



# BEZPIECZNY STYK Z INTERNETEM



# BEZPI



Internet otwiera przed nami wielkie możliwości, ale korzystanie z niego nie jest pozbawione pewnego ryzyka. W drodze do pełnego wykorzystania Internetu wielką rolę do odegrania mają technologie ochrony danych. Każdy użytkownik Internetu musi chronić własne zasoby przed niepożądanym dostępem z zewnątrz. Zagadnienia bezpieczeństwa na styku z Internetem nabierają innego wymiaru, jeśli nasza firma decyduje się prowadzić przez sieć swoje interesy. Internet daje tu szczególnie atrakcyjne możliwości. Od kilku lat na naszych oczach dokonuje się ewolucja stron internetowych, które przestają pełnić funkcje tylko reklamowe, a stają się miejscem przeprowadzania transakcji e-commerce, wartych już dziś setki miliardów dolarów. Internet jest nowym teatrem dla prowadzenia interesów, a wiążąca się z tym redukcja kosztów firm powoduje, że uczestnicwo w gospodarce internetowej przestaje być opcją, a staje się koniecznością. To, co jeszcze dziś jest źródłem przewagi konkurencyjnej, jutro będzie obowiązującym standardem. Niestety, powszechnej adopcji rozwiązań internetowych często towarzyszy ignorowanie problemów związanych z zapewnieniem bezpieczeństwa. Nagłaśniane ostatnio przez media ataki hackerów na popularne sklepy internetowe unaocznily fakt, że nawet najwięksi reprezentanci nowej gospodarki nie ustrzegli się rażących zaniedbań w tej dziedzinie. Tymczasem długofalowe powodzenie przedsięwzięcia wymaga zdobycia zaufania klientów i partnerów, przez zapewnienie ich transakcjom maksymalnego bezpieczeństwa. Problemem, przed jakim stoją firmy chcące budować bezpieczne rozwiązania internetowe, nie jest brak dostępnych rozwiązań, lecz integracja dostępnych środków technicznych w spójny system, gdyż żadne pojedyncze urządzenie nie zapewni pożądanego bezpieczeństwa.

Cisco zaprojektowało całościowe rozwiązanie bezpieczeństwa dla firm korzystających z Internetu i wykorzystujących sieć dla prowadzenia działalności gospodarczej. Niniejsze opracowanie opisuje to rozwiązanie i jego elementy.

## Wymagania stawiane przed bezpiecznym stykiem z Internetem

Infrastruktura sieciowa na styku firmy z Internetem powinna zapewniać użytkownikom:

- bezpieczeństwo
- wydajność
- skalowalność
- niezawodność i wysoką dostępność

### Bezpieczeństwo

Internet przynosi nam oprócz nowych możliwości również nowe zagrożenia. Najpowszechniejsze problemy bezpieczeństwa to świadome lub przypadkowe niszczenie albo modyfikacja danych (bądź podczas transmisji, bądź rezydujących na serwerach), zablokowanie usług (znane jako atak typu Denial of Service) przez zalew fikcyjną informacją zużywającą zasoby sieci i komputerów, podszywanie się pod użytkowników bądź pod serwer, wykonywanie nie autoryzowanych transakcji, bez odpowiednich uprawnień.

Mając świadomość faktu, że nie istnieje żadne pojedyncze rozwiązanie gwarantujące bezpieczeństwo, styk z Internetem należy zaprojektować maksymalnie, wykorzystując dostępne technologie ochrony danych, takie jak:

- kontrola dostępu - firewall Cisco PIX, router z oprogramowaniem IOS<sup>(R)</sup> Firewall Feature Set
- detekcja ataków - Cisco Secure IDS
- kontrola tożsamości - Cisco Secure ACS, SSL
- poufność i integralność - IPSec, SSL
- autentyczność - podpisy cyfrowe, certyfikaty cyfrowe

# E C Z N Y

## Wydajność

Maksymalizacja wydajności zwykle stoi w sprzeczności z chęcią zapewnienia maksymalnego bezpieczeństwa. Odpowiedni dobór urządzeń, takich jak router brzegowy, firewall, sonda IDS, pozwala na częściowe rozwiązanie tego dylematu. Wydajność całego rozwiązania styku z Internetem jest taka, jaka jest wydajność jego najsłabszego ogniwa, tak więc szczególne znaczenie ma poprawne zaprojektowanie całego rozwiązania, tak aby zidentyfikować wszelkie potencjalne wąskie gardła, a następnie je usunąć.

