Technical White Paper

UserGate Firewall & Proxy Server 5

Czym jest UserGate oraz do czego służy?

W jaki sposób UserGate chroni Twoją sieć?

W jaki sposób UserGate zarządza dostępem do Internetu?

W jaki sposób UserGate zarządza aktywnością sieciową oraz Internetową użytkowników?

W jaki sposób UserGate optymalizuje zarządzanie ruchem sieciowym?

Spis treści

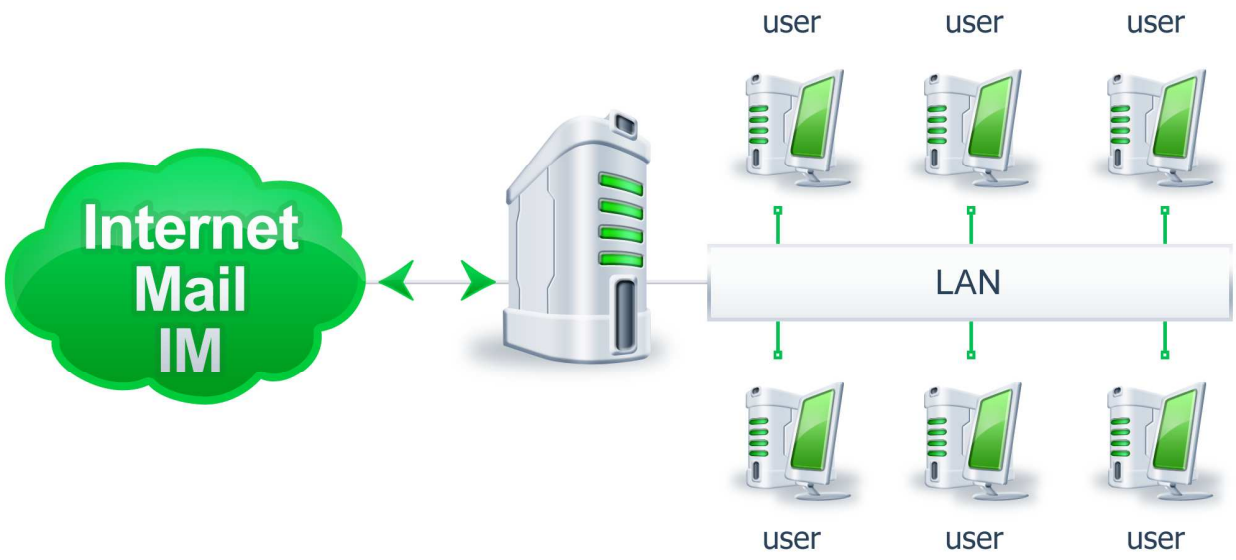
Informacje ogólne

UserGate Firewall & Proxy Server 5 jest bezpiecznym serwerem z funkcjami antywirusowymi oraz antyspamowymi, wbudowaną zaporą sieciową obsługującą NAT oraz proxy filtrującym zawartość internetową niezbędną do kontroli współdzielenia Internetu. Program umożliwia uzyskiwanie dostępu do Internetu z sieci LAN przy użyciu dołączonego filtra Internetowego oraz wbudowanej zapory sieciowej zapewniającej efektywną ochronę przed nieautoryzowanym dostępem. Współdzielony dostęp do Internetu z wykorzystaniem serwera proxy zapewnia użytkownikom sieciowym bezpieczne połączenie z Internetem. Dzięki przejrzystemu interfejsowi internetowemu możliwe jest zarządzanie użytkownikami, uprawnieniami, dostępem do Internetu oraz kontrolą dostępu do serwera. Z uwagi na fakt, że Internet stał się bardzo popularny, organizacje stały się bardziej zależne od Internetu oraz usług, które on oferuje. Przy użyciu programu UserGate Server każda organizacja może wykorzystać zalety Internetu oraz usług takich jak ochrona przed wirusami i intruzami a także współdzielony dostęp do Internetu.

Definiowanie zarządzania dostępem pomiędzy organizacjami

W dzisiejszych czasach Internet jest wykorzystywany nie tylko do rekreacji, lecz również w biznesie. Prace badawcze, sprzedaż, zakupy, obsługa klienta oraz komunikacja biznesowa są tylko kilkoma przykładami tego, w jaki sposób firmy inwestują w zalety Internetu.

W przypadku pojedynczego zewnętrznego połączenia z Internetem oraz wielu użytkowników można łatwo określić priorytety. W przypadku zarządzania biurem lub siecią korporacyjną, bezpieczeństwo i wydajność pracowników są na pierwszym miejscu.



Nie jest łatwo chronić komputery w sieci LAN przed wirusami, atakami oraz oprogramowaniem spyware i malware. Instalacja, konserwacja i aktualizacja oprogramowania antywirusowego na wielu komputerach jest czasochłonna i nie zapewnia 100% ochrony przed najnowszymi zagrożeniami.

