Rosnąca liczba aplikacji wymaga zapewnienia odpowiedniej jakości komunikacji

Obsługa wielu łączy do Internetu i ochrona przed awariami

Mariusz Stawowski
mariusz.stawowski@clico.pl

Bezpieczeństwem IT zajmuje się zawodowo i jako pasjonat od 1996 roku. Obecnie pracuje jako konsultant w firmie CLICO Sp. z o.o. Posiada stopnie specjalizacji w zakresie wiodących technologii zabezpieczeń m.in. Check Point, Entrust, ISS, NetScreen, Nokia i Trend Micro. Jest autorem ponad 50 artykułów w prasie informatycznej oraz dwóch książek o tematyce bezpieczeństwa.

Zakres działania aplikacji sieciowych, od których zależy praca firm jest stale poszerzany, obejmuje kolejne zadania - wspomaga kierownictwo, zarządzanie dokumentami, czy też rozliczanie produkcji i sprzedaży. Rosnąca liczba aplikacji wymaga zapewnienia odpowiedniej jakości komunikacji oraz stałej dostępności infrastruktury sieciowej i Internetu.

Obsługa wielu łączy do Internetu i ochrona przed awariami

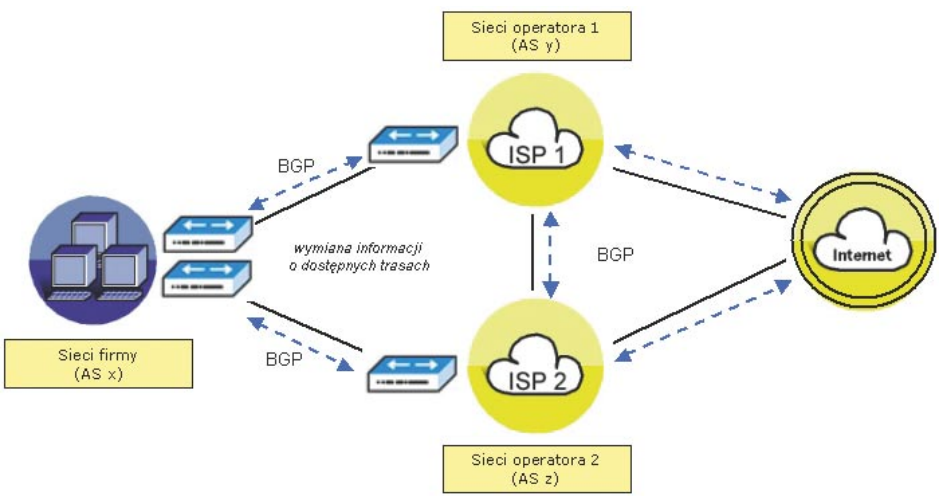
Wdrożenie dwóch lub więcej łączy do Internetu sprawia szereg problemów projektowych, implementacyjnych i administracyjnych. W typowym przypadku firma wykupuje dwa łącza od różnych operatorów Internetu i otrzymuje od nich dwie niezależne pule adresów IP. Już w tym momencie pojawia się problem, które adresy IP należy zastosować i jak postępować w razie wystąpienia awarii łącza operatora, którego adresy są wykorzystywane. Dla komunikacji wychodzącej z sieci prywatnej firmy do Internetu w razie awarii łącza zwykle wystarczy ręcznie zmienić domyślny gateway i adresy wykorzystywane przez NAT (ang. network address translation). Nie ma jednak prostego sposobu obsługi wielu łączy przy udostępnianiu własnych zasobów (np. serwerów e-commerce). Jeżeli serwery zostaną zaadresowane z puli jednego operatora to w razie awarii jego łącza nie będzie możliwości do nich dostępu. Połączenie do adresów IP przyznanych przez jednego operatora nie może być nawiązane przez łącza innych operatorów. Wynika to z przyjętej polityki i konfiguracji rutingu w Internecie. Z kolei ręczne zmiany ustawień adresów IP (zwykle NAT) i rekonfiguracja DNS dla serwerów zajmują zbyt dużo czasu, nie mówiąc o innych komplikacjach.

