

# Nowoczesne sprzętowe systemy ochrony sieci

Marcin Madey  
mmadey@apertos.pl



apertOS

TWOJA SIEĆ POD KONTROLĄ

# Agenda



- Kilka słów o firmie
- apertOS MAIL PROTECT
- apertOS INTERNET PROTECT
- apertOS HA BALANCE
- apertOS NET PROTECT
- Następca systemu Novell BorderManager
- Wsparcie techniczne
- Sieć sprzedaży

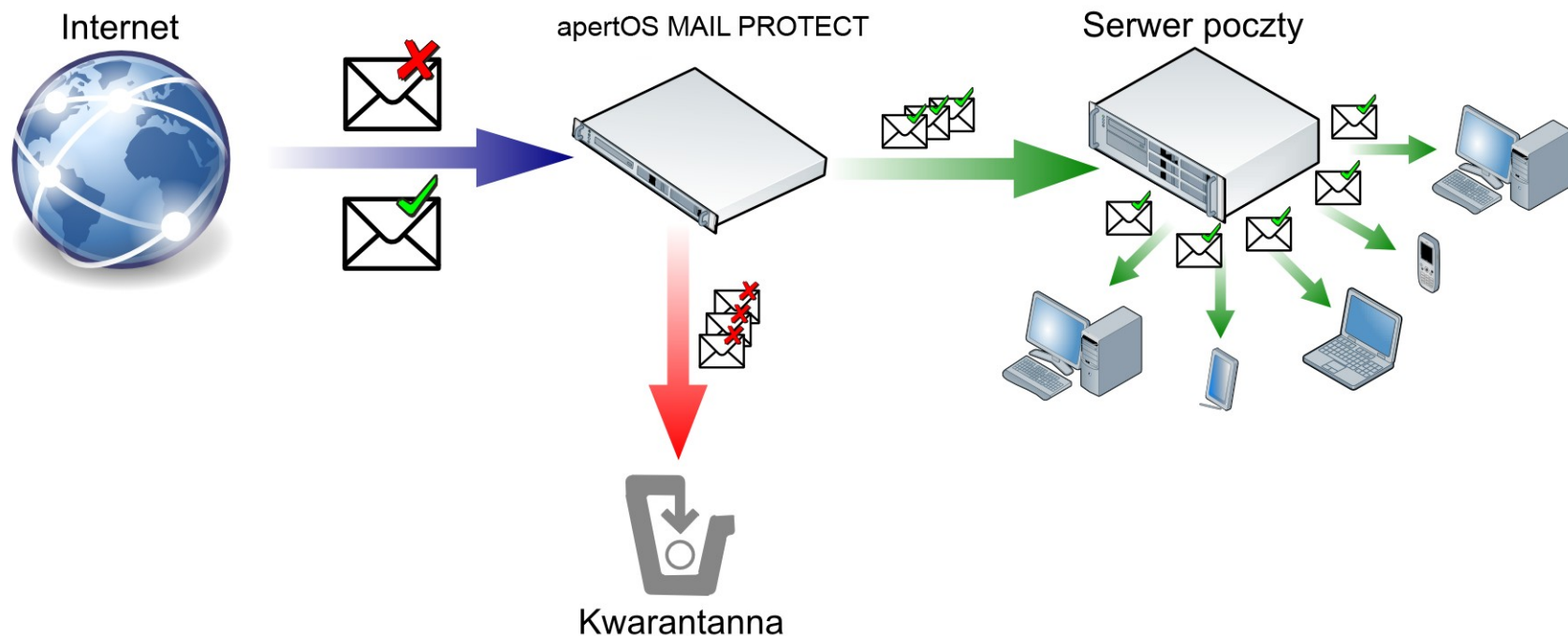
apertOS

- Nazwa pochodzi od apertus (łac. otwarty)
  - Produkty oparte o otwarte standardy
  - Działają z większością rozwiązań na rynku
- Produkty typu „black box” (również jako obraz VMware)
- Doświadczony zespół projektantów i programistów
- Produkt tworzony w Polsce z myślą o polskim rynku
- Współpraca z liderem rozwiązań serwerowych – Action
  - Sprawdzone rozwiązania Actina Solar
  - Niezawodna sieć serwisowa Action

