FIREWALL TO ZA MAŁO.

JAK SKUTECZNIE CHRONIĆ URZĘDOWĄ SIEĆ W DOBIE ATAKÓW TYPU APT I RANSOMWARE?

Paweł Śmigielski
Sales Manager Poland

WYBRANE ATAKI

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

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

17:28
9/3/2014

Atak na polskie samorządy. Złośliwe oprogramowanie udające aktualizację przyszło e-mailem

Autor: redakcja | Tagi: atak, e-mail, malware, phishing, Polska, rząd, social-engineering, spoofing

Doczekaliśmy się (pierwszego?) ataku skierowanego jednostki polskich samorządów terytorialnych. E-mail, podszywający się pod producenta oprogramowania zamówionego przez Ministerstwo Finansów nakłaniał (co rzadko się zdarza) poprawną polszczyzną do zainstalowania fałszywej aktualizacji, zainfekowanej złośliwym oprogramowaniem.

Fałszywa bestia

Jak informuje portalsamorzadowy.pl, kilka jednostek samorządu terytorialnego otrzymało e-maila z fałszywą aktualizacją systemu **BeSTi@** (*Stworzonego przez Sygnity Informatycznego Systemu Zarządzania Budżetami Jednostek Samorządu Terytorialnego, przeznaczonego dla Ministerstwa Finansów, Regionalnej Izby Obrachunkowej i ich Zespołów Zamiejscowych oraz Jednostek Samorządu Terytorialnego i ich Związków*):

> *Mail z fałszywą aktualizacją został wysłany z adresu pomoc@budzetjsf.pl, który jest łudząco podobny do adresu obecnego wykonawcy, czyli pomoc@budzetjst.pl.*

BeSTi@

...iem"

...poczty jest pułapką. Jak

DZIENNIK ZACHODNI

1/4

...a adres

...at wysyłki,

...iała prawo

...my za

...ska.

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

17:28
9/3/2014

Atak na polskie samorządy. Złośliv
udające aktualizację przyszło e-ma

Autor: redakcja | Tagi: atak, e-mail, malware, phishir
engineering, spoofing

Doczekaliśmy się (pierwszego?) ataku skierowanego jedn
terytorialnych. E-mail, podszywający się pod producenta
przez Ministerstwo Finansów nakłaniał (co rzadko się zda
zainstalowania fałszywej aktualizacji, zainfekowanej złośl

Fałszywa bestia

Jak informuje portalsamorzadowy.pl, kilka jednostek samo
maila z fałszywą aktualizacją systemu **BeSTi@** (*Stworzon
Informatycznego Systemu Zarządzania Budżetami Jednos
przeznaczonego dla Ministerstwa Finansów, Regionalnej
Zespołów Zamiejscowych oraz Jednostek Samorządu Ter

> *Mail z fałszywą aktualizacją został wysłany z ad
> który jest łudząco podobny do adresu obecnego
> pomoc@budzetjst.pl.*

To jest generowany automatycznie e-mail, ki

> *From: Pomoc BeSTi@ [mailto...@budzetjsf.pl]*
> *Sent: Monday, March 17, 2014 8:49 AM*
> *To:...*
> *Subject: Aktualizacja systemu BeSTi@ do wersji 3.02.012.07*
>
> *Witamy,*
> *Pragniemy poinformować, iż dnia dzisiejszego została udostępniona nowa aktualizacja do systemu BeSTi@ w wersji 3.02.012.07.*
> *Aktualizacja usuwa błędy związane z bezpieczeństwem bazy danych oraz poprawia problem z podpisem elektronicznym sprawozdań.*
>
> *Instalacja jest bardzo prosta i nie wymaga dodatkowej pomocy oraz czynności.*
> *Ze względu na znaczące poprawki bezpieczeństwa aktualizacja nie jest dostępna z menu programu BeSTia, należy przeprowadzić ją ręcznie.*
>
> *Poniższy plik "Bestia.3.02.012.07" należy zapisać na pulpicie lub w innym miejscu a następnie go uruchomić co spowoduje zainstalowanie uaktualnienia do systemu BeSTi@.*
>
> *hxxp://budzetjsf.pl/Update/BeSTia/Bestia.3.02.012.07.exe*
>
> *Instalacja nie powinna zająć więcej niż minutę.*
> *Dziękujemy i przepraszamy za niedogodności*
>
> ———————
> *Sputnik Software*
> *tel. 61 622 00 60*
> *tel. 32 722 11 96*

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.

STi@ [mailto...@budzetjsf.pl]
larch 17, 2014 8:49 AM

zacja systemu BeSTi@ do wersji 3.02.012.07

ormować, iż dnia dzisiejszego została udostępniona nowa
systemu BeSTi@ w wersji 3.02.012.07.
wa błędy związane z bezpieczeństwem bazy danych oraz
m z podpisem elektronicznym sprawozdań.

ardzo prosta i nie wymaga dodatkowej pomocy oraz

naczące poprawki bezpieczeństwa aktualizacja nie jest
u programu BeSTia, należy przeprowadzić ją ręcznie.

estia.3.02.012.07" należy zapisać na pulpicie lub w
następnie go uruchomić co spowoduje zainstalowanie
systemu BeSTi@.

