FIREMON SECURITY MANAGER

Kompleksowe zarządzanie ryzykiem i politykami bezpieczeństwa na firewallach i urządzeniach sieciowych

1.1. O producencie

FireMon dostarcza rozwiązania do zarządzania bezpieczeństwem, które umożliwiają organizacjom proaktywne działanie w obszarze monitorowanie zdarzeń w sieci i odpowiadanie reagowanie. Koncentrując się na zapewnieniu zaawansowanej widoczności, pomiarów, oceny i usprawnień procesów bezpieczeństwa, produkty FireMon pomagają wykrywać obszary podatności, słabe punkty oraz pomagają znaleźć właściwe rozwiązania w zakresie poprawy poziomu ochrony sieci przed próbami kompromitacji systemów bezpieczeństwa.

Rok założenia: 2004. Podmioty zależne: Lumeta Corporation, Immediate Insight, Inc., FortyCloud, Saperix Technologies LLC

2. Monitorowanie i zarządzanie regułami na firewallach i urządzeniach sieciowych

W heterogenicznej sieci zarządzanej przez kompetencyjne zespoły (sieciowy, bezpieczeństwa, aplikacyjny, bazodanowy, etc.) bardzo ważnym elementem jest utrzymanie spójności polityk bezpieczeństwa na kontrolowanych urządzeniach brzegowych, ale też i sieciowych lub szkieletowych, w szczególności przy dużej różnorodności producentów systemów zabezpieczeń.

Rozwiązanie Firemon Security Manager służy pomocą wszędzie tam, gdzie istnieje potrzeba optymalizacji reguł ze względu na wydajność urządzeń lub szczelność polityk, zawsze gdy pozostawiamy otwarte porty lub trasy aplikacyjne do usuniętych systemów testowych, w przypadkach konieczności weryfikacji zgodności tworzonych reguł z polityką bezpieczeństwa (tzw. compliance) albo wtedy, gdy chcemy ocenić wpływ zagrożeń wynikających ze skanów bezpieczeństwa na propagację zagrożeń w naszej sieci czyli zbadać szczelność.

Obszar zastosowania Firemon Security Manager to m.in. analiza spójności reguł i zarządzanie warstwą bezpieczeństwa firewalli i systemów sieciowych. Rozwiązanie służy do zarządzania zmianami polityk bezpieczeństwa w obrębie urządzeń typu firewall, load balancer,, router (ACL), itp.

Platforma **FireMon Security Manager** zapewnia ciągłą widoczność w czasie rzeczywistym i optymalizację warstwy zabezpieczeń całej sieci, a w szczególności obszarów dotyczących wykorzystania reguł, stanu ryzyka w sieci, skuteczności stosowanych polityk, etc.

FireMon Security Manager oferuje m.in.:

- optymalizację zabezpieczeń sieci na urządzeniach sieciowych
- analizę ochrony sieci przedsiębiorstw
- automatyzację poprawności konfiguracji i zgodności reguł
- polityke zarządzania zmianami
- analizę ryzyka (vulnerability management)

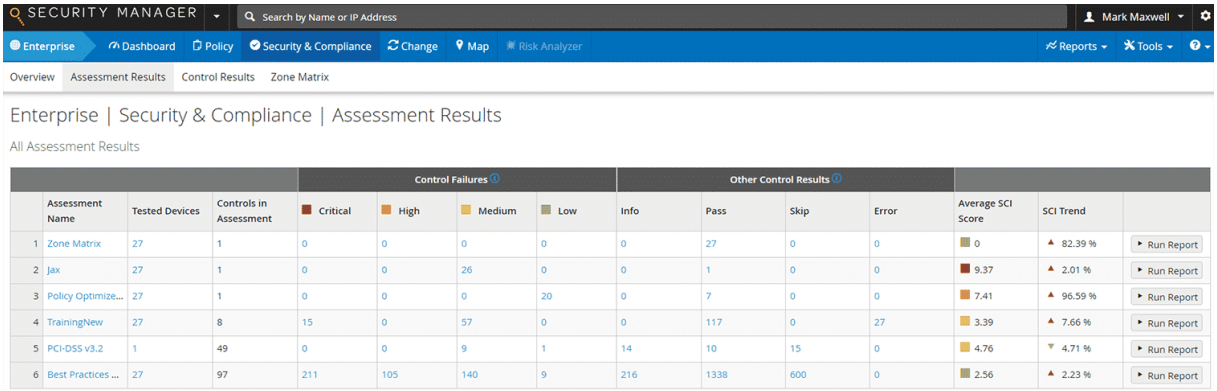
Platforma FireMon składa się z kilku modułów funkcjonalnych:

- Security Manager – System wspierający zarządzanie politykami bezpieczeństwa na urządzeniach bezpieczeństwa.
- Policy Planner – Moduł wspierający zarzadzania politykami bezpieczeństwa poprzez planowanie polityk na urządzenia bezpieczeństwa
- Policy Optimizer – Moduł wspierający zarządzanie politykami bezpieczeństwa poprzez optymalizację polityk bezpieczeństwa na urządzeniach bezpieczeństwa (recertyfikacja polityk bezpieczeństwa)
- Risk Analyzer –Wsparcie analizy ryzyka związanej z infrastrukturą sieciową organizacji
- Immediate Insight - System umożliwiający analizę zdarzeń, posiadający funkcjonalność BigData, w celu wsparcia analityki śledczej i przyspieszenia procesu reakcji na incydenty..
- Global Policy Controller (GPC) - zapewnia połączenie potrzeb biznesowych w kontekście zasobów sieciowych i zapewnia automatyzację alokacji polityk bezpieczeństwa niezbędnych do prawidłowego dostępu za pomocą istniejącej infrastruktury

2.1. Moduł Zarządzania bezpieczeństwem (Security Manager)

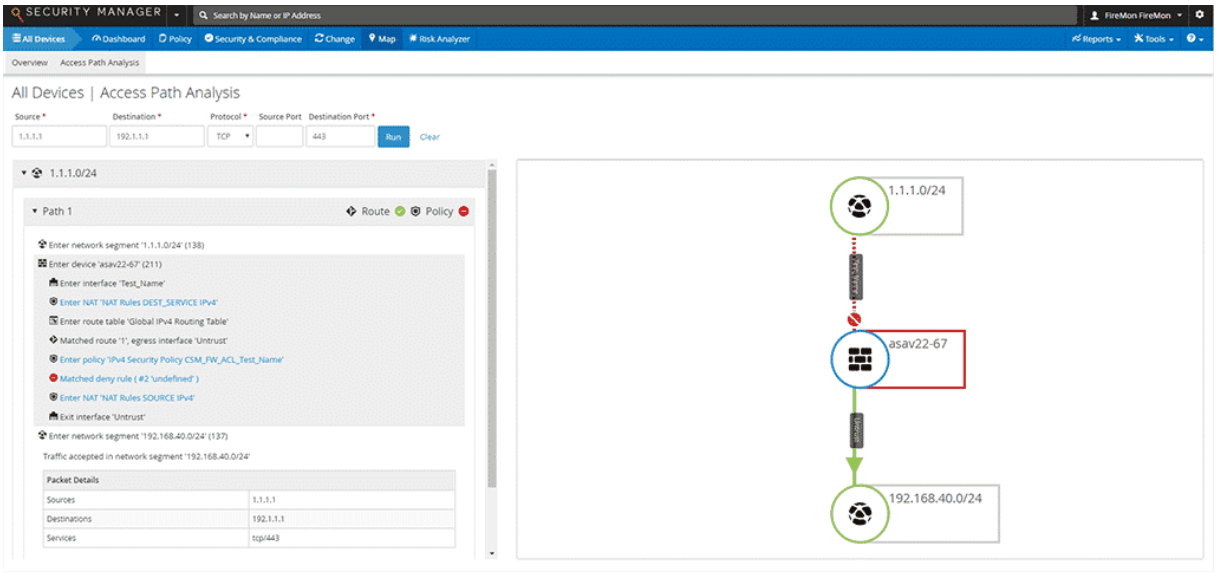
2.1.1. Zapewnienie zgodności

Security Manager zapewnia zautomatyzowane funkcje oceny zgodności, które pomagają w weryfikacji wymagań konfiguracyjnych i ostrzegają o naruszeniach polityk bezpieczeństwa w organizacji. Niezależnie od tego, czy potrzebne są raporty z kontroli gotowych lub dostosowanych do Twoich unikalnych wymagań raportów, Security Manager skraca czas spędzany na konfigurowaniu reguł konfiguracyjnych i daje pewność, że spełniają one wymagania dotyczące kontroli zgodności z podstawowymi zasadami bezpieczeństwa i wewnętrznymi regulacjami.



