybrane łącze ustawiając odpowiednią opcję w menu **Akcja** edytora reguł firewall (więcej o edytorze w dalszej części dokumentacji). Odpowiada za to pozycja *Brama* w sekcji *Routing na podstawie reguł (PBR)*. Wystarczy tutaj jedynie wskazać obiekt typu Host będący bramą wybranego dostawcy Internetu lub wskazać obiekt typu Router (gdzie skonfigurowanych może być więcej dostawców Internetu na zasadzie Load Balancing lub Backup Gateways).

** «	POLITYKI OCHRONY /	POLITYKI OCHRONY / FIREWALLI I NAT									
Szukaj	4 (5) Filter 05	🝷 🛛 Edytuj 👻 📑 Eksportuj	0								
	FIREWALL NAT										
	Szukaj	🕇 + Dodaj 👻 🗙 Usuń 🛛 🏌	🔹 🥐 🖉 🖻 W	ytnij 🔄 🛃 Kopiuj	🕤 Wklej 🛛 🗒	Wyszukaj w logach	🚱 Wyszukaj w mon	itoringu			
Interrejsy	Stan 🖃	Akcja 🚉	Adres źródłowy	Adres docelo	Port docelowy Ana	aliza protokołów	Polityki filtrowania 🔤	Komentarz			
Interfejsy wirtualne	1 💽 włączor	a zezwól Brama: BRAMA-zapas-ISP1-ISP2	Network_internals	Internet	I dns		IPS	DNS - brama podstawowa ISP1, zapasowa ISP2			
Routing multicast	2 💽 włączor	a zezwól Brama: BRAMA-ISP-1	Retwork_internals	Internet	1 http 1 https		IPS	HTTP via ISP1			
Dynamiczny DNS	3 💽 włączor	a zezwól Brama: BRAMA-ISP-2	Retwork_internals	Internet	I smtp I pop3		IPS	Poczta via ISP2			
Serwer DHCP	4 💽 włączor	a 🗢 blokuj	* Any	🛎 Any	* Any		IPS	Domyślna akcja: blokuj wszystko			
Proxy DNS											

Równoważenie Obciążenia / Brama Zapasowa - Load Balancing / Backup Gateways

Równoważenie obciążenia może odbywać się na podstawie adresu źródłowego (SOURCE) lub połączenia (CONNECTION). Włączenie Load Balancingu polega na utworzeniu obiektu typu **Router** ze zdefiniowanymi przynajmniej dwiema bramami na liście używanych bram.

Dla każdej bramy można ustawić sposób weryfikowania jej dostępności (tak aby routowany ruch nie był wysyłany na niesprawną bramę). W celu weryfikacji prawidłowości działania poszczególnych bram urządzanie STORMSHIELD UTM wysyła pakiet Ping do hosta/grupy hostów wskazanych w kolumnie sprawdź





dostępność. Domyślnie testowany jest adres samej bramy, jednak w większości wypadków lepszym rozwiązaniem jest testowanie zewnętrznego publicznego adresu IP (takiego, który jest stabilny i dostępny poprzez sieć Internet). Umożliwi to wykrycie awarii nie tylko naszej bramy (zazwyczaj pierwsze w kolejności urządzenie dostawcy Internetu) ale także problemy w dostępie do Internetu naszego ISP.

W przypadku routingu z Równoważeniem Obciążenia dla poszczególnych bram można określić wagę, która definiuje jak duża część ruchu ma być wysyłana na tą konkretną bramę.

Do przełączania bram wykorzystywany jest algorytm round-robin. Oznacza to, że przy tych samych wagach dla każdej z bram ruch będzie do nich kierowany w jednakowym stopniu. Z kolei asymetryczny podział wag np. BRAMA-ISP-1: 3, BRAMA-ISP-2: 1 spowoduje, że do łącza ISP1 będzie trafiało 75% pakietów kierowanych do Internetu, a do łącza ISP2 25%.

EDYCJA: LOAD-BA	LANCING-ISP1-ISP	2 (ROUTE	R)					
Nazwa: Opis:	Load-ba Równov	lancing-I vażenie o	SP1-ISP2 bciążenia na łączach IPS1 i ISP2	2		^		
LISTA BRAM	ZAPASOWE BRA	MY						
+ Dodaj X	Osun	Maga	Komentera		Przenies do zapasowych bram			
	dns1 google.com	waya	Komental2					
BRAMA-ISP-2	dns1.google.com	1						
Konfiguracja Równoważenie o Włącz bramy i	a zaawansowana obciążenia: zapasowe	Dla ad	dresu źródłowego 👻					
Jeśli żadna	a brama nie jest dos	tępna						
O Jeśli co na	ijmniej jedna brama	jest nied	ostępna					
O Jeśli liczba	O Jeśli liczba dostępnych bram jest mniejsza niż 2							
Włącz bramy	r zapasowe w razie	braku dos	stępności		,	~		
			X ZAMKNIJ V Z	ASTOSUJ				

Działanie bram zapasowych polega na przełączeniu się z bramy podstawowej na bramę zapasową w przypadku awarii tej pierwszej. W celu skonfigurowania bramy zapasowej należy podczas konfiguracji obiektu typu Router na zakładce ZAPASOWE BRAMY wskazać obiekt typu Host reprezentujący adres IP bramy łącza zapasowego.

Routing typu Równoważenie Obciążenia i Bramy Zapasowe można wykorzystywać jednocześnie. Oznacza to, że możliwe jest skonfigurowanie np. dwóch łączy ISP1 i ISP2 na zasadzie równoważenia obciążenia i





jednocześnie skonfigurowanie kolejnej, trzeciej bramy np. na łączu bezprzewodowym LTE jako zapasową, na które urządzenie przełączy się w momencie awarii łączy podstawowych.

Obiekt typu Router reprezentujący routing z Równoważeniem Obciążenia i/lub Bram Zapasowych może być użyty na potrzeby routingu na podstawie reguły (PBR) lub routingu domyślnego (brama domyślna).

Trasy statyczne

Pozwala na określenie tras statycznych do sieci, które nie są podłączone bezpośrednio do interfejsów urządzenia.

Ą	Network Security	MONITORING	Konfiguracja	EVA1 🗤	MSNSX09C0035,	49		
*•	~	KONFIGURACJA SIECI / ROUTING						
•	MODUŁY –							
Szu	kaj 🧩 🖉	TRASY STATYCZNE IPV4 IPV4 ROUTING DYNAMICZNY IPV4 TRASY POWROTNE						
Į∱Į	USTAWIENIA SYSTEMOWE	Ogólne						
<u></u>	KONFIGURACJA SIECI	Brama domyślna (router):		brama-ISP1 💌 🕏				
	Interfejsy							
Interfejsy wirtualne		TRASY STATYCZNE						
	Routing	Wyszukiwanie	+ Dodaj	🗙 Usuń				
	Routing multicast	Stan ≞▼ Si	eć docelowa (host, sieć lul	b grupa obiektó	Interfejs	Adresacje	Brama	
	Dynamiczny DNS	🜑 Włącz si	ec-lokalizacja-1		👼 in	172.16.0.0/24	bramka-vpn	
		🜑 Włącz si	ec-lokalizacja-2		📠 out	172.17.0.0/24	brama-do-sieci-17	
	Serwer DHCP							
	Proxy DNS							

Routing dynamiczny

Pozwala na automatyczną wymianę informacji o trasach routingu oraz aktualizację tablic routingu w środowiskach rozproszonych bądź takich, gdzie trasy routingu mogą się dynamicznie zmieniać. STORMSHIELD UTM obsługuje 3 protokoły routingu dynamicznego, są to: RIPv2, OSPF, BGP. Samo routowanie oparte jest o silnik BIRD (http://bird.network.cz/), a jego konfiguracja opiera się na edycji pliku konfiguracji za pośrednictwem WebGUI.

35





A	Network Security	MONITORING KONFIGURACJA EVA1 VMSNSX09C0035A9						
*	MODUŁY -	KONFIGURACJA SIECI / ROUTING TRASY STATYCZNE IPV4 IPV4 ROUTING DYNAMICZNY IPV4 TRASY POWROTNE Ogólne						
Sz	ukaj 🧩 🖉							
ţţţ	USTAWIENIA SYSTEMOWE							
<u>-1</u> -	KONFIGURACJA SIECI	WŁĄCZ						
	Interfejsy	<pre># The direct protocol automatically generates device routes to all network interfaces. protocol direct { } # This pseudo-protocol performs synchronization between BIRD's routing tables and the kernel.</pre>						
	Interfejsy wirtualne							
	Routing	protocol kernel { learn; # Learn all alien routes from the kernel persistent # Dept servers and the buildown						
	Routing multicast	<pre>persist; # Don't remove routes on bird shutdown scan time 20; # Scan kernel routing table every 20 seconds import all; # Default is import all export all; # Default is export none preference 254; # Protect existing routes } # This pseudo-protocol watches all interface up/down events. protocol device { scan time 10; # Scan interfaces every 10 seconds } log syslog all; </pre>						
	Dynamiczny DNS							
	Serwer DHCP							
	Proxy DNS							
	OBIEKTY							
•	UŻYTKOWNICY	router id 0.0.0.1; filter wan_filter {						
≁ŀ	POLITYKI OCHRONY	if net = 172.17.224.76/32 then reject; #wykluczenie interfejsu WAN z routingu w tunelu IPSec if net = 10.1.1.2/32 then reject; else accept; }						
$\overline{\oslash}$	KONTROLA APLIKACJI							

Routing na podstawie interfejsu

Ten typ trasowania połączeń pozwala na kierowanie całego ruchu przychodzącego na dany interfejs na wskazaną bramę. Ten typ routingu można skonfigurować jedynie z poziomu wiersza poleceń poprzez edycję pliku /usr/Firewall/ConfigFiles/network, przykład poniżej:

```
[ethernet1]
State=1
Name=in
Protected=1
Media=0
Color=408080
Type=1
EEE=0
Address=10.0.0.254
Mask=255.255.255.0
Gateway=BRAMA-ISP-2  # Brama dla całego ruchu przychodzącego tym interfejsem
AddressComment=
```

Brama domyślna

Cały ruch, dla którego nie została znaleziona trasa na podstawie wcześniej omówionych metod routingu będzie skierowany na bramę domyślną (Default Gateway).

Bramę domyślną można skonfigurować w KONFIGURACJA > KONFIGURACJA SIECI > Routing > sekcja Ogólne. W opcji *Brama domyślna (router)* należy wskazać obiekt reprezentujący bramę domyślną i może to być obiekt typu:

- **Host** jedno łącze internetowe, bez testowania dostępności bramy, równoważenia obciążenia czy też bram zapasowych,
- **Router** więcej niż jedno łącze internetowe z możliwością uruchomienia równoważenia obciążenia i/lub bram zapasowych oraz weryfikacji dostępności poszczególnych bram.




* • « * MODUŁY –		CJA SIECI / ROUTING				
Szukaj 🗶 🖉	TRASY STATYCZ	IPV4 ROUT	NG DYNAMICZNY	IPV4 TRASY POWRO	TNE	
	Ogólne					
117 USTAWIENIA STSTEMOWE						
KONFIGURACJA SIECI	Brama domyślna	(router):	brama-domyslna		▼ St	
Interfeisy				Nazwa: brama-domyslna		
				Adres: 192.168.0.1		
Interfejsy wirtualne	TRASY STATYCZN	IE				
Routing	Wyszukiwanie	+ Dodaj	🗙 Usuń			
Routing multicast	Stan 🖃	Sieć docelowa (host, sieć lu	b grupa obiektów)	Interfejs		Adresacje
3						

🕖 Wskazówka

Konfiguracja bramy domyślnej i tras statycznych znajduje się w pliku: /usr/Firewall/ConfigFiles/route

Aby wyświetlić trasy statyczne oraz trasę domyślną można użyć polecenia: netstat -nr

Aby wyświetlić pozostałe metody trasowania należy użyć polecenia: sfctl -s route



NEXT GENERATION FIREWALL PODRĘCZNIK UŻYTKOWNIKA





8. Konfiguracja zapory (firewall)

Konfiguracja Firewall w rozwiązaniach STORMSHIELD UTM podzielona jest na dwie części. Pierwszą z nich są reguły domyślne, a drugą polityki konfigurowane przez administratora.

W pierwszej kolejności pakiet sprawdzany jest przez zbiór **Domyślnych reguł firewall (Implicit rules**). Jeżeli pakiet nie znajdzie dopasowania do żadnej z reguł domyślnych sprawdzane są dopasowania do reguł polityki stworzonej przez administratora tzw. **Polityki lokalnej**.



Domyślne reguły firewall - Implicit Rules

W sekcji **KONFIGURACJA > POLITYKI OCHRONY > Domyślne reguły firewall** widoczne są reguły domyślne ustawione na zaporze. Reguły te mają na celu zapewnienie komunikacji z urządzeniem nawet w sytuacji, kiedy w ramach lokalnej polityki firewall administrator nie stworzyłby reguł umożliwiających komunikację z urządzeniem czy też omyłkowo stworzył reguły blokujące taką komunikację, co w efekcie aktywowania takiej polityki spowodowałoby utratę łączności z urządzeniem. Poniżej przedstawiono dostępne domyślne reguły firewall. Każdą z nich można włączyć bądź wyłączyć, ale nie można dodać nowych bądź usunąć istniejących:



W przypadku reguł domyślnych administrator nie widzi ich pełnej składni, jednak znaczenie poszczególnych reguł można zobaczyć w aplikacji **Real Time Monitor** w zakładce **Reguły firewall**





🕛 Uwaga

Wyłączenie reguł domyślnych (implicit rules) bez wcześniejszego utworzenia odpowiednich reguł Polityki lokalnej może skutkować brakiem dostępu do panelu administracyjnego urządzenia. Zmiany reguł domyślnych powinny być dokładnie przemyślane.

🕖 Wskazówka
Do wyświetlenia aktywnych reguł firewall z poziomu SSH służy polecenie:
sfctl -s filter

Lokalne polityki ochrony

Konfiguracja zapory STORMSHIELD UTM znajduje się w sekcji **KONFIGURACJA > POLITYKI OCHRONY > Firewall i NAT**. Administrator ma do dyspozycji 10 konfigurowalnych zestawów reguł zwanych profilami. W

danej chwili aktywny może być tylko jeden profil, który oznaczony jest ikoną 松 33.



W ramach ustawień profilu określa się politykę filtrowania ruchu sieciowego na poziomie firewall, sposób filtrowania ruchu poprzez system IPS oraz konfiguruje się inne skanery (np. antywirus) i dodatkowe parametry takie jak np. QoS. Poniżej znajduje się okno konfiguracyjne Firewall i NAT, gdzie przedstawiony jest domyślny zestaw reguł, którym jest profil nr 1 o nazwie **Block all**. W ramach tego zestawu możliwe jest podłączenie się do panelu administracyjnego urządzenia (nawet jeśli reguły domyślne są wyłączone) oraz sprawdzenie dostępności urządzenia za pomocą komunikacji *ICMP (PING)*, natomiast każde inne połączenie jest blokowane.





* - «	POLITYKI OCHRONY / FIREWALL I NAT	
Szukai	🥀 (1) Block all 🔹 📔 Edytuj 👻 🛛 🚼 Eksportuj 🛛	
	FIREWALL NAT	
	Szukaj 📔 🕂 Dodaj 👻 X. Usuń 🏦 🌲 🧩 😵 🗁 Wytnij 🔂 Kopiuj 🕥 Wklej 🗒 Wyszukaj w logac	n 🚱 Wyszukaj w monitoringu
KONFIGURACJA SIECI	Stan 💵 Akcja 💵 Adres źródłowy Adres docelowy Port docelowy Analiza protokołów	Polityki filtrowania Komentarz
OBIEKTY	Bemote Management: Go to System - Configuration to setup the web administration application access (zawiera 2 regul, od 1 to 2)	
	1 C włączona O zezwół I Any Ba firewall_all I firewall_srv I thtps	Admin from everywhere
	2 💿 włączona 📀 zezwól 🗳 Any 🛱 firewall_all 🗳 Any wyłącznie icmp (Echo request (Ping))	Allow Ping from everywhere
Firewall i NAT	□ Default policy (zawiera 1 reguł, od 3 to 3)	
Filtrowanie URL	3 🜑 włączona 🗢 blokuj 🗳 Any 🗳 Any	IPS Block all

Górna część okna Firewall i NAT pozwala na zarządzanie profilami oraz regułami firewall.

	FIREWALL I NAT
🦺 (5) Filter 05	▼ Edytuj ▼ I " Eksportuj I I
FIREWALL NAT	
Szukaj	🕂 Dodaj 👻 🗙 Usuń 🏦 🌲 🧩 🦨 🚰 Wytnij 🔄 Kopiuj 🕤 Wklej 🗒 Wyszukaj w logach 🛛 🖓 Wyszukaj w monitoringu

Dostępne akcje zarządzania regułami firewall:

Edytuj	Zmiana nazwy profilu, przywrócenie jego ustawień domyślnych oraz przekopiowanie bieżącego profilu do innego.
Eksportuj	Eksport bieżącego profilu do pliku CSV.
Dodaj	Dodanie nowej reguły lub separatora. Z tego miejsca możliwe jest również uruchomienie kreatora reguł specjalnych: SSL Proxy, http Proxy (typu explicit), reguły uwierzytelniania.
Usuń	Usuwa zaznaczoną regułę.
W górę/W dół 🕇 🕴 37	Przesunięcie zaznaczonej reguły.
Zwiń / Rozwiń (separatory)	Separatory można użyć do grupowania reguł o podobnych zakresach np. reguły dla LAN, reguły dla DMZ. Jak sama nazwa wskazuje przyciski Zwiń /Rozwiń wszystkie separatory służą do szybkiego zwinięcia/rozwinięcia wszystkich separatorów.
Wytnij/Kopiuj/Wklej	Pozwala na szybkie zarządzanie regułami. Reguły można zaznaczać z użyciem klawiszy Shift lub Ctrl w celu zaznaczenia wielu reguł. Można także korzystać ze skrótów klawiszowych Ctrl+c, Ctrl+x, Ctrl+v .
Wyszukaj w logach	Przenosi do sekcji MONITORING > LOGI z aktywnym filtrem wyświetlającym wpisy dziennika tylko zaznaczonej reguły firewall.
Wyszukaj w monitoringu	Przenosi do sekcji MONITORING > MONITOROWANIE > Połączenia z aktywnym filtrem wyświetlającym aktywne połączenia zestawione na podstawie zaznaczonej reguły firewall.





Dolna część okna pozwala na definiowanie poszczególnych reguł firewall. Konfiguracja reguł polega na definiowaniu dopasowania, czyli warunków jakie musi spełnić ruch sieciowy, aby wpaść w regułę oraz akcji – tego co ma się stać z ruchem, który wpadnie w tę regułę.

	Stan 🖃	•	Akcja	E.	Adres źródłowy	Adres docelowy	Port docelowy	Analiza protokołów	Polityki filtrowania	Komentarz
🖃 Remote Mar	agement: Go	to Sy	/stem - Co	nfigura	ation to setup the web	administration applic	ation access (zawie	ra 2 reguł, od 1 to 2)		
1	🔍 włączo	na	🕑 zezw	ól	Any	firewall_all	İ firewall_srvİ https		IPS	Admin from everywhere
2	🔍 włączo	na	📀 zezw	ól	* Any	firewall_all	* Any	wyłącznie icmp (Echo request (Ping))	IPS	Allow Ping from everywhere
Default polic	y (zawiera 1 r	reguł,	, od 3 to 3)							
3	🔍 włączo	na	🗢 bloku	ij	* Any	* Any	* Any		IPS	Block all

Kolumny odpowiedzialne za dopasowanie ruchu do reguły firewall to: Adres źródłowy, Adres docelowy, Port docelowy, Analiza protokołów. Ich konfiguracja obejmuje:

Opcje dostępne w ramach kolumny Adres źródłowy:

Użytkownik – uwierzytelniony użytkownik bazy LDAP.

Adres źródłowy – źródłowy adres IP pakietu inicjującego połączenie. Może to być pojedynczy host, zakres adresów, sieć, grupa adresów.

Interfejs wejściowy – interfejs, na którym pojawia się pierwszy pakiet inicjujący połączenie. Pozwala na tworzenie reguł zależnych od topologii sieci.

EDYCJA REGUŁY NUM	ER 1
Ogólne	ADRES ŹRÓDŁOWY
Akcja	
Adres źródłowy	OGÓLNE GEOLOKACJA / REPUTACJA ZAAWANSOWANE
Adres docelowy	
Port - Protokół	
Polityki filtrowania	Użytkownik: 🕒 🕶 🔁 🕶 Szukaj 💌
	Adres źródłowy: + Dodaj × Usuń 🕒 🗸
	Any
	Interfejs wejściowy: Choose your interface -
	X ANULUJ V OK





Opcje dostępne w ramach kolumny Adres docelowy:

Adres docelowy - adres IP przeznaczenia pakietu. Może to być pojedynczy host, zakres adresów, sieć, grupa adresów.

EDYCJA REGUŁY NUMI	ER 1	
Ogólne		
Akcja		
Adres źródłowy	OGÓLNE GEOLOKACJA / REPUTACJA ZAAWANSOWANE	
Adres docelowy		
Port - Protokół	- Ostawienia ogome	
Polityki filtrowania	Adres docelowy:	0.
		0.
	firewall_all	
	X ANULUJ V OK	

Opcje dostępne w ramach kolumn **Port docelowy i Analiza protokołów** (edycja z poziomu zakładki Port – Protokół edytora reguł):

Port docelowy – określa usługę, z której będą korzystać obiekty określone w **Adresie źródłowym** łącząc się do obiektu określonego w **Adresie docelowym**. Inaczej mówiąc jest to port docelowy połączenia w ramach protokołu sieciowego (TCP/UDP/SCTP). Może to być pojedynczy port, zakres bądź grupa portów działająca na jednym lub dowolnym z protokołów sieciowych.

Protokół – tryb analizy – określa protokół ruchu wpadającego w regułę. Może to być protokół warstwy IP (ICMP, TCP, UDP, ESP, GRE, itp.) lub protokół warstwy aplikacji (HTTP, DNS, DHCP, itp.)

NEXT GENERATION FIREWALL PODRĘCZNIK UŻYTKOWNIKA



Y / _

EDYCJA REGUŁY NUME	R 1		
Ogólne Akcja Adres źródłowy Adres docelowy	PORT - PROTOKÓŁ		
Port - Protokół Polityki filtrowania	Port docelowy:	+ Dodaj X Usuń firewall_srv https	€ •
	Protokół Tryb analizy: Ustaw protokół ręcznie: Protokół warstwy IP:	Rozpoznaj protokół automatycznie (domyślnie) Automatyczne wykrywanie protokołu dowolny	•
	×	ANULUJ V OK	

Jeśli ruch zostanie dopasowany do reguły na podstawie powyższych kolumn, czyli spełni wszystkie określone w nich warunki, to zostaną dla niego wykonane czynności zdefiniowane w kolumnach **Akcja** oraz **Polityki filtrowania**. Ich konfiguracja obejmuje odpowiednio:

Opcje dostępne w ramach kolumny Akcja:

Akcja - akcja jaka ma zostać podjęta dla ruchu, który znalazł dopasowanie w regule. Dostępne opcje to:

- Zezwól przepuszczenie ruchu i wykonywanie dalszej analizy (np. skanowanie antywirusowe);
- Blokuj zablokowanie ruchu bez dalszej analizy;
- Deszyfruj uruchomienie modułu SSL proxy w celu deszyfracji ruchu np. HTTPS, POP3S, SMTPS, itp.;
- Reset zablokowanie ruchu i odesłanie pakietu z flagą RST do nadawcy, bez dalszej analizy;

Logowanie – informacja o dopasowaniu ruchu do reguły firewall może zostać zapisana w logach, dostępne opcje to:

standardowe (logowanie połączeń) – zakończone połączenia, które doszły do skutku (czyli te z akcją zezwól) mogą być zapisane w dzienniku (MONITRONG > LOGI > Ruch sieciowy) w zależności od protokołu połączenia i domyślnej konfiguracji logowania danego protokołu,

NEXT GENERATION FIREWALL PODRĘCZNIK UŻYTKOWNIKA





- szczegółowe (logowanie filtrowania) każda próba połączenia odpowiadająca regule firewall będzie zapisana w dzienniku (MONITRONG > LOGI > Ruch sieciowy). Ta opcja nie jest polecana dla reguł typu "Zablokuj wszystko - Deny all" z wyjątkiem debugowania, ponieważ będzie generowała bardzo dużą ilość logów.
- alarm: priorytet niski lub alarm: priorytet wysoki w momencie dopasowania reguły do połączenia zostanie wygenerowany alarm o wybranym priorytecie. Taki alarm zostanie zapisany w dzienniku Alarmy oraz może być wysłany przez Syslog (Logs Syslog IPFIX) lub powiadomienie email.

Harmonogram – Harmonogram jest opcją dopasowania, a nie filtrowania ruchu. Dzięki wskazaniu obiektu harmonogramu możemy zdefiniować godziny i/lub dni, w których reguła jest aktywna i uwzględniana w ramach polityki filtrowania.

Brama – pozwala na trasowanie ruchu w ramach polityk filtrowania (Routing na podstawie reguły – PBR). W tym miejscu może zostać wskazany obiekt typu Host (pojedyncza brama) lub Router (równoważenie obciążenia/brama zapasowa).

Kolejka QoS – pozwala na przypisanie ruchu do odpowiedniej kolejki QoS, czyli na sterowanie pasmem (kolejki CBQ) lub nadanie określonego priorytetu (kolejki PBQ) połączeniu. Definicja kolejek QoS znajduje się w KONFIGURACJA > POLITYKI OCHRONY > Ustawienia QoS.

Podział względem – pozwala na równe podzielenie przypisanego pasma. Dla opcji **Użytkownik** i **Host** każde ze źródeł ruchu otrzyma taką samą część pasma niezależnie od tego jak wiele sesji generuje. Przy użyciu opcji **Połączenie** podział odbywa się względem połączeń niezależnie od tego ile sesji nawiązuje każde ze źródeł ruchu.

Ogólne	АКСЈА				
Akcja					
Adres źródłowy	USTAWIENIA OGOLNE	KOLEJKA QOS	ZAAWANSOWANE		
Adres docelowy	Ustawienia ogólne				
Port - Protokół					
Polityki filtrowania	Akcja:	📀 zezwól			-
	Logowanie:	standardowe	e (logowanie połączeń)		-
	Harmonogram:			-	=





Opcje dostępne w ramach kolumny Polityki filtrowania:

Tryb pracy:

- IPS (Intrusion Prevention System) system wykrywania i blokowania zagrożeń;
- **IDS** (Intrusion Detection System) wykrywanie zagrożeń bez ich blokowania;
- **Firewall** powoduje, że nie będzie działał moduł ASQ, czyli zagrożenia nie będą ani wykrywane, ani tym bardzie blokowane (ten tryb pracy nazywany jest też tzw. klasycznym firewallem).

Profil ASQ – wybór jednego z 10 profili prac IPS. Wybór *W zależności od kierunku ruchu* oznacza, że do analizy użyty będzie jeden z profili domyślnych, czyli 00 dla ruchu przychodzącego z zewnątrz i 01 dla ruchu wychodzącego z sieci wewnętrznych (chronionych).

Sekcja Filtrowanie treści – konfiguracja poniższych opcji związana jest z działaniem modułów proxy:

- Antywirus włączenie/wyłączenie filtrowania ruchu http, ftp, smtp i pop3 za pomocą skanera AV.
- Sandboxing włączenie/wyłączenie ochrony typu sandboxing (Breach Fighter). Włączenie tej opcji wymaga użycia silnika antywirusa.
- Antyspam włączenie/wyłączenie skanera antyspamowego dla ruchu smtp i pop3.
- **Filtrowanie URL** wybór jednego z 10 profili filtrowania URL dla ruchu WWW. Konfiguracja profili filtrowania URL znajduje się w KONFIGURACJA > POLITYKI OCHRONY > Filtrowanie URL.
- Filtrowanie poczty wybór jednego z 10 profili filtrowania nadawców/odbiorców dla ruchu smtp.
- Filtrowanie FTP włączenie/wyłącznie skanera protokołu ftp.
- **Filtrowanie SSL** wybór jednego z 10 profili filtrowania dla ruchu SSL. Konfiguracja profili filtrowania SSL znajduje się w KONFIGURACJA > POLITYKI OCHRONY > Filtrowanie SSL.

icija Ustawienia ogólne Ustawienia ogólne Ires źródłowy Tryb pracy: IPS Olityki filtrowania Profil ASQ: W zależności od kierunku ruchu	~
dres źródłowy dres docelowy ort - Protokół Diltyki filtrowania Profil ASQ: W zależności od kierunku ruchu	•
Adres docelowy Tryb pracy: Port - Protokół Profil ASQ: W zależności od kierunku ruchu	-
Port - Protokół Tryb pracy: Polityki filtrowania Profil ASQ: W zależności od kierunku ruchu	-
Polityki filtrowania Profil ASQ: W zależności od kierunku ruchu	
	-
Filtrowanie treści	
Antywirus 🔁 : 💿 włączony	•
Sandboxing 1 : Owłączony	-
Antyspam: 🖸 wyłączony	-
Filtrowanie URL: OURLFilter_00	-
Filtrowanie poczty:	-
Filtrowanie FTP: Owyłączony	-
Filtrowanie SSL: Owyłączony	-





🕖 Uwaga

Dopasowanie nowego połączenia do reguły firewall wykonywane jest w kolejności od pierwszej do ostatniej reguły. Jeśli ruch nie "wpadnie" w żadną ze zdefiniowanych reguł zostanie on zablokowany przez politykę domyślną.

Analizator regul

Analizator reguł sprawdza poprawność konfiguracji firewall, tzn. sprawdza, czy stworzone reguły są poprawne pod względem użytych obiektów i metod skanowania ruchu oraz czy nie ma reguł pokrywających się lub wykluczających się. W przypadku wykrycia nieprawidłowości Analizator wyświetli w dolnej części okna

konfiguracyjnego alarm informujący o wykrytym problemie wraz z odpowiednim symbolem: 🥌 50 lub 😢 51. Poniżej znajdują się przykładowe komunikaty Analizatora reguł.

ANALIZATOR	
😢 [Reguła 4] Analiza może być stosowana tylko dla ruchu TCP	
[Reguła 1] Brak zdefiniowanej akcji "rozszyfruj" dla ruchu odnoszącego się do określonych reguł. Nie można zastosować reguł filtrowania. Sprawdź port docelowy wskazanej reguły	
[Reguła 3] Reguła nigdy nie zostanie zastosowana i zostanie zastąpiona przez 2.	

Przykładowe reguły Firewall:

Przepuszczenie ruchu WWW (http i https) z sieci LAN do Internetu:

	Stan 🖃	Akcja 🚉	Adres źródłowy	Adres docelowy	Port docelowy	Analiza protokoł	Polityki filtrowania 🖃
1	 🔍 włączona	🕤 zezwól	Retwork_LAN	Internet	┇ http ┇ https		IPS

Reguła zezwalająca na dostęp administracyjny (SSH, WebGUI) z Internetu do urządzenia:

	Stan ≞▼	Akcja 🚉	Adres źródłowy	Adres docelowy	Port docelowy	Analiza protokoł	Polityki filtrowania 🖃
1 🚥	💶 włączona	📀 zezwól	Internet	Firewall_out	I ssh I https		IPS

Zezwolenie na PING (ICMP) pomiędzy sieciami LAN i DMZ:

	Stan	±.	Akcja	±.	Adres źródłowy	Adres docelowy	Port docelowy	Analiza protokołów	Polityki filtrowania ≞▼
1	💽 włą	czona	🕑 zez	zwól	Retwork_LAN	Retwork_DMZ	* Any	wyłącznie icmp (Echo request (Ping))	IPS





🕖 Wskazówka

W systemie operacyjnym urządzenia - NS-BSD reguły filtrowania przechowywane są odpowiednio w: /usr/Firewall/ConfigFiles/Filter/XX

Gdzie XX jeśli plikiem oznaczającym numer profilu (zestaw reguł).

W przypadku konfiguracji przy użyciu CLI, można aktywować poszczególne profile komendą: enfilter XX

Natomiast polecenie: enfilter off zupełnie wyłączy filtrowanie pakietów (wyłączy firewalla).

Informacja o profilach, czyli ich nazwa i numer znajduje się w pliku: /usr/Firewall/ConfigFiles/Filter/slotinfo







9. Konfiguracja translacji adresów (NAT)

Translacja adresów nazywana również maskaradą IP jest mechanizmem tłumaczenia adresów prywatnych sieci lokalnej na adresy publiczne otrzymane od usługodawcy Internetu (ISP).

Rozróżnia się dwa podstawowe typy translacji adresów:

SNAT (*Source Network Address Translation*) – polega na podmianie źródłowego adresu IP w pakiecie. SNAT stosowany jest w przypadku połączenia z sieci LAN (z adresacją prywatną) do Internetu.

DNAT (*Destination Network Address Translation*) – polega na podmianie docelowego adresu IP w pakiecie. DNAT jest stosowany do udostępnienia w Internecie zasobów sieci wewnętrznej, takich które mają prywatny adres IP.

Oba typy translacji adresów można łączyć, przez co można się również spotkać z jednoczesną translacją adresu źródłowego i docelowego tzw. Source and Destination NAT.

Mechanizm NAT może służyć nie tylko do zmiany adresów IP, ale również do zmiany portów używanych w komunikacji (translacja nagłówka TCP/UDP) jest to tzw. PAT (*Port Address Translation*). PAT jest zazwyczaj połączony z DNAT.

Konfiguracja NAT połączona jest z konfiguracją Firewall i znajduje się w sekcji **KONFIGURACJA > POLITYKI OCHRONY > Firewall i NAT**. Aktywując Firewall aktywuje się również NAT. Połączenie konfiguracji tych modułów oznacza również, że tak jak w zaporze reguły NAT przetwarzane są zgodnie z ich kolejnością (począwszy od góry).

Konfiguracja NAT polega na zdefiniowaniu jak powinien wyglądać nagłówek TCP/IP po przejściu pakietu przez urządzenie i podzielona jest na dwa etapy. W pierwszym definiowane jest dopasowanie ruchu do reguły – jeśli oryginalny nagłówek pakietu znajdzie dopasowanie do reguły NAT, to wykonywany jest drugi etap polegający na podmianie poszczególnych elementów nagłówka TCP/IP.

