Barracuda **Email Security Gateway**

Pełna ochrona przed zagrożeniami przenoszonymi pocztą elektroniczną

- ☑ **Security**
- ☐ Storage
- ☐ Application Delivery

Informatycy potrzebują **wszechstronnego rozwiązania do ochrony poczty elektronicznej — umożliwiającego blokowanie ataków dokonywanych przy użyciu wiadomości e-mail**, wyposażonego w dodatkowe funkcje niezbędne do zapewnienia ciągłości biznesowej, a przy tym oferowanego w przystępnej cenie..

Atuty rozwiązań marki Barracuda

- Bezpłatna warstwa ochrony w chmurze (Cloud Protection Layer) obejmująca:
  - Buforowanie wiadomości e-mail przez maksymalnie 96 godzin
  - Filtrowanie poczty przychodzącej
- Funkcja ochrony w czasie rzeczywistym (Barracuda Real-Time Protection)
- Filtrowanie wiadomości wychodzących w celu zapobiegania wyciekowi danych
- Bezpłatne szyfrowanie oparte na chmurze
- Tworzenie kopii zapasowych konfiguracji w chmurze
- Konfiguracja fabryczna umożliwiająca szybkie wdrożenie
- Brak opłat zależnych od liczby użytkowników lub serwerów

Najważniejsze informacje o produkcie

- Najlepsza w branży ochrona poczty elektronicznej przed spamem i wirusami
- Ochrona przed utratą danych i reputacji
- Funkcja Advanced Threat Detection [1] chroniąca przed oprogramowaniem ransomware i innymi zaawansowanymi zagrożeniami
- Zaawansowane, precyzyjne zarządzanie zasadami

Wszechstronna, długofalowa ochrona

Barracuda Email Security Gateway to kompletne rozwiązanie umożliwiające między innymi blokowanie spamu i wirusów, ochronę danych, zapewnienie ciągłości działania systemu poczty elektronicznej, zapobieganie atakom typu DoS, szyfrowanie oraz zarządzanie zasadami. W miarę pojawiania się nowych wymagań rozwiązanie jest automatycznie rozszerzane o nowe funkcje w celu zapewnienia nieprzerwanej ochrony.

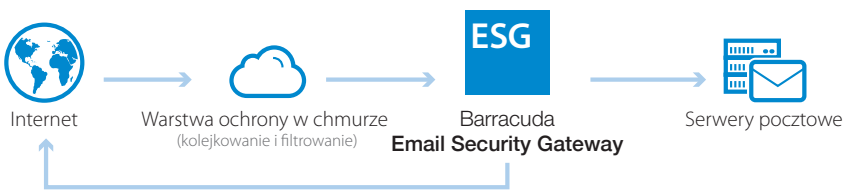
Pełna ochrona przed zagrożeniami związanymi z pocztą elektroniczną

Rozwiązanie Barracuda Email Security Gateway oferuje wielowarstwową ochronę, obejmującą między innymi zapewnienie ciągłości działania systemu poczty elektronicznej i zapobieganie wyciekowi danych. Funkcja wykrywania zaawansowanych zagrożeń (Advanced Threat Detection) [1] łączy technologie analizy behawioralnej i heurystycznej oraz testowania w wydzielonym środowisku w celu zapewnienia ochrony przed nieznanymi dotąd zagrożeniami, atakami ukierunkowanymi i oprogramowaniem ransomware.

Przystępna cena i łatwa obsługa

Szybka i łatwa konfiguracja oraz proste i intuicyjne zarządzanie pozwalają ograniczyć czaso- i pracochłonność obsługi. Integracja z warstwą ochrony w chmurze (Barracuda Cloud Protection Layer) i brak opłat zależnych od liczby użytkowników umożliwiają łatwe, opłacalne skalowanie mocy obliczeniowej w miarę rozwoju przedsiębiorstwa.