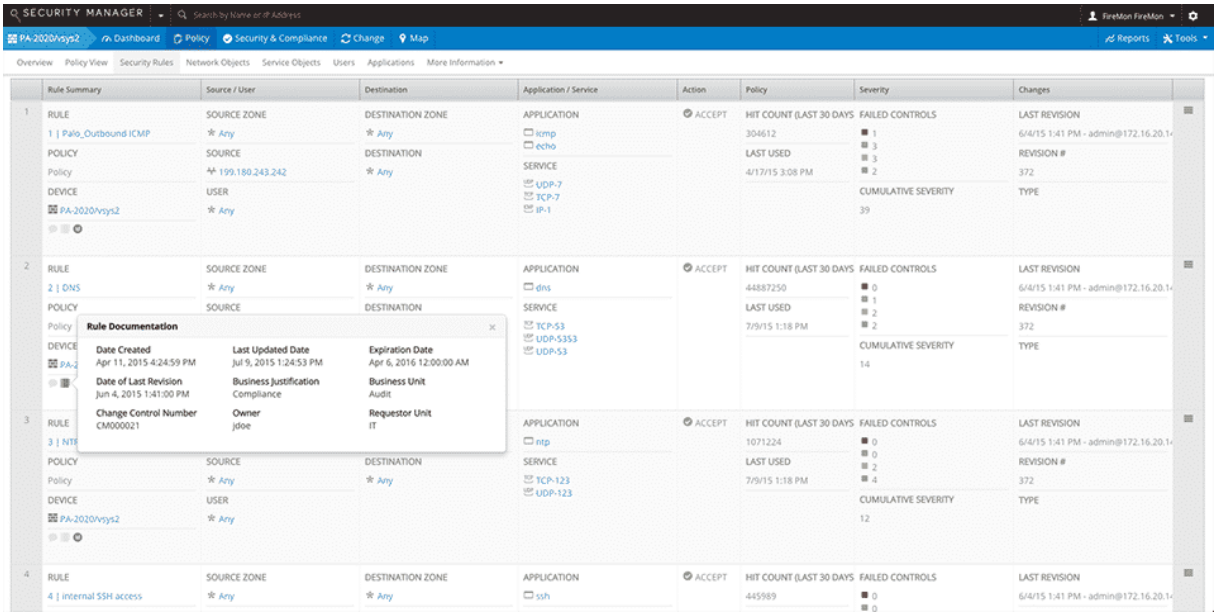
2.1.2. Optymalizacja zarządzania lukami w zabezpieczeniach

Dzięki analizie przepływu ruchu w czasie rzeczywistym Security Manager śledzi zachowanie w sieci, określając które aplikacje są używane w regule oraz między źródłami i punktami docelowymi. Można również skorelować skany podatności z wynikami analizy ścieżek dostępu Security Manager, aby śledzić każdą dostępną ścieżkę wycieku danych, aby skutecznie zmniejszyć potencjalną powierzchnię ataku i błyskawicznie wdrożyć określoną procedurą działań naprawczych.



2.1.3. Automatyzacja i orkiestracja procesów bezpieczeństwa

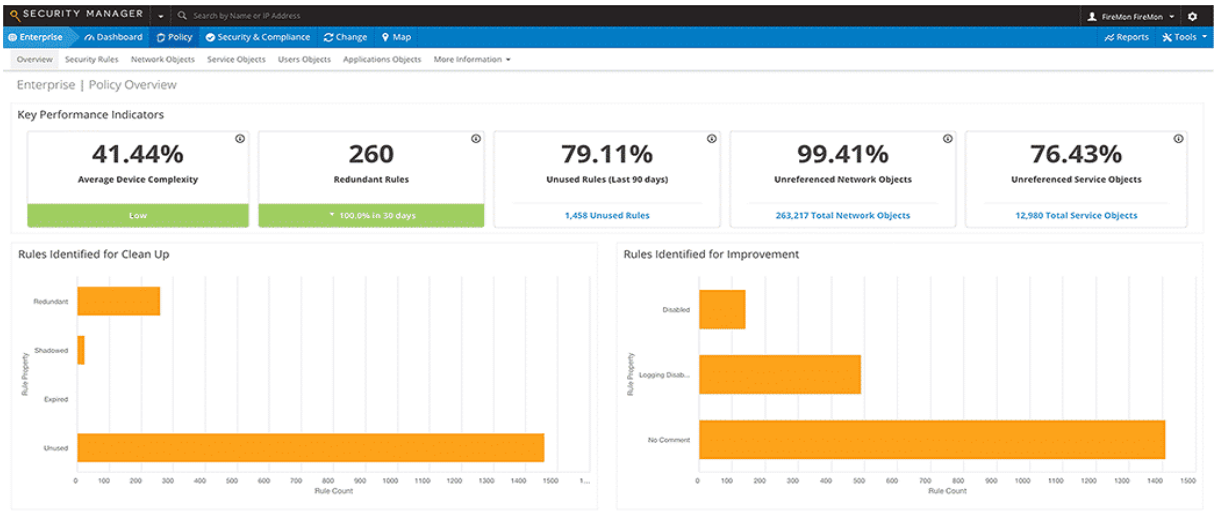
Dzięki modułowi Security Manager można łatwo tworzyć, utrzymywać i rozpowszechniać zasady bezpieczeństwa w wysoce dynamicznych środowiskach sieciowych, a także monitorować zakres wpływu proponowanych zmian polityki na zgodność z regułami bezpieczeństwa. Analiza zmian w czasie rzeczywistym dokumentuje parametry „kto, co, kiedy i dlaczego" każdej zmiany oraz ustala punkty odniesienia dla znormalizowanych reguł urządzenia. Automatyzując i koordynując zarządzanie zmianami, Security Manager zapewnia możliwość działania w środowiskach chmurowych, wirtualnych i hybrydowych.



2.1.4. Minimalizacja ryzyka i złożoności reguł bezpieczeństwa

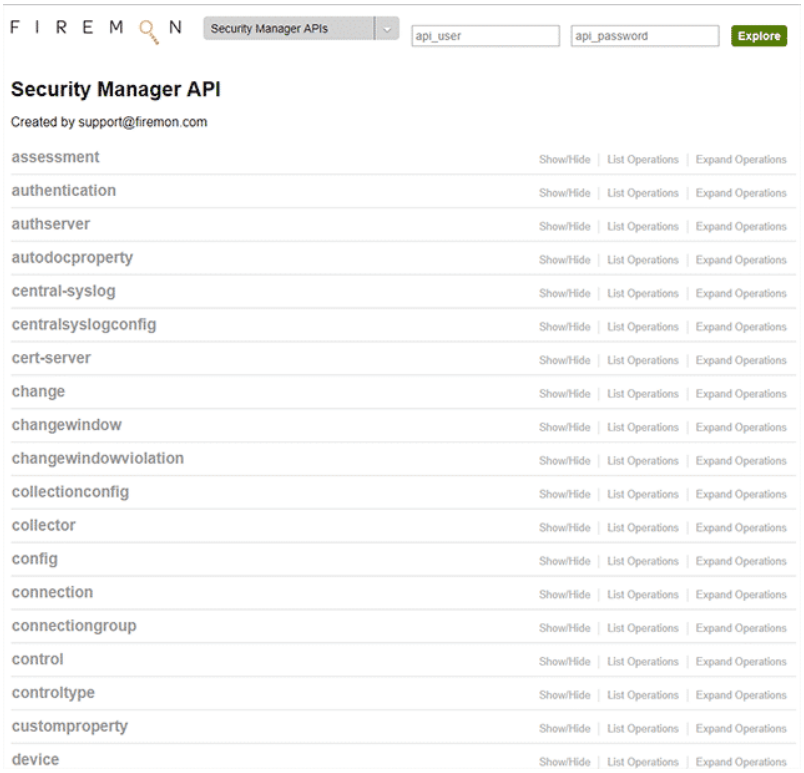
Security Manager pomaga utrzymać polityki bezpieczeństwa na urządzeniach zabezpieczających sieć, aby wyeliminować niepotrzebne/niepożądane ścieżki dostępu i ryzyko z nimi związane. Dzięki kompleksowej analizie reguł i zautomatyzowanym przepływom zadań (workflow) w celu weryfikacji reguł można usunąć błędy techniczne i konfiguracje, usunąć nieużywane polityki dostępu oraz

przejrzeć i udoskonalić używane reguły dostępu, aby zoptymalizować wydajność urządzeń, zmniejszyć złożoność polityk a także poprawić profil samych zabezpieczeń.



