

# Novell® BorderManager® 3.8

Ochrona firmowej Sieci przed zagrożeniami  
wewnętrznymi i zewnętrznymi

[www.novell.pl](http://www.novell.pl)

TECHNICZNY ARTYKUŁ PRZEGLĄDOWY



Novell®

# Skuteczna kontrola dostępu i zabezpieczenia firmowej sieci

Wiele firm wskazuje na obawy dotyczące bezpieczeństwa jako przyczynę swojej niechęci do otwarcia swojej sieci na Internet. Trudno się temu dziwić, skoro do opinii publicznej trafiają tak liczne przykłady naruszeń bezpieczeństwa. W dorocznej ankiecie firmy Computer Institute 90% respondentów z dużych przedsiębiorstw i placówek administracji państwowej przyznało, że w ciągu ostatnich 12 miesięcy w ich organizacjach odnotowano przypadki włamań. Novell® BorderManager® 3.8 może je niemal całkowicie wyeliminować, ponieważ stanowi zintegrowane rozwiązanie zapewniające bezpieczeństwo, które chroni firmowe sieci przed zagrożeniami wewnętrznymi i zewnętrznymi.

## WPROWADZENIE

Novell BorderManager to jedno z najważniejszych rozwiązań Novella do kontroli dostępu i zabezpieczania sieci. Za pomocą jego skutecznych mechanizmów opartych na usługach katalogowych można kontrolować, usprawniać i monitorować dostęp użytkowników do Internetu. Ponieważ BorderManager kontroluje dostęp na podstawie danych identyfikacyjnych i wykorzystuje mechanizm forward proxy, można go stosować do ochrony wewnętrznej sieci przed przedostawaniem się do niej niepożądanych treści internetowych przy zachowaniu wyjątkowo wysokiej wydajności. Novell BorderManager udostępnia ponadto usługi wirtualnych sieci prywatnych (VPN), zapórę (firewall) o jakości potwierdzonej certyfikatem branżowym oraz skalowalny mechanizm filtrowania treści — wszystko po to, by sieć znajdowała się pod ochroną, a użytkownicy mogli spokojnie wykonywać swoją pracę.

Novell BorderManager obsługuje standardy branżowe oraz korzysta z zabezpieczeń i skalowalności usług katalogowych Novell eDirectory™ działających w sieciach NetWare®, Windows NT\*/2000/Me/XP i UNIX\*. W ramach integracji z Novell eDirectory oprogramowanie Novell BorderManager umożliwia przyznawanie dostępu do zasobów na podstawie profilu użytkownika — chroniąc w ten sposób zasoby sieciowe przed nieupoważnionym dostępem i ułatwiając korzystanie z sieci użytkownikom, którzy automatycznie uzyskują dostęp do niezbędnych im zasobów.

Dzięki ochronie zarówno wewnętrznych, jak i zewnętrznych granic sieci, BorderManager umożliwia stworzenie środowiska informatycznego odpowiadającego strategii

ONE NET firmy Novell. Wówczas można wykorzystywać połączone zasoby z intranetu, ekstranetu i Internetu i zapewnić użytkownikom dostęp do wydajnych, bezpiecznych rozwiązań e-biznesowych.

Novell BorderManager jest jednym z ważniejszych rozwiązań Novella do kontroli dostępu i zabezpieczania sieci. Pozwala on firmom na rozwinięcie infrastruktury biznesowej poza obręb firmowej zapory bez narażania się na utratę bezpieczeństwa..

## KONTROLA DOSTĘPU

Ruch w sieci generowany w związku z komunikacją internetową pochłania większość przepustowości łączy. W biurach pozostawionych bez nadzoru użytkownicy poświęcają sporą część swojego czasu pracy na poszukiwanie stron internetowych dla własnej przyjemności (np. serwisów informacyjnych i rozrywkowych), ograniczając tym samym przepustowość dostępną dla innych pracowników.

Mechanizm kontroli dostępu BorderManagera umożliwia wprowadzenie reguł, które ograniczają dostęp użytkowników do treści internetowych według różnych kryteriów. Można np. kontrolować poczynania użytkowników w zależności od typu usługi, węzła lub adresu sieciowego, adresu URL, pory dnia, rodzaju treści, tożsamości użytkownika, przynależności do grupy i wielu innych kryteriów. Kontrola dostępu gwarantuje, że przepustowość łączy wewnętrznej sieci jest wykorzystywana wyłącznie do celów zawodowych, związanych z działalnością firmy. Mechanizm ten może ponadto chronić użytkowników przed dostępem do potencjalnie szkodliwych stron internetowych, np. zawierających wirusy.

