Audyt i zarządzanie zmianami – zapobieganie niedostępności usług systemu informatycznego

Zarządzanie zmianami w systemach informatycznych w sposób zaplanowany i kontrolowany jest kluczowe dla zapewnienia dostępności usług oraz przeciwdziałania incydentom bezpieczeństwa. Jest to możliwe poprzez stosowanie odpowiednich procedur i narzędzi.

Dowiesz się:
- Co jest najczęstrzą przyczyną niedostępności usług systemu informatycznego
- Czym jest organizacja procesu zmian
- Jakie są najlepsze narzędzia wspomagające proces zarządzania zmianami

Powinieneś wiedzieć:
- Zmiany konfiguracji zabezpieczeń sieci często dokonywane są każdego dnia
- Narzędzia Secure Track mogą zostać wykorzystane np. do utrzymania aktualnej bazy inwentaryzacyjnej
- Jaki najczęstrzy problem mają administratorzy

Anna Grzesiakowska, Wojciech Goclon.
Konsultanci, audytorzy z firmy ESECURE Sp. z o. o., wyspecjalizowanej w usługach z obszaru bezpieczeństwa informacji i systemów informatycznych.
Kontakt: sales@esecure.pl, www.esecure.pl.

Najczęstszą przyczyną niedostępności usług systemu informatycznego są przeciążenia, awarie oraz błędy ludzi występujące w trakcie wprowadzania zmian (m.in. w sieci, aplikacjach, konfiguracji). Uniezależnienie się od sytuacji wystąpienia przeciążeń i awarii odbywa się zwykle poprzez stosowanie odpowiednio wydajnych urządzeń i systemów oraz tworzenie konfiguracji redundancyjnych, gdzie kluczowe komponenty systemu informatycznego (m.in. serwery, urządzenia sieci i zabezpieczeń) są złożone z wielu elementów tak, aby w razie awarii jednego z nich, inny sprawny element przejął jego zadania. W praktyce trudniejszym zadaniem jest właściwe wprowadzanie zmian w systemie informatycznym tak, aby zminimalizować liczbę błędów w tym procesie. Jest to możliwe przez opracowanie i wdrożenie w firmie odpowiednich procedur oraz zastosowanie specjalistycznych narzędzi wspomagających realizację tych procedur.

Organizacja procesu zarządzania zmian

Zmiany w systemie informatycznym podyktowane są wieloma, często ważnymi dla firmy względami, np. wprowadzenie nowych usług systemu informatycznego, podniesienie jakości i funkcjonalności istniejących usług, zapewnienie lub zablokowanie dostępności usług dla określonych użytkowników, podwyższenie bezpieczeństwa systemu informatycznego, itp. W wielu przypadkach firma nie może pozwolić sobie na zrezygnowanie ze zmian, ponieważ ucierpieli by na tym jej pracownicy, klienci lub partnerzy handlowi, a w konsekwencji działalność biznesowa firmy. W celu zminimalizowania ryzyka negatywnego wpływu zmian na dostępność i jakość usług IT firma powinna być przygotowana na ich bezpieczne i kontrolowane wprowadzanie.

Zarządzanie zmianami w skali całego systemu informatycznego do złożony proces. Procedury, które ustalają w jaki sposób ten proces powinien się odbywać powinny określać wiele zagadnień, m.in.:
- klasyfikację zmian w systemie informatycznym (objętych określoną procedurą),
- ustalenia kto w firmie ma prawo zgłaszać i akceptować określone zmiany,
- zgłaszanie potrzeb wprowadzenia zmian, m.in.:
  - kto zgłosił zmianę,
  - opis zmiany,
  - jaki jest cel zmiany,
  - ważność zmiany (wg zgłaszającego),