pl/Update/BeSTia/Bestia.3.02.012.07.exe

winna zająć więcej niż minutę.
epraszamy za niedogodności

tel. 32 722 11 96

WYBRANE ATAKI

Hakerzy okrad Malborku. Pra wystarczył jed

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

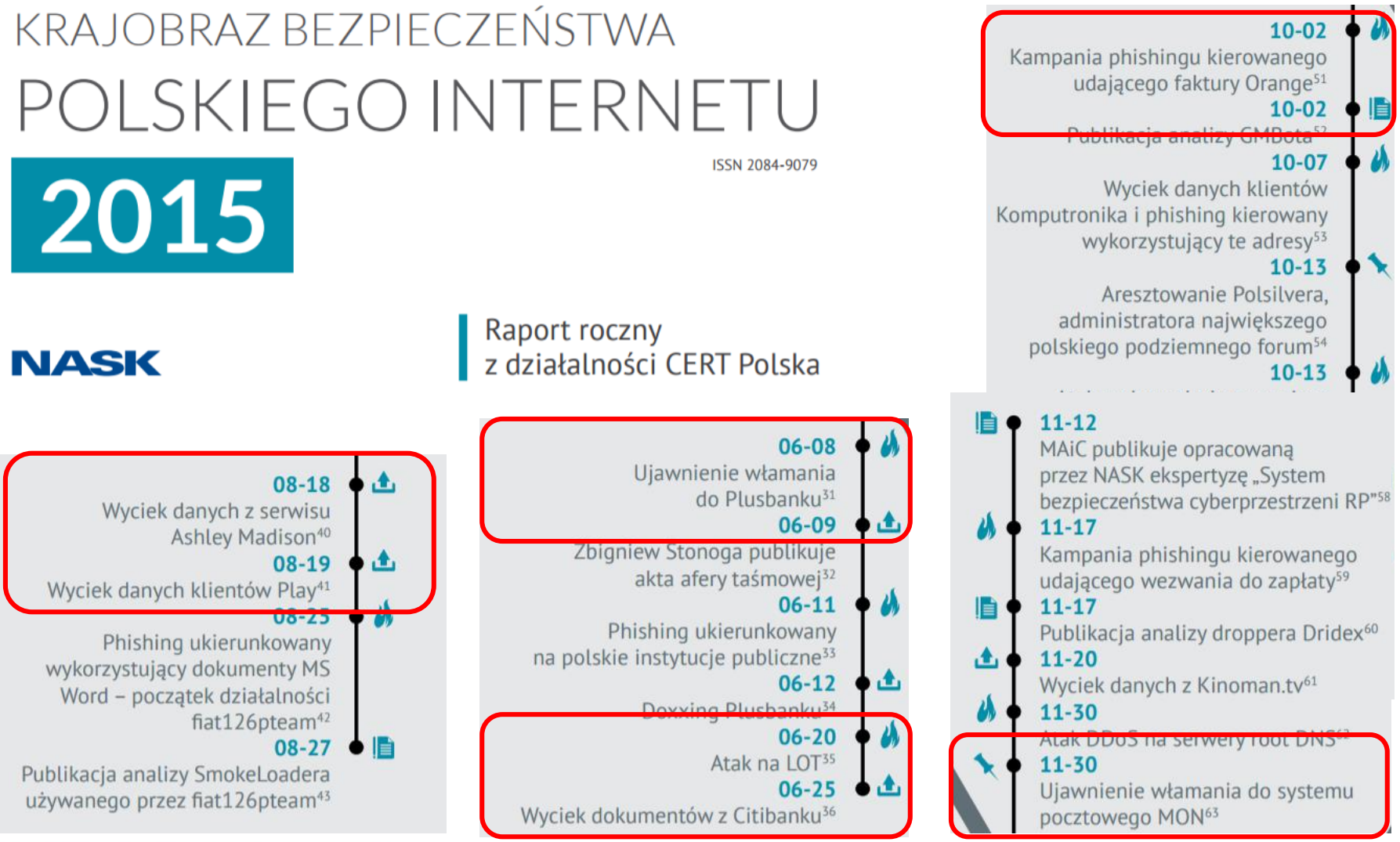
Prokuratura zaznacza, że namierzenie osz

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

Jabłonna. Władze SZPZOZ o zaszyfrowaniu bazy danych pacjentów

22 Września 2016 | Komentarzy: 3 | Jabłonna | Redakcja

CERT 2015


KRAJOBRAZ BEZPIECZEŃSTWA
POLSKIEGO INTERNETU
2015
ISSN 2084-9079
NASK
Raport roczny
z działalności CERT Polska
08-18
Wyciek danych z serwisu Ashley Madison[40]
08-19
Wyciek danych klientów Play[41]
08-25
Phishing ukierunkowany wykorzystujący dokumenty MS Word – początek działalności fiat126pteam[42]
08-27
Publikacja analizy SmokeLoadera używanego przez fiat126pteam[43]
06-08
Ujawnienie włamania do Plusbanku[31]
06-09
Zbigniew Stonoga publikuje akta afery taśmowej[32]
06-11
Phishing ukierunkowany na polskie instytucje publiczne[33]
06-12
Doxxing Plusbanku[34]
06-20
Atak na LOT[35]
06-25
Wyciek dokumentów z Citibanku[36]
10-02
Kampania phishingu kierowanego udającego faktury Orange[51]
10-02
Publikacja analizy GMBota[52]
10-07
Wyciek danych klientów Komputronika i phishing kierowany wykorzystujący te adresy[53]
10-13
Aresztowanie Polsilvera, administratora największego polskiego podziemnego forum[54]
10-13
11-12
MAiC publikuje opracowaną przez NASK ekspertyzę „System bezpieczeństwa cyberprzestrzeni RP"[58]
11-17
Kampania phishingu kierowanego udającego wezwania do zapłaty[59]
11-17
Publikacja analizy droppera Dridex[60]
11-20
Wyciek danych z Kinoman.tv[61]
11-30
Atak DDoS na serwery root DNS[62]
11-30
Ujawnienie włamania do systemu pocztowego MON[63]

REKOMENDACJE CERT

REKOMENDACJE TECHNICZNE

- **REKOMENDACJA 1**: Dokonanie przeglądu infrastruktury sieciowej. Wdrożenie reguł kontroli ruchu na urządzeniach brzegowych oraz systemach bezpieczeństwa. Przygotowanie infrastruktury pod kątem ewentualnego blokowania lub odrzucania niepożądanego ruchu sieciowego poprzez jego analizę i segregację w oparciu o zadane reguły.
- **REKOMENDACJA 2**: Wdrożenie dedykowanych maszyn z systemami firewall (w tym także warstwy aplikacji), IDS/IPS, monitoringu. Przygotowanie infrastruktury do eliminacji ruchu anonimizowanego w przypadku wystąpienia zagrożenia (np. TOR, Open-Proxy, Anon-Proxy, Anon-VPN). Wymuszenie ciągłej aktualizacji mechanizmów bezpieczeństwa.
- **REKOMENDACJA 3**: Systematyczne dokonywanie przeglądu konfiguracji kluczowych urządzeń sieciowych znajdujących się w infrastrukturze instytucji. Bieżące aktualizowanie rozwiązań sprzętowych i programowych użytkowanych przez instytucję.

