

Szanowni Państwo,

W tym roku Firma Clico obchodzi 20 lecie swojego istnienia. Od 20 lat budujemy kompetencje z zakresu najnowocześniejszych systemów i rozwiązań IT, szkolimy inżynierów i administratorów, staramy się wprowadzać na rynek polski sprawdzone i efektywne rozwiązania czołowych producentów światowych. Od 20 lat mamy przyjemność współpracować z Państwem – Naszymi



Klientami i Partnerami. Dziękujemy że byliście i jesteście z nami. Mamy nadzieję, że kolejne owocne lata współpracy są wciąż przed nami.

*Załoga Clico*

## W bieżącym wydaniu...

dr inż. Mariusz Stawowski  
Bartosz Kryński

### Praktyczne testy skuteczności dedykowanych zabezpieczeń IMPERVA Web Application Firewall

Statystyki incydentów oraz wykonywanych testów bezpieczeństwa aplikacji Web pokazują, że ponad 70% aplikacji na świecie posiada poważne błędy zagrażające bezpieczeństwu oraz reputacji firm.(...) Skuteczną ochronę dla aplikacji Web zapewnia dedykowana kategoria zabezpieczeń Web Application Firewall (WAF). System zabezpieczeń WAF bazuje w głównej mierze na automatycznie tworzonym i aktualizowanym profilu chronionej aplikacji Web. WAF „uczy się” struktury aplikacji, URL, parametrów, cookie, itp. Tworzenie profilu ma na celu niezależne odwzorowanie oczekiwanych, poprawnych zachowań użytkowników przy dostępie do aplikacji Web.

Więcej str. 2

Paweł Jakacki

### Przełączniki serii EX firmy Juniper Networks – rozwiązania pozwalające na budowę nowoczesnych sieci teleinformatycznych

Przełączniki serii EX od kilku lat cieszą się rosnącym zainteresowaniem zarówno wśród dużych operatorów teleko-

munikacyjnych jak również mniejszych firm. Rozwiązania Juniper cechują się dużą stabilnością działania, niezawodnością oraz wydajnością. Nie bez znaczenia pozostaje fakt, że produkty z rodziny EX działają w oparciu o sprawdzony, znany z ruterów, system JUNOS. Powyższe cechy rozwiązań firmy Juniper pozwalają spełnić nawet najwyższe wymagania stawiane dzisiaj systemom transmisji danych.

Więcej str. 14

### Nowości w ofercie Websense: Zabezpieczenia Web oraz Email na jednym appliance – TRITON 7.6.1

Więcej str. 16

### Centrum szkoleniowe Clico poleca nowe szkolenia Check Point oraz Juniper Networks

Więcej str. 18

dr inż. Mariusz Stawowski  
Bartosz Kryński

## Praktyczne testy skuteczności dedykowanych zabezpieczeń IMPERVA Web Application Firewall

### Wprowadzenie

Statystyki incydentów oraz wykonywanych testów bezpieczeństwa aplikacji Web pokazują, że ponad 70% aplikacji na świecie posiada poważne błędy zagrażające bezpieczeństwu oraz reputacji firm. Źle zabezpieczone witryny Web są powszechnie wykorzystane przez przestępców do dystrybucji złośliwego oprogramowania (tzw. drive-by download). Większość firm jest tego nieświadoma i łatwo pada ofiarą przestępców i złośliwych aplikacji.

Aplikacje Web tworzone są przez deweloperów na zamówienie firm w celu spełnienia ich specyficznych potrzeb. W praktyce często okazuje się, że deweloper aplikacji posiada ograniczone środki i czas oraz niewystarczające kompetencje w obszarze bezpieczeństwa. Deweloper w pierwszej kolejności koncentruje swoje działania nie na bezpieczeństwie, ale spełnieniu wymagań funkcjonalnych, czego efektem może być oddanie do użytku aplikacji posiadającej podatności. W takiej sytuacji zapewnienie bezpieczeństwa aplikacji możliwe jest poprzez zastosowanie dedykowanych zabezpieczeń Web Application Firewall (WAF) oraz zatrudnienie kompetentnego audytora\*, który zidentyfikuje podatności aplikacji a deweloper poprawi aplikację na podstawie wyników audytu.

Dla aplikacji Web zalecenia w tym zakresie zawarte są, m.in. w standardzie PCI DSS\*\*, który mówi o potrzebie stosowania zabezpieczeń Web Application Firewall. W dalszej części opracowania zostaną dokładniej omówione zasady ochrony aplikacji Web

### Dlaczego konwencjonalne zabezpieczenia nie są wystarczające?

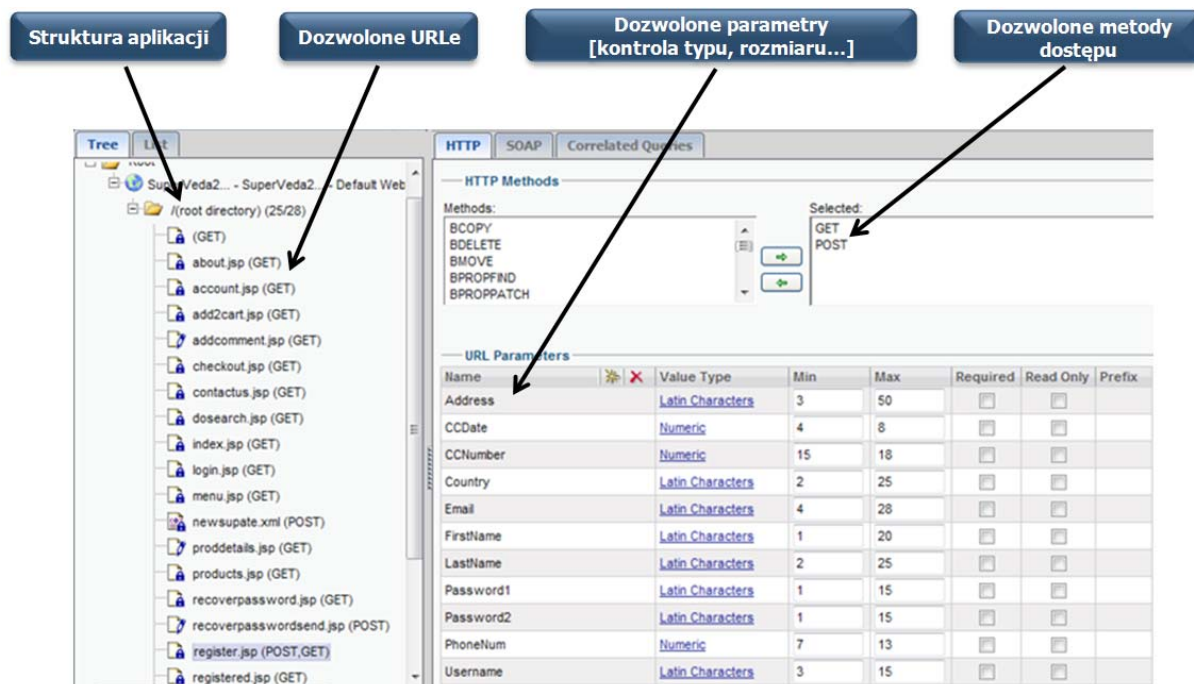
Zabezpieczenia sieciowe firewall i Intrusion Prevention System (IPS) są podstawą do tworzenia architektury bezpieczeństwa sieci (m. in. stref bezpieczeństwa) oraz przeciwdziałania wielu groźnym atakom sieciowym (m. in. exploity na serwisy sieciowe i system operacyjny, propagacja robaków sieciowych, itd.). Zapewnienie bezpieczeństwa aplikacji Web z wykorzystaniem samych konwencjonalnych zabezpieczeń firewall i IPS (w tym UTM) jest w praktyce niemożliwe. Stosują one bowiem techniki ochrony oparte o sygnatury (wzorce ataków). Aplikacje Web zwykle pisane są na zamówienie i posiadają unikalne podatności, których twórcy zabezpieczeń IPS nie znają i nie potrafią utworzyć dla nich odpowiednich sygnatur. W przypadku ochrony aplikacji Web także inne techniki (np. analiza heurystyczna, wykrywanie anomalii protokołów) stosowane przez konwencjonalne zabezpieczenia IPS nie są skuteczne. Ataki na aplikację Web dla IPS wyglądają bowiem jak legalne zapytania HTTP.