2.1.5. Skalowanie ewolucji infrastruktury sieciowej

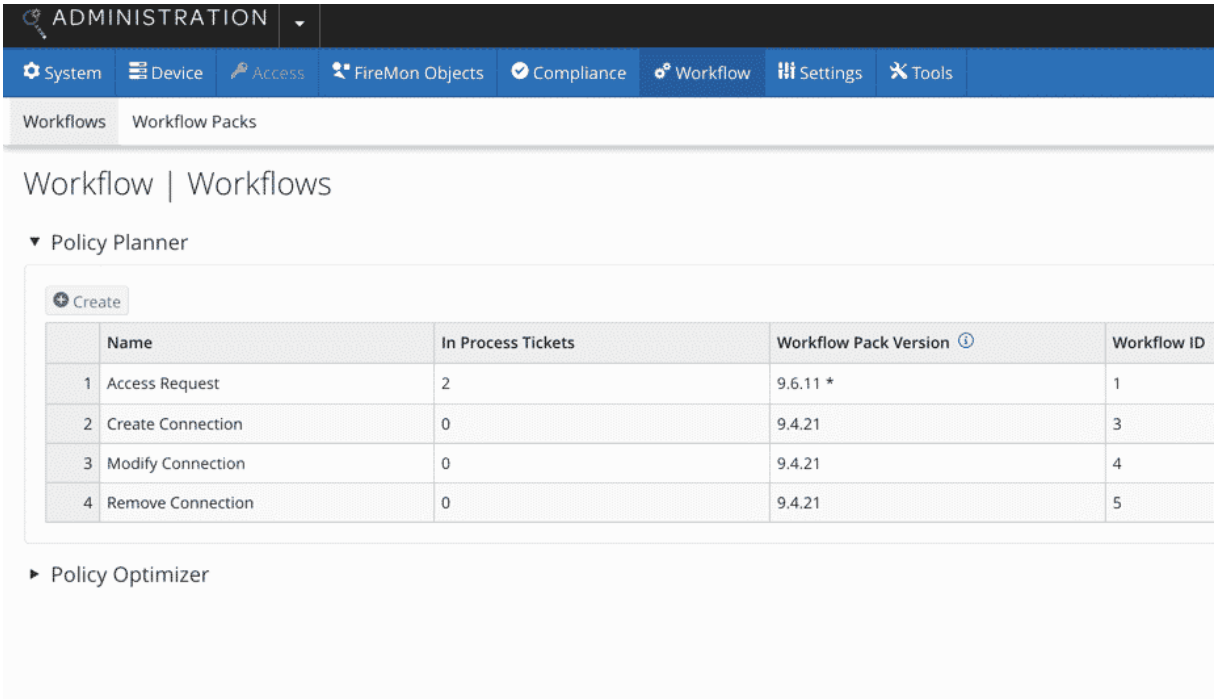
Security Manager zapewnia elastyczne skalowanie, funkcje dogłębnej analizy oraz możliwość integracji z innymi systemami zewnętrznymi, przez co umożliwia scentralizowaną widoczność i kontrolę sieci w czasie rzeczywistym. Można wykonywać jednoczesną analizę i normalizację na wielu platformach różnych producentów, rozdzielając funkcje raportowania na dedykowanym urządzeniu i zachowując dane w nieskończoność bez obniżania wydajności systemu. Elastyczny interfejs API pozwala na zintegrowanie informacji z rozwiązań innych firm w celu kompleksowej, scentralizowanej oceny i zarządzania bezpieczeństwem sieci.



2.2. Moduł dystrybucji zarządzania przepływami (Policy Planner)

2.2.1. Automatyzuj zarządzanie zmianami

Moduł Policy Planner zapewnia kompleksowe zarządzanie cyklem życia reguł, pomagając w automatyzacji każdego etapu procesu zarządzania zmianami. Przepływy pracy można dostosować i zautomatyzować tak, aby dostosować się do celów i standardów bezpieczeństwa, z narzędziami do dyspozycji w celu zarządzania ewolucją polityki i ochrony w miarę upływu czasu.



2.2.2. Ocena ryzyka w czasie rzeczywistym

Policy Planner pozwala na błyskawiczną ocenę ryzyka związanego z pojawiającymi się zleceniami na skonfigurowanie dostępu. Można wykryć, kiedy nowy dostęp spowoduje zagrożenie dla systemów w sieci, sprawdzić zakres proponowanych zmian przed ich wdrożeniem i usprawnić proces zatwierdzania wniosków o przydzielenie dostępu, które nie wpływają na zwiększenie poziomu ryzyka w organizacji. Policy Planner zapewnia taki poziom widoczności sieci, który jest niezbędny w celu zapobiegania wprowadzeniu potencjalnie problematycznych ustawień.

Change ID	Policy
Cisco ASA - 5506X	
RUL-81	Trust_access_in

Create the new rule

An orange token indicates a change input that cannot be resolved (matched) to an existing or newly created object.

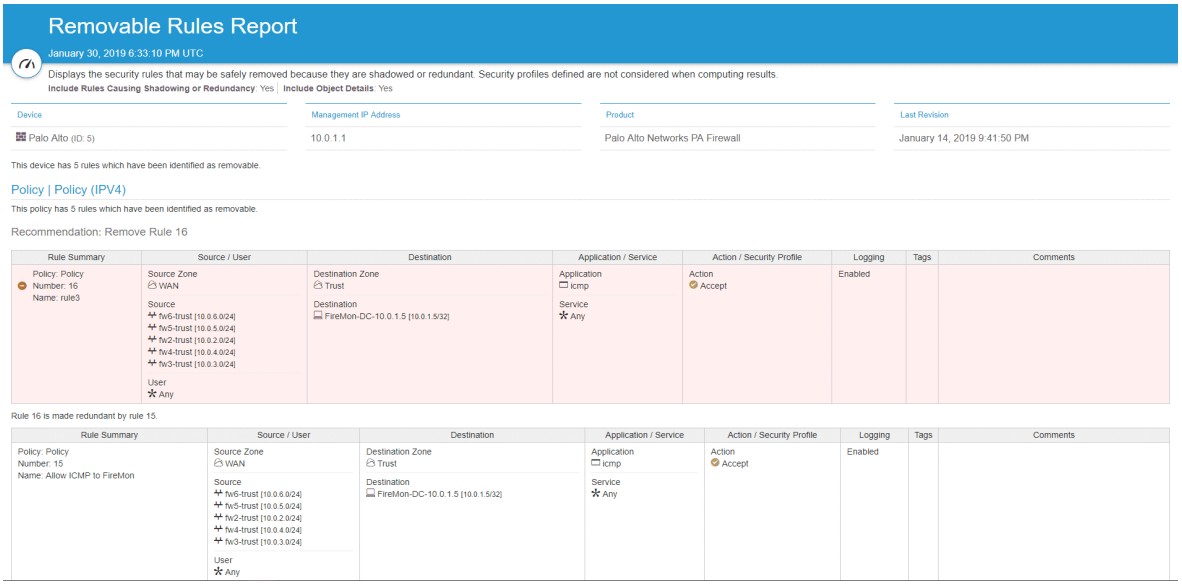
Rule Number	Source/User	
(empty)	Source	User
	DM_INLINE_NETWORK_146	*(empty)*
Rule Name	**Action**	**Log**
AutoTest	Accept	Enabled

Below this rule

Rule Number	Source/User	
9	Source	User
	FM_INLINE_SOURCES_21345	*(empty)*
Rule Name	**Action**	**Log**
line 26	Accept	Enabled