REKOMENDACJE CERT

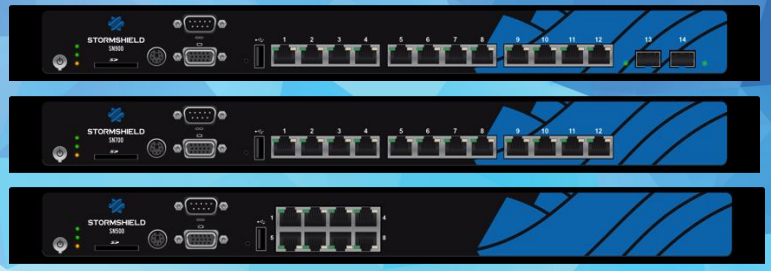
- **REKOMENDACJA 6**: Wprowadzenie na urządzeniach sieciowych blokowania dostępu do złośliwych domen i adresów.
- **REKOMENDACJA 11**: Prowadzenie przeglądów oprogramowania użytkowanego na stacjach roboczych w sieci instytucji (odinstalowanie oprogramowania służącego do celów innych niż służbowe), a także wdrożenie mechanizmów kontrolujących w trybie ciągłym list oprogramowania dopuszczonego do stosowania w sieci.
- **REKOMENDACJA 13**: Wdrożenie centralnego systemu antywirusowego i antyspamowego oraz wymuszanie ich ciągłej aktualizacji na stacjach roboczych lub serwerach na podstawie list RBL czy też aktualizacji wydawanych przez wytwórcę użytkowanego oprogramowania.
- **REKOMENDACJA 14**: Wdrożenie centralnego systemu korelacji danych tzw. SIEM, który m.in. umożliwia centralne zarządzanie bezpieczeństwem TI oraz pozwala na wykrywanie ataków poprzez analizę anomalii.
- **REKOMENDACJA 15**: Stworzenie i właściwa konfiguracja środowisk izolowanych tzw. sandbox, które m.in. pozwalają na izolację potencjalnie niebezpiecznych plików.

ROZWIĄZANIA DLA KAŻDEJ SIECI

MAŁE ORGANIZACJE, ODDZIAŁY (1-70 UŻYTKOWNIKÓW)

DUŻE SIECI, DATACENTER (700-15 000 UŻYTKOWNIKÓW)

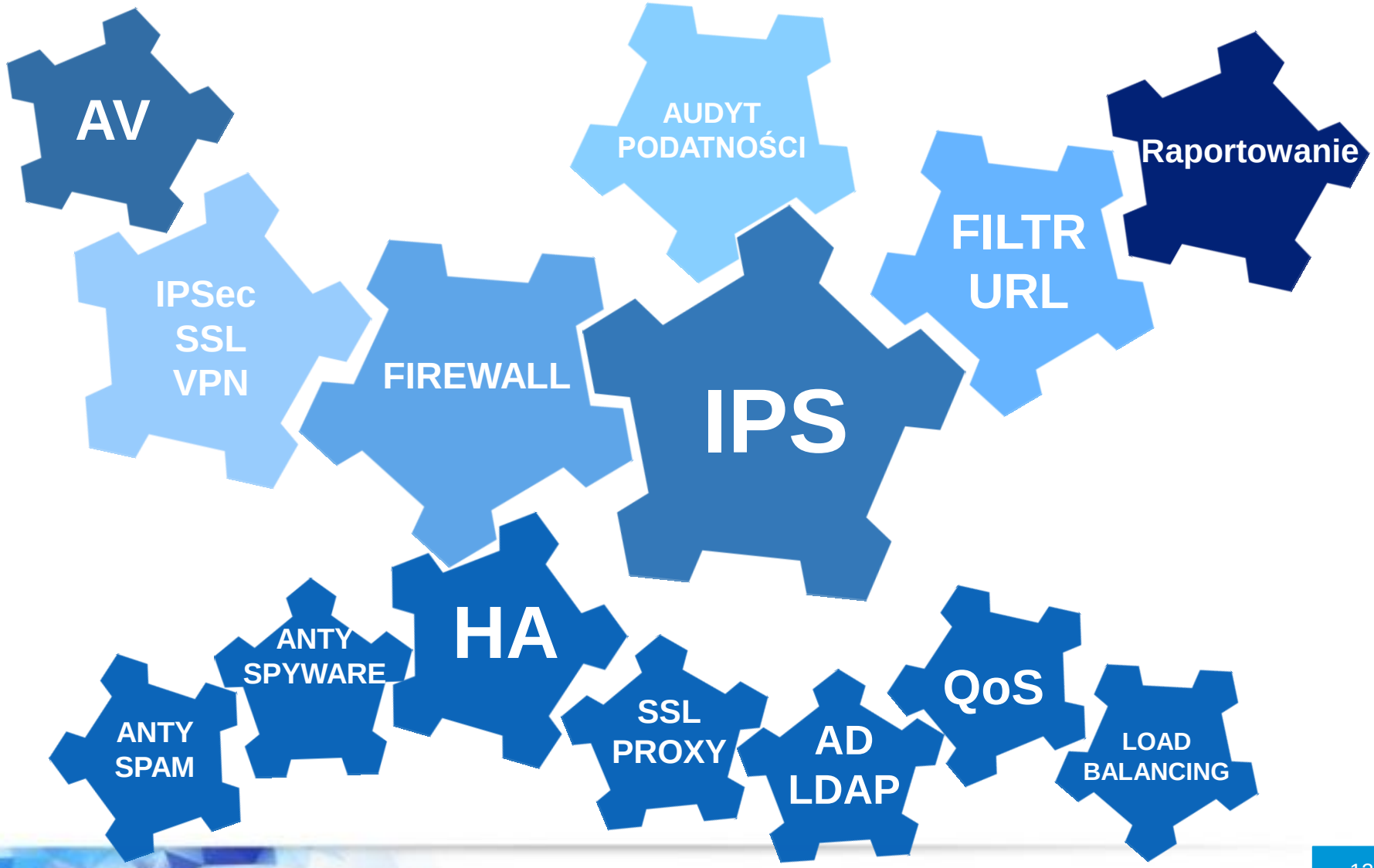
SIECI ŚREDNIEJ WIELKOŚCI (70-700 UŻYTKOWNIKÓW)



WIRTUALNE URZĄDZENIA I UTM W CHMURZE

12

CO OFERUJEMY



KIM JESTEŚMY

- Firma francuska, powstała w 1998, w Polsce od 2007
- Producent rozwiązań zabezpieczających do sieci
- Europejskie certyfikaty bezpieczeństwa
- Kilka tysięcy urządzeń wdrożonych w Polsce
- Polski interfejs, dokumentacja i wsparcie

