

JUNIPER NETWORKS AND TUFIN SECURETRACK FIREWALL OPERATIONS MANAGEMENT SOLUTION

Spójny, kompletny przegląd zapór sieciowych Juniper Networks, pozwalający zarządzać zmianami i neutralizować ryzyka przy zapewnieniu zgodności z regulacjami prawnymi

Problem

Duże przedsiębiorstwa obsługują i korzystają z wielu zapór sieciowych, rozmieszczonych pomiędzy różnymi strefami czasowymi i jednostkami biznesowymi, co wymaga ogromnych nakładów powtarzalnej, manualnej pracy. Administratorzy bezpieczeństwa mają obowiązek bycia na bieżąco z wszelkimi zmianami, jednocześnie utrzymując zgodność z korporacyjnymi politykami i rygorystycznymi regulacjami prawnymi.

Rozwiązanie

SecureTrack firmy Tufin zapewnia dogłębny wgląd we wszelkie działania zapór sieciowych. Dzięki solidnemu śledzeniu zmian, analizie ryzyka i możliwością optymalizacji bezpieczeństwa, SecureTrack pozwala zespołom odpowiedzialnym za zapory sieciowe Juniper Networks wzmocnić bezpieczeństwo sieci i zautomatyzować codzienne zadania.

Korzyści

- radykalna redukcja manualnych, powtarzalnych zadań o wysokiej podatności na błędy,
- optymalizacja użyteczności i wydajności infrastruktury,
- proaktywne wdrażanie korporacyjnych polityk bezpieczeństwa,
- zgodność z korporacyjnymi i przemysłowymi standardami oraz z regulacjami prawnymi,
- egzekwowanie najlepszych praktyk producentów,
- ulepszone zarządzanie ryzykiem.

Obsługa i użytkowanie wielu zapór sieciowych z różnorodnymi obiektami i bazami reguł wymaga ogromnych nakładów powtarzalnej, manualnej pracy. Każdorazowo kiedy wprowadzana jest zmiana do bazy reguł firewall, administratorzy muszą monitorować rodzaj zmian, oraz to, kiedy i przez kogo zostały one dokonane. Następnie muszą upewnić się, że każda ze zmian została poprawnie zaimplementowana, pozostając w zgodzie z polityką korporacyjną i regulacjami prawnymi. Wraz ze zwiększającą się skalą operacji bezpieczeństwa, ich szczegółowe monitorowanie i zagwarantowanie, że nie zostały popełnione żadne ludzkie błędy staje się coraz trudniejsze. W odpowiedzi na ten fakt, myślący przyszłościowo menadżerowie działów IT sięgają po rozwiązanie SecureTrack firmy Tufin do zarządzania operacjami zapór sieciowych Juniper Networks, które automatyzuje i upraszcza zarządzanie zmianami w zaporach firewall, zapewniając zgodność polityki bezpieczeństwa z regulacjami prawnymi.

Problem

Zapewnianie bezpieczeństwa sieciowego dla dużych organizacji stało się niezwykle złożoną operacją, obejmującą setki komponentów infrastruktury i angażującą liczne zespoły bezpieczeństwa na całym świecie. Jednocześnie organizacje mają obowiązek zachować zgodność z rygorystycznymi standardami transparentności i odpowiedzialności. Planowanie, implementacja, egzekwowanie i kontrola korporacyjnych polityk bezpieczeństwa są obecnie kwestiami kluczowymi dla biznesu.

Starając się realizować cele bezpieczeństwa, współcześni menadżerowie polegają na wachlarzu narzędzi administracyjnych pochodzących od różnych producentów aby implementować zmiany w konfiguracji, a także gromadzić i analizować dane dotyczące bezpieczeństwa. Proces ten składa się z wielu powtarzalnych, manualnych zadań o wysokiej podatności na błędy, a jego skuteczność opiera się wyłącznie na nieustannej czujności zespołu operacji bezpieczeństwa.