Kontrola dostępu zapewnia szereg korzyści związanych z bezpieczeństwem, m.in.:

- zapewnia wszystkie poziomy bezpieczeństwa, w tym na poziomie sieci (zapora poziomu I), obwodu (zapora poziomu II) i aplikacji (zapora poziomu III)
- pozwala na stosowanie ogólnych zasad bezpieczeństwa, które można dostosowywać pod kątem poszczególnych użytkowników, grup użytkowników, pór dnia, aplikacji i innych kryteriów
- określa, które żądania mają zostać zrealizowane lub odrzucone; w zależności od tego, czy dane żądania przekazano za pośrednictwem usług proxy, czy wirtualnej sieci prywatnej.

Mechanizm kontroli dostępu Novell BorderManagera obejmuje dwa składniki: reguły dostępu i listy kontroli dostępu.

### Reguły dostępu

Reguły dostępu konfigurowane w Novell eDirectory stanowią główny element kontroli dostępu. Serwer Novell BorderManagera — umieszczony zwykle pomiędzy firmowym intranetem a Internetem — stosuje te reguły do wszystkich żądań, bez względu na to, czy przekazano je za pośrednictwem usług proxy, czy wirtualnej sieci prywatnej.

Tworząc reguły dopuszczania (Allow) lub odrzucania (Deny), można przyznać dostęp do każdego z poniższych zasobów lub odmówić go:

- wiele sieci i usług internetowych
- usługi proxy oprogramowania Novell BorderManager
- wirtualne sieci prywatne
- adresy URL.

Aby zapewnić pełne bezpieczeństwo, reguły dostępu można ponadto skonfigurować na następujących poziomach obiektów Novell eDirectory:

- kraj (Country — C)
- przedsiębiorstwo lub instytucja (Organization — O)
- jednostka organizacyjna (Organizational Unit — OU)
- serwer (Server).

### Listy kontroli dostępu

Gdy Novell BorderManager zostanie załadowany na serwer, gromadzi on reguły dostępu utworzone na każdym poziomie obiektów Novell eDirectory. Najpierw zbiera reguły z obiektu Server, następnie z obiektu Organizational Unit znajdującego się nad obiektem Server itd. Zgromadzone zestawy reguł dostępu są wykorzystywane do utworzenia list

kontroli dostępu (access control lists — ACL) na serwerze Novell BorderManagera. Takie skonsolidowane listy reguł kontrolują miejsca docelowe lub usługi, do których obiekty mogą uzyskać dostęp za pośrednictwem Novell BorderManagera. Decydują one również, kiedy dany obiekt może uzyskać do nich dostęp. Możliwość konfigurowania i przechowywania reguł dostępu w różnych obiektach Novell eDirectory pozwala na utworzenie hierarchicznych zależności między regułami dotyczącymi kontroli dostępu w celu blokowania treści na różnych poziomach. Umożliwia to blokowanie dostępu do Internetu w czasie godzin pracy wszystkim pracownikom, z wyjątkiem np. zatrudnionych w dziale marketingu.

Kontrola dostępu może również chronić firmową sieć przed szkodliwymi lub nielegalnymi treściami, do których użytkownicy mogliby nieumyślnie uzyskać dostęp. Pracownik mógłby np. zajrzeć na strony internetowe, która zawierają wirusy. Pracownik może zainfekować nie tylko własną stację roboczą, lecz również całą wewnętrzną sieć. Kontrola dostępu gwarantuje, że szkodliwe treści nie przedostaną się do firmowej sieci.

## USŁUGI PROXY

Usługi proxy oprogramowania Novell BorderManager zwiększają bezpieczeństwo i wydajność sieci oraz produktywność użytkowników, a przy tym zmniejszają podatność sieci na ataki. Usługi proxy dotyczące aplikacji są brankami na poziomie aplikacji, umożliwiającymi kontrolowanie portów i adresów, do których użytkownicy mają uprawnienia dostępu. Usługi proxy wprowadzają reguły, które decydują o przyznaniu lub odmówieniu dostępu z określonego źródła do określonego punktu docelowego. Źródłem może być adres IP, zakres adresów, adres podsieci lub obiekt Novell eDirectory (użytkownik, grupa lub kontener). Punktami docelowymi mogą być usługi działające na serwerze Novell BorderManagera, adresy/porty IP, wzorce adresów URL lub kategorie z bazy danych SurfControl\* Content Database, N2H2\* lub Connectotel.

Usługa proxy dotycząca aplikacji HTTP sprawdza uprawnienia dostępu za pośrednictwem Novell eDirectory oraz obsługuje tunelowanie w ramach warstwy Secure Sockets Layer (SSL) i certyfikaty użytkowników. Jednoczesne zastosowanie tunelowania SSL i certyfikatów użytkowników tworzy szyfrowane połączenie między klientem a serwerem, które chroni informacje przed przechwyceniem i manipulowaniem.