KIM JESTEŚMY

Stormshield

W pełni należy do Airbus Defence and Space Cybersecurity

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

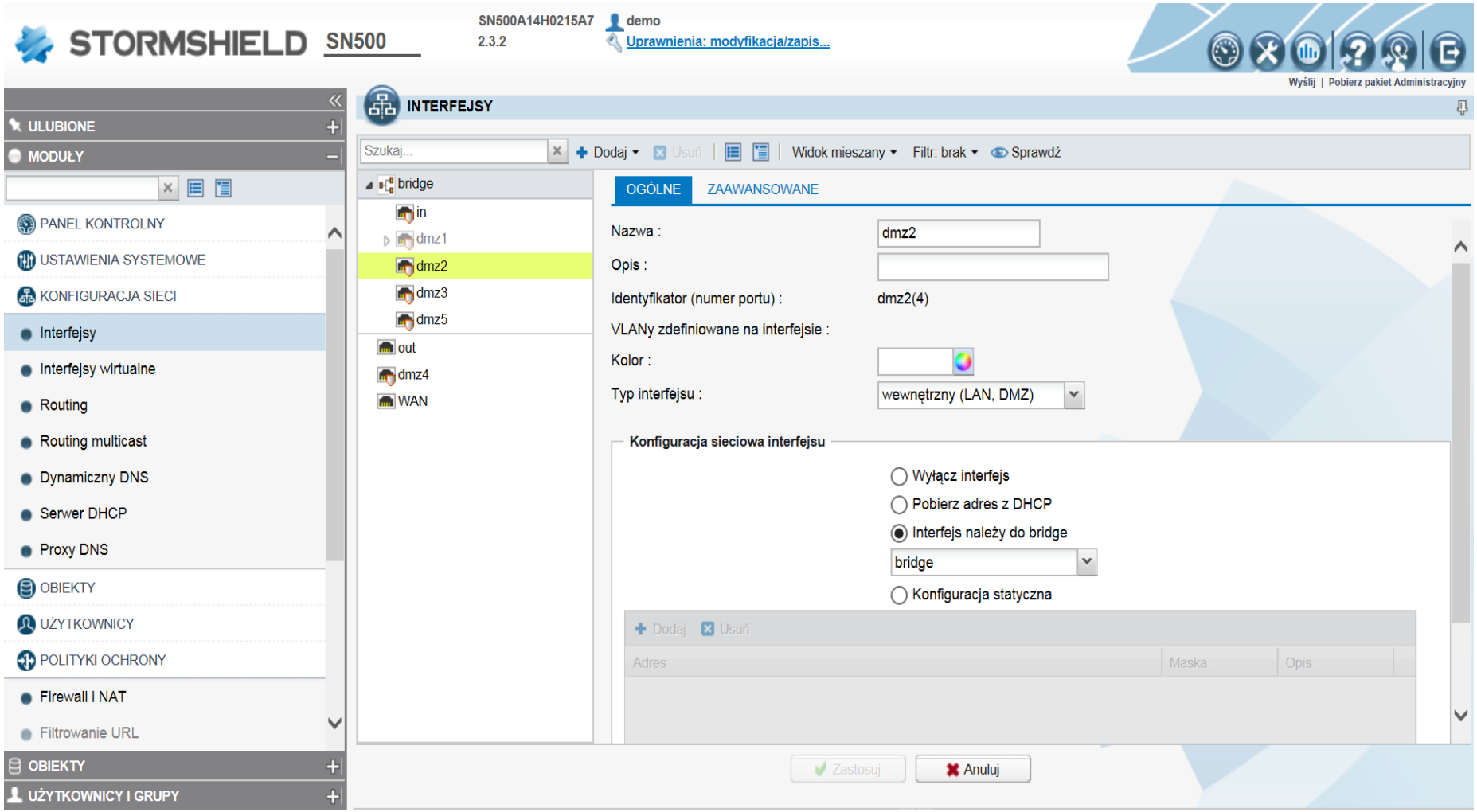
CERTYFIKATY

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

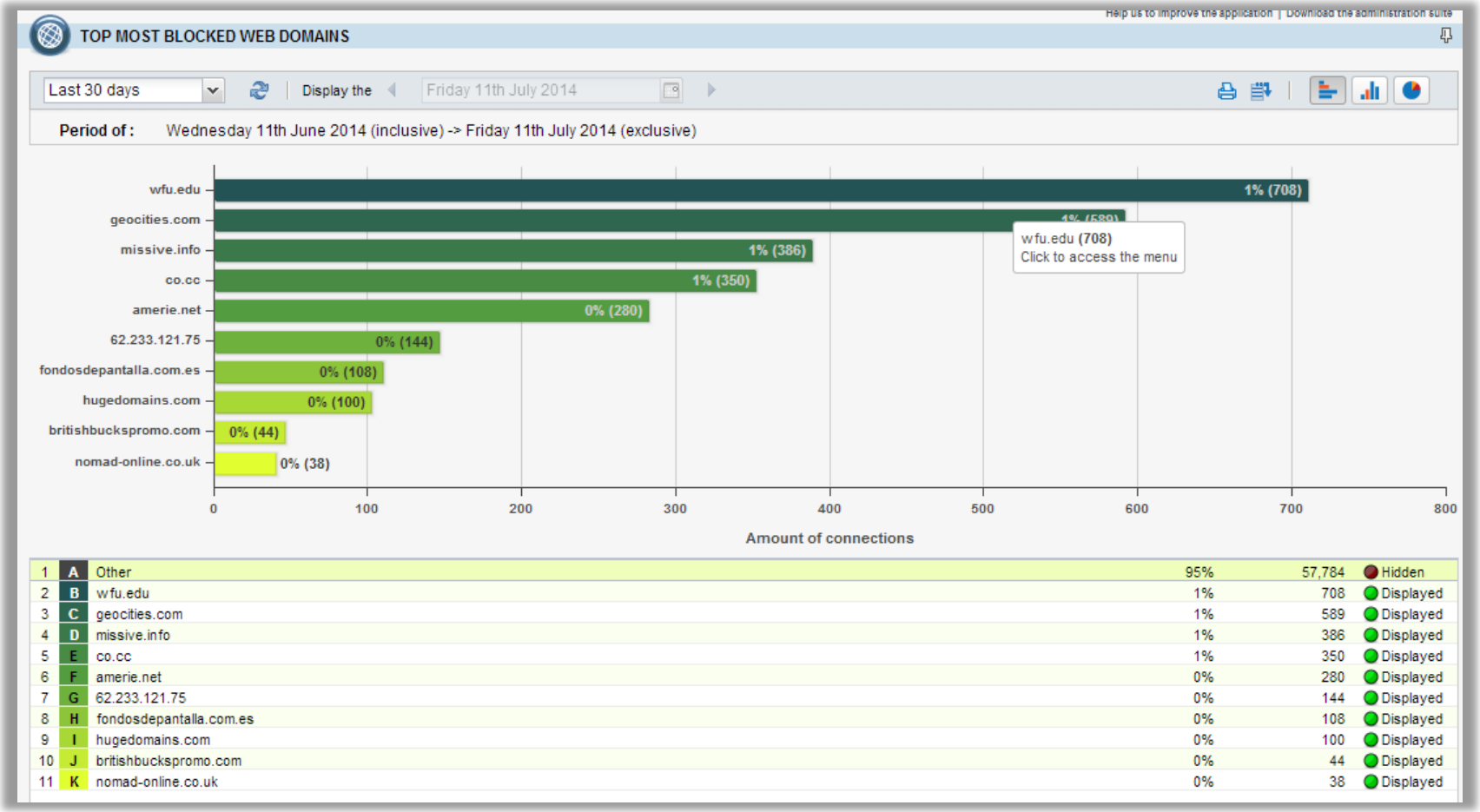
* Origin of the group if the company is a subsidiary.