- Trzy produkty na rozpoczęcie działania
  - System ochrony poczty elektronicznej
  - System ochrony dostępu do Internetu
  - System rozkładania ruchu w klastrach wydajnościowych i wysokiej dostępności
- Czwarty dostępny od 1/10/2010
  - System ściany ogniowej (apertOS NET PROTECT)

apertOS MAIL PROTECT

# Inteligentna, wielopoziomowa ochrona poczty



# Zagrożenia wynikające ze SPAMu



- SPAM wytraca czas
- SPAM może przenosić wirusy, oprogramowanie szpiegujące czy robaki



- SPAM pomaga tworzyć sieci BOTów
- Badania z 2010 roku w Europie, Ameryce Północnej i Australii
  - 45% użytkowników otwiera SPAM pomimo wiedzy o zagrożeniu
- Szacuje się, że 90% poczty to SPAM
  - W 2009 roku straty z tego powodu wyniosły około 130 miliardów USD
- Szacuje się, że każdego dnia jest aktywnych ponad 70 000 komputerów należących do jakichś sieci BOTów
  - Ataki DDoS (Distributed Denial of Service)



# Metody ochrony



- Wielopoziomowe, inteligentne zabezpieczenia
  - Wysoki współczynnik zatrzymania SPAMu > 98%
  - Niski współczynnik FP (False Positive) – bliski 0%
- „Gray listing”
- Listy reputacyjne DNSBL i URIBL
- Białe i czarne listy
  - Firmowe
  - Użytkownika
- Filtr Bayesa
- Reguły firmowe
- Skanowanie antywirusowe



# Tryb serwera pocztowego



- Serwer pocztowy zintegrowany z systemem antyspamowym i antywirusowym
- Dostęp poprzez interfejs WWW
- Dostęp poprzez POP3/IMAP



# Najważniejsze funkcje rozwiązania



- Praca w trybie transparentnego lub aktywnego węzła MTA
- Serwer poczty
- Interfejs WWW, POP3 i IMAP do serwera poczty
- Autoryzacja połączeń SMTP
- Definiowanie polityk dla wiadomości na podstawie zakresów adresacji IP nadawcy wiadomości, nagłówek wiadomości, treści wiadomości, rozmiaru wiadomości, treści załączników lub typu załączników

# Najważniejsze funkcje rozwiązania



- Definiowanie następujących akcji dla wiadomości w ramach polityki:
  - oznaczenie z dostarczeniem,
  - usunięcie,
  - usunięcie z powiadomieniem,
  - dostarczenie,
  - kwarantanna,
  - kwarantanna z powiadomieniem
- Uwierzytelnianie w dowolnym katalogu LDAP (np. eDirectory, SUN Directory Server, OpenLDAP, Active Directory przez LDAP itp.)

# Najważniejsze funkcje rozwiązania



- Listy reputacyjne DNSBL i URIBL
- Raporty
- Logowanie zdarzeń do własnego oraz zewnętrznego systemu zdarzeń
- Praca w trybie klastra wydajnościowego lub wysokiej dostępności