Usługi proxy zwiększają ponadto wydajność sieci poprzez buforowanie informacji, które są najczęściej pobierane z Internetu. Dzięki temu oszczędza się przepustowość łączy poświęcaną na przekazywanie żądań dotyczących tych samych informacji, zmniejsza obciążenie zdalnego serwera

i skraca czas potrzebny na pobranie treści. W konsekwencji wpływa to na zwiększenie produktywności użytkowników.

Usługi proxy Novell BorderManagera wykorzystują trzy główne rodzaje buforowania:

- **Forward proxy (przyspieszenie działania klientów internetowych).** W przypadku forward proxy, serwer proxy jest umieszczony pomiędzy klientami a Internetem. Serwer proxy przekazuje żądania pochodzące od klientów intranetowych do serwerów internetowych, wykorzystując odpowiednie protokoły, np. HTTP, FTP i Gopher. Następnie serwer proxy buforuje najczęstsze żądania dotyczące adresów URL, stron HTML i plików na serwerach FTP. Kolejne żądania dotyczące tych treści są realizowane przy wykorzystaniu bufora serwera proxy. Eliminuje to opóźnienia, które występują w przypadku dostępu do serwerów internetowych oraz minimalizuje ruch na łączach między firmową siecią a Internetem.
- **Hierarchiczne buforowanie dla Internet Caching Protocol (ICP) (przyspieszenie działania sieci).** Hierarchiczne buforowanie ICP jest realizowane za pomocą wielu serwerów proxy, tworzących strukturę hierarchiczną, zwaną inaczej topologią „siatki”. Charakteryzuje się ona tym, że serwery proxy są połączone zależnościami nadrzędny-podrzędny i równorzędne. Jeżeli wystąpi błąd, tj. gdy usługa proxy nie może znaleźć danej informacji na pierwszym serwerze, z jakim się kontaktuje, to komunikuje się z innymi serwerami należącymi do siatki. Najbliższy serwer proxy, w którego buforze znajdują się żądane informacje, przekazuje je do usługi proxy, która z kolei przesyła je do klienta. Dzięki zmniejszeniu obciążenia łączy sieci rozległych (WAN) hierarchiczne buforowanie ICP oszczędza przepustowość. Zostają ponadto zmniejszone opóźnienia w działaniu sieci, ponieważ żądane informacje są wysyłane z najbliższego serwera proxy. Skraca to czas oczekiwania na żądane dane. BorderManager obsługuje również hierarchie buforowanie CERN.
- **Reverse proxy (przyspieszenie działania serwera internetowego lub HTTP).** W przypadku wstecznego buforowania serwer proxy pełni rolę frontonu dla serwerów internetowych i buforuje wszystkie informacje, które są na nich przechowywane. Novell BorderManager zapewnia buforowanie reverse proxy dotychczasowym klientom, jednocześnie

Novell oferuje w pełni uniwersalne rozwiązanie tego typu w ramach Novell iChain®.

Usługi proxy oprogramowania Novell BorderManager obsługują następujące protokoły i aplikacje:

- HTTP (0.9, 1.0 i 1.1), w tym HTTPS i Secure Sockets Layer (SSL)
- FTP
- Domain Name System (DNS)
- Gopher
- Simple Mail Transfer Protocol/Post Office Protocol 3 (SMTP/POP3)
- Network News Transfer Protocol (NNTP)
- RealAudio\* i RealVideo\*
- Real Time Streaming Protocol (RTSP)
- SOCKS 4 i 5
- Generic TCP/UDP
- HTTP Transparent proxy
- Telnet Transparent proxy.

## WIRTUALNA SIEĆ PRYWATNA

Novell BorderManager oferuje ponadto usługi wirtualnych sieci prywatnych (VPN), które zapewniają bezpieczne połączenie z firmowym intranetem innym ośrodkiem intranetowym, zdalnym użytkownikom bądź partnerom handlowym za pośrednictwem publicznych łączy internetowych. Informacje przesyłane wirtualną siecią prywatną za pośrednictwem Internetu są szyfrowane, co zapobiega nieupoważnionemu dostępowi do nich. Sprawdza się ponadto poprawność informacji w celu wykrycia przypadków manipulowania nimi przez hakerów.

Usługi wirtualnych sieci prywatnych działają w protokołach IP i IPX, co pozwala na komunikowanie się z firmową siecią za pośrednictwem łączy internetowych. Usługi te współdziałają ponadto z systemem Novell eDirectory, który ułatwia zarządzanie wirtualną siecią prywatną. Pakiet Novell BorderManager cechuje się wysoką skalowalnością — może obsługiwać maksymalnie 256 ośrodków na jeden tunel i ponad 1500 użytkowników łączących się telefonicznie z zewnątrz na jeden serwer.

Novell BorderManager udostępnia oprogramowanie klienta wirtualnej sieci prywatnej do systemów Windows\* 95, 98, NT 4.0, 2000, Me i XP. Możliwe jest też wykorzystanie oprogramowania klienta VPN innych firm: VPN Tracker dla MAC\* OS i Openswan dla Linuksa.

