

prevenity

SECURITY SOLUTIONS

Skuteczna kontrola aplikacji i działań użytkowników w sieci Rozwiązanie Palo Alto Networks

Marek Janiczek, Prevenity



Agenda

- Wyzwania i potrzeby w zakresie ochrony w warstwie sieciowej
- System zabezpieczeń nowej generacji - Next Generation Firewall
- Rozwiązanie Palo Alto Networks
- Podsumowanie

Wyzwania Dynamika aplikacji

File sharing Webmail VoIP ... Streaming Instant Messaging & Chat

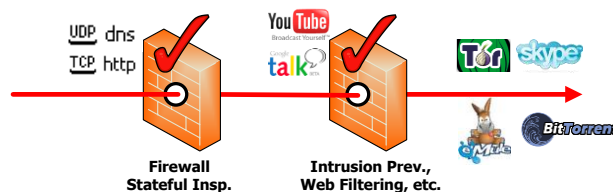
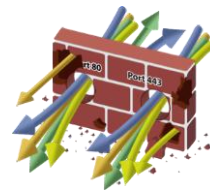


Blokować czy nie blokować ?

- Aplikacje – duża ilość, różne wykorzystywane porty
- Użytkownicy – brak stałej lokalizacji, przydzielane różne adresy IP
- Przesyłana treść – inna niż deklarowana, szyfrowana

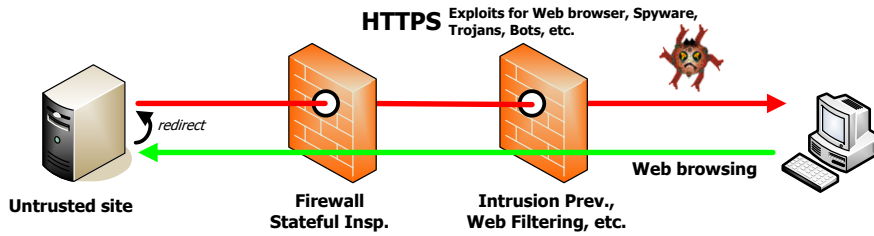
Wyzwania Świadomość warstwy aplikacji

- Aplikacje internetowe w większości:
 - Wykorzystują protokoły HTTP i HTTPS
 - Używają dynamicznych portów
 - Stosują mechanizmy kryptograficznej ochrony informacji
- Standardowe systemy zabezpieczeń sieci:
 - Identyfikują aplikacje Web jako TCP/80, TCP/443
 - Posiadają ograniczoną świadomość warstwy aplikacji
 - Nieefektywnie identyfikują aplikacje działające w oparciu o HTTP i HTTPS

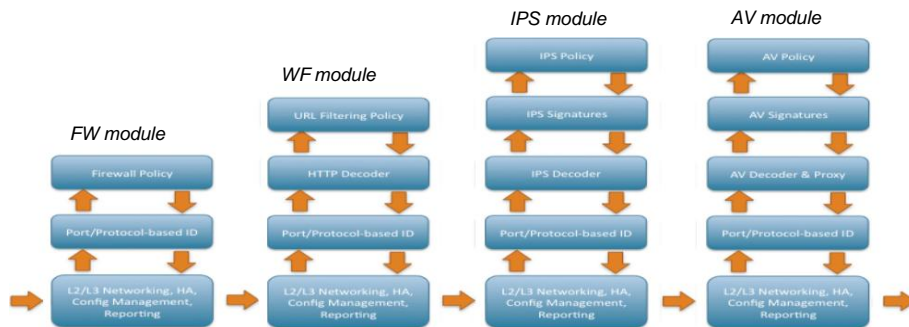


Wyzwania Ruch szyfrowany

- Brak inspekcji zawartości szyfrowanego ruchu
- Wektor ataków na stronę użytkownika



Wyzwania Wydajność



- Standardowo, inspekcja ruchu aplikacyjnego dokonywana jest przez wiele modułów
- Moduły wzajemnie przekazują sobie dane powodując obniżenie wydajności

Stosowane zabezpieczenia Czy jesteśmy bezpieczni?

- Czy stosowane rozwiązania mogą wykryć i blokować niebezpieczne aplikacje:
 - Wymiana i dystrybucja plików (BitTorrent, Gnutella, Rapidshare)
 - Podwyższanie poziomu prywatności w sieci (Tor)
 - Zewnętrzne serwery poczty dostępne poprzez web (Gmail, HotMail)
 - Komunikatory (GG, AIM)
 - Portale społecznościowe (blogi, Facebook, LinkedIn, MySpace, Twitter, Youtube)
- Czy stosowane rozwiązania mogą wykryć i zablokować ataki w ruchu SSL?
- Czy stosowane rozwiązania blokują stosowanie zewnętrznych serwerów proxy?