### Czym jest dedykowany Web Application Firewall?

Skuteczną ochronę dla aplikacji Web zapewnia dedykowana kategoria zabezpieczeń Web Application Firewall (WAF). System zabezpieczeń WAF bazuje w głównej mierze na automatycznie tworzonym i aktualizowanym profilu chronionej aplikacji Web. WAF „uczy się” struktury aplikacji, URL, parametrów, cookie, itp. Tworzenie profilu ma na celu niezależne odwzorowanie oczekiwanych, poprawnych zachowań użytkowników przy dostępie do aplikacji Web. *Rysunek 1* pokazuje fragment profilu aplikacji Web utrzymywanego przez zabezpieczenia WAF.

\* Więcej informacji na temat audytów bezpieczeństwa wykonywanych przez Dział Usług Profesjonalnych CLICO można znaleźć na stronie: <http://www.clico.pl/uslugi/audyt-bezpieczenstwa>

\*\* PCI Data Security Standard (PCI DSS), standard bezpieczeństwa wydany przez PCI Security Standards Council, więcej informacji: <https://www.pcisecuritystandards.org>

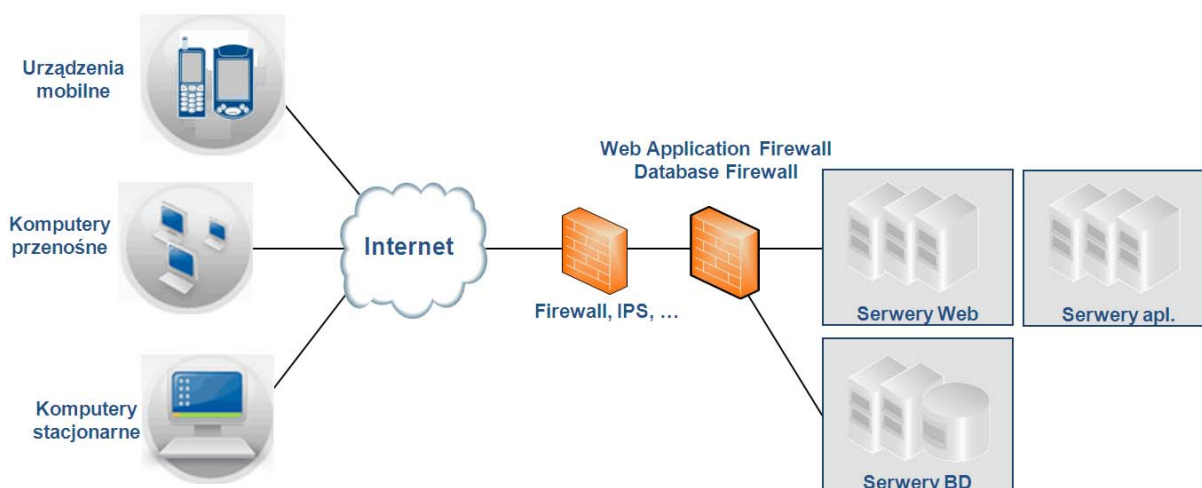


Rysunek 1. Profil ochrony aplikacji Web zbudowany przez zabezpieczenia IMPERVA WAF

Zasadnicza różnica pomiędzy zabezpieczeniami IPS i WAF polega na podejściu do kontroli ruchu sieciowego. IPS stosuje selekcję negatywną (tzw. blacklist approach) polegającą na tym, że przepuszcza cały ruch za wyjątkiem pakietów, które zostały zidentyfikowane jako niedozwolone. W konsekwencji wszystkie ataki nierozpoznane przez IPS dochodzą do aplikacji Web. WAF stosuje selekcję pozytywną (tzw. whitelist approach), polegającą na tym, że w oparciu o zbudowany profil chronionej aplikacji Web przepuszcza wyłącznie ruch, który został zidentyfikowany jako dozwolony. Dzięki temu ruch nierozpoznany jako dozwolony jest przez WAF blokowany i ataki nie dochodzą do aplikacji Web.

Wybór odpowiedniej strategii ochrony aplikacji Web jest uzależniony od specyficznych wymagań projektu (m.in. struktury aplikacji) oraz po-

siadanych już urządzeń sieci i zabezpieczeń. IMPERVA SecureSphere WAF wdrażany jest jako dedykowana warstwa ochrony aplikacji Web. W wielu portalach biznesowych i innych aplikacjach Web (np. e-commerce, e-banking) razem z aplikacją Web ochrony wymaga także baza danych, z której korzysta aplikacja. Rozwiązanie zabezpieczeń IMPERVA SecureSphere WAF w jednej platformie dostarczać może dedykowane zabezpieczenia WAF oraz Database Firewall (DBF). Całość zabezpieczeń aplikacji Web i baz danych zarządzana jest z przeznaczanego tylko do tego celu systemu zarządzania, wyposażonego w odpowiednie narzędzia monitorowania i raportowania IMPERVA Management Server. Koncepcja wdrożenia zabezpieczeń IMPERVA WAF w takiej architekturze została przedstawiona na Rysunku 2.



Rysunek 2. IMPERVA WAF jako dedykowana warstwa ochrony aplikacji Web

## Jak rzeczywiście zabezpieczenia chronią aplikację Web?

W celu dokładniejszego zweryfikowania możliwości zabezpieczeń IPS i WAF w zakresie ochrony aplikacji Web zostały wykonane ataki na testową aplikację Web, wykorzystujące rzeczywiste błędy tej aplikacji. Do testów zostało użyte rozwiązanie WAF firmy IMPERVA oraz rozwiązanie IPS jednego z wiodących światowych producentów zabezpieczeń (włączone wszystkie dostępne techniki detekcji i sygnatury).

W trakcie testów zostały wykonane następujące ataki na aplikację Web:

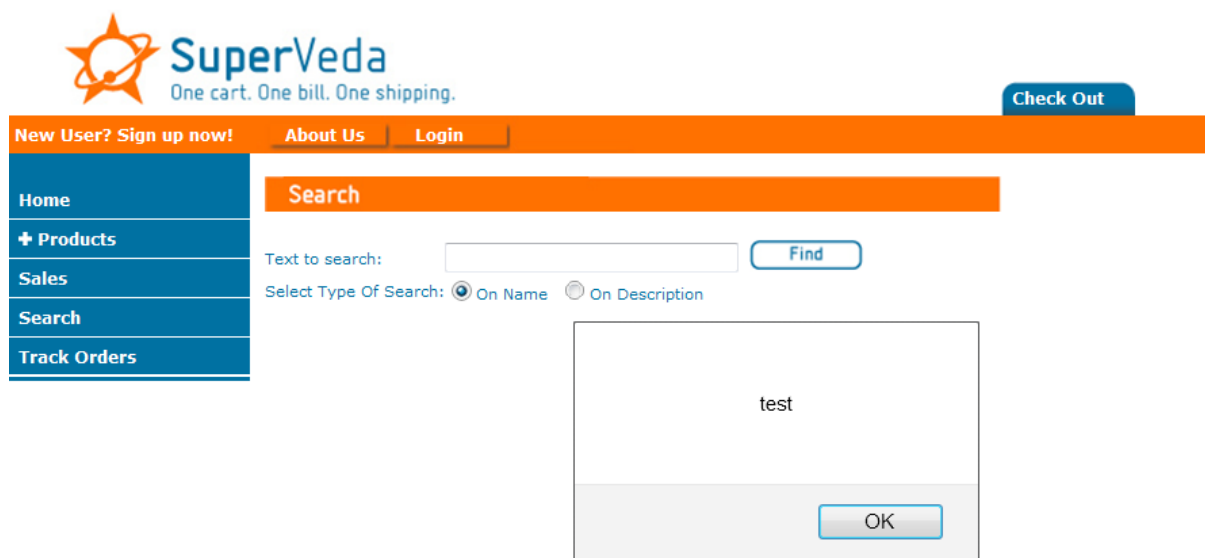
1. Prosty XSS Reflected

2. XSS Reflected z kodowaniem znaków
3. Prosty XSS Stored
4. XSS Stored z kodowaniem znaków
5. Prosty SQL-Injection
6. SQL-Injection z kombinacją zapytania SQL
7. Manipulacja cookie aplikacji Web
8. Forceful Browsing
9. Information Leakage

Podobne testy wykonaliśmy także dla zabezpieczeń F5 ASM. Ich wyniki dostępne są w opracowaniu: <http://www.clico.pl/edukacja/artykuly/web-ochrona>

### Test 1. Prosty atak XSS Reflected

`/dosearch.asp?string=<script>alert("test")<%2Fscript>&Type=Name&submit.x=47`



#### 1a. Reakcja IPS

– IPS wykrywa elementy skryptu w parametrze URL, brak dokładniejszych danych.