Strongly dependant on US interests

POLSKI INTERFEJS UŻYTKOWNIKA

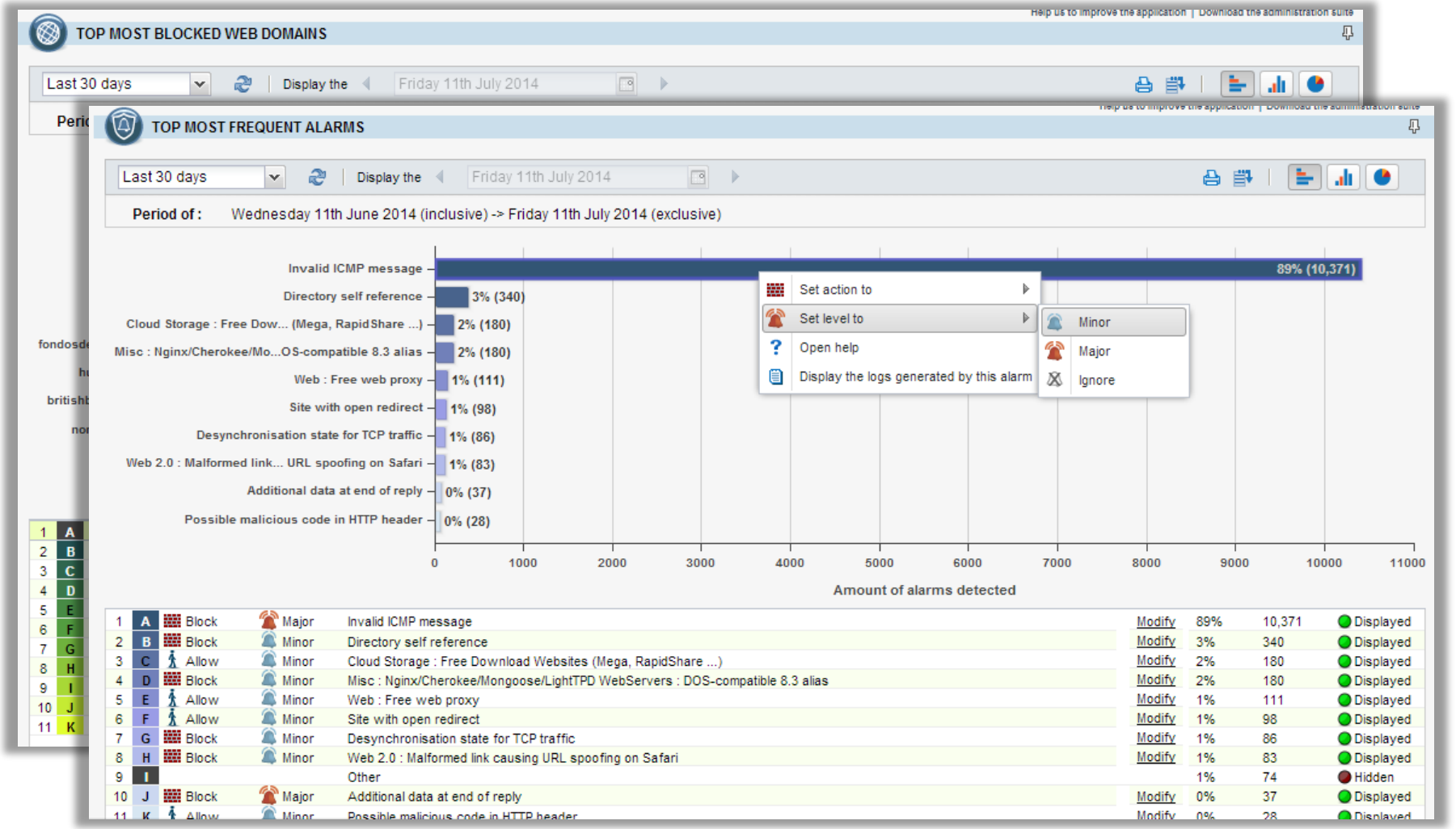


BEZPŁATNE RAPORTOWANIE



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	britishbukspromo.com	0%	44	Displayed
11	K	nomad-online.co.uk	0%	38	Displayed

