

# Tufin SecureTrack

## Pokročilý audit bezpečnostní politiky

**Organizace jsou dnes velmi závislé na počítačových sítích a Internetu. Společně s růstem komplexnosti sítí rostou i požadavky na zabezpečení.**

Nové bezpečnostní hrozby a změny v sítích zvyšují nároky na IT oddělení. Ve velkých společnostech je většinou zaměstnáno několik administrátorů bezpečnostních politik, kteří pracují na správě různých sítí, serverů, aplikací a uživatelů. Základním problémem se stává schopnost bezpečnostního oddělení udržet politiky funkční, konzistentní a odpovídající bezpečnostním standardům.

Příklady bezpečnostních problémů k řešení:

- Nové služby vyžadující speciální kontroly (VoIP, GPRS, atd.).
- Bezpečnostní hrozby na úrovni aplikací.
- Viry a malware schopné vyřadit z provozu komunikační síť organizace.

Navíc k těmto problémům moderní organizace průběžně mění své obchodní a síťové systémy tak, aby byly konkurenceschopné:

- Migrace obchodních operací na systémy CRM a ERP.
- Rozšiřující se služby a konektivita mezi obchodními partnery.
- Velké spektrum mobilních VPN klientů pro vzdálený přístup k intranetu a elektronické poště.

Dalším faktorem ovlivňujícím komplexitu politik je u středních a velkých společností používání více management serverů pro správu narůstajícího počtu firewallů a VPN zařízení. Tento fakt dále komplikuje práci oddělením zodpovědným za udržení politiky v provozovatelném stavu odpovídajícímu celkové bezpečnostní politice společnosti.

Ke zjednodušení operací při správě politik

pomáhá využití efektivních nástrojů pro audit, sledování verzí. Využití takovýchto nástrojů snižuje náklady a minimalizuje riziko chyby.

### Správa změn politiky firewallů

Většina bezpečnostních produktů udržuje takzvaný audit log, který obsahuje základní informace o změnách v politice uplatňované na daném zařízení. Tyto záznamy většinou obsahují informaci o změně, ale neposkytují o ní potřebné informace - většinou chybí přesný záznam o tom, jaká změna byla provedena ve které verzi politiky, zda byly změny uloženy na management, či zda byla politika nainstalována na vlastní firewall.

Mnoho organizací nemá nasazen žádný systém pro sledování změn a spoléhají se například na separátní vedení provozního deníku firewallů administrátory. Tento způsob má velmi malou přidanou hodnotu, protože je závislý na lidském faktoru, a je náchylný k chybám.

Výsledkem tohoto stavu je, že velké společnosti nejsou schopny adekvátně kontrolovat změny politik na bezpečnostních zařízeních a neznají přesnou konfiguraci těchto zařízení v daném časovém okamžiku.

V řadě situací je znalost těchto informací kriticky důležitá:

- Identifikace příčin výpadku sítě po změně na firewallu.
- Vyšetřování bezpečnostního incidentu.
- Sledování změn provedených více administrátory.
- Sledování změn politiky zařízení v rámci outsourcingu (například změny provedené Managed Service Providerem).
- Vnitřní/nezávislý audit bezpečnostní politiky.
- Kontrola aktuálních změn politiky proti plánu.
- Udržování a prosazování politiky přes více organizačních jednotek.