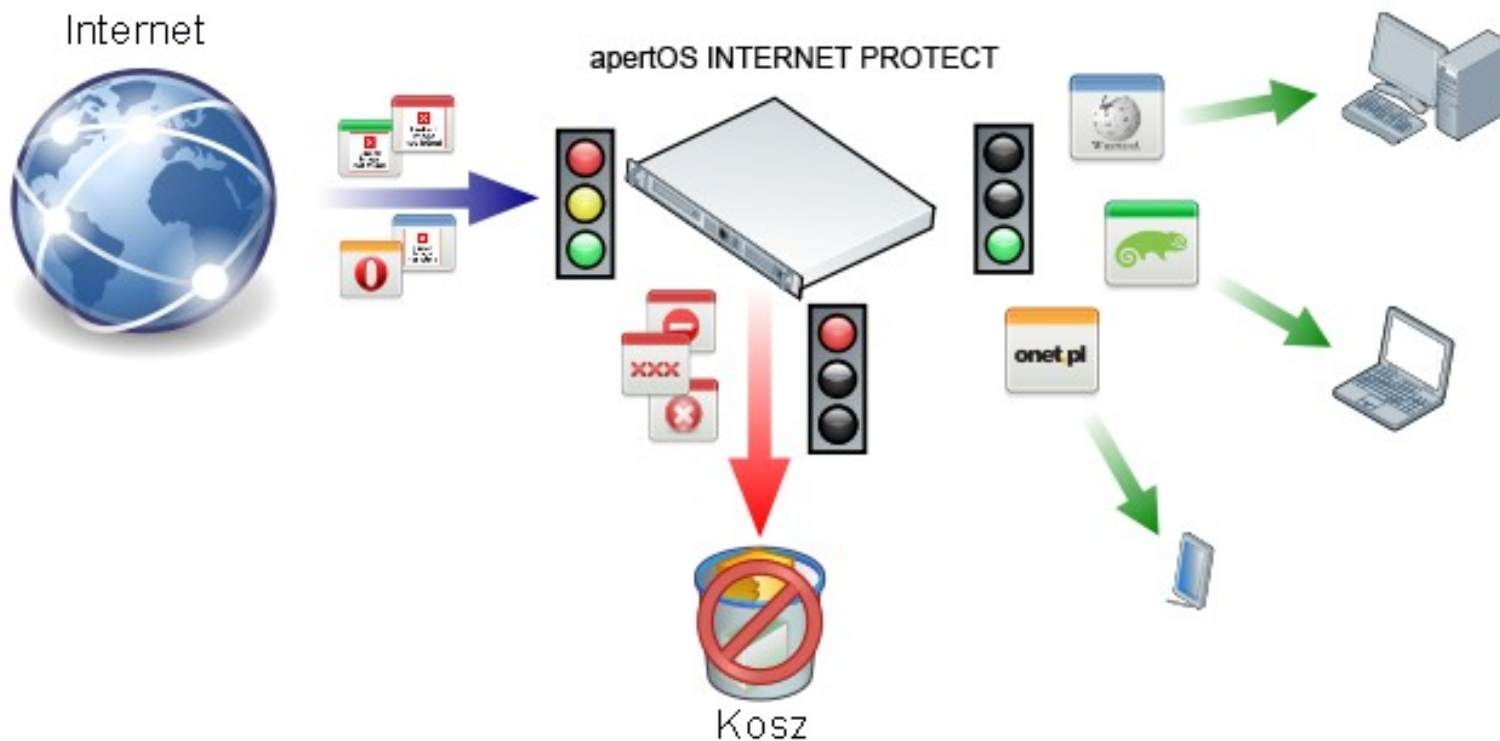
# Modele



Właściwości / Modele	MP 50	MP/S 100	MP/S 500	MP/S 700	MP/S 1000
<b>Właściwości</b>					
Kompatybilny z dowolnym serwerem pocztowym	✓	✓	✓	✓	✓
Inteligentna, wielopoziomowa ochrona poczty	✓	✓	✓	✓	✓
Filtrowanie poczty wychodzącej	✓	✓	✓	✓	✓
Tryb serwera poczty		X / ✓	X / ✓	X / ✓	X / ✓
Interfejs WWW do serwera poczty			X / ✓	X / ✓	X / ✓
Kwarantanna dla każdego użytkownika			✓	✓	✓
Wsparcie dla syslog, raportowanie, wykresy			✓	✓	✓
Wsparcie dla klastrowania				✓	✓
<b>Parametry</b>					
Obudowa	Mini tower	Mini tower	Mini tower	1U	1U
Karta sieciowa	2 x 10/100	2 x 10/100	2 x 1GB	2 x 1GB	2 x 1GB
Pojemność użytkownika dysków twardej	250 GB	250 GB	250 GB	500 GB	2TB
RAID				Hot Swap (1)	Hot Swap (10)
Pamięć ECC				✓	✓
<b>Wydajność</b>					
Sugerowana liczba chronionych kont pocztowych	Do 50	Do 100	Do 1 500	Do 5 000	Do 20 000
Liczba kont pocztowych w serwerze poczty	-	- / 50	- / 500	- / 1000	- / 3000
<b>Wsparcie techniczne</b>					
Poziom wsparcia	Standard	Standard	Standard	Standard	Standard
Okres wsparcia	1 rok	1 rok	1 rok	1 rok	3 lata

apertOS INTERNET PROTECT

# Inteligentna, wielopoziomowa ochrona dostępu do Internetu



# Zagrożenia wynikające z braku ochrony ruchu internetowego



- Internet obniża wydajność pracowników

- > Od 1 do 3 godzin dziennie
- > Google i PAC-MAN
  - » 4,8 mln dodatkowych godzin w piątek spędzonych na stronach Google