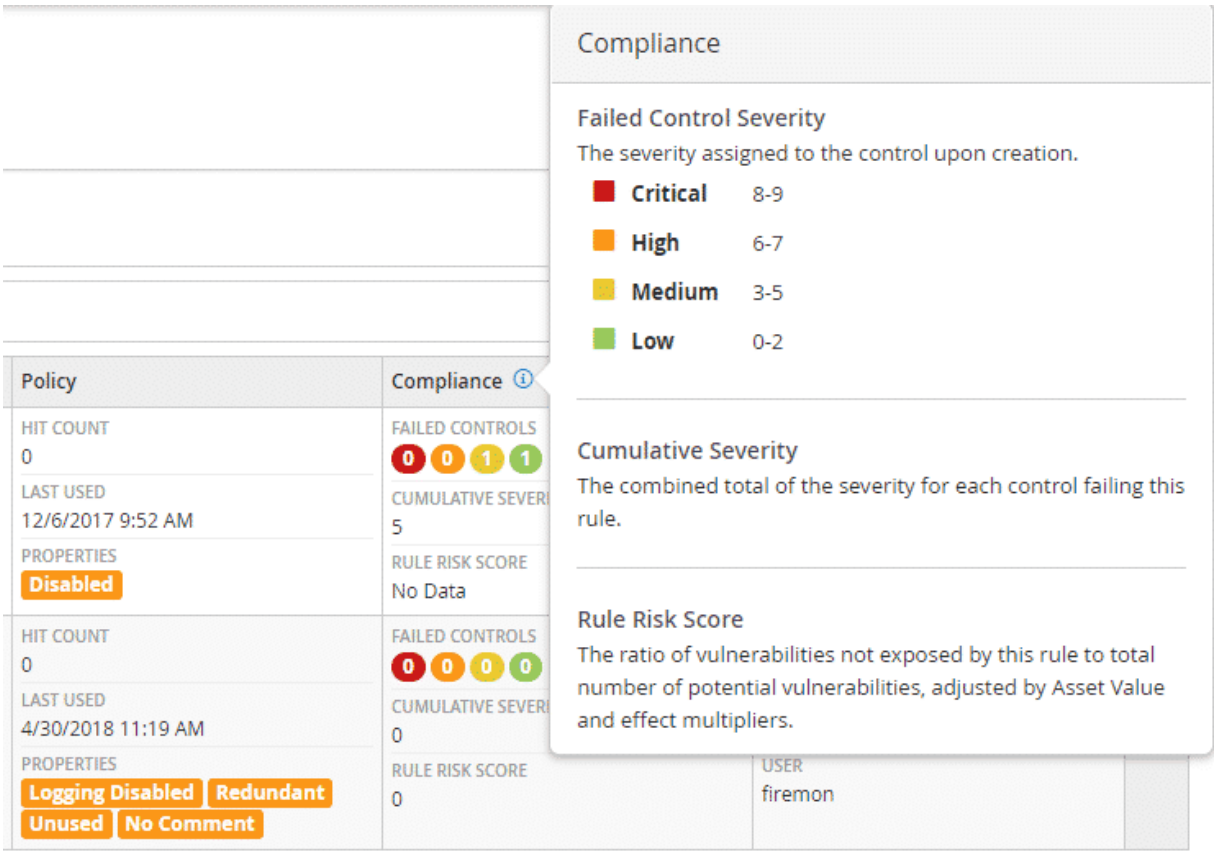
2.2.3. Analiza działania reguł bezpieczeństwa

Narzędzie Policy Planner analizuje bieżące zachowanie zestawów reguł i określa wszelkie niezbędne zmiany w czasie rzeczywistym. Policy Planner ma wgląd we wszelkie żądania, które powielają już uwzględniony dostęp, a także wszelkie reguły, które umożliwiają podobny dostęp do nowego żądania, zmniejszając złożoność i zwiększając wydajność działania urządzeń i sieci.



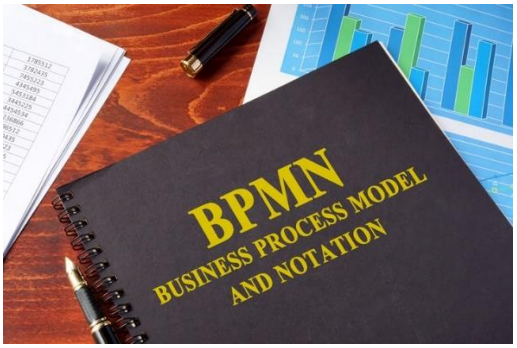
2.2.4. Zapewnienie zgodności i najlepsze praktyki

Program Policy Planner zapewnia, że nowo dodane reguły lub zmiany konfiguracji spełniają istniejące zasady zgodności i najlepsze praktyki już na etapie planowania reguł. Można skonfigurować różne kontrolki dla różnych grup urządzeń i przeglądać wyniki kontroli, aby zweryfikować zmiany reguł przed wdrożeniem i zapewnić pełną zgodność z wymaganiami.



2.2.5. Integracja procesów biznesowych

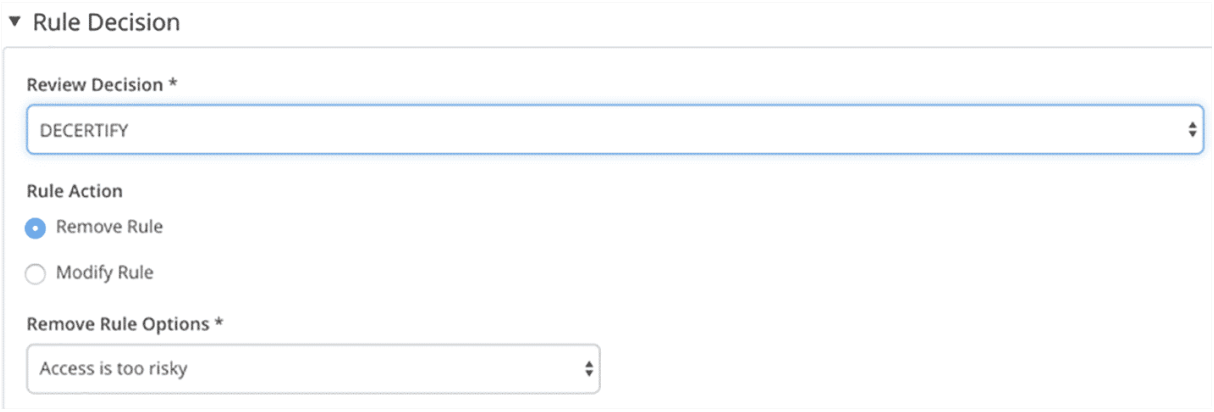
Policy Planner integruje się z istniejącymi rozwiązaniami do zarządzania procesami i dba o przestrzeganie najlepszych praktyk w zakresie procesów biznesowych i notacji (BPMN). Zespoły biznesowe i techniczne mogą wykorzystywać właściwe przepływy zadań (workflow), szablony i obieg dokumentów specyficzny dla swoich procesów, zwiększając wydajność pracy całej organizacji.



2.3. Moduł optymalizacji i zarządzania cyklem życia polityk bezpieczeństwa (Policy Optimizer)

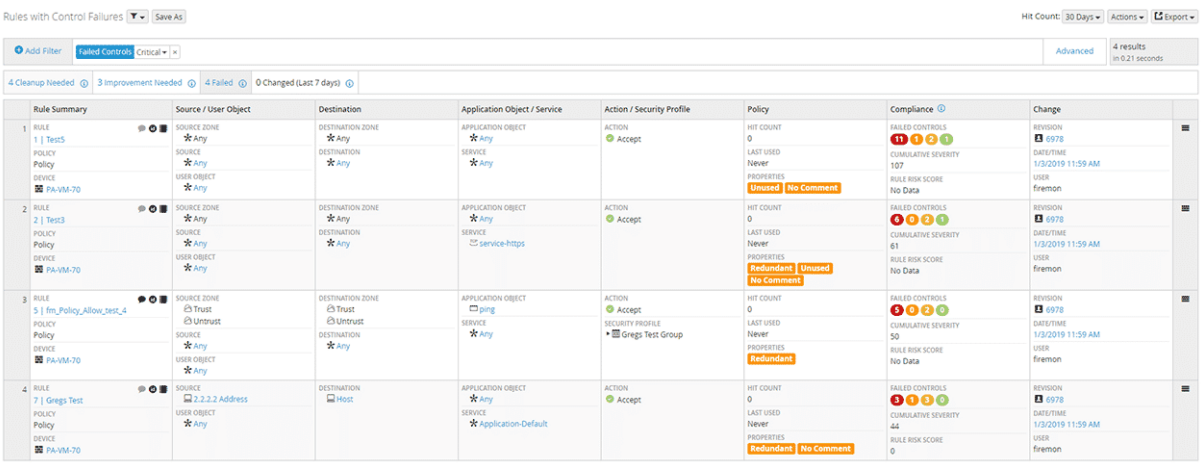
2.3.1. Automatyzacja procesów przeglądu reguł

Policy Optimizer automatyzuje proces przeglądu zmian w politykach bezpieczeństwa, aby pomóc w wykrywaniu nieaktualnych, niepotrzebnych lub nieudokumentowanych reguł. Można przypisać zadania przeglądu w oparciu o istniejące właściwości i dokumentację w ramach istniejących procesów akceptacji, które pasują do standardowych praktyk w celu ich dokumentowania, ponownej certyfikacji, likwidacji i raportowania każdej zmiany/decyzji co do polityki.