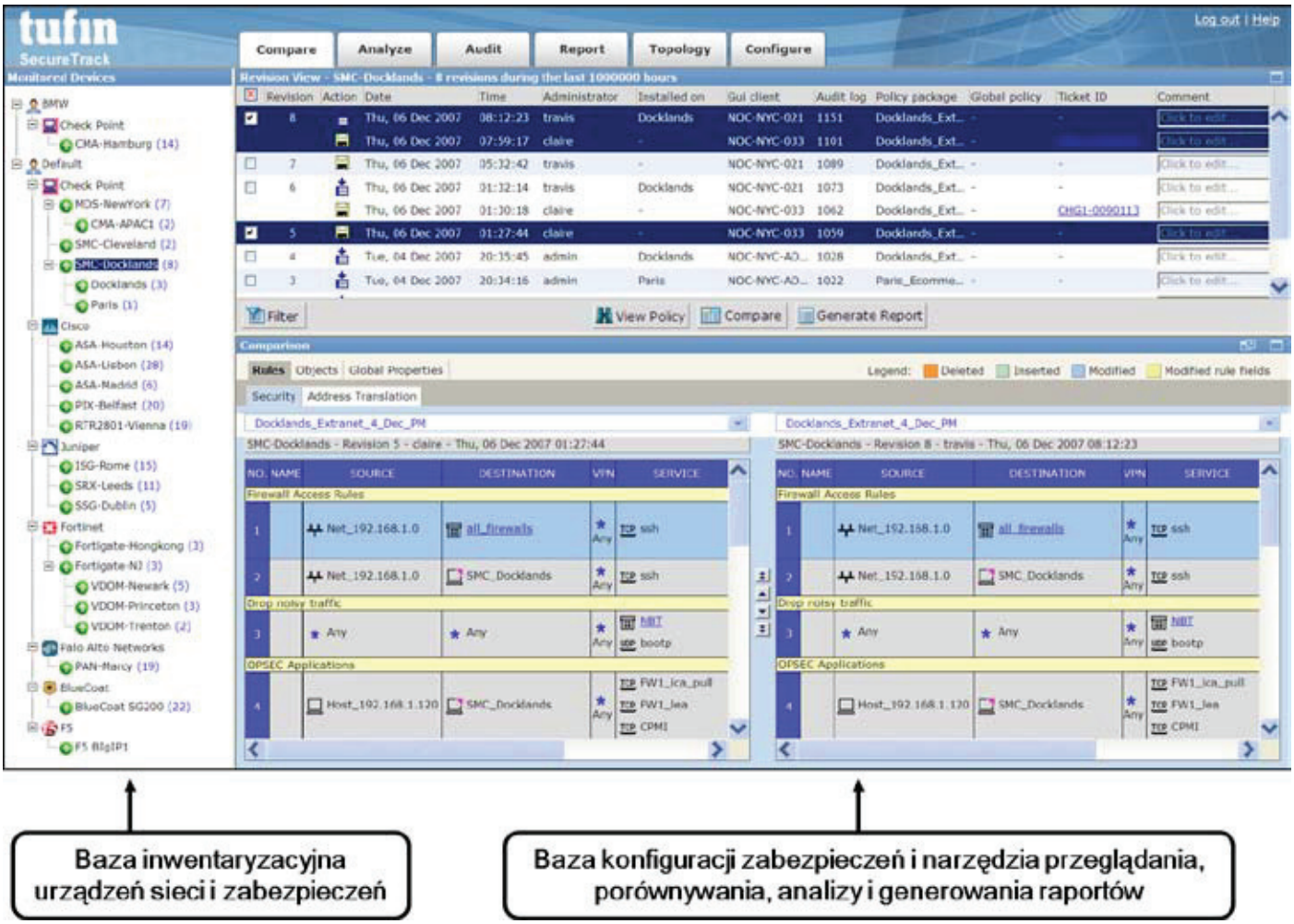
  - na jaki czas zmiana powinna być wprowadzona,
- ocena i akceptacja zmian, m.in.:
  - kto zweryfikował zmianę,
  - jakie są korzyści wprowadzenia zmiany,
  - jakie ryzyko niesie ze sobą wprowadzenie zmiany,
  - środki wymagane na wprowadzenie zmiany,
  - oszacowanie kosztów i czasu wymaganego na wprowadzenie zmiany,
  - priorytet zmiany,
  - wpływ zmiany na inne elementy systemu informatycznego,
  - kto zaakceptował zmianę,
  - kto powinien zaplanować wprowadzenie zmiany),
- planowanie zmian, m.in.:
  - w jaki sposób należy wprowadzić i przetestować zmianę,
  - kto powinien wprowadzić i przetestować zmianę,
  - jak usunąć zmianę,
  - dodatkowo dla systemów informatycznych działających w lokalizacji podstawowej i zapasowej zapewnienie, aby w razie problemów w lokalizacji podstawowej była możliwość przełączenia na lokalizację zapasową,
  - przekazywanie zaakceptowanych zmian do realizacji i ich rozliczanie,
  - rejestrowanie i audytowania zmian dokonywanych w systemie informatycznym.

