STORMSHIELD

BEZPIECZEŃSTWO ROZWIĄZAŃ IT W ADMINISTRACJI PUBLICZNEJ

JAK SKUTECZNIE CHRONIĆ SIEĆ W DOBIE ATAKÓW TYPU RANSOMEWARE?

Paweł Śmigielski
Sales Manager Poland

Aleksander Kostuch
Inżynier wsparcia sprzedaży

WYBRANE ATAKI

"Nie wiemy, kto stoi za atakiem"

22 czerwca 2015, 7:52

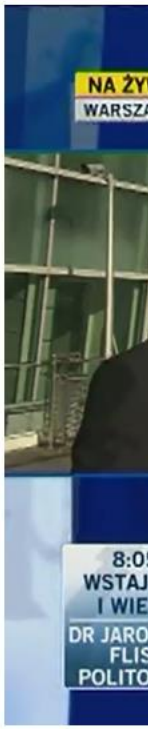
Podziel się 70 Udostępnij

WYBRANE ATAKI

"Nie wiemy, kto stoi za atakiem"

22 czerwca 2015, 7:52

Podziel się 70 Udostępnij



Paczka z poczty to oszustwo. Mail z poczty jest pułapką. Jak uniknąć niebezpieczeństwa?

BP 21 lipca 2015 AKTUALIZACJA: 21 lipca 2015 08:55 DZIENNIK ZACHODNI

1/4

Kurier nie dostarczył przesyłkę do numeru zgłoszenia **RR6475929527PL** na adres **7.20.2015**, ponieważ nikt w tym czasie. Proszę zobaczyć informacje na temat wysyłki, drukowania i iść na pocztę, aby otrzymać pakiet.

Zobacz informacje

Uwaga

Jeżeli przesyłka nie dotrze w ciągu 7 dni roboczych Poczta Polska będzie miała prawo do ubiegania się koszty utrzymania przesyłka 50 zł za jeden dzień. Dziękujemy za korzystanie z naszych usług dostawy. Życząc miłego dnia Twoja Poczta Polska.

To jest generowany automatycznie e-mail, kliknij jeżeli chcesz się wypisać

Najnowsze wiadomości

20:43 Strefa Aktywności Gospodarczej w Zawierciu ma nowego inwestora

20:27 Żarnowiec: Sprawdzali swoją rolniczą wiedzę [FOTO]

20:22 OSTRZEŻENIE METEO! Silne opady, oblodzenia i przymrozki w województwie śląskim

20:00 Sosnowiec: zatrzymany sprawca złamania oczodołu

19:22 Pożar w Miasteczku Śląskim. Pali się pomieszczenie na terenie Huty Cynku

19:13 Styl chalet, czyli jak z każdego mieszkania zrobić górską chatę

ZOBACZ WIĘCEJ

WYBRANE ATAKI

Hakerzy okradli Urząd Pracy w Malborku. Prawdopodobnie wystarczył jeden e-mail

I.O., pszl | publikacja: 10.06.2015 | aktualizacja: 16:57

Prokuratura zaznacza, że namierzenie oszustów będzie bardzo trudne (fot. Pixabay.com)

20 tys. zł przelał za pośrednictwem bankowości elektronicznej jeden z pracowników Powiatowego Urzędu Pracy w Malborku. Nie byłoby w tym nic dziwnego, gdyby nie to, że pieniądze trafiły na zupełnie inny rachunek, niż planowano. Urząd padł ofiarą ataku hakerskiego – sprawą zajęła się prokuratura.

...iem"

...il z poczty jest pułapką. Jak

DZIENNIK ZACHODNI

1/4

...527PL na adres

...e na temat wysyłki,

...będzie miała prawo

Dziękujemy za

...oczta Polska.

To jest generowany automatycznie e-mail, kliknij jeżeli chcesz się wypisać

Najnowsze wiadomości

20:43 Strefa Aktywności Gospodarczej w Zawierciu ma nowego inwestora

20:27 Żarnowiec: Sprawdzali swoją rolniczą wiedzę [FOTO]

20:22 OSTRZEŻENIE METEO! Silne opady, oblodzenia i przymrozki w województwie śląskim

20:00 Sosnowiec: zatrzymany sprawca złamania oczodołu

19:22 Pożar w Miasteczku Śląskim. Pali się pomieszczenie na terenie Huty Cynku

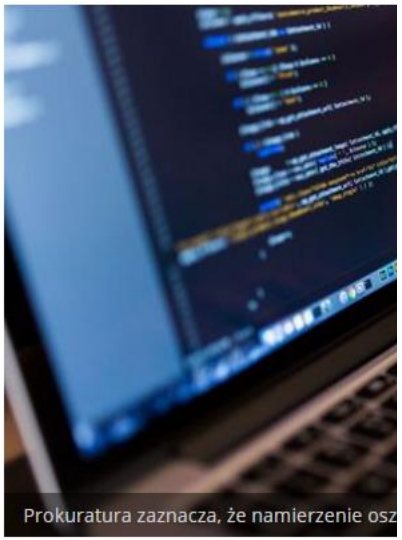
19:13 Styl chalet, czyli jak z każdego mieszkania zrobić górską chatę

ZOBACZ WIĘCEJ

WYBRANE ATAKI

Hakerzy okra
Malborku. Pra
wystarczył jed

I.O., pszl | publikacja: 10.06.2015 | aktualiz



Prokuratura zaznacza, że namierzenie osz

20 tys. zł przelał za pośrednictwe pracowników Powiatowego Urzę dziwnego, gdyby nie to, że pienią planowano. Urząd padł ofiarą ata prokuratura.

To jest generowan

Jabłonna. Władze SZPZOZ o zaszyfrowaniu bazy danych pacjentów

22 Września 2016 | Komentarzy: 3 | Jabłonna | Redakcja

WYBRANE REFERENCJE W POLSCE

Śląskie.
Pozytywna energia

SZPITAL POWIATOWY
w Limanowej
Imienia Miłosierdzia Bożego

URZĄD PATENTOWY
RZECZYPOSPOLITEJ POLSKIEJ

radom
siła w precyzji

WOD KAN
SKIERNIEWICE

POWIAT
ZGORZELECKI
możliwości bez granic

Regionalny Zarząd
Gospodarki Wodnej
we Wrocławiu
Dbamy o przyszłość naszych wód

KARPACZ

POWIATOWY
URZĄD PRACY
DLA POWIATU NOWOSADECKIEGO

Łomża

SĄD OKRĘGOWY w LEGNICY

WYBRANE REFERENCJE W POLSCE

KIM JESTEŚMY

- Firma francuska, powstała w 1998, w Polsce od 2007
- Centrala w Paryżu, 300 pracowników
- Producent rozwiązań zabezpieczających do sieci
- Europejskie certyfikaty bezpieczeństwa
- Polski interfejs, dokumentacja i wsparcie