Kolejna kwestia do rozwiązania to efektywne wykorzystanie łączy. Zakupienie łącza zapasowego, ponoszenie kosztów jego utrzymania i wykorzystywanie go tylko w razie awarii łącza podstawowego jest zwykłym marnotrawstwem. W niektórych urządzeniach (np. NetScreen) można skonfigurować ruting źródłowy (ang. source-based routing) tak, aby część sieci wewnętrznej dostawała się do Internetu przez łącze jednego operatora, a pozostałe komputery przez drugie łącze. Nie rozwiązuje to jednak problemu rekonfiguracji adresów IP i systemu DNS w czasie awarii. W praktyce konieczne jest zastosowanie mechanizmów automatycznego wykrywania awarii i obsługi wielu łączy do Internetu. Najczęściej odbywa się to za pomocą protokołów rutingu lub dedykowanych urządzeń (np. Radware LinkProof).

Protokół BGP

Protokół BGP (ang. border gateway protocol) to standard rutingu w sieciach posiadających wiele połączeń do Internetu. BGP wymienia informacje nt. rutingu pomiędzy różnymi systemami autonomicznymi AS (ang. autonomous system). System autonomiczny w Internecie to sieć lub grupa sieci posiadająca wspólną administrację i politykę rutingu IP. Operatorzy Internetu i korporacje posiadają zwykle swoje systemy autonomiczne. W konfiguracji BGP każdy system autonomiczny w Internecie posiada swój unikalny numer AS. Koncepcja działania protokołu BGP została przedstawiona na rysunku 1.

Wdrożenie BGP wiąże się zwykle ze zmianą adresów IP tak, aby były one niezależne od adresów wykorzystywanych w innych systemach autonomicznych. Firma uzyskując łącze od określonego operatora Internetu uzyskuje od niego pule adresów IP, określanych jako PA (ang. provider aggregatable). Posiadając wiele połączeń do Internetu obsługiwanych przez BGP zalecane jest posiadanie przez firmę adresów IP niezależnych od operatorów Internetu, określanych jako PI (ang. provider independent). Adresy PI w przypadku polskich firm przyznawane są przez RIPE. Wiąże się to z wykonaniem



Rys. 1: Koncepcja działania protokołu BGP

odpowiednich przedsięwzięć organizacyjnych oraz poniesieniem znacznych nakładów finansowych.

BGP umożliwia wykrywanie niedostępności połączeń i sterowanie ruchu sieciowego. Nie uwzględnia jednak przy tym aktualnego obciążenia łączy, opóźnień transmisji danych oraz strat pakietów. Brak wiarygodnych kryteriów wydajnościowych sprawia, że BGP nie steruje rutingiem na podstawie wskaźników jakościowych, co w konsekwencji prowadzi do nieoptymalnego wykorzystania łączy i często nieprzewidywalnego zachowania sieci.

Zarządzanie wieloma łączami do Internetu

Protokoły dynamicznego rutingu umożliwiają dzielenie ruchu sieciowego pomiędzy wiele łączy. Nie posiadają jednak efektywnych mechanizmów równoważenia obciążenia. Nie uwzględniają także faktu, że pewne zasoby Internetu są lepiej osiągalne z określonego punktu poprzez łącze jednego operatora niż innych. Dlatego też firmy często decydują się na stosowanie dedykowanych urządzeń sieciowych. Przykładem takiego rozwiązania jest LinkProof, zaprojektowany przez Radware do obsługi wielu łączy internetowych bez konieczności konfiguracji protokołów dynamicznego rutingu. Umożliwia on przy tym bardziej efektywne od protokołów rutingu wykorzystanie łączy. Do podstawowych własności LinkProof można zaliczyć:

- Dynamiczne wykorzystywanie adresów IP uzyskanych od różnych operatorów Internetu w zależności od aktualnej sytuacji w sieci,
- monitorowanie i szybkie wykrywanie awarii łączy,
- optymalne wykorzystanie łączy poprzez analizowanie stanu sieci i równoważenie ich obciążenia,
- wykorzystanie w zależności od sytuacji różnych algorytmów wyboru najlepszej ścieżki rutingu w oparciu o wskaźniki jakościowe.