- Nielegalne oprogramowanie

- > 80% firm informuje o ściąganiu nielegalnych treści

- Pornografia

- > 70% treści XXX jest pobieranych między 9:00 a 17:00 czasu lokalnego

- Włamania

- > 40% firm było narażonych na ataki dokonane przez swoich pracowników

- Zagrożenia tajemnic firmowych, prawne i finansowe

- Zagrożenia wirusami



# Metody ochrony



- Filtrowanie ruchu HTTP i FTP
- Identyfikacja użytkowników
  - SSO
- Filtrowanie kategorii (uaktualnianie listy)
- Filtrowanie domen i adresów URL
- Filtrowanie słów i wyrażeń
- Filtrowanie plików określonego rodzaju
- Filtrowanie wielkości przesyłanych danych
- Swobodne definiowanie reguł
- Ochrona antywirusowa



# Najważniejsze funkcje rozwiązania



- Praca w trybie jawnego serwera proxy, transparentnego serwera proxy lub transparentnego serwera proxy z wykorzystaniem protokołu WCCP
- Podłączenie do zewnętrznej bazy danych użytkowników za pośrednictwem protokołów LDAP i LDAP SSL w celu autoryzacji i identyfikacji użytkowników
- Mechanizm SSO dla Active Directory i eDirectory
- Blokowanie połączeń, w ramach których przesyłane jest złośliwe oprogramowanie

# Najważniejsze funkcje rozwiązania



- Polityki dostępu dla protokołu HTTP i FTP, w tym tworzone na podstawie:
  - adresów IP,
  - użytkowników lub grup w katalogu
  - dni tygodnia i pory dnia
  - ilości danych pobieranych przez użytkownika
  - rodzaju pobieranych plików
  - typu serwisu WWW
  - treści udostępnianej w serwisie WWW
  - fraz ważonych
  - zdefiniowanych kategorii serwisów

# Najważniejsze funkcje rozwiązania



- Możliwość definiowania komunikatów wyświetlanych w przypadku zablokowania połączenia
- Raporty
- Logowanie zdarzeń do własnego oraz zewnętrznego systemu zdarzeń
- Praca w trybie klastra wydajnościowego lub wysokiej dostępności
- Wraz z apertOS NET PROTECT stanowi zastępstwo dla rozwiązania BorderManager firmy Novell