KIM JESTEŚMY

Stormshield

W pełni należy do Airbus Defence and Space Cybersecurity

KIM JESTEŚMY

Stormshield

oferuje

Innowacyjne rozwiązania zabezpieczeń end-to-end

aby chronić

Sieci

Stormshield Network Security

Komputery

Stormshield Endpoint Security

Informacje

Stormshield Data Security

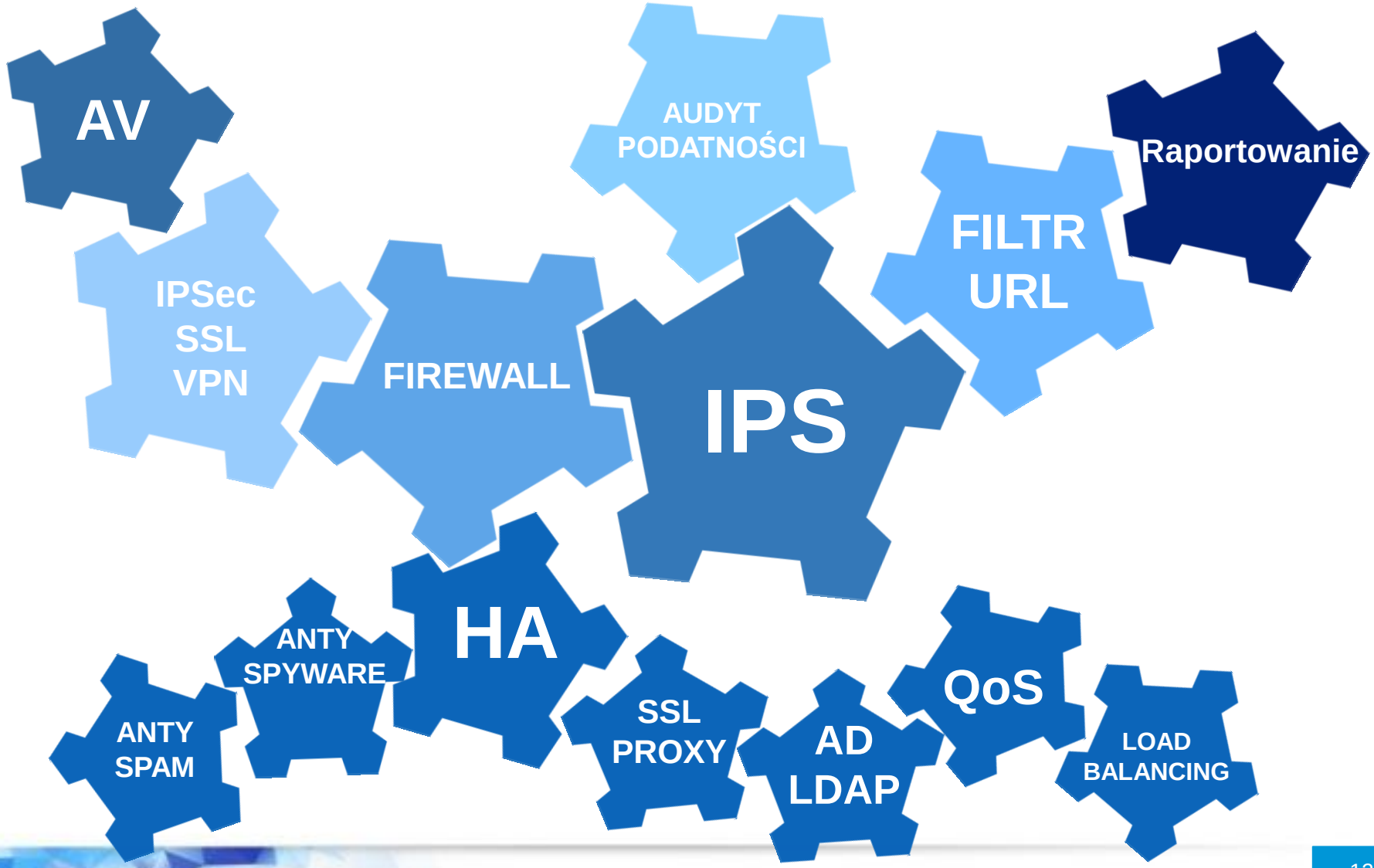
CERTYFIKATY

Vendor	Origin *	CC / cert. country	NATO Restricted	French Qualification	EU Restricted
Astaro/Sophos	UK/US	EAL4+	No	No	No
Check Point	Israel	EAL4+	Yes	No	No
Cisco (ASA)	USA	EAL4+	Yes	No	No
Cyberoam/Sophos	UK/US	EAL4+	No	No	No
Fortinet	USA	EAL4+	No	No	No
Genua	Germany	EAL4+	Only unclassified level	No	No
Juniper	USA	EAL4+	Yes	No	No
Netgear	USA	No	No	No	No
Palo Alto	USA	EAL4+	Yes	No	No
Stonesoft/McAfee	USA	EAL4+	No	Elementary	No
Sonicwall/Dell	USA	EAL4	No	No	No
Watchguard	USA	EAL4+	No (except borderware)	No	No
Stormshield/Airbus DS	FR/GE	EAL4+	Yes	Standard	Yes

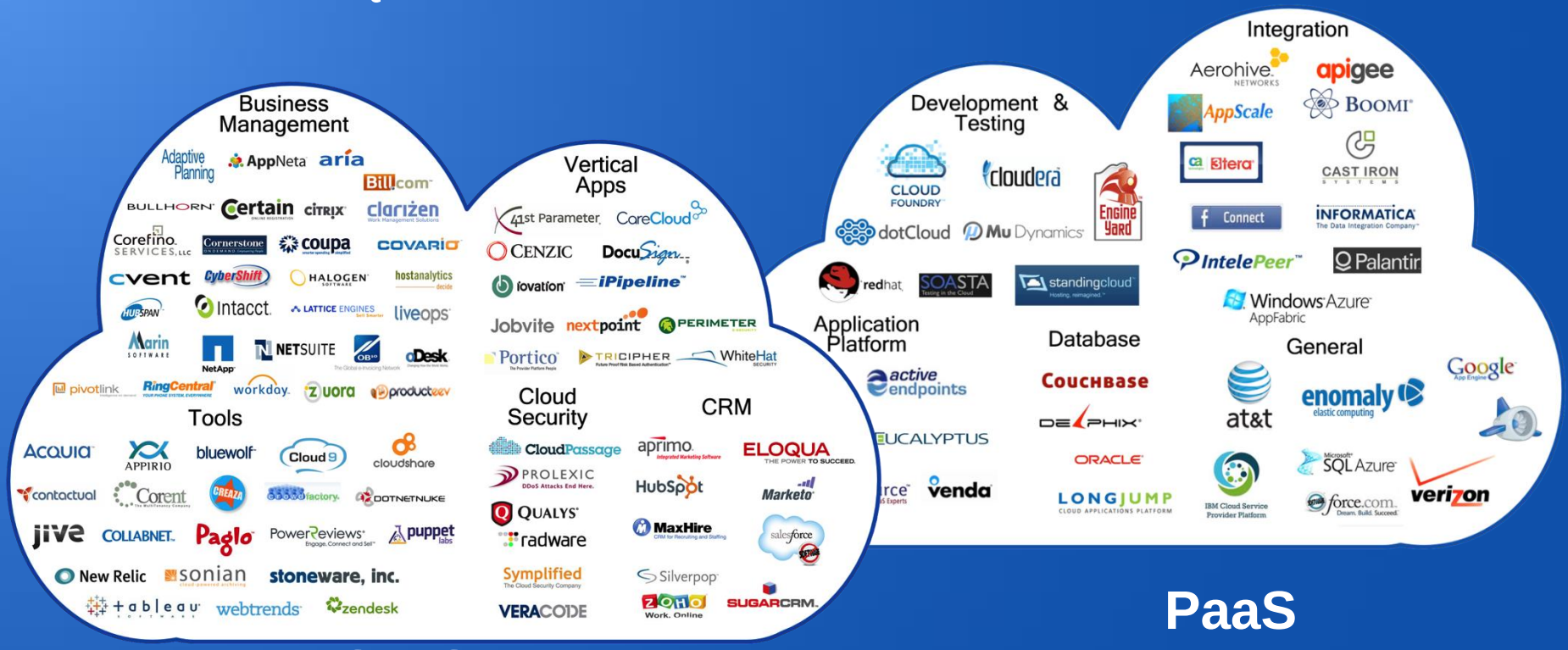
* Origin of the group if the company is a subsidiary.

Strongly dependant on US interests

CO OFERUJEMY



WIĘKSZOŚĆ APLIKACJI W CHMURZE



KONTROLA APLIKACJI

MODELE URZĄDZEŃ W OFERCIE

ROZWIĄZANIA DLA KAŻDEJ SIECI

MAŁE I ŚREDNIE SIECI
[SN150 I SN200 I SN300]

1-10

10-30

30-70

15

ROZWIĄZANIA DLA KAŻDEJ SIECI

DUŻE SIECI
[SN510 I SN710 I SN910]

70-150

150-250

250-500

16

ROZWIĄZANIA DLA KAŻDEJ SIECI

SIECI KORPORACYJNE
[SN2000 I SN3000 I SN6000]

500-1000

1000-2500

5000-...

17

WERSJE WIRTUALNE

CITRIX® ready™

vmware® READY

UTM W CHMURZE

18

FOLDER STORMSHIELD

NETASQ | STORMSHIELD

ZINTEGROWANY SYSTEM OCHRONY SIECI

FUNKCJONALNOŚCI

Firewall zintegrowany z IPS | Filtr URL | Antywirus | IPSec i SSL VPN | Zarządzanie i dwa moduły raportujące w języku polskim | Polskie wsparcie techniczne | Kontrola aplikacji i urządzeń mobilnych Wsparcie IPv6 | Proxy | SSL Proxy | HTTP Proxy cache | Automatyczny backup konfiguracji

STORMSHIELD – NOWA SERIA URZĄDZEŃ UTM OD NETASQ

NETASQ | STORMSHIELD

Unikatowa architektura systemu

Elementem wyróżniającym rozwiązania STORMSHIELD jest integracja zapory sieciowej (Stateful Inspection Firewall) z modułem IPS (Intrusion Prevention System) na poziomie jądra systemu operacyjnego. Tak głęboka integracja dwóch kluczowych modułów pozwala na uzyskanie wysokiej wydajności podczas analizy całego pakietu, a więc jego nagłówka i zawartości. W ten sposób urządzenia STORMSHIELD spełniają dwa najważniejsze oczekiwania klientów wobec tego typu urządzeń – skutecznie eliminują niebezpieczny ruch oraz zapewniają wysoką wydajność skanowania.

Opatentowana technologia wykrywania zagrożeń

Do wykrywania i blokowania włamań rozwiązania STORMSHIELD wykorzystują unikatową technologię Active Security Qualification (ASQ), która dzięki analizie protokołowej połączonej z zaawansowaną heurystyką pozwala na wykrywanie zagrożeń niezależnie od sygnatur (ochrona proaktywna). W ten sposób sieć jest chroniona przed najnowszymi zagrożeniami, dla których sygnatury jeszcze nie powstały, gwarantując pełną ochronę komunikacji sieciowej.

Obsługa kart SD

Rozwiązania STORMSHIELD dają możliwość bezpośredniego zapisywania logów na karty SD oraz SDHC o maksymalnej pojemności 32 GB. To szczególnie przydatna funkcjonalność dla klientów korzystających z modeli SN200 oraz SN300, które nie posiadają wbudowanego dysku twardego.

www.stormshield.pl

STORMSHIELD – NOWA SERIA URZĄDZEŃ UTM OD NETASQ

19

FOLDER STORMSHIELD

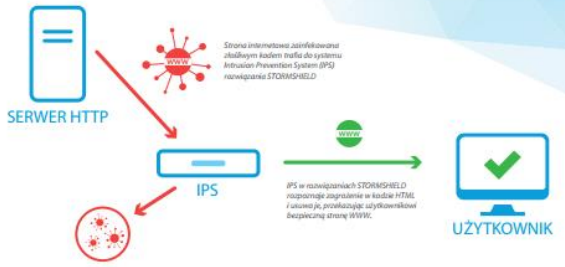
NETAS

ZINTEC
O(

FUNKCJONALNOŚCI
Firewall zintegrowany z IPS |
raportujące w języku polskim
Wsparcie IPv6 | Proxy | SS

STORMSHIELD – N

Jak działa system IPS dla HTTP w STORMSHIELD?



Próbę wizyty na zainfekowanej stronie WWW standardowy IPS po prostu zablokuje. IPS dostępny w urządzeniach STORMSHIELD, rozpozna zagrożenia w kodzie HTML, usunie je i wyświetli użytkownikowi bezpieczną witrynę.

Kontrola ruchu szyfrowanego SSL

Urządzenia STORMSHIELD pozwalają na kontrolę ruchu szyfrowanego za pomocą protokołu SSL. Rozwiązanie działa jako serwer proxy SSL, umożliwiając kontrolę ruchu HTTPS, POP3S, SMTPS oraz FTPS. Sprawdzanie zakodowanych w SSL danych odbywa się po uprzednim zdeszyfrowaniu transmisji. Jeśli przesyłane informacje są bezpieczne, STORMSHIELD ponownie szyfruje dane, podpisuje je własnym certyfikatem i przesyła do użytkownika.