Zarządzanie i przydział adresów IP odbywa się za pomocą mechanizmu SmartNAT. W zależności od bieżącego stanu łączy LinkProof w sposób dynamiczny wykonuje translację NAT, wykorzystując przy tym adresy różnych operatorów Internetu. Jeżeli w danej chwili do transmisji danych wybrane zostanie łącze jednego operatora to SmartNAT zastosuje adresy tego operatora. Dla sesji inicjowanych w sieci wewnętrznej firmy translacji NAT poddawane są źródłowe adresy IP (ang. source address). Dla sesji inicjowanych w Internecie (np. do serwerów DMZ) translacji NAT poddawane są adresy miejsca przeznaczenia (ang. destination address).

Równoważenie obciążenia łączy

Równoważenie obciążenia łączy do Internetu w urządzeniach LinkProof odbywa się w oparciu o przypisane im priorytety (wagi, koszty) oraz następujące algorytmy:

- Cyclic – sesje kierowane są po kolei do wszystkich sprawnych łączy,
- Least Amount of Traffic – sesje kierowane są do łącza, które jest najmniej obciążone,
- Fewest Number of Users – sesje kierowane są do łącza, z którego korzysta najmniejsza liczba użytkowników,
- Private – wybór łącza odbywa się na podstawie analizy parametrów SNMP odczytanych z ruterów dostępowych,
- NT – wybór łącza odbywa się na podstawie analizy statystyk Windows NT SNMP odczytanych z ruterów dostępowych opartych na systemie operacyjnym Windows NT,
- Least Bytes Number – sesje kierowane są do łącza, poprzez które przesłane zostało mniej danych,
- Hashing – wybór łącza odbywa się na podstawie analizy adresów IP klienta i serwera.

Powyższe algorytmy stosowane są przy obsłudze sesji inicjowanych w sieci wewnętrznej firmy, jak i sesji inicjowanych w Internecie. Obsługa sesji nawiązywanych z Internetu odbywa się z zaangażowaniem serwisu DNS. Urządzenie LinkProof odpowiada za rozwiązywanie nazw URL wszystkich zasobów firmy udostępnianych w Internecie. W zależności od aktualnego stanu sieci nazwy URL rozwiązywane są na adresy IP różnych operatorów. LinkProof ustawia przy tym dla rekordów DNS niskie czasy życia TTL tak, aby informacje DNS nie były długo zapamiętywane przez serwery w Internecie. W razie awarii łącza do określonego operatora jego adresy IP nie powinny być wykorzystywane w serwisie DNS. Przykładowe ustawienia systemu DNS dla sieci obsługiwanej przez LinkProof są następujące:

- operator zarządzający domeną wyższego poziomu (np. NASK):

```
firma.pl              IN  NS   serwer_dns_isp1
firma.pl              IN  NS   serwer_dns_isp2
serwer_dns_isp1       IN  A    <IP serwera DNS w ISP1>
serwer_dns_isp2       IN  A    <IP serwera DNS w ISP2>
```

- operator ISP1 (serwer_dns_isp1):

