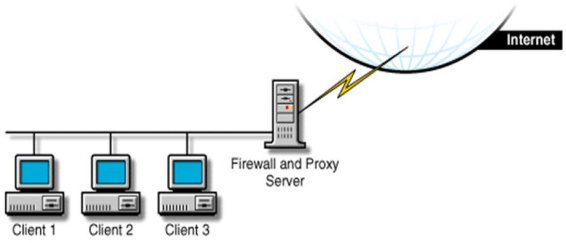
Usługi dodatkowe systemów firewall

Systemy firewall oferują wiele dodatkowych usług, które pomagają zabezpieczyć sieć bądź przyspieszyć jej pracę. Wśród nich na szczególne wyróżnienie zasługują Proxy Cache Services. Usługa ta umożliwia zoptymalizowanie ruchu na łączu WAN poprzez przechowywanie informacji (stron WWW), do których często odwołują się użytkownicy sieci; zwykle jest to element zintegrowany z serwerami pośredniczącymi.

W przypadku przyspieszania pracy klientów lokalnej sieci, Proxy Cache Server umieszczamy pomiędzy nimi a Internetem. Wówczas żądania o strony umieszczone w pamięci serwera są obsługiwane z prędkością LAN, a łącze WAN nie jest wcale obciążane.

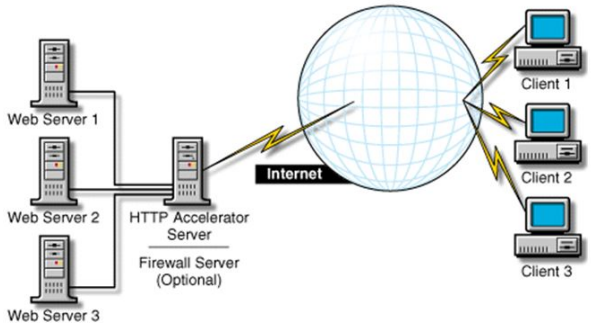
Rysunek 4



źródło własne

W przypadku intensywnie eksploatowanych serwerów WWW, umieszczonych w głębi sieci lokalnej, również warto zastosować Proxy Cache Server. Odciąży on serwery i zmniejszy transmisję w sieci LAN.

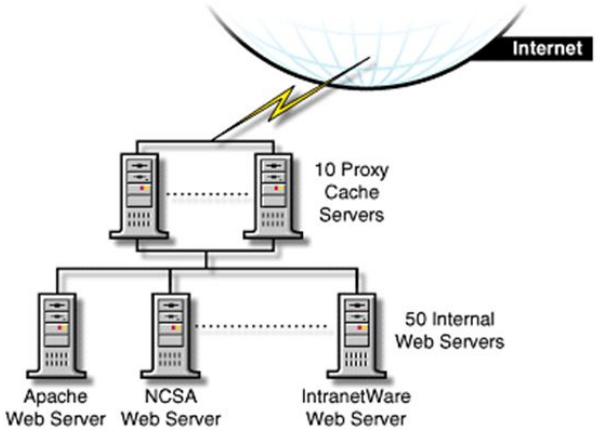
Rysunek 5



źródło własne

W przypadku bardzo dużych i intensywnie eksploatowanych serwisów WWW możemy użyć kilku połączonych równolegle Proxy Cache Server. Mogą one obsługiwać serwery WWW różnych producentów.

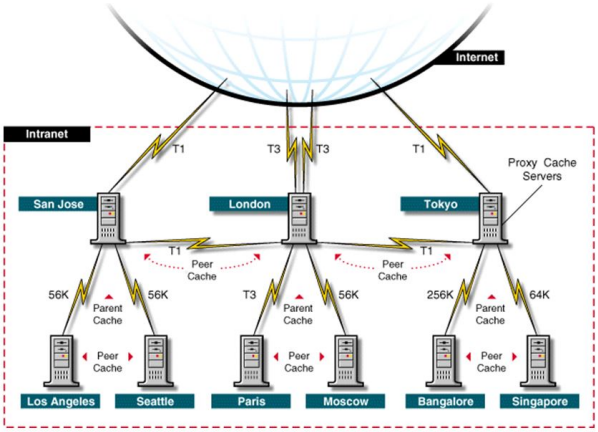
Rysunek 6



źródło własne

Gdy nasza sieć jest jednym z wielu rozrzuconych elementów sieci korporacyjnej, warto zastosować hierarchiczne połączenie wielu Proxy Cache Servers. Można również połączyć serwery na tym samym poziomie drzewa, uzyskując ten sposób wielopiętrowe przyśpieszenie pracy całej sieci. Taka budowa zwiększa szansę na znalezienie poszukiwanej strony w pamięci podręcznej. Dostęp do stron rzadko używanych jest wolniejszy, ale i tak przewyższa prędkość odnalezienia strony w Internecie.