Bezpieczna komunikacja VPN

Wszystkie urządzenia STORMSHIELD pozwalają na szyfrowanie komunikacji pomiędzy lokalizacjami oraz zabezpieczanie zdalnego dostępu do zasobów firmy, protokołami IPSec VPN oraz SSL VPN. W wypadku SSL VPN użytkownik zyskuje dostęp do wszystkich usług i zasobów sieci za pomocą bezpłatnej aplikacji. Dla klientów wymagających zabezpieczenia ciągłości komunikacji na wypadek awarii łącza, każde urządzenie wyposażono w funkcję VPN failover, dzięki której tunel automatycznie zestawi się na zapasowym łączu, gwarantując nieprzerwaną komunikację.

Dwa filtry URL

Rozwiązania STORMSHIELD udostępniają dwa filtry URL, pozwalające blokować użytkownikom sieci firmowej dostęp do wybranych stron internetowych (również tych dostępnych przez HTTPS).
Pierwszy filtr URL jest dedykowany dla polskich użytkowników sieci i jest efektem ścisłej współpracy producenta z polskim dystrybutorem. Baza stron internetowych dla tego filtra powstała na podstawie analizy aktywności w Internecie pracowników polskich firm. Filtr dostarcza ponad 50 kategorii tematycznych, według których klasyfikowane są strony. Jeśli jakiejś strony brakuje w klasyfikacji można ją zgłosić za pomocą specjalnie przygotowanej zakładki na stronie www.stormshield.pl. Zgłoszona w ten sposób strona zostanie sprawdzona i dodana do filtra w ciągu jednego dnia roboczego.
Drugą opcją filtrowania jest rozszerzony filtr URL przechowywany w chmurze, zawierający 65 kategorii – razem to ponad 100 mln adresów URL. Zaletą tego filtra jest przeniesienie procesu weryfikacji danego adresu WWW z urządzenia do chmury, niemal całkowicie eliminując wpływ na wydajność rozwiązania STORMSHIELD.

Konsola zarządzająca urządzeniami STORMSHIELD dostępna jest w języku polskim z poziomu przeglądarki WWW. Wyświetlane treści można dowolnie organizować - poszczególne funkcjonalności mogą być przemieszczane metodą „przeciągnij i upuść". Ta sama metoda pozwala na szybką konfigurację zestawu reguł firewalla.

Zarządzanie w języku polskim

Każde urządzenie STORMSHIELD konfigurowane jest przez konsolę administracyjną w języku polskim, dostępną przez przeglądarkę internetową. Dzięki temu, administrowanie rozwiązaniami STORMSHIELD możliwe jest także za pomocą urządzeń mobilnych.

Polityki bezpieczeństwa w zależności od użytkowników

Dzięki integracji urządzenia STORMSHIELD z bazami użytkowników Active Directory lub LDAP, możliwe jest tworzenie polityk bezpieczeństwa z uwzględnieniem użytkowników i grup. Jeśli w sieci firmowej nie ma jeszcze takiej bazy użytkowników, można ją stworzyć z wykorzystaniem urządzenia STORMSHIELD (baza LDAP na urządzeniu).

Kontrola aplikacji i urządzeń

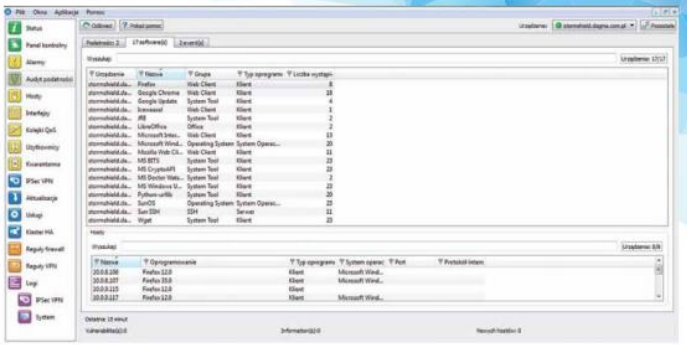
Urządzenia STORMSHIELD pozwalają administratorowi na pełną kontrolę korzystania z aplikacji sieciowych. Dzięki temu możliwe jest m.in. blokowanie niepożądanych w sieci firmowej komunikatorów internetowych (Skype, Gadu-Gadu) oraz aplikacji P2P obciążających łącze. Administrator ma także możliwość kontroli prywatnych urządzeń mobilnych pracowników, wykorzystywanych podczas pracy (tzw. BYOD) – wszystko dzięki modułowi, pozwalającemu na blokowanie dostępu do sieci firmowej z urządzeń mobilnych.

Pełny monitoring sieci

Rozwiązania STORMSHIELD dają administratorowi możliwość pełnej kontroli chronionej sieci. Dzięki aplikacji Real Time Monitor możliwe jest kontrolowanie wszystkich zdarzeń w czasie rzeczywistym. Narzędzie pozwala na śledzenie aktywności poszczególnych użytkowników sieci firmowej i kontrolę transmisji danych.
STORMSHIELD umożliwia administratorowi kontrolę wybranych aplikacji sieciowych, takich jak komunikatory internetowe, programy P2P, a także aplikacje dostępne w serwisie Facebook.

20

FOLDER STORMSHIELD



Audyt Podatności działa na dwa sposoby – identyfikuje aplikacje, z których korzystają na co dzień użytkownicy sieci firmowej oraz wskazuje luki w tych aplikacjach, przyczyniając się do eliminowania podatności sieci firmowej na ataki.

Wykrywanie podatności

Audyt Podatności to narzędzie, które pomaga administratorowi w kontroli aplikacji sieciowych, z których na co dzień korzystają użytkownicy. Narzędzie pomaga monitorować bezpieczeństwo samej sieci, poprzez wykrywanie i wskazywanie wersji oprogramowania, w którym wykryto luki, wrażliwości czy podatności na ataki. Audyt działa każdorazowo, gdy komputer lub serwer z sieci LAN generuje ruch, który jest sprawdzany przez urządzenie STORMSHIELD. Ruch taki jest filtrowany przez firewall i IPS, dzięki czemu identyfikowana jest aplikacja inicjująca dany ruch. Następnie taka aplikacja jest sprawdzana pod kątem wykrytych luk i podatności na ataki.

Audyt Podatności – korzyści

- wykrywanie aplikacji sieciowych zainstalowanych na stacjach roboczych i serwerach
- wykrywanie aplikacji podatnych na ataki
- podpowiadanie niezbędnych działań
- brak wpływu na wydajność systemu
- brak konieczności instalowania agentów na stacjach

Audyt Podatności wykrywa aplikacje sieciowe

Audyt Podatności, dostępny w rozwiązaniach STORMSHIELD, prezentuje administratorowi szczegółową listę aplikacji sieciowych pracujących na stacjach roboczych, np. Google Desktop, Firefox, programy antywirusowe itp. Kliknięcie na wskazaną aplikację powoduje wyświetlenie wszystkich komputerów, na których dany program został zainstalowany, a także pozwala sprawdzić wersję konkretnej aplikacji i system pod jakim działa wybrana stacja.

Audyt Podatności wykrywa i prezentuje szczegółową listę aplikacji sieciowych m.in. Lotus Domino, Apple iTunes, Samba, Apache, MySQL, Mozilla Thunderbird, Skype i wiele innych.

Dwa moduły raportujące w standardzie

Urządzenia STORMSHIELD udostępniają dwa moduły z podstawowymi raportami z aktywności użytkowników w chronionej sieci. Pierwszy z nich jest dostępny z poziomu interfejsu urządzenia. Pozwala na korzystanie z 27 raportów TOP 10, tworzonych w oparciu o logi zapisywane na urządzeniu. Z poziomu wygenerowanego raportu możliwa jest zmiana reguł bezpośrednio na firewallu.

Drugi, Stormshield Log Appliance, to kompletne środowisko, w którym można zbierać i przeglądać logi a także analizować raporty wygenerowane na ich podstawie. Narzędzie dostępne w postaci maszyny wirtualnej pozwala na równoległe zbieranie logów z wielu urządzeń.

STORMSHIELD Event Analyzer

To dodatkowe narzędzie, które dostarcza komplet informacji na temat stanu zabezpieczenia sieci, wykrytych infekcji, prób włamań do sieci, generowanego obciążenia czy identyfikacji niedozwolonych aplikacji sieciowych. Dzięki interaktywnym raportom STORMSHIELD Event Analyzer może informować, m.in. o średnim czasie spędzonym przez pracownika na poszczególnych stronach, najczęściej wpisywanych w wyszukiwarkach frazach czy ilości pobranych danych.

Dzięki STORMSHIELD Event Analyzer administrator może w łatwy sposób monitorować skuteczność ustalonych polityk bezpieczeństwa i generować raporty w oparciu o 200 zdefiniowanych przez producenta wzorów. Raporty powstają na podstawie logów przechowywanych w bazie Microsoft SQL i można je udostępniać za pośrednictwem usługi RSS.

W podstawowej cenie urządzenia STORMSHIELD administrator otrzymuje dwa narzędzia do raportowania - Virtual Log Appliance oraz raporty TOP 10.

...wietlane treści można dowolnie organizować - poszczególne ...rację zestawu reguł firewalla.

...i urządzeń

...pozwalają administratorowi na pełną ...acji sieciowych. Dzięki temu możliwe jest ...anych w sieci firmowej komunikatorów ...-Gadu) oraz aplikacji P2P obciążających ...możliwość kontroli prywatnych urządzeń ...korzystywanych podczas pracy (tzw. BYOD) ...pozwalającemu na blokowanie dostępu do ...bilnych.

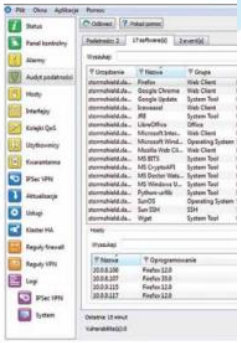
...sieci

...dają administratorowi możliwość pełnej ...ki aplikacji Real Time Monitor możliwe jest ...darzeń w czasie rzeczywistym. Narzędzie ...ności poszczególnych użytkowników sieci ...i danych.

...administratorowi kontrolę wybranych ...jak komunikatory internetowe, programy ...ne w serwisie Facebook.

21

FOLDER STORMSHIELD



Audyt Podatności działa na dwa sposoby – identyfikuje aplikac do eliminowania podatności sieci firmowej na ataki.

