

Analizator Logów Firewalli

F-Deets to narzędzie dla administratorów sieci - zbiera i analizuje logi wygenerowane przez komercyjne systemy firewall. F-Deets pozwala na szybką analizę oraz ekstrakcję danych z logów zbieranych z wielu różnych urządzeń. Dzięki mechanizmowi wbudowanych oraz definiowanych przez użytkownika filtrów możliwe jest ograniczenie zakresu analizy do dowolnie wybranych danych.

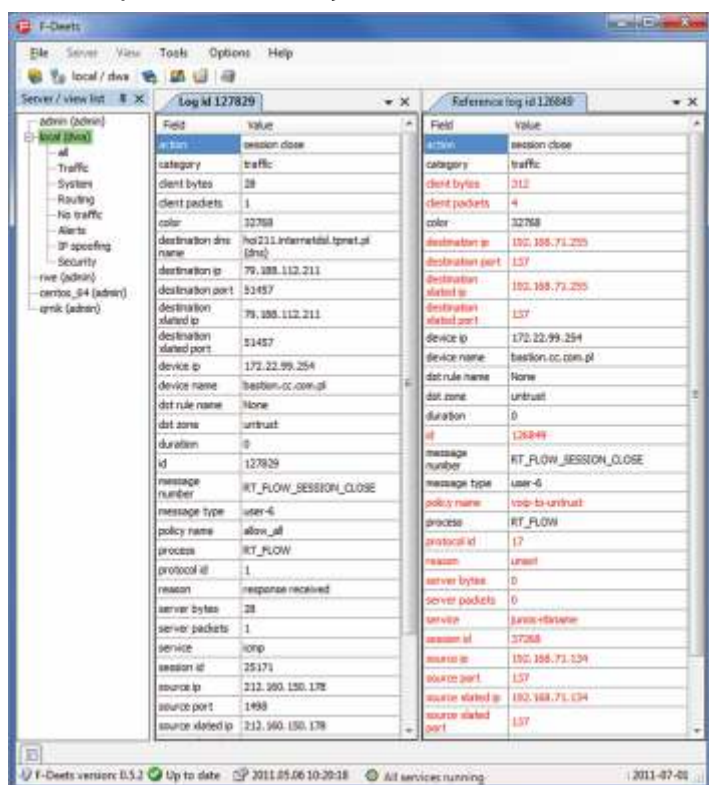
Przykładowe scenariusze zastosowań

- Centralne repozytorium logów zbieranych z wielu urządzeń i systemów sieciowych - integruje wszystkie logowane dane w jednej bazie.
- Przechowywanie i analiza logów „na zewnątrz” systemu firewall - rozwiązanie problemu ograniczonej pojemności systemu logowania wielu systemów typu appliance.
- Realizacja wymagań branżowych takich jak np: PCI, SOX i innych.

- Rotacja logów jest w pełni obsługiwana - oprogramowanie wykrywa zmiany w importowanych plikach; obsługiwany jest też tryb „tail” oraz „read-restart” (po rotacji logu).

GŁÓWNE CECHY

- Prezentuje, filtruje i analizuje logi zgodne ze standardem syslog
- Wyświetla zdarzenia z zadanego okresu czasu oraz w trybie „tail”
- Integruje wiele źródeł danych w jednym widoku
- Moduł serwerowy dostępny dla Microsoft Windows 7, Microsoft Windows XP i Linux 32/64 bit (Intel)
- Rozpoznaje i przetwarza logi generowane przez: appliance Juniper Networks SSG i SRX; firewall-e Palo Alto Networks oraz CISCO PIX i ASA.
- Możliwość rozbudowy o obsługę logów z innych systemów
- Proste do wykorzystania GUI Windows
- Pobierz i zainstaluj w 5 minut!



Zbieranie danych

- Zbiera dane pochodzące z różnych źródeł syslog.
- Dane mogą pochodzić bezpośrednio z serwisa syslog lub też być importowane z plików.
- W wersji dla Windows F-Deets zawiera wbudowany serwer syslog.
- W wersji dla Linuxa używany jest standardowy systemowy syslogd, możliwe jest też wykorzystanie rsyslog lub syslog-ng.