Category	Predefined
Subcategory	HTTP: HTML Script Tag Embedded in URL Parameters
Severity	Major
Device	IPS

#### 1b. Reakcja WAF

– WAF wykrywa i pokazuje nielegalną wartość i rozmiar parametru w URL.

5010	⊖	⚠	15:12:28	1	Parameter Type Violation string in 192.168.53.90/dosearch.asp
5009	⊖	⚠	15:12:14	4	Parameter Value Length Violation string in 192.168.53.90/dosearch.asp
5008	⊖	⚠	15:06:29	4	Multiple XSS - Basic-5 from 192.168.53.2
5002	⊖	⚠	15:04:31	41	Distributed XSS - Basic-5(+)
5004	⊖	⚠	14:56:23	19	Multiple Cross-site scripting from 192.168.53.2

– Administrator WAF może dokładnie przeanalizować zapytanie, posiadając cenne informacje o źródle ataku, jak nazwa uwierzytelnionego użytkownika oraz dodatkowe dane na jego te-

mat (pobrane np. z Active Directory, LDAP, bazy danych czy systemu Human Resources) jak nazwisko, nr. telefonu czy departament do którego przynależy.

Event 5840109955721461989: Parameter Value Length Violation

Key	Value
Violation Description	Parameter Value Length Violation string in 192.168.53.90/dosearch.asp
Violated Item	Parameter: string, URL: /dosearch.asp

Event Details:

Event Time	Gateway	
April 20, 2011 3:22:34 PM	Prima	
Server Group	Service	Application
SuperVeda WWW	www	Default Web Application
Host	Connection	
192.168.53.90	192.168.53.2:63125 → 192.168.53.90:80	
User	Session	
bugsb	5809402039066689539 14:44:34	
Response Code	Response Size	Response Time
	N/A Bytes	N/A msec.

```
GET /dosearch.asp ? string=<script>alert("XSS")</script> & Type=Name & submit.x=47 & submit.y=6 HTTP/1.1
Host: 192.168.53.90
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:5.0) Gecko/20100101 Firefox/5.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: pl,en-us;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Accept-Charset: ISO-8859-2,utf-8;q=0.7,*;q=0.7
Connection: keep-alive
Cookie: ASPSESSIONIDQRRASSD=HGADJOFCLNDHDFKLCGNOCM;Privileges=None
```

File Name	Value	Origin
submit.y	6	Query String
string	<script>alert("XSS")</script>	Query String
submit.x	47	Query String
Type	Name	Query String

File Name	Value
Privileges	None
ASPSESSIONIDQRRASSD	HGADJOFCLNDHDFKLCGNOCM

User Defined Field	Value
FirstName	Bartek
Dept	ProfessionalServicesClico
LastName	Krynski
Mobile	663921549

Event 5474749543255900240: Parameter Value Length Violation

Key	Value
Violation Type	http
Severity	Low
Policy Name	Web Profile Policy
Alert Number	7007
Violation Description	Parameter Value Length Violation string in 192.168.53.90/dosearch.asp
Violated Item	Parameter: string, URL: /dosearch.asp
Immediate Action	Block
Violation Type	Max
Parameter Name	string
Size	29
Limit	7

- nielegalny typ danych wejściowych,

Event 5474749543255900240: Parameter Type Violation

Key	Value
Violation Type	http
Severity	Medium
Policy Name	Web Profile Policy
Alert Number	7005
Violation Description	Parameter Type Violation string in 192.168.53.90/dosearch.asp
Violated Item	Parameter Type Violation
Immediate Action	Block
Parameter Name	string
Parameter Value	<script>alert("XSS")</script> ;
Unexpected Groups	Double Quote, Parenthesis, Angled Brackets, Slash

- identyfikacja ataku poprzez sygnatury,

Event 5840109955721461957: Signature Violation

Key	Value
Violation Description	XSS - Basic-5
Violated Item	Location: parameters, Position: 8

W razie potrzeby administrator WAF może do-  
 stroić wyuczony profil z poziomu konsoli logów lub  
 w samym profilu.

Event 5840109955721461989: Parameter Value Length Violation

Key	Value
Violation Description	Parameter Value Length Violation string in 192.168.53.90/dosearch.asp
Violated Item	Parameter: string, URL: /dosearch.asp

- Administrator WAF może dokładnie przeanalizować powody zablokowania zapytania URL.
- nielegalna wielkość danych wejściowych,

URL Parameters

Name	Value Type	Min	Max	Required	Read Only	Prefix
Type	Latin Characters	0	1000	<input type="checkbox"/>	<input type="checkbox"/>	
string	Foreign Language Characters (UTF-8)	0	7	<input type="checkbox"/>	<input type="checkbox"/>	
submit.x	Numeric					
submit.y	Numeric					

Configure Value Type:

Custom Value Type:

Primary Value Type: Foreign Language Characters (UTF-8)

Additional Allowed Character Groups:

<input type="checkbox"/> Semicolon ;	<input type="checkbox"/> Dash -
<input type="checkbox"/> Ampersand &	<input type="checkbox"/> Others # \$ : @ ^ _
<input type="checkbox"/> Null [NULL]	<input type="checkbox"/> Concatenation
<input type="checkbox"/> Plus Sign +	<input type="checkbox"/> Period .
<input type="checkbox"/> Double Quote "	<input type="checkbox"/> Asterisk *
<input type="checkbox"/> Comma ,	<input type="checkbox"/> OS Related Separators ! ~
<input type="checkbox"/> Parenthesis ()	<input type="checkbox"/> Brackets [] {}
<input type="checkbox"/> Percent Sign %	<input type="checkbox"/> HTTP Query String Separators = ?
<input type="checkbox"/> Angled Brackets > <	<input type="checkbox"/> ASCII Control Characters
<input type="checkbox"/> Slash \ /	<input type="checkbox"/> Quote ' "



### Test 3. Prosty XSS Stored

- W formularzu rejestracyjnym Web w nazwie użytkownika wpisujemy kod wyświetlany następnie przy każdorazowym uwierzytelnieniu użytkownika.

#### Register User

<b>First Name:</b>	<input type="text" value="&lt;script&gt;alert(document.c"/>
<b>Last Name:</b>	<input type="text" value="test"/>
<b>Address:</b>	<input type="text" value="test"/>
<b>Country:</b>	<input type="text" value="Afghanistan"/>
<b>Email:</b>	<input type="text" value="test@wp.pl"/>
<b>Phone Number:</b>	<input type="text" value="123"/>
<b>Username:</b>	<input type="text" value="testowy"/>
<b>Password:</b>	<input type="password" value="••••"/>
<b>Re-Enter Password (for verification):</b>	<input type="password" value="••••"/>
<b>Credit Card Number:</b>	<input type="text" value="1234567890987654"/>
<b>Credit Card Expiration Date: (MM/YY)</b>	<input type="text" value="12/12"/>

- W efekcie po zalogowaniu użytkownikowi aplikacji Web wyświetla się wartość jego cookie.



#### 3a. Reakcja IPS

Nie wykrywa ataku.

#### 3b. Reakcja WAF

- WAF wykrywa nielegalną zawartość zapytania URL.