	POLITYKI OCHRONY / FIREWALL I NAT									
🦺 (5) produkc	ja	🝷 Edytuj 👻 🏪 E	ksportuj 🚯							
FIREWALL	FIREWALL NAT									
Szukaj		🕂 🕂 🕂 🕇 + Dodaj 👻 🗙 Usu	mí † ↓ →	🖌 🛃 🛛 🔁 Wytnij	i Ø	🚰 Kopiuj 🛛 🐑 Wklej	🗒 Wyszukaj w log	jach 🛛 🙀 Wyszukaj w m	onitoringu	
	Eton E	ORY	GINALNY (przed trans	slacją)			NAT (po	translacji)		Komentarz
	Stan	Adres źródłowy	Adres docelowy	Port docelowy		Adres źródłowy	Port źródłowy	Adres docelowy	Port docelowy	Komentarz
1	🔍 włączona	Internet	Firewall_out	覚 http	-	* Any		🛙 www-svr-priv-ip	🕇 http	DNAT
2	🔍 włączona	Network_internals	Internet	🗶 Any	-	E Firewall_out	T ephemeral_fw	🗶 Any		SNAT + PAT - maskarada

Dopasowanie ruchu sieciowego do reguły NAT – pakiet ORYGINALNY (przed translacją)

Kolumna Adres źródłowy:

- Użytkownik uwierzytelniony użytkownik bazy LDAP
- Adres źródłowy źródłowy adres IP pakietu inicjującego połączenie. Może to być pojedynczy host, zakres adresów, sieć, grupa adresów.
- Interfejs wejściowy interfejs, na którym pojawia się pierwszy pakiet inicjujący połączenie.

Kolumna Adres docelowy:

• Adres docelowy – adres IP przeznaczenia pakietu. Może to być pojedynczy host, zakres adresów, sieć, grupa adresów.





• Interfejs wyjściowy – interfejs, którym pakiet opuści urządzenie.

Kolumna Port docelowy:

• **Port docelowy** – określa usługę, z której będą korzystać obiekty określone w **Adresie źródłowym** łącząc się do obiektu określonego w **Adresie docelowym**.

Konfiguracja poszczególnych typów translacji

Source NAT (SNAT)

Rysunek poniżej ilustruje wykorzystanie translacji adresów typu Source NAT.

Następuje tutaj zmiana adresu źródłowego po przejściu pakietu przez router. Jest to tzw. translacja **n:1**, czyli zmiana wielu adresów prywatnych (**n**) (w poniższym przykładzie jest to cała sieć Network_LAN) na jeden publiczny (**1**) (w przykładzie jest to obiekt Firewall_out).



ORYGINALNY (przed translacją)

- Adres źródłowy Sieć LAN (dowolny adres z sieci LAN).
- Adres docelowy Internet (dowolny docelowy adres IP w Internecie), dodatkowo ruch musi być trasowany przez interfejs OUT.
- Port docelowy Any (dowolny).

NAT (po translacji)

- Adres źródłowy Firewall_out czyli obiekt reprezentujący publiczny adres IP urządzenia STORMSHIELD UTM. Warto tutaj zauważyć, że jeśli ruch ma być zmieniony na publiczny adres IP, który nie jest zdefiniowany na żadnym z interfejsów urządzenia, konieczne będzie zaznaczenie opcji *Publikacja ARP*.
- Port źródłowy ephemeral_fw jest to specjalny obiekt reprezentujący pulę wysokich portów (20 000 59 999).
- Adres docelowy Any lub puste pole oznacza, że oryginalny docelowy adres IP pozostanie bez zmian.
- **Port docelowy** Any lub puste pole oznacza, że oryginalny port docelowy TCP/UDP pozostanie bez zmian.







Jak czytać powyższą translację SNAT?

Każde połączenie pochodzące z sieci LAN, które jest kierowane do Internetu i opuści urządzenie interfejsem OUT zostanie poddane translacji NAT, po której źródłowy adres IP zostanie zmieniony na publiczny adres IP urządzenia reprezentowany przez obiekt Firewall_out, a port źródłowy zostanie nadpisany nowym portem wysokim (z zakresu 20 000 – 59 999). Docelowy adres IP nie ulegnie zmianie. Dzięki temu ruch sieciowy z sieci wewnętrznej może zostać przekazany do sieci Internet, a jeśli docelowy host odpowie, to taka odpowiedź trafi do STORMSHIELD UTM, który będzie wiedział, do którego hosta w sieci wewnętrznej ma taką odpowiedź przekazać.

Destination NAT (DNAT)

Translacja adresów **Destination NAT** inaczej zwana również jako tzw. redirect, jest przydatna w przypadku przekierowania usług z zewnętrznego interfejsu STORMSHIELD UTM do sieci lokalnej na adres prywatny. Przykładem takiego przekierowania może być np. przekierowanie połączenia zdalnego pulpitu Windows (Microsoft Terminal Services).



58

Klient sieci Internet będzie łączył się na adres publiczny urządzenia STORMSHIELD UTM, gdzie nastąpi przekierowanie na prywatny adres IP hosta w sieci LAN.

Taka reguła NAT będzie wyglądać następująco.

[ORYGINALNY (przed translacja)			NAT (po t	ranslacji)	
Adres źródłowy	Adres docelowy	Port docelowy		Adres źródłowy	Port źródłowy	Adres docelowy	Port docelowy
Internet	E Firewall_out	İ microsoft-ts	-	* Any		🖪 TS-svr-priv-ip	İ microsoft-ts

ORYGINALNY (przed translacją)

- Adres źródłowy Internet (ruch przychodzący z poza sieci wewnętrznych).
- Adres docelowy Firewall_out czyli obiekt reprezentujący publiczny adres IP urządzenia STORMSHIELD UTM. Podobnie jak w przypadku SNAT jeśli ruch jest kierowany na publiczny adres IP, który nie jest zdefiniowany na żadnym z interfejsów urządzenia, konieczne będzie zaznaczenie opcji *Publikacja ARP*.
- **Port docelowy** Port, na który nawiązywane jest oryginalne połączenie.

NAT (po translacji)

- Adres źródłowy Any lub puste pole oznacza, że oryginalny źródłowy adres IP pozostanie bez zmian.
- **Port źródłowy** Any lub puste pole oznacza, że oryginalny port źródłowy TCP/UDP pozostanie bez zmian.





- Adres docelowy Obiekt reprezentujący prywatny adres IP serwera docelowego.
- Port docelowy Port na którym działa usługa na serwerze docelowym.

Jak czytać powyższą translację DNAT?

Każde połączenie z Internetu, które jest nawiązywane na publiczny adres IP urządzenia na port microsoft-ts (3389 TCP) zostanie poddane translacji NAT, w ramach której źródłowy adres IP i port źródłowy nie zmienią się, natomiast docelowy adres IP zostanie zamieniony na prywatny adres IP serwera terminali z zachowaniem portu docelowego. Dzięki temu serwer ww. usługi w sieci lokalnej będzie widział takie połączenie nie z adresem IP STORMSHIELD UTM lecz urządzenia w sieci Internet, od którego pochodzi ten ruch sieciowy.

Bi-Directional map (BI-MAP)

Operacja **Bi-Directional MAP** jest translacją typu **1:1**, tzn. pozwala na przypisanie adresowi IP z sieci lokalnej wirtualnego adresu publicznego. BI-MAP składa się z dwóch reguł, z których jedna jest regułą SNAT, a druga DNAT. Translacja BI-MAP wymaga użycia adresu IP niebędącego adresem urządzenia STORMSHIELD UTM. Taki rodzaj NAT stosuje się najczęściej w przypadku kiedy serwer ma "wychodzić" do Internetu z takim samym publicznym adresem IP, pod którym odbiera połączenia przychodzące do niego, czyli np. serwer pocztowy. Konfiguracja translacji BI-MAP odbywa się poprzez **Kreator reguły BIMAP (1 do 1)**.

KREATOR REGUŁY BI-DIRECT	TONAL MAP			
Cel: Utworzyć regułę dla transla	cji 1-1. Prywatny adres IP po przejściu przez	z urządzenia otrzyma pub	iczny adres IP (obiekt wirtualny).	
– Ustawienia podstawowe –				
	PRYWATNE		WIRTUALNE (NAT)	
Obiekty z sieci prywatnej:	SMTP-svr-priv-ip 💌 🚍	Wirtualne hosty:	SMTP-svr-pub-ip	- =
		Interfejs:	out	•
Zaawansowane				
Przekierowana usługa:	Any 👻 🚍			
	Publikacja ARP dla sieci zewnętrznych (publiczne)			
	× ANULUJ	🗸 ZAKOŃCZ		
		51		





Zakończenie pracy kreatora owocuje utworzeniem dwóch reguł – jednej dla ruchu wychodzącego z serwera do Internetu i drugiej dla ruchu przychodzącego z Internetu. Ponieważ publiczne IP nie jest zdefiniowane na interfejsie urządzenia należy zaznaczyć opcję *Publikacja ARP*.

c	RYGINALNY (przed translacja)		NAT (po translacji)				
Adres źródłowy	Adres docelowy	Port docelowy		Adres źródłowy	Port źródłowy	Adres docelowy	Port docelowy	
SMTP-svr-priv-ip	Any interfejs wyjściowy: out	* Any	→	IT SMTP-svr-pub-ip				
* Any interfejs wejściowy: out	I SMTP-svr-pub-ip	* Any	+			B SMTP-svr-priv-ip		

Do analizowania i rozwiazywania problemów z translacją NAT można użyć opcji logowania. Każde połączenie odpowiadające regule NAT będzie zapisane w logach. I tak, dla opcji *Logowanie: zapisz w logach* będzie to dziennik Filtering (MONITRONG > LOGI > Ruch sieciowy), natomiast dla opcji *Logowanie: alarm: priorytet niski* lub *alarm: priorytet wysoki* będzie to dziennik Alarmy (MONITRONG > LOGI > Alarmy).

EDYCJA REGUŁY NUME	R 1		
Ogólne	OPCJE		
Oryginalny adres źródł			
Oryginalny adres doce			
Adres źródłowy (po tra	Logowanie:	🗎 zapisz w logach	-
Adres docelowy (po tr		Moduł translacji NAT przed modułem VPN	
Protokół			
Орсје			





10. System wykrywania i blokowania włamań ASQ (IPS)

System zapobiegania włamaniom (IPS: Intrusion Prevention System) w urządzeniach STORMSHIELD UTM wykorzystuje unikalną, stworzoną w laboratoriach firmy STORMSHIELD technologię wykrywania i blokowania ataków ASQ (Active Security Qualification). Analizie w poszukiwaniu zagrożeń i ataków poddawany jest cały ruch sieciowy od trzeciej (Network Layer) do siódmej (Application Layer) warstwy modelu ISO/OSI. Stosowane są trzy podstawowe metody: analiza heurystyczna, analiza protokołów oraz analiza na podstawie sygnatur kontekstowych.

Analiza heurystyczna

W analizie heurystycznej podstawę stanowi analiza statystyczna oraz analiza zachowań. Na podstawie dotychczasowego ruchu i pewnych założeń dotyczących możliwych zmian określa się czy dany ruch jest uznawany za dopuszczalne odchylenie od normy, czy też powinien już zostać uznany za atak.

Analiza protokołów

Podczas analizy protokołów kontrolowana jest zgodność ruchu sieciowego przechodzącego przez urządzanie ze standardami RFC. Tylko ruch zgodny z tymi standardami może zostać przepuszczony. Kontroli poddawane są nie tylko poszczególne pakiety, ale także połączenia i sesje. W ramach technologii ASQ dla poszczególnych typów ruchu sieciowego opracowane zostały specjalne pluginy (wtyczki programowe) pracujące w trybie kernel-mode. Po wykryciu określonego typu ruchu (np. HTTP, FTP, SMTP, DNS, ..., włączając w to także protokoły przemysłowe m.in. Profinet, Modbus, S7, ...) automatycznie uruchamiany jest odpowiedni plugin, który specjalizuje się w ochronie danego protokołu. Tym samym, rodzaj stosowanych zabezpieczeń jest w sposób dynamiczny dostosowywany do rodzaju przepływającego ruchu.

Sygnatury kontekstowe

Ostatni z elementów, to systematycznie aktualizowane sygnatury kontekstowe. Pozwalają one na wykrycie znanych już ataków, które zostały sklasyfikowane i dla których zostały opracowane odpowiednie sygnatury. W tym przypadku zasadnicze znaczenie ma kontekst w jakim zostały wykryte pakiety charakterystyczne dla określonego ataku - tzn. rodzaj połączenia, protokół, port. Wystąpienie sygnatury ataku w niewłaściwym dla tego ataku kontekście nie powoduje reakcji systemu IPS. Dzięki temu zastosowanie sygnatur kontekstowych pozwala na znaczne zwiększenie skuteczności wykrywania ataków przy jednocześnie maksymalnym ograniczeniu ilości fałszywych alarmów. Innym istotnym czynnikiem wpływającym na wydajność stosowania sygnatur jest ich optymalizacja pod kątem skanowania podatności występujących w aplikacjach czy protokołach. Jeśli kilka ataków wykorzystuje tą samą podatność tworzona jest tylko jedna sygnatura dla tej podatności, dzięki czemu skraca się czas analizy, a system IPS zabezpiecza sieć również przed tymi atakami, które choć same nie zostały jeszcze opisane to wykorzystują znane dziury i wady protokołów czy aplikacji.

Konfiguracja domyślnych profili IPS

Konfiguracja IPS zawiera 10 w pełni konfigurowalnych profili. Jednak dwa z nich są szczególnie istotne, ponieważ zawierają one konfigurację domyślną dla skanowania ruchu przychodzącego i wychodzącego. Za ruch przychodzący uważa się ten, którego pierwszy pakiet pojawia się na interfejsie oznaczonym jako Zewnętrzny. Ruch wychodzący to taki, którego pierwszy pakiet transmisji pojawia się na interfejsie Wewnętrznym. Konfigurację profili domyślnych przeprowadza się w sekcji KONFIGURACJA > KONTROLA APLIKACJI > Ustawienia profili, gdzie domyślnie ruch przychodzący skanowany jest profilem IPS_00, a ruch wychodzący profilem IPS_01.





**	«	🕅 KONTROLA APLIKACJI / US	STAWIENIA PROFILI
MODUŁY	-		
Szukaj	12	Konfiguracja protokołu wspólna dla wsz	zystkich profili 13 Pokaż ustawienia dla profilu
🕅 KONTROLA APLIKACJI	^	Domyślne konfiguracje	
Alarmy		🕮 Ruch przychodzący :	(0) IPS_00 👻
Analiza protokołów		📴 Ruch wychodzący :	(1) IPS_01
Ustawienia profili			

Jeśli w ramach filtrowania ruch ma być skanowany innym profilem, to w konfiguracji **Firewall i NAT**, w kolumnie **Polityki filtrowania** należy zmienić opcję **Profil ASQ** z *W zależności od kierunku ruchu*, na wybrany profil.

Ogólne Akcja Akcja Ustawienia ogólne Adres źródłowy Ustawienia ogólne Port - Protokół Tryb pracy: Polityki filtrowania IPS_02 Polityki filtrowania IPS_02 Polityki filtrowania (00) IPS_00 Default INCOMING config: used fo (01) IPS_01 Default OUTGOING config: used fo (01) IPS_01 Default OUTGOING config: used fo (01) IPS_01 Antyspam: (02) IPS_02 IFiltrowanie URL: (03) IPS_03 Filtrowanie URL: (03) IPS_05 Filtrowanie FTP: (07) IPS_07 Filtrowanie SSL: (08) IPS_08	EDYCJA REGUŁY NUMI	ER 1				
Ogonie POLITYKI FILTROWANIA Akcja Ustawienia ogólne Adres źródłowy Ustawienia ogólne Adres docelowy Tryb pracy: Port - Protokół IPS_02 Polityki filtrowania IPS_02 Polityki filtrowania (00) IPS_00 Default INCOMING config: used fo (00) IPS_01 Default OUTGOING config: used fo (01) IPS_01 Default OUTGOING config: used fo (02) IPS_02 (03) IPS_03 filtrowanie URL: Filtrowanie URL: (04) IPS_04 Filtrowanie FTP: (05) IPS_05 Filtrowanie FTP: (07) IPS_07 Filtrowanie SSL: (08) IPS_08	Ogólao					
Akcja Adres źródłowy Adres docelowy Port - Protokół Polityki filtrowania Ustawienia ogólne Tryb pracy: Profil ASQ: IPS_02 V zależności od kierunku ruchu Filtrowanie treści (00) IPS_00 Default INCOMING config: used fo (01) IPS_01 Default INCOMING config: used fo (01) IPS_01 Default OUTGOING config: used fo Antyspam: (02) IPS_02 (03) IPS_03 Filtrowanie URL: Filtrowanie URL: Filtrowanie TP: (04) IPS_04 (05) IPS_05 Filtrowanie FTP: (07) IPS_07 Filtrowanie SSL: (08) IPS_08 (08) IPS_08	Aleia	POLITYKI FILTROWANIA				
Adres 2rodiowy Polityki filtrowania Tryb pracy: IPS_02 IPS_02 Polityki filtrowania Profil ASQ: IPS_00 IPS_00 IPS_00 Filtrowanie treści (00) IPS_00 Default INCOMING config: used fo IOU IPS_01 IPS_01 Antywirus I: (01) IPS_01 Default OUTGOING config: used fo IOU IPS_02 IOU IPS_02 Sandboxing I: Antyspam: (02) IPS_02 IOU IPS_03 IPS_03 IPS_03 Filtrowanie URL: IPS_04 IPS_05 IOU IPS_05 IPS_05 IPS_05 Filtrowanie FTP: (07) IPS_07 IPS_08 IPS_08 IPS_02 IPS_08	Аксја	– Ustawienia ogólne				
Adres docelowy Port - Protokół Polityki filtrowania Image: Profil ASQ: Image:	Adres zrodłowy	ootamenia ogome				
Port - Protokół Profil ASQ: IPS_02 • Polityki filtrowania W zależności od kierunku ruchu • Filtrowanie treści (00) IPS_00 Default INCOMING config: used fo Antywirus • : (01) IPS_01 Default OUTGOING config: used fo Sandboxing • : (02) IPS_02 (03) IPS_03 Filtrowanie URL: (04) IPS_04 (05) IPS_05 Filtrowanie poczty: (06) IPS_06 (06) IPS_07 Filtrowanie SSL: (08) IPS_08 •	Adres docelowy	Tryb pracy:	105	-		
Polityki filtrowania Profil ASQ: IPS_02 IPS_02 W zależności od kierunku ruchu W zależności od kierunku ruchu IPS_00 Filtrowanie treści (00) IPS_00 Default INCOMING config: used fo Antywirus ① : (01) IPS_01 Default OUTGOING config: used fo Sandboxing ① : (02) IPS_02 (03) IPS_03 Antyspam: (02) IPS_02 (03) IPS_03 Filtrowanie URL: (04) IPS_04 (05) IPS_05 Filtrowanie poczty: (06) IPS_06 (06) IPS_06 Filtrowanie FTP: (07) IPS_07 (08) IPS_08	Port - Protokół	nyb pracy.		•		
Filtrowanie treściW zależności od kierunku ruchuFiltrowanie treści(00) IPS_00 Default INCOMING config: used foAntywirus I:(01) IPS_01 Default OUTGOING config: used foSandboxing I:(02) IPS_02 (03) IPS_03Filtrowanie URL:(02) IPS_02 (03) IPS_03Filtrowanie poczty:(04) IPS_04 (05) IPS_05 (06) IPS_06Filtrowanie FTP:(07) IPS_07 (08) IPS_08 (08) IPS_08	Polityki filtrowania	Profil ASQ:	IPS_02	-		
Filtrowanie treści(00) IPS_00Default INCOMING config: used foAntywirus I:Sandboxing I:Sandboxing I:Antyspam:(02) IPS_02(03) IPS_03Filtrowanie URL:Filtrowanie poczty:(05) IPS_05Filtrowanie FTP:(07) IPS_07Filtrowanie SSL:(08) IPS_08			W zależności od kierunku ruchu	^		
AntywirusDefault INCOMING config: used foAntywirus(01) IPS_01Default OUTGOING config: used foAntyspam:(02) IPS_02(03) IPS_03Filtrowanie URL:(04) IPS_04Filtrowanie poczty:(05) IPS_05Filtrowanie FTP:(07) IPS_07Filtrowanie SSL:(08) IPS_08		Filtrowanie treści	(00) IPS_00			
Antywirus ①:: (01) IPS_01 Default OUTGOING config: used fo Antyspam: (02) IPS_02 (03) IPS_03 (04) IPS_04 (05) IPS_05 (06) IPS_05 (06) IPS_06 Filtrowanie FTP: (07) IPS_07 Filtrowanie SSL: (08) IPS_08			Default INCOMING config: used fo			
SandboxingDefault OUTGOING config: used foAntyspam:(02) IPS_02 (03) IPS_03Filtrowanie URL:(04) IPS_04 (05) IPS_05Filtrowanie poczty:(06) IPS_06Filtrowanie FTP:(07) IPS_07Filtrowanie SSL:(08) IPS_08 (08) IPS_02		Antywirus 🕕 :	(01) IPS_01			
Sandboxing C: Antyspam: (02) IPS_02 (03) IPS_03 Filtrowanie URL: Filtrowanie poczty: (04) IPS_04 (05) IPS_05 (06) IPS_06 Filtrowanie FTP: (07) IPS_07 Filtrowanie SSL: (08) IPS_08			Default OUTGOING config: used			
Antyspam: (02) IPS_02 (03) IPS_03 (03) IPS_04 (04) IPS_04 (05) IPS_05 Filtrowanie poczty: (06) IPS_06 Filtrowanie SSL: (07) IPS_07 Filtrowanie SSL: (08) IPS_08		Sandboxing • :	fo			
(03) IPS_03 Filtrowanie URL: (04) IPS_04 (05) IPS_05 (06) IPS_06 Filtrowanie FTP: (07) IPS_07 Filtrowanie SSL: (08) IPS_08		Antyspam:	(02) IPS_02			
Filtrowanie URL: (04) IPS_04 Filtrowanie poczty: (05) IPS_05 filtrowanie FTP: (06) IPS_07 Filtrowanie SSL: (08) IPS_08			(03) IPS_03			
Filtrowanie poczty: (05) IPS_05 (06) IPS_06 Filtrowanie FTP: (07) IPS_07 Filtrowanie SSL: (08) IPS_08		Filtrowanie URL:	(04) IPS_04			
Filtrowanie poczty: (06) IPS_06 Filtrowanie FTP: (07) IPS_07 Filtrowanie SSL: (08) IPS_08		Filtrowopia poarty	(05) IPS_05			
Filtrowanie FTP: (07) IPS_07 Filtrowanie SSL: (08) IPS_08		Filliowanie poczty.	(06) IPS_06			
Filtrowanie SSL: (08) IPS_08		Filtrowanie FTP:	(07) IPS_07			
(00) 100 - 00 V		Filtrowanie SSL:	(08) IPS_08			
			(00) 100 00	~		
		>	🕻 ANULUJ 🔷 OK			
X ANULUJ V OK						

Konfiguracja analizy protokołów

Konfiguracja analizowania protokołów poprzez mechanizm IPS znajduje się w sekcji **KONFIGURACJA > KONTROLA APLIKACJI > Analiza protokołów**. Znajduje się tutaj konfiguracja pluginów dla wszystkich najważniejszych protokołów z warstw od trzeciej (L3) do siódmej (L7) modelu ISO/OSI. Każdy z pluginów zawiera opcje konfiguracyjne dotyczące skanowanych charakterystycznych dla niego parametrów. Dzięki temu efektywność i prędkość skanowania jest maksymalnie zwiększona, ponieważ IPS bada jedynie te





elementy, które mają związek z tym protokołem, natomiast nie analizuje tego co z tym protokołem nie ma żadnego związku.

W początkowej fazie transmisji danych używane są pluginy IP oraz TCP/UDP. Odpowiadają one za prawidłowe otwarcie sesji a więc:

Plugin IP – odpowiada za fragmentację pakietów i ich wielkość.

*- «	🕅 KONTROLA APLIKACJI / ANALIZA PF	ROTOKOŁÓW
Szukaj	Wyszukiwanie 🖈 🖉	Konfiguracja protokolu wspólna dla wszystkich profili 🛛 🕄 Pokaż ustawienia dla profilu
H USTAWIENIA SYSTEMOWE	Komunikatory I Protokoły IP	ANALIZA PROTOKOŁU
KONFIGURACJA SIECI		Analiza protokolu
S OBIEKTY	I SCTP	Orranicz wartość MTU (framentacia) :
	ICP UDP Protokoły Microsoft	Ogranicz Hartoor Hito (raginentacja).
* POLITYKI OCHRONY	Protokoły przemysłowe VoIP / Streaming	Fragmentacja
		Minimalny rozmiar fragmentu : 140 🗸
Analiza protokołów	1 FTP 1 HTTP	
	V NTD	

Plugin TCP/UDP – odpowiada za otwarcie, utrzymanie i zamknięcie sesji.

Do każdego nowego połączenia podłączany jest odpowiedni plugin. O tym, który plugin będzie użyty decyduje port, na którym odbywa się komunikacja. Wybierając opcję **Pokaż ustawienia wspólne dla wszystkich profili** w konfiguracji pluginu mamy możliwość zdefiniowania na jakich portach ten plugin będzie używany. Jeśli żaden z pluginów nie obsługuje komunikacji na porcie używanym w czasie połączenia, to ruch będzie skanowany kolejno przez wszystkie pluginy, które mają zaznaczoną opcję **Automatyczne wykrywanie protokołu** w celu ustalenia jakiego typu jest to ruch, i który plugin powinien się nim zająć.





	* *	(1) http_01	👻 🛛 Edytuj 🕶	0	ta Pokaż ustawienia wspólne dla v	vszystkich profili
 I Komunikatory I Protokoły IP 		ANALIZA PROTOKOŁU	PROXY	ICAP	ANALIZA ZAWARTOŚCI	ANALIZA SANDBOXIN
 Protokoły Microsoft Protokoły przemysłowe VolP / Streaming NS FTP 		 Opcje silnika wyszukiwa Restrykcje dla treści YouT 	nia ube :	Aut	omatyczne wykrywanie protokołu łłącz filtr wyszukiwania (Safesear czony	rch)
1 нттр		ZEZWOLONE DOMENY				
I NTP						
► Dodaj × Usuń Vort						\leftarrow
ttp						
omyślne porty dla protokołu - S	SL					
omyślne porty dla protokołu - S 🕇 Dodaj 🗡 Usuń	SL					
omyślne porty dla protokołu - S • Dodaj × Usuń ^I ort	SL					

Konfiguracja sygnatur kontekstowych

Jak już wspomniano wyżej, sygnatury służą do filtrowania ruchu pod kątem wystąpienia cech charakterystycznych dla konkretnej podatności lub ataku sieciowego. W przypadku wykrycia schematu działania zgodnego z takim zagrożeniem wywoływany jest odpowiedni alarm oraz wykonywane są zdefiniowane dla niego akcje, które mają na celu np. zablokowanie ruchu. Konfiguracja sygnatur odbywa się w zakładce KONFIGURACJA > KONTROLA APLIKACJI > Alarmy.





*	MODURY -	🕅 ко	DNFIGURACJA ALARMÓW IPS					
Sz	ukaj 🦼 🗷	IPS_01	(Default OUTGOING) Szablon • 🏶 Zatwierdź nowe alarmy 🔩 wid	lok: profil				
141		* Ws	zystkie 🔄 Aplikacje 🔟 Zabezpieczenia 🗭 Malware 📗 Szukaj	× Filtr	uj -			
		Alarm		Akcja ≞ ▼	Priorytet ≞▼	Nowy	±•	Kontekst:id
		H 6	P2P : BitTorrent protocol	Zezwól	🔌 Ignoruj	券		bittorrent:client:1
	OBIEKTY	80	P2P : BitTorrent Sync	Zezwól	🖹 Ignoruj	#		bt-sync:client:1
Ť	UZYTKOWNICY		COTP : invalid protocol	🗢 Zablokuj	🎾 Wysoki			cotp:379
৵	POLITYKI OCHRONY		COTP : invalid message length	🗢 Zablokuj	🎾 Wysoki			Ustawienie akcji Zezw
Ø	KONTROLA APLIKACJI		COTP : unexpected TPDU	Zablokuj	箻 Wysoki			cotp:386
	Alarmy		DataHub unicode buffer overflow exploit detected	🗢 Zablokuj	🔍 Niski	券		datahub:client:1
	Analiza protokołów		DCERPC: Invalid path in a NetPathCanonicalize/NetPathCompare MS-RPC request	Zablokuj	🎾 Wysoki	₩		dcerpc:request:data:1
	Ustawienia profili		DCERPC : Microsoft RPCSS service vulnerability (CVE-2003-0352)	🗢 Zablokuj	🎾 Wysoki	#		dcerpc:request:data:2
	Audyt podatności		DCERPC : Microsoft LSASS service vulnerability (CVE-2003-0533)	🗢 Zablokuj	🎾 Wysoki	#		dcerpc:request:data:3
	Reputacia hosta		DCERPC : Microsoft MSMQ service vulnerability (CVE-2005-0059)	🗢 Zablokuj	竿 Wysoki	\$		dcerpc:request:data:4
	Antaviruo		DCERPC : Microsoft DNS service vulnerability (CVE-2007-1748)	🗢 Zablokuj	竿 Wysoki	#		dcerpc:request:data:5
	Antywirds		DCERPC : Invalid path in a MS-RPC request - MS08-067	🗢 Zablokuj	🎾 Wysoki	様		dcerpc:request:data:6
	Antyspam		DCERPC : Microsoft vulnerability in print spooler (CVE-2010-2729) allows remote a	Zezwól	🎾 Wysoki	₩		dcerpc:request:data:7
•	POŁĄCZENIA VPN		DCERPC : WMI is used on the network, it could be abused by attackers	Zezwól	🔌 Ignoruj	様		dcerpc:request:data:8
Ü	ADMINISTRACJA	×	Malware : Conficker Version A payload detected	🗢 Zablokuj	🏩 Niski	券		dcerpc_tcp:client:1

Okno Alarmy zawiera następujące elementy:

- Alarm nazwa alarmu/sygnatury.
- Akcja Zablokuj/Zezwól ruch sieciowy.
- Priorytet określa poziom informowania administratora o pojawieniu się danego zagrożenia. Alarmy z priorytetem Wysokim lub Niskim zapisywane są w logach. Alarmy, dla których ustawiona jest akcja lgnoruj nie są wyświetlane (akcja dla tego alarmu nadal jest wykonywana) opcja ta jest przydatna jeśli jakiś alarm "zaśmieca" logi.
- Nowy w tej kolumnie dla każdej nowej sygnatury pojawia się symbol 469. Laboratoria STORMSHIELD na bieżąco pracują nad wykrywaniem nowych ataków, stąd regularnie będą się pojawiać nowe sygnatury. Ten symbol ma na celu wyróżnienie nowych sygnatur, z którymi powinien się zapoznać administrator.
- Kontekst określa plugin jakim dane połączenie jest obsługiwane, poza kontekstem podawane jest również ID sygnatury, co ułatwia przeszukiwanie bazy sygnatur.
- Zaawansowane pozwala na podjęcie dodatkowych akcji, takich jak: wysłanie powiadomienia email, przeniesienie maszyny generującej dany alarm do kwarantanny na określony czas, wykonanie zrzutu pakietu (dump) czy też zastosowanie kolejki QoS dla ruchu generującego dany alarm.

🚺 Uwaga

Profile **Analizy protokołów** i **Alarmy** są ze sobą ściśle powiązane, tzn. profil np. **http_00** Analizy protokołów oraz profil **IPS_00** Alarmów tworzą profil **ASQ IPS_00**, a profil **http_02** Analizy protokołów oraz profil **IPS_02** Alarmów tworzą Profil **ASQ IPS_02**. Profil ASQ jest filtrem IPS implementowanym na poziomie reguł firewall.

57

NEXT GENERATION FIREWALL PODRĘCZNIK UŻYTKOWNIKA





W celu szybszej oraz sprawniejszej konfiguracji sygnatur można skorzystać z filtrowania na podstawie rodzaju sygnatur tj. Aplikacje, Zabezpieczenia, Malware, a także z pola "Szukaj" lub opcji Filtruj zawierającej predefiniowane kategorie aplikacji.

Ø KONFIGURACJA ALARMÓW IPS								
IPS_01 (Default OUTGOING) Szablon 🔹 🇱 Zatwierdź nowe alarmy 🎦 widok: profil								
📧 Wszystkie 🔝 Aplikacje 🔟 Zabezpieczenia 🗭 Malware 🛛 spoofing 📉 🔀 Filtruj 🕶								
Alarm		Akcja	E▼ Priorytet	±.	Nowy	≞₹	Kontekst:id	
Û	DNS id spoofing	🗢 Zablokuj	🎾 Wysoki				dns:38	
Û	Targeted DNS spoofing	🗢 Zablokuj	🎾 Wysoki				dns:152	
¥	Malware : Tatanga banking trojan detected	🗢 Zablokuj	🔔 Niski		袋		http:url:raw:11	
Û	Web 2.0 : Malformed link causing URL spoofing o	🗢 Zablokuj	😩 Niski		券		http:html:tag:attribute:28	
V	Web 2.0 : Microsoft browser spoofing vulnerability	🗢 Zablokuj	😩 Niski		袋		http:mix:285	
Û	Web 2.0 : Microsoft Edge spoofing vulnerability (C	🗢 Zablokuj	🔔 Niski		券		http:mix:290	
Û	IP loopback address spoofing	🗢 Zablokuj	筆 Wysoki				ip:0	
٢	IP address spoofing	🗢 Zablokuj	筆 Wysoki				ip:1	
Û	IP address spoofing on bridge	🗢 Zablokuj	🔔 Niski				ip:70	
٢	IP address spoofing on IPsec interface	🗢 Zablokuj	🈩 Niski				ip:108	

Monitorowanie działania IPS

Działanie systemu IPS możemy kontrolować z poziomu zakładki **MONITORING > Logi > Alarmy**. Znajdują się tutaj wpisy o wystąpieniach wszystkich **Alarmów** o priorytecie Niski lub Wysoki, a także informacje o ruchu zablokowanym przez **Analizę protokołów** (pluginy).