Zmiany mogą dotyczyć praktycznie każdego obszaru systemu informatycznego i mieć różny charakter (np. dodanie nowego lub usunięcie elementu, zmiana konfiguracji istniejącego elementu, itp.). Proces zarządzania zmianami powinien zostać tak zorganizowany, aby wprowadzanie zmian odbywało się jak najmniejszym kosztem, przy minimalnym ryzyku zakłócenia usług IT oraz zapewnionej pełnej rozliczalności.

Firmy planujące organizację procesu zarządzania zmianami mogą skorzystać z dostępnych standardów zarządzania usług i bezpieczeństwa IT (m.in. ISO/IEC 20000 – ITIL, ISO/IEC 27001, PCI-DSS) oraz usług specjalizujących się w tej dziedzinie firm konsultingowych.

Narzędzia wspomagające proces zarządzania zmianami

Wprowadzenie zmian bez odpowiedniego planowania, testowania i rozliczania jest częstym powodem zakłó-



Rysunek 1. *Centralna baza urządzeń oraz konfiguracji zabezpieczeń sieciowych*

ceń i utraty dostępności usług systemu informatycznego oraz innych naruszeń bezpieczeństwa. Dzieję się tak głównie dlatego, że proces zarządzania zmianami wymaga poświęcenia przez wielu pracowników zbyt dużych nakładów pracy. Przede wszystkim duża ilość informacji nt. wprowadzanych zmian musi być na bieżąco rejestrowana. Po określonym czasie życia systemu informatycznego historia zarejestrowanych zmian zawiera tak wiele informacji, że wyszukanie określonych danych jest bardzo czasochłonne, przez co dalsze rejestrowanie zmian traci swoje uzasadnienie. Rozwiązanie tego problemu jest możliwe poprzez zastosowanie narzędzi, które wspomagają ludzi i automatyzują określone czynności. Na rynku dostępnych jest wiele narzędzi przeznaczonych do tego celu.

Zarządzanie zmianami jest szczególnie uciążliwe w odniesieniu do konfiguracji zabezpieczeń sieci. Sieci są obecnie podstawą funkcjonowania całego systemu informatycznego. Prawie wszystkie współczesne aplikacje działają w środowisku sieciowym i obejmują swoim zasięgiem sieci rozległe WAN i Internet. Błędna konfiguracja zabezpieczeń sieci może spowodować otwarcie możliwości nieupoważnionego dostępu do zasobów systemu informatycznego (np. włamania intruzów lub propagację złośliwych aplikacji), bądź zablokowania dostępu dla legalnych użytkowników i w konsekwencji straty finansowe (np. na skutek nie odbierania zamówień, przestojów w pracy), utratę reputacji firmy, konsekwencje prawne, itd.

W dalszej części artykułu zostaną omówione narzędzia służące do wspomagania procesu zarządzania zmianami konfiguracji zabezpieczeń sieci na przykładzie popularnej aplikacji Tufin SecureTrack™.