Jednym z czynników, który nie jest standardowo dostrzegany jest nieograniczona liczba połączeń Internetowych, które mogą zmniejszyć wydajność pracownika. Gdy chodzi o sieci firmowe, „szybkość” i „nieograniczoność” nie zawsze optymalizują produktywność. Internet jest przepełniony oprogramowaniem spyware oraz wirusami, które mogą stanowić duże zagrożenie dla bezpieczeństwa korporacji oraz produktywności. Wystarczy tylko, aby jeden wirus przedostał się przez zabezpieczenia i zepsuł lub nawet uszkodził informację na wszystkich komputerach w sieci powodując utratę kilku dni lub tygodni na przywracanie. Spyware rutynowo kradnie ważne informacje takie jak hasła i prywatne dokumenty. Dramatycznie zmniejsza to wydajność komputera oraz powoduje wyświetlanie uciążliwych okien wyskakujących, które rozpraszają uwagę i które trzeba stale zamykać. Wirusy oraz oprogramowanie spyware może sparaliżować nawet najbardziej zaawansowaną technologicznie korporację.

Kosztowne zagrożenia dotyczące wydajności nie są zazwyczaj tak dobrze skrywane jak oprogramowanie spyware lub wirusy. Internet oferuje wiele form rozrywki dla pracowników. Stały się one popularne wśród pracowników, którzy wykorzystują swoje komputery firmowe oraz swój czas pracy do grania w gry online i są one zgrabnie nazywane “office killers”. Czaty oraz komunikatory są kolejną formą rozrywki marnującej czas pracownika. Jeżeli płacisz za pasmo Internetowe, pracownik wykorzystujący połączenie z Internetem do pobierania muzyki, gier lub nawet filmów będzie miał bezpośredni wpływ na koszty. Jeżeli twoja organizacja wykorzystuje VoIP w celu zaoszczędzenia na rachunkach za rozmowy, ważne jest aby żaden pracownik nie zużywał całego pasma połączenia internetowego; w przeciwnym wypadku, możesz nie nawiązać połączenia głosowego i np. stracić klienta z powodu nieodebranego połączenia lub żenująco słabej jakości połączenia.

Nawet jeśli te zagrożenia są realne, kilku wyspecjalizowanych inżynierów może wprowadzić proste rozwiązanie w celu ich zminimalizowania, podniesienia produktywności pracowników i zapewnienia całkowitej ochrony dla twojej sieci.

Dlaczego UserGate?

Jeżeli chcesz dzisiaj podłączyć sieć lokalną (LAN) w biurze do Internetu posiadasz wiele opcji do wyboru. Najprościej jest kupić mały router. To urządzenie jest niedrogie, niezawodne i przeważnie jest urządzeniem typu plug-and-play. Jeżeli wiesz, co robisz możesz skonfigurować router i sieć w przeciągu niecałej godziny. Jednakże to może nie być Twój najlepszy wybór.

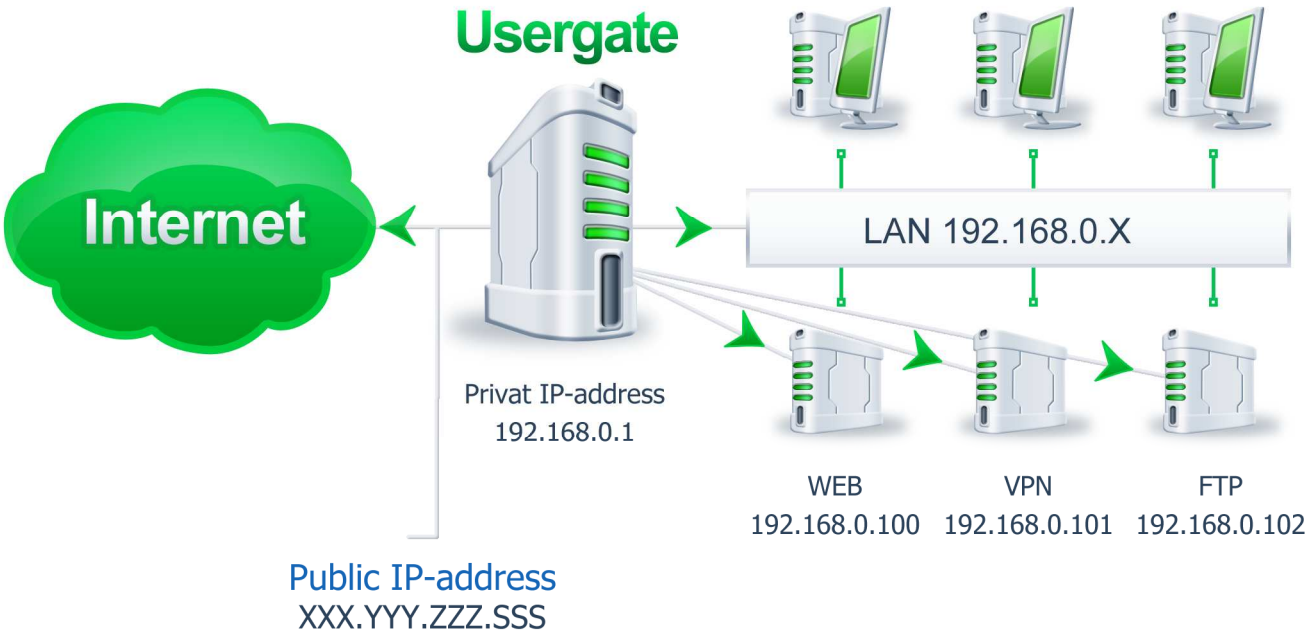
Istnieją ważniejsze powody, dlaczego router nie jest najlepszym rozwiązaniem. Jak bezpieczne powinny być Twoje dane? Czy potrzebujesz (lub chcesz) wiedzieć dokładnie, jaki ruch konsumuje każdy komputer PC? Czy posiadasz ruch priorytetowy, który musi zostać przesłany? Czy posiadasz pracowników, którzy mogą wykorzystywać Internet do celów innych niż praca?