Obecne potrzeby

- Możliwość tworzenia precyzyjnych polityk filtracji ruchu
 - Identyfikacja i kontrola aplikacji, niezależnie od stosowanego portu/protokołu
 - Identyfikacja i kontrola użytkowników, niezależnie od przypisanego adresu IP
 - Kontrola dostępu do aplikacji i ich funkcji
- Możliwość inspekcji ruchu niezaszyfrowanego/zaszyfrowanego (HTTP/HTTPS)
- Możliwość ochrony przed wyciekiem wrażliwych informacji
- Elastyczność i wydajność zabezpieczeń
- Efektywność kosztowa zabezpieczeń

Przykład źródeł wymagań bezpieczeństwa w odniesieniu do kontroli dostępu

- Regulacje, normy, dobra praktyka
 - ISO 27001 – A.11.4.1
 - Zasada minimalnych uprawnień

Next Generation Firewall

- Platforma inspekcji ruchu sieciowego i wymuszania polityki bezpieczeństwa
 - Cechy zapór ogniowych „pierwszej generacji”
 - Filtracja pakietów
 - Translacja adresów
 - Analiza stanu połączeń
 - Zdalny dostęp
 - Zarządzanie pasmem
 - Świadomość warstwy aplikacji
 - Identyfikacja aplikacji i wymuszanie polityk bezpieczeństwa niezależnie od portu/protokołu
 - Blokowanie wybranych funkcji aplikacji (np. blokowanie udostępniania plików)
 - Inspekcja ruchu niezasyfrowanego/zasyfrowanego
 - Ochrona przed wyciekiem wrażliwych informacji
 - Integracja z zewnętrznymi systemami
 - Podwyższenie skuteczności mechanizmów kontroli działań użytkowników



Defining the Next-Generation Firewall

Gartner RAS Core Research Note G00171540, John Pescatore, Greg Young, 12 October 2009, R3210 04102010



Firewalls need to evolve to be more proactive in blocking new threats, such as botnets and targeted attacks. Enterprises need to update their network firewall and intrusion prevention capabilities to protect business systems as attacks get more sophisticated.

Key Findings

- The stateful protocol filtering and limited application awareness offered by first-generation firewalls are not effective in dealing with current and emerging threats.
- Using separate firewalls and intrusion prevention appliances results in higher operational costs and no increase in security over an optimized combined platform.
- Next-generation firewalls (NGFWs) are emerging that can detect application-specific attacks and enforce application-specific granular security policy, both inbound and outbound.
- NGFWs will be most effective when working in conjunction with other layers of security controls.

Recommendations

- If you have not yet deployed network intrusion prevention, require NGFW capabilities of all vendors at your next firewall refresh point.
- If you have deployed both network firewalls and network intrusion prevention, synchronize the refresh cycle for both technologies and migrate to NGFW capabilities.
- If you use managed perimeter security services, look to move up to managed NGFW services at the next contract renewal.

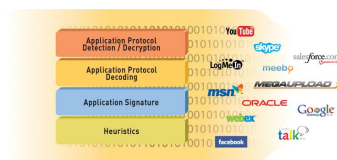
Palo Alto Networks



Rozwiązanie PAN Technologie ochrony

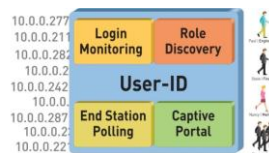
App-ID

Identyfikacja aplikacji



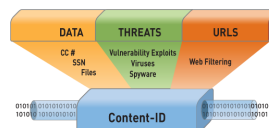
User-ID

Identyfikacja użytkowników

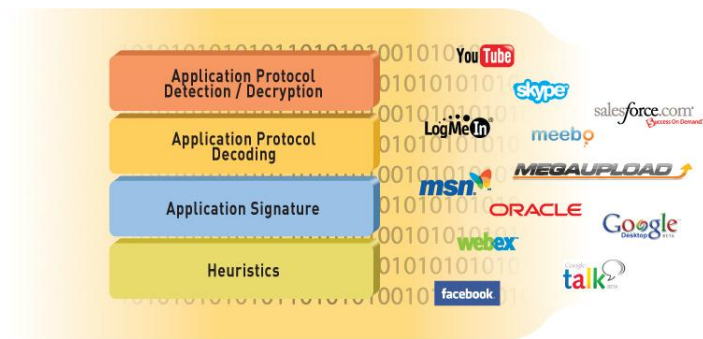


Content-ID

Skanowanie zawartości



App-ID: Identyfikacja i klasyfikacja aplikacji



- Identyfikacja ponad 900 aplikacji, podzielonych na kategorie
- Możliwość definiowania własnych aplikacji
- Rozpoznawanie aplikacji za pomocą sygnatur i heurystyki