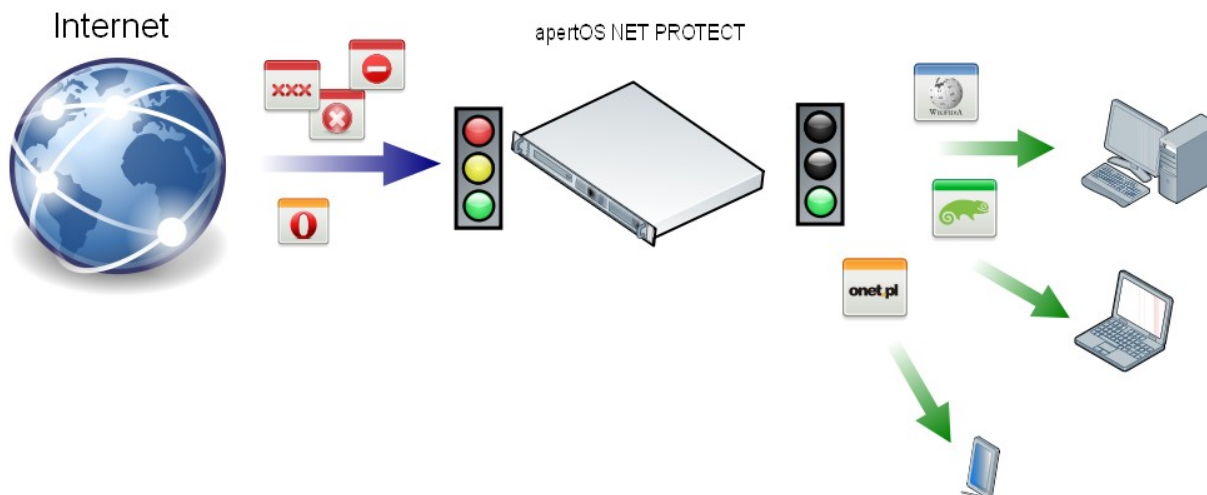
# Modele



Właściwości / Modele	IP 100	IP 500	IP 700	IP 1000
<b>Właściwości</b>				
Kompatybilny z dowolnym serwerem WWW/FTP	✓	✓	✓	✓
Inteligentna, wielopoziomowa ochrona komunikacji	✓	✓	✓	✓
Filtrowanie ruchu wychodzącego i przychodzącego	✓	✓	✓	✓
Mechanizm SSO dla Active Directory i eDirectory	✓	✓	✓	✓
Definiowanie komunikatów wysyłanych przy blokowaniu połączenia	✓	✓	✓	✓
Tryb WCCP		✓	✓	✓
Wsparcie dla syslog, raportowanie, wykresy		✓	✓	✓
Wsparcie dla klastrowania			✓	✓
<b>Parametry</b>				
Obudowa	Mini tower	Mini tower	1U	1U
Karta sieciowa	2 x 10/100	2 x 1GB	2 x 1GB	2 x 1GB
Pojemność użytkownika dysków twardech	250 GB	250 GB	250 GB	500 GB
RAID			Hot Swap (1)	Hot Swap (10)
Pamięć ECC			✓	✓
<b>Wydajność</b>				
Sugerowana liczba chronionych użytkowników	Do 100	Do 1 000	Do 3 000	Do 7 500
<b>Wsparcie techniczne</b>				
Poziom wsparcia	Standard	Standard	Standard	Standard
Okres wsparcia	1 rok	1 rok	1 rok	3 lata

apertOS NET PROTECT

# Ochrona dostępu z/do Internetu



# Zagrożenia wynikające z braku ochrony sieci firmowej



- Włamania

- > Hakerzy i konkurencja
  - » Zmiany witryn WWW
  - » Blokowanie systemów informatycznych
  - » Uszkadzanie danych
  - » Dane
  - » Ataki DoS



- Niechciane aplikacje

- > Komunikatory
  - » Marnowanie czasu pracowników
  - » Umożliwiają przesyłanie plików

- Tworzenie sieci BOTów

- Brak publicznych adresacji IP

# Metody ochrony



- Wydzielanie strefy zdemilitaryzowanej
- Translacja adresów
- Blokowanie ataków DoS
- Filtrowanie ruchu przychodzącego i wychodzącego

# Najważniejsze funkcje rozwiązania



- Podział na strefy
  - Wewnętrzna
  - Zewnętrzna
  - DMZ
- Ochrona przed atakami DoS
  - Ochrona przed atakami SYN-flood
  - Ignorowanie błędnych pakietów
- Translacja adresów
  - Przekierowywanie połączeń
    - > Adresy
    - > Porty

# Najważniejsze funkcje rozwiązania



- Kontrola ruchu
  - Uproszczone reguły połączeń między strefami
    - > Ze strefy do strefy
    - > Wybieramy checkboxami aplikacje/protokoły dozwolone
    - > Wszystko co nie jest dozwolone, jest zabronione
  - Uproszczone reguły połączeń przychodzących
    - > Wybrany zestaw aplikacji/protokołów
    - > Ustawia się dla każdej strefy oddzielnie
  - Zaawansowane reguły połączeń
    - > Predefiniowane protokoły lub „generic” TCP i/lub UDP
    - > Z adresu/sieci do adresu/sieci
    - > Trzy akcje: Przyjmij, Zerwij i Odrzuć