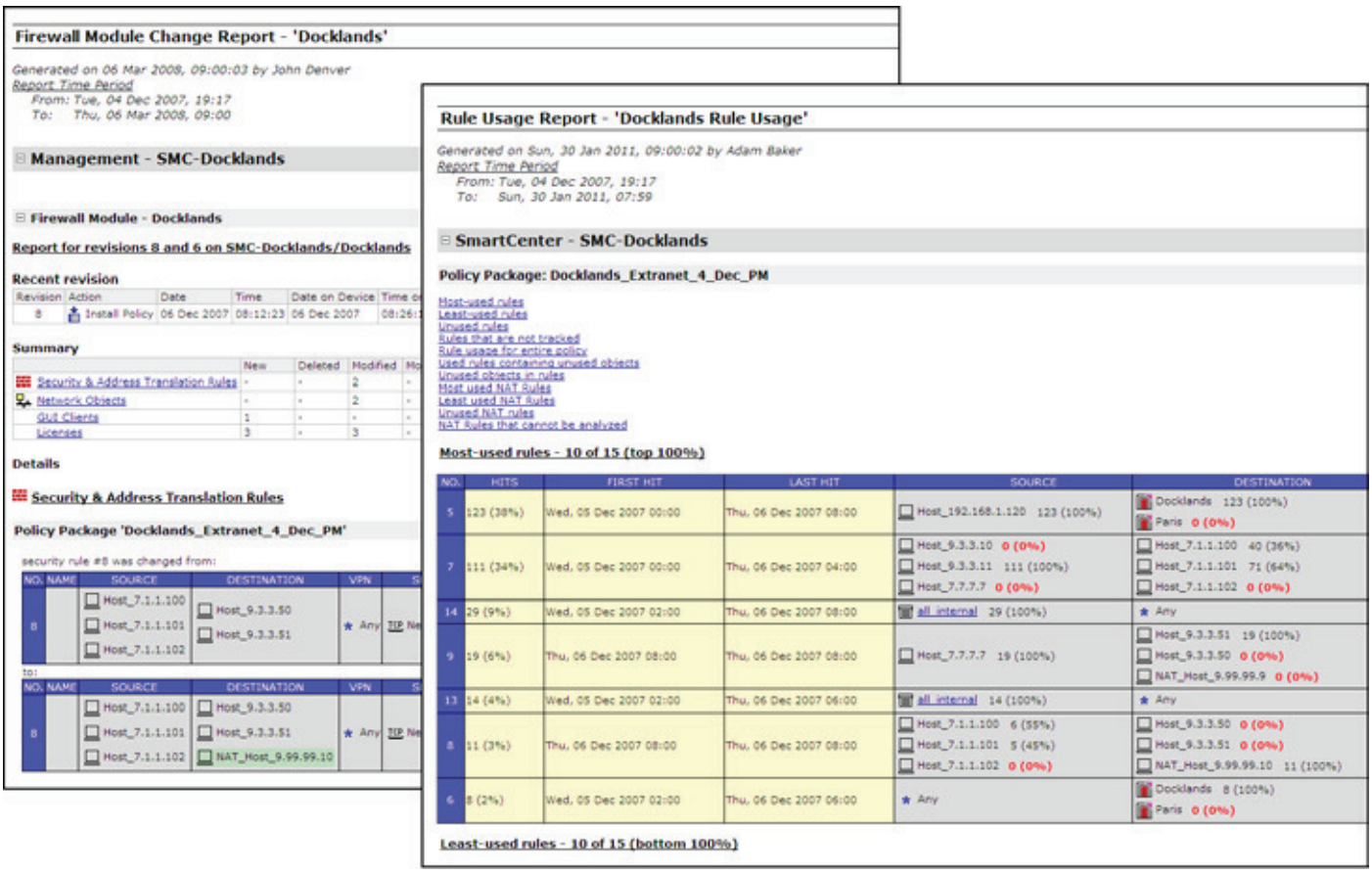
Audyt i zarządzanie zmianami konfiguracji zabezpieczeń sieci

Zmiany konfiguracji zabezpieczeń sieci często dokonywane są każdego dnia przez różnych administratorów. W trakcie eksploatacji zabezpieczeń (np. firewall) ich konfiguracja rozrasta się do dużych rozmiarów i w konsekwencji jej zrozumienie sprawia administratorom trudności. Także audytorzy zatrudnieni przez firmę do weryfikacji bezpieczeństwa systemu informatycznego nie potrafią dokonać oceny poprawności konfiguracji zabezpieczeń.