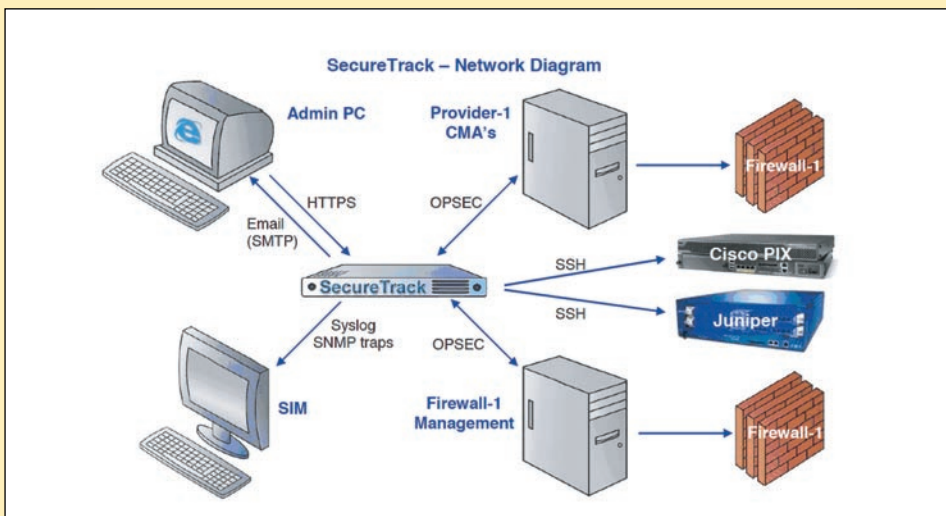
Právě absence robustního procesu kontroly a sledování politik bezpečnostních zařízení vede k neustále se zvyšujícím investicím finančních a lidských zdrojů v oblasti správy politik.

K zachování kontroly nad politikami bezpečnostních zařízení je třeba, aby bylo IT oddělení schopno:

- Uchovávat jednotlivé verze bezpečnostní politiky pro jednotlivá zařízení.
- Identifikovat přesně změny mezi verzemi politik.
- Srovnávat rozdíly mezi libovolnými verzemi politiky.
- Sledovat všechny změny libovolného administrátora.

Vlastnost SecureTrack	Výhody pro zákazníka
Sledování politiky firewallů	Kompletní záznam o každé změně, včetně uložení databáze a instalace politiky.
Neustálá kontrola verzí politiky	Zabezpečená databáze obsahuje informace o verzích politiky až po několik let zpět.
Upozornění na změny v reálném čase	Administrátoři a bezpečnostní pracovníci jsou upozorněni na chyby specifické změny ihned a jsou schopni identifikovat chyby jakmile nastanou.
Porovnání politik	Porovnání jednotlivých politik je snadné, díky zvládnutým změnám zobrazeným vedle sebe v grafickém webovém rozhraní.
Pokročilý reporting	Řešení umožňuje generovat z databáze verzí širokou škálu reportů.
Shoda s politikou organizace	Detailní politiku organizace je možno definovat a vyžadovat shodu politiky firewallů s politikou organizace. Administrátoři mohou být o porušení shody informováni v reálném čase.

Tabulka: Hlavní vlastnosti a výhody poskytované řešením SecureTrack.



Obrázek č.1: Diagram naznačuje součinnost mezi SecureTrack serverem a ostatními komponentami podílejícími se na procesu správy politiky firewallů.

- Zajistit, aby změny v politikách odpovídaly celkové politice společnosti.

## Řešení SecureTrack

Tuffin SecureTrack je pokročilý systém pro sledování změn v politikách firewallů. Umožňuje efektivní sledování všech změn politiky provedených administrátory v prostředích Check Point Firewall-1 a Provider-1. Poskytuje kontrolu nad verzemi politiky firewallů a umožňuje jejich sledování a audit.

## Jak funguje SecureTrack

SecureTrack používá rozhraní Check Point OPSEC (Open Platform for Security) ke sledování všech změn provedených administrátory v aplikaci Check Point SmartDashboard nebo Provider-1 GUI. Kdykoliv administrátor uloží politiku, nebo ji nainstaluje na firewallové moduly, SecureTrack je okamžitě informován o změně. Poté je použito zabezpečené připojení k získání nové verze politiky, která je bezpečně uložena v interní databázi SecureTrack.