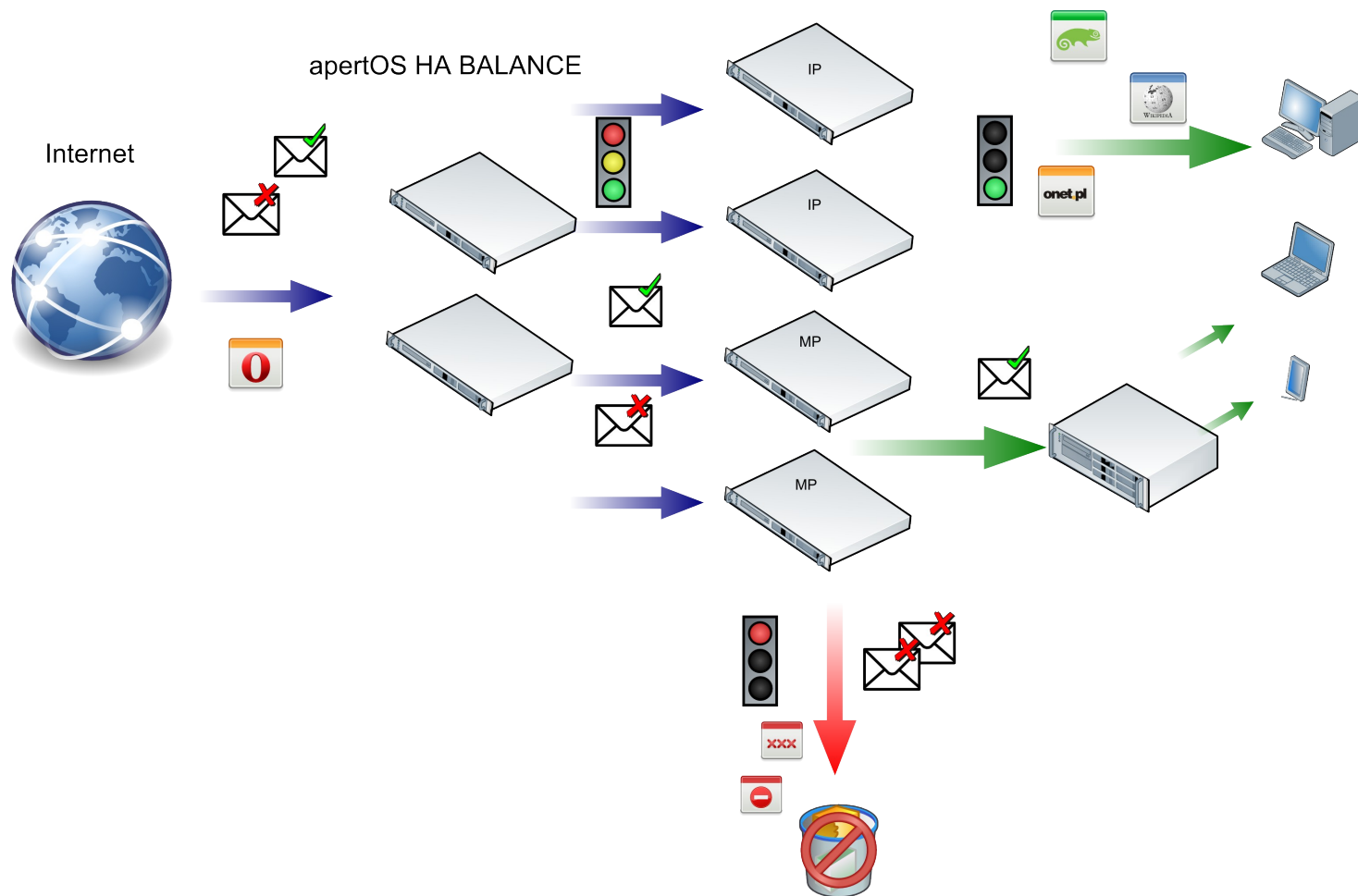
# Modele



Właściwości / Modele	IP 100	IP 500	IP 700	IP 1000
<b>Właściwości</b>				
Filtrowanie ruchu wychodzącego i przychodzącego	✓	✓	✓	✓
Definiowanie stref	✓	✓	✓	✓
Translacja adresów	✓	✓	✓	✓
Uproszczone i zaawansowane reguły filtrowania	✓	✓	✓	✓
Wsparcie dla syslog, raportowanie, wykresy		✓	✓	✓
Wsparcie dla klastrowania			✓	✓
<b>Parametry</b>				
Obudowa	Mini tower	Mini tower	1U	1U
Karta sieciowa	2 x 10/100	2 x 1GB	4 x 1GB	6 x 1GB
Pojemność użytkownika dysków twardej	250 GB	250 GB	250 GB	250 GB
RAID			Hot Swap (1)	Hot Swap (10)
Pamięć ECC			✓	✓
<b>Wydajność</b>				
Sugerowana liczba chronionych użytkowników	Do 100	Do 1 000	Do 3 000	Do 5 000
<b>Wsparcie techniczne</b>				
Poziom wsparcia	Standard	Standard	Standard	Standard
Okres wsparcia	1 rok	1 rok	1 rok	3 lata

apertOS HA BALANCE

# apertOS HA BALANCE



# apertOS HA BALANCE



- Rozłożenie obciążenia pomiędzy wiele urządzeń
- Wsparcie dla dowolnego protokołu wykorzystującego TCP
- Wykrywanie awarii i przekierowywanie ruchu
- Podtrzymywanie sesji HTTP
- Algorytmy równoważenia ruchu do wyboru
- Kontrola nagłówków przekazywanych do serwerów aplikacyjnych
- Możliwość pracy w konfiguracji o wysokiej niezawodności
- Wsparcie dla Virtual Router Redundancy Protocol (VRRP)
- Wydajność do 20 000 żądań na sekundę przy Gigabit Ethernet

# Modele



Właściwości / Modele	HB 500	HB 1000
<b>Właściwości</b>		
Kompatybilny z dowolną aplikacją TCP	✓	✓
Automatyczna detekcja awarii urządzenia docelowego	✓	✓
Rozłożenie obciążenia w edle w wybranego algorytmu	✓	✓