Wykrywanie podatności

Audyt Podatności to narzędzie, które pom torowi w kontroli aplikacji sieciowych, z dzień korzystają użytkownicy. Narzędzie p rować bezpieczeństwo samej sieci, poprz i wskazywanie wersji oprogramowania, w luki, wrażliwości czy podatności na atak każdorazowo, gdy komputer lub serwe generuje ruch, który jest sprawdzany pr STORMSHIELD. Ruch taki jest filtrowany prz dzięki czemu identyfikowana jest aplikacja ruch. Następnie taka aplikacja jest sprawdz wykrytych luk i podatności na ataki.

Audyt Podatności wykryw aplikacje sieciowe

Audyt Podatności, dostępny w STORMSHIELD, prezentuje administratorow listę aplikacji sieciowych pracujących na stac np. Google Desktop, Firefox, programy an Kliknięcie na wskazaną aplikację powodu wszystkich komputerów, na których dany zainstalowany, a także pozwala sprawdzić w aplikacji i system pod jakim działa wybrana

STORMSHIELD – NOWA SERIA URZĄDZE

Opcje serwisowe NETASQ STORMSHIELD

	NGFW + IPS	IPSec + SSL VPN	Audyt Podatności	Antywirus	Filtr URL	Antyspam
Remote Office Security Pack SN150, SN200	✓	✓	✗	✗	✗	✗
Enterprise Security Pack SN300, SN500, SN600	✓	✓	✓	✗	✗	✗
UTM Security Pack SN150, SN200, SN300, SN500, SN510, SN700, SN710, SN900, SN910, SN2000, SN3000	✓	✓	✗	✓ Clam AV	✓ Polski filtr URL 50 kategorii	✓
Premium UTM Security Pack WSZYSTKIE MODELE	✓	✓	✓	✓ Kaspersky AV	✓ Chmurowy filtr URL 65 kategorii	✓

Cztery dostępne opcje serwisowe pozwalają dobrać funkcjonalności STORMSHIELD do potrzeb danej sieci firmowej. Każdy z serwisów można w dowolnym momencie rozszerzyć, dokupując brakujące funkcjonalności.

STORMSHIELD Virtual Appliance

Rozwiązania STORMSHIELD dostępne są zarówno w wersji sprzętowej jak i zwirtualizowanej (na platformach VMware oraz Citrix). Obie wersje stanowią identycznie skuteczne zabezpieczenie chronionej sieci i mogą być administrowane z poziomu przeglądarki internetowej.

Co ważne, istnieje możliwość przenoszenia konfiguracji pomiędzy wersją sprzętową oraz zwirtualizowaną. STORMSHIELD Virtual Appliance zapewnia skuteczną ochronę zarówno pomiędzy maszynami wirtualnymi, jak i w fizycznej części sieci.

Specyfikacja rozwiązań wirtualnych

	Dla sieci					Dla chmury	
GŁÓWNE CECHY	V50	V100	V200	V500	VU	VS5	VS10
Chronione adresy IP	50	100	200	500	nieilimitowane	5	10
Audyt podatności	opcjonalnie	opcjonalnie	opcjonalnie	opcjonalnie	opcjonalnie	✓	✓
Liczba jednoczesnych sesji	100 000	200 000	400 000	600 000	3 000 000	1 000 000	2 000 000
802.1Q VLANs (max)	128	128	128	128	512	512	512
Tunele IPSec VPN (max)	100	500	1 000	1 000	10 000	10 000	10 000
Równoczesne połączenia SSL VPN	20	35	70	175	500	500	500

STORMSHIELD – NOWA SERIA URZĄDZEŃ UTM OD NETASQ

www.stormshield.pl

Specyfikacja rozwiązań sprzętowych

	Małe firmy, agencje, filie			Firmy średniej wielkości, agencje						Duże firmy, centra danych		
	SN150	SN200	SN300	SN500	SN510	SN700	SN710	SN900	SN910	SN2000	SN3000	SN6000
WIELKOŚĆ SIECI												
Sugerowana liczba komputerów w sieci	10	30	70	150	150	250	250	500	700	1 000	2 500	15 000
WYDAJNOŚĆ (Gbps)*												
Firewall	0,4	0,6	0,8	1	5	2	10	4	20	30	50	130
Firewall + IPS (1518-bajtowa ramka danych)	0,2	0,6	0,8	1	3	2	7	3	12,5	20	30	55
ŁĄCZNOŚĆ SIECIOWA												
Liczba jednoczesnych sesji	30 000	75 000	150 000	250 000	500 000	600 000	1 000 000	1 200 000	1 500 000	2 000 000	2 500 000	10 000 000
Nowe sesje / sekundę	2 500	15 000	18 000	20 000	20 000	22 000	40 000	25 000	60 000	90 000	120 000	180 000
802.1Q VLAN (Max)	64	64	64	256	256	256	256	512	512	512	1 024	1 024
VPN (Mbps)												
Przepustowość IPSec (Mbps)	100	250	400	550	1000	650	2 400	800	4 000	5 000	6 500	12 000
Liczba tuneli IPSec VPN	25	50	100	500	500	1 000	1 000	1 000	1 000	5 000	5 000	10 000
Liczba tuneli SSL VPN (full)	5	20	20	25	100	50	150	100	150	200	500	500
Liczba tuneli SSL VPN (portal)	20	20	50	75	75	150	150	300	300	1 024	1 024	2 048
HIGH AVAILABILITY (HA)												
Active / passive	-	-	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
ANTYWIRUS (Mbps)												
Przepustowość HTTP	55	165	200	310	850	450	1 600	300	2 200	3 200	4 000	4 700
SPRZĘT												
Interfejsy 10/100/1000	1 + 4 porty (switch)	1 + 2x2 porty (switch)	8	8	12	12	8-16	12	8-16	10-26	10-26	10-58
Światłowód 1GB lub 10GB (bezpł)	-	-	-	-	-	-	0-4	0-2	0-6	0-16	0-16	0-56
Pamięć wewnętrzna	-	karta SD**	karta SD**	120GB	320GB	120GB	320GB	120GB	120GB	128GB SSD	128GB SSD	256GB SSD
Wielkość urządzenia (mm)	37x176 x107	44,5x210 x195	44,5x210 x195	1U - 19"	1U - 19"	1U - 19"	1U - 19"	1U - 19"	1U - 19"	1U - 19"	1U - 19"	2U - 19"

* Test przeprowadzony w warunkach laboratoryjnych. Wyniki mogą różnić się w zależności od warunków testowych oraz wersji oprogramowania.
** Opcjonalnie (wymaga karty SD oraz rozszerzenia licencji).

Polska pomoc techniczna

Użytkownicy rozwiązań STORMSHIELD z aktywną licencją (serwisem) mogą bezpłatnie korzystać z pomocy technicznej w języku polskim. Pomoc świadczą wykwalifikowani inżynierowie, z którymi można kontaktować się w dni robocze, w godzinach 8-18, telefonicznie 32 259 11 89 lub pisząc na adres pomoc@stormshield.pl.

O firmie NETASQ – producencie STORMSHIELD

Rozwiązania STORMSHIELD tworzone są przez firmę NETASQ, która istnieje od 1998 roku i od kilku lat jest członkiem Airbus Group (dawniej European Aeronautic Defence and Space Company - EADS) – koncernu lotniczo-zbrojeniowego. W 2014 roku NETASQ połączyła się z firmą Arkoon. Produkty Unified Threat Management (UTM) firmy NETASQ bardzo szybko podbiły rynek europejski, dzięki zastosowaniu unikatowej architektury ASQ (Active Security Qualification), analizującej przesyłane pakiety na poziomie jądra systemu operacyjnego. Dzięki temu produkty NETASQ od lat słyną z wysokiej wydajności i skutecznej ochrony. Innowacyjne podejście sprawiło również, że obecny w rozwiązaniach tego producenta system IPS nie tylko blokuje niebezpieczny ruch, ale również usuwa szkodliwą zawartość z kodu HTML i dostarcza użytkownikom bezpieczne strony WWW. Na doświadczeniach i unikatowych rozwiązaniach firmy NETASQ bazują najnowsze urządzenia STORMSHIELD. Rozwiązaniami firmy NETASQ chronią swoje sieci m.in. Unia Europejska, NATO, Orange, Carrefour czy Renault.

Dystrybucja NETASQ STORMSHIELD w Polsce:
DAGMA Biuro Bezpieczeństwa IT | ul. Bażantów 4/2 | 40-668 Katowice
tel. 32 259 11 00 | faks 32 793 11 90
www.stormshield.pl

