

Novell BorderManager - Poradnik kupującego

Czy Państwa firma chciałaby...

- chronić firmę przed nielegalnymi materiałami, które pracownicy mogą pobierać z Internetu?
- chronić firmę przed wirusami, które mogą zostać przypadkowo pobrane z Internetu wraz z innymi plikami?
- bezpiecznie podłączyć do sieci korporacyjnej oddziały i użytkowników mobilnych?
- wykorzystywać Internet jako narzędzie pracy, nie pozwalając jednak, by niepotrzebne informacje rozpraszaly pracowników i odrywały ich od czynności służbowych?
- jak najlepiej wykorzystać dostępną przepustowość, zwiększając wydajność sieci?

Rozwiązanie Państwa problemów biznesowych za pomocą oprogramowania Novell BorderManager

Ochrona firmy

- Funkcja sterowania dostępem z uwzględnieniem ról pozwala określić, do których zasobów użytkownicy mogą uzyskać dostęp. Dotyczy to także zasobów internetowych.
- Rozwiązanie umożliwia wybiórcze blokowanie niepożądanych i nieprzydatnych materiałów tak, aby nie przedostawały się do sieci przedsiębiorstwa.
- Obrzeże sieci zabezpieczają zapory chroniące przed atakami, a także serwery forward-proxy, które można zainstalować na styku sieci przedsiębiorstwa z Internetem.
- Wirtualne sieci prywatne umożliwiają połączenie z oddziałami terenowymi i użytkownikami, nie naruszając poufności przesyłanych danych.
- Mechanizmy filtrowania pozwalają chronić sieć przed szkodliwymi lub nielegalnymi materiałami, nie pozwalając im przedostać się do systemu.
- „BorderManager jest nieodzownym elementem infrastruktury zabezpieczeń. [...] Umożliwia nam monitorowanie i sterowanie dostępem do Internetu, a tym samym wykrywanie potencjalnych nadużyć w naszej sieci” (Lars Wiklund, kierownik projektu, urząd miasta Sztokholmu)

Zapewnienie produktywności

- Rozwiązanie to umożliwia ograniczenie dostępu pracowników do stron internetowych niezwiązanych z wykonywanymi obowiązkami, nie utrudniając zarazem korzystania ze stron zawierających informacje potrzebne do pracy.
- Dostęp z uwzględnieniem tożsamości gwarantuje, że użytkownicy mogą korzystać z zaaprobowanych materiałów dostępnych w Internecie.
- Funkcja filtrowania materiałów umożliwia monitorowanie sposobu, w jaki użytkownicy korzystają z Internetu, aby zapobiec wprowadzaniu do sieci niepożądanych materiałów pobieranych z Internetu. Ograniczenia można dostosować do potrzeb poszczególnych użytkowników.
- „Wyniki różnych badań potwierdzają, że niewłaściwe korzystanie z Internetu wiąże się ze znacznym obniżeniem produktywności. Poważne wątpliwości wiążą się z rodzajem materiałów, do jakich pracownicy mają dostęp. Problemy takie, jak molestowanie seksualne, szerzenie nienawiści itp. wiążą się z materiałami z Internetu, niestosownymi ze względu na atmosferę w firmie” ITWorld, „Peer Pressure: Your Surf Control Advantage” („Wpływ współpracowników. Zalety kontroli dostępu do Internetu”), 28 listopada 2001 r.

Zwiększenie wydajności sieci

- Buforowanie na serwerze proxy jest niedrogą alternatywą wobec kosztownych modernizacji sprzętu. Metoda ta umożliwia maksymalne wykorzystanie dostępnej obecnie przepustowości sieci, bez ponoszenia kolejnych kosztów inwestycyjnych.
- Serwery forward proxy buforują często pobierane materiały tak, aby kolejne żądania pobrania danych nie musiały być realizowane przez Internet.
- Funkcje monitorowania i filtrowania ograniczają ruch niezwiązany z działalnością firmy przesyłany w jej sieci. Pozwala to zachować kosztowną przepustowość wyłącznie do celów służbowych. Dzięki temu pracownicy mogą o wiele szybciej wykonywać zadania, gdyż sieć nie jest zatłoczona zbędnym ruchem niemającym nic wspólnego z działalnością firmy.

Czynniki decydujące o konkurencyjności / mocne strony rozwiązania

- W przypadku innych rozwiązań funkcje filtrowania materiałów oferowane są jako odrębne produkty. Oprogramowanie BorderManager jest zintegrowanym rozwiązaniem zabezpieczającym, dzięki któremu pracownicy mogą koncentrować się na swoich obowiązkach.
- Oprogramowanie sieci VPN innych producentów kosztuje od 2 tys. do 22 tys. USD. W ramach rozwiązania BorderManager jest ono dostępne bezpłatnie.
- Oprogramowanie ISA Server 2000 firmy Microsoft nie obejmuje filtrowania pobieranych materiałów i oferuje mniej warstw zabezpieczeń. Ponadto współpracuje wyłącznie w ramach środowiska Windows 2000.

Wyjaśnianie Państwa wątpliwości

Wątpliwość: Każdy korzysta swobodnie z Internetu. O co tyle hałasu?

Odpowiedź: Nawet gdyby byli Państwo skłonni płacić pracownikom niewykonującym swoich obowiązków, bezproduktywne korzystanie z Internetu może wpłynąć na wyniki finansowe firmy – i to poważnie. Po pierwsze, wiąże się ono z wykorzystaniem części przepustowości sieci, za którą trzeba słono płacić. Jeśli korzystanie z sieci ma związek z działalnością firmy, koszt ten może się kiedyś zwrócić w postaci wyników działań marketingowych czy badawczych, jeśli jednak ma ono na celu wyłącznie rozrywkę, firma nic na tym nie skorzysta. Jeden pracownik pobierający duży plik multimedialny, np. zapowiedź filmu, może poważnie ograniczyć przepustowość sieci i spowolnić jej działanie. Do tego niekontrolowane korzystanie z Internetu naraża firmę na szereg zagrożeń, począwszy od wirusów, a skończywszy na pozwach sądowych. W przypadku braku funkcji filtrowania pobieranych materiałów nie ma możliwości wykrycia wirusów, zanim przedostaną się do sieci. Jeśli zaś pracownik drukuje na służbowej drukarce zdjęcia pornograficzne, firma może zostać pozwana za tworzenie atmosfery molestowania seksualnego w miejscu pracy. Zdaniem jednego z klientów, BorderManager „chroni także studentów i innych mieszkańców przed nieuzasadnionymi oskarżeniami o podejmowanie nielegalnych działań przez Internet. W gruncie rzeczy chcemy, by uczeni pracownicy mogli korzystać z sieci bez cenzury, ale chcemy mieć możliwość śledzenia nadużyć” (Lars Wiklund, urząd miasta Sztokholmu).

Więcej informacji: <http://www.novell.com/products/bordermanager>