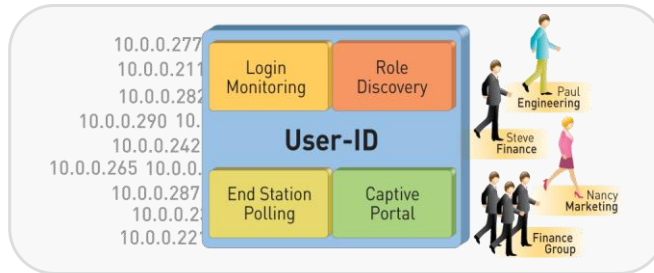
Kontrola aplikacji

Name	Source Zone	Destination Zone	Source Address	Source User	Destination Address	Application	Service	Action	Profile
1 Allow Business Applications	l2-lan-trust	l2-lan-untrust	any	Exec Staff ITAdmins finance marketing	any	business-application networking	any	✓	

- Definicja dozwolonych aplikacji

Category	Subcategory	Technology	Risk	Characteristic
11 business-systems	10 auth-service	41 browser-based	179	107 Vulnerabilities
101 collaboration	10 database	129 client-server	63	155 Prone to Hoax
71 general-internet	11 encrypted-tunnel	49	159	159 Widely used
41 media	7 erp-crm	17	20	20 Excessive Bandwidth
211 networking	10 general-business	103	103	103 Transfers Files
1 unknown	23 infrastructure	26	53	53 Evasive
	116 ip-protocol	4	46	46 Used by Malware
	37 management		61	61 Tunnels Other Apps

User-ID: Identyfikacja użytkowników



- Korelacja adresów IP z użytkownikami aplikacji
- Firewall ma możliwość operowania na nazwach/grupach użytkowników
- Incydenty przypisane do konkretnych użytkowników
- Integracja z Active Directory, eDirectory (User-ID Agent)
- Obsługa Citrix i MS Terminal Services (TS Agent)
- Dla gości „Captive Portal” (Web i NTLM)

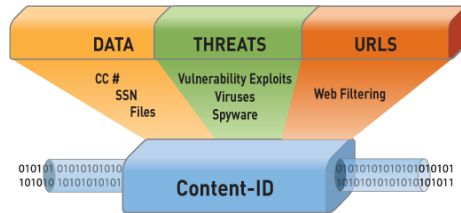
Kontrola użytkowników

Security Rules										
Name	Source Zone	Destination Zone	Source Address	Source User	Destination Address	Application	Service	Action	Profile	
1	Allow Business Applications	I2-lan-trust	I2-lan-untrust	any	Eric Staff ITAdmins Finance marketing	any	business-application networking	any	✓	🛡️ 🛡️ 🛡️ 🛡️

- Polityka firewall precyzyjnie definiuje prawa dostępu użytkowników do określonych usług sieci i jest utrzymana nawet gdy użytkownik zmieni lokalizację i adres IP
- Firewall transparentnie weryfikuje tożsamość użytkowników sieci (integracja z Active Directory, Citrix i MS Terminal Services)



Content-ID: Skanowanie zawartości



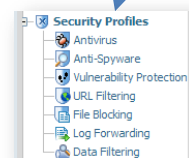
- Wykrywanie i blokowanie ataków, złośliwego kodu i nielegalnego transferu plików
- Kontrolowanie wykorzystania usług Web
- **Anti-Virus, Anti-Spyware, Vulnerability Protection** - baza uniwersalnych sygnatur
- **URL Filtering** - baza URL dostarczana przez BrightCloud
- **File Blocking** - identyfikacja plików na podstawie typu MIME i nagłówka pliku
- **Data Filtering** - identyfikacja wrażliwych danych na podstawie wyrażeń regularnych