Filtrowanie i buforowanie wiadomości przychodzących przy użyciu warstwy ochrony w chmurze (Cloud Protection Layer)



Ochrona antywirusowa oraz filtrowanie poczty przychodzącej i wychodzącej w przystępnej cenie. Gdyby nie rozwiązanie Barracuda Email Security Gateway, najprawdopodobniej wcale nie filtrowalibyśmy poczty, ponieważ rozwiązania innych dostawców — wymagające uiszczania opłat uzależnionych od liczby użytkowników — są zbyt drogie.

Shane Henszey
Kierownik ds. informatyki
U.S. Vision, Inc.

Opis techniczny

Wszechstronna ochrona

- Filtrowanie antyspamowe i antywirusowe
- Warstwa ochrony w chmurze (Cloud Protection Layer)
- Ochrona przed fałszowaniem tożsamości, wyłudzaniem informacji (phishingiem) i złośliwym oprogramowaniem
- Ochrona przed atakami powodującymi odmowę usługi (DoS/DDoS)
- Ochrona przed atakami typu directory harvest
- Filtrowanie poczty wychodzącej

Zapobieganie wyciekom danych i utracie reputacji

- Utrzymanie zgodności z przepisami
- Zapobieganie utracie reputacji i wpisaniu na czarne listy
- Wstępnie zdefiniowane filtry (np. HIPAA, numery kart kredytowych czy amerykańskie numery ubezpieczenia społecznego)

Zaawansowana kontrola zasad

- Filtrowanie na podstawie adresów IP i treści
- Masowe klasyfikowanie wiadomości
- Szyfrowanie treści
- Filtrowanie według nadawcy/odbiorcy
- Obsługa list RBL i DNSBL
- Blokowanie według słów kluczowych
- Blokowanie na podstawie zestawu znaków
- Blokowanie przy użyciu odwrotnej translacji adresów DNS
- Blokowanie według wzorców i kategorii adresów URL
- Zasada szyfrowania TLS
- Dodatkowe uwierzytelnianie

Uwierzytelnianie nadawcy

- SPF i DomainKeys
- Emailreg.org
- Blokowanie nieprawidłowych komunikatów o niedostarczeniu poczty

Filtr antyspamowy

- Kontrola liczby wysyłanych wiadomości
- Analiza reputacji adresów IP
- Analiza odcisków palca i obrazów
- Algorytmy punktowania oparte na regułach
- Funkcja zapobiegania oszustwom (Barracuda Anti-Fraud Intelligence)

Filtr antywirusowy

- Trójwarstwowe blokowanie wirusów
- Zintegrowany agent antywirusowy do oprogramowania Exchange
- Dekompresja archiwów
- Blokowanie konkretnych typów plików
- Sieć Barracuda Antivirus Supercomputing Grid
- Funkcja Advanced Threat Detection[1] chroniąca przed oprogramowaniem ransomware, nieznanymi dotąd zagrożeniami i atakami ukierunkowanymi.

Funkcje systemowe

Administratorzy

- Interfejs oparty na przeglądarce internetowej
- Administrowanie kontami użytkowników
- Raporty, wykresy i statystyka
- Interfejs LDAP
- Obsługa wielu domen
- Bezpieczne zdalne administrowanie
- Delegowane administrowanie domeną
- Delegowana obsługa stanowiska pomocy
- Buforowanie wiadomości e-mail
- Konfigurowanie funkcji tworzenia kopii zapasowych w chmurze

Użytkownicy

- Filtrowanie na podstawie nazwy użytkownika
- Indywidualne punktowanie spamu
- Osobiste listy dozwolonych i zablokowanych adresów
- Kwarantanna i podsumowanie wiadomości e-mail na poziomie użytkownika
- Współpraca z programem Outlook
- Analiza bayesowska

Opcje pomocy technicznej

Usługa Barracuda Energize Updates

- Standardowa pomoc techniczna
- Cogodzinne aktualizacje definicji spamu
- Bazy danych reputacji firmy Barracuda
- Definicje odcisków palca i analiz zamiarów
- Cogodzinne aktualizacje definicji wirusów

Usługa natychmiastowej wymiany

- Wysyłka urządzeń zastępczych na następny dzień roboczy
- Pomoc techniczna przez 24 godziny na dobę, 7 dni w tygodniu
- Modernizacja sprzętu raz na cztery lata