Czynniki te wywołują konieczność wprowadzenia automatyzacji tej dziedziny biznesu i rozwiązań zarządzających, będących w stanie pomóc zespołom odpowiedzialnym za bezpieczeństwo w wydajny sposób zgrać codzienne operacje z korporacyjnymi celami biznesowymi.

Rozwiązanie SecureTrack firmy Tufin do monitorowania zmian konfiguracji zapór sieciowych Juniper Networks

Rozwiązanie SecureTrack firmy Tufin do monitorowania zmian konfiguracji zapór sieciowych Juniper Networks zostało stworzone, aby sprostać tym wyzwaniom. SecureTrack firmy Tufin w ścisły sposób integruje się z rozwiązaniami i produktami firewall/VPN firmy Juniper Networks wzmacniającymi bezpieczeństwo. Jednocześnie redukuje przerwy w dostawie usługi oraz automatyzuje codzienne zadania.



Zarządzanie zmianami reguł bezpieczeństwa zapory sieciowej

Aby sprostać najnowszym wymaganiom dotyczącym bezpieczeństwa sieciowego, duże przedsiębiorstwa aktualnie zarządzają dziesiątkami, jeśli nie setkami, pojedynczych zapór sieciowych. Każdy firewall posiada swą własną politykę – złożony zbiór zasad, określający prawa dostępu i ograniczenia dla konkretnych użytkowników i usług. SecureTrack Tufin dla zapór sieciowych Juniper zapewnia spójny, kompletny wgląd we wszystkie polityki firewall, pozwalając zespołom bezpieczeństwa indywidualnie nadzorować każdy element układowy.

„IDC dostrzega rosnącą potrzebę rozwiązań, które łącząby zarządzanie zmianami oraz zarządzanie ryzykiem i ciągłością funkcjonowania przedsiębiorstwa z integracją z usługami typu helpdesk tego przedsiębiorstwa.”

Dan Yachin

IDC EMEA, Emerging Technologies

SecureTrack firmy Tufin nieustannie monitoruje reguły bezpieczeństwa firewall, wykrywając i raportując zmiany konfiguracji. Dzięki monitorowaniu w czasie rzeczywistym, administratorzy otrzymują szczegółowe powiadomienia o zmianach w momencie kiedy zostaną wprowadzone. System w sposób kompletny i dokładny rejestruje każdą zmianę konfiguracji i jest w stanie przypisać każde działanie do administratora firewall, który je wykonał. Daje to personelowi czuwającemu nad bezpieczeństwem niespotykane dotąd możliwości wglądu w to, kto, kiedy i jakiej zmiany dokonał, analizując efekt, jaki wywarła ona na sieć.

Optymalizacja polityki bezpieczeństwa i czyszczenie

Kiedy tysiące biletów (żądań zmiany) jest przetwarzanych przez zespół obsługi firewall, a korporacyjne cele bezpieczeństwa z biegiem czasu ewoluują, podstawowa baza reguł, zawierająca informacje na temat polityki zapory, zaczyna się skrajnie rozrastać i staje się niezwykle skomplikowana. Zasadniczo wiele z reguł i obiektów typowej bazy reguł firewall jest już przestarzałych. Te nieużywane reguły stanowią potencjalną lukę w systemie bezpieczeństwa i powinny być wyeliminowane. Operatorzy firewall, korzystając ze standardowych narzędzi administracyjnych, nie dysponują środkami w łatwy sposób wykrywającymi tego typu reguły.

Poza ryzykiem jakie stwarza dla bezpieczeństwa, niewłaściwie utrzymana baza reguł może w znaczący sposób wpływać na wydajność. Cała baza reguł jest poddawana analizie składniowej przy każdym połączeniu sieciowym, więc wraz ze wzrostem objętości bazy reguł, zwiększają się również wymagania sprzętowe. Nadmierne skomplikowane bazy reguł są trudne w obsłudze i należy regularnie poddawać je czyszczeniu.