Skanowanie zawartości

Security Rules										
Name	Source Zone	Destination Zone	Source Address	Source User	Destination Address	Application	Service	Action	Profile	
1 Allow Business Applications	l2-lan-trust	l2-lan-untrust	any	Exec Staff ITAdmins finance marketing	any	business-application networking	any	✓		

Buttons: Add Rule, Clone Rule, Delete Rule, Disable Rule, Move Rule: --- Select ---

- Profile ochrony realizują funkcje inspekcji ruchu

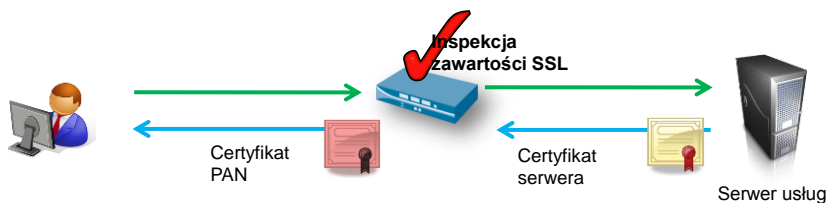


Next Generation Firewall NSS Labs

NSS Labs' Rating: **Recommend**

- Test urządzenia PA-4020
 - Wskaźnik blokowania zagrożeń: 93.4%
 - Odporność na próby oszukania mechanizmów IPS: 100%
 - Wydajność na poziomie 115% w stosunku do specyfikacji

Inspekcja zawartości szyfrowanego ruchu



- Inspekcja zawartości niezaufanego ruchu SSL (wychodzący/przychodzący)
- Ochrona użytkowników przed atakami w komunikacji szyfrowanej
- Wewnętrzny urząd certyfikacji do dynamicznego generowania certyfikatów

Inspekcja zawartości szyfrowanego ruchu

SSL Decryption Rules									
	Name	Source Zone	Destination Zone	Source Address	Source User	Destination Address	Category	Certificate	Action
1	rule1	Users	Internet	any	any	any	financial-services government shopping	forward proxy	no-decrypt
2	rule2	Users	Internet	any	any	any	any	forward proxy	decrypt

Issued To

Common Name (CN) www.google.com
 Organization (O) Google Inc
 Organizational Unit (OU) <Not Part Of Certificate>
 Serial Number 2F:DF:BC:F6:AE:91:52:6D:0F:9A:A3:DF:40:34:3E:9A

Issued By

Common Name (CN) Thawte SGC CA
 Organization (O) Thawte Consulting (Pty) Ltd.
 Organizational Unit (OU) <Not Part Of Certificate>

Validity

Issued On 2009-12-18
 Expires On 2011-12-19

Fingerprints

SHA1 Fingerprint 40:50:62:E5:BE:FD:E4:AF:97:E9:38:2A:F1:6C:C8:7C:8F:B7:C4:E2
 MD5 Fingerprint C4:70:74:FB:69:F9:E3:94:7E:88:28:A4:00:73:DE:01

Issued To

Common Name (CN) www.google.com
 Organization (O) Google Inc
 Organizational Unit (OU) <Not Part Of Certificate>
 Serial Number 2F:DF:BD:0A:64:87:0A:66:0F:9A:A3:DF:40:34:3E:9A

Issued By

Common Name (CN) paloalto.prevenity.com
 Organization (O) Prevenity
 Organizational Unit (OU) Prevenity