Prosta sprzętowa brama internetowa nie wystarczy w tego typu przypadkach. Możesz zainwestować duże pieniądze i zakupić zaawansowane urządzenie, które zaspokoi niektóre z tych potrzeb, lecz nadal nie będzie to optymalne rozwiązanie.

Alternatywą dla drogiego sprzętu jest wydzielenie dedykowanego komputera do kontroli dostępu do Internetu oraz połączeń. W tym przypadku wybór jest ograniczony ekonomicznie

pomiędzy dwie platformy: *nix lub Windows. *nix (Unix, Linux, FreeBSD, itp.) nie jest opłacalnym rozwiązanie w typowej firmie posiadającej wiele komputerów z systemem Windows. System *nix posiada zasadniczą wadę: albo zatrudnisz administratora do zarządzania tym systemem albo nie będziesz w stanie optymalizować dostępu do Internetu i stale będziesz narażony na awarię sieci.

Użycie dedykowanego komputera z systemem Windows do kontroli dostępu do Internetu użytkowników sieci lokalnej jest jedynym wyborem, który pozostał.



Z uwagi na fakt, że system Windows oferuje ograniczony zestaw podstawowych funkcji łączności konieczny będzie zakup i konfiguracja dedykowanego oprogramowania bramy w celu umożliwienia korzystania z zaawansowanych funkcji. UserGate 5 firmy Entensys jest serwerem proxy & firewall dla systemu Windows, który jest nie tylko prostą bramą do konfiguracji i użytkowania, lecz również posiada wszystkie zaawansowane funkcje, które mogą być niezbędne w Twojej firmie.

Dostępne są dwie metody, dzięki którym oprogramowanie UserGate może współdzielić połączenie z Internetem wśród użytkowników sieci lokalnej. Jedną z metod jest konfiguracja oprogramowania, jako bramy w podobny sposób jak samodzielny router sprzętowy. UserGate obsługuje translację NAT adresów oraz mapowanie portów w celu współdzielenia pojedynczego adresu IP pośród wielu użytkowników sieci lokalnej.

Jeżeli niezbędne jest więcej zaawansowanych funkcji takich jak buforowanie połączeń z Internetem można skonfigurować UserGate Proxy Server. Serwer proxy automatycznie buforuje zasoby internetowe, do których użytkownicy sieci lokalnej uzyskują dostęp najczęściej oraz pozwala zaoszczędzić znaczą ilość pasma przepustowości zwiększając tym samym prędkości dostępu.

Nie jest możliwe ominięcie programu UserGate przez użytkowników sieci lokalnej w celu uzyskania dostępu do Internetu, tak więc można utworzyć niezawodne reguły do kontroli dostępu użytkowników do określonych zasobów lub protokołów.

Można również zdefiniować filtrowanie zawartości do blokowania niepożądanych stron internetowych, zasobów lub specyficznych rozszerzeń plików (takich jak MP3).

Twoja sieć lokalna jest zawsze chroniona przed atakami z zewnątrz przy użyciu wbudowanej zapory sieciowej. Wbudowane oprogramowanie antywirusowe umożliwia szybkie skanowanie całego ruchu Internetowego oferując ochronę sieci przed oprogramowaniem spyware, wirusami oraz innym szkodliwym oprogramowaniem.