## Skalowalność

Skalowalność styku z Internetem to skalowalność urządzeń sieciowych, a w przypadku rozwiązań e-commerce również skalowalność serwerów www. W obu przypadkach pełną, liniową skalowalność można uzyskać tylko poprzez dodawanie urządzeń sieciowych (np. firewalli) i serwerów www oraz rozkład obciążenia pomiędzy nimi. Algorytm rozkładu obciążenia powinien reagować na rzeczywiste obciążenie urządzeń. W przypadku rozwiązań typu e-commerce dodatkową trudność sprawia konieczność utrzymania integralności transakcji, poprzez zapewnienie, że wszystkie sesje w ramach jednej transakcji będą obsługiwane przez ten sam serwer. Wszystkie te wymagania realizuje technologia nazywana content switching, obecna na takich urządzeniach, jak Cisco Content Engine i Cisco Content Services Switch.

## Niezawodność i wysoka dostępność

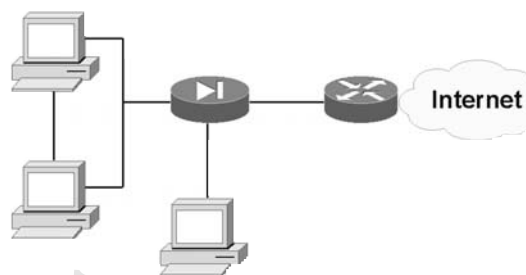
Niezawodność styku z Internetem jest zawsze bardzo istotna, a dla zastosowań typu e-commerce wręcz krytyczna, gdyż każda minuta przestoju oznacza wymierne straty. Wysoka dostępność, czyli zdolność sieci do samonaprawy, wymaga pełnej redundancji wszystkich elementów sieciowych, łącznie z serwerami. Dodatkowo dostępne muszą być technologie pozwalające na szybką identyfikację awarii i szybkie, najlepiej niezauwa-

żalne dla użytkownika, przełączenie na urządzenie zapasowe. Dobrze jest też, jeśli w czasie normalnej pracy jest wykorzystywany element zapasowy, odciążając urządzenie podstawowe.

W przypadku serwerów detekcja awarii powinna polegać nie tyle na weryfikacji, czy dany serwer pracuje, ale na weryfikacji, czy dany serwer aktualnie posiada plik żądany przez użytkownika (tę funkcję realizuje technologia content switching). Poniżej wymienione są technologie spełniające większość przedstawionych wymagań:

- redundancja operatorów internetowych (ISP) - technika multihoming i protokół BGP4
- redundancja przyłącza do operatora internetowego - technika multihoming i protokół BGP4
- redundancja routerów brzegowych - technika Cisco HSRP oraz technika multihoming i protokół BGP4
- redundancja firewalli - funkcja statefull failover firewalla Cisco PIX lub - w przypadku farmy firewalli - technologia content switching
- redundancja serwerów www - technologia content switching

W przypadku rozwiązań e-commerce dodatkowym zabezpieczeniem może być stworzenie dwóch, geograficznie oddalonych, centrów komputerowych, każdego z własnym stykiem z Internetem. Dla użytkownika oba centra powinny być reprezentowane przez jeden adres URL. Jest to możliwe dzięki technologii content routing, wykorzystującej cechy protokołu DNS i podejmującej optymalne decyzje, do którego centrum skierować użytkownika na podstawie takich parametrów jak obciążenie komputerów w centrach czy ich odległość od użytkownika. Technologia content routing jest dostępna na urządzeniach Cisco Distribution Manager i Cisco Content Services Switch.



# Z I N T E R

# STYK

## Elementy składowe bezpiecznego styku z Internetem

### Screening router

Screening router jest to nazwa nadawana routerowi łączącemu firmę z Internetem, stanowiącemu jednocześnie pierwszą linię obrony. Router ten powinien odfiltrowywać niepożądany ruch przed dostaniem się do sieci firmy. Dzięki oprogramowaniu IOS™ Firewall Feature Set dla routerów Cisco filtracja dokonywana przez router nie musi ograniczać się do prostego sprawdzania zawartości nagłówka każdego pakietu, ale może mieć charakter kontekstowy. Router identyfikuje wtedy konwersacje nawiązywane w sieci i interpretuje znaczenie każdego pakietu w kontekście nawiązanych konwersacji (technika ta nosi nazwę Context Based Access Lists - CBAC). Podnosi to znacznie pewność działania filtracji i zmniejsza ryzyko jej przełamania, a sam router nabiera charakteru prostego firewalla. Screening router będzie dobrze pełnił swoją funkcję, jeśli sam będzie dobrze zabezpieczony przed dostępem ze strony osób niepożądanych.