22

FILTROWANIE WWW

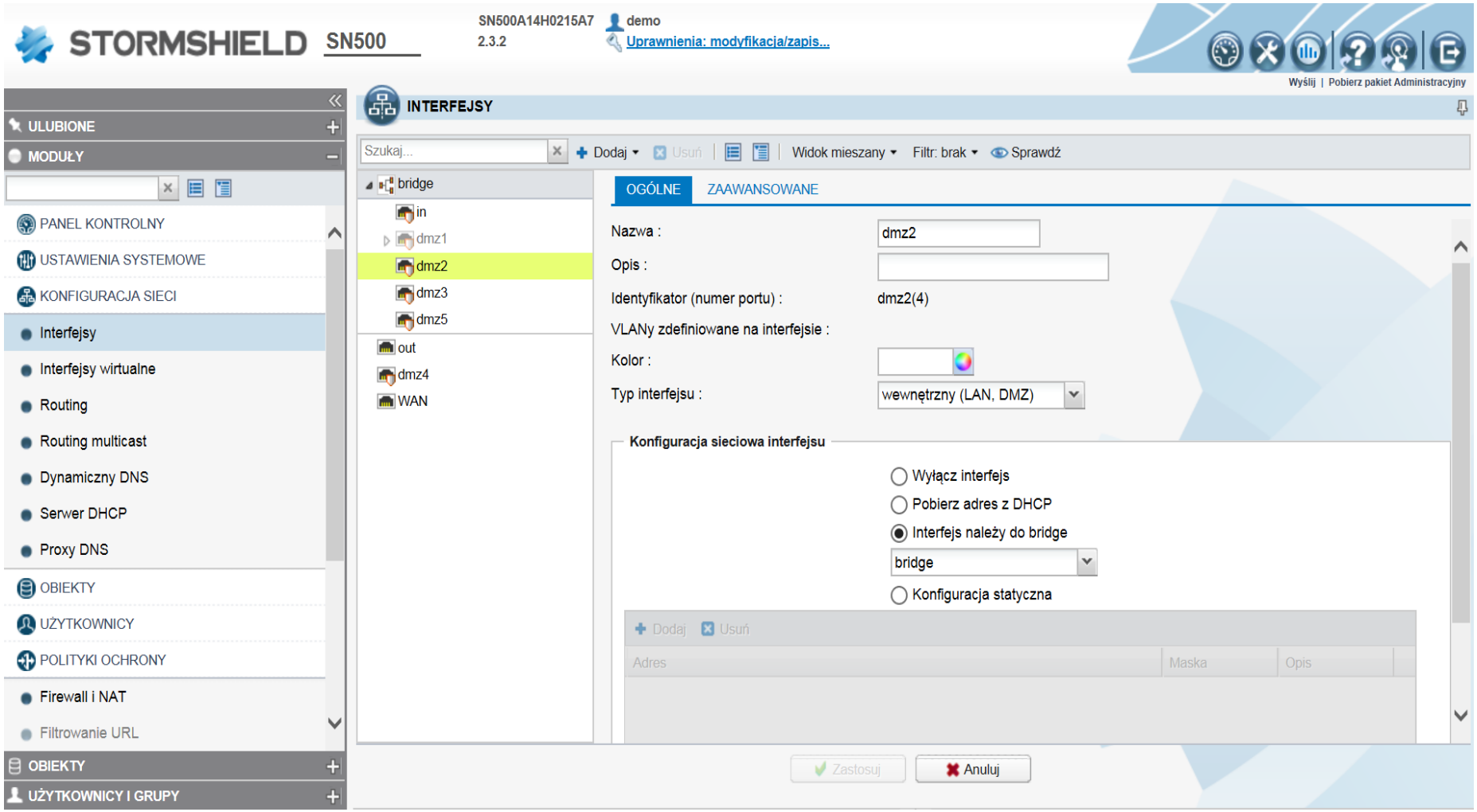
Rozszerzony

Oparty na chmurze

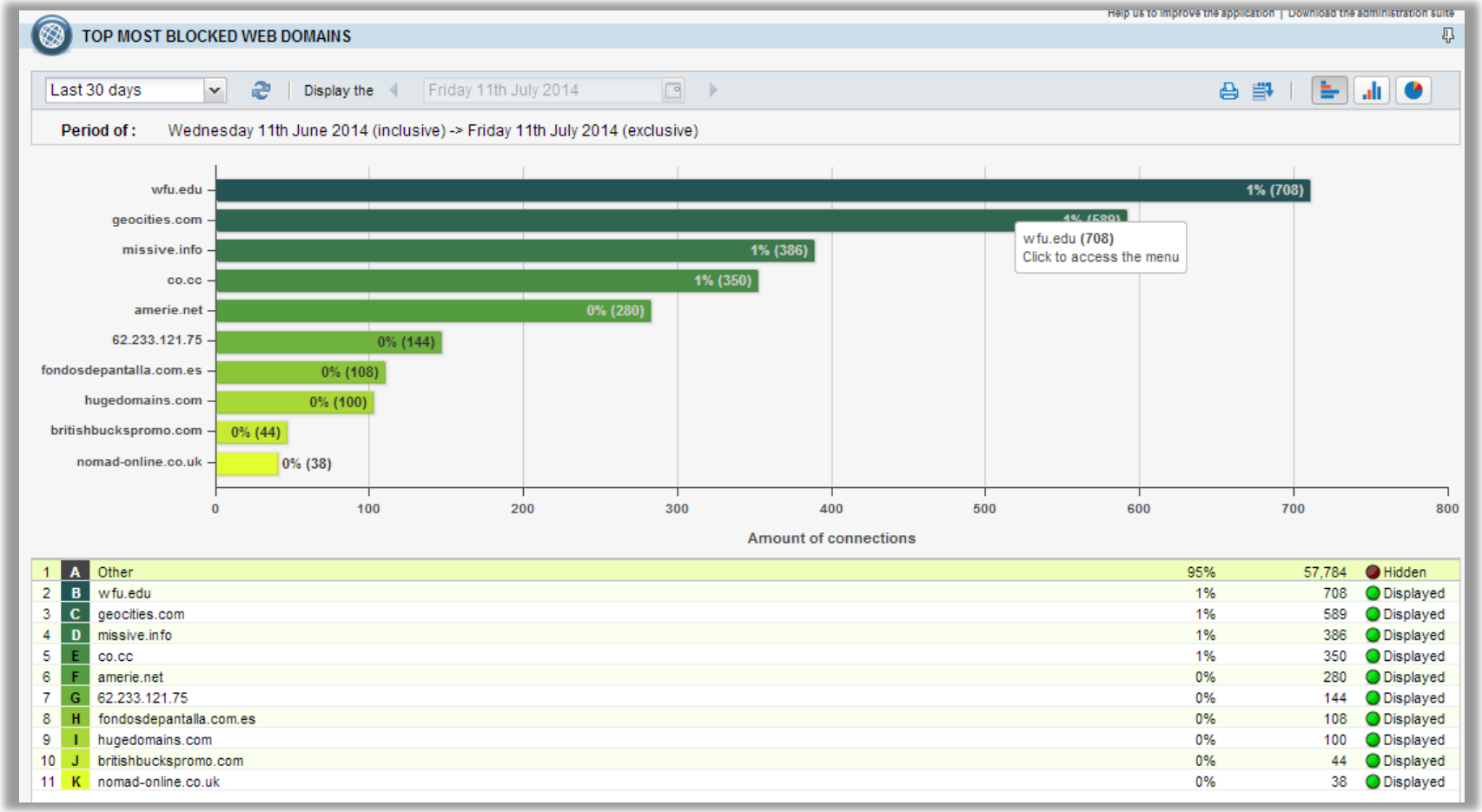
65 kategorii

Standard
+ Polski filtr

POLSKI INTERFEJS UŻYTKOWNIKA

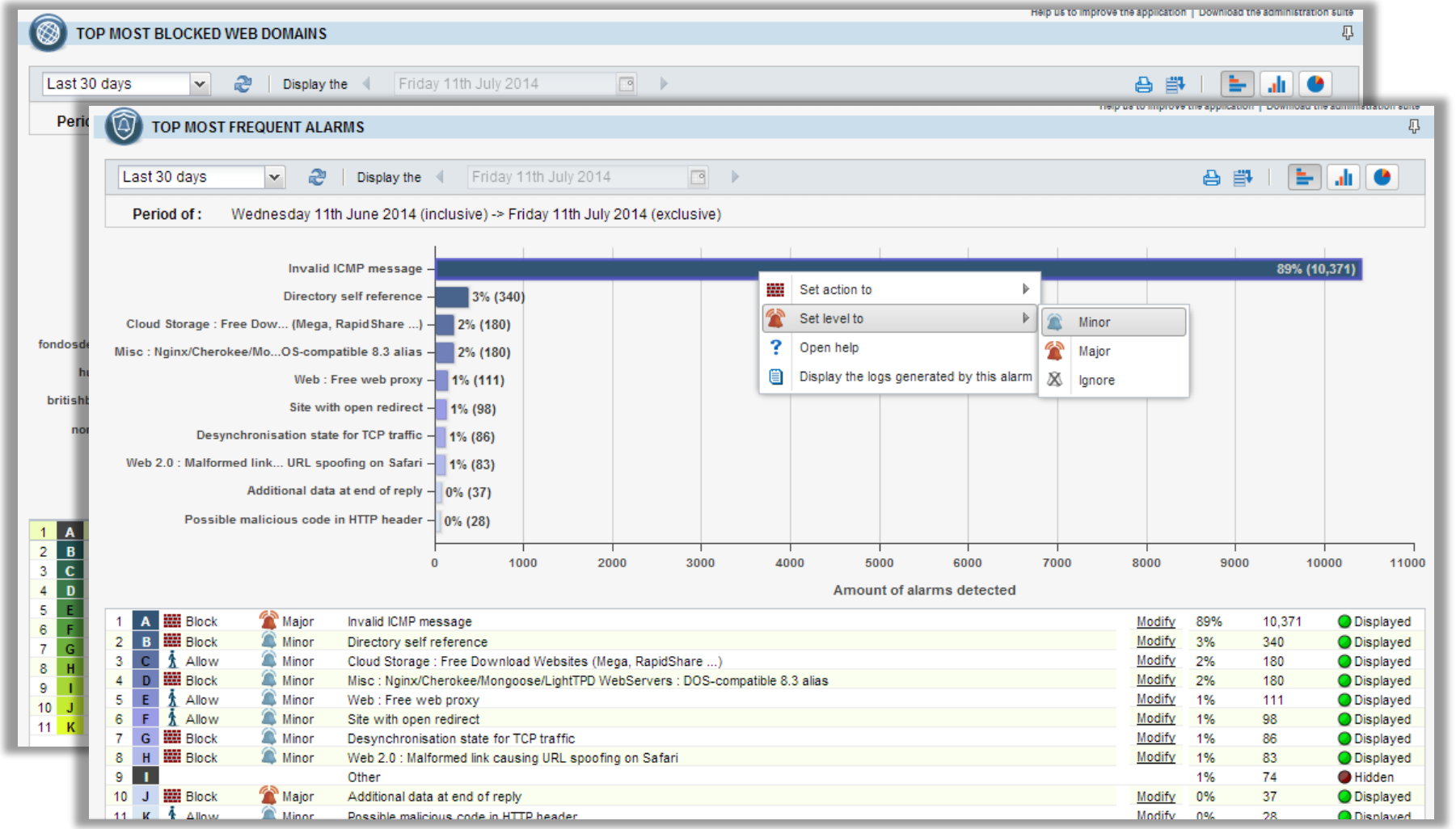


BEZPŁATNE RAPORTOWANIE



1	A	Other	95%	57,784	Hidden
2	B	wfu.edu	1%	708	Displayed
3	C	geocities.com	1%	589	Displayed
4	D	missive.info	1%	386	Displayed
5	E	co.cc	1%	350	Displayed
6	F	amerie.net	0%	280	Displayed
7	G	62.233.121.75	0%	144	Displayed
8	H	fondosdepantalla.com.es	0%	108	Displayed
9	I	hugedomains.com	0%	100	Displayed
10	J	britishbackspromo.com	0%	44	Displayed
11	K	nomad-online.co.uk	0%	38	Displayed