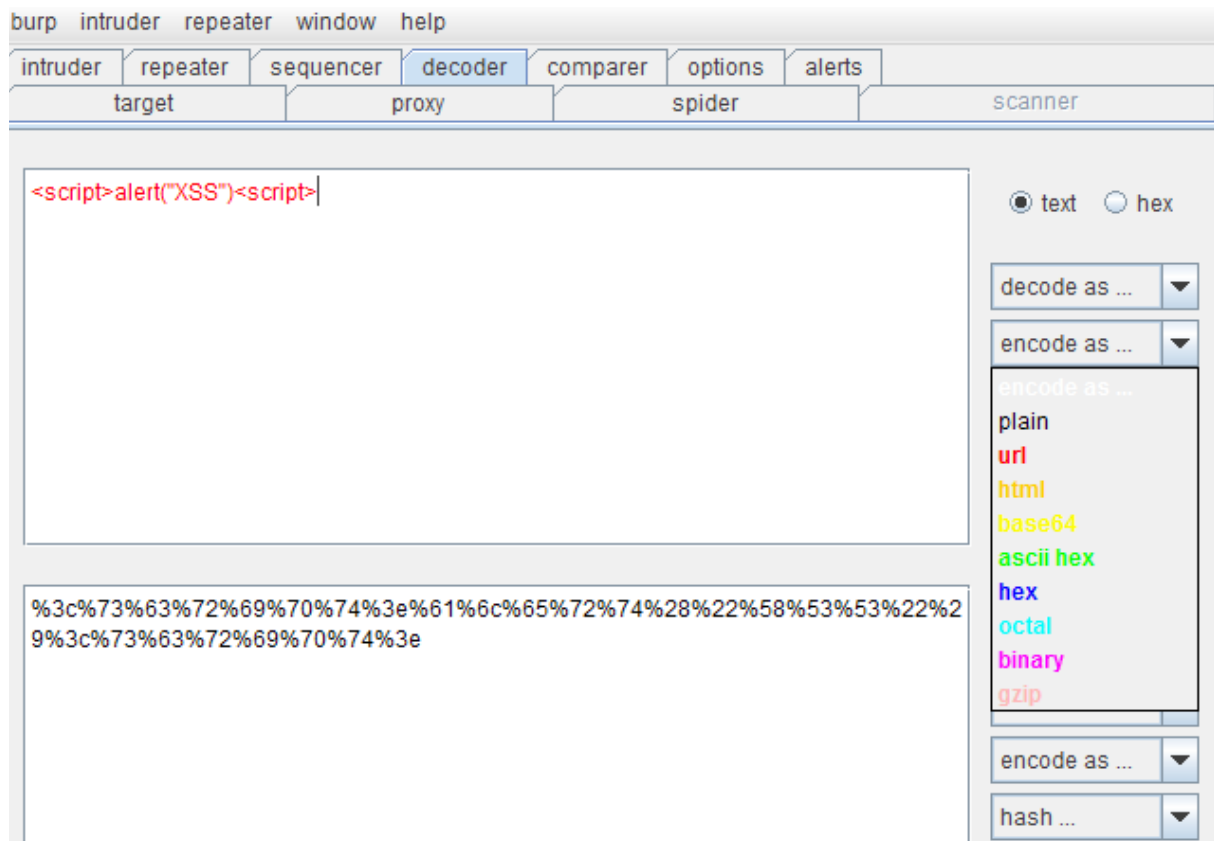
7003	⊖	🔴	10:49:21	9	Cross-site scripting from 192.168.53.2 in /register.asp - FirstName
7002		🟡	10:49:21	9	Unauthorized Method POST for 192.168.53.90/register.asp
7001		🔴	10:49:21	42	Multiple XSS - Basic-5 from 192.168.53.2
7004		🟡	10:49:00	6	Suspicious Response Code

- Dodatkowo WAF posiada funkcje maskowania danych dotyczących klientów, zatem nazwy użytkowników, hasła etc. mogą być zamaskowane w logach.

Event 5474749543255900205: Cross-site scripting !   *e	
Key	Value
<b>Violation Description</b>	Cross-site scripting on parameter FirstName in 192.168.53.90/register.asp
<b>Violated Item</b>	URL: /register.asp
<b>Event Details:</b>	
Event Time: April 21, 2011 10:49:21 AM	
Gateway: Prima	
Server Group: SuperVeda WWW	Service: www
Application: Default Web Application	
Host: 192.168.53.90	Connection: 192.168.53.2:54612 → 192.168.53.90:80
User:	Session: 3969847733505753090 10:39:45
Response Code: 200	Response Size: 2789 Bytes
Response Time: 10 msec.	
<pre>POST /register.asp ? mode=adduser HTTP/1.1 Host: 192.168.53.90 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:5.0) Gecko/20100101 Firefox/5.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: pl,en-us;q=0.7,en;q=0.3 Accept-Encoding: gzip, deflate Accept-Charset: ISO-8859-2,utf-8;q=0.7,*;q=0.7 Connection: keep-alive Referer: http://192.168.53.90/register.asp?mode=newuser Cookie: ASPSESSIONIDQSATTQCR=EPOJLCPDLMPKOPPHOHAIIIQI Content-Type: application/x-www-form-urlencoded Content-Length: 221 FirstName=***** LastName=**** Address=test Country=N1 Email=***** PhoneNum=123 Username=***** Password1=test Password2=test CCNumber=***** CCDate=12/12</pre>	

#### Test 4. XSS Stored z kodowaniem znaków

- Skrypt kodujemy jako URL, następnie modyfikujemy wpisaną przez użytkownika wartość First Name w Proxy:



#### 4a. Reakcja IPS

Nie wykrywa ataku.

#### 4b. Reakcja WAF

- Wykrywa atak i pokazuje zastosowane kodowanie /jak dla poprzedniego ataku/ dodatkowo wskazując inne podejrzane aktywności, jak nieoczekiwana metoda http (wykonana przez intercepting proxy) oraz podejrzana odpowiedź serwera.

Last Hour (7)					
7004			11:39:55	10	Suspicious Response Code
7002			11:39:55	16	Distributed Unauthorized Method for Known URL on 192.168.53.90/register.asp
7003	⊖	⊖	11:07:53	10	Distributed Cross-site scripting in /register.asp - FirstName

#### Test 5. Prosty SQL-Injection

Wprowadzamy zapytanie SQL w pole logowania aplikacji Web i uzyskujemy nieupoważniony dostęp do aplikacji.

#### 5a. Reakcja IPS

- IPS wykrywa atak SQL-Injection w URL, brak dokładniejszych informacji o ataku.

Category	Predefined
Subcategory	HTTP: SQL Injection In URL
Severity	Major
Device	IPS

#### 5b. Reakcja WAF

- Wykrywa atak i pokazuje szczegółowe informacje na jego temat /jak dla poprzednich ataków/.

No.			Updated	#	Alert Description
Last Hour (5)					
7009	⊖	⊖	12:05:39	1	SQL injection on parameter username in 192.168.53.90/login.asp
7008	⊖	⊖	12:05:39	1	Parameter Type Violation username in 192.168.53.90/login.asp

Key	Value
Violation Type	http
Severity	High
Policy Name	Web Correlation Policy
Alert Number	7009
Violation Description	SQL injection on parameter username in 192.168.53.90/login.asp
Violated Item	URL: /login.asp
Immediate Action	Block
Input Type	parameter
Parameter Name	username
Parameter Value	*****

Event Details:	
Event Time	April 21, 2011 12:05:38 PM
Gateway	Prima
Server Group	SuperVeda WWW
Service	www
Application	Default Web Application
Host	192.168.53.90
Connection	192.168.53.2:55492 → 192.168.53.90:80
User	' OR ''='
Session	3969847733505753095 12:05:29

## Test 6. SQL-Injection z kombinacją zapytania SQL

Wprowadzamy zapytanie SQL w zmodyfikowanej formie (np. OR a=a, b=b, 1000=1000, etc).

### 6a. Reakcja IPS

Nie wykrywa ataku.

### 6b. Reakcja WAF

- Wykrywa atak i pokazuje szczegółowe informacje na jego temat /jak dla poprzednich ataków/ przy wykorzystaniu wielu reguł polityki bezpieczeństwa.

7009	⊖	█	12:09:45	5	Distributed SQL injection in /login.asp - username
7011	⊖	█	12:09:45	3	Parameter Value Length Violation password in 192.168.53.90/login.asp
7008	⊖	█	12:09:45	5	Parameter Type Violation username in 192.168.53.90/login.asp

## Test 7. Manipulacja cookie aplikacji Web

Przechwytnijemy odpowiedź do aplikacji Web i modyfikujemy rolę użytkownika.