Z tego poziomu możliwe jest również wyświetlenie strony KB (Knowledge Base) zawierającej pełen opis danego alarmu. Pomoc ta jest dostępna z poziomu menu kontekstowego (po kliknięciu na danym wpisie prawym przyciskiem myszy)

STORMSHIELD V4.0.1			F						
V Network Security	MONITORING	KONFIGUR	ACJA	VMSNSX09C0035A9					
*- «		,							
70 PANEL KONTROLNY	UG/ALARIVIT								
	Ostatnia godzina	- 🗰 ;	C Odśwież	Szukaj			» Zaawa	nsowane wyszukiwa	nie
	SZUKAJ OD - 24.01.2	2020 14:25:42	- DO - 24.01.20	20 15:25:42					
SZUKAJ	Data zapisu	Akcja	Priorytet	Szczegóły	Kn	Nazwa obiektu ź	źródłowego	Nazwa portu źródł	1
Wszystkie	15:25:13		Niski	Privacy access right acquired	1	10.11.11.254			
Ruch sieciowy	15:03:29	Zablokuj	🕊 Wysoki	IP address spoofing (type=1)		10 0 0 2		enhemeral fw ude	
Alama	15:03:29	Zablokuj	🎾 Wysoki	IP address spoofing (type=1)	Q Użyj	wartości jako kryt	erium wyszu	kiwania	
Alarmy	15:03:24	Zablokuj	🎾 Wysoki	IP address spoofing (type=1)	Q Skop	piuj wybrany wiersz	do schowka	L .	
Web	15:03:21	Zablokuj	🎾 Wysoki	IP address spoofing (type=1)	🎭 Prze	jdź do konfiguracji	alarmu		
Podatności	15:03:17	Zablokuj	🎾 Wysoki	IP address spoofing (type=1)	? Otw	órz "Pomoc", aby w	yświetlić szo	zegóły tego alarmu	
E-Mails	15:03:17	Zablokuj	🎾 Wysoki	IP address spoofing (type=1)		10.0.0.2		ephemeral_fw_udp)
VPN	15:03:17		🏩 Niski	Connection terminated for we	eba				





11. Konfiguracja Audytu podatności (SEISMO)

Moduł Audyt podatności jest pasywnym skanerem chronionych sieci. Pasywnym skanerem określamy taki, który nie generuje dodatkowego ruchu w sieci ani nie wymaga instalacji dodatkowego oprogramowania na komputerach w sieci. Skanuje on ruch sieciowy przechodzący poprzez urządzenie STORMSHIELD UTM w kontekście występowania podatności w aplikacjach sieciowych i systemach operacyjnych działających na hostach w tych sieciach.

Audyt podatności wymaga zakupu dodatkowej licencji.

Konfiguracja Audytu podatności odbywa się w zakładce **KONFIGURACJA > KONTROLA APLIKACJI > Audyt podatności**. Jeśli opcji nie da się włączyć oznacza to, iż zainstalowana na urządzeniu licencja nie zawiera funkcji pasywnego skanera sieci.

Audyt podatności nie blokuje żadnego ruchu, a jedynie wyświetla informacje na temat wykrytych zagrożeń.

W przypadku konfiguracji audytu podatności istotne jest:

- Określenie obiektów, które mają być monitorowane host, sieć, grupa hostów, zakres.
- Wybranie profilu prowadzonego audytu dla wskazanych obiektów.
- Skonfigurowanie czasu przez jaki informacje o wykrytych zagrożeniach będą przechowywane.
- Zdefiniowanie BIAŁEJ LISTY wykluczeń ze skanowania.

*	- «						
•	MODUŁY –						
Szu	ukaj 🦼 🦉	Rewindemienia e mail					
÷†‡	USTAWIENIA SYSTEMOWE						
	KONFIGURACJA SIECI	Szczegołowy raport:	Nie wysyłaj w	Wiadomosc V			
0)	OBIEKTY	Uproszczony raport:	Nie wysyłaj wi	wiadomosc 💌			
•	UŻYTKOWNICY						
ᆉ	POLITYKI OCHRONY	MONITOROWANE OBIEKTY					
Ø		Wyszukiwanie	🕂 Dodaj 🗙 Usuń				
		Obiekt (host - sieć - grupa hostów - z	zakres)	Profil			
	Alarmy	WWW-svr-priv-ip		Serwery http			
	Analiza protokołów	SMTP-svr-priv-ip		Serwery pocztowe			
	Ustawienia profili	Network_internals		Wszystkie			
	Audyt podatności	 Zaawansowane 					
	Reputacja hosta	Okres przechowywania informac	cji (dni): 7	÷			
	Antywirus	BIAŁA LISTA					
	Antyspam	🕂 Dodaj 🗙 Usuń					
-	POŁĄCZENIA VPN	Obiekt (host - sieć - grupa hostów	ı - zakres)				
[]	ADMINISTRACJA	lab					

Domyślnie skanowany jest cały ruch generowany przez grupę **Network_Internals,** czyli wszystkie stacje podłączone do interfejsów określonych jako **Wewnętrzne (LAN,DMZ)**.

Informacje zebrane przez moduł Audyt podatności można przeglądać w dziennikach logowania MONITORING > LOGI >Podatności lub z poziomu monitorowania hostów MONITORING > MONITOROWANIE > Hosty, po zaznaczeniu interesującego nas hosta dostępna jest zakładka PODATNOŚCI zawierająca





podatności wykryte dla danego hosta. Kolejne zakładki APLIKACJE, USŁUGI, INFORMACJE zawierają dodatkowe informacje generowane przez audyt podatności dotyczące aplikacji oraz systemów działających na hoście. Dzięki temu Audyt podatności jest także doskonałym narzędziem do monitorowania zainstalowanych aplikacji sieciowych i systemów operacyjnych, które działają w sieciach chronionych przez STORMSHIELD UTM.

LOG / PODATNOŚCI PANEL KONTROLNY - 💼 C Odśwież | Szuka Dzisiaj » Zaaw ≡ Czv ość 🕶 KONFIGURACJA LOGÓW SZUKAJ OD - 14.01.2020 00:00:00 - DO - 14.01.2020 15:42:55 SZCZEGÓŁ Y DOTYCZACE DZIENNIKA iom zag... Szczegóły Data Data zapisu III Wysoki Mozilla Firefox / Thunderbird Multiple Vulne Mer 12:56:42 Data zapisu 12:56:42 Go Q. Użyj wartości jako kryte 12:54:21 Wysoki Google Chrome Multiple Vulnerabilities Fixed by 50.0.2661.94 Data i godzina rozpoczecia 12:56:42 Anonymized Go Q, Skopiuj wybrany wiersz do scho Wysoki Google Chrome Multiple Vulnerabilities Fixed by 50.0.2661.75 12:54:21 Anonymized Różnica czasu (różnica między GM... +0100 Δlarmy 12:54:21 Wysoki Google Chrome Multiple Vulnerabilities Fixed by 50.0.2661.102 grupa:Różne Go ? Ot noc", aby wy 12:54:21 Google Chrome Multiple Vulnerabilities Fixed by 51.0.2704.79 Google Chrome 49 0 2623 112 Plik logu Wyenki 12:54:21 Google Chrome Unspecified Vulnerabilities Fixed by 51.0.2704.103 Google_Chrome_49.0.2623.112 Anonymized Poziom zagrożenia Wysoki Wysoki 12:54:21 Google Chrome Multiple Vulnerabilities Fixed by 52.0.2743.82 Google_Chrome_49.0.2623.112 E-Mails Mozilla Firefox / Th Szczegóły Wysoki Google Chrome OS Unspecified Vulnerabilities Fixed by 60.0.3112.112 12:54:21 Vulnerat Anonymized Google_Chrome_49.0.2623.112 Nazwa Firefox_30.0 12:54:21 Wyseki Google Chrome OS Unspecified Vulnerabilities Fixed by 60.0 3112 101 Google Chrome 49.0.2623.112 Anonymized ID podatnośc Anonymized 140455 12:54:21 Wysoki Google Chrome Multiple Vulnerabilities Fixed by 59.0.3071.86 Google_Chrome_49.0.2623.112 Argumer Firefox_30.0 12:54:21 Google Chrome Multiple Vulnerabilities Fixed by 60.0.3112.7 oogle_Chrome_49.0.2623.112 Google_Chrome_49.0.2623.112 eb Client 12:54:21 Wytoki Google Chrome Multiple Vulnerabilities Fixed by 59.0.3071.104 Grupa Anonymized Exploit 🖒 Zdalny 12:54:21 Wysoki Google Chrome OS Unspecified Vulnerabilities Fixed by 58.0.3029.140 Anonymized Google_Chrome_49.0.2623.112 12:54:21 Wysoki Google Chrome Multiple Vulnerabilities Fixed by 57.0.2987.133 Google_Chrome_49.0.2623.112 Rozwiąza Rozwiaza Google Chrome OS Unspecified Vulnerabilities Fixed by 57.0.2987 123 Wyseki 12:54:21 Anonymized Google_Chrome_49.0.2623.112 Wysoki Google Chrome Multiple Vulnerabilities Fixed by 56.0.2924.76 Google_Chrome_49.0.2623.112 12:54:21 Anonymized Rozwia 2014-07-23 12:54:21 Wysoki Google Chrome Multiple Vulnerabilities Fixed by 55.0.2883.75 Google_Chrome_49.0.2623.112 Priorytet 🌋 Wysoki 12:54:21 Wysoki Google Chrome Multiple Vulnerabilities Fixed by 54.0.2840.98 and 54.0.2840... Anonymized Google_Chrome_49.0.2623.112 Źródło 12:54:21 Wysoki Google Chrome V8 Out-of-Bounds Memory Access Vulnerability Fixed by 54.0., Anonymized Google_Chrome_49.0.2623.112 Wysoki Google Chrome Multiple Vulnerabilities Fixed by 54.0.2840.59 Anonymized 12:54:21 Google_Chrome_49.0.2623.112

Poniżej przedstawiony jest przykładowy wynik działania modułu Audyt podatności:

W raporcie znajdziemy między innymi informację o poziomie ważności wykrytego zagrożenia, typie zagrożenia (Web Client itp.), sposobie jego wywołania (Zdalne/Lokalne), informacje o komputerze, na którym została wykryta podatna aplikacja oraz o tym w jakiej wersji jest ta aplikacja. Aby uzyskać dodatkowe informacje o zagrożeniu można z poziomu menu kontekstowego kliknąć **Otwórz "Pomoc", aby wyświetlić szczegóły tej podatności**. Na stronie pomocy można znaleźć dokładny opis zagrożenia oraz linki do stron, na których zostało ono opisane, a także wyjaśnienie jakie czynności należy podjąć, aby wyeliminować to zagrożenie.







12. Autoryzacja użytkowników

W celu określenia obiektu źródłowego, z którego pochodzi ruch sieciowy zazwyczaj stosuje się adres IP takiego hosta. Jednak takie podejście nie informuje o konkretnym użytkowniku lecz o wszystkich użytkownikach danego hosta.

Aby określić konkretnego użytkownika, od którego pochodzi dany ruch sieciowy można skorzystać z mechanizmu autoryzacji użytkowników.

Urządzenie STORMSHIELD UTM pozwala na to poprzez skorzystanie z usług katalogowych. Dostępne są trzy typy takich usług:

- Microsoft Active Directory,
- LDAP,
- LDAP za pośrednictwem PosixAccount.

Dodatkowo istnieje możliwość utworzenia jednej wewnętrznej bazy LDAP bezpośrednio w urządzeniu. Należy jednak pamiętać, iż jednocześnie można skonfigurować w urządzeniu maksymalnie pięć takich usług katalogowych: jednej wewnętrznej bazy i czterech zewnętrznych lub pięciu zewnętrznych baz.

Każda z tych baz może być użyta do:

- tworzenia reguł filtrowania/NAT per użytkownik (nie wymaga adresów IP w regułach),
- tworzenia tuneli VPN typu Client-to-Site,
- delegowania zadań administracji urządzeniem na użytkowników.

Tworzenie wewnętrznej bazy użytkowników

Aby skonfigurować wewnętrzną bazę użytkowników na urządzeniu STORMSHIELD UTM należy przejść na zakładkę **KONFIGURACJA > UŻYTKOWNICY > Konfiguracja bazy LDAP**. Jeżeli na urządzeniu nie ma skonfigurowanej żadnej bazy użytkowników uruchomi się KREATOR KONFIGURACJI, jeśli jakakolwiek baza była wcześniej utworzona, należy wybrać opcję **Dodaj nowy LDAP**. W kreatorze konfiguracji należy wybrać opcję **Utwórz wewnętrzną bazę LDAP**.





UŻYJ KREATORA KONFIGURACJI		
WYBIERZ TYP BAZY LDAP - KROK 1 Z 3		
 Podłącz do bazy Microsoft Active Directory 		
 Podłącz do zewnętrznej bazy LDAP 		
O Podłącz do PosixAccount zewnętrznej bazy LDAP		
Utwórz wewnętrzną bazę LDAP		
	× ANULUJ « WSTECZ	DALEJ »

W kolejnym oknie konfiguracyjnym należy wypełnić odpowiednie opcje:

- Organizacja nazwa firmy np. Stormshield;
- **Domena** nazwa domeny;
- Hasło i Potwierdź hasło hasło administratora domeny (może być użyte do integracji zewnętrznej usługi z lokalną bazą LDAP).

62





UŻYJ KREATORA KONFIGU	RACJI				
KONFIGURACJA DOSTEP	U - KROK 2 Z 3				
Organizacja:	Stormshield				
Domena:	stormshield.local				
Hasło:	•••••	7			
Potwierdź hasło:	•••••				
	Bardzo silne				
			× ANULUJ	≪ WSTECZ	DALEJ »

W kolejnym oknie kreatora można skonfigurować dodatkowe opcje bazy LDAP:

• Aktywne uwierzytelnianie dla profilu 0 na wybranym interfejsie – na wskazanym interfejsie zostanie automatycznie uruchomiony portal uwierzytelniania (Captive portal), o którym nieco szerzej w dalszej części tej dokumentacji.

Jeśli profil 0 (internal) jest już przypisany do jakiegokolwiek interfejsu opcja będzie nieaktywna;

- Włącz żądania użytkowników dla profilu 0 na portalu uwierzytelniania włącza usługę rejestracji użytkowników poprzez którą użytkownicy będą mogli zgłaszać prośby o założenie konta w usłudze LDAP, dzięki temu rola administratora może być ograniczona tylko do aktywowania kont zakładanych przez użytkowników;
- Publiczna baza LDAP baza użytkowników może być wykorzystywana przez inne, zewnętrzne usługi sieciowe takie jak np. serwer FTP.



NEXT GENERATION FIREWALL PODRĘCZNIK UŻYTKOWNIKA





UŻYJ KREATORA KONFIGURACJI
UWIERZYTELNIANIE - KROK 3 Z 3
Aktywne uwierzytelnianie dla profilu 0 na wybranym interfejsie:
📧 Włącz żądania użytkowników dla profilu 0 na portalu uwierzytelniania
Publiczna baza LDAP
X ANULUJ

Wybranie przycisku **Zakończ** kończy pracę kreatora i pojawi się okno konfiguracyjne bazy LDAP, w którym możemy wybrać między innymi czy możliwa ma być komunikacja z tą bazą z zewnątrz i czy ma odbywać się w formie zaszyfrowanej czy też nie.





*-	W UŻYTKOWNICY / KONFIGU	RACJA BAZY LDAP
MODUŁY		
Szukaj	SKONFIGUROWANE BAZY UZYTKO	WNIK
耕 USTAWIENIA SYSTEM	+ Dodaj nowy LDAP =	Akcja Konfiguracja
	Domain name	
	عان Stormsnield.stormsnield.local	Włącz usługę LDAP/Active Directory
COBIEKTY		Organizacja: Stormshield
		Domena: stormshield.local
Użytkownicy i grupy		Login: cn=NetasqAdmin
Konta tymczasowe		Hasio:
Polityki dostępu		
Portal uwierzytelniania		Sila hasla
Żadania użytkowników		
Konfiguracja bazy LDA	P	Dostęp z zewnątrz do bazy LDAP
POLITYKI OCHRONY		
KONTROLA APLIKACJI		Zezwól na dostęp bez szyfrowania (PLAIN)
		Aktywuj dostęp SSL
		Użyj certyfikatu: Trak certyfikatu Trak vertyfikatu
ADMINISTRACJA		
		A Zaawansowane
		Użyj konta urządzenia do sprawdzenia poprawności konfiguracji bazy
		Zezwalaj na zagnieżdżanie grup

Integracja STORMSHIELD UTM z Microsoft Active Directory

Pierwsze okno kreatora jest takie samo jak w przypadku tworzenia wewnętrznej bazy LDAP. Należy w nim wybrać **Podłącz do Microsoft Active Directory.**

W kolejnym oknie konfiguracyjnym dostępne są następujące pola:

- Nazwa domeny nazwa umożliwiająca identyfikację bazy AD szczególnie przydatna, gdy na urządzeniu będzie skonfigurowanych kilka baz LDAP. Zalecane jest aby w tym polu była wprowadzona nazwa DNS domeny.
- Serwer obiekt reprezentujący adres IP kontrolera domeny;
- Port port używany do komunikacji z LDAP (domyślnie TCP 389);
- Domena typu root (Base DN) pełna nazwa domeny, np.: dla domeny stormshield.internal będzie to DC=Stormshield,DC=internal;
- Login (DN użytkownika) login użytkownika używanego do integracji z AD wraz ze wskazaniem kontenera (CN) lub jednostką organizacyjną (OU) AD, w którym znajduje się ten użytkownik. Przykładowo, jeśli do integracji utworzymy dedykowane konto *Stormshield*, które umieścimy w kontenerze *Users*, to w polu *Login* należy wpisać: *CN=Stormshield,CN=Users*;
- Hasło hasło domenowe użytkownika wskazanego w polu Login.





UŻYJ KREATORA KONFIGURA	CJI				
KONFIGURACJA DOSTEPU -	KROK 2 Z 2				
			AND DESCRIPTION OF ADDRESS		
Nazwa domeny:	stormshield.internal				
Serwer:	ADDC1	▼ 8.			
Port:	Idap	▼ 8+			
Domena typu root (Base DN):	DC=Stormshield,DC=internal				
Login (DN użytkownika):	CN=Stormshield,CN=Users				
Hasło:	•••••	Þ			
			× ANULUJ	WSTECZ	✓ ZAKOŃCZ

\rm 🛛 Uwaga

Najczęstsze problemy związane z integracją z domeną AD polegają na wykorzystaniu konta, które nie znajduje się w kontenerze *Users* domeny AD (należy stworzyć użytkownika w kontenerze *Users* i wyłączyć rotację haseł)

W kolejnym oknie kreatora można włączyć opcję *Aktywne uwierzytelnianie dla profilu 0 na wybranym interfejsie*.









UŻYJ KREATORA KONFIGURACJI		
UWIERZYTELNIANIE - KROK 3 Z 3		
Aktywne uwierzytelnianie dla profilu 0 na wybranym interfejsie: in	*	
	X ANULUJ « WSTECZ ✓ ZAKOŃCZ	

Po zakończeniu pracy kreatora powinno pojawić się poniższe okno, które będzie potwierdzeniem poprawnej integracji.

MODUŁY -	L UŻYTKOWNICY / KO	INFIGURACJA B	AZY LDAP			
Szukaj 🗶 🦉	+ Dodai nowy I DAP					
USTAWIENIA SYSTEMOWE	Domain name		KONFIGURACJA STR	UKTURA		
KONFIGURACJA SIECI	Stormshield.internal		Dostęp do serwera			
S OBIEKTY						
			☑ Włącz usługę LDAP//	Active Directory		
Lizetkownicy i grupy			Serwer:	ADDC1	▼ 5.	
Vente transmissing rigraph			Port:	ар	▼ 20+	
Konta tymczasóWe			Podstawowy DN:	DC=Stormshield,DC=internal		
Polityki dostępu			Login:	CN=Stormshield,CN=Users		
Portal uwierzytelniania			Hasło:			
Żądania użytkowników						
Konfiguracja bazy LDAP			 Połączenie do serwer 	a za pomocą protokołu SSL		
POLITYKI OCHRONY			Aktywuj dostęp SSL			
KONTROLA APLIKACJI			Sprawdź certyfikat C/			
POŁĄCZENIA VPN			Wybierz zaufane CA:		- ×	
D ADMINISTRACJA						
			 Zaawansowane 			
			Serwer zanasowy:	ADDC2	× 8.	
			Użvi konta urządzenia	do sprawdzenia poprawności konf	iguracii bazy	
			Nie dodawan nazwy (lomeny (Base DN) do nazwy użytko	wnika (ID)	
			Zezwalaj na zagnježo		(10)	
			Co zezmalaj na zaginezo	raine Brab		

Okno to pozwala między innymi na wskazanie dodatkowego, zapasowego kontrolera domeny czy też na określenie sposobu łączenia się z bazą Active Directory.





Zarządzanie użytkownikami

Zarządzanie kontami użytkowników odbywa się w sekcji **KONFIGURACJA > UŻYTKOWNICY > Użytkownicy i grupy**. Po przejściu do tego okna konfiguracyjnego możliwe jest tworzenie, modyfikowanie oraz usuwanie kont użytkowników i grup w domyślnej bazie LDAP. Należy pamiętać, że domyślnie lista użytkowników jest pusta. Aby wyświetlić użytkowników należy skorzystać z pola *Szukaj…* bądź też użyć filtr *Wszyscy(Brak)/Użytkownicy/Grupy*.

*-	«	💄 υŻΥΤΚΟΨΝΙCY / UŻΥΤΚ	OWNICY I GRUP	Y		
Szukai		Szukaj	🐣 Wszyscy 🔻	+ Nowy użytk	rtkownik 🕂 Nowa grupa 🗙 Usuń 👁 Sprawdź	
		Nazwa pospolita				
州 USTAWIENIA SYSTEMOWE	- 1	Lan Kowalski@stormshield.sto	rmshield.local	👗 kowalski (K	(Kowalski Jan)	
KONFIGURACJA SIECI	_	Adam Nowak@stormshield.sto	ormshield.local	конто	CERTYFIKAT CZŁONEK GRUPY	
S OBIEKTY	- 1	Ewa Mazur@stormshield.storm	nshield.local	P Lietaw lub	uh zmień bach Ukrawni	ienia
	- 1	Anna Dudek@stormshield.stor	mshield.local	, caturitab		icinu
	_	Administratorzy@stormshield.	stormshield.local	Login:	kowalski	
Użytkownicy i grupy				Nazwisko:	Kowalski	
Konta tymczasowe	_			lmię:	Jan	
Polityki dostępu	_			Adres e-mail:	il: jk@stormshield.pl	
Portal uwierzytelniania	_			Telefon:		
Żądania użytkowników	- 1			Opis:		

Konto użytkownika pozwala na skonfigurowanie następujących parametrów:

- Login nazwa używana podczas logowania.
- Nazwisko i Imię nazwisko i imię użytkownika.
- Adres e-mail adres e-mail użytkownika. Zawartość tego pola powinna być unikatowa, ponieważ na jego podstawie generowany jest certyfikat użytkownika, ponadto może ono służyć jako identyfikator użytkownika w procesie tworzenia tuneli IPsec VPN.
- Telefon numer telefonu użytkownika.
- Opis opis ułatwiający identyfikację użytkownika w systemie.
- **Certyfikat** certyfikat użytkownika
- Członek grupy określa przynależność użytkownika do określonych grup bazy LDAP.

Konto grupy pozwala na zdefiniowanie następujących parametrów:

- Nazwa grupy nazwa grupy.
- **Opis** opis ułatwiający identyfikację grupy.
- Członkowie grupy pole zawierające listę wszystkich członków danej grupy.

*	- « MODUŁY –	L UŻYTKOWNICY / UŻYTKOWNICY I GRUP	ΥY		
Sz	ukai 🦼 🎜	Szukaj 😫 Wszyscy 🔻	+ Nowy użytk	wnik 🕂 Nowa grupa 🗙 Usuń 👁 Sprawdź	
		Nazwa pospolita			
÷ţļ	USTAWIENIA SYSTEMOWE	Lan Kowalski@stormshield.stormshield.local	📽 Grupa Adm	histratorzy	
di.	KONFIGURACJA SIECI	Adam Nowak@stormshield.stormshield.local	Nazwa grupy:	Administratorzy	
	OBIEKTY	Ewa Mazur@stormshield.stormshield.local	Opis:	Opis grupy	
	UŻYTKOWNICY	Anna Dudek@stormshield.stormshield.local	Szukaj	🕂 Dodaj 🗙 Usuń	Uprawnienia
	Utility and a second	Administratorzy@stormshield.stormshield.local	Nazwa pospoli	3	
	Uzytkownicy i grupy		Ewa Mazur	Retormshield stormshield local	
	Konta tymczasowe		Lan Kewali		
	Polityki dostanu		- Jan Kowais	agistormsniela.stormsniela.tocai	





Należy zwrócić uwagę na to, że zarządzanie użytkownikami z poziomu STORMSHIELD UTM jest możliwe dla wewnętrznej bazy LDAP. Zarządzenie użytkownikami baz zewnętrznych wykonuje się bezpośrednio w tych bazach.

Portal uwierzytelniania (Captive portal)

Portal uwierzytelniania (Portal autoryzacji) jest specjalną stroną udostępnianą pod adresem https://IP_STORMSHIELD/auth/ i wykorzystywaną w celu autoryzacji użytkowników.

👹 UWIERZYTELNIANIE	× +				- 🗆 ×
← → ♂ ☆	🔽 🔒 https://10.11.11.	/auth/	⊠ ☆ >	K 🖪 🌢 🗡 🌣	<u>↓</u> III\ 🗊 🛛 ≡
Netwo	rk Security				PL.
ZALOGUJ / WYLO	GUJ NOWY UŻYTKOW	lik			
Uż	zytkownik Username				
Czas trwa	ania sesji 4 godzin		~		
	Wyloguj	Zaloguj			
	Jeśli jesteś już czas wybierają	uwierzytelniony, rozszerz : opcję zaloguj.	zysz okres uwierzytelnier	nia o wybrany	

Mechanizm Portalu uwierzytelniania wykorzystywany jest zarówno do autoryzacji użytkowników LAN (np. polityki filtrowania ruchu na podstawie nazwy użytkownika lub grupy) jak i WAN (np. SSL VPN). Konfiguracja Portalu uwierzytelniania odbywa się w sekcji **KONFIGURACJA > UŻYTKOWNICY > Portal uwierzytelniania**.

Konfiguracja portalu podzielona jest na dwa etapy:

- **Portal uwierzytelniania** ogólna konfiguracja portalu wraz z profilami przypisanymi do poszczególnych interfejsów urządzenia.
- Profil portalu autoryzacji szczegółowa konfiguracja poszczególnych profili portalu.

69

NEXT GENERATION FIREWALL

PODRĘCZNIK UŻYTKOWNIKA





Poniższe okno zawiera ogólną konfigurację portalu i obejmuje następujące funkcje:

ONDEXY	*	• «		PORTAL UWIERZYTEI NIANI	A	
Excliqi DOSTEPNE METODY METODA UWIERZYTELNIANIA PORTALU AUTORYZACJI # USTAWENIA SYSTEMOWE Portal uwierzyteiniania Portal uwierzyteiniania © ORIFICITY UZYTKOWNICY Interingi Porfil Domysłna metoda kb baza LDAP W Uzytkownicy i grupy Konta tymczasow Porfil Domysłna metoda kb baza LDAP Interingi Portal uwierzyteiniania Zagdania użytkowników Konta tymczasow Resetuj wzystwied kotopa Interingi Portal uwierzyteiniania Zagdania użytkowników Konta tymczasow Internal LDAP (normahield atomahield local) V Kontraut APLIKACJI Server SSL Vistor Vistor Vistor © Polz ADJANINSTRACJA Warzystania z dostępu do Internetu Wczyłaj treść warunków korzystania z dostępu do Internetu Internetu (tmt): Internetu (tmt): W Kontali APLIKACJI Wizyłaj treść warunków korzystania z dostępu do Internetu Internetu (tmt): Internetu (tmt): Internetu (tmt): Wizyłaj treść warunków korzystania z dostępu do Internetu (tmt): Internetu (tmt): Internetu Wizyłaj treść warunków korzystania z dostępu do Internetu (tmt): Internetu (trup): Internetu (trup): Internetu (trup): W	٥	MODUŁY –				
H USTANIENIA SYSTEMOWE IM KONFIGURACJA SECI OBEKTY PROFIL UWERZYTELNIANIA ORAZ INTERFEJS UZYTKOVNICY UJytkownicy i grupy Kota tymczasowe Profil Poltył dostępu Serwer SSL Ządania uzytkowników Kota tymczasowe Kontiguracja bazy LDAP Klucz prywatny lub Wzytkowników Klucz prywatny lub Wiczytali teść warunków korzystania z dostępu do Internetu Wczytaj treść warunków korzystania z dostępu do Internetu Portal uwierzytelniania Portal uwierzytelniania Portal uwierzytelniania Portal uwierzytelniania Portal uwierzytelniania Portal uwierzytelniania Wybierz logo dita portalu internetowego:	Szu	ukaj 🗶 🦉	DOSTEPNE METODY	METODA UWIERZYTELNIAN	A PORTAL UWIERZYTELNIANIA	PROFIL PORTALU AUTORYZACJI
KONFIGURACJA SECI GOBEKTY LIZYTKOWNICY Uzytkownicy i grupy Konta tymczasowe Polityki dostępu Portal uwiezytelniania Ządania użytkowników Konfguracja bazy LDAP Portal uwiezytelniania Ządania użytkowników Konfguracja bazy LDAP Portal uwiezytelniania Ządania użytkowników Konfguracja bazy LDAP Warunki kozystania z dostępu do Internetu Warunki kozystania z dostępu do Internetu Warunki dostępu do Internetu Wczytaj treść warunków kozystania z dostępu do Internetu Wczytaj treść warunków kozystania z dostępu do Internetu Wczytaj treść warunków kozystania z dostępu do Internetu Wczytaj treść warunków kozystania z dostępu do Internetu Wczytaj treść warunki dostępu do Internetu Portal uwiezystelniania Portal uwiezystelniania Portal uwiezystelniania Portal uwiezystelniania Portal uwiezystelniania Portal uwiezystelniania Portal uwiezystelniania Portal uwiezystelniania Portal uwiezystelniania Portal uwiezystelniania Portal uwiezystelniania Portal uwiezystelniania Portal uwiezystelniania Portal uwiezystelniania Portal uwiezystelniania Portal uwiezystelniania Portal uwiezystelniania	訲	USTAWIENIA SYSTEMOWE	— Portal uwierzytelniania			
S OBJEKTY LUZYTKOWNICY LUZYTKOWNICY LUZYtKOWNICY Uzytkownicy i grupy Konta tymczasowe Polityki dostępu Połtał uwiezytelniania Zadania uzytkowników Konta tymczasowe Polityki dostępu Serwer SSL Zadania uzytkowników Kontra ULAAP (stormahield stormahield		KONFIGURACJA SIECI	PROFIL UWIERZYTELN	IANIA ORAZ INTERFEJS		
LUZYTKOWNICY UZYTKOWNICY UZYtKOWNICY UZYtKOWNICY UZYtKOWNICY UZYtKOWNICY Konta tymczasowe Połtyki dostępu Portal uwierzytelniania Ządania uzytkowników Konfguracja bazy LDAP Serwer SSL Ządania uzytkowników Kontguracja bazy LDAP VortroLA APUKACJI Vorunki korzystania z dostępu do Internetu Wczytaj treść warunków korzystania z dostępu do Internetu (LMTI): Wczytaj treść warunków korzystania z dostępu do Internetu (LMTI): Wczytaj treść warunków korzystania z dostępu do Internetu (LMTI): Wzytaj treść warunków korzystania z dostępu do Internetu (LMTI): Wzytaj treść warunków korzystania z dostępu do Internetu (LOT): Zawansowane Zawansowane Portal uwierzytelniania Port portalu uniternetvowego: Inttps ▼ 5, Ukryj górny baner portalu (logo) Wybierz logo dia portalu autoryzacji (Captive Portal): Wybierz logo dia portalu autoryzacji (Captive Portal): W		OBIEKTY	🕂 Dodaj 🗙 Usuń			
Użytkownicy i grupy in insenal LDAP (atomathield atomathield.local) Portal uwierzytelniania Server SSL Żądania użytkowników Kłuż prywatny lub Vybierz KONTROLA APUIKACJI Warunki korzystania z dostępu do Internetu • × PoLityvi dochrony Warunki korzystania z dostępu do Internetu • • • • • • • • • • • • • • • • • • •	•	UŻYTKOWNICY	Interfejs	Profil	Domyślna metoda lub baza LDAP	
Konta tymczasowe Polityki dostępu Pottal uwierzytelniania Żądania użytkowników Kontguracja bazy LDAP POLTYKI OCHRONY KONTROLA APLIKACJI POLĄCZENIA VPN ADMINISTRACJA Waunki korzystania z dostępu do Internetu Wczytaj treść warunków korzystania z dostępu do Wczytaj treść warunków korzystania z dostępu do Wczytaj treść warunków korzystania z dostępu do Wczytaj treść warunków korzystania z dostępu do Wczytaj treść warunków korzystania z dostępu do Wczytaj treść warunków korzystania z dostępu do Wczytaj treść warunków korzystania z dostępu do Wczytaj treść warunków korzystania z dostępu do Wczytaj treść warunków korzystania z dostępu do Wczytaj treść warunków korzystania z dostępu do Portyntiau winki dostępu do Internetu Port portal uwierzytelniania Port portal uwierzytelniania Port portalu internetowego: https Ukyty jórny baner portalu (logo) Wybierz logo dla portalu autoryzacji (Captive Portal):		Użytkownicy i grupy	👦 in	Internal	LDAP (stormshield.stormshield.local)	
Polityki dostępu Potłal uwierzytelniania Żądania użytkowników Konfugracja bazy LDAP POLTYKI OCHRONY KONTROLA APLIKACJI POLĄCZENIA VPN ADMINISTRACJA Wczytaj treść warunków korzystania z dostępu do Internetu Wczytaj treść warunków korzystania z dostępu do Internetu Wczytaj treść warunków korzystania z dostępu do Internetu Wczytaj treść warunków korzystania z dostępu do Internetu Wczytaj treść warunków korzystania z dostępu do Internetu Wczytaj treść warunków korzystania z dostępu do Internetu Wczytaj treść warunków korzystania z dostępu do Internetu Wczytaj treść warunków korzystania z dostępu do Internetu Wczytaj treść warunków korzystania z dostępu do Internetu Wczytaj treść warunków korzystania z dostępu do Internetu Potłaj uwierzytelniania Portal uwierzytelniania Port portalu uwierzytelniania Port portalu internetowego: Interneto (Intri) Wybierz loopo dia portalu autoryzacji (Captive Portal);		Konta tymczasowe				
Portal uwierzytelniania Żądania użytkowników Konfiguracja bazy LDAP POLITYKI OCHRONY KONTROLA APLIKACJI POLĄCZENIA VPN ADMINISTRACJA Wczytaj treść warunków korzystania z dostępu do Internetu Wczytaj treść warunków korzystania z dostępu do Internetu Wczytaj treść warunków korzystania z dostępu do Internetu Wczytaj treść warunków korzystania z dostępu do Internetu Wczytaj treść warunków korzystania z dostępu do Internetu Wczytaj treść warunków korzystania z dostępu do Internetu Wczytaj treść warunków korzystania z dostępu do Internetu Wczytaj treść warunków korzystania z dostępu do Internetu Wczytaj treść warunków korzystania z dostępu do Internetu Wczytaj treść warunków korzystania z dostępu do Internetu Wczytaj treść warunków korzystania z dostępu do Internetu Potral uwierzytelniania Portal uwierzytelniania Port portalu uwierzytelniania Port portalu internetowego: https://wity.jomy baner portalu (togo) Wybierz togo dia portalu autoryzacji (Captive Portal):		Polityki dostępu				
Żądania użytkowników Konfiguracja bazy LDAP POLITYKI OCHRONY KONTROLA APLIKACJI POLĄCZENIA VPN ADMINISTRACJA Wczytaj treść warunków korzystania z dostępu do Internetu Wczytaj treść warunków korzystania z dostępu do Internetu Wczytaj treść warunków korzystania z dostępu do Internetu Wczytaj treść warunków korzystania z dostępu do Internetu Wczytaj treść warunków korzystania z dostępu do Internetu Wczytaj treść warunków korzystania z dostępu do Internetu Wczytaj treść warunków korzystania z dostępu do Internetu Wczytaj treść warunków korzystania z dostępu do Internetu Wczytaj treść warunków korzystania z dostępu do Internetu Wczytaj treść warunków korzystania z dostępu do Internetu Portz ordiwież warunki dostępu do Internetu Port portalu uniternetu (pd): Port portalu internetowego: Port portalu uniternetowego: Port portalu uniternetowego: Port portalu uniternetowego: Wybierz logo dla portalu autoryzacji (Captive Portaj):		Portal uwierzytelniania	Serwer SSL			
Konfiguracja bazy LDAP Vectrytik ochrony KontrolA APLIKACJI POLACZENIA VPN POLACZENIA VPN ADMINISTRACJA Warunki korzystania z dostępu do Internetu Wczytaj treść warunków korzystania z dostępu do Wczytaj treść warunków korzystania z dostępu do Internetu (html): Odśwież warunków korzystania z dostępu do Internetu (html): Potaśwież warunków korzystania z dostępu do Internetu (html): Potaśwież warunków korzystania z dostępu do Internetu (html): Potaśwież warunki dostępu do Internetu Pottal uwierzytelniania Portal uwierzytelniania Portalu internetowego: https://protalu (logo) Wybierz logo dla portalu autoryzacji (Captive Portal):		Żądania użytkowników				
 POLITYKI OCHRONY KONTROLA APLIKACJI Warunki korzystania z dostępu do Internetu POŁĄCZENIA VPN ADMINISTRACJA Wczytaj treść warunków korzystania z dostępu do Internetu (.htm): Wczytaj treść warunków korzystania z dostępu do Internetu (.pdf): Zaawansowane Zaawansowane Portalu wierzytelniania Portalu wierzytelniania Port portalu internetowego: https:::::::::::::::::::::::::::::::::::		Konfiguracja bazy LDAP	Klucz prywatny lub certyfikat:	Wybierz		▼ X
 KONTROLA APLIKACJI POŁĄCZENIA VPN ADMINISTRACJA Wczytaj treść warunków korzystania z dostępu do Internetu (1htmi): Wczytaj treść warunków kor	৵	POLITYKI OCHRONY				
POŁĄCZENIA VPN Wczytaj trść warunków korzystania z dostępu do internetu (.html): Wczytaj trść warunków korzystania z dostępu do internetu (.html): Wczytaj trść warunków korzystania z dostępu do internetu Mczytaj trść warunków korzystania z dostępu do internetu Wczytaj trść warunków korzystania z dostępu do internetu Mczytaj trść warunków korzystania z dostępu do internetu Wczytaj trść warunków korzystania z dostępu do internetu Mczytaj trść warunków korzystania z dostępu do internetu Mczytaj trść warunki dostępu do internetu Mczytaj trść warunki dostępu do internetu Mczytaj trść warunki dostępu do internetu Potśwież warunki dostępu do internetu Potłał uwierzyteiniania Portal uwierzyteiniania Port portalu internetowego: https://www.ika.przy.jego usuwaniu (TCP/UDP) Wybierz logo dla portalu autoryzacji (Captive Portal):	Ø	KONTROLA APLIKACJI	— Warunki korzystania z d	lostepu do Internetu		
ADMINISTRACJA Wczytaj treść warunków korzystania z dostępu do Internetu (.ntm): Wczytaj treść warunków korzystania z dostępu do Internetu (.ntm): Wczytaj treść warunków korzystania z dostępu do Internetu (.ntm): Zaawansowane Zaawansowane Plik automatycznej konfiguracji Proxy (.pac): Portal uwierzytelniania Port portalu internetowego: Inttps Internetu (.ntm): Ukryj górny baner portalu (logo)	•	POŁĄCZENIA VPN				
Wczytaj treść warunków korzystania z dostępu do Internetu Image: Construction of the second secon		ADMINISTRACJA	Internetu (.html):	korzystania z dostępu do		🖲
• Zaawansowane • Zaawansowane • Dik automatycznej konfiguracji Proxy (.pac): • Portal uwierzytelniania • Portal u internetowego: • https • • • • • • • • • • • • • • • • • • •			Wczytaj treść warunków Internetu (.pdf):	korzystania z dostępu do		
 ▲ Zaawansowane ☐ Resetuj wszystkie połączenia dla użytkownika przy jego usuwaniu (TCP/UDP) Plik automatycznej konfiguracji Proxy (.pac): ☐ Portal uwierzytelniania Port portalu internetowego: https ■ ■ ☐ Ukryj górny baner portalu (logo) Wybierz logo dla portalu autoryzacji (Captive Portal): 			🕤 Odśwież warunki dos	stępu do Internetu		
Zaawansowane Resetuj wszystkie połączenia dla użytkownika przy jego usuwaniu (TCP/UDP) Plik automatycznej konfiguracji Proxy (.pac): Portal uwierzytelniania Port portalu internetowego: https Ukryj górny baner portalu (logo) Wybierz logo dla portalu autoryzacji (Captive Portal):						
Resetuj wszystkie połączenia dla użytkownika przy jego usuwaniu (TCP/UDP) Plik automatycznej konfiguracji Proxy (.pac): Portal uwierzytelniania Port portalu internetowego: https D Ukryj górny baner portalu (logo) Wybierz logo dla portalu autoryzacji (Captive Portal):			 Zaawansowane 			
Plik automatycznej konfiguracji Proxy (.pac): Portal uwierzytelniania Port portalu internetowego: https Ukryj górny baner portalu (logo) Wybierz logo dla portalu autoryzacji (Captive Portal):					🗆 Posotuj wszystkie połaczonia dla	użytkownika przy jego usuwaniu
Plik automatycznej konfiguracji Proxy (.pac):					(TCP/UDP)	uzytkownika przy jego usuwaniu
Portal uwierzytelniania Port portalu internetowego: https • • • • • • • • • • • • • • • • • • •			Plik automatycznej kont	figuracji Proxy (.pac):		👁
Port portalu internetowego: https Ukryj górny baner portalu (logo) Wybierz logo dla portalu autoryzacji (Captive Portal):			Portal uwierzytelnian	nia		
Port portalu internetowego: https 💌 🛼						
Ukryj górny baner portalu (logo) Wybierz logo dla portalu autoryzacji (Captive Portal):			Port portalu interne	etowego:	https 💌 🕏	
Wybierz logo dla portalu autoryzacji (Captive Portal):					🗌 Ukryj górny baner portalu (log	10)
			Wybierz logo dla po	ortalu autoryzacji (Captive Portal)	:	
Wybierz szablon css dla portalu autoryzacji (Captive			Wybierz szablon cs:	s dla portalu autoryzacji (Captive	•	
Reset			Res	et		

- **Profil uwierzytelniania oraz interfejs** tabela zawierająca powiązania profili Portalu uwierzytelniania z interfejsami urządzenia, znajdują się tu trzy kolumny:
 - o Interfejs interfejs urządzenia, do którego ma być przypisany profil,
 - **Profil** profil portalu uwierzytelniania. Konfiguracja profili znajduje się z zakładce *Profil portalu autoryzacji,*
 - **Domyślna metoda lub baza LDAP** domyślna metoda lub baza LDAP wskazana w wybranym profilu uwierzytelniania (tylko podgląd);



- Klucz prywatny lub certyfikat pozwala na wybór certyfikatu jaki będzie użyty do podpisania portalu autoryzacji. Certyfikat musi być wcześniej utworzony lub zaimportowany na urządzenie poprzez sekcję KONFIGURACJA > OBIEKTY > Certyfikaty – PKI;
- Wczytaj treść warunków korzystania dostępu do Internetu (.html) / (.pdf) możliwość wprowadzenia regulaminu dostępu do Internetu, który będzie wyświetlony użytkownikom na Portalu uwierzytelniania. Użytkownik będzie musiał zatwierdzić regulamin zanim zostanie zautoryzowany;
- Resetuj wszystkie połączenia dla użytkownika przy jego usuwaniu (TCP/UDP) po zaznaczeniu tej opcji w momencie kiedy upłynie czas autentykacji użytkownika wszystkie jego połączenia zostaną przerwane;
- Plik automatycznej konfiguracji Proxy (.pac) pole umożliwia wczytanie pliku zawierającego automatyczną konfigurację proxy (Proxy Auto-Config);
- **Port portalu internetowego** nr portu na którym działa portal uwierzytelniania, domyślnie 443 (obiekt https);
- Ukryj górny baner portalu (logo) włączenie tej opcji ukrywa (ze względów bezpieczeństwa) logo "Stormshield Network Security" znajdujące się w górnym banerze portalu;
- Wybierz logo dla portalu autoryzacji możliwość personalizacji Portalu uwierzytelniania poprzez wczytanie nagłówka (logo) portalu, obrazek 800x50px;
- Wybierz szablon CSS dla portalu autoryzacji import własnego arkusza styli CSS, który zmodyfikuje oryginalny wygląd Portalu uwierzytelniania;
- Reset przywrócenie oryginalnego wyglądu Portalu uwierzytelniana (reset logo i styli CSS).

NEXT GENERATION FIREWALL

PODRĘCZNIK UŻYTKOWNIKA





Zakładka *PROFIL PORTALU AUTORYZACJI* umożliwia konfigurację poszczególnych profili Portalu uwierzytelniana. Dostępnych jest 10 profili w tym 5 wstępnie skonfigurowanych.

Image: Contract of the contract	IODOL I		
VSTEADOVE VSTEAD	j 🖌 🖉	DOSTEPNE METODY METODA	JWIERZYTELNIANIA PORTAL UWIERZYTELNIANIA PROFIL PORTALU AUTORYZACJI
A SECI A SECI A SECI Demyérina metoda lub LDAP: LDAP: (stormahied, stormahied, local) Puty rusy owe a a seriania Crestoffinedé vyj sintélania: Crestoffinedé vyj sintélania: Mainy CLAP Polin n: 3: Polin n: 3: Polin n: 3: Polin n: 3: Crestoffinedé vyj sintélania: Mainy CLAP Polin n: 3: Polin n: 3: Polin n: 4: Crestoffinedé vyj sintélania: Mainy CLAP Polin n: 4: Polin n: 4	STAWIENIA SYSTEMOWE	Internal	azwę 🛈
Configuracja obstugi zgdał nejestracji ucytkownika e wacystał zgdania docłania do bazy LDAP Konfiguracja obstugi zgdał nejestracji ucytkownika e może zmień katas Configuracja obstugi zgdał nejestracji ucytkownika e może zmień katas Konfiguracja obstugi zgdał nejestracji ucytkownika e może zmień katas Konfiguracja obstugi zgdał nejestracji ucytkownika e może zmień katas Konfiguracja obstugi zgdał nejestracji ucytkownika e może zmień katas Konfiguracja obstugi zgdał nejestracji ucytkownika e może zmień katas Konfiguracja obstugi zgdał nejestracji ucytkownika e może zmień katas Konfiguracja obstugi zgdał nejestracji ucytkownika e może zmień katas Konfiguracja obstugi zgdał nejestracji ucytkownika e może zmień katas Konfiguracja obstugi zgdał nejestracji ucytkownika e może zmień katas Konfiguracja obstugi zgdał nejestracji ucytkownika e może zmień katas Konfiguracja obstugi zgdał nejestracji ucytkownika e może zmień katas Konfiguracja obstugi zgdał nejestracji ucytkownika e może zmień katas Konfiguracja obstugi zgdał nejestracji ucytkownika e może zmień katas Konfiguracja obstugi zgdał nejestracji ucytkownika e może zmień katas Konfiguracja obstugi zgdał nejestracji ucytkownika e może zmień katas Konfiguracja obstugi zgdał nejestracji ucytkownika e może zmień katas Konfiguracja obstugi zgdał nejestracji ucytkownika e może zmień katas Konfiguracja obstugi zgdał nejestracji ucytkownika e może zmień katasi ob bazy LDAP Konfiguracja obstugi zgdał nejestracji ucytkownika e może zmień katasi ob bazy LDAP Konfiguracja obstugi zgdał nejestracji ucytkownika e może zmień katasi ob bazy LDAP Konfiguracja obstugi zgdał nejestracji ucytkownika e może zmień katasi ob bazy LDAP	ONFIGURACJA SIECI	Uwierzytelnianie	
Image: Control of the second of the secon	BIEKTY	Domyślna metoda lub LDAP:	LDAP (stormshield.local)
Juny ware ware Warenki korzystania z dostępu do internetu wareki warenia Wareki korzystania z dostępu do internetu Częstotliwość wyjiwietlanie Roty DNY UKACJI Personalizacja portalu autoryzacji (tyko dla trybu gościa) Pelene: 1: Pelene: 1: Pelene: 1: Pelene: 2: Pelene: 3: Pelene: 3: Pelene: 3: Pelene: 4: Czas trwania eseji uwierzytetniania Minut (makrymity czas (makrybi) Wierzytycznialu klienta * Zaawansowane * Zaawansowane * Zaawansowane * Włącz portal uwierzytelniania Wyłącz stone wyłogowania Besterowania ustawiski portalu autoryzacji (bywie klienty ustawie artesów IP jednocześnie Pottyka dotycząca COOKIES: Przechonywane przez okreściony czas Pottal uwierzytelniania Wyłącz społowania Wytórz speriodowana Wytórz speriodowana Wytórz speriodowana Wytórz speriodowana wytowani zazamie	ŻYTKOWNICY		Włącz polecanie
Warunki korzystania z dostępu do internetu w definina workdow workdow kary LDAP Personalizacja portalu autoryzacji (tytko dla trybu gościa) Pełden 1: Pełden 2: Putry Matsymaliy Czas Wijkicz strong wijcogowania Czas trvania seśli uwierzytelniania Wijkicz strong wijcogowania Czas dotogo cołości ji Wyłacz strong wijcogowania Czastrvania secji uwierzytelniania Wijkicz strong wijcogowania Czastrvanie strone i bosta ukterytelnian	żytkownicy i grupy		
u Witcz wytwictkiele warutków korzystala z dostipu do internetu winikow Częstotliwość wytwietkieli i i i u u u u u u u u u u u u u u u u	onta tymczasowe	Warunki korzystania z dostępu do Int	ernetu
Createdbined& wydwiddadia: 18 Personalizacja portalu autoryzacji (tytko dla trybu golda) Personalizacja portalu autoryzacji (tytko dla trybu golda) Potie nr. 1: Potie nr. 2: Putie nr. 3: Cras trwania segi uwierzytelniania Minimitry czas Uwierzytelniania klenta Umirzytelniania klenta Uwierzytelniania klenta Uwierzytelniania klenta Uwierzytelniania klenta Umirzytelniania Waterzytelniania Umirzytelniania Uwierzytelniania Umirzytelniania Uwierzytelniania Umirzytelniania Uwierzytelniania Uwierzytelniania Uwierzytelniania Umirzytelniania Uwierzytelniania Uprawnienia uzytkownik nie może zmienić hasia Uprawnienia uzytkownik nie może zmienić hasia Uzytkownik może zmienić hasia Uzytkownik może zmienić hasia Uzytkownik może zmienić hasia Uzytkownik może zmienić hasia Uzytkownik może zmienić hasia Uzytkownik może zmienić hasia Uzytkownik może zmienić hasia Uzytkownik może zmienić hasia Uzytkownik może zmienić hasia Uzytkownik może zmienić hasia Uzytko	ontol uwiorzytelpiopio		Włącz wyświetlanie warunków korzystania z dostępu do Internetu
Annume DOLY DOLY UKACJI PN JA Crass trwania sesji uvierzytelniania Minimainy crass UWERZYEINiania kienta UWERZYEINiania kienta UWERZYEINiania kienta UWERZYEINiania kienta UWERZYEINiania kienta UWERZYEINiania kienta UWERZYEINiania kienta UWERZYEINiania kienta UWERZYEINiania UWERZYEINI	lania użytkowników	Częstotliwość wyświetlania:	
NoW NoW URACJI VPN JA Cas twania sesji uwiezytetniania Minimality czas uwiezytetniania klienta Immunity Resonante Wiezytetniania klienta Immunity Resonante Immunity Pole nc. 3: Cas twania sesji uwiezytetniania Immunity Immunity Immunity Immunity Immunity Cas twania sesji uwiezytetniania Immunity	guracia bazy I DAP	Personalizacja portalu autoryzacji	(tylko dla trybu gościa)
LIKACJI PN JA Czas trwania seji uwierzytelniania Umerzytelniania kterita Umerzytelniania kterita Umerzytelniania kterita Umerzytelniania Czas trwania seji uwierzytelniania Umerzytelniania Czas trwania seji uwierzytelniania Umerzytelniania Czas trwania seji uwierzytelniania Umerzytelniania Czas trwania seji uwierzytelniania Umerzytelniania Czas transitiona Czas trwania seji uwierzytelniania Umerzytelniania Czas transitiona Czas transitiona	YKI OCHRONY	Pole nr. 1:	Pustv
Point: 3: Puty JA Cas trvania seiji uvierzyteiniania 	ROLA APLIKACJI	Pole nr. 2:	Pusty
JA Czas twania seşii uwierzytelniania Minimatiyo czas Wietzytelniania klienta (ministy): SSO (ministy): * Zaawansowane * Zaawansowane Biokuj uwiezytelniania Włącz stronę wyłogowania Czewół na dostęp óp piku. PAC dla tego profilu Biokuj uwiezytelniania Wybiez spersonaliżowana Wiedownik może zmienić hasta Wybiez zpersonaliżowana Wiedownik nie może zmienić hasta Użytkownik nie wytysinia żądania dotania do bazy LDAP Zzewół na wytysinia żądania dotania do bazy LDAP Zzewół na wytysinia żądania dotania do bazy LDAP Zzewół na wytysinia żądania dotania do bazy LDAP	JIA VPN	Pole nr. 3:	Pusty 👻
Czas trwania seji uwiezrytelniania Minimairy czas uwierzytelniania klienta Maksymairy czas uwierzytelniania klienta Maksymairy czas uwierzytelniania klienta Wierzytelniania klienta Wierzytelniania klienta Połężyncze logowanie SBO (minuty): * Zaawansowane Włącz stronę wyłogowania Zezwół na dostęp do pliku. JAC dla tego profilu Biokuj uwierzytelniania Wyłącz stronę wyłogowania Zezwół na dostęp do pliku. JAC dla tego profilu Biokuj uwierzytelniania Wybierz spersonaliżowana Wybierz spersonaliżowana W ułącz stronę wyłogowania Użytkownik nie może zmienić hasia Użytkownik ni wytywieżej dziad i dodania do bazy LDAP	FRACJA		
Czas trvania sesiji uvierzytelniania Winimalny czas uvierzytelniania klienta I diaksymalny czas uvierzytelniania klienta I diaksymalny czas uvierzytelniania klienta I diaksymalny czas I diaksymalny			
Minimalny czas wierzyteiniania klienta I Godzin 15 Minut Meksymalny czas wierzyteiniania klienta I Godzin 0 Minut Pojedyncze logowanie- SO (minuty): Zawansowane Viłącz portal uwierzyteiniania I Zetwół na dostąp do piłku JAC dla tego profilu Błokuj uwierzyteiniania Zetwół na dostąp do piłku JAC dla tego profilu Błokuj uwierzyteinianie jednego użytkownika z wielu dreśów IP jednocześnie Polityka dotycząca COOKIES: Przechowywane przez określony czas Potral uwierzyteiniania Wybierz spersonalizowaną wiadomość (piłk HTML): I Resetowanie uutawień portulu autentykacji Uprawnienia użytkownika Wybierz spersonalizowaną wiadomość (piłk HTML): Codmów użytkownikom wysyłania żądania do bazy LDAP O ddmów użytkownikom wysyłania żądania do bazy LDAP Zezwół na wysyłanie żądań dodania do bazy LDAP		— Czas trwania sesji uwierzytelniania —	
wwierzyteiniania klienta 0 Godzin 15 Minut (minuty): Maksymathy czas 4 Godzin 0 Minut Pojedyncze logowanie 4 Godzin 0 Minut * Zaawansowane * Godzin 0 Minut * Zaawansowane * Włącz stronę wyłogowania 2 Zezwól na dostęp do pliku. PAC dla tego profilu Biokuj uwierzytelnienie jednego użytkownika z wielu adresów IP jednocześnie Polityka dotycząca COOKIES: Przechowywane przez określony czas Pottal uwierzytelniania Wybierz spersonalizowaną • • Wybierz spersonalizowaną • Użytkownik nie może zmienić hasia Użytkownika Wybierz spersonalizowaną • Użytkownik nie może zmienić hasia • • Wybierz spersonalizowaną • • • • • Wybierz spersonalizowanie ustawień portalu autentykacji • • • • • Wybierz spersonalizowanie • Użytkownik nie może zmienić hasia • • • • • Wołodocić hasta (dni): • • • • •		Minimalny czas	
Weidernamicy Casas 4 Godzin Minut Pojedyncze logowanie - 500 (minuty): Minut SSO (minuty): 4 Godzin Minut * Zaawansowane Włącz portal uwierzytelniania Minut Włącz stronę wylogowania 2zzwół na dostęp do piłku. PAC dla tego profilu Blokuj uwierzytelnienie jednego użytkownika z wielu adresów IP jednocześnie Polityka dotycząca COOKIES: Przechowywane przez określony czas wielu adresów IP jednocześnie Potral uwierzytelniania wielu adresów IP jednocześnie wielu adresów IP jednocześnie Potral uwierzytelniania wielu adresów IP jednocześnie wielu adresów IP jednocześnie Potral uwierzytelniania wielu adresów IP jednocześnie wielu adresów IP jednocześnie Wybierz spersonalizowaną wiadomość f plik HTML); Im czesowaną wielu adresów IP jednocześnie Wybierz spersonalizowaną wielu adresów IP jednocześnie wielu adresów IP jednocześnie Wybierz spersonalizowaną wielu adresów IP jednocześnie wielu adresów IP jednocześnie Wybierz spersonalizowaną wielu adresów IP jednocześnie wielu adresów IP jednocześnie Wybierz spersonalizowaną wielu adresów IP jednocześnie wielu zytkownik może zmienić hasia W		uwierzytelniania klienta (minuty):	Godzin 15
Pojedyncze logowanie - 4		uwierzytelniania klienta 4 (minuty):	Godzin 0 C Minut
Zawansowane Zawansowane Wiącz portal uwierzytelniania Wiącz stronę wyłogowania Zezwól na dostęp do pliku. PAC dla tego profilu Biokuj uwierzytelnienie jednego użytkownika z wielu adresów IP jednocześnie Polityka dotycząca COOKIES: Przechowywane przez określony czas Portal uwierzytelniania Wybierz spersonalizowaną wiadomość (plik HTML): wiadomość (plik HTML): wiadomość (plik HTML): wiadomość (plik HTML): wiadomość (plik HTML): wiadomość (plik HTML): wiadomość (plik HTML): wiadomość (plik HTML): wiadomość (plik HTML): wiadomość (plik HTML): wiadomość (plik HTML): wiadomość (plik HTML): wiadomość (plik HTML): wiadomość (plik HTML): wiadomość (plik HTML): wiadomość (plik HTML): wiadomość (plik HTML): wiazowiek na wysłanie zadania do bazy LDAP @ Użytkownik mo wzytkownika wuszność hasta (dni):		Pojedyncze logowanie - 4 SSO (minuty):	Codzin 0 CMInut
Polityka dotycząca COOKIES: Przechowywane przez określony czas Portal uwierzytelniania Wybierz spersonalizowaną wiadomość (plik HTML): Resetowanie ustawień portalu autentykacji Uprawnienia użytkownika Uprawnienia użytkownika Uzytkownik nie może zmienić hasła Użytkownik noże zmienić hasła Użytkownika ważność hasła (dni): Konfiguracja obsługi żądań rejestracji użytkowników Codmów użytkownikom wysyłania żądania do bazy LDAP Zezwół na wysyłanie żądań dodania do bazy LDAP			 Włącz portal uwierzytelniania Włącz stronę wylogowania Zezwól na dostęp do pliku .PAC dla tego profilu Blokuj uwierzytelnienie jednego użytkownika z wielu adresów IP jednocześnie
Portal uwierzytelniania Wybierz spersonalizowaną wiadomość (plik HTML): Image: Comparison of the set of the s		Polityka dotycząca COOKIES:	Przechowywane przez określony czas
Wybierz spersonalizowaną wiadomość (plik HTML): Image: Construction of the state of the st		Portal uwierzytelniania	
Resetowanie ustawień portalu autentykacji Uprawnienia użytkownika Użytkownik nie może zmienić hasła Użytkownik może zmienić hasła Użytkownik może zmienić hasła Użytkownika Wymuś zmianę hasła użytkownika Wymuś zmianę hasła użytkownika Konfiguracja obsługi żądań rejestracji użytkowników Konfiguracja obsługi żądań rejestracji użytkowników Odmów użytkownikom wysyłania żądania dodania do bazy LDAP Zezwól na wysyłanie żądań dodania do bazy LDAP Zezwól na wysyłanie żądań dodania do bazy LDAP Zezwól na wysyłanie żądań dodania do bazy LDAP Wyślij powiadomienie w przypadku Nie wysyłaj władomości		Wybierz spersonalizowaną wiadomość (plik HTML):	@
Uprawnienia użytkownika Image: Strategy of the state of the strategy of the s		Resetowanie ustawień portalu aut	tentykacji
 Użytkownik nie może zmienić hasła Użytkownik może zmienić hasła Użytkownik może zmienić hasła Wymuś zmianę hasła użytkownika Wymuś zmianę hasła użytkownika O Konfiguracja obsługi żądań rejestracji użytkowników Codmów użytkownikom wysyłania żądania dodania do bazy LDAP Zezwół na wysyłanie żądań dodania do bazy LDAP Zezwół na wysyłanie żądań dodania do bazy LDAP Zezwół na wysyłanie żądań dodania do bazy LDAP Zezwół na wysyłanie żądań dodania do bazy LDAP Zezwół na wysyłanie żądań dodania do bazy LDAP 		Uprawnienia użytkownika	
ważność hasła (dni): 0 Konfiguracja obsługi żądań rejestracji użytkowników Odmów użytkownikóm wysyłania żądania dodania do bazy LDAP © 2czwól na wysyłanie żądań dodania do bazy LDAP O Zezwól na wysyłanie żądań dodania do bazy LDAP Vyślij powiadomienie w przypadku Nie wysyłaj wiadomości			 Użytkownik nie może zmienić hasła Użytkownik może zmienić hasło Wymuś zmianę hasła użytkownika
Konfiguracja obsługi żądań rejestracji użytkowników Odmów użytkownikom wysyłania żądania do bazy LDAP Image: Start St		ważność hasła (dni):	0
 Odmów użytkownikom wysyłania żądania dobazy LDAP Zezwól na wysyłanie żądań dodania do bazy LDAP Zezwól na wysyłanie żądań dodania do bazy LDAP oraz żądania certyfikatów PKI Wyślij powiadomienie w przypadku Nie wysyłaj wiadomości 		Konfiguracja obsługi żądań rejestra	icji użytkowników
Wyślij powiadomienie w przypadku wysłania żądania:			Odmów użytkownikom wysyłania żądania dodania do bazy LDAP Zezwól na wysyłanie żądań dodania do bazy LDAP Zezwól na wysyłanie żądań dodania do bazy LDAP Zezwól na wysyłanie żądań dodania do bazy LDAP
		Wyślij powiadomienie w przypadku	

NEXT GENERATION FIREWALL PODRĘCZNIK UŻYTKOWNIKA




- Zmień nazwę możliwość zmiany nazwy wybranego profilu;
- **Domyślna metoda lub LDAP** wskazanie domyślnej metody autoryzacji lub bazy LDAP (w przypadku jeśli na urządzeniu jest skonfigurowanych kilka baz LDAP);
- Włącz polecanie możliwość włączenia metody Uwierzytelnianie przez polecającego (Sponsor). Ta opcja jest domyślnie włączona jeśli jako domyślna metoda wskazana jest metoda Sponsor.
- Włącz wyświetlanie warunków korzystania z dostępu do Internetu włączenie wyświetlania regulaminu dostępu do Internetu. Regulamin ten będzie wyświetlony użytkownikowi na Portalu uwierzytelniania podczas autentykacji i będzie musiał zostać zatwierdzony zanim użytkownik zostanie zautoryzowany. Treść regulaminu można wczytać w ogólnej konfiguracji Portalu uwierzytelniania.
- **Częstotliwość wyświetlania** jak często zautoryzowanym użytkownikom będzie wyświetlany regulamin dostępu do Internetu;
- Personalizacja portalu autoryzacji opcja dotyczy jedynie metody dostępu typu Gość i umożliwia dodanie do trzech pól formularza do strony portalu uwierzytelniania wyświetlającej regulamin dostępu do Internetu. Dostępne typy pól to: Pusty (pole nie będzie wyświetlane), Imię, Nazwisko, Telefon, E-Mail, Informacja, Firma;
- Czas trwania sesji uwierzytelniania maksymalny czas trwania pojedynczej sesji logowania. Na czas trwania sesji konto użytkownika jest "wiązane" z adresem IP, z którego użytkownik się zalogował. Określenie czasu minimalnego i maksymalnego sesji spowoduje, że użytkownik będzie mógł sam wybrać czas trwania sesji;
- Włącz portal uwierzytelniania włącza autentykację z wykorzystaniem danego profilu autoryzacji;
- Włącz stronę wylogowania włączenie tej opcji spowoduje pojawienie się odrębnej strony umożliwiającej zautoryzowanemu użytkownikowi wylogowanie się z portalu;
- Zezwól na dostęp do pliku .PAC dla tego profilu zezwala na dostęp do pliku .pac (Proxy Auto-Config) użytkownikom logującym się na podstawie danego profilu autoryzacji;
- Blokuj uwierzytelnienie jednego użytkownika z wielu adresów IP jednocześnie funkcja uniemożliwia zalogowanie jednego użytkownika na wielu komputerach, użycie tej opcji eliminuje "pożyczanie kont" pomiędzy użytkownikami;
- Polityka dotycząca COOKIES wykorzystanie mechanizmu cookies w procesie uwierzytelniania użytkownika pozwala na wprowadzenie dodatkowego poziomu zabezpieczeń. Po pomyślnym zautoryzowaniu użytkownika Portal uwierzytelniania tworzy w przeglądarce specjalny określony odpowiednim czasem życia plik *connection cookie*. Usunięcie tego pliku bądź jego wygaśnięcie spowoduje unieważnienie autoryzacji użytkownika. Mechanizm ten można jednak wyłączyć;
- Wybierz spersonalizowaną wiadomość (plik HTML) umożliwia dodanie wiadomości zawierającej tekst i obrazy umieszczonej pod tytułem portalu uwierzytelniania. Wiadomość musi być w formacie HTML;
- Resetowanie ustawień portalu autentykacji ... usunięcie wiadomości spersonalizowanej;
- Uprawnienia użytkownika uprawnienia użytkownika do zarządzania własnym hasłem;
- Konfiguracja obsługi żądań rejestracji użytkowników konfiguracja funkcji, która umożliwia użytkownikom wysyłanie żądań założenia konta oraz utworzenia/pobrania certyfikatów. Użytkownik

NEXT GENERATION FIREWALL PODRĘCZNIK UŻYTKOWNIKA





wypełnia pola właściwości konta swoimi danymi, a rola administratora ogranicza się do weryfikacji tych danych i ewentualnej akceptacji utworzenia konta.

Powyższa metoda autoryzacji wymaga aby użytkownik wszedł na stronę portalu i podał swój login oraz hasło. Istnieje jednak metoda wymuszania na przeglądarce otwarcia strony autoryzacji podczas próby wejścia na strony WWW przez niezautoryzowanego użytkownika.

Należy w tym celu uruchomić **Kreator reguły uwierzytelniania** z menu **KONFIGURACJA > POLITYKI OCHRONY > Firewall i NAT > Dodaj,** następnie wypełniamy kreator.

KREATOR UWIERZY				3	
Cel: Uruchomić przek Kto: Obiekt źródłowy:	ierowanie ruchu HTTP do specjalne ADRES ŹRÓDŁOWY Nieuwierzytelniony użytkownik Network_internals	e portalu w celu wy	muszenia autoryzacji użytk Obiekt docelowy: Oprócz adresów:	ADRES DOCELOWY Internet + Dodaj ×	v ≡ Usuń
		× ANULUJ	✓ ΖΑΚΟŃCZ		

Do zdefiniowania mamy:

- Obiekt źródłowy adres hosta, zakres hostów, całe podsieci, które mają być uwzględniane w trakcie autoryzacji;
- **Obiekt docelowy** przeznaczenie ruchu sieciowego pochodzącego z obiektu źródłowego (najczęściej Internet);
- **Oprócz adresów** grupy URL stron, które będą dostępne bez konieczności autoryzacji (np. serwery aktualizacyjne systemów operacyjnych, antywirusowych itp.).

