Infoblox Security Device Controller

S rostoucí firmou jde ruku v ruce rostoucí počet počítačů a tím pádem také bezpečnostních zařízení v rozpínající se infrastruktuře. Jakýkoli zásah do sítě, včetně implementace nových prvků, se tak stává operací velice náročnou na zdroje firmy i čas síťových administrátorů. Zásah do jednoho místa v síti vždy vyvolá řetězovou reakci, která se rozšíří do všech jejich koutů nezávisle na tom, k čemu daný prvek v síti slouží nebo kým byl vyroben.

Klíčové charakteristiky

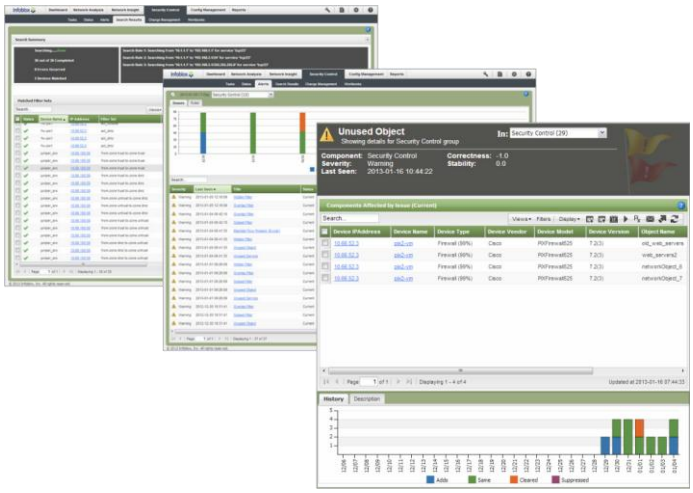
- ⇒ **Správa a nasazování bezpečnostních řešení různých výrobců.**
- ⇒ **Jediné prostředí zastřešující veškeré procesy správy bezpečnosti sítě.**
- ⇒ **Automatická analýza sítě** a náhledy topologie.
- ⇒ Automaticky generované soubory pravidel pro **vytváření modelů a testování před vlastním nasazením do sítě.**
- ⇒ **Notifikace v případě, že nové změny mohou ohrozit stávající konfiguraci sítě.**
- ⇒ Vyhledávání mezi různorodými platformami od různých výrobců.
- ⇒ **Automatická varování při změnách** v infrastruktuře nebo nalezení nepoužitých, duplicitních, skrytých nebo překrývajících se pravidel.
- ⇒ Alerting je uživatelsky přizpůsobitelný danému stavu a topologii sítě.

Přínosy

- ⇒ **Snížení množství procesů náchylných k chybám**, díky integrovaným znalostem bezpečnostních zařízení různých výrobců a jejich centrální správě.
- ⇒ **Snížení časové náročnosti potřebné k nasazení nových řešení** do stávající infrastruktury snížením nároků na obsluhu a náročnosti iniciálního nastavení.
- ⇒ **Eliminace manuálních kroků** díky automatizaci a intuitivnímu rozhraní.
- ⇒ **Zaručení standardizace infrastruktury** trvalým monitoringem, real-time náhledy pro troubleshooting a reporty "jedním kliknutím".
- ⇒ **Eliminace neplánovaných a nechtěných problémů** pomocí kontroly, ověřování a schvalování procesů.

Značným ulehčením v těchto situacích pro Vás zajisté bude novinka od společnosti Infoblox - Security Device Controller. Infoblox Security Device Controller, jako jediné řešení svého druhu, výrazně zkracuje tradiční a časově náročný proces manuální tvorby návrhu a implementace změn v síťové bezpečnosti a změn v přístupových pravidlech. Platforma integruje unikátní databázi analýz řešení jiných výrobců, společně se schopností distribuovat mezi ně změny v nastaveních, a to vše přes jedno rozhraní. Integrované znalosti eliminují potřebu jednotlivých pracovníků, kteří by byli odborníky na syntaxe a nuance všech jednotlivých zařízení. Dává Vám tak možnost integrace nových bezpečnostních prvků a služeb v rámci minut namísto dní.

Centrální distribuce pravidel a nastavení různým bezpečnostním prvkům v síti z jediného místa.



Security Device Controller automaticky vyhledává síťová zařízení, sbírá jejich konfigurace a automaticky podle toho aktualizuje bezpečnostní konfiguraci. Prostřednictvím stálého prozkoumávání prostředí a díky aktualizacím rychle se měnících informací, poskytuje toto řešení důležité informace síťovému nebo bezpečnostnímu administrátorovi (např. dodavatele, typ zařízení, routing, informace o virtuálních sítích a další). Ten je schopen na základě těchto informací určit, která zařízení budou ovlivněna změnou pravidel.

COMGUARD security & networking
COMGUARD s.r.o.
Sochorova 38, CZ 616 00 Brno
tel. +420 513 035 400
info@comguard.cz | www.comguard.cz

Infoblox DNS Firewall

Variabilita hackerských útoků stoupá, ovšem v některých případech jsou to tradiční metody útoků, které slaví úspěch. V posledních letech se počet nových malwarových hrozeb pohybuje v řádech milionů měsíčně. Celých 69 % průniků do korporátních infrastruktur a úniků dat za tentýž rok má na svědomí malware. Téměř všechny tyto útoky jsou pak odhaleny subjekty mimo napadenou organizaci.