- Modyfikujemy wartość cookie z None na na Discount.

raw	params	headers	hex
GET request to /add2cart.asp			
type	name	value	
URL	ProdID	6	
URL	sale	no	
cookie	ASPSESSIONIDQSA...	PPOJLCPDIJMDGNJOAEDDMBBL	
cookie	Privileges	Discount	

- W efekcie otrzymujemy dodatkową zniżkę na produkt w wysokości 10%.

```

Products Total:  $91.85
Shipping:      $0
Discount (10%): $9.185
=====
Total:         $82.665
  
```

W analogiczny sposób wykorzystać można podatność aplikacji, która nie weryfikuje wartości przekazywanych w ukrytym dla przeglądarki parametrze Discount, poprzez proxy przechwytyjące intruz jest w stanie podmieniać wartość parametru dzięki czemu uzyska odpowiednie zniżki.

### 7a. Reakcja IPS

Nie wykrywa ataku.

**7b. Reakcja WAF**

- Wykrywa atak Cookie Tampering i pokazuje szczegółowe informacje na jego temat /jak dla poprzednich ataków/.

Event 5474749543255900807: Cookie Tampering

Key	Value
Violation Type	http
Severity	Medium
Policy Name	Web Profile Policy
Alert Number	7014
Violation Description	Cookie Tampering on cookie Privileges: Expected NA, Observed Discount
Violated Item	Cookie: Privileges
Immediate Action	None
Cookie Name	Privileges
Observed Value	Discount
Allowed Value	NA

```
GET /add2cart.asp ? ProdID=13 & sale=no HTTP/1.1
Accept: */*
Accept-Language: pl-PL
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C)
Accept-Encoding: gzip, deflate
Proxy-Connection: Keep-Alive
Host: 192.168.53.90
Cookie: ASPSESSIONIDQSATTQCR=PPOJLCPDIJMDGNJOAEDDMBBL;Privileges=Discount
```

**Parameters:**

File Name	Value	Origin
sale	no	Query String
ProdID	13	Query String

**Cookies:**

File Name	Value
ASPSESSIONIDQSATTQCR	PPOJLCPDIJMDGNJOAEDDMBBL
Privileges	Discount

**Enrichment Data:**

User Defined Field	Value
FirstName	Bartek
Mobile	663921549
LastName	Krynski
Dept	ProfessionalServicesClico

**Test 8. Forceful Browsing**

Bez logowania do aplikacji wywołujemy URL strony z konfiguracją aplikacji /includes/config.inc.php.old

**8a. Reakcja IPS**

Nie wykrywa ataku.

**8b. Reakcja WAF**

- Wykrywa atak i pokazuje szczegółowe informacje na jego temat /jak dla poprzednich ataków/.

Last Hour (4)

7016		13:35:59	1	Unauthorized URL Access to 192.168.53.90/includes/config.inc.php.old
7015		13:35:58	1	Efone Config.INC Information Disclosure attempt

## Test 9. Wyciek poufnych danych (Information Leakage)

Odczyt numerów kart kredytowych z bazy danych za pomocą ataku SQL Injection w formularzu wyszukiwania:

**, UNION SELECT 1,1,CCNumber,'1',1,1,'1' from users where ,%=''**

Zwrotnie oprócz poszukiwanych produktów intruzowi zwracane są numery kredytowe wszystkich zarejestrowanych klientów.

Text to search:

Select Type Of Search:  On Name  On Description

1234123412341234

1234567890987654

214999060738825

3337330229108020

4111111111111111

5431111111111110

869910717225031

### 9a. Reakcja IPS

Nie wykrywa ataku.

### 9b. Reakcja WAF

- WAF identyfikuje numery kart kredytowych poprzez zdefiniowane wyrażenia regularne, dodatkowo posiadając funkcję weryfikacji poprzez algorytm Luhn.

Display Name	Type	Pattern	Elements without Masking
Visa Short Credit Card Numbers - 1	Advanced	part="400", rgxp="([0-9]{4})([0-9]{3})([0-9]{3})([0-9]{4})"	\$1.\$3.\$5.\$7.\$8.\$9
Visa Short Credit Card Numbers - 100	Advanced	part="409", rgxp="([0-9]{4})([0-9]{3})([0-9]{3})([0-9]{4})"	\$1.\$3.\$5.\$7.\$8.\$9
Visa Short Credit Card Numbers - 10	Advanced	part="499", rgxp="([0-9]{4})([0-9]{3})([0-9]{3})([0-9]{4})"	\$1.\$3.\$5.\$7.\$8.\$9
Visa Short Credit Card Numbers - 11	Advanced	part="410", rgxp="([0-9]{4})([0-9]{3})([0-9]{3})([0-9]{4})"	\$1.\$3.\$5.\$7.\$8.\$9
Visa Short Credit Card Numbers - 12	Advanced	part="411", rgxp="([0-9]{4})([0-9]{3})([0-9]{3})([0-9]{4})"	\$1.\$3.\$5.\$7.\$8.\$9

WAF wykrywa atak oraz pokazuje szczegółowe informacje na jego temat /jak dla poprzednich ataków/. Dodatkowo, jeśli WAF wdrożony jest w trybie reverse proxy posiada możliwość maskowania informacji wrażliwych.

Key	Value
Violation Description	Data Leakage - Visa, Long Credit Card Numbers
Violated Item	Custom Violation

Event Details:

Event Time	Gateway
April 21, 2011 1:53:37 PM	Prima

Server Group	Service	Application
SuperVeda WWW	www	Default Web Application

Host	Connection
192.168.53.90	192.168.53.2:61706 → 192.168.53.90:80

User	Session
bugsb	3969847733505753103 13:35:57

Response Code	Response Size	Response Time
200	12489 Bytes	4 msec.

GET /dosearch.asp ? string=' UNION SELECT 1,1,CCNumber,'1',1,1,'1' from users where '%=' & submit.x=60 & submit.y=14 & Type=Name HTTP/1.1

Host: 192.168.53.90

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:5.0) Gecko/20100101 Firefox/5.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Language: pl,en-us;q=0.7,en;q=0.3

Accept-Encoding: gzip, deflate

Accept-Charset: ISO-8859-2,utf-8;q=0.7,\*;q=0.7

Connection: keep-alive

Referer: http://192.168.53.90/search.htm

Cookie: ASPSESSIONIDQSATTQCR=EPOJLCPDLMKOPPNHOAIIIOI;Privileges=None

Poniżej zamieszczona tabelka przedstawia podsumowanie testów skuteczności zabezpieczeń IPS i WAF przed atakami na aplikację Web.