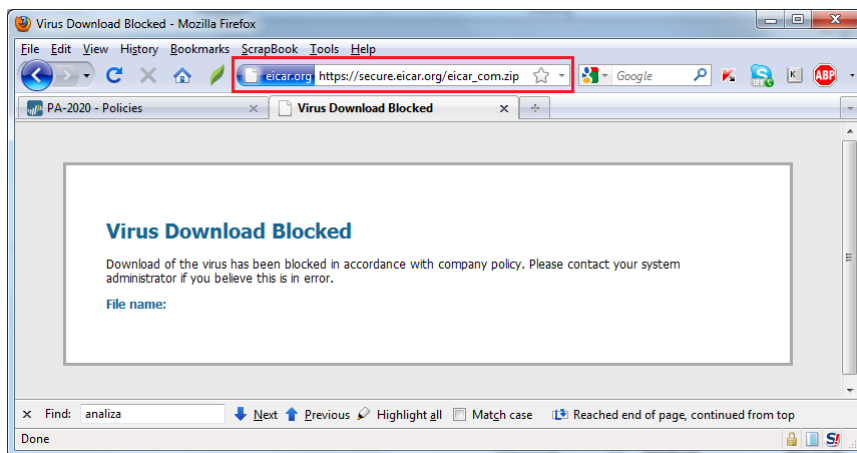
Validity

Issued On 2009-12-18
 Expires On 2011-12-19

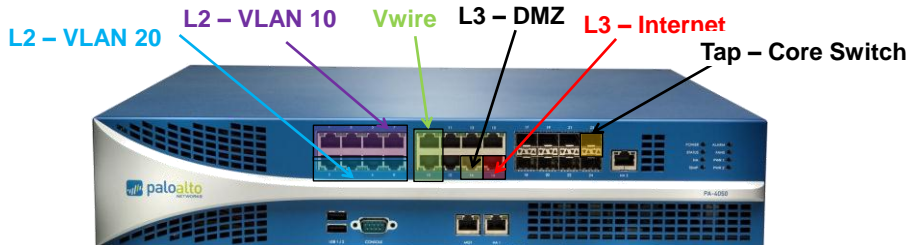
Fingerprints

SHA1 Fingerprint 71:CA:14:64:62:62:33:2A:14:80:32:C0:65:69:B2:18:65:07:C8:01
 MD5 Fingerprint DB:C3:F3:20:E9:D0:2A:66:AB:D8:9C:8E:0F:92:A0:89

Inspekcja zawartości szyfrowanego ruchu

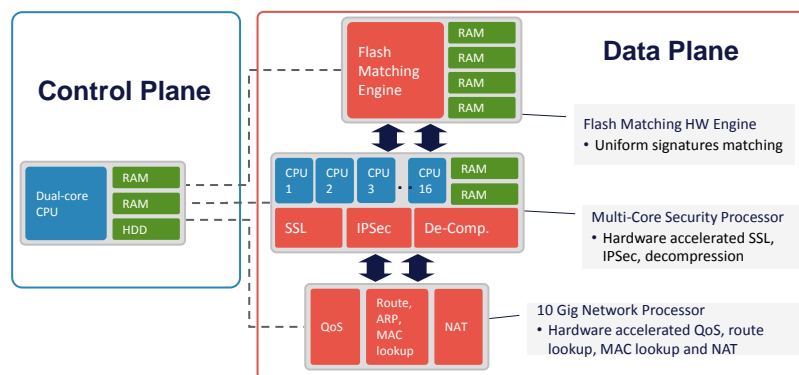


Elastyczność systemu zabezpieczeń



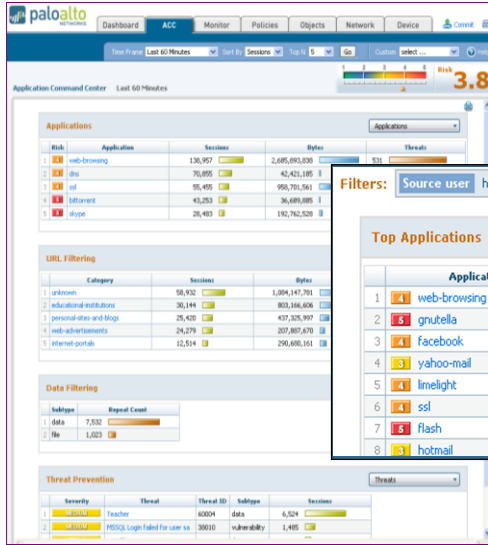
- Wiele trybów pracy (w jednym urządzeniu interfejsy mogą działać w różnych trybach)
 - Tap Mode
 - Virtual Wire
 - Layer 2
 - Layer 3
- Wirtualizacja zabezpieczeń - interfejsy VLAN (L2 i L3), wirtualne routery, wirtualne systemy

Kontrola ruchu bez degradacji wydajności



- Jeden moduł analizy ruchu wykorzystujący wspólną bazę uniwersalnych sygnatur
- Dedykowana konstrukcja sprzętowa:
 - zadania ochrony wykonywane przez specjalizowane elementy sprzętowe
 - rozdzielenie modułu zarządzania i przetwarzania ruchu

Analiza, monitorowanie i raportowanie



- Dedykowane graficzne narzędzia do wizualizacji ruchu - aplikacje, użytkownicy i zawartość
- Monitorowanie i raportowanie w czasie rzeczywistym