Tyto operace probíhají automaticky a bez potřeby interakce administrátora. Ve chvíli, kdy je stažena nová verze politiky, SecureTrack provede analýzu změn a pošle předkonfigurovaná upozornění:

- e-mail registrovaným administrátorům s detaily provedených změn
- syslog záznam na definované syslog servery s detaily provedených změn
- SNMP trap registrovaným aplikacím obsahující detailní záznam o změnách

Tato upozornění poskytují informace o změnách politiky v reálném čase a umožňují tak integraci s další infrastrukturou bezpečnostního dohledu (SIM/SOC). Administrátor může konfigurovat vlastní upozornění reagující pouze na specifické změny na základě konfigurovatelné notifikační politiky.

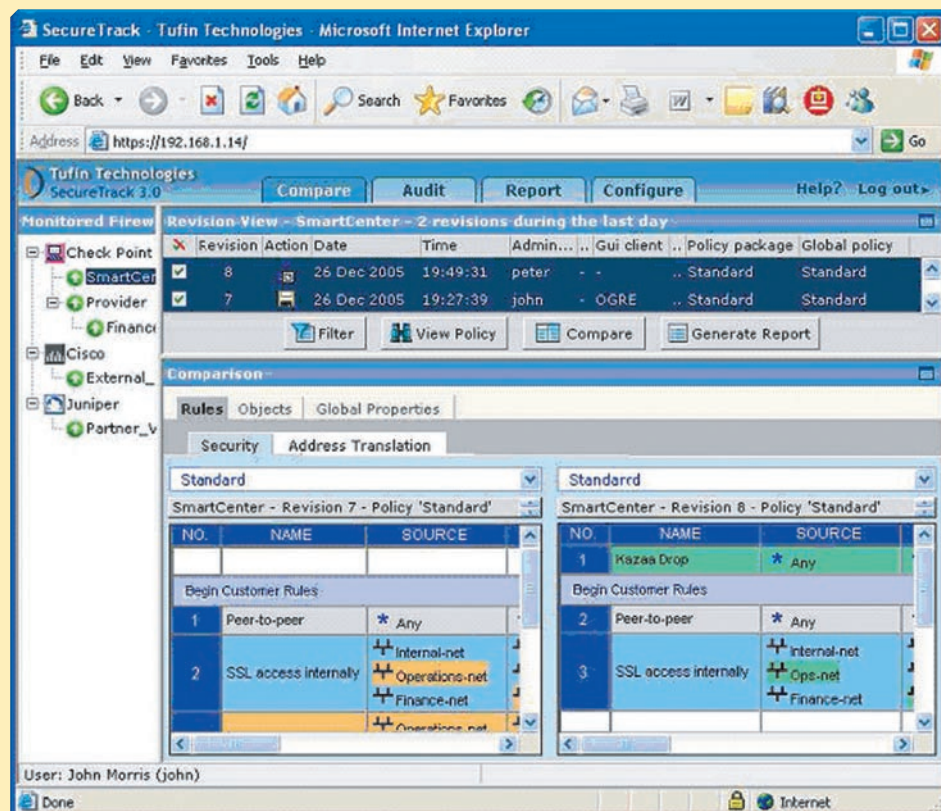
Na obrázku č.1 je znázorněn server s ope-

račním systémem RedHat Linux a systémem SecureTrack. S využitím API OPSEC monitoruje prostředí Check Point Firewall-1 a jednotlivých CMA systému Provider-1, navíc je schopen protokolem SSH monitorovat i zařízení Cisco PIX a firewally Juniper. Administrátoři SecureTrack dostávají upozornění ze systému přes e-mail, syslog nebo SNMP, a to jak do klasického poštovního klienta, tak přímo do aplikací pro řešení bezpečnostních incidentů (SIM) umístěných v operačním centru (SOC). Pro konfiguraci systému a porovnávání verzí politiky používá administrátor webové rozhraní.