Po zakończeniu kreatora otrzymujemy regułę:

NEXT GENERATION FIREWALL

PODRĘCZNIK UŻYTKOWNIKA





	POLITYKI OCHRONY / FIREWALL I NAT											
(5) Filter 05	(5) Filter 05 🔹 ksportuj V 🗓 Eksportuj 🕴											
FIREWALL	FIREWALL NAT											
Szukaj			🕇 🕇 Dodaj 🝷	🗙 Usuń 🕇	4 x ^e	a 🔄 Wytnij 🛛 🖸	🕈 Kopiuj 🛛 🕙 Wklej	🖳 🖳 Wyszukaj w I	logach 🛛 🖓 Wyszuk	aj w monitoringu		
	Stan	E.	Akcja	≞	Adres źródłow	vy	Adres docelowy	Port docelowy	Analiza protokołów	Polityki filtrowania 🖃	Komentarz	
1 💽 włączon		ączona	➡ Portal uwie Z wyjątkien	rzytelniania n:	2º unknown	@ 🕮 Network_intern	als 🕀 Internet	₿ http		IPS		

Jak powyżej widać każde połączenie zainicjowane przez nieznanego użytkownika z sieci chronionej, do sieci Internet, które zostanie nawiązane na porcie http STORMSHIELD UTM przekaże do Portalu uwierzytelniania. W przypadku chęci przekierowania ruchu **https** na Portal uwierzytelniania należy odpowiednio zmodyfikować powyższą regułę dodając w porcie docelowym również port https.

Jednak, aby takie przekierowanie działało należy wcześniej zdeszyfrować ruch https, czyli uruchomić moduł SSL Proxy.

Transparentne uwierzytelnianie SSO

W przypadku korzystania z usługi katalogowej Active Directory istnieje możliwość pominięcia autoryzacji z użyciem Portalu uwierzytelniania na rzecz transparentnego uwierzytelniania SSO (Single Sign-On).

W tym celu należy zainstalować oprogramowanie **Stormshield SSO Agent** na kontrolerze domeny (bądź innym, stale uruchomionym hoście znajdującym się w tej domenie) oraz skonfigurować odpowiednią metodę autoryzacji na urządzeniu STORMSHIELD UTM.

Najnowszą dostępną wersję Agenta SSO można pobrać ze strefy klienta (https://mystormshield.eu) w sekcji Download:

🧠 STORMSHI	ELD	Legal terms	Terms of Use and Services -	My profile	Log out	CONTACT & ASSISTANCE
ORDER -	DASHBOARD DOWNLOADS ®					
Create a new order List of drafts Orders in progress Realized orders list Serial number database DEAL RECISTRATION	Io view your download, click on a category below : STORMSHIELD NETWORK S CEURITY STORMSHIELD DATA SECURITY STORMSHIELD DENDPOINT SECURITY STORMSHIELD VISIBILITY CENTER NETASQ	ADMINISTRA CENTRALIZE EVENT ANAL FIRMWARE MANAGEMEN SOO AGENT TOOLS	TION SUITE D MANAGER YZER IT CENTER - SMC			
Register a new Deal Deal List User Guide RMA Details	STORMSHIELD NETWORK SECURITY - SSO A	VPN CLIENT VPN SSL GENT - V 1.9.0		×		Published the 2018-06-05
Product Details PRODUCT	Release Note : EN / FR NAME SSO agent version 1.9.0		TYPE SSO Agent ex	FORMAT	L	ANGUAGE SIZE SHA256 fr. en 17M Display
Product management Register a product		GENT - V 1.8.0				Published the 2018-04-25
DOWNLOADS	STORMSHIELD NETWORK SECURITY - SSO A STORMSHIELD NETWORK SECURITY - SSO A	GENT - V 1.6.0				Published the 2017-07-04
Downloads Help for migration to V9	STORMSHIELD NETWORK SECURITY - SSO A STORMSHIELD NETWORK SECURITY - SSO A	GENT - V 1.5.0 GENT - V 1.4.0				Published the 2017-06-01 Published the 2016-11-15
TECHNICAL SUPPORT Manage cases Olicid Packers	STORMSHIELD NETWORK SECURITY - SSO A	GENT - V 1.3.0				Published the 2015-04-10
Self-Test USB Recovery	STORMSHIELD NETWORK SECURITY - SSO A STORMSHIELD NETWORK SECURITY - SSO A	GENT - V 1.2.0 GENT - V 1.1.0				Published the 2014-07-02

NEXT GENERATION FIREWALL PODRĘCZNIK UŻYTKOWNIKA





Podczas instalacji oprogramowania należy wybrać odpowiednią opcję w zależności od tego gdzie je instalujemy. Jeżeli instalacja odbywa się bezpośrednio na kontrolerze domeny to należy wybrać pierwszą opcję:

n Stormshield SSO Agent Setup	\times
Installation Select an option and click Next to continue.	STORMSHIELD
Please define the host on which you are installing Stormshield Agent SSO and th this service:	ne account used for
 You are on the domain controller and wish to use the local system account You wish to enter an account dedicated to the service 	
< <u>B</u> ack <u>N</u> ext >	<u>C</u> ancel

Następnie należy podać hasło współdzielone, które później trzeba będzie podać także po stronie konfiguracji urządzenia STORMSHIELD UTM:





n Stormshield SSO Agent Setup	×
Entering the SSL encryption key Fill in the items below and click Next to continue.	
Please define the pre-shared key that would allow securing communication betw Stomshield SSO Agent and a Stomshield firewall. This key has to be the same as the one configured on the Stomshield firewall. Enter the pre-shared key:	ween the
Confirm the key:	
•••••	
< <u>B</u> ack <u>N</u> ext >	<u>C</u> ancel

W ostatnim kroku należy zalogować się do urządzenia i przejść do menu **KONFIGURACJA > UŻYTKOWNICY > Portal uwierzytelniania**, a następnie w zakładce **Dostępne metody** dodać nową metodę autoryzacji o nazwie **Agent SSO**.

Po dodaniu nowej metody we właściwościach należy wskazać domenę, której dotyczy połączenie z agentem SSO, adres IP hosta, na którym jest zainstalowany agent SSO (w naszym przypadku są to kontrolery domeny: ADDC1 i ADDC2), następnie podać hasło współdzielone, które zostało zdefiniowane podczas instalacji agenta.







+ Dodaj metode - X Usuń	Agent SSO		
Metody	Agent 350		
	Nazwa domeny:	stotmshield.internal	
▲? Dostep dla gości	Agent SSO		
Uwierzytelnianie poprzez polecającego			
Agent SSO	Adres IP:	ADDC1	▼ 8.
	Port:	agent_ad	- 5.
	Hasło:	•••••	
	Potwierdź hasło:	•••••	
	Siła hasła:	Silne	
	Port: Hasło:	agent_ad	▲ St
	Hasto:	•••••	
	Potwierdz Hasto.	Silas	
	Sira nasra.	Sinc	
	Kontroler domeny		
		alta Da dai hantarlar damanya 💙 Usuf	
	Wyszukiwanie	T Dodaj kontroler domeny 🔨 Usun	
	Wyszukiwanie ADDC1	T Dodaj kontroler domeny 🔨 Osun	

Po skonfigurowaniu metody autoryzacji *Agent SSO* pozostaje aktywować tę metodę w zakładce **Metody Uwierzytelniania**:

L UŻ	YTKOWNICY / I	PORTAL U	JWIERZYTELNIANIA		
DOS	TEPNE METODY	METOD	DA UWIERZYTELNIANIA PORTAL UWIERZYT	ELNIANIA PROFIL PORTA	ALU AUTORYZACJI
Wyszu	ıkaj użytkownika		🕂 Nowa reguła 👻 🗙 Usuń 🏦 W górę 🛛 🌲	W dół 🗁 Wytnij 🛛 🗗 Kop	biuj 🐑 Wklej
	Status	Źródło		Metoda uwierzytelniania	Komentarz
1	💭 właczona	Any us	ser@stotmshield.internal	1 💷 Agent SSO	

Na koniec należy zastosować wprowadzone zmiany i od tego momentu można tworzyć reguły filtrowania z uwzględnieniem zalogowanych użytkowników.

Inne metody autoryzacji

Poza powyższym sposobem autoryzacji użytkowników istnieje również kilka innych metod autoryzacji. Poniżej zostały opisane pozostałe metody autoryzacji w urządzeniu STORMSHIELD UTM:

NEXT GENERATION FIREWALL PODRĘCZNIK UŻYTKOWNIKA

>//





UŻYTKOWNICY / PORTAL UWIERZYTELNIANIA DOSTEPNE METODY METODA UWIERZYTELNIANIA PORTAL UWIERZYTELNIANIA PROFIL PORTALU AUTORYZACJI 🕂 Dodaj metodę 👻 💛 Usuń LDAP LDAP Konfiguracja LDAP Certyfikat (SSL) Radius Kerberos Transparentne uwierzytelnianie (SPNEGO) Agent SSO Uwierzytelnianie gości Konta tymczasowe Uwierzytelnianie poprzez polecającego

- LDAP standardowa metoda uwierzytelniania w oparciu o login oraz hasło podane przez użytkownika (metoda domyślna);
- **Certyfikat (SSL)** umożliwia automatyczne uwierzytelnienie użytkownika na urządzeniu za pośrednictwem certyfikatu zaimportowanego wcześniej do jego przeglądarki. Sama autoryzacja jest automatyczna i odbywa się "w tle" podczas otwierania dowolnej strony WWW;
- Radius umożliwia automatyczne uwierzytelnienie użytkownika za pośrednictwem zewnętrznego serwera RADIUS;
- Kerberos umożliwia uwierzytelnienie użytkownika za pośrednictwem zewnętrznego serwera KERBEROS;
- Transparentne uwierzytelnianie (SPNEGO) umożliwia transparentne uwierzytelnienie użytkowników w AD za pośrednictwem przeglądarki internetowej. Metoda ta wymaga wysłania zapytania HTTP/GET, a więc autoryzacja nie działa od razu po zalogowaniu się do domeny. Jest to metoda obecnie wyparta przez Agenta SSO;
- Agent SSO metoda typu Single Sign-On, pozwala na automatyczną autoryzację wymagająca od użytkownika jedynie zalogowania się do domeny Active Directory. Wymaga ona głębszej integracji ze środowiskiem (instalacja specjalnego agenta w domenie), jednak daje największą wygodę oraz prostotę korzystania przez co jest zalecaną metodą autoryzacji;
- Uwierzytelnianie gości jest to metoda umożliwiająca "uwierzytelnianie" użytkowników bez konieczności podawania poświadczeń. Podczas logowania użytkownikowi wyświetli się regulamin korzystania z dostępu do sieci i jedynie jego zaakceptowanie umożliwi dostęp. Metoda ta jest przydatna w przypadku publicznych sieci Wi-Fi. Warto zwrócić tutaj uwagę na to, że po pomyślnym uwierzytelnieniu logowany jest adres MAC hosta użytego przy połączeniu;
- Konta tymczasowe ten typ uwierzytelnienia umożliwia zarządzanie kontami o ograniczonym okresie ważności. Konta te mają na celu zapewnienie tymczasowego dostępu np. do Internetu osobom spoza organizacji. Kontami tymczasowymi można zarządzać w KONFIGURACJA > UŻYTKOWNICY > Konta tymczasowe. Konta tymczasowe nie są zapisywane w lokalnej bazie LDAP;
- Uwierzytelnianie przez polecającego umożliwia identyfikację użytkownika bez konieczności uwierzytelnienia się w Portalu uwierzytelniania. Użytkownik chcąc zostać zautoryzowanym będzie musiał wpisać swoje imię i nazwisko oraz adres e-mail "Sponsora". Sponsor (uprawniony użytkownik





naszej organizacji) otrzyma wówczas wiadomość e-mail zawierającą link potwierdzający taką prośbę. Po zatwierdzeniu żądania strona sponsorowana zostanie automatycznie przekierowana z Portalu dostępowego na żądaną stronę internetową.

Tworzenie reguł filtrowania w oparciu o zalogowanego użytkownika

Poniższy zrzut ekranu obrazuje przykładowe reguły zapory stworzone dla zalogowanych użytkowników.

🤹 (5) Filter 05		🝷 📔 Edytuj 🝷 📔 🏪 Eksportuj	0				
FIREWALL	NAT						
Szukaj		🕂 Dodaj 👻 🗙 Usuń 🏌	💶 📲 🖃 🔁 Wytnij 🖸 Ko	opiuj 🐑 Wklej	🗒 Wyszukaj w log	jach 🚱 Wyszuka	j w monitoringu
	Stan ≞▼	Akcja 🚉	Adres źródłowy	Adres docelowy	Port docelowy	Analiza protokoł	Polityki filtrowania
1	💽 włączona	🕤 zezwól	Reference Network_internals	DNS-svrs	İ dns_udp		IPS
2	💽 włączona	🕤 zezwól	💄 kowalski @ 🕮 Network_internals	Internet	* Any		FW
3	💽 włączona	 zezwól 	IT @ 聞 Network_internals	H Internet	1 http 1 https 1 ssh		IDS
4	🔍 włączona	zezwól	marketing @ 🛱 Network_internals	Internet	Ϊ http Ϊ https		IPS
5 ====	💶 włączona	 Portal uwierzytelniania Z wyjątkiem: authentication_bypass 	unknown @ 🕮 Network_internals	Internet	Ï http		IPS
6	💽 włączona	🗢 blokuj	* Any	* Any	* Any		IPS

Reguły te odpowiadają kolejno za:

- 1. Zezwolenie na dostęp dowolnych hostów ze wszystkich sieci chronionych do wskazanych w obiekcie DNS-svrs serwerów dns na porcie 53/UDP.
- 2. Zezwolenie na dostęp do wszystkich usług w Internecie dla użytkownika kowalski łączącego się z sieci chronionych z wyłączeniem analizy IPS.
- 3. Zezwolenie użytkownikom należącym do grupy IT łączącym się z sieci chronionych na połączenia realizowane do sieci Internet w ramach portów http, https, ssh z analizą IDS.
- 4. Zezwolenie użytkownikom należącym do grupy marketing łączącym się z sieci chronionych na połączenia realizowane do sieci Internet w ramach portów http, https.
- 5. Przekierowanie na Portal uwierzytelniania wszystkich użytkowników nieuwierzytelnionych próbujących wykonać połączenia do sieci Internet na porcie http z sieci chronionych (z wykluczeniem stron zdefiniowanych w obiekcie authentication_bypass).
- 6. Zablokowanie wszystkich innych połączeń.

80





Delegowanie zadań administracyjnych użytkownikom bazy LDAP

Konfiguracja delegacji uprawnień odbywa się w sekcji KONFIGURACJA > USTAWIENIA SYSTEMOWE > Administratorzy. Konfiguracja pozwala na określenie zakresu dostępu do zarządzania urządzeniem przez poszczególnych użytkowników. Uprawnienia mogą być **pełne** lub **tylko do odczytu** i obejmują wszystkie podstawowe funkcje urządzenia takie jak Firewall i NAT, VPN, konfigurację logów, IPS, filtry treści, konfigurację sieci, itp.

STOTMSHIELD.INTE + C ×	₩ USTAWIENIA SYSTEMOWE / ADMINISTRATORZY										
MODUŁY – UPRAWNIENIA KONTO ADMINISTRATORA ZARZĄDZAJ ZGŁOSZENIAMI											
Szukaj 💉 💒	Dodaj administratora 👻 V. Usuń 🏌 🌲 🚰 Kopiuj 👻 Wklej 😒 Pelna kontrola 🎝 Widok zaawansowany										
	Użytkownik lub Grupa użytkowników System Sieć Użytkownicy Zapora sieciowa Nasłuchiwanie Konta tymczasow										
11 USTAWIENIA SYSTEMOWE	1 🕹 kowalski@stormshield.stormshi 🗸 🗸 🗸 🗸										
Konfiguracja urządzenia	2 L mazur@stormshield X X X X X X										
Administratorzy	3 🛓 krawczyk@stormshield.stormshi X X X X X 🗴 🗸										



NEXT GENERATION FIREWALL PODRĘCZNIK UŻYTKOWNIKA





13. Wirtualne sieci prywatne (VPN)

VPN to technologia tworzenia bezpiecznych tuneli komunikacyjnych, w ramach których możliwy jest bezpieczny dostęp do zasobów firmowych. Ze względu na sposób połączenia VPN dzielimy na:

- **Site-to-Site** gdzie tunel ustanawiany jest pomiędzy dwoma urządzeniami, co pozwala na bezpieczne połączenie sieci chronionych przez te urządzenia.
- **Client-to-Site** umożliwia bezpośrednie połączenie komputera z siecią firmową. Ten typ tunelu wykorzystywany jest przede wszystkim przez użytkowników pracujących mobilnie.
- Client-to-Site (portal) umożliwia połączenie do usługi wewnątrz sieci firmowej z wykorzystaniem przeglądarki internetowej. Ten typ tunelu wykorzystywany jest przede wszystkim przez użytkowników pracujących mobilnie potrzebujących uzyskać szybki dostęp do konkretnej usługi bez konieczności instalacji/konfiguracji oprogramowania dedykowanego do nawiązywania połączeń VPN.

W przypadku urządzeń STORMSHIELD UTM dostępne są cztery możliwości tworzenia kanałów VPN:

- Protokół IPsec VPN w trybie Client-to-Site oraz Site-to-Site;
- Protokół SSL VPN w trybie Client-to-Site;
- **Portal SSL VPN** w trybie Client-to-Site (portal);
- **Protokół PPTP VPN** w trybie Client-to-Site.

Zastosowanie wybranego protokołu VPN powinno być podyktowane przede wszystkim względami bezpieczeństwa oraz funkcjonalnością wybranego typu połączenia.

Konfiguracja uprawnień użytkowników

W przypadku połączeń Client-to-Site przed przystąpieniem do konfiguracji wybranego typu tunelu najpierw należy skonfigurować uprawnienia użytkowników.

Mając skonfigurowaną już na urządzeniu STORMSHIELD UTM bazę użytkowników (wewnętrzną bądź zewnętrzną) można przystąpić do konfiguracji reguł dostępu. Dokonuje się tego w sekcji **KONFIGURACJA > UŻYTKOWNICY > Polityki dostępu**. W zakładce **Domyślne reguły dostępu** można wskazać domyślne ustawienia dla poszczególnych typów połączeń VPN, które będą zastosowane dla wszystkich użytkowników za wyjątkiem tych, dla których określono inne ustawienia na zakładce **Szczegółowy dostęp**.

*- «	💄 UŻYTKOWNICY / POLITYKI [DOSTĘPU
Szukaj * *	DOMYŚLNE REGUŁY DOSTEPU	SZCZEGÓŁOWY DOSTEP KONFIGURACJA PPTP VPN
Image: Ward with a system own own own own own own own own own own	Kiedy została zdefiniowana reguła dostę dostęp VPN Profil SSL VPN: Polityka IPSec: Polityka SSL VPN:	pu dostęp zabroniony dostęp zabroniony dostęp zabroniony
Polityki dostępu Portal uwierzytelniania Żądania użytkowników Konfiguracja bazy LDAP POLITYKI OCHRONY	Sponsoring Polityka sponsoringu:	Sezwói ▼





Jeśli użytkownik ma mieć inny niż domyślny poziom dostępu taką konfigurację przeprowadza się na zakładce **Szczegółowy dostęp**.

*	MODUŁY –	•	UŻYTKOWNIC	Y / POLITY	(I DOSTĘPU					
Sz	ukaj 🦼 🦉		DOMYŚLNE REGU	ŁY DOSTEPU	SZCZEGÓŁOWY DO	STEP	KONFIGURACJA F	PTP VPN		
ł#	USTAWIENIA SYSTEMOWE	W	yszukaj		+ Dodaj 🗙 Usuń	1 V	W górę 👃 W dół			
			Status	Użytkownik lu	ib grupa		Potral SSL VPN	IPSEC	Tunel SSL VPN	Sponsoring
=1=	KONFIGURACJA SIECI	1	🔍 włączona	A IT@storm	shield.stormshield.local		Administratorzy	O dopuszczony	Odopuszczony	Zablokuj
0)	OBIEKTY	2	🜑 włączona	L krawczyk	@stormshield.stormshield	local	🗗 Ksiegowosc	zabroniony	Odopuszczony	Zablokuj
-	UŻYTKOWNICY	3	🜑 włączona	💄 nowak@s	tormshield.stormshield.loo	al	🗗 www	zabroniony	zabroniony	🗢 Zablokuj
	Użytkownicy i grupy									
	Konta tymczasowe									
	Polityki dostępu									

W zależności od wybranego typu tunelu VPN interesują nas następujące opcje:

- **Protokół IPsec VPN** w Domyślnych regułach dostępu **Polityka IPsec**, a w Szczegółowym dostępie kolumna **IPSEC**;
- Protokół SSL VPN odpowiednio Polityka SSL VPN oraz kolumna Tunel SSL VPN;
- Portal SSL VPN tutaj będzie to Profil SSL VPN oraz kolumna Portal SSL VPN;
- Protokół PPTP VPN ten typ tunelu posiada odrębną konfigurację na zakładce Konfiguracja PPTP VPN.

W przypadku Portal SSL VPN na zakładce *Szczegółowy dostęp* można wskazać konkretny profil połączeń SSL VPN w trybie portal tak, aby dany użytkownik po połączeniu miał dostęp tylko do określonych usług. Opis konfiguracji profili Portalu SSL VPN znajduje się w dalszej części dokumentu.

IPsec VPN

Protokół IPsec jest najbezpieczniejszym i najwszechstronniejszym protokołem VPN jaki można skonfigurować na urządzeniu STORMSHIELD UTM. Pozwala na budowanie tuneli **Client-to-Site** jak i **Site-to-Site**, a jego użycie pozwala uzyskać pełen dostęp do zasobów w sieci.

Implementacja IPsec VPN w urządzeniach STORMSHIELD UTM jest w pełni zgodna ze standardem IPsec (zarówno w wersji IKEv1 jak i IKEv2), dzięki czemu możliwe jest zestawienie tunelu VPN z dowolnymi urządzeniami bądź aplikacjami klienckimi, które również wykorzystują zgodną z RFC implementację tego protokołu.

Konfiguracja IPsec odbywa się w sekcji **KONFIGURACJA > POŁĄCZENIA VPN > IPsec VPN**. Widok okna konfiguracyjnego przedstawiono poniżej:

83





*		ĸ	CO P	OŁĄCZE	NIA	VPN / IPSEC	VPN						
Szu	ukaj 💉 🖌		KON	KONFIGURACJA TUNELI IPSEC KLIENCI MOBILNI I ZDALNE LOKALIZACJE CERTYFIKATY I KLUCZE WSPÓŁDZIELONE PROFILE IPSEC									
挝	拼 USTAWIENIA SYSTEMOWE												
	KONFIGURACJA SIECI												
	OBIEKTY		Wyszu	ukiwany tek	st	× +	Dodaj - 🗙 Usuń 🕇 W gó	rej 🖡 W dół 🛛 🖙 Wytr	nij 🖻 Kopiuj 🕙 Wklej				
-	UŻYTKOWNICY		Lp.	Status		Sieć lokalna	Lokalizacja zdalna	Sieć zdalna	Profil IPSec (faza 2)	Czas życia	Opis		
≁	POLITYKI OCHRONY		1	💽 on	۲	Network_in	Oddzial-Kat-ipsec-gw	VPN-siec-zdalna	StrongEncryption	0			
Ø	KONTROLA APLIKACJI												
E 0	POŁĄCZENIA VPN												
	IPSec VPN												

Ponieważ konfiguracja IPsec uważana jest za bardzo skomplikowaną STORMSHIELD przygotował ułatwienia w postaci kreatorów, dzięki którym konfiguracja VPN jest łatwa, szybka i intuicyjna. Tunele IPsec składają się z dwóch faz. Po wybraniu opcji *Dodaj* i wybraniu interesującej nas opcji, uruchomi się kreator, który pomoże skonfigurować zarówno pierwszą jak i drugą fazę tunelu IPsec.

W obu fazach poza algorytmami szyfrowania definiuje się tzw. **Tunel endpoints** oraz **Traffic endpoints**. **Tunel endpoints** to dwa adresy reprezentujące publiczne adresy IP urządzeń, pomiędzy którymi zestawiany jest tunel. Z kolei **Traffic endpoints** określają sieci wewnętrzne jakie będą brały udział w komunikacji. Poniższy rysunek przedstawia czym są Tunel endpoints, a czym Traffic endpoints:



Konfiguracja połączenia typu Site-to-Site

Kreator konfiguracji tunelu IPsec umożliwia stworzenie w szybki i prosty sposób tunelu IPsec. Wystarczy jedynie zdefiniować dwie sieci prywatne biorące udział w komunikacji oraz bramę zdalną, z którą będziemy się komunikować.







KREATOR KONFIGURACJI TUNELU IPSEC		*
Sieć lokalna :	Wybierz zdalną lokalizacje :	Sieć zdalna (lokalizacja) :
Network_in 🗸 😝	Oddzial-Kat-ipsec-gw	VPN-siec-zdalna 🗸 😝
	Dodaj zdalną lokalizację IKEv1	< >
	Dodaj zdalna lokalizacje IKEv2	
	× Anulu	Wstecz Zakończ

Po wskazaniu sieci lokalnej oraz zdalnej (jeśli wcześniej nie została zdefiniowana na urządzeniu

STORMSHIELD UTM, można ją dodać z tego poziomu poprzez kliknięcie na ikonie 14) należy wskazać zdalną lokalizację. Jeśli zdalna lokalizacja nie została jeszcze skonfigurowana wybieramy opcję **Dodaj zdalną lokalizację IKEv1** bądź **Dodaj zdalną lokalizację IKEv2** w zależności od użytej wersji protokołu IKE. Spowoduje to otwarcie kreatora zdalnej lokalizacji.









KREATOR KONFIGURACJI ZDALNEJ LOKALIZACJI IKEV1	*
WYBÓR BRAMY - KREATORA KONFIGURACJI ZDALNEJ L	OKALIZACJI
Wybierz zdalną bramę :	VPN-bama-zdalna V 🗣
Nazwa zidentyfikowanej konfiguracji :	Oddzial-Kat-ipsec-gw
	× Anuluj «Wstecz » Dalej

Kreator ten pozwala skonfigurować Tunel endpoints oraz hasło/certyfikat zabezpieczające komunikację.



Po zakończeniu pracy obu kreatorów należy jeszcze skonfigurować Profile IPsec oraz aktywować profil.

86





Profile IPsec określają jakie algorytmy i klucze mają być użyte do zabezpieczenia tunelu. Można skorzystać z profili domyślnych lub stworzyć własne, zgodne z wymaganiami polityki bezpieczeństwa. Okno konfiguracyjne profili zostało przedstawione poniżej:

~ «		ĄCZENIA VPN / IPSEC VPN	I						
MODUŁY –	KONE						DZIELONE		
лкај 💉 🛃	KUNP	IGURACJA TUNELI IPSEC N	LIENCIMOB	ILNI I ZDALNE LUP	CALIZACJE CERT	TFINALT I KLUGZE WSPG	CUZIELONE	PROFILE IPSEC	·
USTAWIENIA SYSTEMOWE	Dom	yślne wartości dla nowej konfigu	iracji						
KONFIGURACJA SIECI	Domy	ślny profil IKE (faza 1) :	Strong	Encryption	~				
OBIEKTY	Domy	Domyślny profil IPSec (faza 2) : StrongEncryption							
UŻYTKOWNICY									
POLITYKI OCHRONY	+ Doc	daj - 🗙 Usuń	_ (Ogólne					
KONTROLA APLIKACJI	Тур	Nazwa	0	pis :		ANSSI RGSv2 compliant			
POŁACZENIA VPN	IKE	StrongEncryption	D	iffie-Hellman :		DH14 MODB Crown (2048	(bita)	~	
TOEQUZENIA VI N	IKE	GoodEncryption				DH 14 MODP Group (2040	-bits)		
IPSec VPN	IKE	Mobile	N	laksymalny czas ży	/cia (w sekundach) :	21600			
Portal SSL VPN	IPSEC	StrongEncryption							
	IPSEC	GoodEncryption	PR	OPOZYCJE					
SSL VPN	IPSEC	Mobile	+	Dodai 🗙 Usuń	🕈 W góre 👃 W dół				
PPTP VPN					Szyfrowanie			Uwierzy	rtelnianie
ADMINISTRACJA				Algorytm	Długos	ść klucza	Algorytm		Długość klucza
			1	aes	256		sha2_256		256
			2	aes	128		sha2_256		256
	MODULY - Jkaj > USTAWIENIA SYSTEMOWE KONFIGURACJA SIECI OBIEKTY UŻYTKOWNICY POLITYKI OCHRONY KONTROLA APLIKACJI POLĄCZENIA VPN IPSec VPN Portal SSL VPN PSTP VPN ADMINISTRACJA	Image: Constraint of the sector of the se	MODULY - Jkaj - USTAWIENIA SYSTEMOWE KONFIGURACJA TUNELI IPSEC KONFIGURACJA SIECI Domyślne wartości dla nowej konfigu OBIEKTY UŻYTKOWNICY POLĄCZENIA VPN Domyślne wartości dla nowej konfigu UŻYTKOWNICY Domyślne wartości dla nowej konfigu POLITYKI OCHRONY Domyślne wartości dla nowej konfigu KONTROLA APLIKACJI Domyślny profil IPSec (faza 2): POLĄCZENIA VPN IKE IPSec VPN Nazwa Portal SSL VPN IKE PPTP VPN ADMINISTRACJA	Image: Constraint of the second se	Composition Composition Composition MODULY - - - ika] Composition - USTAWIENIA SYSTEMOWE Composition Composition - KONFIGURACJA SIECI Domyśline wartości dla nowej konfiguracji - - OBIEKTY UŻYTKOWNICY Domyśline wartości dla nowej konfiguracji - - POLĄCZENIA VPN - - - - - IPSec VPN - <td>Image: Constraint of the second se</td> <td>Image: Control of the sector of the secto</td> <td>MODULY MADILY ACJA MADINISTRACJA POLACZENIA VPN / IPSEC VPN MADINISTRACJA POLACZENIA VPN MADINISTRACJA POLACZENIA VPN MADINISTRACJA POLACZENIA VPN POLACZENIA VPN</td> <td>MODULY → Main CD POLĄCZENIA VPN / IPSEC VPN Main KONFIGURACJA TUNELI IPSEC KLIENCI MOBILNI I ZDALNE LOKALIZACJE CERTVFIKATY I KLUCZE WSPÓLDZIELONE PROFILE IPSEC USTAWIENIA SYSTEMOWE KONFIGURACJA TUNELI IPSEC KLIENCI MOBILNI I ZDALNE LOKALIZACJE CERTVFIKATY I KLUCZE WSPÓLDZIELONE PROFILE IPSEC USTAWIENIA SYSTEMOWE KONFIGURACJA SIECI Domyślne wartości dla nowej konfiguracji OBJEKTY UZYTKOWNICY Domyślne wartości (faza 2): StrongEncryption Ogóine ODITYKI OCHRONY KE StrongEncryption Ogóine Ogóine Optal SSL VPN KE StrongEncryption Diffie Heliman : DH14 MODP Group (2048-bits) Maksymainy czas życia (w sekundach) : 21600 POTal SSL VPN IPSEC GoodEncryption IPSEC GoodEncryption Maksymainy czas życia (w sekundach) : 21600 POPOZYCJE AdministracJA IpseC GoodEncryption IpseC GoodEncryption IpseC GoodEncryption Ipsec doodEncryption</td>	Image: Constraint of the second se	Image: Control of the sector of the secto	MODULY MADILY ACJA MADINISTRACJA POLACZENIA VPN / IPSEC VPN MADINISTRACJA POLACZENIA VPN MADINISTRACJA POLACZENIA VPN MADINISTRACJA POLACZENIA VPN POLACZENIA VPN	MODULY → Main CD POLĄCZENIA VPN / IPSEC VPN Main KONFIGURACJA TUNELI IPSEC KLIENCI MOBILNI I ZDALNE LOKALIZACJE CERTVFIKATY I KLUCZE WSPÓLDZIELONE PROFILE IPSEC USTAWIENIA SYSTEMOWE KONFIGURACJA TUNELI IPSEC KLIENCI MOBILNI I ZDALNE LOKALIZACJE CERTVFIKATY I KLUCZE WSPÓLDZIELONE PROFILE IPSEC USTAWIENIA SYSTEMOWE KONFIGURACJA SIECI Domyślne wartości dla nowej konfiguracji OBJEKTY UZYTKOWNICY Domyślne wartości (faza 2): StrongEncryption Ogóine ODITYKI OCHRONY KE StrongEncryption Ogóine Ogóine Optal SSL VPN KE StrongEncryption Diffie Heliman : DH14 MODP Group (2048-bits) Maksymainy czas życia (w sekundach) : 21600 POTal SSL VPN IPSEC GoodEncryption IPSEC GoodEncryption Maksymainy czas życia (w sekundach) : 21600 POPOZYCJE AdministracJA IpseC GoodEncryption IpseC GoodEncryption IpseC GoodEncryption Ipsec doodEncryption

Profile IKE są profilami fazy pierwszej, natomiast profile IPsec są profilami fazy drugiej.

\rm 🛛 Uwaga

Najczęstsze problemy z połączeniem IPsec Site-to-Site wynikają z błędnie ustawionych profili IKE i/lub IPsec. Bardzo ważne jest to aby obie strony tunelu miały ustawione takie same algorytmy. Jeżeli jedna ze stron będzie miała inne parametry nie dojdzie do zestawienia tunelu VPN.





Konfiguracja połączenia Client-to-Site z użyciem STORMSHIELD VPN Client

Konfiguracja po stronie STORMSHIELD

W sekcji KONFIGURACJA > POŁĄCZENIA VPN > IPsec VPN należy przejść do zakładki Konfiguracja Tuneli IPsec > Konfiguracja klientów mobilnych i wybrać Dodaj > Nowa polityka Config mode. Podobnie jak w przypadku konfiguracji Site-to-Site uruchamia się kreator, w którym należy zdefiniować sieci jakie będą dostępne w tunelu: Sieć lokalna, Sieć zdalna (unikalna sieć, w ramach której przydzielane będą adresy klientom VPN) oraz wybrać Stwórz klienta mobilnego (IKEv1 lub IKEv2).