Popatrzmy w jakim zakresie specjalistyczne narzędzia mogą przydać się administratorom i audytorom. Narzędzia nie zastąpią ludzi, ale mogą znacznie usprawnić ich pracę, przez co zarządzanie zmianami nie będzie tak czasochłonne i będzie odbywało się w sposób należyty.

Dla przykładu, narzędzia SecureTrack mogą zostać wykorzystane w następującym zakresie:

- utrzymanie aktualnej bazy inwentaryzacyjnej urządzeń sieci i zabezpieczeń (m.in. firewall, ruter, przełącznik) – patrz przykład na rysunku 1,



Rysunek 2. *Raporty nt. zmian konfiguracji zabezpieczeń w określonym czasie*

- wizualizacja topologii sieci oraz raporty nt. zmian konfiguracji pomagają administratorom w ich zrozumieniu i analizie – patrz przykłady na rysunkach 2 i 3,
- automatyczne rejestrowanie zmian wprowadzanych przez administratorów do konfiguracji zabezpieczeń,
- szybkie wyszukiwanie zmian wprowadzonych w przeszłości i ich porównywanie do aktualnych konfiguracji,
- optymalizacja, porządkowanie i „uszczelnianie" konfiguracji zabezpieczeń,
- przeprowadzanie symulacji zmian i ocena ich ryzyka,
- ocena zgodności konfiguracji zabezpieczeń z dobrymi praktykami, standardami IT i polityką bezpieczeństwa firmy.

Omawiana w artykule aplikacja wspomagająca zarządzanie zmianami konfiguracji zabezpieczeń sieci jest wyposażona w bazę danych, gdzie zarejestrowane są wszystkie monitorowane urządzenia. Aplikacja na bieżąco monitoruje urządzenia i automatycznie rejestruje każdą wprowadzoną zmianę zabezpieczeń (w zakresie konfiguracji objętej monitorowaniem, np. polityki zabezpieczeń firewall). Dedykowane narzędzia w oparciu o informacje automatycznie zapisywane w bazie danych umożliwiają szybkie wyszukiwanie, analizę, rozliczanie i porównywanie różnych, także historycznych konfiguracji. Dodatkowo aplikacja wyposażona jest w liczne narzędzia uzupełniające, które mogą zostać wykorzystane np. w trakcie audytów bezpieczeństwa. Dla przykładu, dostępne są narzędzia umożliwiające analizę poprawności wprowadzanych zmian konfiguracji, m.in. zgodności konfiguracji ze specyficznymi wymaganiami bezpieczeństwa firmy.

Jednym z zadań realizowanych w ramach zarządzania zmianami jest optymalizacja i porządkowanie konfiguracji zabezpieczeń, a także jej „uszczelnianie". Odbywa się to poprzez wyszukiwanie i zmianę kolejności elementów konfiguracji (reguł polityki firewall), które są najczęściej i najrzadziej wykorzystywane do analizy ruchu sieciowego, a także elementów konfiguracji, które w ogóle nie są używane i można je usunąć. W tym celu aplikacja SecureTrack oprócz rejestrowania zmian konfiguracji odczytuje także zdarzenia (logi) zapisywane przez monitorowane urządzenia zabezpieczeń i na ich podstawie analizuje konfigurację.

W praktyce zabezpieczenia, które były eksploatowane przez dłuższy czas zawierają wiele zbędnych elementów (np. reguł polityki firewall, obiektów w regułach, itp.). Często dostęp do zasobów IT jest zezwalany na określony czas i administratorzy zapominają, aby zablokować dostęp po upływie tego czasu. Usunięcie zbędnych reguł i obiektów polityki firewall powoduje, że system zabezpieczeń jest bardziej szczelny i wydajny. Zredukowana konfiguracja jest także bardziej zrozumiała dla administratorów.