Klíčové charakteristiky

Díky Infoblox DNS Firewallu se nyní můžete bránit před malwarem využívajícím slabin DNS systému.

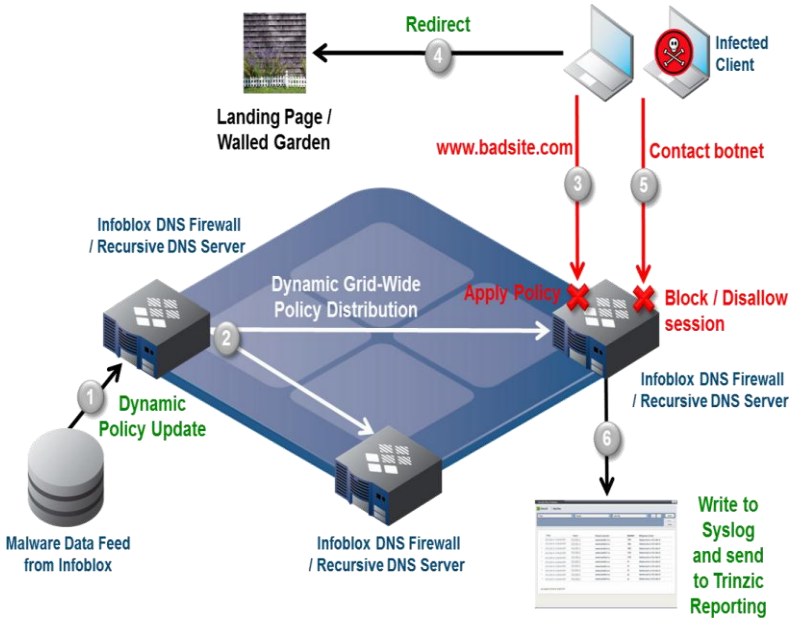
⇒ **Proaktivní:** zamezí klientům přístup k infikovaným stránkám a identifikuje již infikované klienty.

⇒ **Aktuální:** využívá komplexní, přesná a aktuální data o malware pro detekci, eliminaci a blokování malwaru o týdny a měsíce rychleji než běžná řešení.

⇒ **Variabilní:** umožňuje přesměrování NXDOMAIN, definici hierarchických politik (pro DNS, malware a další), a tak zvyšuje užitnou hodnotu reputačních dat o malware v konkrétním prostředí zákazníka.

Jedním z nejnebezpečnějších typů malware je takzvaný „DNS-based malware". Škodlivý kód využívá principu funkce DNS služeb, které dnes využívá každá běžná síť. Většinou je navržen právě pro průnik do systému a dlouhodobé krádeže dat. Čím častěji si zaměstnanci nosí vlastní zařízení do firemních prostředí nebo naopak firemní zařízení mimo ochranu firemní infrastruktury, tím větší je možnost zavlečení malwaru do interní firemní sítě. Ten tak není nucen překonávat firewall nebo jiné ochranné prvky sítě a pomocí DNS protokolu velice lehce pronikne přes současné bezpečnostní technologie na bázi IP adres.

V okamžiku kdy experti Infobloxu detekují nový malware, jsou nová data okamžitě zasílána zákazníkům a distribuována rekurzivním Infoblox DNS serverům buď přímo nebo prostřednictvím Grid technologie. Pokud chce uživatel navštívit nebezpečnou stránku, bude tento pokus zablokován na úrovni DNS protokolu. Spojení bude přesměrováno na stránku danou administrátorem. Pokud je již klient nakažen (typicky uživatelem vlastněné zařízení), pokusí se použít DNS příkazy, aby kontaktoval hlavní botnet kontrolér. Infoblox DNS Firewall pak zablokuje tuto komunikaci a efektivně ochromí botnet. Všechny aktivity jsou zapisovány do standardního Syslog formátu, takže zjistit zdroj malwarových odkazů nebo dohledat nakaženého klienta není žádný problém. Data jsou také směrována do Infoblox Triznic Reportingu na analýzu a tvorbu reportů.



Přínosy

⇒ **Minimalizuje zdroje vynaložené na eliminaci malwaru a jeho následků:** Infoblox DNS Firewall zastavuje hrozby předtím, než mají možnost začít svůj útok. Identifikuje všechny infikované klienty, aby jejich zařízení mohla být "vyčištěna", a to včetně zařízení vlastněných přímo uživateli.

⇒ **Zakomponuje ochranu proti malware trvale do Vaší infrastruktury:** po iniciální konfiguraci není třeba žádných dalších nastavení a přesto máte vždy aktuální ochranu před malwarem, 24 hodin denně, 7 dní v týdnu. Díky logům a reportům máte podklady potřebné pro audit a zároveň seznam infikovaných klientů pro Vaše IT oddělení.

COMGUARD security & networking
COMGUARD s.r.o.
Sochorova 38, CZ 616 00 Brno
tel. +420 513 035 400
info@comguard.cz | www.comguard.cz