Wirtualna sieć prywatna zapewnia zdalnym użytkownikom dostęp do zasobów sieciowych, a nad bezpieczeństwem tego dostępu czuwa zapora Novell Client Firewall 2.0, wchodząca w skład Novell BorderManagera.

## Architektura wirtualnej sieci prywatnej

Usługi wirtualnych sieci prywatnych są oparte na architekturze standardowej, zintegrowanej z technologią katalogową Novell eDirectory lub inną – zgodną z protokołem LDAP. Zapewnia to maksymalną elastyczność, ułatwia zarządzanie i administrowanie wirtualną siecią prywatną oraz pozwala użytkownikom na dostęp do zasobów sieciowych po jednokrotnej rejestracji.

## Zaawansowane metody uwierzytelniania

Novell BorderManager zawiera w sobie funkcjonalność Novell Modular Authentication Service (NMAS). Dzięki temu kontrola tożsamości użytkownika może być realizowana na wiele (ponad 50) zaawansowanych sposobów.

## Zgodność ze standardami

Jako rozwiązanie oparte o IPSec, Novell BorderManager współpracuje z dowolnymi urządzeniami certyfikowanymi pod kątem IPSec. Tunelowanie na potrzeby wirtualnej sieci prywatnej jest realizowane przy wykorzystaniu protokołów Internet Key Exchange (IKE) oraz Simple Key Management for Internet Protocols (SKIP). Pakiet ten korzysta z infrastruktury Novell International Cryptographic Infrastructure (NICI), standardowego oprogramowania szyfrującego firmy Novell. Umożliwia ona swobodne stosowanie kodu źródłowego na całym świecie bez naruszania ograniczeń licencyjnych RSA.

Novell BorderManager wspiera funkcje hash (Triple-DES, DES, SHA1, MD5 i inne) współużytkownika kluczy i mechanizmy szyfrowania danych.

## Integracja z Novell eDirectory

Novell BorderManager uwierzytelnia użytkowników za pośrednictwem Novell eDirectory, by zagwarantować, że z wirtualnej sieci prywatnej korzystają tylko upoważnione do tego osoby. Administratorzy mogą kontrolować dostęp do wirtualnej sieci prywatnej za pomocą list kontroli dostępu użytkowników, przechowywanych w drzewie katalogowym Novell eDirectory. Oznacza to, że administratorzy mogą zarządzać użytkownikami wirtualnej sieci prywatnej przy wykorzystaniu tego samego drzewa katalogowego Novell eDirectory, które służy im do zarządzania pozostałymi użytkownikami sieci. Nie muszą oni utrzymywać osobnego drzewa katalogowego dla użytkowników wirtualnej sieci prywatnej.

## Konfiguracja wirtualnej sieci prywatnej

Novell BorderManager pozwala firmom na ekonomiczne zapewnienie zdalnym użytkownikom komunikacji z sieciami lokalnymi przy

wykorzystaniu Internetu w charakterze taniej sieci szkieletowej. Można zastosować jedną z dwóch konfiguracji wirtualnej sieci prywatnej: ośrodek-ośrodek i klient-serwer.

## Wirtualna sieć prywatna typu ośrodek-ośrodek

Stosując wirtualną sieć prywatną typu ośrodek-ośrodek, przedsiębiorstwo może zespolić niezależne części sieci lokalnej w jedną, spójną sieć rozległą (WAN) przy wykorzystaniu Internetu w charakterze elementu łączącego. Dzięki temu, że usługi wirtualnych sieci prywatnych oprogramowania Novell BorderManager obsługują protokoły IP i IPX, części sieci lokalnej mogą być dowolnymi kombinacjami sieci IP i IPX™.

Wirtualną sieć prywatną typu ośrodek-ośrodek wdraża się, instalując serwer BorderManagera w każdym ośrodku i łącząc te serwery za pośrednictwem Internetu. Serwery można połączyć w topologii siatki, pierścienia lub gwiazdy. Wirtualną sieć prywatną typu ośrodek-ośrodek można również wykorzystać do zbudowania ekstranetu, który łączy firmową sieć z sieciami partnerów handlowych.

## Wirtualna sieć prywatna typu klient-serwer

Wdrażając wirtualną sieć prywatną typu klient-serwer, firma może zapewnić zdalnym użytkownikom ekonomiczny i bezpieczny dostęp do niezbędnych im zasobów sieciowych, niezależnie do miejsca pobytu użytkowników i lokalizacji zasobów.

Aby skorzystać z wirtualnej sieci prywatnej typu klient-serwer, użytkownik oprogramowania klienta Novell BorderManagera łączy się z serwerem Novell BorderManagera, który pełni rolę bramki do wirtualnej sieci prywatnej. Użytkownik może nawiązać połączenie PPP (Point-to-Point Protocol) z serwerem wirtualnej sieci prywatnej albo za pośrednictwem operatora Internetu, albo za pomocą oprogramowania do dostępu zdalnego.