2.3.2. Przegląd reguł oparty na zdarzeniach

Narzędzie Policy Optimizer umożliwia automatyczne identyfikowanie reguł, które wymagają natychmiastowej analizy na podstawie rzeczywistych zdarzeń. Reguły sterowane zdarzeniami są analizowane na podstawie kryteriów, takich jak wygasanie w czasie, naruszenie zasad kontroli bezpieczeństwa, okresowe przeglądy lub zapytania typu ad-hoc w celu określenia odpowiednich środków naprawczych.



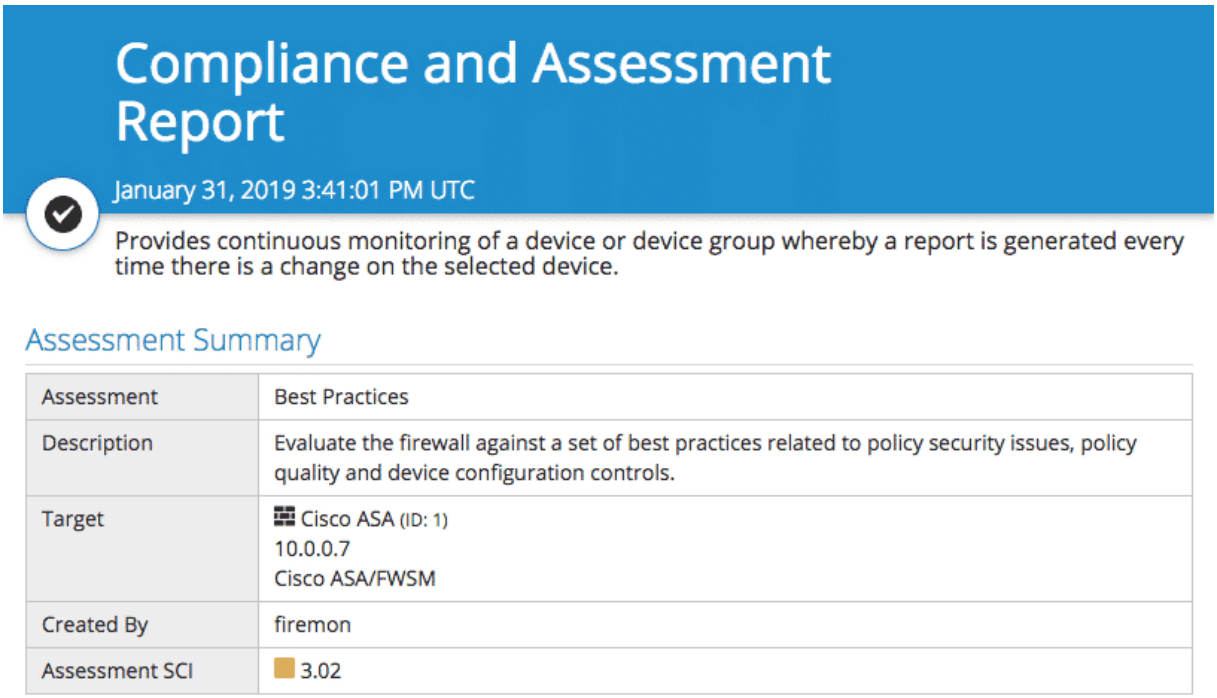
2.3.3. Dostosowanie procesów „workflow”

Policy Optimizer umożliwia dostosowanie wbudowanego modułu Workflow i integrację z istniejącymi zewnętrznymi systemami zarządzania procesami w organizacji (np. ServiceNow, BMC Remedy itp.).

Po zintegrowaniu z FireMon Policy Planner, Policy Optimizer może zostać rozszerzony tak, aby generować „tickety” na potrzeby zmian dla wymienianych reguł i przygotowywać zalecenia specyficzne dla każdej aplikacji.

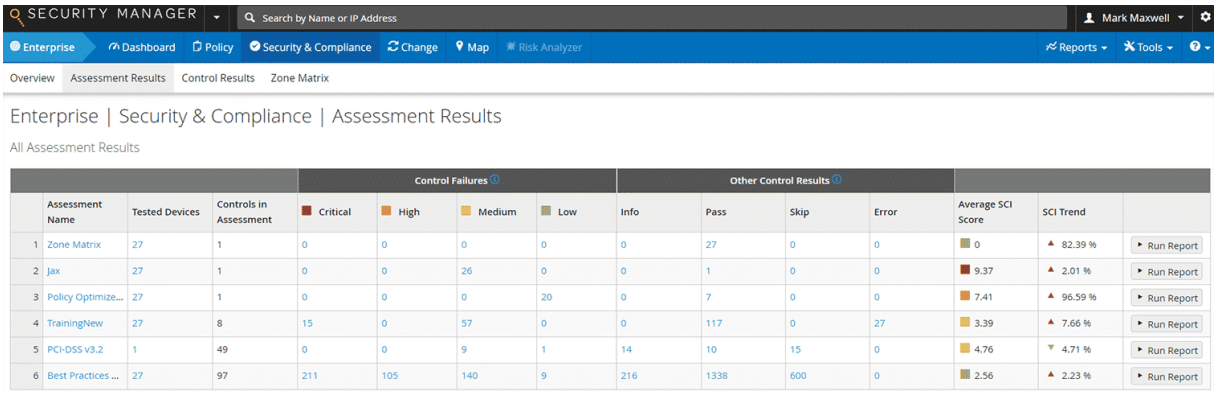
2.3.4. Poprawa wydajności i stosowanie najlepszych praktyk

Policy Optimizer pobiera szczegółowe informacje dotyczące każdej sprawdzanej reguły, z możliwością zatwierdzenia lub odrzucenia bieżących konfiguracji tych reguł. Pozwala to na ustalenie zasad współpracy z zespołami biznesowymi, aby usunąć niezgodne reguły, które mogą utrudniać działanie firewalli i powodować przerwy w świadczeniu usług. W ten sposób wspiera propagowanie najlepszych praktyk bezpieczeństwa.



2.3.5. Ciągłość zapewniania zgodności

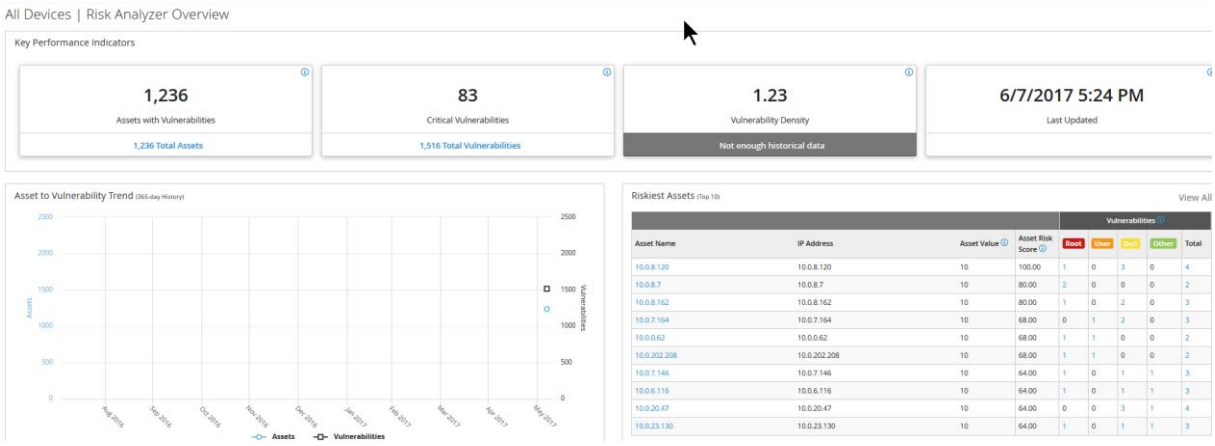
Policy Optimizer ułatwia zapewnienie wewnętrznej zgodności z zasadami bezpieczeństwa w organizacji, a także zewnętrznej zgodności ze standardami regulacyjnymi, w tym PCI DSS, NERC-CIP, HIPAA i SOX. Można tworzyć raporty zawierające szczegóły dotyczące przeglądu reguł dla audytorów, dostosowywać raporty do konkretnych wymagań i utrzymywać repozytorium dokumentacji zmian.



