



# STORMSHIELD

## Stormshield Network Security v3.0

Nowy firmware dla urządzeń STORMSHIELD

Najnowsza wersja firmware'u dla rozwiązań STORMSHIELD (Stormshield Network Security v3.0) zawiera nowe funkcjonalności pozwalające, m.in. na integrację z wieloma bazami użytkowników, zdalne tworzenie tymczasowych użytkowników, czy filtrowanie oparte o lokalizację hosta.

### Nowy panel administracyjny

Najnowsza wersja firmware to możliwość pełnego zarządzania urządzeniem z poziomu przeglądarki internetowej. WebGUI daje możliwość administracji urządzeniem, monitorowania w czasie rzeczywistym parametrów jego pracy, takich jak obciążenie procesora, pamięci czy interfejsów. Dostarcza również informacji o zalogowanych użytkownikach i aktywnych połączeniach sieciowych. Z panelu administracyjnego dostępne są raporty i logi, które umożliwiają bezpośrednią rekonfigurację dotychczasowych polityk urządzenia.

### Integracja z wieloma bazami użytkowników

W Stormshield Network Security w wersji 3.0 pojawia się opcja uwierzytelniania użytkowników w wielu bazach Active Directory i LDAP. Dzięki integracji wielu baz LDAP urządzenia Stormshield dają możliwość tworzenia różnych reguł i polityk dostępu dla różnych użytkowników. Integracja z wieloma bazami danych daje również możliwość przydzielania uprawnień administracji urządzeniem użytkownikom różnych baz.

### Użytkownicy tymczasowi

Z sieci firmowej korzystają nie tylko pracownicy, ale również goście i klienci, dlatego urządzenia Stormshield pozwalają na tworzenie tymczasowych kont użytkowników i polityk specjalnie dla tych użytkowników. Takie konta mogą być tworzone przez głównego administratora. Może je też utworzyć oddelegowany do tego administrator baz użytkowników.

### IP geolocation – filtrowanie oparte o lokalizację hosta

Dzięki funkcji geolokacji administrator wie nie tylko z jakimi adresami IP źródłowymi i docelowymi nawiązywane są połączenia, ale również, gdzie te adresy się znajdują. Geoobiekty pozwalają również na tworzenie polityk filtrowania według kraju czy kontynentu, powiązanego z adresem IP połączenia.

### IP Reputation – reputacja hostów zewnętrznych

IP Reputation to kolejna funkcja, obok geolokacji, która podnosi bezpieczeństwo sieci poprzez ograniczenie ruchu z hostami, rozpoznawanymi jako zagrożenie. Publiczne adresy IP o niskiej reputacji (np. węzły sieci TOR, serwery rozsyłające spam) są przypisywane do jednej z automatycznie aktualizowanych kategorii reputacji. Dzięki temu administrator ma możliwość blokowania połączeń z hostami o złej reputacji, a tym samym uniknięcia zagrożeń przez nie rozsyłanych.



# STORMSHIELD

## Dynamic Host Reputation – reputacja komputerów sieci wewnętrznej

Procesowi badania reputacji zostały poddane również komputery sieci wewnętrznych. Dzięki analizie samych komputerów oraz inspekcji ruchu przez nie generowanego, rozwiązanie UTM firmy Stormshield pozwala utworzenie reguł filtrowania, na podstawie ustalonej wcześniej reputacji. Administrator ma możliwość śledzenia historycznych zmian reputacji komputerów wewnętrznych i wykluczanie stacji o niskim poziomie zaufania.

## Obiekty DNS (FQDN)

Najnowszy firmware wprowadza nową kategorię obiektów DNS. Jeśli nazwa domenowa rozwiązywana jest na wiele adresów IP (np. google.com, office365.com) UTM automatycznie pobierze wszystkie adresy i użyje ich w polityce filtrowania.

## Wsparcie dla nowych wirtualizatorów

Wraz z nowym firmware 3.0 wprowadzone zostało wsparcie dla nowych platform wirtualizacyjnych. Od teraz wspierane są środowiska Microsoft Hyper-V oraz KVM, a odpowiednie maszyny wirtualne dostępne są bezpośrednio w Strefie Klienta (<https://mystormshield.eu>).

## Wsparcie dla modemów 3G/4G

Zapewnienie ciągłego i bezpiecznego dostępu do Internetu jest kluczowym zadaniem rozwiązań UTM. Dzięki możliwości podłączenia zewnętrznego modemu zadanie to staje się szczególnie łatwe, a możliwość użycia modemów 4G gwarantuje dodatkowo szybkość takiego połączenia.

## Pozostałe nowości:

- Wsparcie dla logów w formacie IPFIX/Netflow
- Szyfrowanie komunikacji z serwerem syslog
- Analiza IPS dla protokołów przemysłowych
- Możliwość tworzenia własnych sygnatur IPS
- Możliwość importowania/eksportowania obiektów sieciowych
- Nowe typy logów i raportowanie dla modułu Sandbox