Narzędzia zarządzania zmianami zabezpieczeń sieci rozwijają się w kierunku wspomagania coraz większej liczby czynności, które sprawiają administratorom problemy. Dla przykładu, problem z jakim borykają się administratorzy zabezpieczeń w sieciach gdzie działa wiele aplikacji to ustalenie szczelnej konfiguracji (np. reguł polityki firewall zapewniających kontrolę dostępu do aplikacji). Admi-

Rysunek 3. *Wizualizacja topologii sieci pomaga administratorom w analizie zmian*

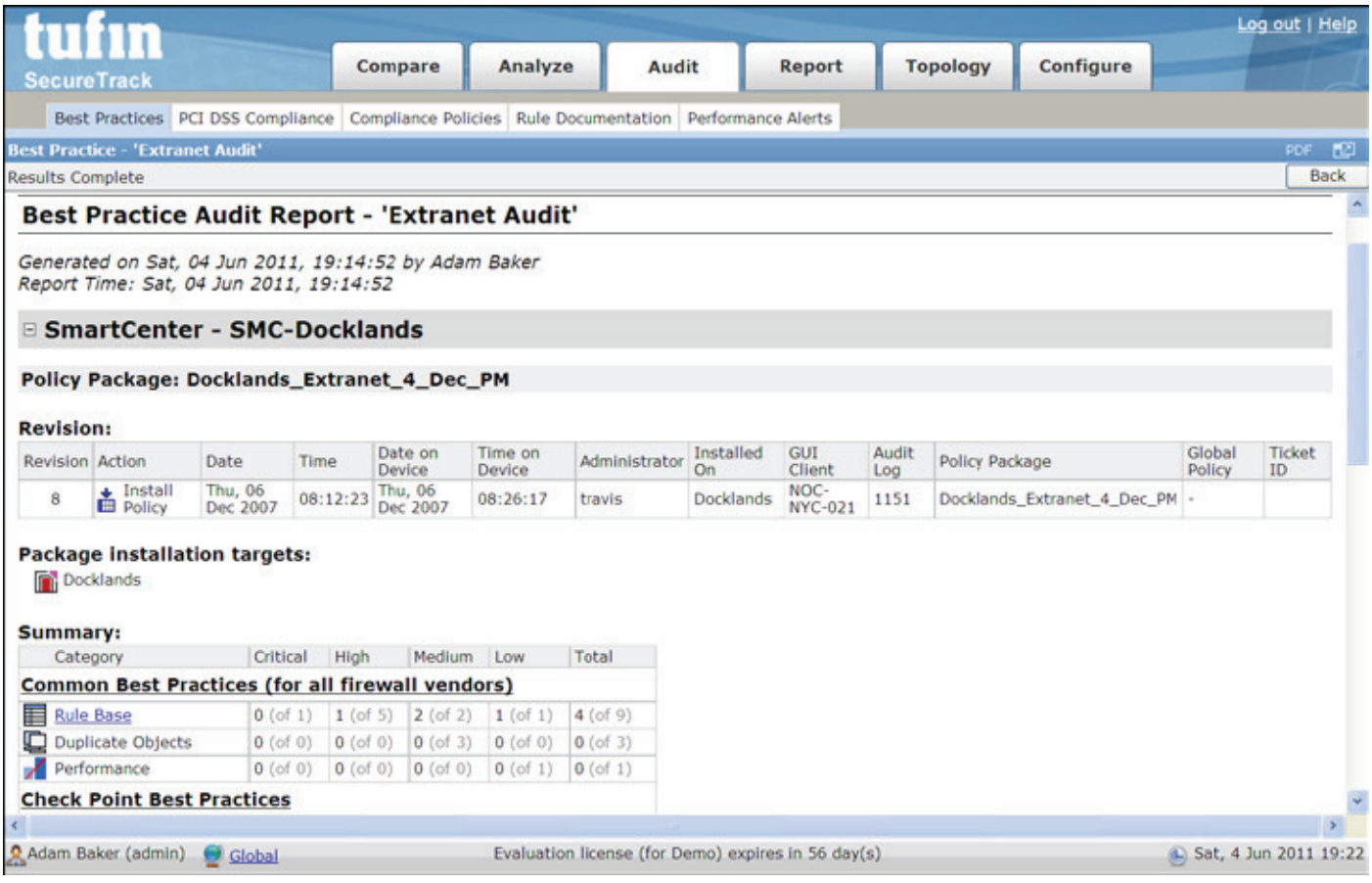
nistratorzy aplikacji często nie potrafią przekazać im dokładnych informacji, jakie adresy IP i protokoły sieciowe powinny zostać zezwolone do poprawnego działania aplikacji. Ustalenie tych informacji z analizy ruchu sieciowego jest czasochłonne i ryzykowane, ponieważ wprowadzenie zbyt restrykcyjnej kontroli spowoduje niedostępność aplikacji dla legalnych użytkowników. W takiej sytuacji administrator zabezpieczeń, który dysponuje odpowiednimi narzędziami może automatycznie wygenerować właściwą konfigurację zabezpieczeń.