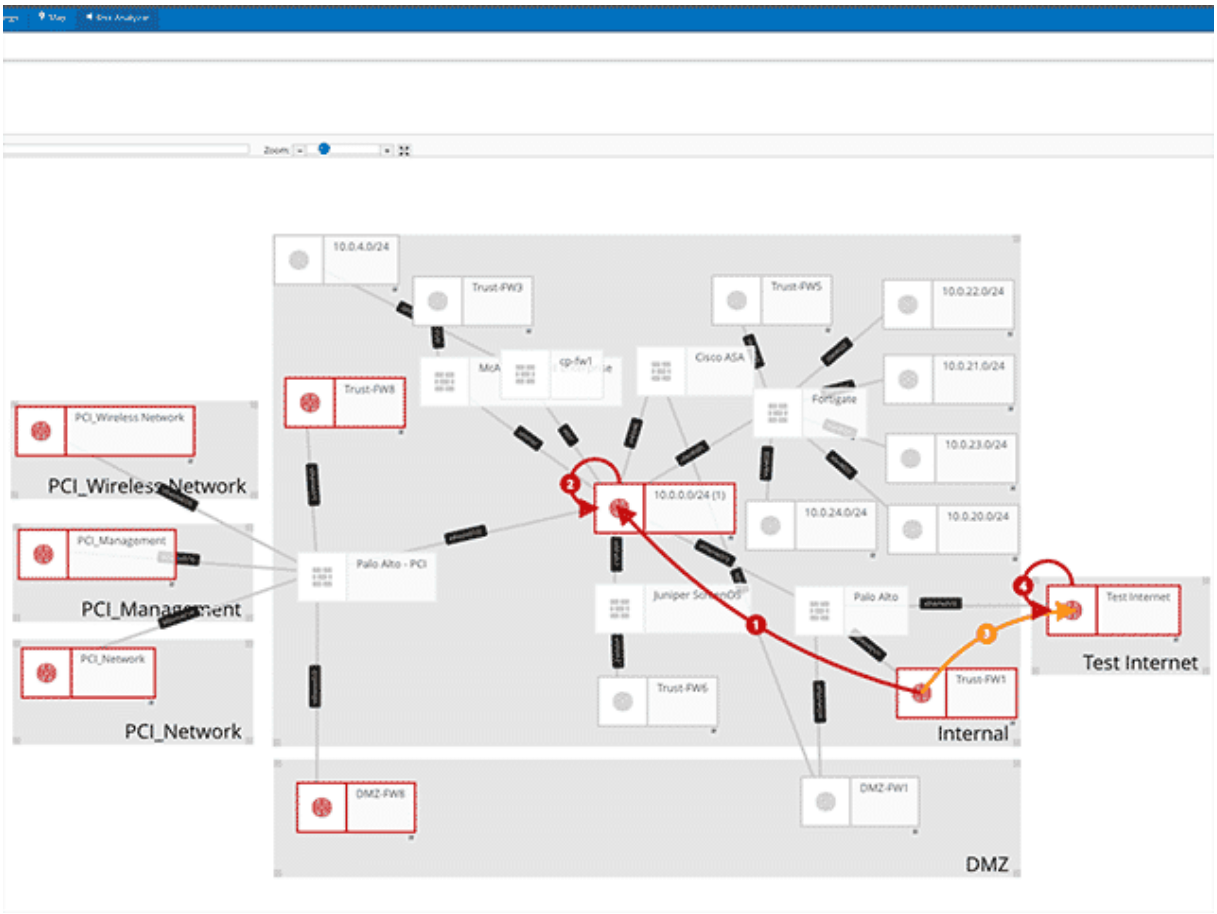
2.4. Analiza Ryzyka (Risk Analyzer)

Analizator ryzyka pomaga m.in.:

- Proaktywnie redukować ryzyko w oparciu o ekspozycję sieciową i dostępność hostów
- Uwzględnienie w analizie wyników skanowania podatności
- Ustalanie priorytetów luk w zabezpieczeniach
- Zrozumienie dalszych skutków zmian i określenie kroków zaradczych
- Symulację i ocenę ryzyka
- Śledzenie zmian w dostępie do sieci

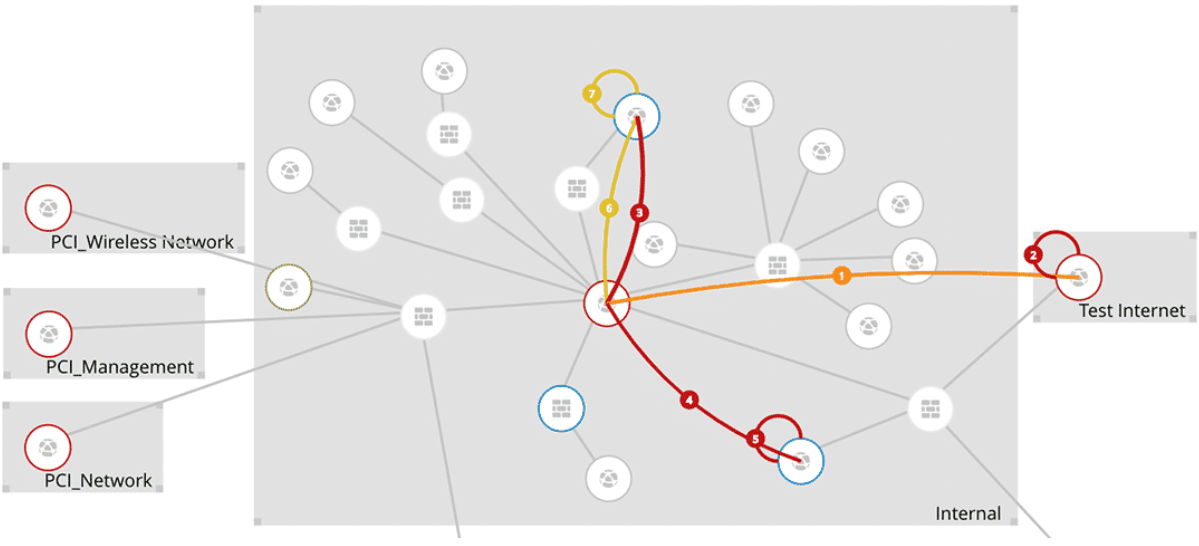


Risk Analyzer umożliwia wyświetlanie i zarządzanie poziomem ryzyka w sieci w czasie rzeczywistym. Gotowa do użytku w przedsiębiorstwach architektura Risk Analyzer obsługuje duże, złożone sieci hybrydowe z dziesiątkami tysięcy hostów i systemów bezpieczeństwa oraz może łatwo określić potencjalne ścieżki dostępu atakującego do sieci, jak też ocenić potencjalne zagrożenie i szkody.



2.4.1. Symulowanie potencjalnych ataków

Analizator ryzyka (Risk Analyzer) może śledzić możliwe ścieżki, które atakujący mogą wykorzystać, aby uzyskać dostęp do krytycznych zasobów w organizacji. Za pomocą Risk Analyzer można określić, gdzie można wykorzystać np. exploity w celu penetracji sieci. Korzystając z wizualizacji potencjalnych ścieżek ataku i wykresów ataków zero-day, można ocenić wpływ takich ataków i nadać priorytety poprawkom lub dostosować reguły urządzenia tak, aby przekonfigurować dostęp w celu szybkiego rozwiązania problemu.