Analiza danych

- Filtrowanie i analiza zebranych logów.
- Autonomiczny klient GUI może być podłączony do wielu serwerów F-Deets jednocześnie.
- Można zdefiniować wiele równoległych połączeń i wiele widoków danych o zróżnicowanych uprawnieniach.



- Użytkownik może zdefiniować własne reguły przetwarzania logów - dla nieobsługiwanych standardowo formatów - dzięki mechanizmowi przetwarzania wykorzystującemu reguły (pattern matching rules).

Wizualizacja danych i raportowanie

- Przeglądanie listy i szczegółów zdarzeń.
- Definiowanie własnych filtrów danych na podstawie: adresu IP, nazwy DNS, czasu, typu zdarzenia oraz innych parametrów.
- Porównanie poszczególnych zdarzeń z podświetleniem różnic.
- Śledzenie sesji.
- Generowanie raportów w formatach: HTML, CSV i PDF.

GUI

- Łatwa w instalacji i prosta w wykorzystaniu aplikacja Windows.
- Dostępne polska i angielska wersja językowa.

Bezpieczeństwo

- Całość komunikacji pomiędzy GUI i serwerem zawsze szyfrowana jest poprzez SSL wykorzystywane w trybie end-to-end.
- Do autoryzacji GUI wykorzystywany jest standardowy certyfikat PKI.

Licencjonowanie, ceny, zamówienia

Produkt jest licencjonowany na podstawie liczby przetwarzanych dziennie zdarzeń uśrednionej w okresie 7 dni. Klient GUI pracujący pod systemem Windows nie podlega licencjonowaniu. Licencja „per-event” związana jest z modułem serwera logów. Licencja uprawnia do wykorzystania dowolnej liczby klientów GUI oraz dowolnej liczby źródeł danych (syslog lub pliki). Dostępna

OBSŁUGIWANE SYSTEMY I FORMATY LOGÓW

- Systemy firewall:
 - Juniper Networks SSG (ScreenOS)
 - Juniper Networks SRX (Junos)
 - rodzina Palo Alto Networks
 - CISCO PIX i ASA
- Inne formaty mogą być obsługiwane dzięki mechanizmowi definiowanym przez użytkownika reguł parsera
- Obsługiwane pod MS Windows XP i Windows 7 32/64 bit oraz Linux (GUI – tylko Windows)
- Wsparcie dla Linux-a obejmuje: Red Hat, Enterprise Linux 5.1 32 bit; CentOS 5.5 32/64 bit; Gentoo 64 bit
- Prosta instalacja i konfiguracja dzięki instalatorowi i kreatorowi konfiguracji dla Microsoft Windows XP and Microsoft Windows 7 (wersje 32- 64bit)

jest darmowa licencja ewaluacyjna o pełnej funkcjonalności jedynie z ograniczeniem czasowym - <http://www.f-deets.com/> - rejestracja nie jest wymagana.

Licencje:

- SME: poniżej 100 K rekordów / dzień*
- Enterprise: 100 K – 500 K rekordów / dzień
- Unlimited: bez limitu rekordów / dzień

(*) szacunkowo można przyjąć, że 100 K odpowiada 30 MB, a 500 K 250 MB logów dziennie.

Dostępne jest też wsparcie w postaci pakietów 1,3-y i 5-o letnich. Wsparcie uprawnia do: instalacji poprawek i nowych wersji oprogramowania oraz zgłaszania problemów poprzez listę e-mail i/lub forum dyskusyjne Web.



CC
Otwarte Systemy
Komputerowe Sp. z o.o.

ul. Rakowiecka 36, 02-532 Warszawa
tel. +48 22 646-68-73; fax +48 22 606-37-80
e-mail: office@cc.com.pl

Więcej informacji znajdziecie Państwo w Internecie, na stronach:
<http://www.cc.com.pl/>

Kontakt:
Dział Techniczny: tech@cc.com.pl
Dział Handlowy: sales@cc.com.pl