W celu zagwarantowania optymalnej wydajności można tak skonfigurować oprogramowanie klienta Novell BorderManagera, aby szyfrowało tylko informacje wysyłane do i odbierane z chronionych sieci (zamiast szyfrowania wszystkich danych, niezależnie od miejsca ich przeznaczenia).

## ZAPORA

Zapory były pierwotnie barierami, które uniemożliwiały przedostawanie się do środka. Obecnie zaporą musi działać bardziej selektywnie. Jej zadanie nadal polega na blokowaniu nieupoważnionych użytkowników, ale musi ona ponadto umożliwiać dostęp do zasobów sieciowych klientom, partnerom, dostawcom i pracownikom. Zaporą Novell BorderManagera ma certyfikat ICASA

i zapewnia skuteczną ochronę przed niepożądanymi treściami internetowymi.

Novell BorderManager wykorzystuje kilka rodzajów filtrowania, dzięki czemu można bardzo dokładnie określić, jaki rodzaj ruchu w sieci będzie przekraczał granicę firmowej infrastruktury informatycznej. Dokładność ta jest konieczna w celu ochrony przed wirusami i atakami, m.in. typu denial-of-service (odmowa usługi). Dzięki filtrowaniu można ponadto kontrolować, do których serwisów internetowych mają dostęp pracownicy, eliminując w ten sposób pokusę zaglądania w czasie pracy na nieodpowiednie strony internetowe. Filtry oferowane przez oprogramowanie BorderManager konfiguruje się bardzo prosto za pomocą interfejsu przeglądarki internetowej.

W przypadku rozszerzania granic firmowej sieci przy wykorzystaniu usług wirtualnych sieci prywatnych, komputery-klienci użytkowników stają się punktami wejściowymi do wewnętrznej infrastruktury informatycznej. Dlatego Novell BorderManager zawiera zaporę Novell Client Firewall 2.0, która chroni użytkowników wirtualnej sieci prywatnej przed nieupoważnionym dostępem.

Pakiet Novell BorderManager zawiera następujące składniki zapor i filtrowania:

- filtrowanie pakietów
  - statyczne
  - dynamiczne
  - filtrowanie z dokładnością do części pakietów
  - filtrowanie bitów TCP ACK
- filtrowanie przy użyciu wzorców wirusów
- filtrowanie treści.

## Filtrowanie pakietów

Novell BorderManager wykorzystuje mechanizmy filtrowania pakietów, aby zapewnić podstawowy poziom ochrony sieci. Filtrowanie pakietów korzysta z adresów IP, co umożliwia odrzucenie żądań pochodzących z nieupoważnionych aplikacji internetowych. Można np. w godzinach pracy zablokować dostęp do programu typu komunikator (Instant Messenger) lub do radiostacji internetowych.

Novell BorderManager wykorzystuje kilka różnych metod filtrowania pakietów, w tym:

- statyczne filtrowanie pakietów
- dynamiczne filtrowanie pakietów
- filtrowanie pofragmentowanych pakietów
- filtrowanie bitów TCP ACK.

Każdy rodzaj filtrowania ma zalety, ale i ograniczenia, o czym można przeczytać niżej. Novell BorderManager oferuje najskuteczniejsze filtrowanie pakietów, jakie jest dostępne, umożliwiając łączenie wszystkich czterech metod.

## Stacyjne filtrowanie pakietów

To najmniej wyrafinowany rodzaj filtrowania. Akceptuje lub odrzuca pakiety według następujących czterech kryteriów:

- identyfikator protokołu, np. Transmission Control Protocol (TCP), User Datagram Protocol (UDP) i Internet Control Message Protocol (ICMP)
- źródłowy adres IP i numer portu
- docelowy adres IP i numer portu
- interfejs routera na potrzeby pakietów wchodzących lub wychodzących.

Reguły dotyczące statycznego filtrowania pakietów są wyjątkowo proste — przekazywane są albo wszystkie pakiety, albo żaden. Akceptuje się np. wszystkie pakiety TCP lub nie akceptuje się żadnego, albo zatwierdza się wszystkie żądania kierowane do konkretnego serwera internetowego lub nie zatwierdza się żadnego. Ten rodzaj filtrowania jest użyteczny przy blokowaniu komunikacji z całym serwisami internetowymi, np. Dilbert Zone czy eBay. Dzięki swej prostocie jest on bardzo efektywny, gdyż jego realizacja wymaga mniejszej mocy obliczeniowej i przepustowości niż w przypadku pozostałych rodzajów filtrowania. Połączenia z różnymi usługami, np. pocztą elektroniczną, FTP i Telnetem, mogą zostać zablokowane poprzez filtrowanie pakietów, próbujących skorzystać z danej usługi lub określonego numeru portu.