2.4.2. Określenie ryzyka na skali punktowej

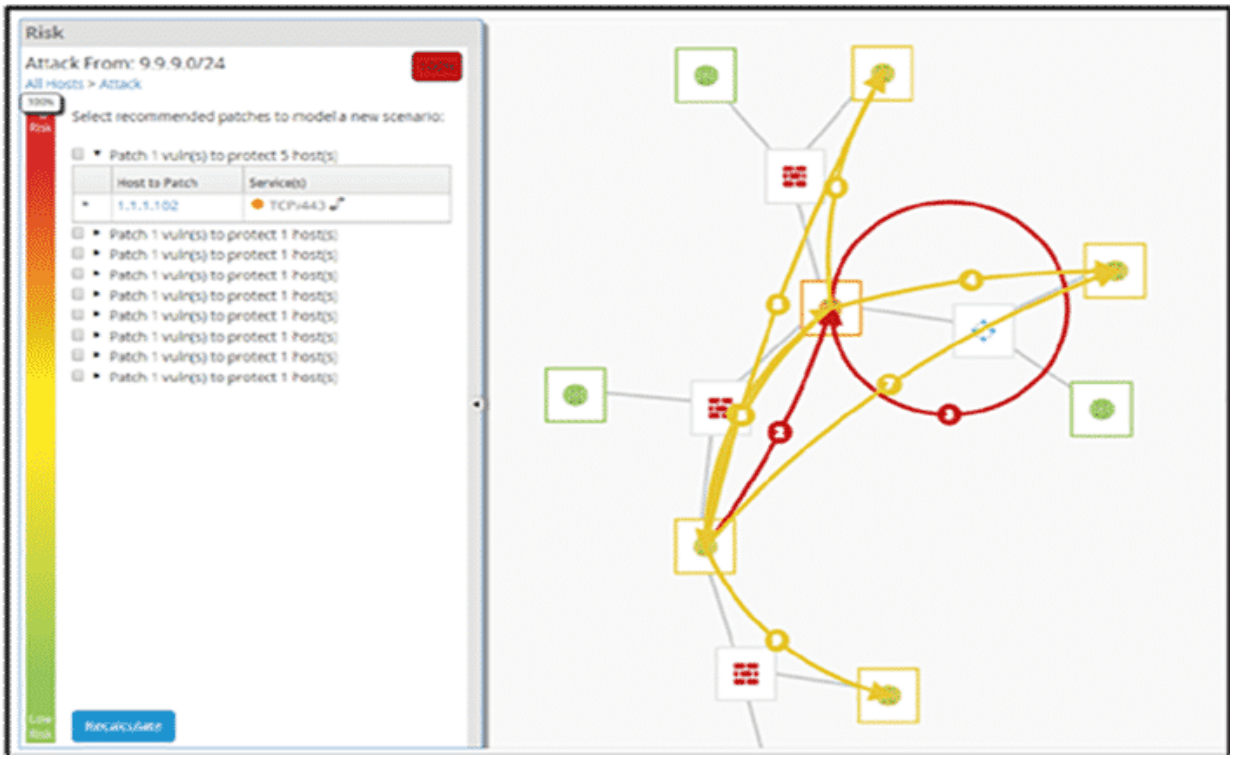
Risk Analyzer może oceniać wszystkie symulacje ataków pod kątem ryzyka i wpływu, a następnie ponownie określić poziom ryzyka po wprowadzeniu ulepszeń w celu określenia zmian wpływu. Można uzyskać pełną ocenę ryzyka sieciowego za pomocą pulpitu użytkownika, który zapewnia widoczność ryzyka w czasie rzeczywistym według reguły i zasobu.

Riskiest Assets (Top 10) View All

				Vulnerabilities				
Asset Name	IP Address	Asset Value	Asset Risk Score	Root	User	DoS	Other	Total
1.1.1.2	1.1.1.2	10	100.00	0	1	4	1	6
10.0.8.120	10.0.8.120	10	89.29	1	0	3	0	4
10.0.8.162	10.0.8.162	10	71.43	1	0	2	0	3
10.0.8.7	10.0.8.7	10	71.43	2	0	0	0	2
10.0.7.164	10.0.7.164	10	60.71	0	1	2	0	3
10.0.202.208	10.0.202.208	10	60.71	1	1	0	0	2
10.0.0.62	10.0.0.62	10	60.71	1	1	0	0	2
10.0.7.146	10.0.7.146	10	57.14	1	0	1	1	3
10.0.23.130	10.0.23.130	10	57.14	1	0	1	1	3
10.0.20.47	10.0.20.47	10	57.14	0	0	3	1	4

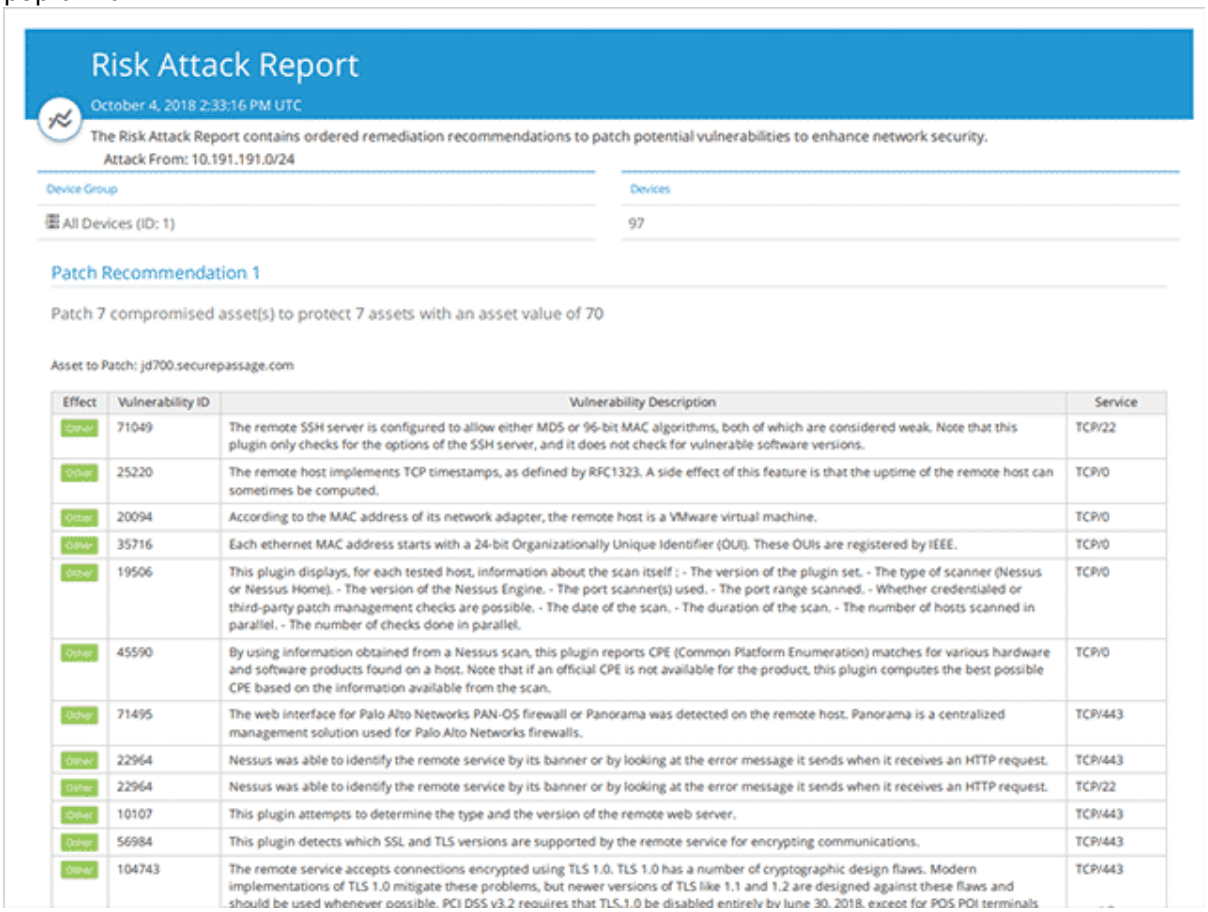
2.4.3. Analiza scenariuszy „Co jeśli?”

Risk Analyzer umożliwia wirtualne łatanie systemów i powtarzające się analizy ryzyka w celu porównania z innymi scenariuszami. Można również zdecydować, gdzie należy będzie niezbędne użycie wielu exploitów, aby dotrzeć do określonego zasobu.



2.4.4. Integracja ze skanerami podatności

Risk Analyzer integruje się z rozwiązaniami do zarządzania lukami w zabezpieczeniach (Qualys, Rapid7 i Tenable), aby zmierzyć ryzyko i zidentyfikować potencjalną formę penetracji i ataku na sieć. Zbierając i raportując konfiguracje w czasie rzeczywistym w zakresie dostępu do sieci, które jest wdrożone na urządzeniach zabezpieczających. Risk Analyzer dostarcza dokładne zalecenia dotyczące działań naprawczych, dzięki czemu można ustalić priorytety i zoptymalizować strategię zarządzania poprawkami.



Risk Attack Report

October 4, 2018 2:33:16 PM UTC

The Risk Attack Report contains ordered remediation recommendations to patch potential vulnerabilities to enhance network security.