### Firewall

Firewall stanowi kluczowy element zabezpieczający firmę przed zewnętrznym światem Internetu. Ponosi on główną odpowiedzialność za bezpieczeństwo sieci wewnętrznej firmy i to on realizuje właściwe mechanizmy ochrony danych. Firewall Cisco PIX, typowo skonfigurowany, wykorzystuje do zabezpieczenia sieci wewnętrznej firmy następujące technologie:

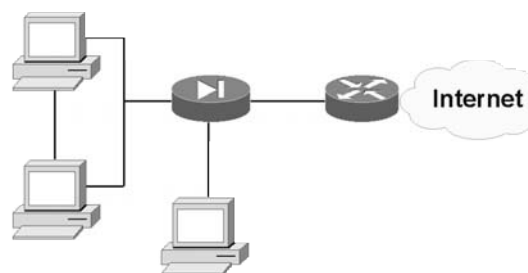
- Adaptive Security Algorithm, monitorujący konwersacje w sieci i powodujący, że firewall działa w trybie tzw. stateful security
- translacja adresów sieciowych (NAT) dla ruchu wchodzącego i wychodzącego
- obrona przed atakami typu Denial of Service (funkcja nazywana również Sync Flood Defend)
- technika cut-through proxy, umożliwiająca weryfikację tożsamości użytkownika przy jednoczesnym zachowaniu wydajności sieci

- filtracja ruchu w oparciu o adres URL
- filtracja apletów Javy i elementów ActiveX

Nie należy jednak zapominać, że firewall jest również urządzeniem transmitującym dane i łatwo może stać się wąskim gardłem na styku firmy z Internetem. Firewall Cisco PIX jest skonstruowany tak, aby połączyć wysoką wydajność z wysokim poziomem bezpieczeństwa, dając możliwość obsługi do 500 000 równoległych sesji.

### Intrusion Detection System

Intrusion Detection System to rozwiązanie pozwalające na monitoring w czasie rzeczywistym zdarzeń zachodzących w sieci oraz - w razie potrzeby - reagujące na niepożądane zjawiska. Generalnie umożliwia on wykluczenie z monitorowanego segmentu sieci intruza próbującego jakiegokolwiek aktywności. W skład rozwiązania wchodzi sonda (Cisco Secure IDS Sensor), będąca urządzeniem monitorującym konkretny segment sieci lokalnej, oraz konsola operatorska (Cisco Secure IDS Director), stanowiąca aplikację wizualizującą w czasie rzeczywistym informacje o atakach w sieci. Kluczowym elementem rozwiązania jest baza danych z wzorcami znanych ataków (tzw. sygnaturami), pozwalająca na ich identyfikację.



W typowej implementacji systemu IDS sondy rozmieszcza się przed i za każdym firewallem. Dzięki temu otrzymujemy pełny obraz jego skuteczności, gdyż dostajemy informacje o

# NETEM

wszystkich atakach, jakie dotyczą naszą sieć, oraz o tych z nich, które zdołały przeniknąć przez firewall. Aplikację Cisco Secure IDS Director umieszcza się w sieci wewnętrznej (za firewallem), a sondy komunikują się z nią wydzielonymi łączami. Sama sonda nie stanowi osłabienia systemu bezpieczeństwa, gdyż jest zupełnie niewidoczna w sieci, nie jest też wąskim gardłem, gdyż jedynie podsłuchuje ruch w segmencie ethernet, nie uczestnicząc w transmisji.

### Content Switch

Content Switch to specjalizowane urządzenie dla środowisk e-commerce i portali internetowych. Jego zadaniem jest skierowanie żądania klienta do właściwego serwera www lub urządzenia typu cache. Decyzja o tym, do którego serwera skierować żądanie, podejmowana jest w oparciu o szereg konfigurowalnych parametrów:

- dostępność serwera
- obciążenie serwera
- czas odpowiedzi z serwera
- dostępność żadanego pliku na serwerze
- parametry sieciowe warstwy 3 i 4 żądania (adres IP, port TCP, itp.)
- parametry sieciowe warstwy 5, 6 i 7 żądania, takie jak adres URL, identyfikator sesji SSL czy obecne w żądaniu Cookie

W sytuacji gdy wszystkie dostępne serwery są przeciążone, przełącznik może uruchomić dodatkowe serwery lub urządzenia typu cache, będące w rezerwie, kopiując na nie szczególnie często żądane pliki i dodając je do farmy serwerów do czasu zmniejszenia „popytu”.

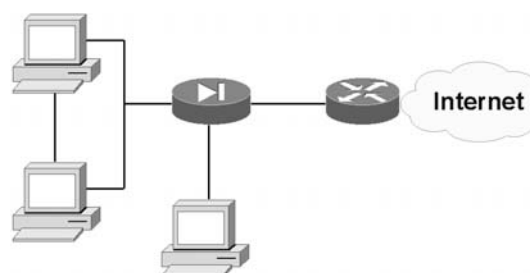
Rezultatem działania content switcha jest minimalizacja czasu odpowiedzi z serwera obserwowana przez klienta i eliminacja okresów niedostępności usług. Ubocznym efektem jego pracy jest dodatkowa ochrona serwerów www, gdyż content switch - podobnie jak firewall - działa w trybie stateful security. Przełączniki te, np. Cisco Content Services Switch 11000 lub

Cisco Content Engine umieszczone są bezpośrednio przed serwerami www. W przypadku rozbudowanych data center możliwe jest stworzenie wielopoziomowej hierarchii przełączników typu content switch.

