Riverbed SteelCentral Packet Analyzer

Analiza i wizualizacja pakietów w celu szybkiego rozwiązywania problemów w sieciach LAN

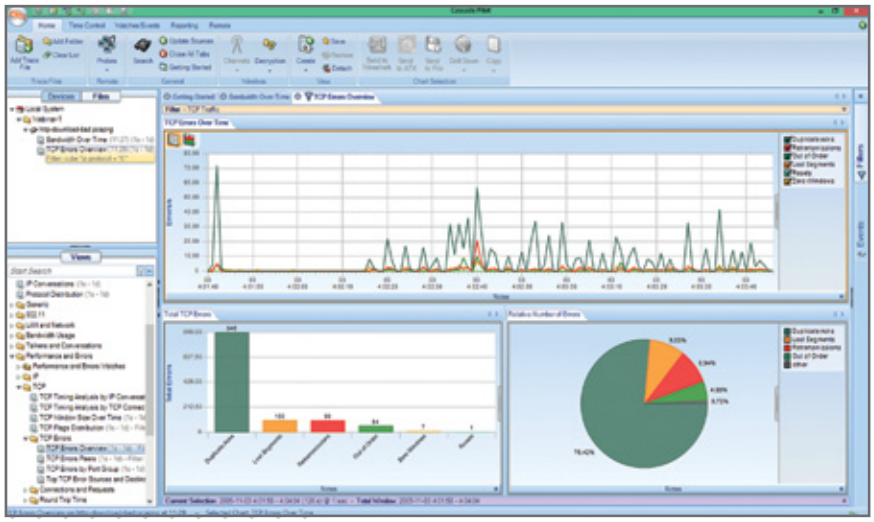
Riverbed Steel Central Packet Analyzer (wcześniej Cascade Pilot) jest narzędziem umożliwiającym wizualizację i analizę ruchu w sieciach LAN w oparciu o dane pochodzące z urządzeń do przechwytywania pakietów. Intuicyjny, graficzny interfejs pozwala zidentyfikować incydenty i odchylenia zanim zostaną zgłoszone przez użytkowników oraz wyodrębnić pakiety wymagające analizy. Narzędzie umożliwia głęboką analizę protokołów HTTP/S, VoIP, FIX, CIFS, MSSQL, LSE ITCH, GTP, MYSQL oraz analizę VDI (virtual desktop infrastructure) VMWare PCoIP, Citrix ICA, CGP.

Współpraca z urządzeniem Riverbed NetShark, które przechwytuje, indeksuje i przechowuje pakiety sieciowe eliminuje konieczność przesyłania przez sieć dużych plików ze zgromadzonymi danymi.

Packet Analyzer jest też ściśle zintegrowany z narzędziem Wireshark - najpopularniejszym darmowym analizatorem pakietów. Dzięki funkcji „Send to Wireshark" można wyeksportować informacje o wybranym ruchu sieciowym i przeprowadzić szczegółową analizy pakietów programie Wireshark.

Passus SA | ul. Wiktorska 63, 02-587 Warszawa | tel. +48 22 540 18 42 | e-mail: passus@passus.com.pl | www.passus.com.pl

Statystyki dotyczące ruchu sieciowego prezentowane w czasie rzeczywistym.



Szeroki zbiór graficznych widoków analitycznych pozwala szybko określić źródło problemów.

Cechy i zastosowania rozwiązania Riverbed Packet Analyzer:

- Łatwość izolacji konkretnych pakietów za pomocą graficznego interfejsu i technologii drag and drop.
- Szeroki zbiór graficznych widoków analitycznych pozwala szybko określić źródło problemów.
- Statystyki dot. aktualnego i historycznego ruchu sieciowego prezentowane w czasie rzeczywistym.
- Szybka analiza nawet kilkudziesięciogigabajtowych plików z przechwyconymi pakietami.
- Możliwość tworzenia wielu zadań (capture jobs) rejestrujących ruch sieciowy z prędkością nawet do kilku gigabitów na sekundę.
- Nagrywanie ruchu bez utraty pakietów.
- Możliwość analizy na poziomie transakcji.
- Definiowalne wartości brzegowe i powiązane z nimi alarmy.
- Opcjonalne powiadomienia (e-mail, SNMP Trap, SysLog) po przekroczeniu wartości brzegowych zadanych w alarmach.
- Możliwość tworzenia profesjonalnych raportów bezpośrednio z widoków analitycznych.
- Możliwość wysłania wyselekcjonowanego ruchu do analizatora Wireshark oraz narzędzia Riverbed Transaction Analyzer w celu dokonania bardziej szczegółowych analiz.