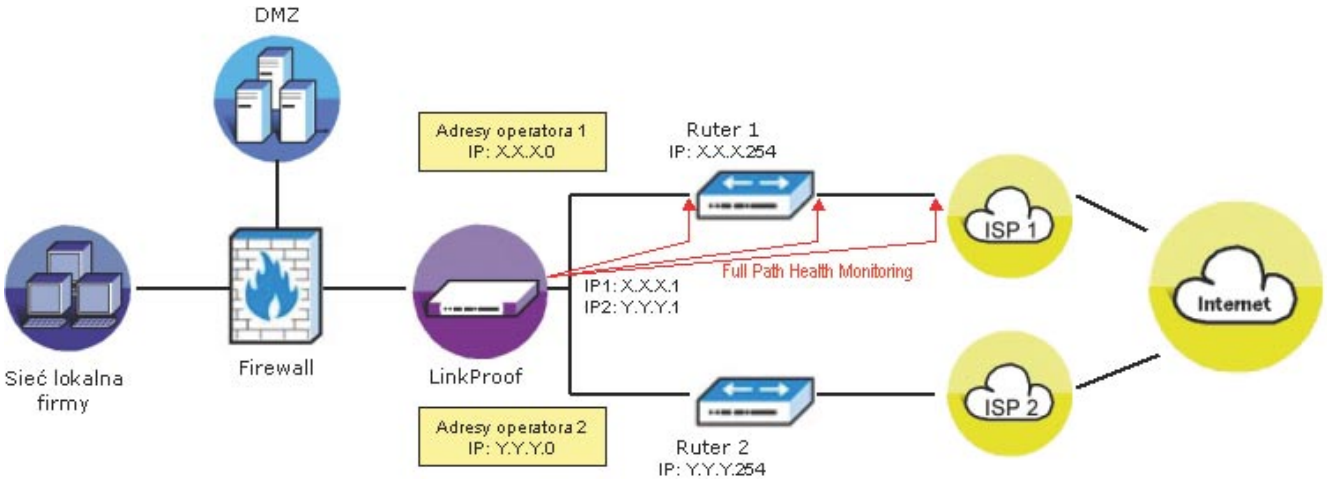
```
www.firma.pl          IN  NS   linkproof1.firma.pl
linkproof1.firma.pl   IN  A    <IP LinkProof od strony ISP1>
ftp.firma.pl          IN  NS   linkproof1.firma.pl
...
www.firma.pl          IN  NS   linkproof2.firma.pl
linkproof2.firma.pl   IN  A    <IP LinkProof od strony ISP2>
ftp.firma.pl          IN  NS   linkproof2.firma.pl
...
```

- operator ISP2 (serwer_dns_isp2):

```
www.firma.pl          IN  NS   linkproof2.firma.pl
linkproof2.firma.pl   IN  A    <IP LinkProof od strony ISP2>
ftp.firma.pl          IN  NS   linkproof2.firma.pl
...
www.firma.pl          IN  NS   linkproof1.firma.pl
linkproof1.firma.pl   IN  A    <IP LinkProof od strony ISP1>
ftp.firma.pl          IN  NS   linkproof1.firma.pl
...
```

Wykrywanie awarii łączy

Zastosowany w LinkProof algorytm Full Path Health Monitoring (rysunek 2) odpowiada za wykrywanie awarii łączy na całej ścieżce transmisji danych. Odbywa się to poprzez analizowanie stanu urządzeń występujących na drodze transmisji jak np. ruterów, serwerów, czy systemów firewall/IDS. Równoważenie obciążenia ruchu sieciowego odbywa się tylko na sprawnych łączach. Mechanizm wykry-

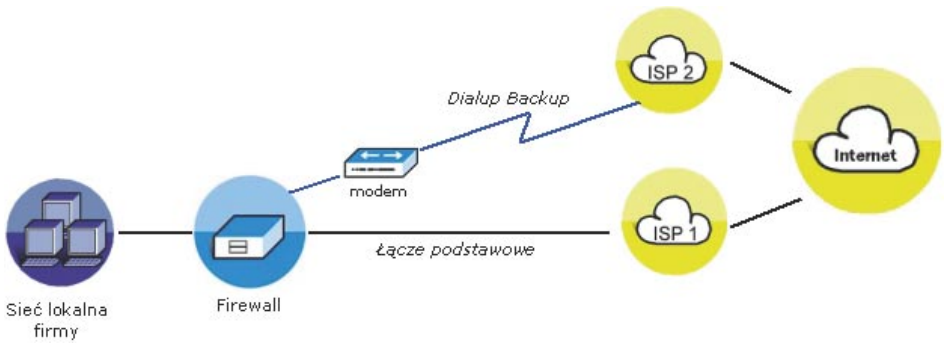


Rys. 2: Analiza stanu łącza odbywa się na całej ścieżce transmisji danych

wania awarii może w zależności o potrzeb wykorzystywać następujące techniki:

- ARP - wysyłane jest zapytanie ARP do adresu docelowego i analizowana odpowiedź ARP,
- Ping - wysyłane jest zapytanie ICMP Echo do adresu docelowego i analizowana odpowiedź,
- FTP - wykonywane są polecenia USER i PASS na serwerze FTP, a po zalogowaniu analizowany wynik polecenia SYST,
- HTTP - wysyłane jest zapytanie HTTP i testowany określony URL (metody GET, POST lub HEAD),
- HTTP format (proxy/Web) - wysyłane jest zapytanie HTTP i analizowany nagłówek i treść odpowiedzi HTTP w zakresie zawartości określonego tekstu (w razie potrzeby wykonywane jest uwierzytelnianie użytkownika HTTP),
- IMAP4 - wykonywane jest polecenie LOGIN na serwerze IMAP,
- LDAP - wykonywane są operacje dowiązania i odłączenia od serwera LDAP.

Urządzenie odpowiedzialne za obsługę i wykrywanie awarii łączy samo powinno działać w konfiguracji HA (ang. high availability). W przypadku LinkProof polega to na połączeniu dwóch fizycznych urządzeń w klaster tak, aby tworzyły jeden logiczny, odporny na awarie system. Dodatkowo od urządzeń brzegowych sieci wymagane są możliwości zarządzania pasmem i ochrony przed intruzami. LinkProof posiada wbudowany, pełnowartościowy system wykrywania intruzów Radware DefensePro funkcjonujący w trybie in-line. Pozwala także na skonfigurowanie portów lustrzanych (ang. port mirroring) i podłączenie do nich zewnętrznych systemów wykrywania intruzów (np. NetScreen-IDP, Snort, ISS). Zarządzanie pasmem polega na ustalaniu dla poszczególnych użytkowników i aplikacji wartości dostępnego pasma sieci oraz pasma gwarantowanego i priorytetów. Dodatkowo LinkProof umożliwia klasyfikowanie pakietów poprzez wartości Diffserv (Differentiated Services Code Point) lub ToS (Type of Service).



Rys. 3: Urządzenie firewall/VPN automatycznie zestawia łącze zapasowe Dialup

Zapasowe łącze Dialup

Protokoły dynamicznego rutingu oraz dedykowane urządzenia do obsługi wielu łączy są powszechnie wykorzystywane w centralach i większych oddziałach firm. W przypadku małych sieci rozwiązania takie są zbyt kosztowne. Producenci firewall/VPN opracowali dla takich zastosowań urządzenia obsługujące zapasowe łącze Dialup. W razie awarii łącza podstawowego urządzenie firewall/VPN automatycznie poprzez modem zestawia drugie połączenie i kontynuuje komunikację.

Koncepcja ochrony przed awariami łącza w urządzeniach firewall/VPN została przedstawiona na rysunku 3. Taką funkcjonalność dostarcza m.in. NetScreen w modelach 5XT i 5GT, Check Point w urządzeniach VPN-1 Edge X16, X32 i XU (pierwszy kwartał 2004) oraz SonicWall w modelach TELE3 SP i TELE3 Spi. Oprócz obsługi zapasowego łącza Dialup wymagane jest także skuteczne wykrywanie awarii łącza podstawowego oraz odtwarzanie otwartych tuneli VPN.

Więcej informacji na temat rozwiązań przedstawionych w artykule można znaleźć w serwisie www.clico.pl