BEZPŁATNE RAPORTOWANIE



AUDYT PODATNOŚCI

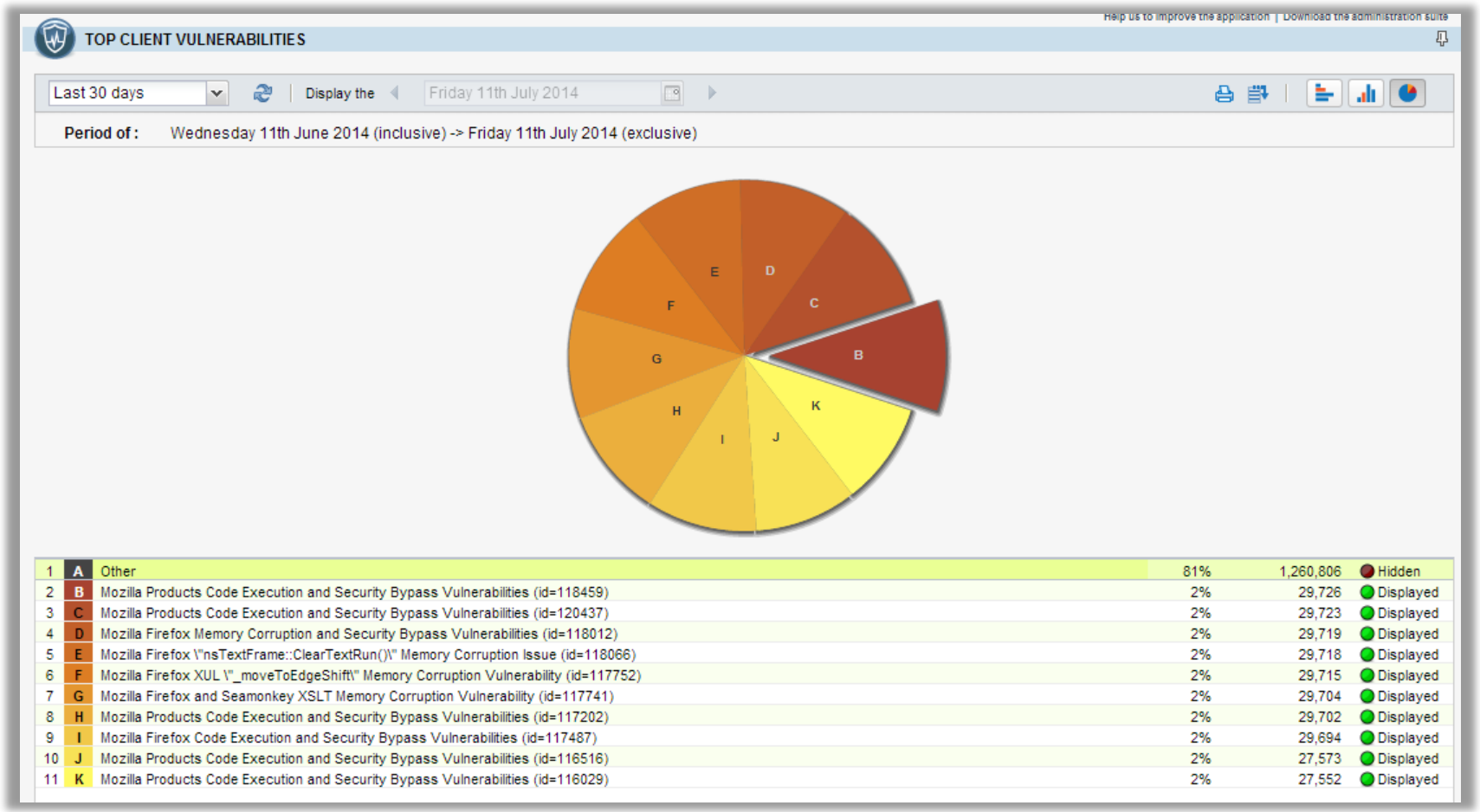
BRAK WPŁYWU NA WYDAJNOŚĆ SIECI

WYSZUKIWANIE SŁABYCH PUNKTÓW
STANOWIĄCYCH ZAGROŻENIA

SUGEROWANIE SPOSOBU ROZWIĄZANIA
WYKRYTYCH PODATNOŚCI

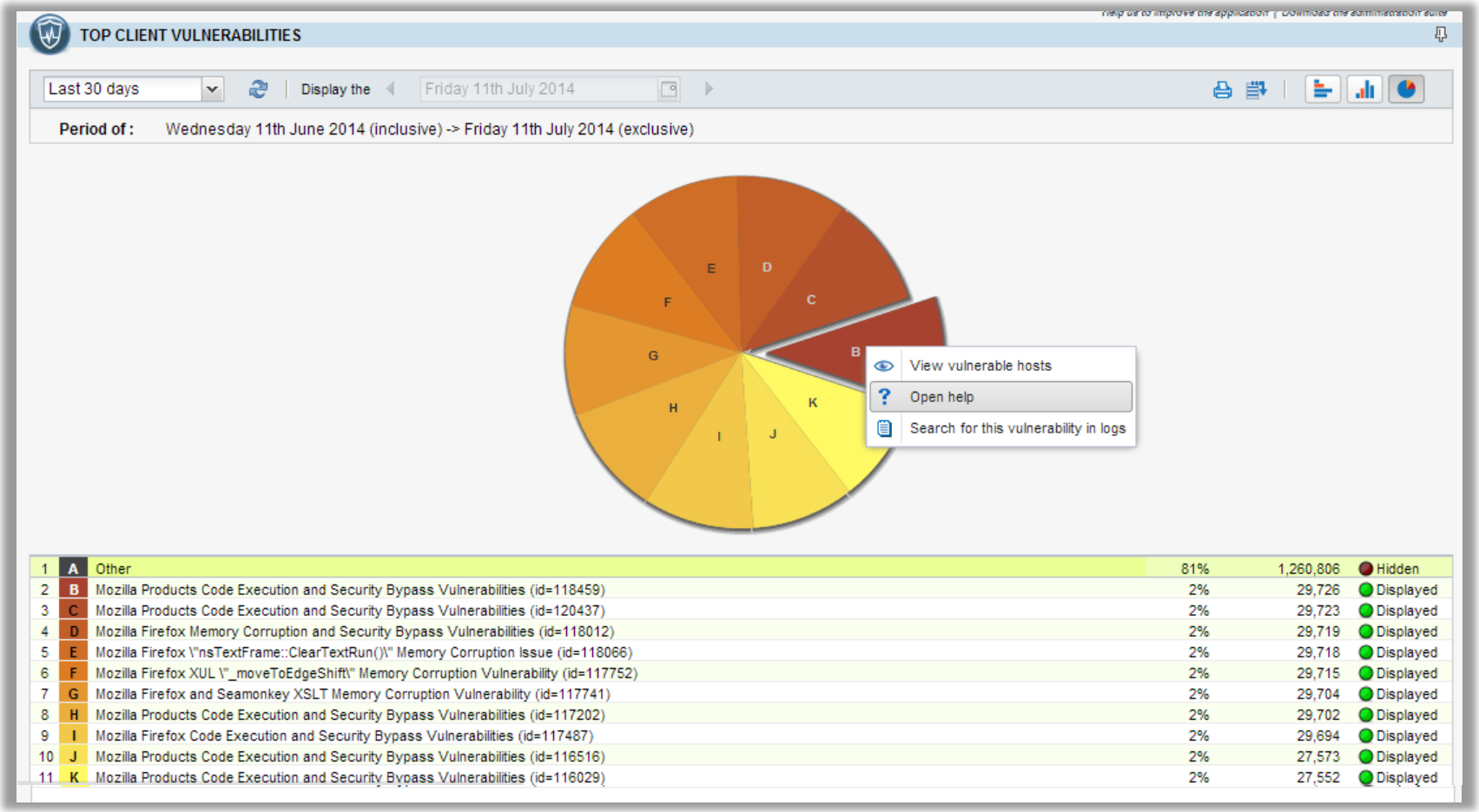
WYKRYWANIE NIEDOZWOLONEGO RUCHU

ANALIZA RYZYKA



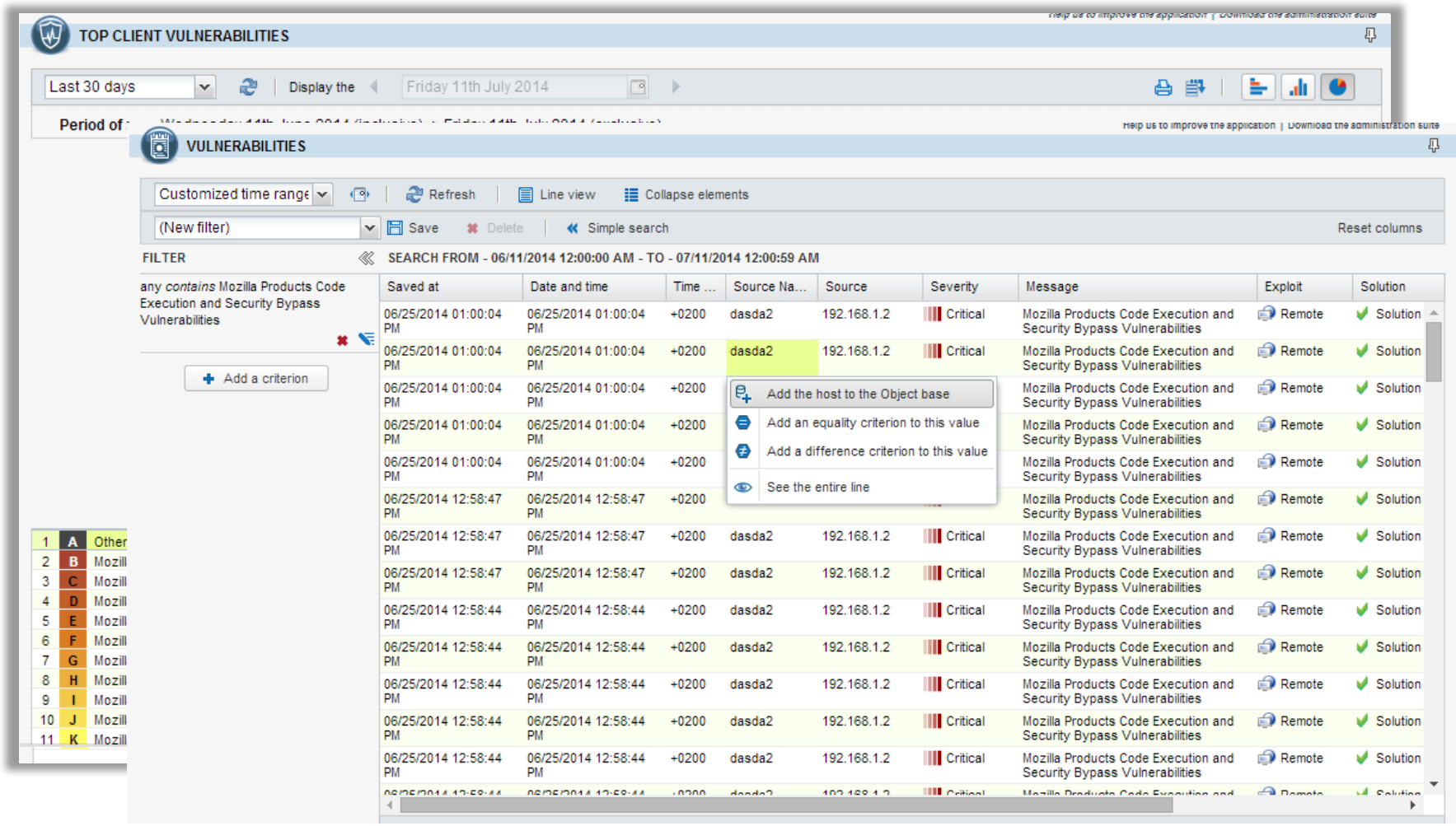
1	A	Other	81%	1,260,806	Hidden
2	B	Mozilla Products Code Execution and Security Bypass Vulnerabilities (id=118459)	2%	29,726	Displayed
3	C	Mozilla Products Code Execution and Security Bypass Vulnerabilities (id=120437)	2%	29,723	Displayed
4	D	Mozilla Firefox Memory Corruption and Security Bypass Vulnerabilities (id=118012)	2%	29,719	Displayed
5	E	Mozilla Firefox \"nsTextFrame::ClearTextRun()\" Memory Corruption Issue (id=118066)	2%	29,718	Displayed
6	F	Mozilla Firefox XUL \"_moveToEdgeShift\" Memory Corruption Vulnerability (id=117752)	2%	29,715	Displayed
7	G	Mozilla Firefox and Seamonkey XSLT Memory Corruption Vulnerability (id=117741)	2%	29,704	Displayed
8	H	Mozilla Products Code Execution and Security Bypass Vulnerabilities (id=117202)	2%	29,702	Displayed
9	I	Mozilla Firefox Code Execution and Security Bypass Vulnerabilities (id=117487)	2%	29,694	Displayed
10	J	Mozilla Products Code Execution and Security Bypass Vulnerabilities (id=116516)	2%	27,573	Displayed
11	K	Mozilla Products Code Execution and Security Bypass Vulnerabilities (id=116029)	2%	27,552	Displayed

ANALIZA RYZYKA



1	A	Other	81%	1,260,806	Hidden