KREATOR IPSEC VPN CLIENT TO SITE (CONFIG MODE)		\$
	Lokalizacja zdalna :	
	Stwórz klienta mobilnego IKEv1	
Tunel IPSec Client to site w trybie Config mode, daje moż W trybie Config mode, użytkownicy zdalni będą używać a	Stworz kilenta mobilnego IKEV2	ryzacji użytkownika.
Sieć lokalna : Network_in 👻 🗣	Sieć zdalna :	VPN-siec-c2s 💌 😜
	× Anuluj	≪ Wstecz ✓ Zakończ

Kreator dodawania nowego klienta pozwoli na zdefiniowanie mechanizmu uwierzytelniania wykorzystywanego przez urządzenie. Najprostszym mechanizmem jest uwierzytelnianie z użyciem identyfikatora i hasła (klucz współdzielony).

88





KREATOR KONFIGURACJI ZDALNEJ LOKALIZACJI IKEV1			×
UWIERZYTELNIANIE HOSTÓW - KREATOR KONFIGURACJI KLIENTA MOBILNEGO)		
UWIERZYTELNIENIE LOKALIZACJI Z	ZDALNEJ		
◯ Certyfikat			
⊖ Hybrydowe			
Certyfikat + Xauth (iPhone)			
Klucz współdzielony (hasło)			
~			N = 1 .
~	Anuluj	Wstecz	» Dalej

Na etapie kreatora można stworzyć listę uwierzytelniania, ale można to zrobić również później na zakładce **Certyfikaty i klucze współdzielone**.

KREATOR KONFIGURACJI ZDALNEJ LOKALIZACJI	I IKEV1			>
UWIERZYTELNIANIE HOSTÓW - KREATOR KONF	IGURACJI KLIENTA MOB	LNEGO		
Wyszukiwany teks	t × + Dodaj ×	Usuń		
Identyfikator	Klucz współdzielony (ha	sło) 🔻		
jk@stormshield.pl	0x265e4867617939372	55e26484949306f69	697725	
🚺 🖣 🗍 Strona	1 z 1 🕨 🕅 🔒 🖓	à	>>>	
		× Anuluj	≪ Wstecz	≫ Dalej
	89			

NEXT GENERATION FIREWALL PODRĘCZNIK UŻYTKOWNIKA





Jeżeli nie zrobiono tego wcześniej, to należy jeszcze dokonać konfiguracji uprawnień użytkowników (Polityka IPsec / kolumna IPSEC) oraz dodać reguły firewall zezwalające na nawiązywanie połączeń IPsec typu Clientto-Site. Uprawnienia użytkowników do dostępu do usługi VPN nadawane są w sekcji **KONFIGURACAJ > UŻYTKOWNICY > Polityki dostępu** szczegółowo opisanej wyżej.

Konfiguracja firewall powinna zawierać reguły pozwalające na nawiązanie połączeń na portach 500UDP (isakmp), 4500UDP (isakmp_natt) oraz protokołu VPN-ESP. Ponadto należy skonfigurować regułę pozwalającą na ruch wewnątrz tunelu VPN.

Poniżej przedstawiono jak takie reguły powinny wyglądać:

+) POI	LITYKI (DCHRONY / FIF	REWALL I NAT					
🦺 (5) F	Filter 05		▼ Edytuj ▼	🖫 Eksportuj 🟮				
FIREW	/ALL	NAT						
Szukaj			🕂 🕂 Dodaj 🝷	X Usuń 🕇 👢 🖡	🗶 🛃 🚰 Wytnij 🛛 🖻 Ko	piuj 🐑 Wklej	🗒 Wyszukaj w loga	ch 📴 Wyszukaj w
		Stan ≞•	Akcja 🖃	Adres źródłowy	Adres docelowy	Port docelowy	Analiza protokołów	Polityki filtrowania
🗏 IP:	sec VPN o	client-to-site (zawie	era 2 reguł, od 1 to	2)				
1		🔍 włączona	zezwól	Internet	E Firewall_out	Ï isakmp Ï isakmp_natt		IPS
2		💽 włączona	zezwól	Internet	Firewall_out	* Any	wyłącznie vpn-esp	IPS
🗉 kli	enty IPse	c do siec lokalna (a	zawiera 1 reguł, od	1 3 to 3)				
3		🔍 włączona	🕤 zezwól	명물 VPN-siec-c2s przez IPSec	명 Network_in	* Any		IPS







Konfiguracja klienta STORMSHIELD VPN Client

Oprogramowanie Stormshield VPN Client jest dostępne do pobrania ze strefy klienta - <u>https://mystormshield.eu</u>. Do aktywacji oprogramowania wymagana jest dodatkowa licencja.

Po przeprowadzonej instalacji w kliencie VPN uruchamiamy kreator konfiguracji (Plik > Kreator konfiguracji).

Poniżej przedstawiono konfigurację klienta Stormshield VPN Client na potrzeby połączenia z urządzeniem STORMSHIELD UTM w ramach protokołu IPsec IKEv1.

W kreatorze należy wybrać opcję **Brama IKEv1**, a następnie publiczny adres IP lub FQDN urządzenia STORMSHIELD UTM, hasło współdzielone (nadane dla użytkownika podczas konfiguracji urządzenia) oraz adres sieci wewnętrznej udostępnianej przez urządzenie STORMSHIELD UTM (*Sieć lokalna* w konfiguracji IPsec na urządzeniu):

VPN Client		_	\times
Konfigurację Narzędzia	?		
Stormshield	VPN Client owered by TheGreenBow		
	IKE V1		
Konfiguracja VPN KE V1 KE V1 KE V1 KE V	Wizard Konfiguracji Klienta VPN: Krok 1 z 3		
Ikev1Gatewa Ikev1Tunne	Parametry tunelu VPN 2/3		
IKE V2	Wprowadź następujące parametry tunelu VPN:	tyle faz 1 tiem ie faz 1 i	
	Publiczny adres IP lub DNS (zewnętrzny: vpn.firma.pl zdalnej bramy		
	Wspólne hasło: •••••• Prywatny (wewnętrzny) adres IP sieci zdalnej 192 . 168 . 100 . 0		
	Poprzednie Następne Anuluj		
 VPN gotowa 			

NEXT GENERATION FIREWALL PODRĘCZNIK UŻYTKOWNIKA





Po zakończeniu Kreatora konfiguracji należy zmodyfikować niektóre z ustawień domyślnych, tak aby były zgodne z konfiguracją profili IKE i IPSEC na urządzeniu oraz podać dane autoryzacyjne:

1. W menu **Ikev1Gateway** na zakładce **Uwierzytelnianie** w sekcji **Kryptografia** należy zweryfikować zgodność użytych algorytmów:

VPN Client				_		\times			
Konfigurację Narzędzia ?									
Stormshield VPN C Powered by TheGr	lient					X			
Ikev1Gateway: Uwierzytelnianie									
Konfiguracja VPN	Uwierzytelnianie	Protokół Brama	Certyfikat						
Parametry IKE V1	Zdalna bra	imka				-			
Ikev 1 unnel		Interfejs:	Każdy		\sim				
SSL SSL		Zdalna bramka	ka vpn.firma.pl						
	Uwierzytelnianie								
	⊚w	spólne hasło	•••••						
		Potwierdź:	•••••						
	00	ertyfikat							
	X-Auth —					-			
	□w	łączony	X-Auth Popup						
		Login		R	az				
		Hasło		(i) □⊓	ryb hybrydov	Ny			
	Kryptogra	fia ———				-			
		Kodowanie	AES256 \checkmark						
		Uwierzytelnianie	SHA-256 \vee						
		Grupa Haseł	DH14 (2048) 🗸 🗸 🗸						
 VPN gotowa 	r.								

NEXT GENERATION FIREWALL

PODRĘCZNIK UŻYTKOWNIKA





2. Na zakładce **Protokół** w sekcji **Tożsamość** należy wskazać sposób identyfikacji klienta IPsec (jako identyfikator należy wybrać adres e-mail użytkownika zdefiniowanego w usłudze katalogowej LDAP bądź AD), a w sekcji **Zaawansowane właściwości** należy włączyć **Tryb Konfiguracji** i **Tryb Agresywny**

VPN Client						_	\times
Konfigurację Narzędzia ?							
Stormshield VPN C Powered by TheG	Client reenBow		X				
	Ikev1Gatev	way: Uwi	erzyteln	ianie			
🗏 Konfiguracja VPN	Uwierzytelnianie	Protokół	Brama Ce	ertyfikat			
Parametry IKE V1 Parametry IKE V1 Ikev1Gateway KE V2 IKE V2	Tożsamo	ść ———					
SSL SSL	Lokalne ID	E-mail	~	jk@stor	mshield.pl		
	Zdalne ID		~				
	Zaawans 4	owane włas agmentacja I Port NAT Po Tryb Konfig Tryb Agres	ściwości – KEv2 □ IKE □ ort : □ uracji ☑ ywny ☑	Rozmi	ar fragmentu	IATT	
VPN gotowa							





3. Należy też zwrócić uwagę na ustawienie czasu życia fazy 1 (IKE) – zakładka Brama, sekcja Czas życia. Domyślnym ustawieniem tego parametru na urządzeniu STORMSHIELD UTM jest 21600 (domyślnie użyty profil IKE - StrongEncryption).

VPN Client			- 🗆 X
Konfigurację Narzędzia ?			
Stormshield VPN C Powered by The	Client		
	Ikev1Gateway: Uwier	rzytelnianie	
Konfiguracja VPN KE V1 RE V1 Parametry IKE V1	Uwierzytelnianie Protokół Br Wykrywanie martwyc	rama Certyfikat	
• Ikev1Tunnel			
	Sprawdź interwał (sek) 30 sek.	
	Maksymalna liczba pró	ib 3	
	Opóźnienie pomiędz	zy 15 sek.	
	Czas życia ————		
	Czas życi	ia 21600 sek.	
	Parametry związane z	bramą ————	
	Brama redundantn	na	
	Retransmisj	je 3	
VPN gotowa			







4. Ustawienia dotyczące fazy 2 (IPSEC) znajdują się w menu **lkev1Tunnel**. Szczególną uwagę należy zwrócić na ustawienia na zakładce **IPsec** i sekcje: **Adresy** – Adres zdalnej sieci LAN (*Sieć lokalna* w ustawieniach urządzenia Stormshield), **ESP** – algorytmy szyfrowania i uwierzytelniania, **PFS** oraz **Czas życia**. Wszystkie powyższe ustawienia muszą być zgodne z ustawieniami drugiej strony tunelu VPN (urządzenie STORMSHIELD UTM). Domyślny profil dla takich połączeń (IPSEC - StrongEncryption) na urządzeniu STORMSHIELD UTM posiada odpowiednio AES256, SHA-256, PFS - DH14 (2048-bits), czas życia – 3600.

VPN Client	-	- 🗆 🗙	
Konfigurację Narzędzia ?			
Stormshield VPN C Powered by TheG	Client		
	Ikev1Tunnel: IPsec		
Konfiguracja VPN	IPsec Zaawansowane Automatyzacja Zdalne udostępnianie Adresy Adres Klienta VPN 0 . 0 . 0 . 0 0 Typ adresu Adres podsieci ✓ Adres zdalnej sieci LAN 192 . 168 . 100 . 0 0 Maska podsieci 255 . 255 . 255 . 0 0 ESP Kodowanie AES256 ✓ Uwierzytelnianie SHA-256 ✓ Tryb Tunel ✓		
	PFS Grupa DH14 (2048) ✓ Czas życia Czas życia Ipsec 3600 sek.		
 VPN gotowa 			

NEXT GENERATION FIREWALL PODRĘCZNIK UŻYTKOWNIKA





Aby zakończyć konfigurację klienta należy wybrać opcję **Plik > Zapisz** i przejść do panelu połączeń (Ctrl + Enter). W celu zestawienia tunelu VPN należy kliknąć przycisk **Otwórz**. Po zestawieniu tunelu VPN panel powinien wyglądać jak poniżej:









🕖 Wskazówka

W menu **MONITORING > MONITOROWANE > Tunele IPsec VPN** można monitorować aktualnie zestawione tunele IPsec VPN

Polityki								
Filtr:	Wyszukiwanie	×						
🗆 Ukryj zestaw	vione tunele, aby wyśw	ietlić tylko polityki z problema	ami					
Stan	Sieć lokalna	Nazwa sieci lokalnej	Nazwa bramy lokalnej	Katalog 1	Nazwa bramy zdalnej	Sieć z	dalna	Nazwa siec
Polityka: none	127.0.0.0	rfc5735_loopback		🗧 in		0.0.0.0	D	any
Polityka: none	127.0.0.0	rfc5735_loopback		⇒ out		0.0.0.0	0	any
1 Tunel(e)	192.168.100.0	Network_in	Firewall_out	🗧 🔒 in	184.165.11.41	192.1	68.200.0	
1 Tunel(e)	192.168.100.0	Network_in	Firewall_out	🔿 🔒 out	184.165.11.41	192.1	68.200.0	
Tunele	ko tunele odpowiadaja	ce wybranej polityce						
Nazwa bramy lo	kalnej Nazv	va bramy zdalnej	Z	Dane wychod	Dane przycho	Stan	Szyfrowanie	Autentykac
					400.1			have also

126

Jeśli występują jakiekolwiek problemy z zestawieniem tunelu VPN w pierwszej kolejności należy zweryfikować logi połączeń VPN znajdujące się w MONITORING >LOGI > VPN.

SSL VPN

Full SSL VPN

Tunelowanie SSL VPN pozwala na zestawienie pełnego tunelu **Client-to-Site** pomiędzy klientem mobilnym (stacja robocza, smartfon, itp.), a siecią firmową.

Tunelowanie to jest oparte na serwerze OpenVPN i łączy w sobie prostotę konfiguracji oraz zachowanie wysokiego poziomu bezpieczeństwa z uwagi na zastosowanie algorytmu AES.

W trakcie nawiązywania łączności użytkownik musi podać jedynie adres IP oraz poświadczenia, wszystkie pozostałe parametry związane z szyfrowaniem połączenia są synchronizowane w tle.

Konfiguracja SSL VPN odbywa się w sekcji **KONFIGURACJA > POŁĄCZENIA VPN > SSL VPN**. Widok okna konfiguracyjnego przedstawiono poniżej.

97





*	~	«			
ф	MODULY	-	POLĄCZENIA VPN / SSL VPN		
Sz	ıkaj	- Ko	Ą CZ		
11	USTAWIENIA SYSTEMOWE				
	KONEIGURAC, IA SIECI	Zev	vnętrzny adres IP lub nazwa domeny:	vpn.stormsnieid.pi	
_		Zas	Zasoby dostępne poprez SSL VPN:	Network_internals	-
8	OBIEKTY	Sie	ć zdalna (UDP):	ssl-vpn-udp	-
-	UŻYTKOWNICY	Sie	Sieć zdalna (TCP):	ssl-vpn-tcp	- 8
乧	POLITYKI OCHRONY	Ma	ksymalna liczba jednoczesnych	126	
Ø	KONTROLA APLIKACJI	poł	ączen SSL VPN:		
(a)	POŁĄCZENIA VPN	— Pa	rametry dla klienta SSL VPN		
	IPSec VPN		-		
	Portal SSL VDN	Naz	zwa domeny:		
	FUITAI SSE VEN	Pre	ferowany serwer DNS:	Wybierz serwer DNS	-
	SSL VPN	Alte	ernatywny serwer DNS:	Wybierz serwer DNS	-
	PPTP VPN		initial priori prior		
1	ADMINISTRACJA	_ •	Zaawansowane		

- Zewnętrzny adres IP lub nazwa domeny jednoznacznie identyfikuje publiczny adres IP/domenę, pod którą będzie dostępny serwer SSL VPN (zazwyczaj jest to po prostu adres IP przypisany do interfejsu zewnętrznego STORMSHIELD UTM);
- Zasoby dostępne poprzez SSL VPN wskazuje, które z dostępnych na urządzeniu STORMSHIELD UTM sieci mają być osiągalne dla klientów VPN po zestawieniu tunelu;
- Sieć zdalna (UDP) zakres adresów przydzielany klientom łączącym się za pośrednictwem protokołu UDP (domyślnie port 1194).
- Sieć zdalna (TCP) zakres adresów przydzielany klientom łączącym się za pośrednictwem protokołu TCP (domyślnie port 443).
- Maksymalna liczba jednoczesnych połączeń SSL VPN ilość tuneli, które mogą być jednocześnie uruchomione. Liczba ta zależy od modelu urządzenia, oraz sieci przypisanych klientom zdalnym.
- Nazwa domeny opcjonalna nazwa domeny.
- Preferowany/Alternatywny serwer DNS adres serwera DNS dla klientów mobilnych.

\rm 🛛 Uwaga

Zarówno **Sieć zdalna (UDP)** jak i **Sieć zdalna (TCP)** nie mogą w żadnej części pokrywać się z wcześniej zdefiniowanymi sieciami na interfejsach urządzenia STORMSHIELD UTM. Sieci te muszą być unikalne.

Należy pamiętać aby poza samą konfiguracją SSL VPN udzielić użytkownikom zdefiniowanym na urządzeniu odpowiednich uprawnień dostępowych (KONFIGURACJA > UŻYTKOWNICY > Polityki dostępu).

Domyślny mechanizm działania tuneli SSL VPN na urządzeniach STORMSHIELD UTM wykorzystuje Portal Uwierzytelniania do synchronizacji konfiguracji klienta Stormshield SSL VPN. Konieczne zatem jest włączenie odpowiedniego profilu autoryzacji (zalecanym profilem jest profil External) na zewnętrznym interfejsie urządzenia, na który będą przychodziły połączenia SSL VPN. Poniżej przykład takiej konfiguracji:





*	MODUŁY –		PORTAL UWIERZYTI	ELNIANIA		
Sz	ukaj 🦼 🖉	DOSTEPNE METODY	METODA UWIERZY	TELNIANIA	PORTAL UWIERZYTELNIANIA	PROFIL PORTALU AUTORYZACJI
+†1	USTAWIENIA SYSTEMOWE	Portal uwierzytelniania				
	KONFIGURACJA SIECI	PROFIL UWIERZYTELN	NIANIA ORAZ INTERFE.	JS		
	OBIEKTY	🕂 Dodaj 🛛 🗙 Usuń				
-	UŻYTKOWNICY	Interfejs	Profil	Don	nyślna metoda lub baza LDAP	
	Użytkownicy i grupy	out	External	LDA	P (stormshield.stormshield.local)	
	Konta tymczasowe					
	Polityki dostępu					
	Portal uwierzytelniania					

Klient Stormshield SSL VPN

W celu połączenia się poprzez **Tunel SSL VPN** można skorzystać z darmowego klienta VPN SSL Client dostępnego w sekcji **Download** na portalu https://mystormshield.eu.

Po poprawnej instalacji w zasobniku ukaże się ikona klienta. Klikając dwukrotnie lub wchodząc poprzez menu kontekstowe i wybierając *Start VPN* można przejść do konfiguracji klienta.



Sama konfiguracja klienta polega na wypełnienia trzech pól:

Stormshield	×				
Firewall address	vpn.stormshield.pl				
Username	kowalski				
Password	•••••				
	ОК	Cancel			

- Firewall address publiczny adres IP/domena urządzenia, z którym zestawiany jest tunel VPN.
- Username nazwa użytkownika.
- Password hasło wskazanego użytkownika.

W przypadku posiadania większej ilości urządzeń przydatna może okazać się funkcja książki adresowej (Address book).





🚺 Książka ad	💵 Książka adresowa 🛛 ? 🗙						
Wyszukaj:				Urządzenia: 1/1			
Nazwa	Adres IP	Nazwa użytkownika	Hasło	Opis		🚯 Doda	ij
Stormshield	vpn.stomshield.pl	kowalski	*****			怪 Zmie	ń
						🜒 Usur	i
					Po	każ hasł	a
					1	👌 Import	tuj
					\$	Ekspor	tuj
					Liczba	a pozycji:	: 1
✓ Szyfruj plik ks	siążki adresowej 🎤 Zm	nień hasło	- 🖬 :	Zapisz Wybi	erz	Can	cel

Portal SSL VPN

W odróżnieniu od Full SSL VPN, SSL VPN w trybie Portal nie wymaga instalacji dodatkowego oprogramowania. Klientem dla tego rodzaju połączeń VPN jest przeglądarka internetowa. Jedyny wymóg po stronie klienta to zainstalowana przeglądarka internetowa i oprogramowanie Java (w przypadku korzystania z serwerów aplikacyjnych).

W przypadku Portal SSL VPN każdy z kanałów jest tworzony dla pojedynczej usługi w odniesieniu do konkretnego serwisu. Czyli tunel VPN jest tworzony do konkretnego SERWERA na konkretny PORT. Portal SSL VPN najczęściej stosowany jest do tunelowania połączeń zdalnego pulpitu (RDP) lub połączeń do wewnętrznych serwerów http.

🚺 Uwaga

Należy pamiętać, że połączenia są zestawiane na zasadzie Client-to-Site (service) więc dostępny jest tylko jeden port. Jeśli usługa jest wieloportowa nie będzie możliwe jej udostępnienie za pomocą portalu SSL VPN.

100





Konfigurację SSL VPN należy rozpocząć od włączenia Portalu uwierzytelniania na zewnętrznym interfejsie urządzenia. Konfiguracji tej należy dokonać w sekcji **KONFIGURACJA > UŻYTKOWNICY > Portal uwierzytelniania**.

*	MODUŁY -		PORTAL UWIERZYT	ELNIANIA				
Szu	Jkaj "* "*	DOSTEPNE METODY	METODA UWIERZY	TELNIANIA	PORTAL UWIERZYTELNIANIA	PROFIL PORTALU AUTORYZACJI		
÷†‡	USTAWIENIA SYSTEMOWE	Portal uwierzytelniani	ia					
	KONFIGURACJA SIECI	PROFIL UWIERZYTEL	LNIANIA ORAZ INTERFE	JS				
0))	OBIEKTY	+ Dodaj 🗙 Usur	+ Dodaj X Usuń					
-	UŻYTKOWNICY	Interfejs	Profil	Dom	nyślna metoda lub baza LDAP			
	Użytkownicy i grupy	m out	External	LDA	P (stormshield.stormshield.local)			
	Konta tymczasowe							
	Polityki dostępu							
	Portal uwierzytelniania							

Aby skonfigurować serwer SSL VPN w trybie Portal należy przejść do sekcji **KONFIGURACJA > POŁĄCZENIA VPN > Portal SSL VPN** i zaznaczyć opcję *Włącz SSL VPN*. Następnie należy wybrać jakiego typu usługi chcemy udostępnić za pomocą **SSL VPN**.

*	•	«
0	MODUŁY	-
Sz	ukaj	12
ļţļ	USTAWIENIA SYSTEMOWE	
ЦĽ	KONFIGURACJA SIECI	- 1
8	OBIEKTY	_
•	UŻYTKOWNICY	
乧	POLITYKI OCHRONY	_
Ø	KONTROLA APLIKACJI	_
•	POŁĄCZENIA VPN	_
	IPSec VPN	
	Portal SSL VPN	

101

NEXT GENERATION FIREWALL

PODRĘCZNIK UŻYTKOWNIKA





SERWERY HTTP - połączenia do serwerów intranetowych

Na zakładce **SERWERY HTTP** należy użyć przycisku **Dodaj** w celu skonfigurowania nowego zasobu. Do wyboru jest dostęp do zwykłego serwera http lub jeden z predefiniowanych szablonów dostępu do takich usług jak Microsoft OWA czy Lotus Domino.

*	- « MODUŁY –	e	D POŁĄCZ	ENIA VPN / PORT	FAL SSL VPN	
Szu	Jkaj 🧩 🖉	Ι.	OGÓLNE	SERWERY HTTP	SERWERY APLIKACYJNE PROFILE SSL V	/PN
ļţļ	USTAWIENIA SYSTEMOWE		+ _{Dodaj} -	× Usuń	Serwery HTTP	
	KONFIGURACJA SIECI		Serwer	нттр	daj lub wybierz serwer.	
9	OBIEKTY		Serwer	HTTP (OWA 2003) Prer	mium	
•	UŻYTKOWNICY		Serwer	HTTP (OWA 2007) Prer HTTP (Lotus Domino)	mium	
৵	POLITYKI OCHRONY					
0	KONTROLA APLIKACJI					
(a))	POŁĄCZENIA VPN					
	IPSec VPN					
	Portal SSL VPN					

W oknie konfiguracji dostępu do serwera http można skonfigurować między innymi:

- Serwer obiekt reprezentujący adres IP serwera docelowego;
- Port port usługi http serwera, zazwyczaj jest to port http (80/TCP);
- Adres URL serwera HTTP pozwala na wskazanie podstrony, na którą będzie automatycznie przekierowany ruch;
- Odnośnik do serwera w tym miejscu znajduje się odnośnik, który jest dynamicznie tworzony na podstawie powyższych parametrów;
- Nazwa odnośnika na portalu nazwa pod jaką będzie widoczne połączenie w oknie portalu SSL VPN. Nazwa powinna ułatwiać użytkownikom identyfikację usługi.

** «	D POŁĄCZENIA VPN / PORTAL SSL VPN
Szukaj x ^k x ⁿ	OGÓLNE SERWERY HTTP SERWERY APLIKACYJNE PROFILE SSL VPN
₩ USTAWIENIA SYSTEMOWE ▲ KONFIGURACJA SIECI ● OBJEKTY ▲ UŻYTKOWNICY ◆ POLITYKI OCHRONY ♥ KONTROLA APLIKACJI ■ POŁĄCZENIA VPN IPSec VPN Portal SSL VPN	+ Dodaj• X Usuń Nazwa Serwer Web Serwer WWW Serwer WWW Serwer : Yort : http Adres URL serwera HTTP : cms Odnośnik do serwera : http://WWW-svr-priv-ip/cms Nazwa odnośnika na portalu : Wewnętrzny serwer WWW - ▽ Zaawansowane -
	102

NEXT GENERATION FIREWALL PODRĘCZNIK UŻYTKOWNIKA





Kolejnym krokiem jest stworzenie odpowiedniego profilu SSL VPN, czynność ta została opisana w <u>kolejnych</u> <u>rozdziałach</u> niniejszej dokumentacji.

SERWERY APLIKACYJNE

Dostęp do serwerów aplikacyjnych realizowany jest za pomocą aplikacji Java. Działanie tego połączenia opiera się o przechwycenie przez aplet Java połączeń na port loopback komputera klienta (127.0.0.1) i tunelowanie ich wewnątrz połączenia SSL VPN do serwera docelowego.

Przykład konfiguracji dostępu do serwerów aplikacyjnych został przedstawiony poniżej i obejmuje:

- Serwer obiekt reprezentujący adres IP serwera docelowego;
- Port port usługi serwera, która ma zostać udostępniona;
- Konfiguracja klienta
 - Adres IP adres IP, z którego Java będzie przechwytywała połączenia;
 - **Port** port, z którego Java będzie przechwytywała połączenia.

*- «	TO POŁACZENIA VPN / PORTAL SSL VPN						
🌣 MODUŁY 🚽							
Szukaj 💉 🖉	OGÓLNE SERWERY HTTP SERWERY APLIKACYJNE PROFILE SSL VPN						
H USTAWIENIA SYSTEMOWE	+ Dodaj• × Usuń Serwery aplikacyjne RDP						
KONFIGURACJA SIECI	Nazwa Serwer : SQL-svr-privip V						
S OBIEKTY	SQL-RDP Port : microsoft-ts Y 4						
LUŻYTKOWNICY	Konfiguracja klienta						
POLITYKI OCHRONY	Adres IP : 127.0.0.1						
KONTROLA APLIKACJI	Port: 11220						
D POŁĄCZENIA VPN							
IPSec VPN	Zgodny z Citrix						
Portal SSL VPN	Wykonaj polecenie : mstsc - v localhost:11220						
SSL VPN							
-							

Bardzo przydatnym parametrem jest opcja **Wykonaj polecenie** w ustawieniach zaawansowanych, która pozwala na określenie polecenia, jakie zostanie wykonane po uruchomieniu apletu Java i wybraniu odpowiedniego linku. W tym wypadku będzie to polecenie *mstsc –v localhost:11220*, które wywołuje klienta zdalnego pulpitu (mstsc) i uruchamia połączenie do adresu 127.0.0.1 na port 11220. Dzięki temu użytkownik po zalogowaniu się nie musi uruchamiać klienta RDP i wpisywać adresu ręcznie. Wystarczy, że kliknie link, co spowoduje automatyczne uruchomienie się klienta zdalnego pulpitu wraz z niezbędnymi do połączenia opcjami.







Profile SSL VPN

Profile umożliwiają nadanie użytkownikom uprawnień jedynie do wybranych połączeń w ramach całego serwera SSL VPN w trybie Portalu. Zakładka **Profile SSL VPN** służy do konfiguracji, które serwery maja być dostępne w ramach którego profilu.

★ -						
Szukaj	OGÓLNE SERWERY HTTP	SERWERY APLIKACYJNE PROFILE SSL VPN				
料 USTAWIENIA SYSTEMOWE	+ Dodaj × Usuń	Profil Ksiegowosc				
KONFIGURACJA SIECI	Nazwa	Opis :				
S OBIEKTY	WWW	SERWERY HTTP	SERWERY APLIKACYJNE			
	Ksiegowosc	Status Nazwa	Status Nazwa			
	Administratorzy	właczona Serwer WWW	właczona SQL-RDP			
POLITYKI OCHRONY			www.cona ERP-test			
Ø KONTROLA APLIKACJI			- wyiączona			
DOŁĄCZENIA VPN						
IPSec VPN						
Portal SSL VPN						

Dowiązania profilu SSL VPN do użytkownika dokonuje się w menu **KONFIGURACJA > UŻYTKOWNICY > Polityki** dostępu.









PPTP VPN (Point to Point Tunneling Protocol)

PPTP jest protokołem najprostszym w konfiguracji jednak najmniej bezpiecznym i odradza się jego użycie z wyjątkiem sytuacji gdzie musimy zestawić tunel VPN z klientem, który nie obsługuje innych typów połączeń VPN. Protokół PPTP pozwala na tworzenie tuneli typu **Client-to-Site** z wykorzystaniem klienta wbudowanego w system Microsoft Windows. Po stronie systemu operacyjnego w ustawieniach **Sieć i Internet > VPN** należy **Dodać połączenie VPN** i podać parametry połączenia PPTP.

Ustawienia		-
ŵ Strona główna	VPN	
Znajdž ustawienie	+ Dodaj połączenie VPN	
🖨 Stan	Opcje zaawansowa	Dodaj połączenie VPN
토 Ethernet	Włączone	Dostawca sieci VPN
ි Telefoniczne	Zezwalaj na połączenia VPI	Windows (wbudowane)
% VPN		Nazwa połączenia PPTP do Firmy
r [™] Tryb samolotowy	Pokrewne ustawien	Nazwa lub adres serwera
🕒 Zużycie danych	Zmień opcje karty Zmień opcje za wansowan	vpn.firma.pl
Serwer proxy	Centrum sieci i udostępnia	Typ sieci VPN
		Protokół PPTP (Point to Point Tunneling Protoco 🗸
		Typ informacji logowania
		Zapisz Anuluj

Po stronie STORMSHIELD UTM stosownej konfiguracji należy dokonać w sekcji **KONFIGURACJA > POŁĄCZENIA** VPN > PPTP VPN.









POŁĄCZENIA VPN / PPTP VPN		
Uruchom serwer PPTP VPN Zakres przydzielanych adresów klientom :	klienci-pptp	~ Ę
Parametry dla klienta PPTP		
Serwer DNS :	AD-DNS-svr	▼ € ₁
Serwer NetBIOS (WINS) :		~ Ę
- ▽ Zaawansowane		

W tym miejscu należy skonfigurować następujące opcje:

- Uruchom serwer PPTP VPN włączenie/wyłączenie usługi PPTP na urządzeniu;
- Zakres przydzielanych adresów klientom zakres adresów IP jakie będą uzyskiwali klienci łącząc się poprzez tunel PPTP. Ważne jest, aby ten zakres nie pokrywał się z adresami IP wykorzystywanym przez inne hosty w sieci LAN, jednak (w przeciwieństwie do konfiguracji SSL VPN oraz IPsec VPN) musi on zawierać się w tej samej podsieci, do której zestawiany jest tunel VPN (np. gdy używana jest sieć 192.168.1.0/24 to na potrzeby PPTP VPN można użyć zakresu adresów od 192.168.1.240-192.168.1.250);
- Serwer DNS adres serwera DNS dla klientów PPTP VPN;
- Serwer NetBIOS (WINS) adres serwera usługi NetBIOS dla klientów PPTP VPN.

Ostatnim krokiem jest nadanie praw użytkownikom do tworzenia tuneli PPTP VPN. Konfiguracji tej należy dokonać w sekcji **KONFIGURACJA > UŻYTKOWNICY > Polityki dostępu** w zakładce **Konfiguracja PPTP VPN**.

🚺 Uwaga

Z uwagi na luki w protokole PPTP, przy konfiguracji polityk dostępu dla PPTP należy zdefiniować nowe (najlepiej inne) hasło użytkownika.

106

NEXT GENERATION FIREWALL PODRĘCZNIK UŻYTKOWNIKA





14. Konfiguracja proxy HTTP, SMTP, POP3, FTP, SSL

Każdy z mechanizmów proxy w urządzeniach STORMSHIELD UTM może działać w sposób transparentny dla użytkownika, tzn. nie wymagać konfiguracji przeglądarki czy innego oprogramowania zależnie od protokołu. Ponadto dla urządzeń działających w trybie bridge możliwe jest przełączenie mechanizmu proxy w tryb transparentny z punktu widzenia sieci, tzn. dla ruchu proxy pozostawiany jest każdorazowo oryginalny nagłówek TCP/IP. W przypadku protokołu HTTP możliwe jest również skonfigurowanie proxy w trybie explicit proxy, tzn. takiego, które jest jawnie skonfigurowane w przeglądarce.

Poniżej przedstawiono funkcjonalność najpopularniejszych z mechanizmów proxy:

HTTP proxy

- klasyfikacja URL (filtrowanie dostępu do wybranych grup stron www),
- konfiguracja strony informującej o zablokowaniu dostępu do strony www (Block page),
- skanowanie antywirusowe dla ruchu http,
- analiza z użyciem mechanizmu Sandboxing (Stormshield Breach Fighter),
- analiza WEB 2.0 analiza kodu HTML i JavaScript,
- określenie maksymalnego rozmiaru pliku pobieranego przez http,
- filtrowanie plików po typie (MIME Type),
- buforowanie zawartości stron (proxy cache).

POP3 proxy

- skaner antyspam (wiadomość SPAM jest oznaczana przedrostkiem w temacie wiadomości lub może być blokowana),
- skaner antywirusowy,
- analiza z użyciem mechanizmu Sandboxing (Stormshield Breach Fighter),
- kontrola komend w ramach protokołu pop3.