Attack From: 10.191.191.0/24

Device Group	Devices
All Devices (ID: 1)	97

Patch Recommendation 1

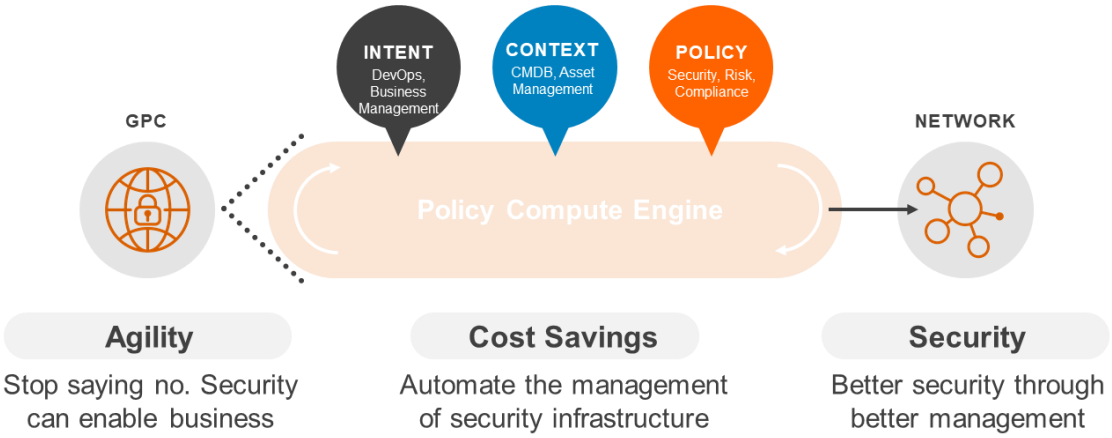
Patch 7 compromised asset(s) to protect 7 assets with an asset value of 70

Asset to Patch: jd700.securepassage.com

Effect	Vulnerability ID	Vulnerability Description	Service
Other	71049	The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak. Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.	TCP/22
Other	25220	The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.	TCP/0
Other	20094	According to the MAC address of its network adapter, the remote host is a VMware virtual machine.	TCP/0
Other	35716	Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE.	TCP/0
Other	19506	This plugin displays, for each tested host, information about the scan itself : - The version of the plugin set. - The type of scanner (Nessus or Nessus Home). - The version of the Nessus Engine. - The port scanner(s) used. - The port range scanned. - Whether credentialed or third-party patch management checks are possible. - The date of the scan. - The duration of the scan. - The number of hosts scanned in parallel. - The number of checks done in parallel.	TCP/0
Other	45590	By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host. Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.	TCP/0
Other	71495	The web interface for Palo Alto Networks PAN-OS firewall or Panorama was detected on the remote host. Panorama is a centralized management solution used for Palo Alto Networks firewalls.	TCP/443
Other	22964	Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.	TCP/443
Other	22964	Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.	TCP/22
Other	10107	This plugin attempts to determine the type and the version of the remote web server.	TCP/443
Other	56984	This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.	TCP/443
Other	104743	The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.1 and 1.2 are designed against these flaws and should be used whenever possible. PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals	TCP/443

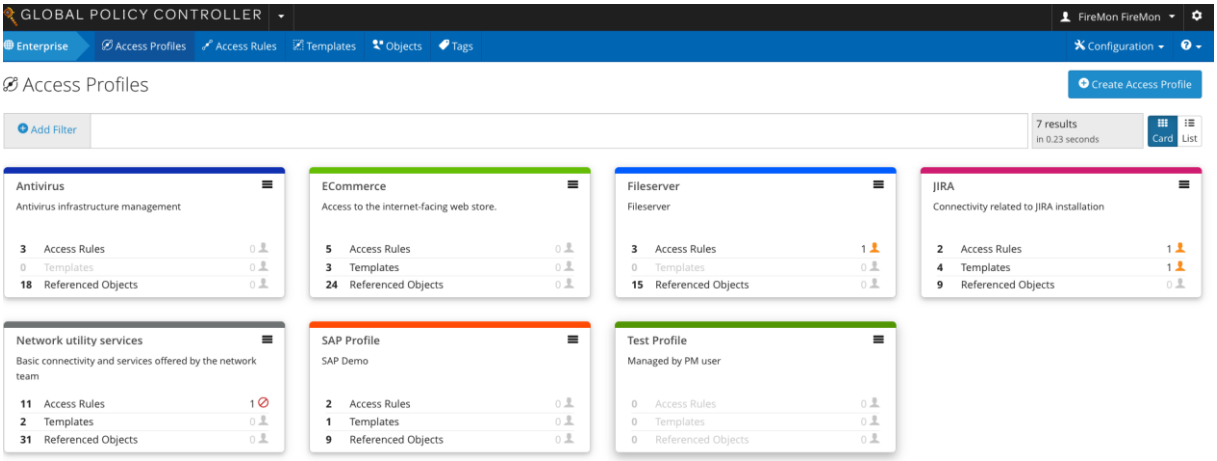
3. Global Policy Controller - scentralizowane zarządzanie politykami w infrastrukturze hybrydowej

Global Policy Controller (GPC) zapewnia połączenie potrzeb biznesowych w kontekście zasobów sieciowych i zapewnia automatyzację alokacji polityk bezpieczeństwa niezbędnych do prawidłowego dostępu za pomocą istniejącej infrastruktury

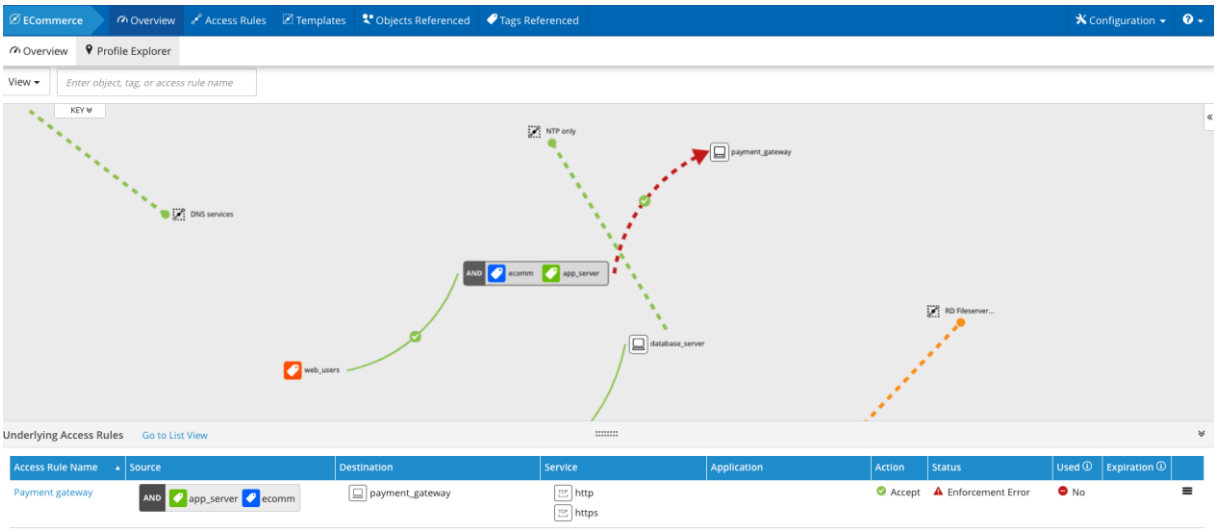


Zarządzanie bezpieczeństwem sieci w różnych technologiach, takich jak zasoby chmurowe, kontenery i tradycyjna infrastruktura staje się coraz bardziej złożone. Na przykład, wdrożenie zerowego zaufania i architektury mikro-segmentowej wymagają precyzyjnego monitorowania widoczności w hybrydowym środowisku. Jako odpowiedzialne za bezpieczeństwo sieci, zespoły IT są proszone o coraz więcej, ale przy krótszych czasach wdrożenia, przerwach w dostawie usług i zachowanych zabezpieczeniach, co staje się coraz większym problemem organizacyjnym i kosztem. Jednocześnie wymagania biznesowe zmieniają się szybko, gdy zachowania klientów i pracowników ulegają zmianom. Aplikacje i zasoby muszą być tworzone i wdrażane szybciej niż kiedykolwiek. W celu umożliwienia szybszych dostaw, zespoły DevOps szybko budują, wdrażają i zarządzają zaktualizowanymi nowymi aplikacjami. Wyzwaniem dla IT jest zatem wspieranie tego nowego paradygmatu bez narażania zasad zgodności z politykami bezpieczeństwa.

W celu realizacji tych zadań, każda aplikacja ma określany profil, który jest zdefiniowany i oznakowany w FireMon, udostępniany i oceniany pod kątem zgodności.



Tworzona jest też kompletna mapa połączeń profilu aplikacji w całym przedsiębiorstwie



FireMon Global Policy Controller (GPC) to pierwsze tego typu rozwiązanie zapewniające ciągłe bezpieczeństwo
i orkiestrację w organizacji hybrydowej. GPC osiąga to poprzez połączenie interesów menedżerów bezpieczeństwa IT z DevOps oraz innymi właścicielami obszarów biznesowych w spójnym, równoległym modelu operacyjnym, który koncentruje się na poprawie bezpieczeństwo i sprawności działania systemów IT, przy jednoczesnym zmniejszeniu kosztów. Rezultatem tego działania jest platforma do orkiestracji polityk, która zapewnia wydajne, zgodne z politykami konfiguracje zabezpieczeń, globalną widoczność i zarządzanie stanem bezpieczeństwa całej sieci a także ciągłą kontrolę bezpieczeństwa dla tradycyjnych i wirtualne platform.

- koniec dokumentu -