Obrázek č.2 znázorňuje SecureTrack GUI, kde je naznačeno, jak může administrátor porovnávat různé politiky, což poskytuje velmi mocný nástroj pro analýzu změn mezi jednotlivými verzemi politik.

Navíc může administrátor SecureTrack využít pokročilého systému pro vytváření reportů k provádění vlastních dotazů do interní databáze, což umožňuje efektivní data-mining přes různé verze politik, včetně:

- Sledování aktivit specifického administrátora firewallu.



Obrázek č.2: Znázorňuje SecureTrack GUI.

Čas	Událost
11:00	Bezpečnostní správce provede chybnou změnu v pravidlech firewallu, která pokrývá HTTP provoz a blokuje veškeré přístupy ke korporátnímu webu.
11:01	Bezpečnostní oddělení a manažer IT Helpdesku obdrží notifikaci o provedené změně (e-mail, syslog, SNMP trap).
11:05	IT Helpdesk začíná přijímat stížnosti na nedostupnost webu.
11:10	Manažer IT Helpdesku je schopen spojit nedostupnost webové služby s poslední změnou politiky a kontaktuje bezpečnostní oddělení.
11:15	S využitím SecureTrack jsou provedené změny okamžitě viditelné a problém je rychle identifikován.
11:20	Problém je vyřešen.

Příklad

- Sledování změn v určitém časovém období na libovolném management serveru.

### Zvyšování dostupnosti služeb s pomocí sledování politik v reálném čase

Společnosti jsou v dnešní době závislé na různých technologiích, které umožňují nebo podporují jejich obchodní operace. Výpadek takovýchto služeb tedy může způsobit značné škody obchodním aktivitám.

Nedávná studie společnosti Infonetics Research ("The Cost of Enterprise Downtime, North America 2004", Infonetics Research Inc.) odhaduje, že velké společnosti ztratí přibližně 3,6 % příjmů díky výpadekům aplikačních služeb. Navíc ze studie vyplývá, že 22 % těchto výpadeků je způsobeno lidskou chybou. Následky chyb v politice firewallů mohou být

fatální, protože tato bezpečnostní zařízení řídí veškerý síťový provoz a konektivitu.

Efektivní metoda zamezení takovýchto výpadků je založena na sledování a auditu politik firewallů v reálném čase. Umožňuje to IT pracovníkům korelovat změny v politikách s případným výpadkem aplikační služby a včasnou nápravou minimalizovat dobu výpadku.

Pokud by v příkladu uvedeném výše nebyl využit SecureTrack, mohlo by se provázání chyby administrátora se stížnostmi na IT Helpdesku prodloužit na hodiny místo minut. Vzhledem k tomu, že výpadky aplikací nebo konektivity způsobují vysoké škody, přispívá SecureTrack, díky minimalizaci frekvence a doby výpadků, významným způsobem k návratnosti investic (ROI).

Tuřin SecureTrack pomáhá IT Security pracovníkům poskytováním pokročilých nástrojů pro správu, sledování a audit bezpečnostních politik v reálném čase. Zároveň umožňuje uchovávat historické verze politik pro budoucí porovnání a případné odstranění chyb.

#### Základní výhody využití SecureTrack:

- Sledování a záznam všech změn v politikách na firewallech.
- Konfigurovatelná upozornění na změny v reálném čase.
- Jednoduché a intuitivní srovnání mezi verzemi politik.
- Podrobné reporty o aktivitách jednotlivých administrátorů.
- Rychlá detekce a oprava chyb vedoucí k urychlení návratnosti investic.

Při využití SecureTrack jsou IT oddělení schopna zvýšit svoji efektivitu a poskytovat organizaci služby na lepší úrovni. Jednoduché a škálovatelné řešení poskytuje administrátorům okamžité výhody, díky nimž jsou schopni efektivně spravovat stále komplexnější politiky na firewallech.

Autor:

Pavel Šesták a Martin Slavík  
Actinet Informační systémy s.r.o.