### Content Router

Content Router znajduje swoje zastosowanie w sytuacji budowy wielu, geograficznie oddalonych, centrów danych. Jego zadaniem jest skierowanie żądania klienta do właściwego centrum. Router może skorzystać tu z kombinacji następujących kryteriów:

- dostępność żadanego pliku w danym data center
- obciążenie danego data center
- odległość data center od użytkownika, który wygenerował żądanie
- aktualny stan sieci



Najczęściej stosowaną przez content router techniką skierowania klienta do wybranego data center jest współpraca z systemem DNS i zwrócenie powiązania stosowanego przez użytkownika adresu URL z wybranym adresem IP właściwego data center. Proces ten jest zupełnie niezauważalny z punktu widzenia klienta. Efektem działania content routera jest minimalizacja czasu odpowiedzi obserwowana przez klienta i eliminacja okresów niedostępności usług.

## Cache

Integralnym elementem łączy internetowego każdej firmy powinien być cache internetowy. Urządzenie to znajduje zastosowanie zarówno w przypadku korzystania z Internetu przez pracowników naszej firmy, jak i w przypadku udostępniania naszych serwerów www użytkownikom Internetu, jednak jego rola jest w każdej z tych sytuacji różna.

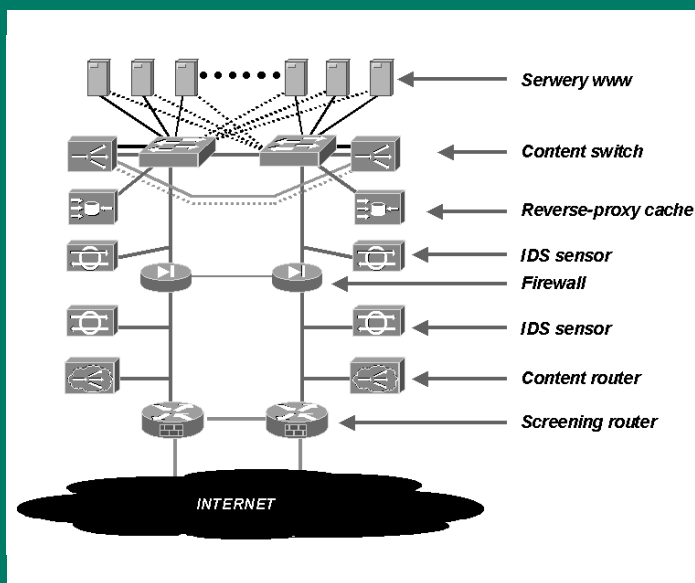
W pierwszym przypadku urządzenie cache działa w trybie transparent caching. Polega on na niewidocznym dla użytkowników przekierowywaniu odwołań do serwisów internetowych i skierowywaniu ich do urządzenia cache. Urządzeniem przekierowującym odwołania jest najczęściej router znajdujący się na styku z Internetem (screening router). Cache w imieniu użytkownika znajduje informację na Internecie i odpowiada na żądanie. Celem działania transparent cache jest skrócenie czasu odpowiedzi dla użytkowników i zmniejszenie obciążenia łączy transmisją powtarzających się informacji.

W przypadku drugim urządzenie cache działa w trybie reverse-proxy

caching. W tym trybie cache obsługuje żądania klientów „w imieniu“ danej grupy serwerów www. Celem działania reverse cache jest odciążenie serwerów www z transmisji pewnych, najczęściej statycznych, informacji. Użytkownicy są w sposób przezroczysty, ale wybiórczy, przekierowywani do urządzenia cache, a urządzeniem przekierowującym jest najczęściej content switch.

## Podsumowanie - całościowy obraz rozwiązania

Poniższy rysunek przedstawia całościowy obraz rozwiązania.

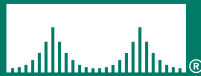


www.dokumenty.pl, e-mail: synetrix@dokumenty.pl

**synetrix**

98-200 Sieradz, ul. Wodna 7  
tel. +48 (43) 822 18 71, (42) 209 30 60  
fax +48 (42) 299 68 75

**CISCO SYSTEMS**



Cisco Systems Poland Sp. z o.o.  
Al. Jerozolimskie 146C  
02-305 Warszawa  
Tel.: (022) 572 27 00  
Fax: (022) 572 27 01  
WWW: <http://www.cisco.com/pl>