SMTP proxy

- skaner antyspam (wiadomość SPAM jest oznaczana przedrostkiem w temacie wiadomości lub może być blokowana),
- skaner antywirusowy,
- analiza z użyciem mechanizmu Sandboxing (Stormshield Breach Fighter),
- filtr SMTP określający reguły filtrowania wiadomości e-mail w odniesieniu do nadawcy lub odbiorcy,
- kontrola komend w ramach protokołu smtp,
- określenie limitów wielkości poczty i liczby odbiorców.

FTP proxy

- skaner antywirusowy,
- analiza z użyciem mechanizmu Sandboxing (Stormshield Breach Fighter),
- możliwość określenia dozwolonych trybów transmisji FTP,
- możliwość kontroli dostępu na podstawie białej / czarnej listy użytkowników FTP,
- kontrola komend w ramach protokołu FTP.

SSL proxy

• skanowanie certyfikatów SSL (sprawdzanie poprawności, filtrowanie dostępu na podstawie CN),

NEXT GENERATION FIREWALL PODRĘCZNIK UŻYTKOWNIKA





• umożliwienie pozostałym usługom proxy na analizę szyfrowanych wersji protokołów (https, smtps, pop3s).

Uruchomienie proxy odbywa się poprzez włączenie w regule firewall w kolumnie **Polityki filtrowania** jednego z modułów **Filtrowania treści**.

Włączenie skanowania proxy dla reguły firewall jest jednak ostatnim krokiem konfiguracji. Wcześniej należy skonfigurować ogólne ustawienia proxy oraz skanery i filtry, które będą używane podczas skanowania ruchu.

HTTP proxy

Ogólna konfiguracja proxy http znajduje się w pluginie HTTP a więc w sekcji **KONFIGURACJA > KONTROLA APLIKACJI > Analiza protokołów > HTTP**. Znajduje się tutaj między innymi konfiguracja trybu pracy modułu proxy czy konfiguracja usługi ICAP.

*- «	🕅 KONTROLA APLIKACJI / ANALIZA P	ROTOKOŁÓW	
🏟 MODUŁY 🚽			
Szukaj 🗶 🛃	Wyszukiwanie	(1) http_01 Edytuj V 🚺 💶 Pokaż ustawienia wspólne dla wszystkich profili	
批 USTAWIENIA SYSTEMOWE	Komunikatory Protokoły IP	ANALIZA PROTOKOŁU PROXY ICAP ANALIZA ZAWARTOŚCI ANALIZA SANDBOXING	
KONFIGURACJA SIECI	 Protokoły Microsoft Protokoły przemysłowe 	HTML/Javascript	
S OBIEKTY	VoIP / Streaming NNS	Maksymalna długość dla tagu HTML : 24576	
	I FTP	Analizuj JAVASCRIPT	
POLITYKI OCHRONY	🖁 НТТР	Automatycznie usuwaj niebezpieczny kod	
KONTROLA APLIKACJI	I NTP	✓ Dekompresja w locie	
Alarmy	POP3	LISTA WYJĄTKÓW W KONTEKŚCIE USUWANIA NIEBEZPIECZNEGO KODU (USER-AGENT)	
Analiza protokołów	I SMTP I SNMP	+ Dodaj × Usuń	
Ustawienia profili	SSL .	Mozilla/2	^
Audut podotności	I TFTP	MSIE 4.0b2	
Addyr podatilosof	1 inne	RealPlayer 4.0	
Reputacja hosta		Java/1.0	~
Antywirus			
Antyspam		Uwierzytelnianie	
D POŁĄCZENIA VPN		Sprawdzaj użytkownika	
ADMINISTRACJA			
		Maksymalne wartości parametrów dla HTTP URL (w bajtach)	
		Długość URL (domena + ścieżka) : 2048	
		Maksymalna długość dla parametru (po 1024 🗘	
		Calkowita dlugość URL (URL + 2048	

Konfiguracja zakładek Analiza zawartości i Analiza Sandboxing jest podobna we wszystkich protokołach, dla których można uruchomić proxy i obejmuje konfigurację systemu antywirusowego, tzn. określa Maksymalny rozmiar pliku dla analizy antywirusowej i Sandbox (kB) oraz zachowanie systemu AV w przypadku wykrycia wirusa, analizy zakończonej błędem lub sytuacji kiedy nie można odczytać danych.

Maksymalny rozmiar pliku dla analizy antywirusowej i Sandbox (KB) :	~
Akcje dla skanera antywirusowego	
W przypadku wykrycia wirusa : Zablokuj	¥
Jeżeli analiza zakończona błędem : Zablokuj	*
Jeżeli nie można odczytać danych : Zezwól bez skanowania	~




Z kolei w przypadku Analizy Sandboxing obejmuje możliwość wyłączenia analizy dla wskazanych typów plików oraz definicję podjętej akcji w przypadku **wykrytego malware** lub jeżeli **analiza Sandbox zakończy się błędem.**

ANALIZA PROTO	KOŁU PROXY	ICAP ANALIZA ZAW	ARTOŚCI	ANALIZA SANDBOXING
Sandboxing				
Stan	Typ pliku		Ma	ksymalny rozmiar pliku dla analizy (KB)
 włączona 	Pliki archiwum			
 włączona 	Dokumenty pakietu Of	fice		
 włączona 	Pliki wykonywalne			
 włączona 	Dokumenty PDF			
 włączona 	Flash			
 włączona 	Java			
Akcja dla plików				
Akcja dla wykryteg	go malware :	Zablokuj	~	
Jeżeli analiza San błędem :	dbox zakończona	Zezwól bez skanowania	*	

W przypadku protokołu http w zakładce **Analiza zawartości** znajdują się funkcje niedostępne w innych protokołach i są to:

- **Częściowe pobieranie plików** opcja odpowiedzialna za buforowanie danych przed poddaniem ich analizie antywirusowej;
- Maksymalny rozmiar pliku (kB) określenie maksymalnej wielkości pliku jaki będzie można pobrać poprzez protokół http;
- Filtr pliku ze względu na typ MIME pozwala na blokowanie plików określonego typu np. plików audio.

🚺 Uwaga

Jeśli włączona jest analiza AV zalecane jest przełączenie opcji **Częściowe pobieranie plików** na **Zezwól**. W przypadku innej konfiguracji może dojść do problemów z pobieraniem plików np. z aktualizacjami Microsoft czy Adobe.





Konfiguracja filtra URL

Dostęp do stron internetowych można ograniczać wykorzystując wbudowany w urządzenie filtr URL. Do wyboru są następujące filtry URL:

- baza podstawowa 16 kategorii tematycznych,
- baza podstawowa z polską klasyfikacją stron ponad 50 kategorii tematycznych,
- **baza producenta przechowywana w chmurze (Extended Web Control URL)** ponad 100 mln stron w 65 kategoriach tematycznych,
- klasyfikacja URL stworzona przez administratora.

Konfiguracja klasyfikacji URL znajduje się w zakładce **KONFIGURACJA > OBIEKTY > Klasyfikacja URL**. W zakładce **Klasyfikacja producenta** można znaleźć informację o tym jaka baza URL jest obecnie wykorzystywana przez urządzenie oraz jakie kategorie tematyczne są dostępne w ramach tej klasyfikacji, a także można z tego poziomu zmienić tą klasyfikację.

🕖 Wskazówka

Najprostszym sposobem zmiany klasyfikacji URL na **bazę podstawowa z polską klasyfikacją stron** jest wykonanie kilku poleceń z poziomu konsoli. Zanim jednak polecenia takie będą wykonane należy upewnić się, że w WebGUI *KONFIGURACJA > OBIEKTY > Klasyfikacja URL > Klasyfikacja producenta* ustawiona jest **Podstawowa baza URL**. Po weryfikacji ustawień łączymy się do urządzenia z użyciem protokołu SSH (np. programem PuTTY) i wykonujemy poniższe polecenia:

```
setconf ~/ConfigFiles/object Host update.stormshield.pl 91.201.154.218,resolve=dynamic
setconf ~/ConfigFiles/autoupdate URLFiltering URL http://update.stormshield.pl/1
setconf ~/ConfigFiles/autoupdate URLFiltering Secure 0
enobject
objectsync
autoupdate -f -t URLFiltering
```

Po wydaniu polecenia nastąpi automatyczne pobranie nowej klasyfikacji URL. W kolejnym kroku można rozpocząć konfigurację Filtrowania URL w oparciu o nowe kategorie.

Klasyfikacja URL stworzona przez administratora

Tworzenie własnych grup klasyfikacji polega na określeniu łańcucha znaków, które są porównywane z adresem URL w nagłówku http podczas nawiązania połączenia z serwerem www. Przykładowo aby zablokować wszystkie strony, gdzie w adresie pojawi się łańcuch znaków "moto" należy zdefiniować następujący wpis: *moto*

Tak zdefiniowany wpis *moto* będzie znajdował dopasowanie np. w adresach: *www.motoryzacja.pl, www.moto.de,* motory.com.pl, itp.

Innym przykładem zastosowania własnych kategorii URL jest możliwość blokowania plików po ich rozszerzeniach. Jeśli administrator zdefiniuje maskę w formacie **.exe* to pod taki wpis będą znajdowały dopasowanie wszystkie adresy URL kończące się znakami '.exe' a więc adresy będące linkami do plików wykonywalnych exe.

110





Poniższy zrzut ekranu pokazuje konfiguracje obu przykładów.

* • «	SOBIEKTY / KLASYFIKACJA URL
Szukaj 💉 🛃	KLASYFIKACJA WŁASNA NAZWA CERTYFIKATU GRUPY CERTYFIKATÓW KLASYFIKACJA PRODUCENTA
H USTAWIENIA SYSTEMOWE	Dodaj Usuń 👁 Sprawdź Sprawdź klasyfikację adresu 🗟 Klasyfikacja
KONFIGURACJA SIECI	Nazwa Opis Format dla adresu URL
S OBIEKTY	Klasyfikacja-własna dozwolone znaki *, ?, /, _[a-z]
Objekty siesiowe	vpnsLowa przykład www.google.com/* zykłod.com/*
Objekty sieciowe	authentiation buoass
Klasyfikacja URL	
Certyfikaty - PKI	KLASYFIKACJA-WLASNA
	Dodaj adres URL Usuń adres URL
1	URL A Komentarz
* POLITYKI OCHRONY	*.exe
KONTROLA APLIKACJI	*moto*
D POŁACZENIA VPN	

Polityka Filtrowania URL

Polityka filtrowania URL określa, jakie kategorie mają być dozwolone a jakie zablokowane w ramach określonego profilu konfiguracji. Profili **Filtrowania URL** jest 10, co umożliwia stworzenie 10 niezależnych zestawów reguł dostępu do stron www. Konfiguracja polityk znajduje się w sekcji **KONFIGURACJA > POLITYKI OCHRONY > Filtrowanie URL**. W ramach polityki możliwe jest zdefiniowanie następujących akcji dla każdej z kategorii:

- Zezwól strony z tej kategorii nie są blokowane;
- Zablokuj dostęp do stron zostanie zablokowany;
- **BlockPage_00** do **BlockPage_03** dostęp do stron zostanie zablokowany z komunikatem w formie strony www. Do dyspozycji administratora są cztery takie strony, które może dowolnie modyfikować.

Ponadto można skorzystać również z następujących opcji okna konfiguracyjnego:

- Dodaj wszystkie wbudowane kategorie spowoduje wypełnienie listy wszystkimi kategoriami dostępnymi w bazie;
- Sprawdź klasyfikację adresu weryfikuje do jakich kategorii należy wskazana strona WWW.

Poniższy obraz pokazuje przykładową konfigurację polityki filtrowania URL.

*- «	+ POLITYKI OCHRONY / FILTROWAN	ANIE URL
🌣 MODULY -		
Szukaj 🧩 🖉	(0) URLFilter_00 + Edy	Jytuj * 1 🛡 Dostawca kategorii uri: <u>Rozszerzona baza URL w chmurze</u>
	🕂 Dodaj 🗙 Usuń 🕇 W górę 🖡	🛛 W dół 🚰 Wytnij 💽 Kopiuj 🕑 Wklej 🕂 Dodaj wszystkie wbudowane kategorie Sprawdź klasyfikację adresu 🖉 Klasyfikacja
TIT USTAWIENIA SYSTEMOWE	Status 🚉 Akcja 🚉	r Grupa URL Komentarz
KONFIGURACJA SIECI	1 🖸 Wyłącz 💿 Zezwól	authentication_bypass authorize the URLs of authentication_bypass group
S OBIEKTY	2 💽 Włącz 💿 Zezwól	Unknown
	3 💽 Włącz 😪 BlockPage_00	Advertisements & Pop-Ups
	4 💿 Włącz 💿 Zezwól	D Alcohol & Tobacco
	5 💽 Włącz 😪 BlockPage_00	D Anonymizers
Firewall i NAT	6 💽 Włącz 💿 Zezwól	D Arts
Filtrowanie URL	7 💽 Włącz 💿 Zezwól	Business
Filtrowanie SSL	8 💽 Włącz 💿 Zezwól	D Transportation
Filtreuropie poestu	9 💽 Włącz 💿 Zezwól	D Chat
Fill Owalle poczty	10 💿 Włącz 💿 Zezwól	Forums & Newsgroups
Ustawienia QoS	11 🜑 Włącz 🗣 BlockPage_00	D Compromised
Domyślne reguły firewall	12 💽 Włącz 💿 Zezwól	Computers & Technology
KONTROLA APLIKACJI	13 🜑 Włącz 🗣 BlockPage_00	Criminal Activity
	14 🜑 Włącz 😪 BlockPage_00	Dating & Personals
m m	15 🜑 Włącz 😪 BlockPage_00	Download Sites
U ADMINISTRACJA	16 💽 Włącz 💿 Zezwól	Education





🚺 Uwaga

Tak jak w przypadku reguł Firewall i NAT kolejność reguł Filtrowania URL ma znacznie, ponieważ reguły sprawdzane są od pierwszej do ostatniej (kolejność reguł zdefiniowana przez administratora). Jeżeli dana strona należy do więcej niż jednej Grupy URL będzie wykonana akcja zdefiniowana w pierwszej napotkanej regule. Kolejne reguły nie będą przetwarzane.

🕖 Wskazówka

Istnieje możliwość zgłoszenia niesklasyfikowanego adresu URL. Dokonać tego można, dla polskiej klasyfikacji URL. Wystarczy wejść na stronę http://www.stormshield.pl/pl/Dodaj_adres_URL.html. Z kolei dla klasyfikacji podstawowej i chmurowej można to zrobić na portalu https://mystormshield.eu/ w sekcji *Technical Support > Report an Netasq / Stormshield URL* lub Report an Extended Web Control URL – odpowiednio dla każdej z klasyfikacji. Po podaniu adresu URL należy zaproponować kategorie, do których strona powinna przynależeć. Po zweryfikowaniu poprawności zaproponowanej klasyfikacji strona zostanie dodana do właściwej klasyfikacji.

Strona blokowania

Strona blokowania jest stroną zdefiniowana w języku html. Będzie się ona pojawiała użytkownikom próbującym wejść na stronę, do której nie mają dostępu.



Dostęp do tej strony został zablokowany zgodnie z polityką filtrowania dostępu do stron.

Użytkownik: kowalski Strona www: hide.me/pl/proxy Kategoria: Anonymizers

Jeśli uważasz, ze klasyfikacja jest niepoprawna kliknij na link : Wyślij żądanie dostępu do strony

112

NEXT GENERATION FIREWALL

PODRĘCZNIK UŻYTKOWNIKA





Dużą zaletą stosowania strony blokowania jest możliwość zdefiniowania własnego komunikatu, dzięki któremu użytkownik dowie się o powodzie blokady oraz uzyska informację o tym jak zgłosić stronę do odblokowania.

Modyfikację strony blokowania można wykonać w KONFIGURACJA > ADMINISTRACJA > Komunikaty proxy > Strona blokowania http proxy.

ANTYW	IRUS STRON	A BLOKOWANI	A HTTP PROXY			
BLOCK	PAGE_00 BLC	CKPAGE_01	BLOCKPAGE_02	BLOCKPAGE_03		
🖉 Edytuj	•					
		De	ostęp do tej strony	został zablokowany zgodnie z polityką filtrowania dostępu do stron.		
		De	ostęp do tej strony	został zablokowany zgodnie z polityką filtrowania dostępu do stron. Użytkownik: Suser Strona wywy: SkostSurl		
		D	ostęp do tej strony	został zablokowany zgodnie z polityką filtrowania dostępu do stron. Użytkownik: Suser Strona www: ShostSurl Kategoria: Surl_group		
PROSTY	<u>(EDYTOR</u> ED	De	ostęp do tej strony	został zablokowany zgodnie z polityką filtrowania dostępu do stron. Użytkownik: S <i>user</i> Strona www: ShostSurl Kategoria: Surl_group		
PROST	<mark>∕EDYTOR</mark> ED × Usuń ★ Zr	De PYTOR HTML mień obrazek U	ostęp do tej strony Istaw domyślną wersję	został zablokowany zgodnie z polityką filtrowania dostępu do stron. Użytkownik: Suser Strona www: ShostSurl Kategoria: Surl_group		
PROST Dodaj Versja jęz	Y EDYTOR EL X Usuń ↓ 2 Zr Tytuł strony	De PYTOR HTML mień obrazek U T	ostęp do tej strony Jstaw domyślną wersję reść blokady	został zablokowany zgodnie z polityką filtrowania dostępu do stron. Użytkownik: Suser Strona www: ShostSurl Kategoria: Surl_group	Adres kontaktowy	
PROST Dodaj Versja jęz n	Y EDYTOR EL X Usuń ↓ Zr Tytuł strony Blocked URL	De PYTOR HTML mień obrazek U A	ostęp do tej strony Jstaw domyślną wersję reść blokady uccess to this website is	został zablokowany zgodnie z polityką filtrowania dostępu do stron. Użytkownik: Suser Strona www: ShostSurl Kategoria: Surl_group	Adres kontaktowy	Edytuj
PROST Dodaj Versja jęz n	✓ EDYTOR EL × Usuń ≥ Zr Tytuł strony Blocked URL URL bloquée	De PYTOR HTML mień obrazek U A C	ostęp do tej strony Jstaw domyślną wersję Treść blokady uccess to this website is accès à ce site web a é	został zablokowany zgodnie z polityką filtrowania dostępu do stron. Użytkownik: Suser Strona www: ShostSurl Kategoria: Surl_group zzykową pl v robidden in accordance with the internet access policy of your company. by otpo-dobu company. company. by otpo-dobu company. by otpo-d	Adres kontaktowy	<u>Edytuj</u>







15. Konfiguracja serwera DHCP

Serwer DHCP służy do przydzielania adresów IP komputerom w sieci LAN. Konfiguracji DHCP można dokonać w zakładce **KONFIGURACJA > KONFIGURACJA SIECI > Serwer DHCP**.

Uwaga

W domyślnej konfiguracji STORMSHIELD UTM usługa serwera DHCP jest włączona. W przypadku posiadania drugiego serwera DHCP (uruchomionego w tej samej sieci) może to spowodować konflikt w sieci i doprowadzić do jej niestabilnego działania.

W pierwszej kolejności należy skonfigurować to jak STORMSHIELD UTM będzie działał – czy jako **DHCP SERWER**, czy też ma być jedynie przekaźnikiem (**DHCP RELAY**) dla zapytań DHCP do innego serwera DHCP w sieci.

KC Szukaj Szukaj KC KC Int Ro Ro	ODUŁY – I * STAWIENIA SYSTEMOWE DNFIGURACJA SIECI terfejsy terfejsy wirtualne puting	Ogólne WŁĄCZ		(Tryb [
Szukaj Szukaj Szukaj KO Int Ro Ro	STAWIENIA SYSTEMOWE DNFIGURACJA SIECI terfejsy terfejsy wirtualne puting	Ogóine WŁĄCZ		(Tryb [HCP SERWER		
바 US • KC Int Ro Ro	STAWIENIA SYSTEMOWE DNFIGURACJA SIECI terfejsy terfejsy wirtualne puting	WŁĄCZ		(Tryb [HCP SERWER		
KC Int Int Ro Ro	DNFIGURACJA SIECI terfejsy terfejsy wirtualne puting			(Tryb I	HCP SERWER		
Int Int Ro Ro	terfejsy terfejsy wirtualne puting					HOI DERMER		
Int Ro Ro	terfejsy wirtualne buting			C) Tryb (HCP RELAY		
Ro Ro	puting							
Ro		Ustawienia						
	outing multicast							
Dy	ynamiczny DNS	Nazwa domeny:			storms	ield.local		
Se	erwer DHCP	Domysina brama głown	Domyślna brama główna:		Firewall_in			
Pr	oxy DNS	Alternatywny serwer DN	s. Is:		one one			
S OE	BIEKTY	Attended with server bit			one.one			
💄 UŻ	ŻYTKOWNICY							
-∯ РО	DLITYKI OCHRONY	ZAKRES ADRESÓW						
🕅 ко	ONTROLA APLIKACJI	Wyszukiwanie		+ Dodaj	× Us	uń		
D PC	DŁĄCZENIA VPN	Zakres	Brama	3		Preferowany serwer DNS	Alternatywny serwer D	Nazwa domeny
🗓 AD	DMINISTRACJA	zakres-dhcp	Firewa	ll_in		Firewall_in	one.one.one	Nazwa domeny

W trybie pracy DHCP SERWER możemy skonfigurować odpowiednie parametry pracy usługi tj.:

- **Domyślna brama główna** domyślna brama dostępu do Internetu dla hostów sieci LAN. Obiekt ten powinien być wewnętrznym adresem IP STORMSHIELD UTM;
- Preferowany, Alternatywny serwer DNS podstawowy i zapasowy serwer DNS;
- ZAKRES ADRESÓW wskazujemy, z jakiego zakresu serwer DHCP będzie przydzielał dynamiczne adresy IP. Jeśli STORMSHIELD UTM obsługuje wiele podsieci, dla każdej z nich można utworzyć odpowiedni zakres adresów IP, w kolumnie **Brama** należy wtedy wskazać właściwy dla tej podsieci obiekt reprezentujący adres bramy domyślnej oraz odpowiednie serwery DNS;





- KONFIGURACJA STATYCZNYCH REZERWACJI DHCP pozwala skonfigurować usługę serwera DHCP w taki sposób, aby komputer, o konkretnym adresie MAC mógł otrzymać zawsze ten sam adres IP. Aby to uzyskać muszą być spełnione następujące warunki:
 - Komputer musi być reprezentowany przez obiekt typu Host zawierający adres IP oraz adres MAC.
 - Adres IP tego komputera nie może należeć do zakresu adresów rozgłaszanych przez serwer DHCP (czyli tych zdefiniowanych w ramach ZAKRESU ADRESÓW).

Tryb **DHCP RELAY** służy do przekazywania zapytań DHCP do istniejącego w sieci, innego serwera DHCP. Polega to na tym, że STORMSHIELD UTM nasłuchuje zapytań DHCP na wszystkich lub na wskazanych w sekcji **INTERFEJSY DLA DHCP RELAY** interfejsach sieciowych i jeżeli natrafi na zapytanie o adres IP, to przekazuje je do serwera określonego w polu **Serwer DHCP RELAY**.

*	- «		Нор	
ф	MODUŁY –	KUNFIGURACJA SIECI / SERWER DI	nce	
Sz	ukaj 🧩 🖉	Ogólne		
	USTAWIENIA SYSTEMOWE	WŁĄCZ		
	KONFIGURACJA SIECI		O Tryb DHCP SERWER	
	Interfejsy		Tryb DHCP RELAY	
	Interfejsy wirtualne			
	Routing	Hetawienia		
	Routing multicast	Ustawienia		
	Dynamiczny DNS	Serwer DHCP RELAY:	DHCP-svr	▼ 8
	Serwer DHCP	Adres IP używany przez DHCP Relay dla IPSec:	automatyczny	▼ 8
	Proxy DNS		Wymuś nasłuchiwanie na wszystkich interfejsach	
9	OBIEKTY			
•	UŻYTKOWNICY			
⇒ŀ	POLITYKI OCHRONY	INTERFEJSY DLA DHCP RELAY		
Ø	KONTROLA APLIKACJI	+ Dodaj × Usuń		
•	POŁĄCZENIA VPN	Interfejsy		
[]	ADMINISTRACJA	n		

🕖 Wskazówka

Informację o aktualnych dzierżawach adresów IP przez hosty można uzyskać w zakładce **MONITORING > MONITOROWNIE> DHCP**.

115

NEXT GENERATION FIREWALL

PODRĘCZNIK UŻYTKOWNIKA





16. Klaster wysokiej dostępności (HA)

Klaster HA są to dwa połączone ze sobą urządzenia STORMSHIELD UTM w celu zapewnienia ciągłości pracy sieci w przypadku awarii jednego z tych urządzeń. Klaster w rozwiązaniach STORMSHIELD jest klastrem typu **Active/Passive** co oznacza, że całość ruchu jest filtrowana przez jedno urządzenie (Active) podczas gdy drugie (Passive) jest gotowe do przejęcia ruchu w przypadku wykrycia niedostępności pierwszego lub obniżenia jego sprawności działania (zmniejszonej ilości aktywnych interfejsów sieciowych).

Aby podłączyć dwa urządzenia w klaster wymagane jest wygenerowanie na każdym z nich odpowiedniej licencji, tj. licencji typu **Master/Slave**. Można sprawdzić czy urządzenia mają licencje Master lub Slave logując się do portalu https://mystormshield.eu. Poniżej przykład takiej licencji:

			Legal terms	Terms of Use and	Services -	My profile	Log out	CONTACT & ASSIS
ORDER	×	DASH	BOARD REPO	RT AN APPLICATION	EXTENDED	WEB CONTROL	PRODUCT D	ETAILS 🖲
Create a new order List of drafts Orders in progress Realized orders list Serial number database			Serial number:	VMSNSXXC00XXX9				
DEAL REGISTRATION Register a new Deal Deal List			Details Registrati Custom	on date : 2015-05-06 er code : DAGMA	Express Warr Customer n	ranty:- name:DAGMAspzo.o		HA State : Master
User Guide RMA Details Product Details			License End	of update : 2020-07-04 Antispam : 2020-07-04	Antiviru Antispam VA	s ClamAV : 2020-07-04 DERETRO : 2020-07-04	Antivirus	s Kaspersky : 2020-07-04 Pattern ASQ : 2020-07-04
PRODUCT Product management Register a product			UR Externa	L Filtering : 2020-07-04 Il Storage : Yes Industrial : 2020-07-04	OPTENET URI	L Filtering : 2020-07-04 SSL Level : null	Vulnerab Bre	ily Manager : 2020-07-04 each Fighter : 2020-07-04
End of life DOWNLOADS							Get	Details Generate PDF

W celu skonfigurowania klastra HA należy na urządzeniu Master wejść na zakładkę **USTAWIENIA SYSTEMOWE** > Klaster HA i wybrać opcję **Utwórz klaster**. W kolejnym kroku należy wybrać interfejs sieciowy, który będzie używany do komunikacji pomiędzy urządzeniami (m.in. tzw. heartbeat) oraz skonfigurować adresację sieciową dla tego interfejsu.

Urządzenia w klastrze HA mogą komunikować się wykorzystując jeden lub dwa interfejsy sieciowe. W celu uniknięcia problemów z połączeniem zalecane jest łączenie urządzeń bezpośrednio bez użycia przełączników czy innych urządzeń sieciowych mogących powodować opóźnienia w komunikacji.

\rm Uwaga

Ponieważ klastra HA nie można wyłączyć z poziomu interfejsu urządzenia i aby wyłączyć działanie HA należy zrestartować urządzenia do ustawień fabrycznych bądź odtworzyć backup konfiguracji, który nie zawiera informacji o konfiguracji HA – zachęcamy do wykonania backupu konfiguracji obu urządzeń przed połączeniem ich w klaster HA.





★- 《 料 UST	AWIENIA SYSTEMOWE / KREATOR: KLASTER HA	
MODULY -		
Szukaj x x	RUJ INTERFEJSY SIECIOWE DO KOMUNIKACJI POMIĘDZ	T URZĄDZENIAMI - KRUK Z Z 4
밖 USTAWIENIA SYSTEMOWE		
Konfiguracja urządzenia		
Administratorzy		
Licencje		
System		komunikacja pomiędzy urządzeniami w klastrze. Obydwa urządzenia w klastrze muszą używać tych samych, wewnętrznych interfejsów.
Aktualizacje	and the second s	
Klaster HA	Interfejs główny HA	
Management Center	Interfejs główny :	dmz4 ¥
Wiersz poleceń	Nazwa interfejsu :	HA1
KONFIGURACJA SIECI	Adres IP oraz maska :	172.31.255.1/30
S OBIEKTY	Połaczenie zapasowe (opcionalnie)	
		☑ Interfeis zapasowy HA
POLITYKI OCHRONY	Interfejs zapasowy :	dmz3 ¥
KONTROLA APLIKACJI	Nazwa interfejsu :	HA2
DOŁĄCZENIA VPN	Adres IP :	172.31.255.5/30
m		

W kolejnym oknie kreatora należy skonfigurować hasło, które będzie używane do autoryzacji urządzeń i w razie potrzeby włączyć szyfrowanie komunikacji pomiędzy urządzeniami.

*- «	
MODUŁY –	THE USTAWIENIA STSTEMOWE / KREATOR, KLASTER HA
Szukaj 🧩 💒	HASŁO KLASTRA - KROK 3 Z 4
뷰 USTAWIENIA SYSTEMOWE	
Konfiguracja urządzenia	
Administratorzy	
Licencje	
System	
Aktualizacje	
Klaster HA	
Management Center	
Wiersz poleceń	Hasło używane przez urządzenie UTM do tworzenia lub dołączenia do klastra
KONFIGURACJA SIECI	Hasto:
S OBIEKTY	Sila hada: Barito Sila
LŻYTKOWNICY	Komunikacia nomiedzy urządzeniami w klastrze
POLITYKI OCHRONY	Szyfrui komunikacie pomiedzy urządzeniami.
KONTROLA APLIKACJI	
DOŁĄCZENIA VPN	
m	1

Ostatni krok kreatora kończy się przejściem urządzenia w tryb Master i oczekiwania na urządzenie Slave.

🚺 Uwaga

Domyślnie komunikacja pomiędzy urządzeniami w klastrze jest nie szyfrowana. Powodem tego jest fakt, że jest to dedykowane, bezpośrednie połączenie między urządzeniami działającymi w klastrze HA. Włączenie opcji szyfrowania połączenia HA może obniżyć wydajność klastra HA.





Na urządzeniu Slave należy w oknie kreatora konfiguracji HA wybrać opcję **Dołącz do klastra** a następnie skonfigurować interfejs do połączenia urządzeń. W kolejnym oknie kreatora należy wskazać adres IP urządzenia Master,



a następnie podać hasło do zabezpieczenia komunikacji (to samo, które zostało zdefiniowane na urządzeniu Master).

*	- «
¢	MODUŁY -
Sz	ukaj 🧩 🖉
抖	USTAWIENIA SYSTEMOWE
	Konfiguracja urządzenia
	Administratorzy
	Licencje
	System
	Aktualizacje
	Klaster HA
	Management Center
	Wiersz poleceń
	KONFIGURACJA SIECI
	OBIEKTY
•	UŻYTKOWNICY
⇒₽	POLITYKI OCHRONY
Ø	KONTROLA APLIKACJI
_	

Zakończenie pracy kreatora spowoduje restart urządzenia Slave i dołączenie go do klastra HA.









Synchronizacja konfiguracji możliwa jest poprzez użycie przycisku 146 - **Synchronizuj urządzenie pasywne z bieżącą konfiguracją** dostępnego w górnym menu interfejsu administracyjnego lub podczas wylogowania z urządzenia, dlatego niezalecane jest kończenie pracy z interfejsem administracyjnym bez poprawnego wylogowania z GUI.

Uwaga

Po każdej zmianie w konfiguracji urządzenia Master należy pamiętać o tym aby zsynchronizować klaster HA poprzez kliknięcie na powyższej ikonie synchronizacji. Urządzenia nie wykonują tej czynności automatycznie z powodów bezpieczeństwa (gdyby administrator pomylił się w konfiguracji urządzenia Master, co spowodowałoby awarię sieci bądź niedostępność usług i synchronizacja odbywała się automatycznie, to ta pomyłka zostałaby powielona na urządzeniu Slave).

Jeśli klaster działa poprawnie to stosowna informacja wyświetlona będzie w Panelu kontrolnym,

*- 0			
PANEL KONTROLNY	PANEL KUNTRULINT		
📓 KONFIGURACJA LOGÓW H	SIEĆ		OCHRONA
I RAPORTY			Data Wiadomość Akcja Priorytet I Żródło Cel
	0 0	3 4 5 6 7 8 9 10 11 12	Additional data at end of reply (cel: c.cwip.eset.com) (1)
Szukaj			⊕ 🌋 HA: Mode change : Switching to mode Active, reason: Only firewall online (1)
Sprzet / Klaster H&			🗄 🗯 HA: Mode change : Switching to mode Passive, reason: Quality difference (local firewall: 10% ; SN510A5988
Dustase	WŁAŚCIWOŚCI		E 1 HA: Deer lost - Erewall SN5104598827247 doesn't reply to requests anymore (was None). Starting (CMP my
System	Nazwa:	SN510A59B8273A7	
Interfejsy	Model:	SN510	🗄 🇯 HA: Peer lost : Firewall SN510A59B8272A7 doesn't reply to requests anymore (was Passive). Starting ICMP
QoS	Numer seryjny:	SN510A59B8273A7	HA: Peer lost : Unexpected loss of firewall SN510A5988272A7 (was None) - no ICMP reply (8:68/S:80) (1)
	Wersja:	4.0.1	
Hosty	Partycja zapasowa:	3.9.2 (12.02.2020)	HA: Peer lost SN510A59B8272A7 (cel: 0.0.0.0) (4)
Użytkownicy	Czas pracy:	45m 40s	Problem reported on passive Node admin password; Admin password is set to factory default! (1)
Połaczenia	Data:	12.02.2020 12:30:15	
. enferenne	Data wygaśnięcia serwisu:	31.12.2020	⊞ Tink local' addresses (RFC 3330) (cel: 224.0.0.22) (2)
Bramy	Data wygaśnięcia serwisu (partr	er 31.12.2020	Connection terminated for webadmin (timeout) (1)
DHCP	HA):		⊕ DNS : suspicious overly long query (cel: dns1.google.com) (1)
Tunele SSI VPN			· · · · · · · · · · · · · · · · · · ·
			STAN UDZADZENIA
Tunele IPSec VPN			
Białe / czarne listy			

Po kliknięciu ikony LINK HA zostanie otwarta strona z podsumowaniem stanu klastra HA.