Jeżeli posiadasz różne rodzaje ruchu, takie jak VoIP, można w prosty sposób ograniczać maksymalny transfer dla każdego użytkownika w celu zagwarantowania odpowiedniego transferu użytkownikom o wysokim priorytecie. Możliwe jest również ograniczanie prędkości połączenia dla dowolnego użytkownika sieci oraz kontrolowanie maksymalnego obciążenia łącza Internetowego.

UserGate przechowuje kompletne statystyki odnośnie każdego użytkownika sieci lokalnej, łącznie z historią odwiedzanych stron internetowych oraz czasem spędzonym online.

Wbudowany system statystyk czyni program UserGate idealnym rozwiązaniem do współdzielenia pojedynczego połączenia Internetowego pomiędzy wieloma użytkownikami.

Najnowsza wersja programu zapewnia obsługę sieci VPN i oferuje te same funkcje współdzielenia połaczenia oraz statystyki dla prywatnych i publicznych sieci. Możliwość obsługi VPN, a także przeźroczyste proxy, czynią program UserGate idealnym rozwiązaniem do bezpiecznego współdzielenia połączenia Internetowego.

Podstawowe funkcje programu UserGate

UserGate Proxy & Firewall server 5 jest oprogramowaniem do ochrony oferującym wszechstronną ochronę przy użyciu podstawowych funkcji ochronnych sieci:

- **Zapora sieciowa** – zintegrowany moduł umożliwiający zarządzanie aplikacjami Internetowymi oraz ograniczaniem ich użycia według wersji, typu, protokołu lub nazwy.
- **Dwa silniki antywirusowe** – Silniki antywirusowe Panda Security oraz Kaspersky Lab filtrują pocztę, FTP oraz ruch HTTP w poszukiwaniu wirusów.
- **Sterownik NAT** – precyzyjne szacowanie ruchu, obsługa przeźroczystego proxy, publikacja zasobów, routing oraz obsługa wielu dostawców usług Internetowych.
- **Filtrowanie URL** – Łącznie z filtrowaniem BrightCloud adresów URL. Filtrowanie, które ogranicza dostęp do pewnych kategorii stron internetowych uznawanych za nieprzydatne dla firmy.
- **Menadżer ostrzeżeń** to system wiadomości generowanych przez serwer UserGate w odpowiedzi na wykrycie wirusa, ataków z zewnątrz, dostępnych aktualizacjach definicji wirusów i innych.
- **Captive portal Software —** funkcje dla HotSpot, NAP (Network Access Point), i systemów użytkowników kart Wi-Fi.
- **Serwer VPN oparty na SSL** - zintegrowane komponenty VPN, brama-brama i zdalny klient-brama pozwalają na elastyczny zdalny dostęp zapewniając jednocześnie dodatkową ochronę poprzez zintegrowaną chronioną przez proxy technologię VPN, która zapewnia administratorom możliwość monitorowania ruchu na poziomie warstwy aplikacji, a nie tylko na poziomie warstwy sieci.

- **Menadżer przepstowości pasma** – dynamiczny system zarządzania ruchem używa modeli symulacyjnych w połączeniu z informacjami o ruchu rzeczywistym i o źródle-przeznaczeniu w celu przewidzenia efektów różnych strategii zarządzania, które pozwalają na bardziej efektywne zarządzanie i dostarczają lepszych, niż aktualnie dostępne, informacji o ruchu.
- **Moduł statystyk internetowych** – wbudowany komponent UserGate, który pozwala na przeglądanie statystyk użytkowników poprzez przeglądarkę internetową, filtrowanie statystyk pod względem określonych pól i na generowanie wielu rodzajów raportów, schematów i wykresów.

Zasada działania

INFORMACJA: Przy pomocy jednego komputera, jednego konta internetowego i jednego połączenia internetowego jakakolwiek organizacja może poszerzyć możliwości swojej sieci i w pełni bezpiecznie podłączyć się do internetu. Każdy rodzaj podłączenia do internetu może być wykorzystany. UserGate 5 może być zainstalowany na Windows/NT/2000/XP/2003.

UserGate 5 obsługuje tylu użytkowników ile dostępnych jest licencji. Jeżeli posiadasz 10 licencji to tylko 10 użytkowników będzie mogło łączyć się poprzez NAT lub proxy jednocześnie.

Współdzielenie połączenia z Internetem

Obsługiwane rodzaje połączenia z Internetem
Obsługa DSL, modemów kablowych, ISDN, połączeń satelitarnych, połączeń dial-up lub Internetu bezprzewodowego pozwalającego użytkownikom na rozsyłanie programu UserGate Proxy & Firewall w sieciach o dowolnym rozmiarze i lokalizacji.

Connection failover
Gdy program UserGate Proxy & Firewall wykryje że podstawowe połączenie Internetowe jest niedostępne, uaktywni automatycznie zapasowe połączenie. Zapasowe połączenie może wykorzystywać dowolny modem lub kartę sieciową.