Lp.	Atak na aplikację Web	IPS	WAF
1.	Prosty XSS Reflected	<ul style="list-style-type: none"> <li>Atak wykryty jako skrypt w parametrze URL</li> <li>Brak dokładniejszych informacji o ataku</li> </ul>	<ul style="list-style-type: none"> <li>Wykryta nielegalna wartość parametru HTTP GET</li> <li>Szczegółowe informacje o ataku</li> </ul>
2.	XSS Reflected z kodowaniem znaków	<ul style="list-style-type: none"> <li>Nie wykrywa ataku<sup>1</sup></li> </ul>	<ul style="list-style-type: none"> <li>Wykryta nielegalna wartość parametru URL</li> <li>Szczegółowe informacje o ataku, w tym pokazuje zastosowane kodowanie</li> </ul>
3.	Prosty XSS Stored	<ul style="list-style-type: none"> <li>Nie wykrywa ataku</li> </ul>	<ul style="list-style-type: none"> <li>Wykryta nielegalna zawartość zapytania HTTP POST</li> <li>Szczegółowe informacje o ataku</li> </ul>
4.	XSS Stored z kodowaniem znaków	<ul style="list-style-type: none"> <li>Nie wykrywa ataku</li> </ul>	<ul style="list-style-type: none"> <li>Wykryta nielegalna zawartość zapytania HTTP POST</li> <li>Szczegółowe informacje o ataku, w tym pokazuje zastosowane kodowanie</li> </ul>
5.	Prosty SQL-Injection	<ul style="list-style-type: none"> <li>Wykryty atak SQL-Injection w URL</li> <li>Brak dokładniejszych informacji o ataku</li> </ul>	<ul style="list-style-type: none"> <li>Wykryta nielegalna wartość parametru HTTP GET</li> <li>Szczegółowe informacje o ataku</li> </ul>
6.	SQL-Injection z kombinacją zapytania SQL	<ul style="list-style-type: none"> <li>Nie wykrywa ataku</li> </ul>	<ul style="list-style-type: none"> <li>Wykryta nielegalna wartość parametru HTTP GET</li> <li>Szczegółowe informacje o ataku</li> </ul>
7.	Manipulacja Cookie aplikacji Web	<ul style="list-style-type: none"> <li>Nie wykrywa ataku</li> </ul>	<ul style="list-style-type: none"> <li>Wykryta nielegalną wartość cookie</li> <li>Szczegółowe informacje o ataku</li> </ul>
8.	Forceful browsing	<ul style="list-style-type: none"> <li>Nie wykrywa ataku</li> </ul>	<ul style="list-style-type: none"> <li>Wykrywa dostęp do nieznanego URL</li> </ul>
9.	Wyciek informacji (Information Leakage)	<ul style="list-style-type: none"> <li>Nie wykrywa ataku</li> </ul>	<ul style="list-style-type: none"> <li>Identyfikuje atak i maskuje poufne dane</li> </ul>

W niniejszych testach zostały wykorzystane najbardziej popularne i proste do wykonania ataki. Aplikacje Web mogą zostać poddane wielu innym atakom, dla których konwencjonalne zabezpieczenia (FW, IPS, UTM) także nie stanowią zabezpieczenia, m.in.: Cross Site Request Forgery (CSRF), nielegalny dostęp do plików i danych serwera Web (enumeracja plików), cookie poisoning, manipulacja ukrytych pól.

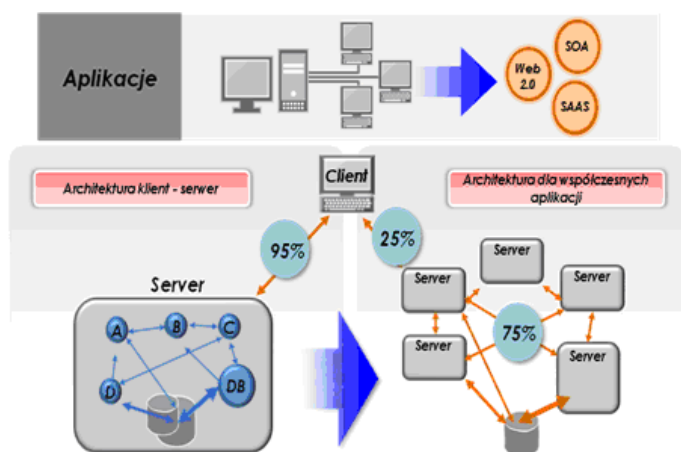
<sup>1</sup> Ten i inne przedstawione w tabelce ataki Web mogłyby zostać wykryte przez IPS po napisaniu odpowiednich sygnatur dla tych konkretnych ataków. Do napisania sygnatur IPS wymagane są jednak informacje jak ataki zostaną wykonane. W rzeczywistości jest to niemożliwe, ponieważ producenci IPS nie wiedzą jakie dokładnie błędy mają napisane dla firm aplikacje Web i w jaki sposób te błędy mogą zostać wykorzystane. Ataki XSS, SQL-Injection, itd. mogą zostać wykonane na wiele różnych sposobów. Nie ma możliwości napisania dla wszystkich tych ataków sygnatur IPS. Dlatego też IPS za pomocą tzw. uniwersalnych sygnatur wykrywa tylko podstawowe ataki Web wykonywane w typowy sposób.

## Przełączniki serii EX firmy Juniper Networks – rozwiązania pozwalające na budowę nowoczesnych sieci teleinformatycznych

Przełączniki serii EX od kilku lat cieszą się rosnącym zainteresowaniem zarówno wśród dużych operatorów telekomunikacyjnych jak również mniejszych firm. Rozwiązania Juniper cechują się dużą stabilnością działania, niezawodnością oraz wydajnością. Nie bez znaczenia pozostaje fakt, że produkty z rodziny EX działają w oparciu o sprawdzony, znany z ruterów, system JUNOS. Powyższe cechy rozwiązań firmy Juniper pozwalają spełnić nawet najwyższe wymagania stawiane dzisiaj systemom transmisji danych.

### Nowe wymagania dla centrów przetwarzania danych

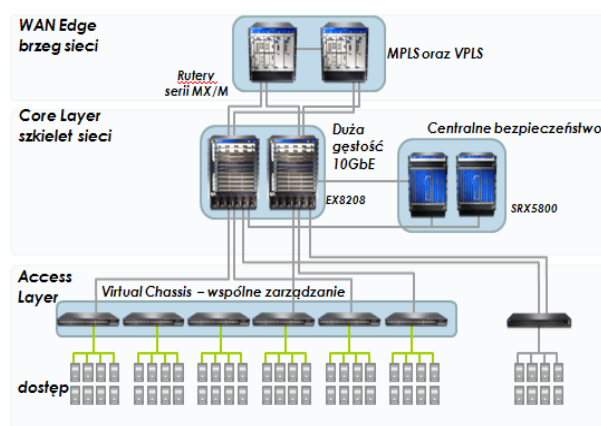
Od pewnego czasu obserwujemy dynamiczny rozwój aplikacji m.in. Web 2.0, SaaS, w których zauważamy zmianę charakteru przepływu informacji. W typowych aplikacjach klient-serwer większość ruchu odbywa się pomiędzy komputerem klienta aplikacji a serwerem. Nowoczesne rozwiązania składają się z wielu elementów silnie ze sobą powiązanych. W trakcie wykonywania działania w aplikacji uruchamiany jest zestaw interakcji między poszczególnymi jej komponentami. Generowane jest wtedy ok. 75% całego ruchu sieciowego związanego z obsługą działań klienta aplikacji. Fakt ten jest istotnym elementem, który powinniśmy wziąć pod uwagę przy projektowaniu rozwiązań sieciowych.



Rysunek 1. Przepływ informacji klient-serwer

### Architektura centrów przetwarzania danych

Rozwiązaniem zwiększającym przepustowość a także zmniejszającym opóźnienie pakietów jest uproszczenie struktury sieciowej centrum przetwarzania danych poprzez rezygnację z warstwy agregacyjnej oraz budowę warstwy dostępowej w oparciu o przełączniki połączone w stos w technologii Juniper Virtual Chassis (VC).



Rysunek 2. Uproszczona struktura sieci dla centrum przetwarzania danych

Technologia VC wprowadza ponadto możliwość centralnego zarządzania grupą przełączników. Uproszczenie struktury sieci pozwala także zminimalizować koszty infrastruktury – redukując ilość sprzętu zmniejszamy zapotrzebowanie na RU oraz minimalizujemy koszty zasilania i klimatyzacji.

### Juniper Virtual Chassis w praktyce

Juniper Virtual Chassis możemy zbudować w oparciu o następujące modele przełączników:

- EX 3300 – do sześciu przełączników łączonych poprzez porty uplink 10 GbE (tzw. Virtual Chassis Lite),
- EX 4200 – do dziesięciu przełączników połączonych dedykowanymi portami VCP na odległość do 5 metrów lub portami uplink 1/10 GbE na odległość do 70 km,

- EX 4500 – dwa przełączniki łączone portami dedykowanymi VCP lub portami uplink 10 GbE,
- EX 4200/4500 – VC w trybie *Mixed* pozwalające na użycie dwóch przełączników EX 4500 i ośmiu przełączników EX 4200 w ramach jednego VC,
- EX 8200 – do czterech przełączników EX 8208/8216 w ramach VC. Do zestawienia VC potrzebny jest zewnętrzny moduł rutujący XRE (eXternal Routing Engine). Virtual Chassis zbudowane w oparciu o przełączniki serii 8200 możemy rozciągnąć na odległość do 40 km.