BEZPŁATNE RAPORTOWANIE



AUDYT PODATNOŚCI

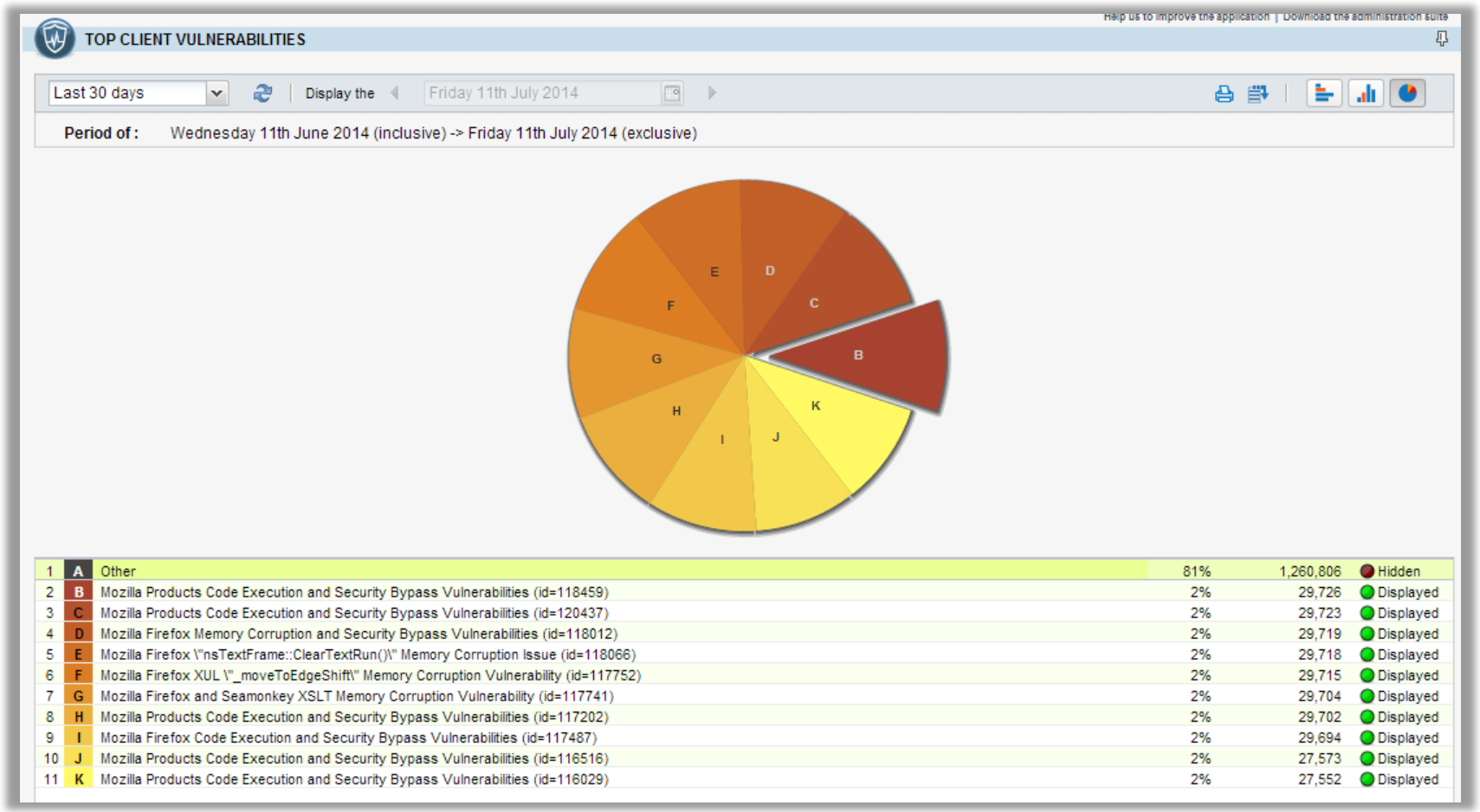
BRAK WPŁYWU NA WYDAJNOŚĆ SIECI

WYSZUKIWANIE SŁABYCH PUNKTÓW
STANOWIĄCYCH ZAGROŻENIA

SUGEROWANIE SPOSOBU ROZWIĄZANIA
WYKRYTYCH PODATNOŚCI

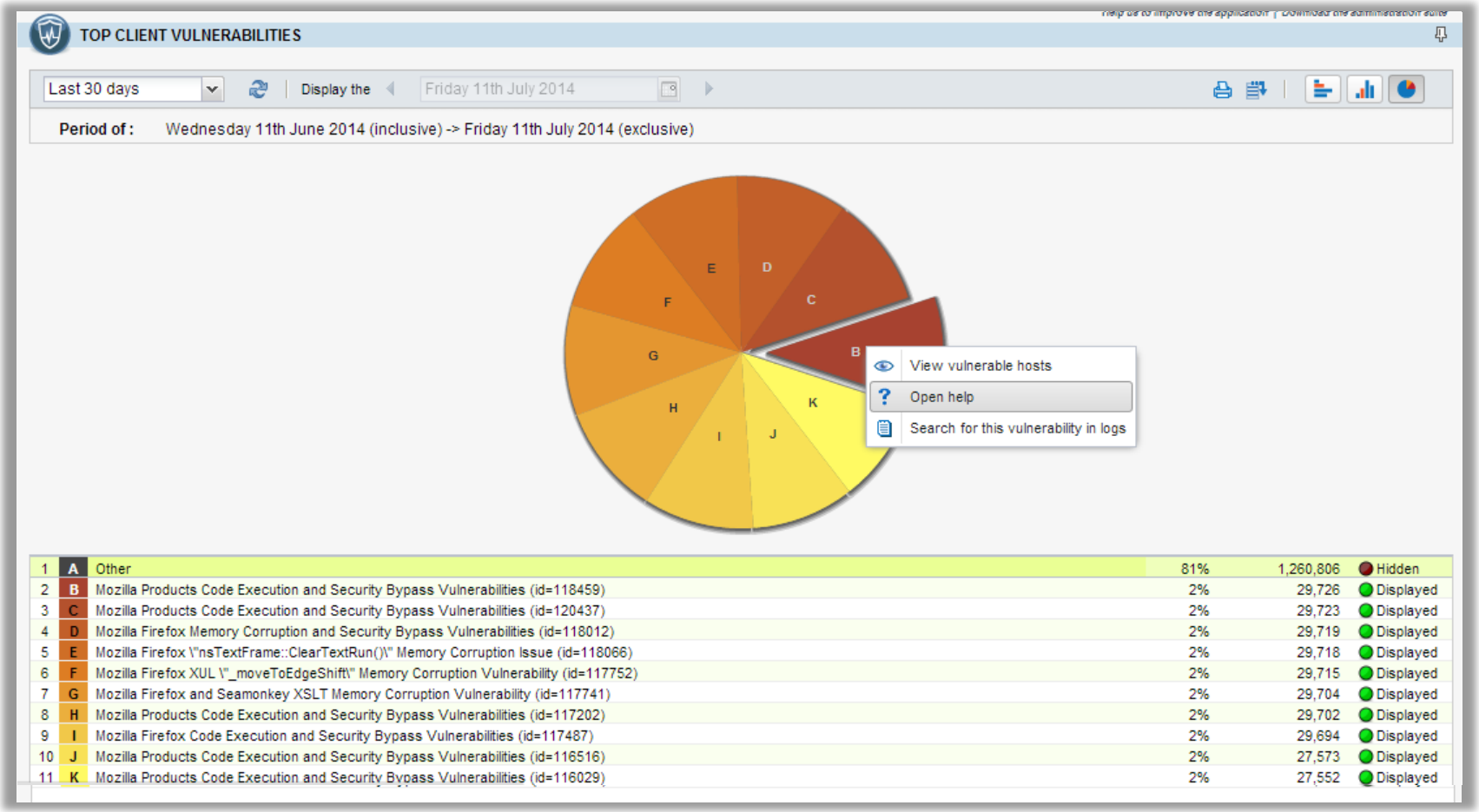
WYKRYWANIE NIEDOZWOLONEGO RUCHU

ANALIZA RYZYKA



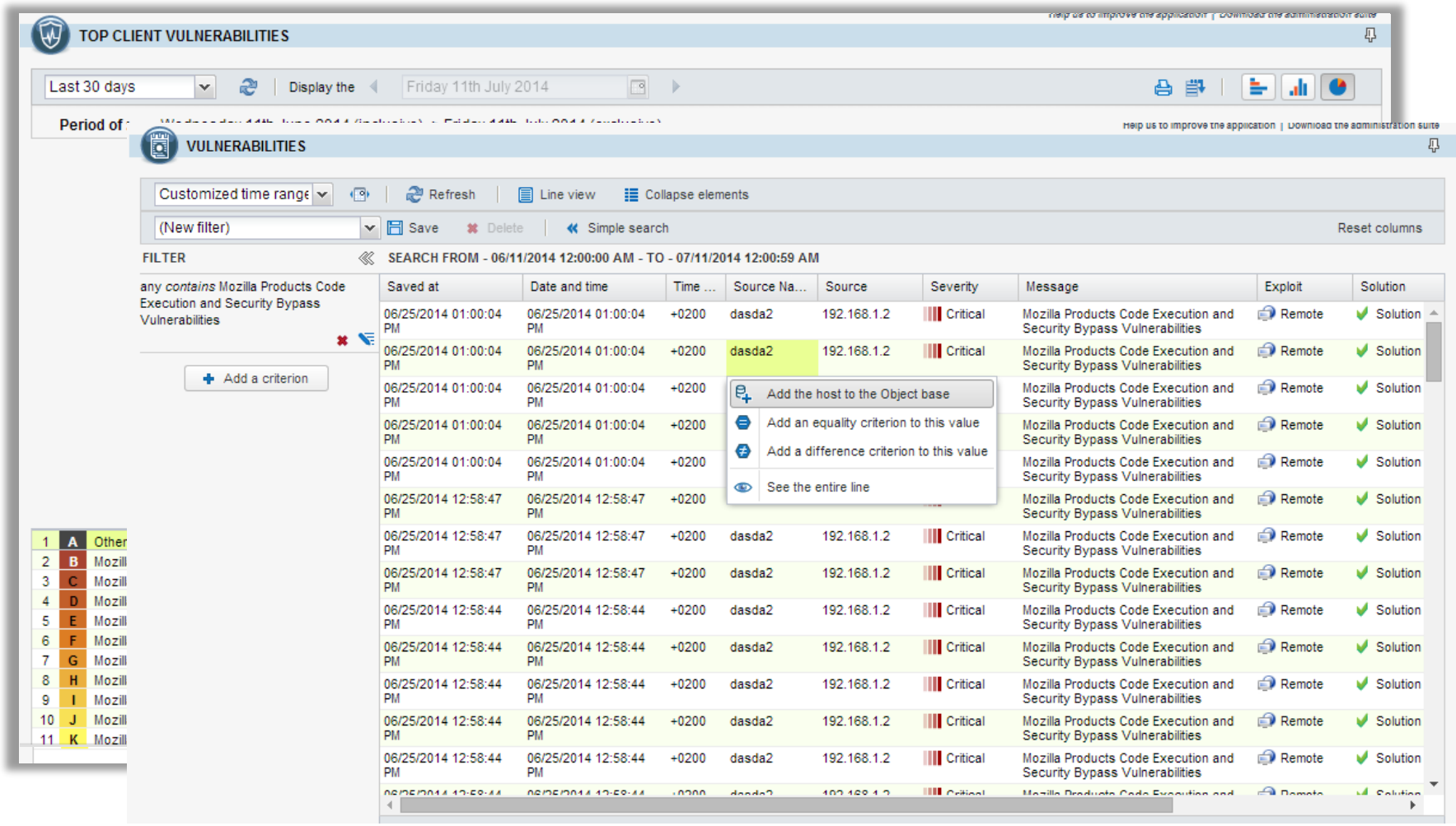
1	A	Other	81%	1,260,806	Hidden
2	B	Mozilla Products Code Execution and Security Bypass Vulnerabilities (id=118459)	2%	29,726	Displayed
3	C	Mozilla Products Code Execution and Security Bypass Vulnerabilities (id=120437)	2%	29,723	Displayed
4	D	Mozilla Firefox Memory Corruption and Security Bypass Vulnerabilities (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