Analiza SecureTrack Rule and Object Usage rejestruje logi ruchu sieciowego pochodzące z modułów zapór sieciowych i menadżera NSM firmy Juniper Networks, aby przeprowadzać statystyczną analizę faktycznego zastosowania każdej z reguł i obiektów w różnych przedziałach czasowych. Będąc w posiadaniu tych informacji, przeglądając bazy reguł każdej z zapór sieciowych, administratorzy są w stanie optymalizować ich działanie i czyścić je z nieużywanych reguł.

ID	HTS	FIRST HIT	LAST HIT	Source	Destination	Service	Action
1033	(27%)	Tue, 13 May 2008 15:00	Tue, 13 May 2008 15:00	Lab_Server 33 (100%)	RemoteSrv_33 (100%)	SSH 33 (100%)	✓
944	(22%)	Tue, 13 May 2008 15:00	Tue, 13 May 2008 15:00	Lab 17 (39%)	RemoteSrv_21 44 (100%)	FTP 0 (0%) HTTP 44 (100%)	✓
3241	(21%)	Tue, 13 May 2008 15:00	Wed, 23 Jul 2008 09:03	Any	Any	SYSLOG 6 (15%)	✓
822	(11%)	Tue, 13 May 2008 15:00	Tue, 13 May 2008 15:00	10.23.23.100/32 0 (0%)	Lab 22 (100%)	TELNET 0 (0%)	✗
2323	(10%)	Tue, 13 May 2008 15:00	Tue, 13 May 2008 15:00	shayehay 0 (0%)	Lab 20 (100%)	ANY	✗

ID	HTS	FIRST HIT	LAST HIT	Source	Destination	Service	Action
237	(4%)	Tue, 13 May 2008 15:00	Tue, 13 May 2008 15:00	192.168.5.75/32 0 (0%)	172.14.2.0/24 0 (0%)	2_2008-0002_1 7 (100%)	✓
313	(5%)	Tue, 13 May 2008 16:00	Tue, 13 May 2008 16:00	Amsterdam 0 (0%) Paris 10 (100%)	Lab_Server 10 (100%)	LDAP 0 (0%) SSH 10 (100%) TELNET 0 (0%)	✗
2323	(10%)	Tue, 13 May 2008 15:00	Tue, 13 May 2008 15:00	shayehay 0 (0%)	Lab 20 (100%)	ANY	✗
822	(11%)	Tue, 13 May 2008 15:00	Tue, 13 May 2008 15:00	10.23.23.100/32 0 (0%)	Lab 22 (100%)	TELNET 0 (0%)	✗
3241	(21%)	Tue, 13 May 2008 15:00	Wed, 23 Jul 2008 09:03	Any	Any	SYSLOG 6 (15%)	✓

ID	HTS	FIRST HIT	LAST HIT	Source	Destination	Service	Action
200				all	any	2_2008-0002_1	✓
150				internal	any	HTTP	✓
160				any	any	2000-2000_1	✗

Schemat 1: analiza SecureTrack Rule and Object Usage umożliwia administratorom optymalizację baz reguł i wydajności firewall.

Zarządzanie analizą ryzyka i ciągłością funkcjonowania przedsiębiorstwa

Konsekwencje błędów w regułach bezpieczeństwa zapory sieciowej mogą być surowe – począwszy od naruszeń bezpieczeństwa, poprzez przerwy w dostawie usługi sieciowej, a skończywszy nawet na przestoju sieci. W związku z tym, niezwykle istotna jest analiza potencjalnych skutków każdej zmiany, zanim zostanie ona zaimplementowana w praktyce. Biorąc pod uwagę rozmiary i złożoność bazy reguł firewall, zadanie to jest bardzo skomplikowane. Mimo to, jest ono powszechnie wykonywane manualnie przez administratorów zapór sieciowych, nie posiadających jednak narzędzi odpowiednich do analizy bazy reguł.