2	B	Mozilla Products Code Execution and Security Bypass Vulnerabilities (id=118459)	2%	29,726	Displayed
3	C	Mozilla Products Code Execution and Security Bypass Vulnerabilities (id=120437)	2%	29,723	Displayed
4	D	Mozilla Firefox Memory Corruption and Security Bypass Vulnerabilities (id=118012)	2%	29,719	Displayed
5	E	Mozilla Firefox \"nsTextFrame::ClearTextRun()\" Memory Corruption Issue (id=118066)	2%	29,718	Displayed
6	F	Mozilla Firefox XUL \"_moveToEdgeShift\" Memory Corruption Vulnerability (id=117752)	2%	29,715	Displayed
7	G	Mozilla Firefox and Seamonkey XSLT Memory Corruption Vulnerability (id=117741)	2%	29,704	Displayed
8	H	Mozilla Products Code Execution and Security Bypass Vulnerabilities (id=117202)	2%	29,702	Displayed
9	I	Mozilla Firefox Code Execution and Security Bypass Vulnerabilities (id=117487)	2%	29,694	Displayed
10	J	Mozilla Products Code Execution and Security Bypass Vulnerabilities (id=116516)	2%	27,573	Displayed
11	K	Mozilla Products Code Execution and Security Bypass Vulnerabilities (id=116029)	2%	27,552	Displayed

ANALIZA RYZYKA



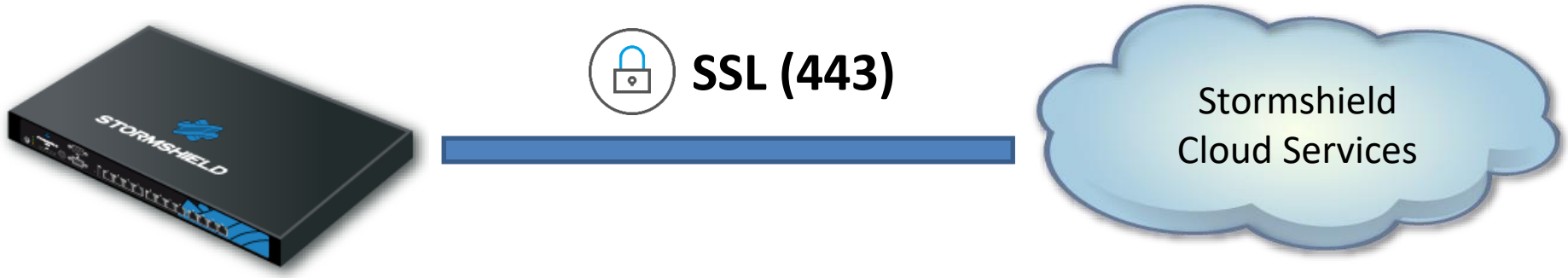
Sandboxing/Detonowanie

Advenced Threat Protection

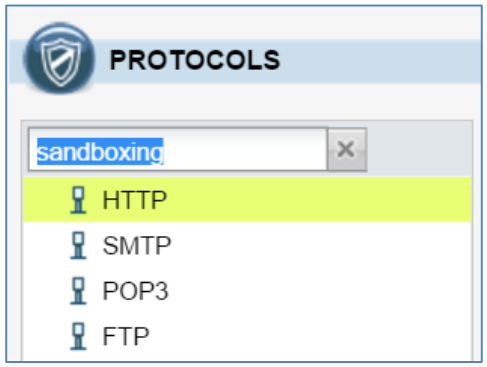
Wykrywanie nieznanych obiektów w wirtualnym środowisku aby zidentyfikować sposób działania

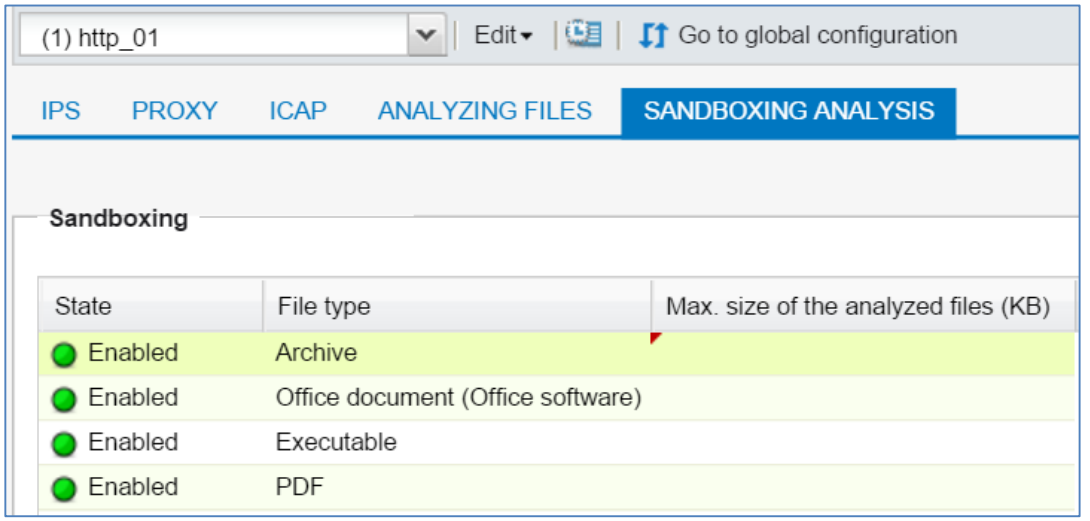
SZYFROWANY TUNEL

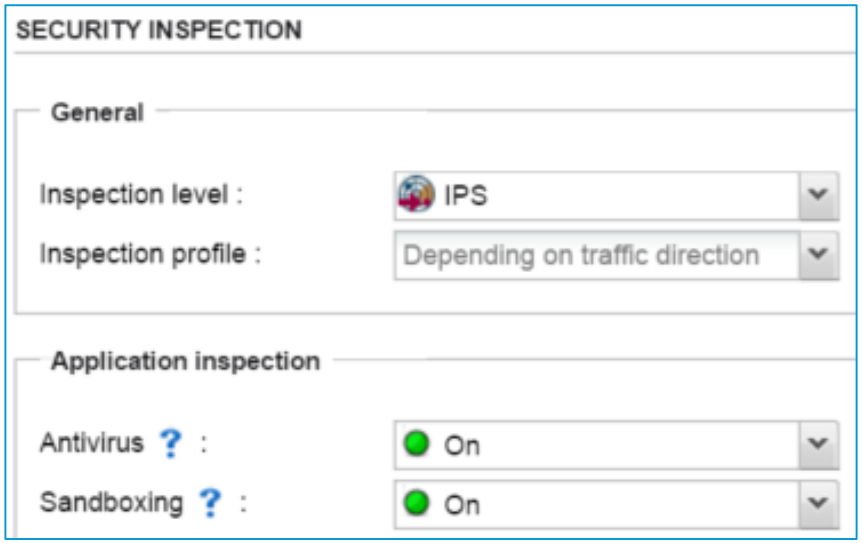
1. SNS autoryzują się własnym certyfikatem
2. SNS sprawdza zaufanie certyfikatu „Cloud services”
3. Komunikacja pomiędzy SNS i Cloud services jest bezpieczna.