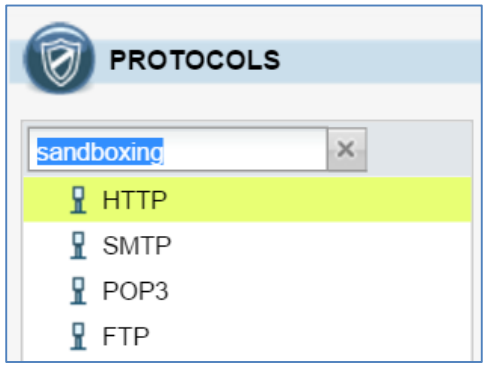


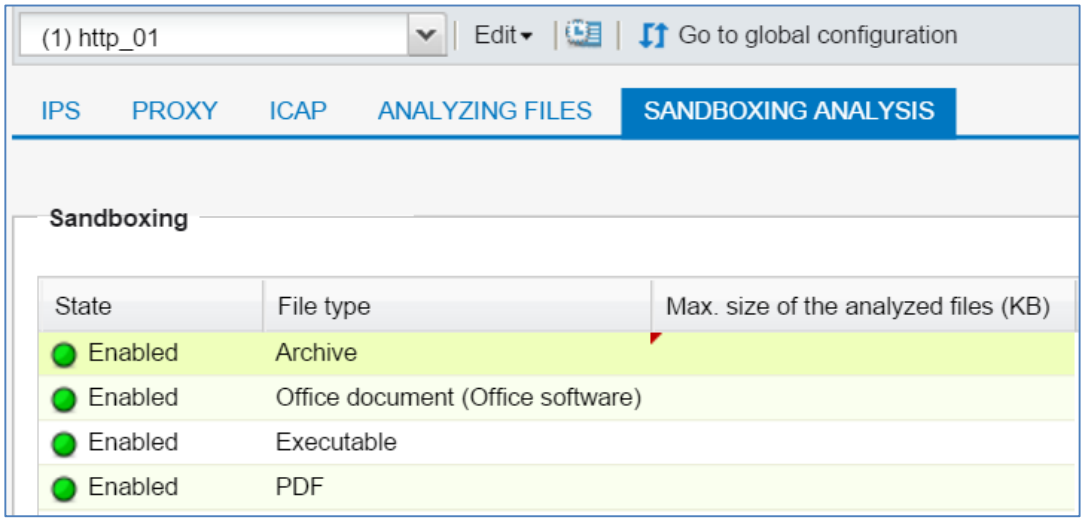
Sandboxing/Detonowanie

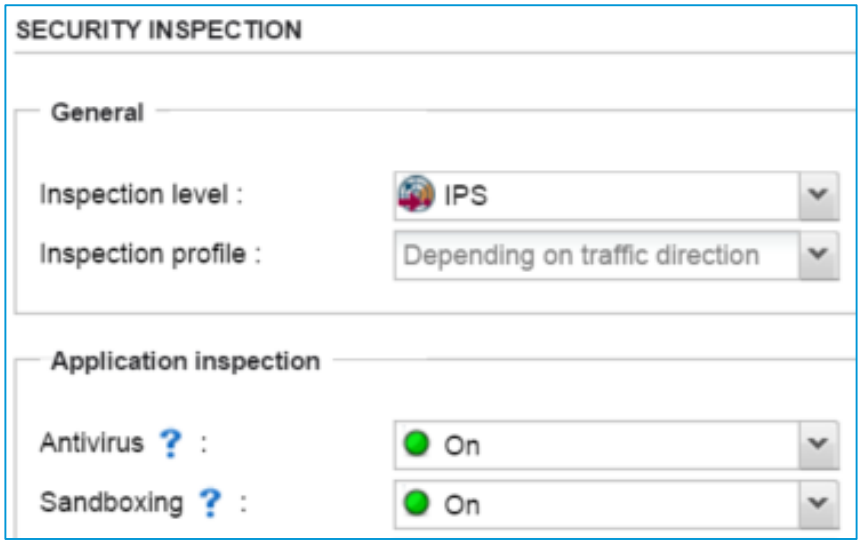
Advenced Threat Protection

Wykrywanie nieznanych obiektów w wirtualnym środowisku aby zidentyfikować sposób działania

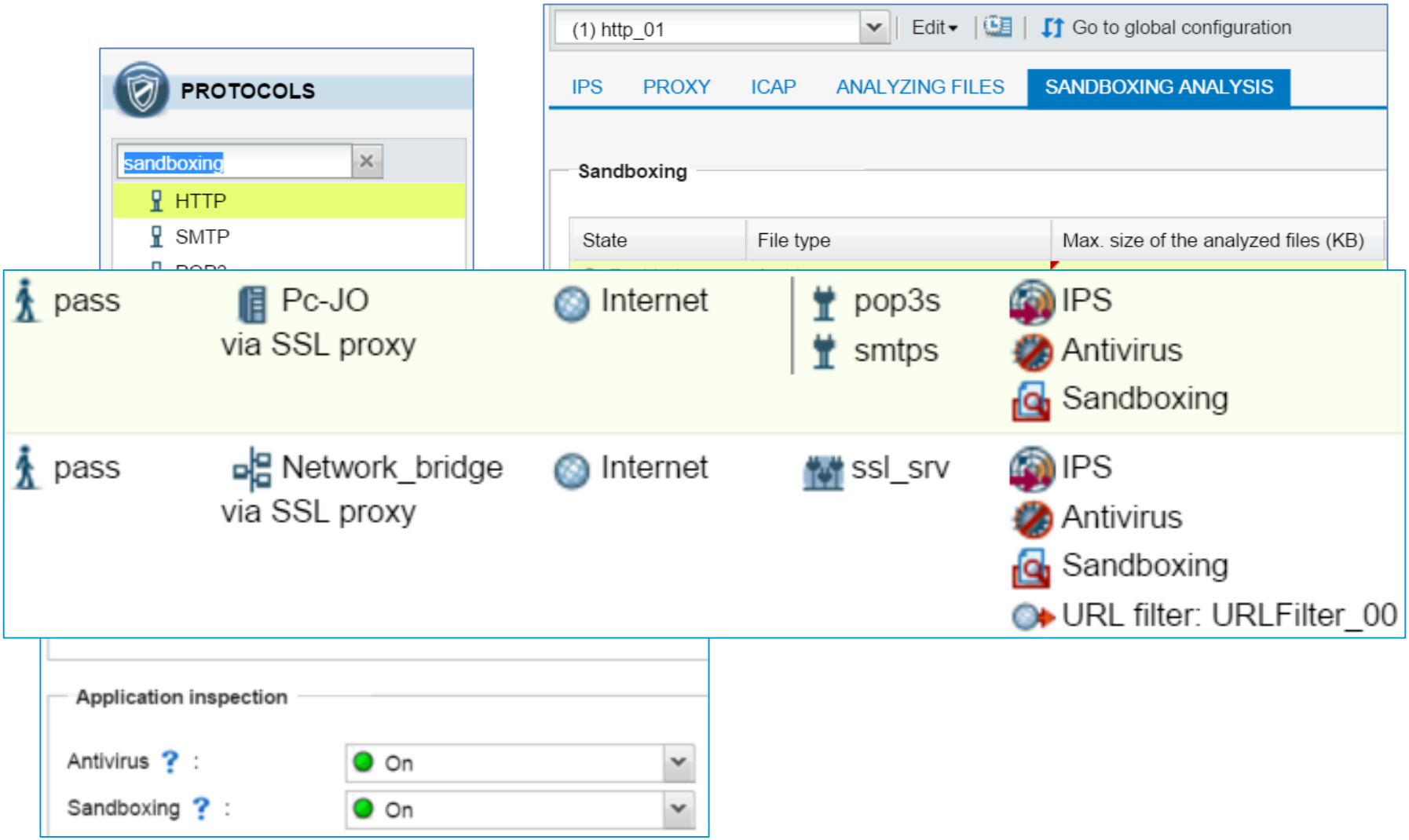
KONFIGURACJA







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

ZAPRASZAMY DO KONTAKTU