Właściwość SecureTrack Policy Analysis firmy Tufin pozwala na przeprowadzenie symulacji bazy reguł, aby sprawdzić, czy dany wzorzec ruchu sieciowego jest aktualnie zablokowany czy dozwolony i aby przedstawić sugestie, dotyczące zalecanych działań korygujących. Ponadto, w celu zapobiegania naruszeniom bezpieczeństwa i przerwom w dostawie usługi, mechanizm Compliance Alerts analizuje każdą zmianę i powiadamia o zmianach, które mogą zezwalać na nieautoryzowany ruch sieciowy lub go blokować.

Kontrola korporacyjnej polityki bezpieczeństwa, zgodność z regulacjami prawnymi i najlepsze praktyki

Firmy zaczęły uświadamiać sobie wpływ bezpieczeństwa sieciowego na funkcjonowanie i zyski przedsiębiorstwa. Wymagają więc najwyższego poziomu transparentności i odpowiedzialności. Aby sprostać tym oczekiwaniom, organizacje muszą mieć możliwość przeprowadzania okresowych kontroli, aby zapewnić zgodność z trzema różnymi poziomami dyrektyw bezpieczeństwa: polityką korporacyjną, regulacjami prawnymi i najlepszymi praktykami. Z powodu rozmiarów i dynamicznej natury polityki bezpieczeństwa zapór sieciowych, przeprowadzanie tych kontroli manualnie jest zbyt skomplikowane i pochłania za wiele czasu.

SecureTrack umożliwia zastosowanie korporacyjnej polityki bezpieczeństwa danej organizacji, jako podstawy do codziennego zarządzania firewall. Każda zmiana jest monitorowana w kontekście polityki korporacyjnej, a powiadomienia o braku zgodności wysyłane są w czasie rzeczywistym. SecureTrack ulepsza również procedury i procesy zarządzania bezpieczeństwem, takie jak analiza polityki zapory sieciowej, które w standardach przemysłu i regulacjach rządowych stanowią podstawowe wymagania dla bezpieczeństwa IT. SecureTrack gwarantuje zgodność z tymi standardami poprzez wprowadzenie skutecznych środków kontroli operacji IT oraz redukcję ryzyka związanego ze zmianami wprowadzanymi do zapór sieciowych.

Biorąc pod uwagę różnorodność urządzeń – różne wersje i narzędzia administracyjne – egzekwowanie najlepszych praktyk nie jest w obrębie organizacji prostą sprawą. Przykładowo, najlepsze praktyki zostały stworzone, aby nazywać zmiany i tworzyć komentarze wyjaśniające każdą zmianę. Dzięki SecureTrack, menadżerowie mogą zdefiniować najlepsze praktyki i są w stanie wykryć brak zgodności we wszystkich urządzeniach odpowiedzialnych za bezpieczeństwo.

Właściwości i korzyści

SecureTrack firmy Tufin pomaga zespołom odpowiedzialnym za operacje bezpieczeństwa zarządzać zmianami, minimalizować ryzyko i radykalnie zredukować konieczność manualnych, powtarzalnych zadań dzięki automatyzacji tych procesów.