Widoki

Packet Analyzer oferuje szeroki wybór widoków, które przyspieszają i ułatwiają rozwiązywanie problemów sieciowych. Należą do nich:

- Rozwiązywanie problemów WLAN 802.11 (wykrywanie, przepustowość, wykorzystanie kanałów, retransmisje, sygnały i szumy).
- Rozwiązywanie problemów sieciowych i LAN (MAC, VLAN, ARP, ICMP, DHCP, DNS).
- Wykorzystanie przepustowości (łącznie z mikroanomaliami, IP, TCP, Web, VoIP).
- Komunikatory i rozmowy (IP, podsieci, TCP, Web, VoIP)
- Wydajność i błędy (IP, TCP, Web, VoIP).
- Aktywność użytkowników (Web, VoIP).

Wykresy

Packet Analyzer zawiera kompletny zbiór interaktywnych widoków zawierających rozbudowane wykresy, z możliwością ich edytowania lub tworzenia własnych. Wykresy pozwalają na lepsze zobrazowanie całego przechwyconego ruchu.

Drill-Down i dogłębna analiza pakietów

Drill-Down jest jedną z najbardziej przydatnych funkcji rozwiązania Packet Analyzer. Daje możliwość wgłębiania się w szczegóły w celu wyodrębnienia interesującej pojedynczej transakcji.

Packet Analyzer pozwala na wyodrębnienie mikroanomalii przyczyniających się do powstawania problemów w sieciach LAN. Dokonuje tego dzięki możliwości analizy z dokładnością do 100 mikrosekund.

Kontrola czasu: Elastyczne, długoterminowe trendy, monitorowanie i śledzenie

Packet Analyzer ma możliwość pracy na osi czasu. Przedstawienie danych w różnych okresach czasu z różną granulacją pozwala na dokładne i kompleksowe zobrazowanie ruchu.

Automatyzacja: Zaawansowany mechanizm wyzwalania i ostrzegania

Packet Analyzer posiada możliwość definiowania wartości brzegowych i alarmów w celu wychwycenia anomalii. Po przekroczeniu wartości brzegowej uruchomiony zostaje alarm, np. komunikat o wysokim wykorzystaniu przepustowości, długim czasie odpowiedzi serwera, dużych opóźnieniach w sieci itp. Dodatkowo wraz z alarmem może zostać wykonana dodatkowa akcja np. wysłanie wiadomości e-mail, SNMP Trap, SysLog czy rozpoczęcie przechwytywania pakietów.

Raportowanie

Packet Analyzer umożliwia tworzenie profesjonalnych raportów bezpośrednio z poziomu danego widoku analitycznego. Raporty mogą być generowane w formatach PDF, Word, Excel, .txt, .html, .zip. Raport jest generowany dwoma kliknięciami. Packet Analyzer posiada możliwość edytowania szablonów raportów i tworzenia własnych.

Zdalne zarządzanie

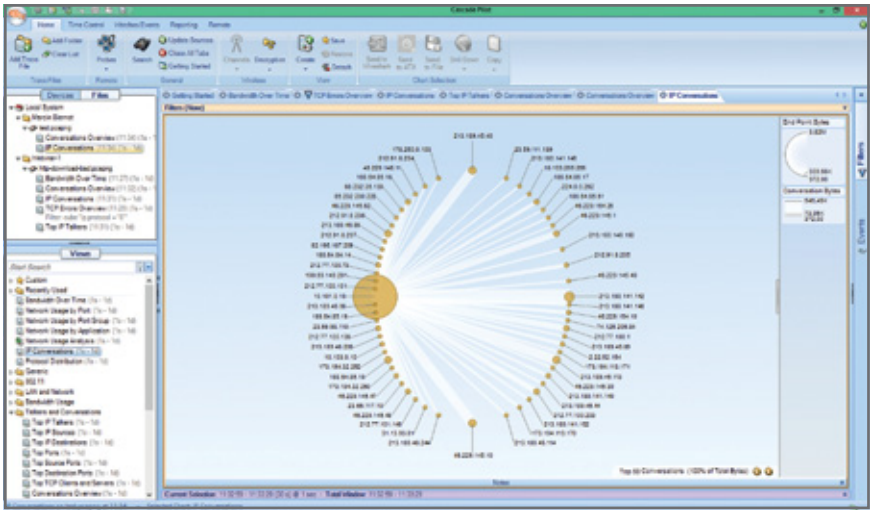
Packet Analyzer dzięki możliwości zdalnej kontroli sond SteelCentral NetShark i modułów NetShark wbudowanych w urządzenia SteelHead/AppResponse ułatwia diagnozowanie problemów w oddziałach bez konieczności wysyłania do nich administratorów.