*	•	«
Ch	PANEL KONTROLNY	
	KONFIGURACJA LOGÓW	+
al	RAPORTY	+
	MONITOROWANIE	-
Szu	Jkaj	
	Sprzęt / Klaster HA	
	System	
	Interfejsy	
	QoS	
	Hosty	
	Użytkownicy	
	D ()	

MONITOR / SPRZĘT / KLASTER HA

SPRZET SZCZEGÓŁY KLASTRA HA

Wskaźnik	Lokalny firewall	Zdalny firewall
🗆 Ustawienia		
Status	Active	Passive
Wersja	4.0.1	4.0.1
Stan wymuszony	No	No
Indeks jakości	2 0	٥
Priorytet		
Synchronizacja konfiguracji	 Zsynchronizowane 	 Zsynchronizowane
Stan łącza HA	🗢 ок	🖉 ок
Stan zapasowego łącza HA	< ок	🖉 ок
🕀 Ustawienia zaawansowane		







17. Wsparcie dla protokołu IPv6

Wszystkie urządzenia z serii STORMSHIELD UTM wspierają natywnie protokół IPv6, jednak opcja ta jest domyślnie wyłączona.

Aby aktywować tą funkcjonalność należy w menu **KONFIGURACJA > USTAWIENIA SYSTEMOWE > Konfiguracja urządzenia > Ustawienia sieciowe** wcisnąć przycisk **Włącz** w sekcji Wsparcie dla IPv6.

*-	*	持 USTAWIENIA SYSTEMOWE / KONFIGURACJA URZĄDZENIA
MODUŁY	-	
	1 ⁴ 2 ⁸	USTAWIENIA OGÓLNE DOSTEP ADMINISTRACYJNY USTAWIENIA SIECIOWE
# USTAWIENIA SYSTEM	OWE	Wsparcie dla IPv6
Konfiguracja urządzeni	a	WŁĄCZ
Administratorzy		
Licencje		WŁĄCZ IPV6
System		A Przed włączeniem wsparcia dla IPv6 konfiguracja będzie zapisana i dostępna do pobrania
Aktualizacje		
Klaster HA		NIE WŁĄCZAJ IPV6 ZAPISZ KONFIGURACJĘ I WŁĄCZ IPV6
Management Center		

Aktywacja obsługi IPv6 spowoduje automatyczne zapisanie i wyeksportowanie obecnej konfiguracji dla IPv4, po czym nastąpi ponowne uruchomienie urządzenia.

Konfiguracja urządzenia nie ulegnie zmianie, wszystkie wcześniej zdefiniowane moduły będą działały w taki sam sposób jak przed aktywacją, natomiast pojawią się nowe opcje konfiguracyjne m.in.:

🚺 Uwaga

Po włączeniu obsługi protokołu IPv6 nie można jej wyłączyć w inny sposób niż przez przewrócenie ustawień fabrycznych bądź wczytanie backupu konfiguracji urządzenia wykonanego przed włączeniem obsługi protokołu IPv6.





Konfiguracja interfejsów sieciowych IPv6

Po włączeniu obsługi protokołu IPv6 w trybie edycji interfejsu (zakładka **Ogólne**) pojawi się sekcja **Adres IPv6**, gdzie będzie możliwość skonfigurowania adresu IPv6.

ukaj 🚽 🖉	Q Wprowadż filtr	* * O 4	Edycja 🔹 🕂 Dodaj 👻 Vsuń 🛛 🖓 Mo	nitor 🖏 Przejdź do monitoringu	Sprawdź
	Inter	fejs	KONFIGURACJA IN		
USTAWIENIA SYSTEMOWE	m out	- •	OGÓLNE KONFIGURACJA ROUTINGU	ZAAWANSOWANE	
KONFIGURACJA SIECI	in 🗖	*1 🖉	Zakres adresów		
Interfejsy	m dmz?			_	_
Interfejsy wirtualne	m dmz3		Zakres adresów:	 Zakres adresów odziedziczony z bridge 	 Oynamiczny / Statyczny
Routing	🖱 dmz4		Adres IPv4:	O Pobierz adres z DHCP	Sonfiguracja statyczna
Routing multicast	n dmz5		🕂 Dodaj 🗙 Usuń		
Dynamiczny DNS	m dmz6		Adres/ Maska	Opis	
Serwer DHCP			10.11.11.2/255.255.255.0		
Proxy DNS					
OBIEKTY					
UŻYTKOWNICY			Adres IPv6:	O Pobierz adres z DHCP	Konfiguracja statyczna
POLITYKI OCHRONY			+ Dodaj 🗙 Usuń		
KONTROLA APLIKACJI			Adres/ Maska	Opis	
POŁĄCZENIA VPN			FC80::1/64		

Dodatkowo pojawi się nowa zakładka **Konfiguracja routingu**, której opcje są odpowiedzialne za informowanie innych hostów w sieci IPv6 o obecności urządzenia co ułatwia lokalną komunikację.

	« -	💼 KONFIGURACJA SIE	CI / INTERFEJSY				
Szukaj	11	Q Wprowadź filtr	* 2 C 2	Edycja 👻 🕂	🕂 Dodaj 👻 🗙 Usuń 🔀 Monitor 🛛 🖓 Przejdź	do monitoringu 👁 Sprawdź	
		Interfejs		🏠 KONFIGU	JRACJA IN		
뷰 USTAWIE	ENIA SYSTEMOWE	m out		OGÔL NE		ANE	
KONFIGU	JRACJA SIECI	🖳 in	📲 🛃	OUDENL			
		🗂 dmz1		Ustawienia	a automatycznej konfiguracji		
Interrejsy	/	m dmz2	ootaniona aatonatyozhoj konigaraoji				
Interfejsy	/ wirtualne	🖱 dmz3			Wykrywanie au	utomatyczne	
Routing		🗂 dmz4			O Wyślij RA		
Routing multicast		🖱 dmz5			○ Wyłącz		
		👘 dmz6					

Pozostała konfiguracja związana z IPv6 jest rozsiana po całym urządzeniu m.in. w sekcjach:

- routing,
- serwer DHCP,
- konfiguracja obiektów,
- reguły filtrowania firewall,
- IPsec.





18. MONITOROWANIE

Urządzenie STORMSHIELD UTM umożliwia monitorowanie pracy urządzenia oraz stanu sieci z poziomu WebGUI.



Z poziomu menu **MONITORING > MONITOROWANIE** mamy dostęp do szeregu informacji na temat bieżącej pracy urządzenia takich jak:

- Sprzęt / Klaster HA temperatura urządzenia oraz stan klastra HA;
- **System** obciążenie procesora i pamięci RAM urządzenia, Uptime urządzenia, Uptime i obciążenie poszczególnych usług, stan aktualizacji poszczególnych modułów urządzenia;
- Interfejsy użyte pasmo oraz ilość połączeń na poszczególnych interfejsach. Włączenie monitoringu na danym interfejsie można wykonać w KONFIGURACJA > ADMINISTRACJA > Konfiguracja monitoringu > Konfiguracja interfejsu;
- QoS użyte pasmo poszczególnych kolejek QoS. Włączenie monitoringu kolejki QoS można wykonać w KONFIGURACJA > ADMINISTRACJA > Konfiguracja monitoringu > Konfiguracja QoS.
- Hosty aktywne hosty, których połączenia przychodzą do lub przez urządzenie STORMSHIELD UTM, ich reputacja, użyte pasmo, ilość wysłanych/odebranych danych, geolokalizacja, reputacja IP, wszystkie połączenia danego wybranego hosta, podatności, aplikacje i usługi wykryte na hoście, a także dodatkowe informacje o hoście i historia jego reputacji.

Po kliknięciu prawym przyciskiem myszy na nazwie wybranego hosta pojawi się menu kontekstowe umożliwiające dodatkowe działania takie jak:

- Wyszukaj frazę we wszystkich logach wyszukuje wpisy dotyczące wybranego hosta w logach;
- Sprawdź hosta wskazuje pozycje konfiguracji, w których użyty jest wskazany host;
- Pokaż szczegóły hosta szczegółowe informacje o hoście;





- Umieść na czarnej liście (1, 5, 30 minut, 3 godziny) blokuje komunikację hosta na wskazany czas;
- Skopiuj wybrany wiersz do schowka;
- **Dodaj nowy host a następnie dodaj go do grupy** umożliwia utworzenie obiektu typu host o adresie IP oraz MAC wybranego hosta oraz dodanie go do Grupy IP;
- Użytkownicy informacje o zautentykowanych użytkownikach, adresach IP stacji, na których użytkownik się zautentykował, bazie użytkowników, grupie, dacie wygaśnięcia autentykacji, metodzie uwierzytelnienia, przynależności do grupy administratorów urządzenia Stormshield, uprawnieniach dostępu do usług VPN, wszystkich połączeniach zainicjowanych przez użytkownika oraz podatnościach, aplikacjach usługach i informacjach dotyczących hostów, na których dany użytkownik jest zalogowany.

Podobnie jak w przypadku hostów także tutaj dostępne jest menu kontekstowe z dodatkowymi opcjami dotyczącymi użytkowników;

- **Połączenia** informacje o wszystkich trwających połączeniach przechodzących przez urządzenie;
- **Bramy** monitoring routerów użytych w konfiguracji routingu urządzenia STORMSHIELD UTM takich jak: obiekty typu router, brama domyślna, bramy użyte w routingu na podstawie reguł (PBR) i trasy powrotne;
- DHCP lista hostów, które uzyskały adres IP z lokalnego serwera DHCP;
- **Tunele SSL VPN** lista hostów, które zestawiły połączenie z urządzeniem STORMSHIELD UTM poprzez tunel SSL VPN;
- Tunele IPsec VPN lista tuneli VPN w aktywnej polityce IPsec VPN. W sekcji Polityki widoczny jest stan poszczególnych tuneli (zestawiony lub nie), informacje o sieci i bramie zdalnej oraz lokalnej. W sekcji Tunele dostępne są bardziej szczegółowe informacje o zestawionych tunelach m.in. ilość przesłanych danych, czas życia tunelu, oraz użyte algorytmy szyfrowania i autentykacji;
- Białe / czarne listy lista hostów, które trafiły na białe lub czarne listy urządzenia. Jeśli host np. błędnie trafił na czarną listę, można po wskazaniu takiego hosta usunąć go z tej listy klikając przycisk Usuń element z czarnej listy.





19. LOGI

Logowanie zdarzeń

Wszystkie urządzenia STORMSHIELD UTM wyposażone w nośnik danych umożliwiają zapisywanie zdarzeń związanych z ruchem sieciowym oraz z pracą samego urządzenia. Urządzenia posiadające wbudowany dysk twardy tj. SNi40, SN510 oraz wszystkie wyższe modele są w stanie przechowywać logi bezpośrednio w pamięci urządzenia. W przypadku mniejszych modeli tj. SN160(W), SN210(W) i SN310 możliwa jest instalacja karty SD (co najmniej Class 10, UHS Class 1 (U1) lub App Performance 1 (A1) – SDHC lub SDXC) o maksymalnej pojemności 2TB. Producent rekomenduje użycie kart o wysokiej wytrzymałości / przemysłowych lub najlepiej tych, które mają wbudowany układ flash MLC opracowany przez wiodące marki (np. SanDisk, Western Digital, Innodisk, Transcend, itp.).

Domyślnie wszystkie logi są zapisywane, jednak w sekcji KONFIGURACJA > ADMINISTRACJA > Logi – Syslog – IPFIX > Logi na dysku można wyłączyć niektóre kategorie bądź zmniejszyć procentową rezerwację miejsca na poszczególne dzienniki na dysku (kolumna %).

*-	«							
•	MODUŁY –		(ACJA / LOGI - SYSLO	G-IPFIX				
Szuk	(aj 💉 🖉	LOGI NA DYSKI	J SYSLOG IPFIX	(
+†‡ (USTAWIENIA SYSTEMOWE	WŁĄCZ						
-i- i	KONFIGURACJA SIECI	Pamięć —						
8 (OBIEKTY	Urządzenie:		Dysk twardy 4	GiB	•	C Odśwież	🗳 Sformatuj
. (UŻYTKOWNICY							
-\$ ₽	POLITYKI OCHRONY				u opós			
1	KONTROLA APLIKACJI	When we we the	Wukaz wazyatkia	DEGU Z TYPUW	LOGOV	v		
(1)		Włącz wszystkie Właczony	Typ logów (nazwa pliku)	%		Rozmiar		
m		włączona	Zarządzanie (I_server)	2		81.9 MiB		
,	ADMINISTRACJA	🔍 włączona	Uwierzytelanianie (l_auth)	2		81.9 MiB		
	Logi - Syslog - IPFIX	💽 włączona	Połączenia (l_conn)	2	5	1 GiB		
\$	SNMP	💽 włączona	Dzienniki systemowe (l_s)	ystem) 1		41 MiB		
I	Powiadomienia	🔍 włączona	Alarmy (l_alarm)	1	5	614.4 MiB		
	Alarmy systemowe	🔍 włączona	Klasyfikacja URL (l_web)	1	0	409.6 MiB		
	Komunikaty proxy	💽 włączona	Analiza protokołów (l_plug	gin) 1	5	614.4 MiB		
		💽 włączona	SMTP Proxy (l_smtp)	4		163.8 MiB		
1	Kontiguracja raportow	💽 włączona	Firewall (I_filter)	8		327.7 MiB		
1	Konfiguracja monitoringu	🜑 włączona	IPSec VPN (l_vpn)	2		81.9 MiB		
		🔍 włączona	SSL VPN (l_xvpn)	2		81.9 MiB		
		🔍 włączona	POP3 Proxy (l_pop3)	3		122.9 MiB		
		🔍 włączona	Statystyki (l_monitor)	1		41 MiB		
		💽 włączona	Audyt podatności (l_pvm)	2		81.9 MiB		
		 włączona 	FTP Proxy (l_ftp)	4		163.8 MiB		
		💽 włączona	SSL proxy (l_ssl)	3		122.9 MiB		
		 włączona 	Sandboxing	1		41 MiB		
				Całkowita wy	korzysta	na ilość miejsca nie przekr	acza przydzieloneg	o miejsca na dysku (użyto 100%)

Możliwa jest także konfiguracja do 4 zewnętrznych serwerów syslog (zakładka **Syslog**), na które będą wysyłane logi.

125





*	~ «	ADMINISTRACIA / LOGI - SYSLO	G - IPEIX	
•	MODUŁY –			
Sz	ukaj 🧩 🖉	LOGI NA DYSKU SYSLOG IPFI	K	
<u>+</u> †+	USTAWIENIA SYSTEMOWE	PROFIL SYSLOG	Szczegóły	
	KONFIGURACJA SIECI	Stan Nazwa		
		💽 włączona Syslog	Nazwa:	Syslog
	OBIEKTY	🗇 wyłączona 🛛 Syslog Profile 1	Komentarz:	
-	UŻYTKOWNICY	🔿 wyłączona 🛛 Syslog Profile 2	Serwer syslog:	SYSLOG-svr 💌 🛼
≁ŀ	POLITYKI OCHRONY	🔿 wyłączona 🛛 Syslog Profile 3	Protokół:	TCP 💌
$\overline{\mathcal{O}}$	KONTROLA APLIKACJI		Port:	syslog-conn 💌 🕏
C 10	POŁĄCZENIA VPN		CA:	- ×
	ADMINISTRACJA		Certyfikat serwera:	X
	Logi - Syslog - IPFIX		Certyfikat klienta:	- ×
	SNMP		Format:	RFC5424 -
	Powiadomienia		Zaawansowane	
	Alarmy systemowe			

Przeglądanie logów

Logi gromadzone na urządzeniu dostępne są w **MONITORING > LOGI**. To menu dostępne jest jedynie na urządzeniach wyposażonych w nośnik danych. Można tu przeglądać logi gromadzone na urządzeniu grupowane w dziennikach takich jak: Ruch sieciowy, Alarmy, Web, Podatności, E-Mails, VPN, Zdarzenia systemowe, Firewall, Sandboxing, Użytkownicy.

★ - «	LOG / RUCH	ISIECIOWY								
🗎 KONFIGURACJA LOGÓW -	Ostatnia godzina	- 💼	C Odśwież Szukaj				» Zaa	wansowane wyszukiwanie		\equiv Czynność 🔹
Szukai	SZUKAJ OD - 18.	SZUKAJ OD - 18.02.2020 11:58:57 - D0 - 18.02.2020 12:58:57 SZUKAJ OD - 18.02.2020 12:57 SZUKAJ OD - 18.02.2020 12:57 SZUKAJ OD - 19.02 SZUKAJ OD - 18.02.2020 12:57 SZUKAJ OD - 18.02.2020 12:57 SZUKAJ OD - 18.02.2020 12:57 SZUKAJ OD - 18.02.2020 12:57 SZUKAJ OD - 18.02.2020 12:57 SZUKAJ OD - 18.02.2020 12:57 SZUKAJ OD - 18.02.2020 12:57 SZUKAJ OD - 18.02.2020 12:57 SZUKAJ OD - 18.02.2020 12:57 SZUKAJ OD - 18.02.2020 12:57 SZUKAJ OD - 18.02.2020 12:57 SZUKAJ OD - 18.02 SZUKAJ OD -						•		
	Data zapisu	Akcja	Użytkownik	Kn	Nazwa obiektu źródłowego	Kn	Nazwa obiektu do	Data		~
Wszystkie	12:58:54	🕑 Zezwól			Firewall_out		webres.4.geo.	Data zapisu	12:58:54	
Ruch sieciowy	12:58:29	Zezwól			Firewall_out		webres.1.geo.	Data i godzina rozpoczęcia	30.01.2020 18:20:43	
Alarmy	12:58:14	Zezwól			Firewall_out	1220	webres.2.geo.	Różnica czasu (różnica między G	+0100	
, and the second s	12:57:51	Zezwól			Firewall_out		webres.4.geo.	Czas trwania	2m 4s 940ms	
Web	12:57:44	Zezwól			Firewall_out	*	webres.5.geo.	Odebrano	656 b	

Po przejściu do widoku logów pojawi się tabela zawierająca poszczególne wpisy wybranego dziennika. W górnej części interfejsu można wybrać predefiniowany przedział czasu z jakiego chcemy przeglądać logi lub wskazać własny klikając ikonę **Zmień zakres czasu**.

Przycisk **Odśwież** ponownie odczytuje zapisane logi. W polu szukaj można wprowadzić dowolny ciąg znaków wg. którego urządzenie STORMSHIELD UTM ma przefiltrować listę logów – może to być np. nazwa użytkownika, nazwa lub adres obiektu źródłowego bądź docelowego, nazwa lub nr portu, itp. Po wybraniu opcji **Zaawansowane wyszukiwanie** będzie można wskazać szczegółowe kryteria wyszukiwania, a także zapisać utworzony szablonu wyszukiwania lub wskazać wcześniej przygotowany szablon.







Po prawej stronie górnego menu pod przyciskiem **Czynność** można wykonać eksport logów z bieżącego widoku do pliku CSV, wydrukować go lub skopiować do schowka.

Czynność ▼
 Rozwiń
 Eksportuj dane
 Drukuj
 Kopiuj do schowka
 Resetuj widok

W części głównej widoku logów wyświetlane są poszczególne wpisy dziennika. Domyślny widok wyświetla najbardziej niezbędne informacje. Jednak można dostosować rodzaj wyświetlanych informacji po najechaniu wskaźnikiem myszki na nagłówek dowolnej kolumny i kliknięciu na trójkąt pojawiający się w prawej części nagłówka kolumny – dzięki temu będzie można zmodyfikować liczbę wyświetlanych kolumn.

									Data i godzina rozpoczęcia
UG/RUCHS	IECIUWY								Różnica czasu (różnica między GMT a czasem lokalnym
Ostatnie 30 dni	- 💼 🤇	C Odśwież Szukaj					» z	a	🗹 Akcja
SZUKAJ OD - 19.01.	2020 14:20:42 -	DO - 18.02.2020 14:2	0:42						U Wersja protokołu IP
Data zapisu	Akcja	Użytkownik	Kri	Nazwa obiektu źródłoweg	o‴ K	in 1	Nazwa obiektu	dc	🗹 Użytkownik
🗆 Nazwa obiektu źród	lłowego : 192.168	3.43.180 (21)				Kol	umny		Domena
12:41:35	Zezwól			192.168.43.180	æ	Gru	ipuj po tym pol		🕑 Kraj źródła ruchu
12:41:35	Zezwól			192.168.43.180		Pol	każ w grupach		Kontynent adresu źródłowego
12:41:35	Zezwól			192.168.43.180		• c	loudurl5-sns.s	01	Nazwa obiektu źródłowego
12:41:35	7ezwól			192.168.43.180			loudurl2-sns.s	0	Źródło

Po kliknięciu wiersza wpisu dziennika po prawej stronie pojawi się okno zawierające pełne informacje zawarte w tym konkretnym wpisie.







Uwaga

Aby zachować zgodność z europejskim rozporządzeniem RODO (Ogólne rozporządzenie o ochronie danych), dane wrażliwe (nazwa użytkownika, źródłowy adres IP, nazwa źródła, źródłowy adres MAC) nie są wyświetlane w dziennikach i raportach i są zastąpione słowem "Anonimowy".

Aby wyświetlić te wrażliwe dane, administrator musi aktywować "*Pełny dostęp do dzienników (danych wrażliwych)*", klikając opcję **Uzyskaj prawo dostępu do wrażliwych danych (logów)** w menu rozwijanym pod nazwą zalogowanego użytkownika (górny baner interfejsu administracyjnego).







20. STORMSHIELD VISIBILITY CENTER

STORMSHIELD Visibility Center (SVC) to system zbierania, zarządzania logami i raportowania. Narzędzie jest kolejną wersją Virtual Log Appliance. Dzięki tej funkcjonalności możliwe jest zbieranie i przeglądanie logów, a także analizowanie raportów wygenerowanych na ich podstawie. Narzędzie dostępne jest w postaci maszyny wirtualnej i pozwala na równoległe zbieranie logów z wielu urządzeń. STORMSHIELD Visibility Center dostępne jest w postaci maszyny wirtualnej (do pobrania z portalu https://mystormshield.eu) kompatybilnej z platformą VMware oraz Hyper-V.

Narzędzie jest w pełni darmowe.







Administrator otrzymuje także możliwość analizy zdarzeń w sieci. Duża ilość informacji przechowywana w bazie danych umożliwia weryfikację wszystkich szczegółów komunikacji, wśród nich:

- adres źródłowy,
- adres docelowy,
- użytkownik,
- wykorzystywane porty,
- geograficzne źródła i cele komunikacji,
- a także wiele, wiele innych przydatnych informacji!

Dzięki narzędziu STORMSHIELD Visibility Center można:

- archiwizować logi z wielu urządzeń w jednym miejscu,
- przeglądać graficzne raporty na komputerze, tablecie czy smartfonie,
- szybko znaleźć potrzebne informacje wygodnie filtrując dane.







Po uruchomieniu i podstawowej konfiguracji **SVC** jest gotowe do zbierania logów, które są wysyłane przez urządzenie STORMSHIELD UTM.

Konfiguracja po stronie STORMSHIELD UTM sprowadza się do aktywowania wysyłania logów, podobnie jak w przypadku serwera syslog. Wykonuje się to w sekcji **KONFIGUACJA > ADMINISTRACJA > Logi-Syslog-IPFIX** w zakładce **Syslog**. Wystarczy podać adres IP maszyny wirtualnej SVC, a także protokół, port oraz format wysyłanych danych.

*-	«	I ADMINISTRACJA / LOGI - SYSLO	G - IPFIX	
Szu	MODUŁY – kaj "* "*	LOGI NA DYSKU SYSLOG IPFIX		
耕	USTAWIENIA SYSTEMOWE	PROFIL SYSLOG	Szczegóły	
	KONFIGURACJA SIECI	Stan Nazwa C włączona SVC	Nazwa:	SVC
00	OBIEKTY	🖸 wyłączona Syslog Profile 1	Komentarz:	Stormshield Visibility Center
*	UŻYTKOWNICY	🗘 wyłączona 🛛 Syslog Profile 2	Serwer syslog:	SVC-svr 👻 🕏
⇒₽	POLITYKI OCHRONY	🗇 wyłączona 🛛 Syslog Profile 3	Protokół:	TCP
$\overline{\oslash}$	KONTROLA APLIKACJI		Port:	syslog-conn 💌 🕏
•	POŁĄCZENIA VPN		CA:	▼ ×
[]	ADMINISTRACJA		Certyfikat serwera:	- × ×
	Logi - Syslog - IPFIX		Certyfikat klienta:	× ×
	SNMP		Format:	RFC5424 -
	Powiadomienia		- 🔻 Zaawansowane	
	Alarmy systemowe			

Uwaga!

Dla **STORMSHIELD Visibility Center** dostępna jest osobna dokumentacja, którą można pobrać ze strony www.stormshield.pl lub www.mystormshield.eu





21. RAPORTY

Menu raportów będzie dostępne tylko wtedy, gdy w konfiguracji urządzenia zostały włączone raporty statystyczne – KONFIGURACJA > ADMINISTRACJA > Konfiguracja raportów.

Moduł Raporty zawiera raporty "Top 10" w kategoriach: Web, IPS, Antywirus, Antyspam, Audyt podatności, Konfiguracja sieci, Sieć przemysłowa, Sandboxing. Dzięki temu w łatwy sposób można zweryfikować w jaki sposób wykorzystywany jest dostęp do Internetu, jakie ataki zostały zablokowane przez urządzenie STORMSHIELD UTM, a także jakie podatności występują w sieci firmowej. Wiele interaktywnych funkcji pozwala bezpośrednio z poziomu raportów dostroić konfigurację urządzenia.

*- «	III ADMINISTRACIA / KONFIGURACIA RAPORTÓW								
🍄 MODUŁY –									
Szukaj 🦼 🖉	Ogólne								
해 USTAWIENIA SYSTEMOWE	Raporty statystyczne: WŁĄCZ Historia wykresów: WŁĄCZ								
KONFIGURACJA SIECI OBIEKTY	Uwaga: Włączenie raportów może wpłynąć na wydajność urządzenia.								
POLITYKI OCHRONY	LISTA RAPORTÓW LISTA WYKRESÓW HISTORYCZNYCH								
KONTROLA APLIKACJI	Szukaj w kategorii Wszystkie 🔹 🗨 🖝 Włącz zaznaczone 🔹								
DOŁĄCZENIA VPN	Status Kategoria Opis								
ADMINISTRACJA	Włącz Antyspam Współczynnik spamu								
	Włącz Antyspam Użytkownicy otrzymujący najwięcej spamu								
Logi - Syslog - IPFIX	Włącz Antywirus Wirusy najczęściej wykrywane w wiadomościach e-mail								
SNMP	D Wyłącz Antywirus Najczęstsi nadawcy wiadomości e-mail zawierających wirusy								
Powiadomienia	CD Wyłącz Antywirus Najczęściej wykrywane wirusy na stronach www								
Alarmy systemowe	Włącz Audyt podatności Komputery z największą liczbą wykrytych zagrożeń								
	Włącz Audyt podatności Najczęściej wykrywane podatności								
Komunikaty proxy	Wyłącz Audyt podatności Najbardziej podatne serwery								
Konfiguracja raportów	CD Wyłącz Audyt podatności Najbardziej podatne aplikacje								
Konfiguracja monitoringu	Włącz IPS Współczynnik wykrywania przez silnik detekcji								
	CD Wyłącz IPS Sesje administracyjne								







0 5 10 15 20 25 30 35 40 45 50 55 60 65 70 75 80 85 90 95 105 115 125 135 145 156 165 175 185 195 205 215 225 TWBW:shumber of Hits

*-

PANEL KONTROLNY

I RAPORTY

RAPORTY WEB

KONFIGURACJA LOGÓW

Naicześciej odwiedzane st

Najczęściej odwiedzane d...

Odwiedzane kategorie URL

Strony www pod względe...

Kategorie stron www pod ...

Użytkownicy pod względe...

Najczęściej blokowane str... RAPORTY IPS

RAPORTY AUDYTU PODAT...

RAPORTY KONFIGURACJI ... RAPORTY ANTYSPAM

SANDBOXING

133





22. Najczęściej zadawane pytania (FAQ)

Jak przywrócić urządzenie do ustawień fabrycznych z poziomu CLI (command line)?

Aby przywrócić urządzenie do ustawień fabrycznych należy skorzystać z polecenia *defaultconfig*. Użycie polecenia **defaultconfig** –**f** –**r** spowoduje przywrócenie ustawień fabrycznych bez wyświetlania komunikatów o błędach i wykona restart urządzenia. Więcej o opcjach polecenia *defautlconfig* można przeczytać wywołując jego pomoc przy użyciu komendy **defaultconfig** –**h**

Gdzie znajdują się pliki konfiguracyjne na dysku urządzenia?

Pliki konfiguracyjne urządzenia znajdują się w folderze /usr/Firewall/ConfigFiles. Pliki umieszczone są bezpośrednio w tym folderze jak np. /usr/Firewall/ConfigFiles/network odpowiedzialny za konfigurację interfejsów sieciowych, lub znajdują się w podfolderach tak jak /usr/Firewall/ConfigFiles/Filter/10, który przechowuje konfigurację 10 slotu konfiguracyjnego Firewall i NAT

Skąd mogę pobrać najnowszą wersję firmware?

Najnowszą wersję można pobrać z sekcji Download po zalogowaniu się na stronie https://mystormshield.eu. Przed pobraniem plików należy wybrać swoją wersja produktu. W strefie Klienta poza najnowszymi wersjami firmware można znaleźć zasobów, między innymi najnowsze wersje klientów VPN, agenta SSO, czy dokumenty Release Note, które opisują zmiany jakie zostały wprowadzone w poszczególnych wersjach oprogramowania (zachęcamy do zapoznania się z tym dokumentem każdorazowo przed aktualizacją firmware urządzenia STORMSHIELD UTM).

Jak uruchomić dostęp przez SSH do urządzenia STORMSHIELD UTM?

Dostęp do urządzenia poprzez SSH konfiguruje się w sekcji **KONFIGURACJA > USTAWIENIA SYSTEMOWE > Konfiguracja** na zakładce *Dostęp administracyjny*. Dostęp może się odbywać z wykorzystaniem hasła (opcja niezalecana) lub z użyciem pary kluczy publiczno-prywatnych, które można pobrać w sekcji **KONFIGURACJA > USTAWIENIA SYSTEMOWE > Administratorzy** na zakładce **Konto Administratora**.

Uwaga! dostęp do urządzenia poprzez SSH jest możliwy jedynie dla głównego konta administratora (konto admin).

Co to jest TECHNICAL REPORT i jak go wygenerować?

Technical Report (Raport techniczny) jest plikiem zawierającym informacje o konfiguracji urządzenia oraz o jego bieżącym stanie. Technical Report jest jednym z podstawowych źródeł informacji używanych przez dział pomocy technicznej do diagnostyki problemów, dlatego powinien być dołączany do każdego zgłoszenia supportowego.

Aby wygenerować Technical Report należy wejść do sekcji **KONFIGURACJA > USTAWIENIA SYSTEMOWE > System,** a następnie na zakładce **Konfiguracja** wybrać przycisk **Pobierz raport**.

Uwaga! Do pobrania raportu technicznego niezbędny jest pełny dostęp do danych wrażliwych Z poziomi CLI raport można wygenerować używając komendy **sysinfo**.





Jak zmienić hasło użytkownika admin

Aby zmienić hasło użytkownika admin należy przejść do sekcji **KONFIGURACJA > USTAWIENIA SYSTEMOWE > Administratorzy** na zakładkę Konto Administratora, a następnie dwukrotnie podać nowe hasło. Z poziomu CLI hasło można zmienić korzystając z polecenia **fwpasswd**.

\rm Uwaga!

Hasło użytkownika **admin** można zmienić jedynie będąc zalogowanym jako **admin**.

Jak wygląda procedura aktualizacji firmware?

Aby zaktualizować firmware należy przejść do sekcji **KONFIGURACJA > USTAWIENIA SYSTEMOWE > System**, a następnie na zakładce **Aktualizacja systemu** należy wybrać plik z najnowszą wersją firmware pobrany uprzednio ze strony https://mystormshield.eu. Należy upewnić się, że została wybrana opcja **Kopiuj bieżącą partycję na zapasową** przed aktualizacją (dotyczy jedynie wersji sprzętowych rozwiązania). Kopia znajdująca się na partycji zapasowej pozwoli na szybki powrót do poprzedniej wersji firmware i konfiguracji w przypadku niepowodzenia procesu aktualizacji. Po wybraniu przycisku *Aktualizuj System* rozpocznie się proces aktualizacji, który trwa zazwyczaj kilka minut. Podczas aktualizacji firmware nie należy wyłączać urządzenia.

Uwaga!

Przed aktualizacją firmware zalecane jest zapoznanie się z dokumentem Release Note opisującym jakie zmiany zostały wprowadzone w nowej wersji oprogramowania.

Zapomniałem hasła dla użytkownika admin. Czy istnieje procedura restartu hasła?

Aby zresetować hasło do urządzenia należy podłączyć się do urządzenia przez port konsolowy lub za pomocą monitora i klawiatury (w zależności od modelu urządzenia STORMSHIELD UTM), a następnie zrestartować urządzenie.

Podczas procedury rozruchu pojawi się opcja wyboru, z której partycji ma startować urządzenie:

>>FW
1) Main
2) Backup
choose:

W tym momencie należy nacisnąć kilkukrotnie przycisk spacji.

Po uzyskaniu znaku zachęty loader> wpisujemy: boot -s i przyciskamy ENTER.

Po pojawieniu się komunikatu Enter full pathname of shell or RETURN for /bin/sh: należy zatwierdzić przyciskiem ENTER.

Następnie wpisujemy: /usr/Firewall/sbin/chpwd i wybieramy ENTER, po chwili ukaże się prośba o nadanie nowego hasła. Po weryfikacji poprawności wpisanego hasła nastąpi restart, który kończy procedurę resetu hasła.

Czy dla urządzeń STORMSHIELD UTM dostępny jest tzw. KNOWLEDGE BASE?

Tak, KNOWLEDGE BASE znajduje się pod adresem https://kb.stormshield.eu i dostępny jest dla każdego zarejestrowanego klienta STORMSHIELD.



STORMSHIELD