Serwer NAT oraz Proxy
NAT jest najprostszą i najbardziej wydajną techniką współdzielenia połączenia Internetowego. Obsługuje on wirtualnie dowolną aplikację Internetową bez konieczności jakiejkolwiek konfiguracji. Wymagane jest tylko jedno połączenie z internetem (jeden adres IP) i dowolny typ dostępu do Internetu, łączenie z dial-up, DSL, modemem kablowym, T1, dostępem satelitranym lub innym. Jest to najbardziej popularna metoda współdzielenia połączenia z Internetem dla domowych biur i sieci w średniej wielkości firmach. Obsługuje ono wiele sieci prywatnych i można je skonfigurować do zezwalania/zabraniania dostępu poprzez wbudowany filtr IP.

NAT Router udostępnia przeźroczysty dostęp do Internetu wszystkim komputerom w sieci lokalnej i pracuje doskonale z prawie każdym protokołem.

Proxy Server imituje komputer kliencki dla zdalnego hosta. W związku z jego stopniem skomplikowania, technologia proxy obsługuje tylko garstkę protokołów. Jednakże, serwer proxy dostarcza zaawansowanych funkcji dla obsługiwanych protokołów takich, jak np. autentykacja i kontrola dostępu na poziomie użytkownika.

DNS forwarder
Wbudowany forwarder DNS przyśpiesza generowanie zapytań DNS przy każdej próbie uzyskania dostępu do strony internetowej przez użytkownika. Przesyła on zapytania DNS do wybranego serwera DNS znajdującego się w Internecie i przechowuje ostatnie wyniki przez określony okres czasu. Dlatego też na kolejne ponawiane zapytania odpowiedzi uzyskiwane są natychmiast.

HTTP proxy cache server
Wbudowany przeźroczysty serwer HTTP proxy buforuje zawartość podczas przeglądania stron internetowych z dużymi prędkościami. UserGate Proxy & Firewall może przechowywać strony internetowe w lokalnym buforze przez ograniczony czas w celu zaoszczędzenia przepustowości pasma. Dla określonych witryn można zdefiniować wyjątki tak, aby nie były one umieszczane nigdy w buforze.

Połączenie na żądanie
W przypadku sieci dial-up, VPN, ISDN, PPPoE lub innych typów połączeń wykorzystujących Windows' Remote Access Service (RAS), UserGate Proxy & Firewall może łączyć się z Internetem każdorazowo podczas próby nawiązania połączenia z Internetem przez użytkownika.

UserGate Proxy & Firewall może automatycznie łączyć się z internetem za każdym razem gdy pojawia się ruch wychodzący (wymagający połączenia) lub gdy jest to szczególnie wymagane przez konsolę administracji UserGate Proxy & Firewall lub interfejs internetowy (łączenie ręczne). Może także łączyć się automatycznie o określonej porze (harmonogram połączeń).

Mapowanie połączeń

Mapowanie połączeń tworzy „most” pomiędzy siecią wewnętrzną a internetem (lub vice versa). Jeśli aplikacja nie obsługuje proxy (HTTP, SOCKS, itd.), połączenie musi być nawiązane aby aplikacja mogła się połączyć z komputerem, na którym działa serwer UserGate Proxy & Firewall. Gdy połączenie dotrze do serwera na określonym porcie, połączy się on z określonym IP/Hostem na określonym porcie. Połączenia mogą być oparte o TCP lub datagramy UDP.

Najwyższy poziom ochrony sieci

Zaawansowany firewall

Wbudowana zapora sieciowa zapewnia dodatkową ochronę bramy Internetowej blokując ruch sieciowy na określonych portach (TCP, UDP lub inny port IP) i tym samym chroniąc przed atakami hakerów i innych intruzów.

Zapora sieciowa programu UserGate przetwarza pakiety, które nie zostały przetworzone przez reguły NAT. Jeżeli pakiet jest przetwarzany przez sterownik NAT nie będzie on przetwarzany przez zaporę sieciową programu UserGate.

Porty zdefiniowane w ustawieniach proxy (HTTP, FTP, SOCKS, itp.), a także porty zdefiniowane przez parametr Port Mapping są dołączone a generowane automatycznie reguły zapory sieciowej (typ auto). UserGate Proxy ułatwia tworzenie zestawu reguł. Połączenie sieci lokalnej z Internetem wymaga jedynie kilku minut na konfigurację zapory sieciowej. Reguły tworzone są tylko na jednym serwerze, tak więc administratorzy mogą być pewni że ochrona nie jest zależna od ustawień dokonanych przez indywidualnych użytkowników na ich lokalnych komputerach.

System zapobiegania włamaniom udostępniony dzięki integracji wielu technologii ochronnych został zaprojektowany do przeciwdziałania wszystkim znanym i wielu nieznanym typom ataków.