Integracja z Wireshark

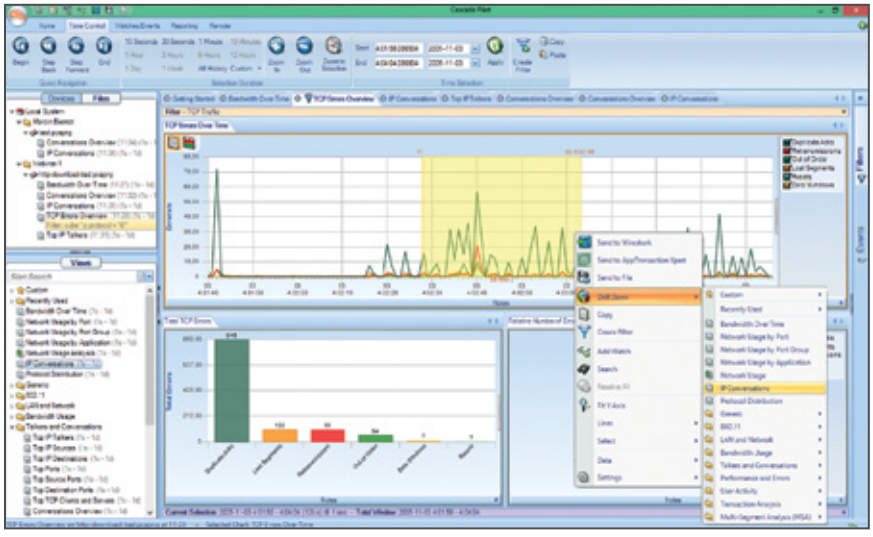
Riverbed Packet Analyzer jest w pełni zintegrowanym z darmowym analizatorem Wireshark. Integracja ta obejmuje zbiór filtrów do przechwytywania i wyświetlania. Packet Analyzer wyodrębnia konkretne dane, a następnie przesyła je bezpośrednio do Wiresharka, co eliminuje konieczność ponownej analizy całego pliku.

Współpraca z innymi rozwiązaniami Riverbed

Integracja Riverbed NetShark, Packet Analyzer i Transaction Analyzer pozwala wyodrębnić przenalizować pojedynczą transakcję z dowolnej ilości pakietów. Wykorzystanie rozwiązania Transaction Analyzer pozwala na dokładne wskazanie miejsca i przyczyny problemu oraz przedstawienie jego rozwiązania.



Widok umozliwiający podgląd konwersacji IP.



Funkcja Drill Down daje możliwość wgłębiania się w szczegóły w celu wyodrębnienia interesującej pojedynczej transakcji.

Passus Spółka Akcyjna jest polskim integratorem i dostawcą wysoko specjalizowanych rozwiązań informatycznych obejmujących w szczególności:

- rozwiązania do monitorowania i rozwiązywania problemów z wydajnością sieci oraz aplikacji;
- rozwiązania z zakresu bezpieczeństwa IT m.in. do wykrywania podatności, zabezpieczenia sieci, aplikacji oraz danych przed zaawansowanymi atakami oraz zagrożeniami wskutek nadużyć lub zaniedbań wewnętrznych;
- rozwiązania do projektowania, budowy i modernizacji wydajnych sieci WiFi w tym realizacji specjalistycznych projektów „pod klucz" (m.in. captive portal, lokalizacja zasobów, dostęp WiFi w środkach komunikacji i transportu).

Do grona Klientów w Polsce należą tak wymagający partnerzy, jak m.in. Ministerstwo Obrony Narodowej, T-Mobile, Narodowy Bank Polski, Grupa Enea, Centrum Onkologii w Gliwicach, Komisja Nadzoru Finansowego, Orange, PGE, Swedwood, PKO BP, PZU, Volkswagen Polska, Politechnika Rzeszowska, Orlen, Grupa PKP SA, Wojskowy Instytut Medyczny.

Bazując na własnych produktach i usługach oraz technologiach uznanych światowych producentów, Passus SA tworzy i wdraża rozwiązania, precyzyjnie dostosowane do wymagań klienta. Firma jest partnerem takich producentów jak: Riverbed, Core Security, GD Fidelis, Fluke Networks, Cisco, Invea-Tech oraz Qualys. Passus posiada także własny zespołów programistów i inżynierów realizujących projekty na indywidualne zamówienie. Na bazie zebranych doświadczeń, w maju 2014 roku, zespół ten przygotował unikalne w skali światowej rozwiązanie umożliwiające identyfikację nadużyć i incydentów w oparciu o analizę ruchu sieciowego – Passus Security Anomaly Detector.

Firma Passus SA powstała w wyniku wydzielenia Działu Sieci i Bezpieczeństwa IT z Passus sp. z o.o., działającej w branży IT od 1992 roku. Zatrudnia blisko 30 wykwalifikowanych pracowników – inżynierów, programistów i specjalistów. Potwierdzeniem kompetencji zespołu, obok wielu udanych wdrożeń, jest blisko 40 indywidualnych certyfikatów m.in.: poświadczenie bezpieczeństwa osobowego do klauzuli „Tajne" oraz „NATO Secret", CISA, CISSP, Riverbed Certified Solutions Professional, Cisco Associate oraz Professional w zakresie R&S (routing & switching), Security oraz Wireless, Core Impact Certified Professional, Audytor wiodący ISO 27001, Riverbed Network and Application Performance Management Qualified Trainer oraz Fluke Networks Application Performance Appliance Certified Trainer.