Zapory, których działanie opiera się na statycznym filtrowaniu pakietów, są urządzeniami warstwy sieciowej, które nie potrafią przetwarzać informacji dotyczących wyższych warstw. Nie mogą one sprawdzać żądań aplikacji ani śledzić danych o stanie aplikacji. Zapora obsługująca statyczne filtrowanie pakietów nie potrafi ustalić, sprawdzając po prostu nagłówek wchodzącego pakietu, czy dany pakiet jest pierwszym przesyłanym z zewnętrznego klienta do wewnętrznego serwera, czy też stanowi odpowiedź zewnętrznego serwera dla wewnętrznego klienta. Poziom bezpieczeństwa zapewniany przez tego rodzaju zaporę jest ograniczony.

## Dynamiczne filtrowanie pakietów

Dynamiczne filtrowanie pakietów, jakie oferuje Novell BorderManager, przewyższa ograniczenia narzucone przez reguły „wszystkie lub żaden”, które stosuje się w przypadku statycznego filtrowania pakietów. Filtrowanie dynamiczne pozwala wewnętrznemu klientowi na zainicjowanie sesji komunikacyjnej z zewnętrznym serwerem internetowym, ale uniemożliwia temu serwerowi zainicjowanie sesji z klientami wewnętrznymi. Kiedy wychodzący pakiet jest kierowany do Internetu, zostaje utworzony dynamicznie filtr odwrotny, który umożliwi przesłanie z powrotem pakietu z odpowiedzią.

Filtr odwrotny jest tworzony poprzez wydobycie następujących informacji o pakiecie:

- źródłowego adresu IP
- źródłowego interfejsu
- źródłowego portu
- docelowego adresu IP
- docelowego interfejsu
- docelowego portu
- typu protokołu.

Informacje te są przechowywane w tabeli, która jest porównywana z odpowiedzią. Jeżeli przychodząca wiadomość nie jest odpowiedzią na oryginalne żądanie, zostaje odrzucona. Ten tworzony dynamicznie zestaw filtrów jest wykorzystywany do decydowania o przekazywaniu kolejnych pakietów, aż do zamknięcia połączenia.

Aby pakiet przychodzący został uznany za odpowiedź, musi pochodzić z serwera i portu, do których został wysłany pakiet wychodzący. Dynamiczne filtrowanie pakietów obsługuje protokoły zarówno połączeniowe, jak i bezpołączeniowe (TCP, UDP, ICMP itd.).

Funkcja dynamicznego filtrowania pakietów monitoruje każde połączenie i ustanawia dla danego połączenia tymczasowy (ograniczony czasowo) wyjątek filtru wiadomości przychodzących. Umożliwia to blokowanie informacji pochodzących z określonego numeru portu i adresu, a jednocześnie przekazywanie danych płynących w przeciwną stronę z tego samego numeru portu i adresu.

### Filtrowanie pofragmentowanych pakietów

Funkcja filtrowania pofragmentowanych pakietów pomaga chronić sieć przed atakami typu denial-of-service (odmowa usługi), ponieważ sprawdza wszystkie pakiety i ich części.

Jedną z metod przeprowadzenia takiego ataku jest wykorzystanie części pakietów. Niektóre datagramy Warstwy 2 są dłuższe, niż przewiduje ustalony limit, są zatem dzielone na części. Pierwsza część zawiera pełny nagłówek i informacje transportowe, a kolejne pakiety wskazują tylko, do której części należą i w jakim porządku w niej występują.

Typowe zapory sprawdzają tylko pierwszy pakiet i przekazują kolejne części bez żadnej kontroli. Jeżeli pierwsza część zostanie odrzucona, serwer docelowy nie może odtworzyć kolejnych części i połączenie nie zostanie nawiązane.

Obecnie jednak hakerzy zalewają sieci wieloczęściowymi pakietami, które angażują dostatecznie dużo mocy obliczeniowej i przepustowości, aby spowolnić lub nawet zatrzymać ruch w sieci.

Niesprawdzone części pakietów powodują ponadto, że sieć staje się podatna na skanowanie portów. Działanie to daje hakerom informacje

o oprogramowaniu, które działa na danym komputerze, co może z kolei posłużyć do odkrycia słabych punktów serwera. Włączając bit informujący o podziale na części do pakietu, który tak naprawdę stanowi zamkniętą całość, potencjalni włamywacze mogą przysyłać pakiety poprzez zapory i otrzymywać z powrotem pakiety zawierające informacje o portach.