Firewall warstwy aplikacji
Zintegrowana zapora sieciowa oparta na zaporze programu UserGate Firewall. Ta zapora sieciowa oferuje pełną inspekcję pakietów, technologię proxy dla aplikacji oraz zautomatyzowany system ochronny do ochrony sieci korporacyjnych przed atakami Internetowymi oraz ograniczaniem użycia określonych aplikacji.

W celu kontroli dostępu do internetu UserGate 5 udostępnia proxy warstwy aplikacji, które zapewniają najwyższy poziom kontroli dostępu. Wszystkie porty proxy można w pełni konfigurować w celu łatwej integracji z każdym środowiskiem sieciowym. UserGate 5 udostępnia następujące proxy warstwy aplikacji:

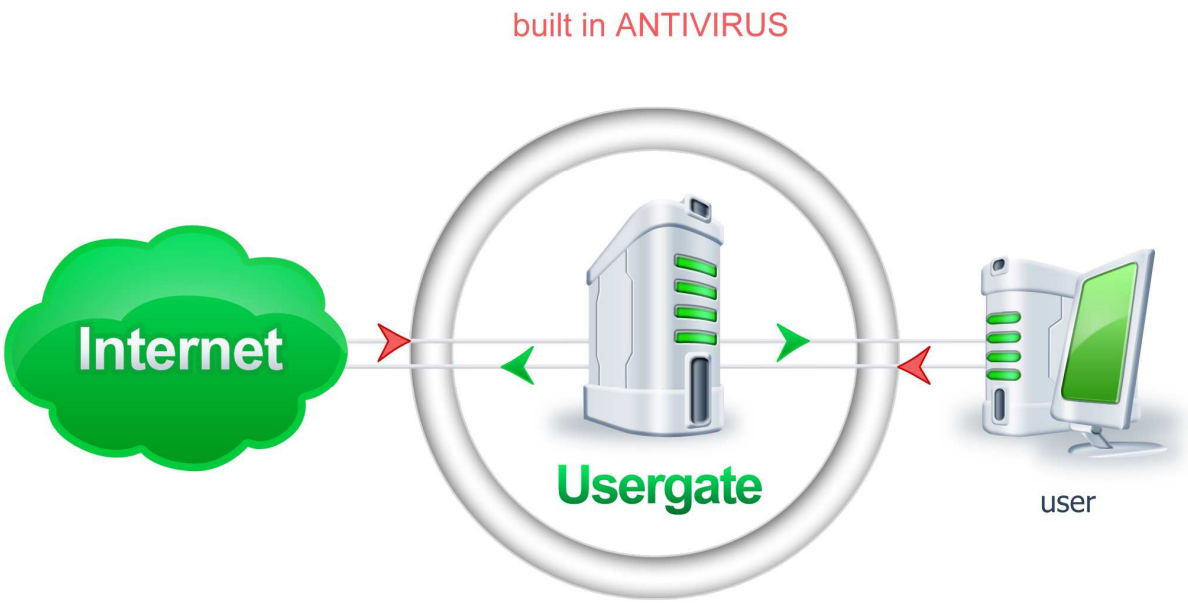
- SOCKS v4 & v5
- HTTP/HTTPS
- HTTP-FTP
- FTP
- Telnet
- RealAudio (PNA)

Organizacje, które chcą podzielić łącza internetowe między stacje robocze sieci będą musiały stawić czoła kwestii przepustowości. Przy użyciu zintegrowanego bufora proxy można przechowywać treści/zasoby internetowe, które mogą być użyte w przypadku gdy ten sam użytkownik będzie żądał dostepu do tych samych informacji w okresie czasu określonym w ustawieniach bufora. Bufor może być skonfigurowany tak, aby opróżniał się sam co *x* minut. Można określić maksymalną ilość miejsca na dysku jaką bufor może zająć na swoje potrzeby oraz określić to, jak obiekty są buforowane. Strony dynamiczne oraz instrukcje meta HTTP będą decydowały jak bufor ma działać aby użytkownicy zawsze otrzymywali najświeższe informacje.

Dwa silniki antywirusowe

UserGate zapewnia pełną kontrolę ruchu bramy włączając podwójną ochronę antywirusową. Obydwa silniki antywirusowe, Panda i Kaspersky, są w pełni zintegrowane z UserGate Proxy i

współpracują ze sobą tworząc dwuwarstwową ochronę przechwytującą wszystkie dane transmitowane przez różne protokoły internetowe.



UserGate łączy w pełni wielofunkcyjność z wysokim poziomem ochrony dla bezpiecznego dostępu do internetu. Dostarcza łatwych w użyciu narzędzi administracyjnych, które sprawiają że UserGate szybko i łatwo się instaluje, używa i zarządza.