Podtrzymywanie sesji HTTP	✓	✓
Wsparcie dla syslog, raportowanie, wykresy	✓	✓
Wsparcie dla klastrowania		✓
<b>Parametry</b>		
Obudowa	Mini tower	1U
Karta sieciowa	2 x 1GB	4 x 1GB
Pojemność użytkownika dysków twardech	250 GB	250 GB
RAID		Hot Swap (1)
Redundantne zasilacze		✓
Pamięć ECC		✓
<b>Wydajność</b>		
Żądań na sekundę	Do 20 000	Do 40 000
<b>Wsparcie techniczne</b>		
Poziom wsparcia	Standard	Standard
Okres wsparcia	1 rok	3 lata

Następcą systemu Novell BorderManager

# Następca BorderManagera



- Dla klientów, którzy mają BorderManagera lub chcieliby mieć podobną funkcjonalność
  - apertOS NET + INTERNET PROTECT
    - > Funkcje zapory sieciowej
    - > Filtrowanie i buforowanie ruchu HTTP, FTP i HTTPS
    - > Raportowanie
    - > SSO dla eDirectory i Active Directory
    - > Oraz dodatkowo:
      - » Sprawdzanie antywirusowe i antymalware komunikacji (uaktualnienia sygnatur w cenie produktu)
      - » Predefiniowane kategorie serwisów WWW (uaktualnienia w cenie produktu)
      - » Weryfikacja użytkowników w dowolnym katalogu LDAP

# Porównanie



Usługi HTTP	BorderManager	apertOS
Proxy na porcie	Tak	Tak
Proxy transparentne	Tak	Tak
Generic/Tunnel Proxy	Tak	Tak
Redirect Proxy	Nie	Tak
DNS Cache	Tak	Tak
FTP Proxy	Tak	Tak

Hierarchia	BorderManager	apertOS
ICP Hierarchy	Tak	Tak
Hierarchia CERN/HTTP	Tak	Tak
Przekierowuj przez hierarchię	Tak	Tak

Ogólne	BorderManager	apertOS
Alarmy (SNMP, Email, Log Files, Syslog)	Tak	Tak
Logowanie	Tak	Tak
Wsparcie dla WCCP v1 & v2	Tak	Tak
Cache Bypass	Tak	Tak