Aby zapewnić ochronę przed atakami wykorzystującymi fragmentację pakietów, Novell BorderManager sprawdza wszystkie pakiety, łącznie z ich częściami. Jeśli pierwszy pakiet zostaje odrzucony, Novell BorderManager odrzuca także wszystkie kolejne części, które mają te same źródłowe i docelowe adresy IP i interfejsy. Mechanizm ten jest wbudowany w stos IP (a nie do narzędzi filtrujących), dzięki czemu powstaje znacznie skuteczniejszy system zabezpieczeń.

### Filtrowanie bitów Transmission Control Protocol ACK (TCP ACK)

TCP to połączeniowy, niezawodny protokół komunikacyjny. Jeśli filtrowanie bitów TCP ACK jest uaktywnione, można zapobiec przedostawianiu się do sieci przychodzących pakietów żądań TCP. Uniemożliwia to włamywaczom inicjowanie sesji komunikacyjnych TCP z wewnętrznymi serwerami lub klientami. Jednocześnie nie blokuje to użytkownikom wewnętrznym możliwości inicjowania sesji komunikacyjnych TCP ze światem zewnętrznym.

Włączenie filtru bitów TCP ACK chroni ponadto sieć przed typowymi atakami, np. zsynchronizowany (SYN) zalew łączy.

### Filtrowanie treści

Aby ułatwić monitorowanie wykorzystywania Internetu oraz ustalanie i stosowanie reguł dostępu do niego, Novell BorderManager współpracuje z ponad 40 zdefiniowanymi przez partnerów (SurfControl, N2H2, Connectotel, ...) bazami kategorii internetowych.

Poprzez integrację z Connectotel obsługuje również darmową bazę squidGuard. Oprogramowanie to oferuje m.in. opcję sporządzania raportów, które mogą pomóc w śledzeniu wykorzystania Internetu w całej firmie lub przez poszczególnych pracowników.

Administratorzy ustalają reguły dostępu przy użyciu kategorii. Reguły te można umieszczać na serwerze, w jednostce organizacyjnej lub w obiektach należących do organizacji.

### Filtrowanie przy użyciu wzorców wirusów

Novell BorderManager oferuje ponadto mechanizm filtrowania przy użyciu wzorców wirusów, który chroni przed wirusami korzystającymi z protokołu HTTP, np. Nimda.

## ROZWIĄZANIA DO KONTROLI DOSTĘPU I ZABEZPIECZANIA SIECI

Novell BorderManager jest tylko jednym z rozwiązań Novella do kontroli dostępu i zabezpieczania sieci, które razem stanowią niezwykle efektywne połączenie produktów Novella. Wszystkie produkty Novella zapewniające bezpieczeństwo są oparte na usługach katalogowych, co umożliwia kontrolowanie dostępu do zasobów sieciowych z uwzględnieniem reguł ustalonych w firmie i danych identyfikacyjnych użytkowników. Do rozwiązań Novella zapewniających bezpieczeństwo należą m.in.:

- **Novell eDirectory** — umożliwia gromadzenie, przechowywanie, porządkowanie i wykorzystywanie wszystkich danych identyfikacyjnych, jakie są niezbędne w celu przyznawania pracownikom, klientom i partnerom indywidualnych uprawnień dostępu.
- **Novell Account Management** — integruje wszystkie platformy występujące w firmowej sieci, dzięki czemu można nimi zarządzać przy użyciu danych identyfikacyjnych przechowywanych w drzewie katalogowym eDirectory.
- **Novell iChain** — pomaga kontrolować w całej firmie zindywidualizowany dostęp do aplikacji oraz zasobów internetowych i sieciowych.
- **Novell Modular Authentication Service (NMAS)** — umożliwia stosowanie całego szeregu metod uwierzytelniania w celu zapewnienia najwyższego bezpieczeństwa sieci.
- **Novell SecureLogin** — pozwala użytkownikom na dostęp do wielu zasobów w drodze jednokrotnej rejestracji.
- **Novell BorderManager** — reguluje dostęp pracowników do Internetu i przyspiesza dostarczanie treści.
- **Novell Nsure Identity Manager™** — ogranicza zadania administracyjne, konwertując informacje i dostarczając je do wszystkich drzew katalogowych, baz danych i aplikacji.
- **Novell exteNd** — konsoliduje wszystkie zasoby sieciowe, udostępniając je pod postacią wygodnej, łatwej w użyciu strony internetowej.

Rozwiązania Novella do kontroli dostępu i zabezpieczania sieci pozwalają urzeczywistnić wizję ONE NET. Firmowy intranet, ekstranet i Internet mogą bezpiecznie współdziałać, tworząc jedną Sieć, zapewniającą klientom, partnerom i pracownikom bezpieczny i łatwy dostęp do zasobów sieciowych.

## PODSUMOWANIE

Novell BorderManager umożliwia firmom bezpieczne otwarcie granic ich sieci. Oferowane przez ten pakiet usługi zapór i wirtualnych sieci prywatnych zapewniają bezkonkurencyjną ochronę przed atakami zewnętrznymi i wewnętrznymi.