Rysunek 3. Przełączniki EX 3300 połączone w Virtual Chassis

VC zachowuje się identycznie jak duży przełącznik modułarny (chassis) posiadający jeden interfejs do zarządzania oraz konfigurację. VC kontrolowane

jest przez jeden z przełączników, który działa jako Routing Engine, inny pełni rolę zapasowego Routing Engine'u. Pozostałe przełączniki funkcjonują jako karty liniowe (realizują funkcje Packet Forwarding Engine'u).

Przełączniki łączymy w stos poprzez dwa dedykowane porty VCP o przepustowości 64 Gb/s, tworzące nieblokującą wirtualną magistralę backplane 128 Gb/s. Ponadto istnieje możliwość budowy Virtual Chassis w oparciu o porty 10 GbE znajdujące się w modułach uplink. Rozwiązanie to pozwala na połączenie w VC przełączników znajdujących się w różnych lokalizacjach fizycznych.

Virtual Chassis tworzy redundantną strukturę, w której wykorzystane są optymalnie wszystkie połączenia fizyczne – pomimo architektury pierścienia nie ma potrzeby wykorzystania protokołu Spanning Tree. Z punktu widzenia innych urządzeń sieciowych Virtual Chassis jest widziane jako pojedynczy obiekt, z którym można zestawiać łącza typu multilink (802.3ad), chociaż poszczególne połączenia fizyczne zestawione są z różnymi przełącznikami EX. Daje to dodatkową korzyść, obok redundancji, w postaci zwiększenia dostępnej przepustowości.

Aby zestawić Virtual Chassis należy zdefiniować tryb pracy stosu. Dostępne są dwa tryby:

- Dynamic – ustawiamy parametr priority, który decyduje o roli urządzenia w stosie (routing-engine, line-card), im wyższa wartość tym większe prawdopodobieństwo, że przełącznik zostanie RE (1-255, domyślnie 128)

```
set virtual chassis member 0 mastership-priority 220
```

Listing 1. Ustawienie priorytetu przełącznika

- Preprovisioned – definiujemy rolę dla przełącznika

```
Set virtual-chassis preprovisioned
set member 0 serial-number BM0208366926 role routing-engine
```

Listing 2. Przypisanie roli dla przełącznika

Definiując priorytety dla przełączników należy pamiętać o kryterium wyboru przełącznika pełniącego rolę Routing Engine:

- Member priority (wyższy wygrywa)
- Member, który pracował wcześniej jako master (np. przed rebootem)
- Member z najdłuższym czasie uptime
- Member z najniższym MAC adresem

Następnym krokiem jest inicjalizacja portów VCP:

```
request virtual-chassis vc-port set interface vcp-0
```

*Listing 3. Inicjalizacja portów VCP*

Jeżeli planujemy wykorzystać porty uplink należy posłużyć się poleceniem:

```
Request virtual-chassis vc-port set pic-slot 1 port 0
```

*Listing 4. Inicjalizacja portów uplink do pracy w VC*

Polecenie *show virtual-chassis* umożliwia weryfikację stanu stosu.

```
root@vc-1> show virtual-chassis

Virtual Chassis ID: 68a2.849f.140c
Virtual Chassis Mode: Enabled

Member ID  Status  Serial No  Model  Mstr  Role  Mixed Neighbor List
0 (FPC 0)  Prsnt   BM0208366926  ex4200-24t  254  Master*  N 1 vcp-0
1 (FPC 1)  Prsnt   BM0208124474  ex4200-24t  250  Backup   N 0 vcp-0
                                0 vcp-1

Member ID for next new member: 2 (FPC 2)
```

*Listing 5. Weryfikacja stanu Virtual Chassis*








Do zatwierdzania konfiguracji VC należy używać polecenia **commit synchronize** – propaguje zmiany na cały klaster urządzeń.



## Razem różnie: Zabezpieczenia Web oraz Email na jednym appliance – TRITON 7.6.1

Websense dostarcza uznanych na rynku rozwiązań bezpieczeństwa Web, Email oraz DLP. Rozwiązania te dostępne są w postaci oprogramowania instalowanego na serwerach oraz uruchamianego na платфор-

mie Websense V-Series Appliance. Dostępne są dwa modele urządzeń: V5000 oraz V10000 Appliance. Dotychczas rozwiązania Websense mogły być na nich uruchamiane w następującej konfiguracji:

Model appliance produkt	V5000	V10000
Web Security		
Web Security Gateway (Anywhere)		
Email Security Gateway (Anywhere)		
Web Security Gateway (Anywhere) + Email Security Gateway Anywhere = <b>TRITON Security Gateway Anywhere</b>		

Wraz z wersją 7.6.1 Websense umożliwia dodatkowo uruchomienie Web Security oraz Email Security Gateway Anywhere na jednym urządzeniu V5000 lub V10000.

Web Security + Email Security Gateway Anywhere		
--	--	--

Opis wybranych z wyżej wymienionych produktów Websense:

**Email Security Gateway Anywhere (ESGA)** – Bezpieczeństwo poczty elektronicznej dostępne wyłącznie na platformie Websense V-series Appliance połączone z usługą Hosted Email Security, co umożliwia wstępne filtrowanie poczty, np.: zablokowanie spamu już na poziomie chmury. Pakiet zawiera ochronę przed wyciekiem istotnych informacji klasy enterprise (DLP dla poczty elektronicznej, pełną ochronę DLP oferuje Data Security Suite).

**Web Security Gateway Anywhere (WSGA)** – To nie tylko URL filtering, ale również skuteczna ochrona przed zagrożeniami Web 2.0, kategoryzacja i skanowanie bezpieczeństwa na bieżąco. Rozwiązanie umożliwia również zarządzanie szyfrowanymi połączeniami HTTPS oraz kontrolowanie poszczególnych funkcji dostępnych w portalach społecznościowych. Pakiet WSGA zawiera ochronę przed wyciekiem istotnych informacji klasy enterprise (DLP w kanale Web, pełną ochronę DLP oferuje Data Security Suite).

**Data Security Suite (DSS)** – Rozwiązania ochrony przed wyciekiem istotnych informacji pomagają wykryć, monitorować, oraz chronić dane ważne dla Twojej firmy. Narzędzia te pozwalają kontrolować które dane są istotne, gdzie są przechowywane, kto ich używa, dokąd i komu wysyła, jak również zabezpieczyć wszystkie najważniejsze informacje.

**Więcej informacji o produktach Websense znajdziecie Państwo na stronach Clico oraz Websense.**

**Chętnie odpowiemy na wszelkie pytania dotyczące produktów Websense, wdrożeń testowych oraz docelowych, naszych własnych oraz autoryzowanych szkoleń Websense. Jesteśmy do Państwa dyspozycji: [psk@clico.pl](mailto:psk@clico.pl)**



**Zaskoczony** tym, co naprawdę **dzieje się** w Twojej sieci ?

A może przez przypadek wysłałeś **ten** plik do **niewłaściwej** osoby ?

**Check Point Security Day 2011**

powered by CLICO

**25 października 2011**

Szanowni Państwo,

Clico wraz z Check Point mają przyjemność zaprosić Państwa do udziału w konferencji Check Point Security Day 2011. Mamy nadzieję, że jak co roku, już od 11 lat, impreza ta spotka się z zainteresowaniem z Państwa strony. Konferencja odbędzie się 25 października w Warszawie, w Multikinie Ursynów i będzie połączona z projekcją filmu „Baby są jakieś inne”.