Właściwości

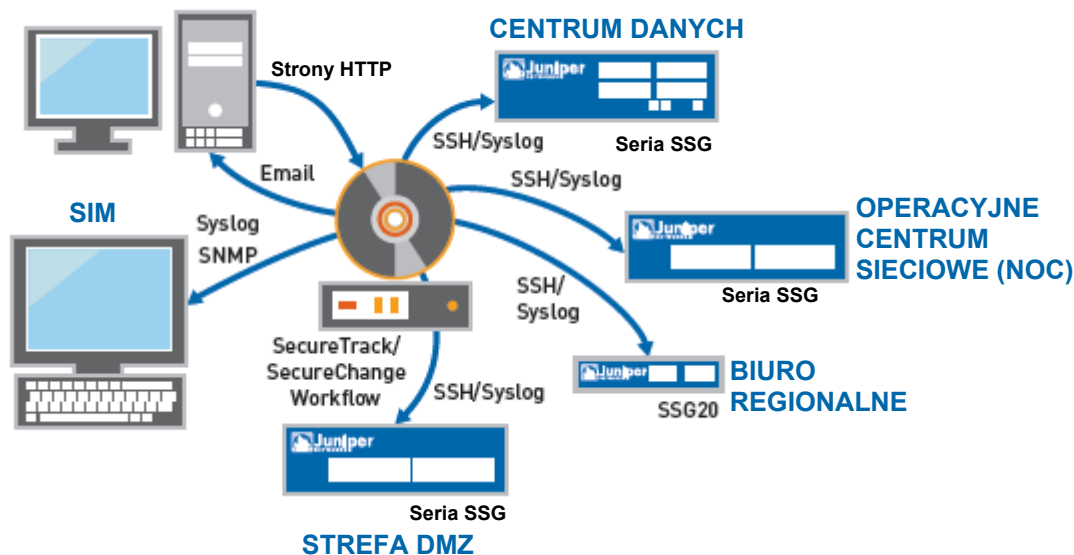
- Zarządzanie zmianami: Monitorowanie zmian reguł bezpieczeństwa zapór sieciowych, raportowanie ich w czasie rzeczywistym i rejestrowanie kompletnej, precyzyjnej ścieżki przebiegu kontroli, w celu zachowania pełnej odpowiedzialności.
- Optymalizacja polityki bezpieczeństwa i czyszczenie: Analiza i czyszczenie złożonych baz reguł i obiektów, aby wyeliminować potencjalne naruszenia bezpieczeństwa i zwiększyć wydajność.
- Analiza ryzyka i ciągłość funkcjonowania przedsiębiorstwa: Szczegółowa symulacja i analiza ryzyka, aby zidentyfikować potencjalne ryzyka dla bezpieczeństwa, zapewnić zgodność z korporacyjnymi standardami bezpieczeństwa i zapobiegać przerwom w dostawie usługi.
- Automatyzacja zmian: Automatyczne przetwarzanie żądań zmian dotyczących bezpieczeństwa, aby ułatwić obsługę użytkownikowi przy jednoczesnym zwiększeniu skuteczności działania administratorów sieci. Zarządzany jest całkowity cykl życiowy żądania zmiany polityki, począwszy od przyjęcia żądania, poprzez projektowanie, analizę ryzyka, zatwierdzenie, implementację i kontrolę.
- Międzyplatformowe monitorowanie graficzne: Intuicyjny graficzny wgląd w polityki firewall, bazy reguł i zmiany konfiguracji dla zapór sieciowych zarówno Juniper Networks, jak i innych firm.
- Kontrola i zgodność z regulacjami prawnymi: Szczegółowa kontrola zmian reguł bezpieczeństwa zapór sieciowych przy zastosowaniu zewnętrznych, obiektywnych regulacji przemysłowych, obejmujących PCI-DSS, SOX, HIPAA, ISO 17799 oraz Basel II.

Korzyści

- Radykalna redukcja manualnych, powtarzalnych zadań o wysokiej podatności na błędy.
- Zoptymalizowana użyteczność i wydajność infrastruktury.
- Ulepszone bezpieczeństwo sieciowe i czas działania bez przestoju.
- Egzekwowanie korporacyjnych polityk bezpieczeństwa.
- Gwarancja ciągłości funkcjonowania przedsiębiorstwa.
- Zgodność z korporacyjnymi i przemysłowymi standardami oraz z regulacjami prawnymi.
- Egzekwowanie najlepszych praktyk producentów.
- Ulepszone zarządzanie ryzykiem.

„Właściwości rozwiązania SecureTrack, takie jak szczegółowe monitorowanie i analiza w czasie rzeczywistym, sprawiają, że praca włożona w zarządzanie zmianami w zaporach sieciowych i w egzekwowanie zgodności z polityką bezpieczeństwa staje się lekka.”