Charakterystyka sprzętu

Złącza

- Standardowe VGA
- Klawiatura/mysz PS/2
- Ethernet (patrz tabela poniżej)

Urządzenie wirtualne

- System operacyjny o podwyższonym poziomie bezpieczeństwa
- Siedem modeli do wyboru
- Obsługa najpopularniejszych hiperwizorów, w tym VMware ESX i Workstation, Oracle VirtualBox, Citrix Xen oraz Microsoft Hyper-V

PORÓWNANIE MODELI	100*	200	300*	400*	600*	800*	900*	1000*
POJEMNOŚĆ								
Aktywni użytkownicy poczty elektronicznej	1-50	51-500	300-1.000	1.000-5.000	3.000-10.000	8.000-22.000	15.000-30.000	25.000-100.000
Domeny	10	50	250	500	5.000	5.000	5.000	5.000
Pamięć dziennika wiadomości	8 GB	10 GB	12 GB	24 GB	72 GB	120 GB	240 GB	512 GB
Pamięć kwarantanny			20 GB	60 GB	180 GB	360 GB	1 TB	2 TB
SPRZĘT								
Obudowa stelażowa	1U Mini	1U Mini	1U Mini	1U Mini	1U pełnowymiarowa	2U pełnowymiarowa	2U pełnowymiarowa	2U pełnowymiarowa
Wymiary (cm)	42,7 x 22,9 x 4,3	42,7 x 22,9 x 4,3	42,7 x 40,6 x 4,6	42,7 x 40,6 x 4,6	42,7 x 57,4 x 4,3	44,2 x 64,8 x 8,9	44,2 x 64.8,x 8,9	43,7 x 69,3 x 8,9
Masa (kg)	3,6	3,6	5	5,5	11,8	20,9	23,6	23,6
Ethernet	1 x 10/100	1 x 10/100	1 x Gigabit	1 x Gigabit	2 x Gigabit	2 x Gigabit	2 x Gigabit	2 x Gigabit
Prąd wejściowy AC (A)	0,5	0,5	0,6	0,7	0,9	2,1	2,8	3,8
Power Consumption (W)	120	120	144	168	206	492	648	864
Macierz dysków (RAID)				●	Wymienne podczas pracy	Wymienne podczas pracy	Wymienne podczas pracy	Wymienne podczas pracy
Pamięć z korekcją błędów (ECC)					●	●	●	●
Zasilacz rezerwowy						Wymienne podczas pracy	Wymienne podczas pracy	Wymienne podczas pracy
FUNKCJE								
Zaawansowane wykrywanie zagrożeń (Advanced Threat Detection) [1]	●	●	●	●	●	●	●	●
Filtrowanie poczty wychodzącej	●	●	●	●	●	●	●	●
Szyfrowanie poczty	●	●	●	●	●	●	●	●
Warstwa ochrony w chmurze (Cloud Protection Layer)	●	●	●	●	●	●	●	●
Akcelerator MS Exchange/LDAP			●	●	●	●	●	●
Indywidualne ustawienia i kwarantanna dla poszczególnych użytkowników			●	●	●	●	●	●
Delegowana obsługa stanowiska pomocy			●	●	●	●	●	●
Obsługa dziennika systemowego			●	●	●	●	●	●
Klastrowanie standardowe i zdalne				●	●	●	●	●
Odrębne ustawienia dla każdej domeny				●	●	●	●	●
Jednokrotne logowanie				●	●	●	●	●
SNMP/API				●	●	●	●	●
Konfigurowalne oznakowanie marką					●	●	●	●
Indywidualne ustawienia punktowania spamu dla każdego użytkownika					●	●	●	●
Delegowane administrowanie domeną					●	●	●	●

*Dostępne również w wersji Vx (edycja wirtualna)

Dane techniczne mogą ulec zmianie bez powiadomienia.

[1] Funkcja Advanced Threat Detection (ATD) jest dostępna w ramach dodatkowej subskrypcji..