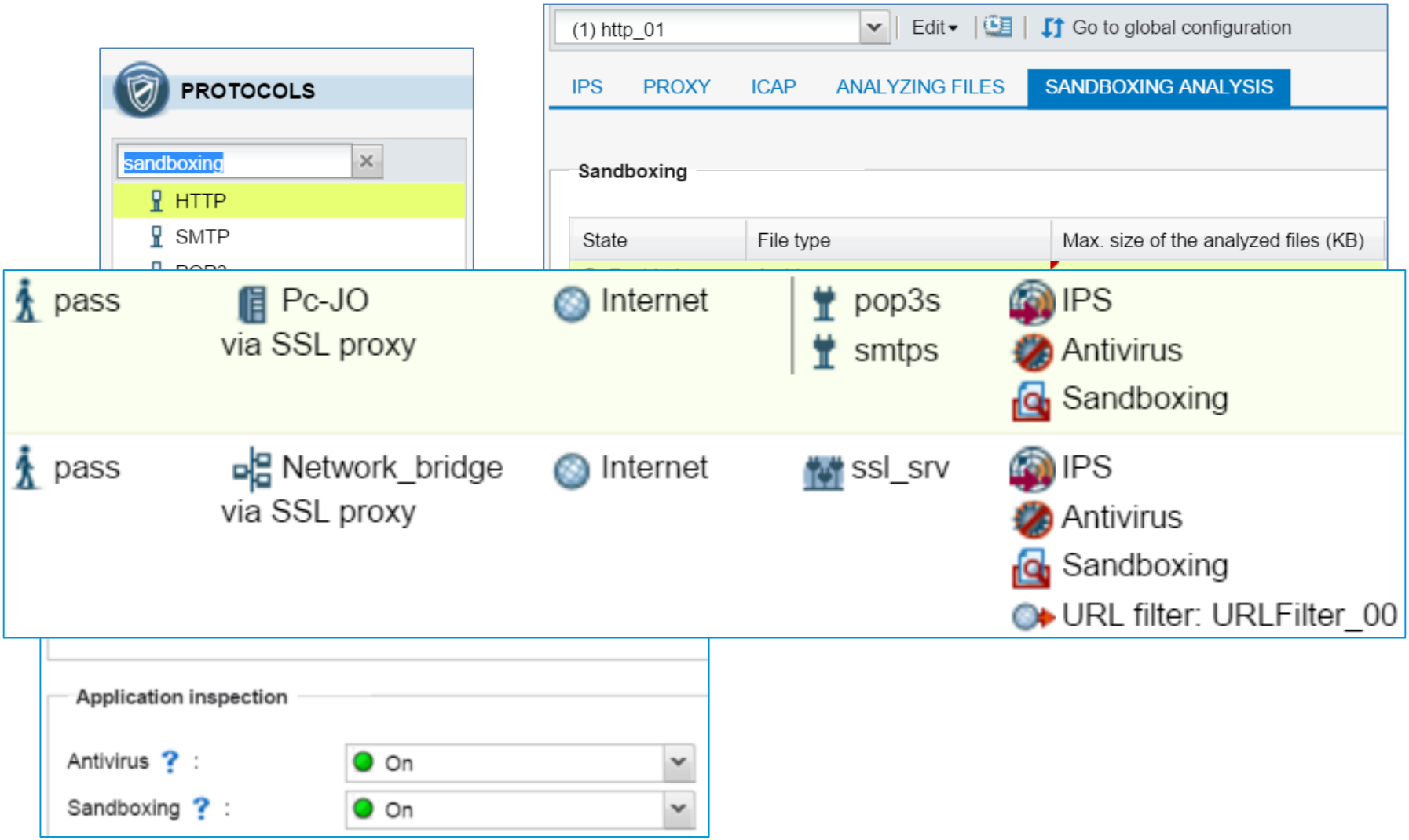
KONFIGURACJA







KONFIGURACJA



CO OFERUJEMY:

- Najszybszy IPS z firewall’em na rynku
- Polskie: interfejs użytkownika, wsparcie techniczne i dokumentacja
- 2 moduły raportujące oraz filtr www w cenie serwisu podstawowego
- Po wygaśnięciu licencji moduły nadal działają
- Bezagentowy skaner podatności w sieci

SZKOLENIA

Certified Stormshield Network Administrator (CSNA):

- podłączenie i tryby pracy
- konfiguracja obiektów i podstawowych usług
- autoryzacja użytkowników
- konfiguracja Audytu Podatności

Certified Stormshield Network Expert (CSNE):

- ustawianie routing by interface
- klastrowanie dwóch urządzeń
- optymalne łączenie reguły zapory z profilami IPS
- zaawansowana translacja adresów.

DOKUMENTACJA

Dokumentacja i pliki do pobrania

Dokumentacja - Firmware Stormshield v2

- Stormshield Podręcznik użytkownika - **PL** - 7 MB

Dokumentacja - Firmware v9

- NETASQ Podręcznik użytkownika - **PL** - 17 MB
- NETASQ Podręcznik użytkownika - **EN** - 7 MB
- NETASQ Unified Manager - **EN** - 4 MB
- NETASQ Real-Time Monitor - **EN**- 5 MB
- NETASQ Event Reporter - **EN** - 2 MB

Pliki do pobrania

- Stormshield Log Appliance
  Plik .ova - 817 MB
- Stormshield SSL VPN Client
  Plik .exe - 15 MB
- STORMSHIELD Administration Suite
  Plik .exe - 58 MB
  Pakiet programów do zarządzania, w skład którego wchodzą:
  - Stormshield Real-Time Monitor
  - Stormshield Event Reporter
  - Stormshield Global Administration
- NETASQ Administration Suite

Wsparcie techniczne

Nie znalazłeś rozwiązania Twojego problemu? Wyślij zgłoszenie!

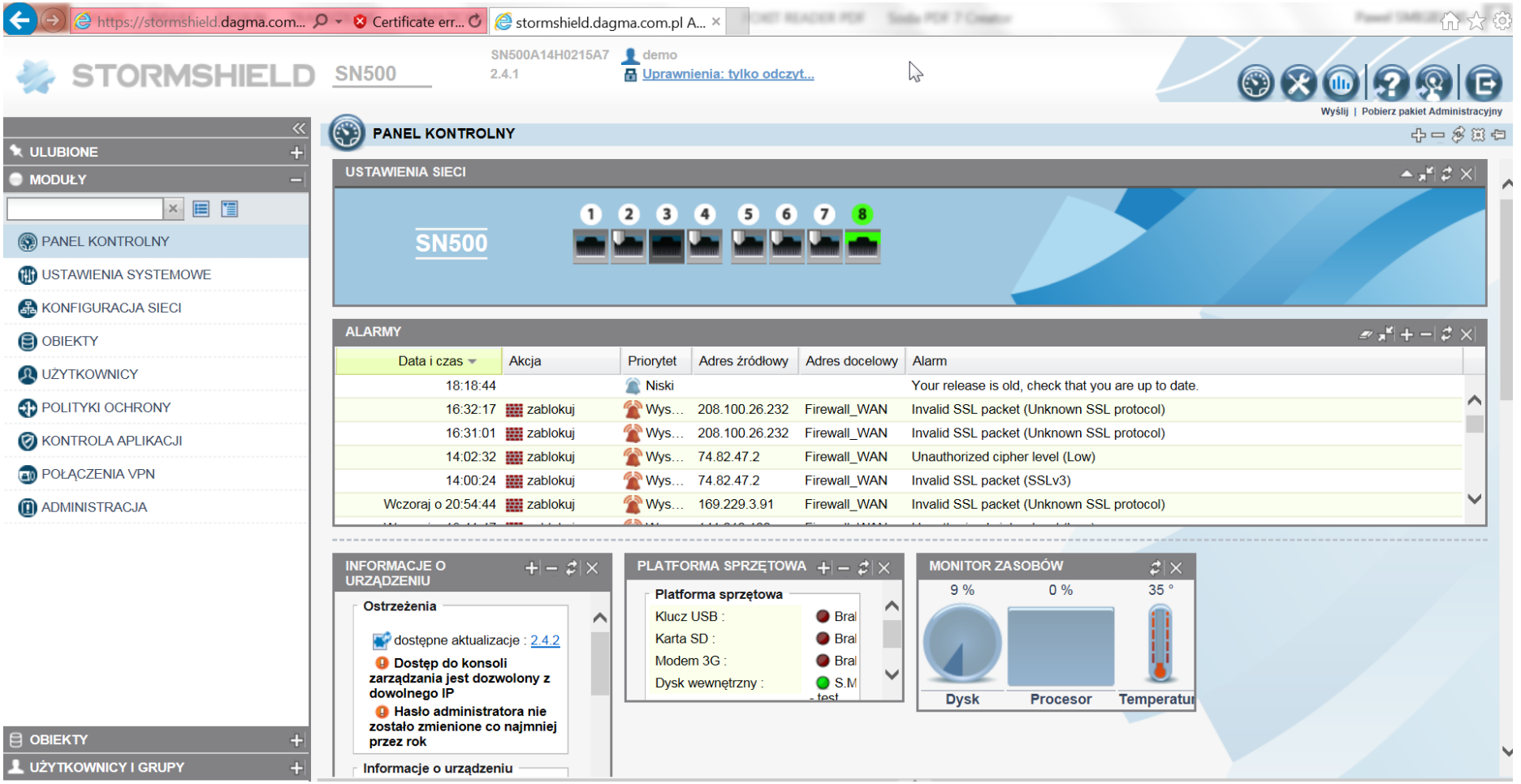
Skontaktuj się z Działem Pomocy Technicznej rozwiązań STORMSHIELD pod numerem **32 793 11 89** (w dni robocze w godzinach 8:00-18:00) lub wyślij nam zgłoszenie problemu korzystając z formularza zgłoszeniowego.

Zgłoś problem

Dodatkowe informacje:

FAQ

DEMO/KONSOLA ONLINE



ZAPRASZAMY DO KONTAKTU