Z kolei usługi przekazywania proxy i mechanizmy buforowania zwiększają efektywność pracy i szybkość dostępu do Internetu, jak również umożliwiają filtrowanie szkodliwych lub niepożądanych treści internetowych.

## WYMAGANIA SYSTEMOWE

Wymagania sprzętowe serwera

- serwer PC wyposażony w procesor Pentium\* II lub szybszy
- karta graficzna o rozdzielczości Super VGA lub wyższej
- co najmniej jedna karta sieciowa
- napęd CD
- zalecana myszka podłączana do portu PS/2 lub szeregowego (nie jest konieczna)
- partycja systemu DOS o wielkości przynajmniej 250 MB
- zalecana wielkość woluminu SYS: 4 GB
- zalecany wolumin CACHE o wielkości co najmniej 2 GB
- zalecane 256 MB pamięci RAM

Wymagania dotyczące oprogramowania serwera

- system NetWare 5.1 z zestawem SP 6, NetWare 6.0 z zestawem SP3 lub NetWare 6.5
- eDirectory 8.6.2 (minimum) lub 8.7.1 (zalecane) z włączoną obsługą protokołu LDAP.

Wymagania dotyczące stacji roboczych

- z większości usług pakietu Novell BorderManagera można korzystać za pomocą dowolnego komputera dostosowanego do komunikacji w protokole IP, bez względu na konfigurację sprzętową czy system operacyjny
- jednokrotna rejestracja proxy jest dostępna na stacjach roboczych Windows z działającym klientem NetWare
- oprogramowanie klienta wirtualnej sieci prywatnej jest dostępne do systemów Windows 98, NT 4, 2000, Me i XP.

### **Informacje o firmie Novell**

Novell Inc. jest wiodącym dostawcą rozwiązań informatycznych zapewniających bezpieczne zarządzanie tożsamością (Novell Nsure), umożliwiających tworzenie aplikacji sieci Web (Novell exteNd) oraz oferujących międzyplatformowe usługi sieciowe (Novell Nterprise). Wszystkie te rozwiązania są wspierane przez doradztwo strategiczne i usługi profesjonalne (Novell Ngage). Novell działa aktywnie w społeczności open source i jest właścicielem marek Ximian i SUSE LINUX. Silnie angażuje się w rozwój rozwiązań open source i oferuje kompleksowe rozwiązania i usługi linuksowe dla przedsiębiorstw obejmujące wszystkie elementy: od komputerów biurowych aż po serwer. Stworzona przez Novella wizja jednej Sieci (one Net) — świata pozbawionego ograniczeń w przepływie informacji — pozwala korzystać z informacji w sposób bezpieczny i opłacalny.

Dodatkowe informacje można uzyskać w Centrum Obsługi Klienta firmy Novell pod numerem 0-800-22-NOVL (0-800-22-6685) lub znaleźć pod adresem [www.novell.pl](http://www.novell.pl)

© 2004 Novell Inc. Wszelkie prawa zastrzeżone. Novell, NetWare, BorderManager i iChain są zastrzeżonymi znakami towarowymi, a eDirectory, IPX, NMAS i Novell Authorized Reseller znakami towarowymi firmy Novell Inc. w Stanach Zjednoczonych i w innych krajach.

\*Windows jest zastrzeżonym znakiem towarowym firmy Microsoft Corporation. UNIX jest zastrzeżonym znakiem towarowym firmy X/Open Company Ltd. SurfControl jest zastrzeżonym znakiem towarowym firmy SurfControl Plc. RealAudio jest zastrzeżonym znakiem towarowym, a RealVideo jest znakiem towarowym firmy RealNetworks Inc. Pentium jest zastrzeżonym znakiem towarowym firmy Intel Corporation. Inne wymienione znaki towarowe są własnością odpowiednich podmiotów.

## Szkolenia

Listę autoryzowanych ośrodków szkoleniowych w Polsce, informacje o szkoleniach i programach przyznawania certyfikatów można znaleźć pod adresem [www.novell.pl/programs/index.html](http://www.novell.pl/programs/index.html)

## Usługi pomocy technicznej

Informacje o usługach doradztwa i pomocy technicznej można znaleźć pod adresem <http://www.novell.pl/npsp>

## Informacje dodatkowe

Więcej informacji można uzyskać kontaktując się z bezpłatną infolinią firmy Novell w Polsce — 0 800 22 66 85 oraz na stronach internetowych [www.novell.pl](http://www.novell.pl)

## Novell Polska

ul. Wspólna 47/49  
00-684 Warszawa  
Tel. (22) 537 5000  
Faks (22) 537 5098

## Bezpłatna infolinia:

0-800-22-NOVL  
(0-800 226685)  
[infolinia@novell.pl](mailto:infolinia@novell.pl)

[www.novell.pl](http://www.novell.pl)