Ochrona przed wirusami z sieci firmy Kaspersky

Kaspersky Lab dostarcza najlepszej obecnie ochrony przed zagrożeniami takimi, jak wirusy, programy szpiegujące, programy crimeware, hakerzy, phishing i spam. Produkty Kaspersky Lab mają najlepszą wykrywalność, najszybszy czas reakcji na zagrożenie dla użytkowników domowych, SMB, dużych przedsiębiorstw i urządzeń mobilnych. Technologia Kaspersky® jest także używana na całym świecie w celu ochrony produktów i usług czołowych dostawców rozwiązań bezpieczeństwa IT. Ponad dekada doświadczenia zapewnia szybką reakcję na nowe zagrożenia, dostarczając użytkownikom narzędzi i informacji do walki z zagrożeniami. Kolekcja definicji wirusów Kaspersky Lab jest największa na świecie i zawiera ponad 200 000 definicji.

Antywirus Kaspersky wbudowany w UserGate Proxy działa jak filtr dla wszystkich danych transmitowanych za pomocą głównych protokołów internetowych. Wybiera tylko te obiekty ruchu internetowego, które mogą być zagrożeniem i sprawdza je pod względem zawartości wirusów i programów szpiegowskich. Administrator może wyłączyć tę funkcję dla określonych użytkowników.

Panda Antivirus

Entensys nawiązał współpracę z Panda Software w celu zapewnienia UserGate fukcji skanowania antywirusowego.

Panda Security jest jednym z czołowych dostawców rozwiązań dla ochrony IT, z milionem klientów w ponad 200 krajach i produktami w 23 językach. Celem firmy jest stworzenie rozwiązań globalnych, które zabezpieczyłyby zasoby IT klientów przed zniszczeniem przez wirusy i inne zagrożenia, jak najniższym kosztem.

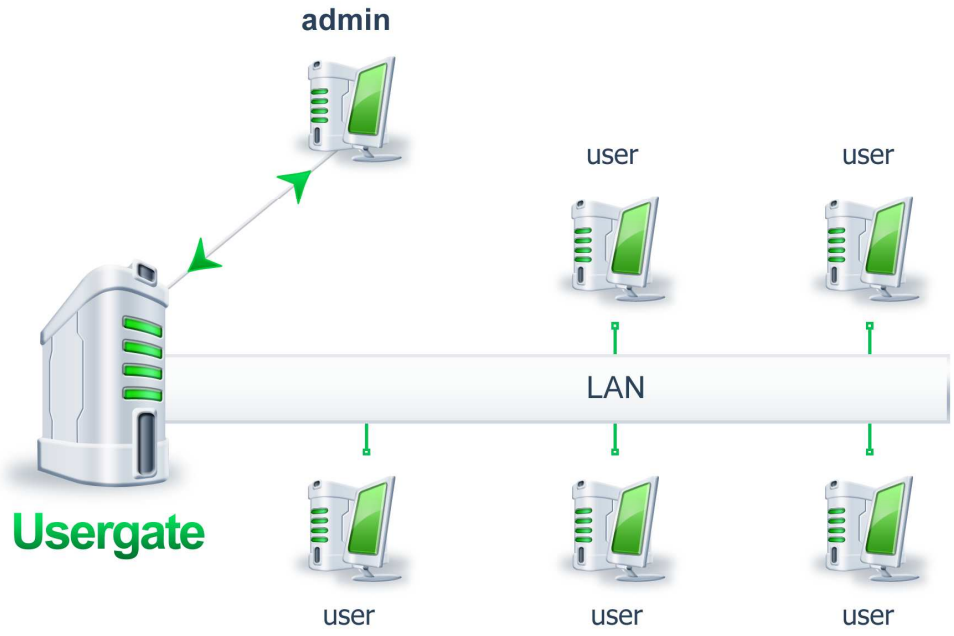
Panda Security proponuje nowy model ochrony, opracowany aby dostarczyć potężnego rozwiązania do walki z najnowszymi technikami cyber-przestępstw. Ma to odzwierciedlenie w wydajności technologii i produktów firmy, których wykrywalność plasuje się wysoko ponad średnią na rynku.

Silnik **Panda Antivirus** jest wbudowany w UserGate Proxy wraz z całym jego potencjałem. Pozwala to Panda Software działać, jako filtr przechwytujący oprogramowanie malware przesyłane przez główne protokoły transmisyjne. Wybiera tylko te obiekty, które mogą stanowić zagrożenie i analizuje je pod względem zawartości wirusów i programów szpiegowskich. Administrator może wyłączyć tę funkcję dla określonych użytkowników.