# Porównanie



Reguły filtrowania	BorderManager	apertOS
Zarządzanie dostępem przez role	Tak	Tak
Predefiniowane kategorie stron	Nie	Tak
Filtrowanie według słów kluczowych	Nie	Tak
Filtrowanie frazami ważonymi	Nie	Tak
Filtrowanie według URL	Tak	Tak
Filtrowanie według rozszerzeń i typów MIME plików	Nie	Tak
Filtrowanie dla grup, użytkowników, adresów IP	Nie	Tak

# Porównanie



Bezpieczeństwo	BorderManager	apertOS
Virtual Private Network (VPN)	Tak	v. 1.1
<b>Uwierzytelnianie</b>		
Podstawowe (Basic)	Tak	Tak
Secure Form Based	Tak	Tak
eDir (NDS)	Tak	Tak
eDir SSO – wymaga Client32 na stacji	Nie	Tak
eDir SSO – wymaga ClientTrust na stacji	Tak	Nie
LDAP	Nie	Tak
NTLM (AD)	Nie	Tak
NTLM SSO (AD)	Nie	Tak
NT Domain	Nie	Tak
<b>Firewall</b>		
Filtrowanie pakietów (Port, IP, zakres IP, itp.)	Tak	Tak
Stateful Packet Inspection	Tak	Tak
Predefiniowane reguły dla popularnych aplikacji	Nie	Tak
Konfiguracja stref (Wewnętrzna, Publiczna, DMZ)	Nie	Tak
<b>Antywirus</b>		
Skanowanie antywirusowe ruchu HTTP	Nie	Tak
Skanowanie antywirusowe ruchu FTP	Nie	Tak

# Porównanie



Monitorowanie	BorderManager	apertOS
Aktywność urządzenia	Tak	Tak
Statystyki	Tak	Tak
Raporty z proxy	Nie	Tak
Grafy statystyczne	Nie	Tak

Narzędzia do zarządzania	BorderManager	apertOS
Interfejs WWW	Tak	Tak
Interfejs „command line”	Tak	Nie
Dostępny w formie appliance	Nie	Tak
Uaktualnienie poprzez sieć	Nie	Tak
Uaktualnienia sygnatur antywirusowych	Nie	Tak
Uaktualnienia list kategorii	Nie	Tak

Wsparcie techniczne

# Dwa poziomy wsparcia



- apertOS Standard Support
  - Automatyczne uaktualnienia bazy SPAMu, wirusów, RBL, URIBL oraz predefiniowanych kategorii
  - Roczna gwarancja z serwisem typu urządzenie zastępcze - 72h
  - Pomoc techniczna od poniedziałku do piątku, z wyłączeniem świąt w godzinach 9:00 – 17:00
- apertOS Premium Support
  - Automatyczne uaktualnienia bazy SPAMu, wirusów, RBL, URIBL oraz predefiniowanych kategorii
  - Roczna gwarancja z serwisem typu urządzenie zastępcze - 48h
  - Pomoc techniczna 24x7
- Wsparcie jest dostępne na 1 rok, 3 lata lub 5 lat

Jak i gdzie można kupić?

# Sieć sprzedaży rozwiązań apertOS



- Rozwiązania sprzętowe
  - Sprzedawane przez sieć partnerów Action
  - Nielimitowana liczba użytkowników na urządzeniu
  - Osoby kontaktowe:
    - > Marcin Bogusz – Action
    - > Marcin Madey – apertOS
- Rozwiązania oparte o wirtualne maszyny VMware
  - Sprzedawane bezpośrednio przez firmy apertOS i Novell
  - Licencja na użytkownika
  - Osoby kontaktowe:
    - > Marcin Madey – apertOS
    - > Tomasz Surmacz – Novell

# Dane kontaktowe



- Kontakt

- Marcin Madey – [mmadey@apertos.pl](mailto:mmadey@apertos.pl)

- apertOS Sp. z o.o. Sp. k.

- tel. 22 537 5090

- Marcin Bogusz – [Marcin.Bogusz@action.pl](mailto:Marcin.Bogusz@action.pl)

- ACTION S.A.

- Tel. 22 332 1600

- Tomasz Surmacz – [turmacz@novell.pl](mailto:turmacz@novell.pl)

- Novell Sp. z o.o.

- Tel. 22 537 5000

# Dziękujemy za uwagę

apert   TWOJA SIEĆ POD KONTROLĄ