Rysunek 7

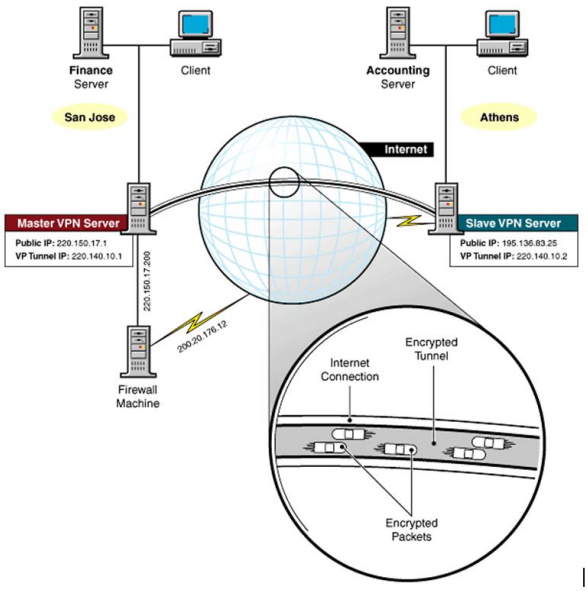


źródło własne

W pracy serwera bardzo istotne jest odpowiednie ustawienie parametrów. Przede wszystkim czasu przechowywania stron w pamięci podręcznej, czasu, po którym strona staje się nie aktualna, ilość miejsca przeznaczonego na cache.

Wiele firm, które potrzebują ciągłej wymiany informacji, staje przed dużym problemem – jak połączyć sieci lokalne wielu oddziałów oddalonych od siebie o setki, a nawet tysiące kilometrów. Wykupienie łącza dzierżawionego jest bardzo drogie, a czasem wręcz niemożliwe. Jedynym wyjściem staje się podłączenie wszystkich filii do sieci globalnej, takiej jak Internet. Virtual Private Network to usługa, która pozwala łączyć kilka sieci prywatnych tunelami, przez które przenoszone są tylko informacje zaszyfrowane. Szyfrowanie całych pakietów znacznie zwiększa bezpieczeństwo połączenia, ponieważ ukrywa numery połączeń i przesyłane dane.

Rysunek 8



źródło własne

Serwer z VPN zainstalowany na obrzeżu sieci umożliwia zarządzanie całą siecią wirtualną z dowolnego miejsca, co dodatkowo upraszcza administrację. Jedynym elementem, który powinien zostać przekazany tradycyjną metodą jest klucz (w BorderManager firmy Novell klucz jest 40- lub 128-bitowy; na eksport poza terytorium USA klucza 128-bitowego nałożone są spore restrykcje) umożliwiający nawiązanie zaszyfrowanego połączenia.

Narzędzia w rodzaju Novell IP Gateway umożliwiają sieciom pracującym z innymi protokołami, bądź z adresami IP, które nie są unikalne, korzystanie z sieci Internet. Dają możliwość całemu systemowi na korzystanie z jednego adresu IP, który również może być przydzielany dynamicznie. Umożliwia to firmie korzystającej np. z protokołu IPX na podłączenie do Internetu za pomocą modemu u dostawcy przydzielającego adresy dynamicznie (TP S.A.). Dodatkową zaletą zwiększającą bezpieczeństwo przy korzystaniu z takich usług jest ukrycie adresów lokalnych systemu.

Usługa Network Address Translation (NAT), podobnie jak IP Gateway, pozwala klientom, którzy nie posiadają unikalnych adresów, korzystać z Internetu. Dodatkowo może pracować jako filtr pozwalający tylko na niektóre połączenia z zewnątrz i

gwarantujący, że wewnętrzne połączenia nie będą inicjowane z sieci publicznej.

W celu precyzyjnego określenia praw rządzących dostępem do sieci tworzy się tak zwane listy reguł. Listy takie opisują prawa poszczególnych obiektów do korzystania z określonych usług/protokołów sieciowych, zezwalają na pewne rodzaje połączeń z zewnątrz jednocześnie zabraniając innych, mogą limitować liczbę połączeń z jakiegoś adresu albo ograniczać liczbę jednoczesnych połączeń. Przykładowo, kierownictwo firmy może zabronić pracownikom w określonych godzinach korzystania z usługi http z konkretnych miejsc sieci (co, oczywiście, jest decyzją polityczną). Edytor reguł jest narzędziem, przy pomocy którego budujemy i modyfikujemy zbiory reguł oraz wiążemy aplikacje z protokołami, a tym z kolei przypisujemy interfejsy sieciowe. Na użytek zaawansowanych administratorów tworzone są specjalne języki skryptowe, ułatwiające automatyzowanie konfigurowania serwera.

Integralną częścią systemów firewall jest mechanizm o zbliżonej roli do „czarnej skrzynki" w samolotach, śledzący i rejestrujący wszelkie wydarzenia w sieci. Dzięki monitorowaniu uwadze administratora z pewnością nie umknie, na przykład, 30-krotna nieudana próba zdalnego logowania się do systemu. Innym zastosowaniem jest analiza adresów, z którymi najczęściej nawiązywane są połączenia przez lokalnych użytkowników, gdyż dane takie są istotne do efektywnego skonfigurowania serwera proxy. Jednocześnie zarządca ma wgląd w dziennik błędów, gdzie zachowywane są ostrzeżenia o występowaniu wszelkich problemów z poprawnością transmisji. W przypadkach, gdy zachodzi uzasadnione podejrzenie, iż nastąpiło włamanie do sieci, system monitorujący może samodzielnie podjąć akcję zdefiniowaną przez administratora, na przykład decyzję o zerwaniu połączenia albo uruchomieniu „alarmu".

polecamy stronę pisanie prac - fachowa pomoc w pisaniu prac.