Omawiana w artykule aplikacja wspomagająca zarządzanie zmianami zabezpieczeń sieci może zostać rozszerzona o dodatkowy moduł SecureChange Workflow™, który standaryzuje i automatyzuje czynności związane z przekazywaniem zgłoszeń o wprowadzenie zmian oraz ich planowaniem, weryfikacją i akceptacją. Umożliwia zdefiniowane zestawu działań specyficznych dla określonej firmy (np. otwieranie zgłoszenia, konstruowanie zmiany, akceptowanie zmiany, wprowadzanie zmiany). Poszczególne osoby uczestniczące w tym procesie (np. zgłaszający, konstruujący, akceptujący i implementujący) są automatycznie powiadamiane o czekającym na nich zadaniu. Każde zadanie ma przypisany termin realizacji. Wszystkie te czynności są automatycznie rejestrowane i nawet po dłuższym okresie czasu możliwe jest ustalenie jakie były powody wprowadzenia zmiany i kto jej dokonał.

Podsumowanie

Wprowadzanie zmian w systemie informatycznym bez odpowiedniego planowania i testowania jest częstym powodem zakłóceń i utraty dostępności usług IT oraz innych naruszeń bezpieczeństwa. Proces zarządzania zmianami powinien zostać tak zorganizowany, aby wprowadzanie zmian odbywało się jak najmniejszym kosztem, przy minimalnym ryzyku zakłócenia usług IT oraz zapewnionej pełnej rozliczalności. Jest to możliwe poprzez stosowanie odpowiednich procedur opartych na standardach i dobrych praktykach oraz użycie specjalistycznych narzędzi wspomagających realizację tych procedur.

Zarządzanie zmianami jest szczególnie istotne w odniesieniu do konfiguracji zabezpieczeń sieci. Sieci są obecnie podstawą funkcjonowania całego systemu informatycznego. Zmiany zabezpieczeń sieci dokonywane są zwykle każdego dnia na wielu urządzeniach, często przez różnych administratorów. Błędna konfiguracja zabezpieczeń sieci może spowodować otwarcie możliwości nieupoważnionego dostępu do zasobów systemu informatycznego (np. włamania intruzów lub propagację złośliwych aplikacji), bądź zablokowania dostępu dla legalnych użytkowników i w konsekwencji straty finansowe, utratę reputacji firmy, konsekwencje prawne, itd. Na rynku dostępne są narzędzia usprawniające ten proces. Narzędzia nie zastąpią ludzi, ale mogą znacznie usprawnić ich pracę, przez co zarządzanie zmianami nie będzie czasochłonne i będzie odbywało się w sposób należyty.



Rysunek 4. *Audytowanie zmian konfiguracji pod kątem zgodności z dobrymi praktykami, standardami i polityką bezpieczeństwa firmy*