Uczestnictwo w konferencji jest bezpłatne. Prosimy o rejestrację tutaj: [https://mnt.clico.pl/konferencje/index.jsp?id\\_konferencji=361](https://mnt.clico.pl/konferencje/index.jsp?id_konferencji=361)

### Agenda konferencji

9:30 – 10:00	Rejestracja uczestników, kawa powitalna
10:00 – 10:30	Powitanie gości
10:30 – 11:00	Co nowego w Check Point?
11:00 – 11:45	Firewall nowej generacji Check Point R75.20 – pokaz „na żywo” ochrony przed atakami.
11:45 – 12:30	Czy wiesz, gdzie trafiają dane? Prezentacja rozwiązania DLP
12:30 – 13:15	Lunch
13:15 – 13:45	Check Point EPS – kompletne zabezpieczenia desktopowe do zastosowań firmowych.
13:45 – 14:30	Zarządzanie zmianami w systemach zabezpieczeń – rozwiązanie Tufin SecureTrack.
14:30 – 14:50	Losowanie nagród w konkursie
15:00 – 16:30	Projekcja filmu „Baby są jakieś inne”

## Nowe szkolenia Check Point R75



**Check Point**  
SOFTWARE TECHNOLOGIES LTD.

### Skomponuj program swojego szkolenia!

Wersja R75 szkoleń Check Point jest początkiem innowacyjnego oraz elastycznego podejścia firmy do treningów systemu bezpieczeństwa. Rozpoczynając od wersji szkoleń R75, uczestnik zyskuje możliwość dużo większego wyboru zagadnień, które go interesują w tematyce Check Point. Szkolenia będą się składać z części „głównej” (CCSA lub CCSE) oraz dodatkowych, krótkich, tematycznych

modułów szkoleniowych, tak zwanych „Training Blade”. Przykładem takiego uzupełniającego szkolenia może być „Application Control Training Blade”, pozwalające uczestnikom na dokładne zapoznanie się z funkcjami „blade” kontrolującego ruch, na poziomie warstwy aplikacji. Lista „dodatkowych” szkoleń, jest cały czas poszerzana i aktualizowana przez Check Point.

## CCSA R75

Kurs Check Point Certified Security Administrator, skierowany jest zarówno do administratorów systemów Check Point, jak i dla ludzi dopiero poznających ten system. Wiedza przekazywana kursantom podczas szkolenia obejmuje takie zagadnienia jak:

### Tworzenie oraz instalowanie polityk bezpieczeństwa

Tworzenie, kompilowanie oraz wdrażanie polityk bezpieczeństwa, to pojęcia, które powinny być doskonale znane każdemu administratorowi systemów Check Point. Podczas szkolenia CCSA, zarówno wykładów jak i specjalnie przygotowanych laboratoriów, uczestnikom zostaną przedstawione wszystkie reguły oraz sposoby przygotowywania i wdrażania skutecznych polityk.

### Projektowanie i wdrażanie tablic translacji adresów (NAT)

Zarządzanie translacją adresów to jedna z podstawowych umiejętności administratorów sieci IPv4. Szkolenie CCSA pozwala uczestnikom zapoznać się z metodami budowania reguł translacji adresów oraz ich wdrażania w systemach Check Point.

### Monitorowanie ruchu przy pomocy narzędzi Check Point

Check Point to nie tylko wymuszanie bezpieczeństwa za pomocą zapory ogniowej, VPN, czy kontroli IPS. Check Point daje też administratorom praktycznie nieograniczone możliwości monitoringu oraz raportowania zdarzeń wykrytych przez moduły egzekwujące polityki bezpieczeństwa. Podczas szkolenia uczestnicy poznają sposoby wykorzystania monitorowania systemu przy użyciu takich aplikacji, jak Smart View Tracker, czy Smart View Monitor.

### Zarządzanie użytkownikami oraz przyznawanie uprawnień do zabezpieczonych zasobów sieciowych

W dzisiejszych czasach administratorzy zapór sieciowych przy budowaniu polityk bezpieczeństwa nie mogą już kierować się jedynie podstawowymi informacjami, takimi jak adres IP, czy numery portów. Aby skutecznie zapewnić bezpieczeństwo, administratorzy są zmuszeni do rozróżniania poszczególnych użytkowników bez względu na komputer, przy którym aktualnie dany użytkownik pracuje. Tak granularnego tworzenia polityk bezpieczeństwa, uczyć się będą uczestnicy szkolenia podczas bloków tematycznych dotyczących „User / Client / Session Authentication” oraz „Identity Awareness”.

## Tworzenie oraz wdrażanie bezpiecznych połączeń VPN

Tworzenie bezpiecznych połączeń VPN to funkcja, która od wielu lat jest zaimplementowana w systemach Check Point. Szkolenie CCSA pozwala na poznanie tajników tworzenia tuneli VPN za pomocą innowacyjnego sposobu „Domain Based VPN”.

## CCSE R75

Szkolenie CCSE od zawsze pozwalało administratorom na dogłębne zrozumienie zasad działania technologii Check Point. Takie zagadnienia jak na przykład akceleracja, klastrowanie są podczas szkolenia dokładnie wyjaśniane przez instruktora, potem każdy z uczestników ma możliwość ich przeciwnienia, podczas specjalnie przygotowanych laboratoriów.

Podczas szkolenia CCSE administrator poznaje:

### Procedury aktualizacji

Administratorzy zyskują umiejętności pozwalające im na skuteczne tworzenie kopii zapasowych systemów Check Point, ich przywracanie oraz wykorzystanie ich podczas procesu aktualizacji systemu. Osobnym zagadnieniem są procedury związane z aktualizacją środowiska środowiska wykorzystującego mechanizmy klastrowania.

### Zaawansowane zarządzanie użytkownikami, monitorowanie i rozwiązywanie problemów związanych z blade „Identity Awareness”

Dzięki szkoleniu CCSE uczestnicy szkolenia zdobywają wiedzę, pozwalającą im na integrację środowiska Check Point z zewnętrznymi bazami użytkowników czy konfigurację „Smart Directory”. Informacje te mogą następnie być użyte przy konfiguracji dostępu do sieci LAN z zewnątrz organizacji. Dodatkowo przekazywana jest wiedza dotycząca monitorowania i debugowania procesu autoryzacji użytkowników na zaporach Check Point.

### Klastrowanie zapór ogniowych i centralnego zarządzania

Administratorzy zapoznają się z metodami tworzenia klastrów opartych na technologiach High Availability oraz Multicast Load Sharing (ClusterXL), konfiguracji akceleracji Check Point przy użyciu produktów CoreXL oraz SecureXL.

## Zaawansowane zastosowanie VPN

Uczestnicy szkolenie zapoznają się z zaawansowanymi metodami debugowania połączeń VPN, tworzenia nowych oraz optymalizacji już istniejących połączeń, na przykład przy użyciu technologii Multi – Endpoint VPN.

### Narzędzia raportujące, ich wdrażanie i funkcje.

Tworzenie rozbudowanych raportów, sprawne korzystanie z aplikacji Smart Event to umiejętności pozwalające administratorom zapanować nad ogromem zdarzeń sieciowych wykrywanych oraz logowanych przez systemy Check Point. Te umiejętności pozwolą administratorom na natychmiastowe wychwycenie kluczowych dla bezpieczeństwa sieci informacji.

## Harmonogram szkoleń Check Point

Nazwa szkolenia	Czas trwania	Data rozpoczęcia
CCSA R70/R71	5 dni	21.11. 2011 5.12.2011
CCSE R70/R71	5 dni	17.10.2011 28.11.2011 12.12.2011
CCSA R75	3 dni	7.11.2011
CCSE R75	3 dni	26.10.2011 16.11.2011 19.12.2011

Szczegółowych informacji o szkoleniach Check Point udziela Pani Bożena Tarasiuk:  
bozena.tarasiuk@clico.pl

## Szkolenia Juniper Networks



Szanowni Państwo,

Autoryzowane Centrum Szkoleniowe Clico od września 2011 uruchamia szkolenia Juniper Networks dla branży Service Provider. W naszej ofercie dostępne będą szkolenia:

1. AJSPP - zaawansowany ruting IP w sieciach operatorskich
2. JIR – ruting dla średniozaawansowanych

Więcej informacji o szkoleniach Juniper Networks znajdziecie Państwo na stronie WWW.szkolenia.clico.pl Harmonogram szkoleń na najbliższe miesiące przedstawia się następująco:

Nazwa szkolenia	Termin	Termin
IJS	25 października 2011	15 listopada 2011
JRE	26 października 2011	16 listopada 2011
JIR	17-18 listopada 2011	-
JEX	27-28 października 2011	-
JSEC	23 - 25 listopada 2011	

Zajęcia odbywają się w Centrum Szkoleniowym Clico w Warszawie. Zgłoszenia i zapytania prosimy kierować do Agnieszki Muchy: agnieszka.mucha@clico.pl, tel. 22 518 02 71