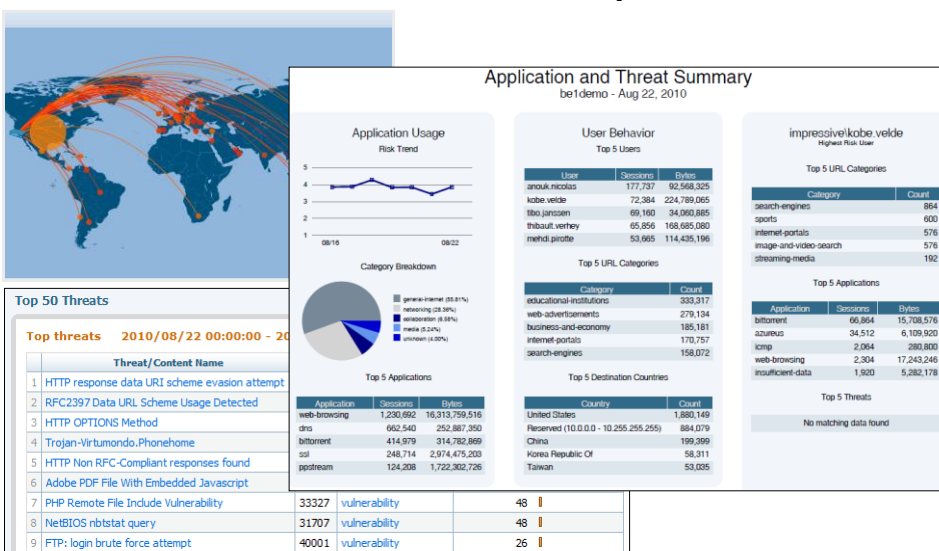
Filters: Source user: hzielski

Top Applications

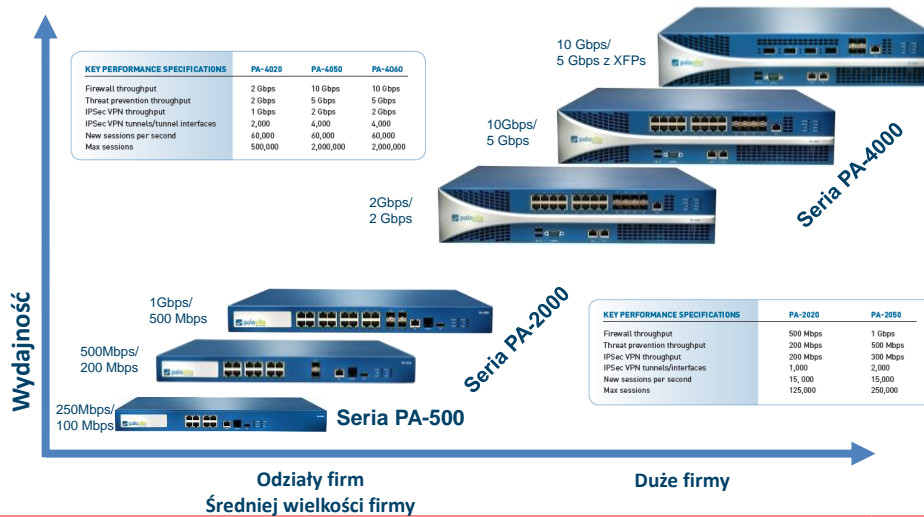
Application	Sessions	Bytes
1 web-browsing	6,142	73,161,316
2 gnutella	1,046	1,187,576
3 facebook	883	24,229,786
4 yahoo-mail	300	4,552,200
5 limelight	228	1,330,026
6 ssl	206	1,582,127
7 flash	191	13,918,590
8 hotmail	176	1,419,816

Szczegółowa analiza działań użytkownika

Analiza, monitorowanie i raportowanie



Modele urządzeń



© 2010 Prevenity Sp. z o.o. Wszelkie prawa zastrzeżone.

Podsumowanie PAN

- Rozpoznawanie i kontrola aplikacji
- Ustalanie tożsamości użytkowników sieci
- Ochrona przed atakami i złośliwym kodem (również w komunikacji szyfrowanej)
- Wykrywanie i filtracja niedozwolonych danych przesyłanych przez sieć
- Precyzyjne zarządzanie pasmem sieci
- Monitorowanie i raportowanie
- Różne tryby pracy
- Wielo-gigabitowa wydajność

© 2010 Prevenity Sp. z o.o. Wszelkie prawa zastrzeżone.

Kontakt

marek.janiczek@prevenity.com

info@prevenity.com

www.prevenity.com