SC Magazine



Schemat 2: Środowisko sieciowe SecureTrack

Komponenty rozwiązania

Produkt SecureTrack jest dostępny zarówno w formie oprogramowania, jak i urządzenia. Oprogramowanie jest instalowane na serwerze Redhat Linux lub CentOS. Urządzenie to wzmocniony serwer Linux. Klienci wdrażający rozwiązanie SecureTrack stosują je do monitorowania urządzeń firewall z różnych rodzin produktów Juniper, takich jak bezpieczne bramy sieciowe Secure Services Gateways serii SSG Juniper Networks i zintegrowane bramy sieciowe Integrated Security Gateways serii ISG Juniper Networks. Standardowo rozwiązanie SecureTrack wdrażane jest w centrum operacyjnym i łączy się ono z urządzeniami, rozlokowanymi w innych centrach operacyjnych, centrach danych i biurach regionalnych.

SecureTrack używa Syslog, aby śledzić wszelkie zmiany dokonywane na ScreenOS5.X i ScreenOS6.X w czasie rzeczywistym. Każdorazowo kiedy rozwiązanie SecureTrack jest powiadamiane o zmianie przez urządzenie firewall lub przez menadżera NSM, odzyskuje ono aktualną politykę poprzez SSH. SecureTrack przechowuje te polityki jako korekty w swojej bazie danych.

Korekty te są przechowywane w formacie pozwalającym na szybką i skuteczną analizę służącą zarządzaniu zmianami, w celach porównawczych i kontrolnych.

Aby optymalizować bazę reguł Juniper, SecureTrack gromadzi również dane dotyczące użytkowania reguł i obiektów, pochodzące z urządzeń i z menadżera NSM, wykorzystując Syslog. Ta funkcjonalność pozwala użytkownikom na identyfikację nieużywanych reguł i obiektów, które należałoby usunąć, jako mogące stanowić potencjalne ryzyko dla bezpieczeństwa. Może być ona także wykorzystana w celu optymalizacji wydajności bazy reguł i zapory sieciowej poprzez identyfikację najrzadziej używanych reguł (mogą być one przesunięte w dół w hierarchii bazy reguł) i tych, które stosowane są najczęściej (mogą być one przesunięte ku górze w hierarchii bazy reguł).

Podsumowanie – spełnianie dzisiejszych wymagań dotyczących bezpieczeństwa sieci

SecureTrack firmy Tufin pomaga spełnić nowoczesne wymagania dotyczące bezpieczeństwa sieci, zapewniając kompletny wgląd w polityki zapór sieciowych Juniper wśród wszystkich klientów i obiektów. Ujednolicony interfejs graficzny SecureTrack ułatwia administratorom wizualizację polityki zapory, zrozumienie zmian i podjęcie stosownego działania.

SecureTrack to także wszechstronne właściwości kontroli, służące egzekwowaniu zgodności z korporacyjnymi procedurami wprowadzania zmian, a także kontrole zewnętrzne. SecureTrack zapewnia zgodność z międzynarodowymi standardami, takimi jak PCI-DSS, SOX, HIPAA, ISO 17799 oraz Basel II.

„Zgodność i złożoność wymagają skuteczniejszych możliwości optymalizacji istniejącej już bazy reguł zapory sieciowej oraz analizy potencjalnych skutków każdej zaproponowanej zmiany reguł.”

Greg Young
Gartner

Kolejne kroki

W celu uzyskania dalszych informacji, obejrzenia demonstracji produktu lub złożenia wniosku o wycenę, zapraszamy do odwiedzenia strony www.tufin.com lub skontaktowania się z jednym z wymienionych biur firmy Tufin:

Dział handlowy US

Email: sales@tufin.com
Telefon: 1-877-270-7711

Dział handlowy UK

Email: uksales@tufin.com

Dział handlowy dla Centralnej i Środkowej Europy

Email: centesales@tufin.com
Telefon: +49-89-99-216-441

Dział handlowy Włochy

Email: itasales@tufin.com
Telefon: +39-06-43-40-90-17

Dział handlowy Beneluxs

Email: beneluxsales@tufin.com
Phone: +31-64-178-9667

Siedziba główna

Email: sales@tufin.com
Telefon: +972-3-612-8118

Kontakt do dystrybutora w Polsce

Dział handlowy:

Email: sales@clico.pl
Telefon: 012 292 80 56

Dział techniczny

Email: psw@clico.pl
Telefon: 022 515 02 71

O Juniper Networks

Juniper Networks, Inc. Jest liderem w dziedzinie wysoko wydajnych rozwiązań sieciowych. Juniper zapewnia wysoce wydajną infrastrukturę sieciową, która stwarza elastyczne i godne zaufania środowisko, aby przyspieszać wdrażanie usług i aplikacji do pojedynczej sieci. Służy to napędzaniu przedsięwzięć o dużym potencjale rozwoju. Więcej informacji znaleźć można na stronie www.juniper.net

O Tufin Technologies

O SecureTrack

SecureTrack™ firmy Tufin jest wiodącym na rynku rozwiązaniem klasy SOM (Security Operations Management). SecureTrack umożliwia organizacjom wzmocnienie ochrony, redukcję przerw w dostawie usługi i automatyzację codziennych zadań, dzięki kompleksowym możliwościom zarządzania firewall i raportowania. SecureTrack pomaga zespołom odpowiedzialnym za operacje bezpieczeństwa kontrolować i zarządzać zmianami polityk, analizować ryzyko, a także zapewniać ciągłość funkcjonowania przedsiębiorstwa. Menadżerowie natomiast mają możliwość zrozumienia szerszego kontekstu całości przedsięwzięcia i zapewnienia zgodności operacji z korporacyjnymi i rządowymi standardami.

O Tufin Technologies

Firma Tufin Technologies jest liderem w dziedzinie rozwiązań zarządzania cyklem życiowym bezpieczeństwa (Security Lifecycle Management), umożliwiających dużym organizacjom wzmocnienie ochrony, zapewnienie ciągłości funkcjonowania przedsiębiorstwa i zwiększenie wydajności operacyjnej. Produkty SecureTrack™ i SecureChange™ Workflow firmy Tufin, pomagają zespołom odpowiedzialnym za operacje bezpieczeństwa zarządzać zmianami polityk, minimalizować ryzyko i radykalnie redukować manualne, powtarzalne zadania dzięki automatyzacji. Przez połączenie dokładności i prostoty, Tufin umożliwia pracownikom odpowiedzialnym za bezpieczeństwo przeprowadzanie miarodajnych kontroli i wykazywanie zgodności z korporacyjnymi i rządowymi standardami. Firma Tufin, założona w 2003 roku przez wiodących specjalistów w dziedzinie zapór sieciowych i systemów biznesowych, obecnie obsługuje ponad 215 klientów na całym świecie, włączając w to wiodących dostawców usług finansowych i telekomunikacyjnych, firmy transportowe, koncerny energetyczne i farmaceutyczne. Więcej informacji dostępnych jest na stronie www.tufin.com.

Autoryzowanym dystrybutorem w Polsce produktów Juniper Networks i Tufin Technologies jest firma Clico Sp. z o.o.



CLICO Sp. z o.o.
Budynek CC Oleandry
30-063 Kraków, ul. Oleandry 2
tel. 012 378-37-00
tel. 012 632-51-66
tel. 012 292-75-22 ... 24
fax 012 632-36-98
e-mail: sales@clico.pl
www.clico.pl

CLICO Oddział Katowice
40-568 Katowice, ul. Ligocka 103
tel. 032 444-65-11
tel. 032 203-92-35
tel. 32 609-80-50...51
fax 032 203-97-93
e-mail: katowice@clico.pl

CLICO Oddział Warszawa
Budynek Centrum Milenium
03-738 Warszawa, ul. Kijowska 1
tel. 022 201-06-88
tel. 022 518-02-70...75
fax 022 518-02-73
e-mail: warszawa@clico.pl

© 2009 CLICO Sp. z o.o. (polska wersja językowa). CLICO i CLICO logo są zarejestrowanymi znakami towarowymi CLICO Sp. z o.o.