Zadaniem skanerów antywirusowych zawsze było wykrycie zagrożeń technicznie znanych, jako trojany, robaki lub wirusy. UserGate z wbudowanym silnikiem skanera Panda pozwala na wykrycie różnego rodzaju zagrożeń biorąc pod uwagę zawartość pliku, bez względu na jego „wygląd”, czyli np. jego nazwę czy rozszerzenie. UserGate potrafi teraz wykryć i zmienić programy malware w plikach skompresowanych (ZIP, RAR, ARJ, ARC, BZIP2, LHA, CAB, ZOO, LZOP) a także w innych popularnych formatach plików takich, jak DOC, PDF, CHM, TAR, RTF, Quake, itp.

Elastyczne i scentralizowane zarządzanie siecią

Zdalne zarządzanie pozwala administratorom sieci na zdalną pracę oraz większą mobilność:



Serwer DHCP

Dynamic Host Configuration Protocol (DHCP) zapewnia mechanizm przy wykorzystaniu, którego komputery korzystające z protokołu TCP/IP mogą automatycznie poprzez sieć uzyskiwać parametry konfiguracyjne protokołu. DHCP jest otwartym standardem stworzonym przez grupę Dynamic Host Configuration workgroup of the Internet Engineering Task Force.

Precyzyjna optymalizacja ruchu sieciowego

Menadżer przepustowości pasma

System dynamicznego zarządzania ruchem sieciowym wykorzystuje modele symulacji w połączeniu z ruchem sieciowym w czasie rzeczywistym oraz oryginalnymi informacjami o lokalizacji docelowej do przewidywania efektów różnych strategii zarządzania, pozwalając tym samym na bardziej efektywne zarządzanie i oferując lepsze informacje o ruchu sieciowym, który jest aktualnie możliwy.

Wykorzystując menadżera przepustowości pasma administratorzy mogą nakładać ograniczenia użytkownikom, którzy pobierają duże pliki zapewniając tym samym komfort pracy pozostałym użytkownikom. Alternatywnie Menadżer przepustowości pasma może ustawić, zmieniając dynamicznie, i podzielić określoną wielkość pasma pomiędzy użytkowników/protokoły w celu optymalizacji obciążeń kanałów.

Skategoryzowane filtrowanie adresów URL od BrightCloud

UserGate 5 Content Filter (filtr treści) obejmuje wiele kategorii niepożądanych i niestosownych treści internetowych od BrightCloud dając ci całkowitą kontrolę dostępu do Internetu. Pomoże ci to ponieść produktywność, ograniczyć surfowanie po Internecie w celach osobistych oraz zmniejszy odpowiedzialność prawną związaną z pobieraniem pornografii i nielegalnych plików.

Usługa BrightCloud jest wbudowana w UserGate Proxy tak, więc klienci mogą używać filtrowania, jako części proxy.

Poprzez przeglądanie Internetu użytkownicy UserGate będą w stanie nałożyć akceptowalną politykę używania Internetu właściwą dla nich. Żądanie otwarcia strony internetowej jest przekazywane usłudze BrigthCloud i głównej bazie danych BrightCloud w celu określenia kategorii strony. Wbudowany mechanizm polityki UserGate stosuje odpowiednią politykę np. blokując dostęp do niestosownych stron, stron phishingowych lub stron zainfekowanych przez wirusy.

Moduł szczegółowych statystyk internetowych

UserGate Proxy oferuje szeroką gamę metod analizy ruchu internetowego. Można przeglądać szczegółowe statystyki dla każdego użytkownika, przejrzeć ruch przychodzący, strony odwiedzone itd. Wszystko to można przejrzeć przy pomocy przeglądarki internetowej lub poprzez e-mail. Opcjonalnie, statystyki mogą być wyeksportowane do formatu MS Excel.

Wymagania i ograniczenia programu UserGate

Element	Wymagania minimalne	Zalecana konfiguracja
Wymagania sprzętowe:	Procesor Pentium 1GHz oraz 512 MB pamięci RAM	Procesor Pentium 2 GHz oraz 1 GB pamięci RAM
System operacyjny:	Obsługiwane platformy: Windows 2000, XP (SP2, SP3), Server 2003 (tylko edycja 32-bitowa)	Windows Server 2003
Połączenie z Internetem:	Połączenie ISDN/ Linia dzierżawiona / T1	T1/Połączenie przewodowe

Informacje o firmie Entensys

Firma Entensys jest międzynarodowym producentem oprogramowania do ochrony danych oraz produktów do współdzielenia połączenia Internetowego i zapory sieciowej posiadających łatwy w użyciu interfejs administracyjny oraz wielofunkcyjne usługi. Firma Entensys jest producentem popularnego serwera UserGate przeznaczonego do scentralizowanego zarządzania siecią oraz ochrony przed różnymi zagrożeniami Internetowymi. Produkty firmy Entensys rozwiązują złożone problemy związane z ochroną danych i bezpieczeństwem.