Řízení firewallových politik

Část druhá: Doporučení pro řízení firewallů

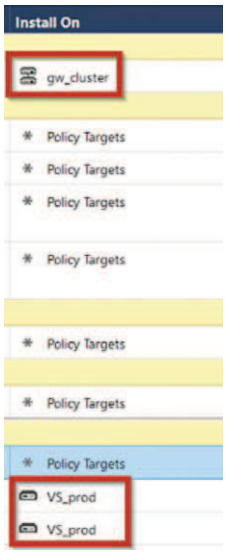
Lukáš Solil

V první části článku v minulém vydání IT Systems jsme se podívali na to, jaké chyby se nejčastěji dělají při správě firewallů a jejich politik. Nezůstali jsme jen u seznamu nedostatků, ale přidali jsme i rady z praxe, které by měly pomoct se jim vyhnout. V této části článku budeme ve výčtu obvyklých chyb pokračovat. Kromě toho se ale také zaměříme na doporučení, která vám mohou při řízení firewallů a při nastavování procesů pro jeho řízení přijít vhod.

Mixování politik více firewallů

Některé technologie umožňují vytvořit jednu politiku pro všechny brány, pro některá pravidla specificky vydefinovat bránu, na kterou se bude dané pravidlo vztahovat. Toto pravidlo se pak normálně zobrazuje v politice, ale neplatí pro všechny firewally, což může být velmi matoucí. Jsou situace, kdy se tato vlastnost hodí. Například ve chvíli, kdy je jednotná politika pro všechny pobočky, a tímto způsobem jsou řešeny drobné odchylky. Obvykle je ale použití nevhodné a nepřehledné.

Kombinování jednotné politiky a odchylek v jednotlivých pravidlech může jednoduše vést k chybě administrátora. Z toho důvodu je vhodnější se této funkcionalitě vyhnout. Pokud je její využití opravdu nutné, je nutné definovat postup, kdy a jak pravidla pro specifický firewall vytvořit. Je vhodné, aby taková pravidla byla vždy v samostatně a jasně vyznačené sekci. Pokud to daná technologie umožňuje, je lepší pro každý firewall vytvořit vlastní politiku a případně část politiky mezi firewally sdílet.



Obr. 1: Příklad instalace vybraných pravidel na různé firewally

Používání obecného objektu

Další chybou, která se vyskytuje téměř ve všech prostředích, je využívání obecného objektu v povolovacích pravidlech. Obecným objektem je zde myšlen objekt reprezentující všechny IP adresy či porty, obvykle bývá označován klíčovým slovem „Any“. Chybou je zejména jeho použití jako zdroje, cíle nebo služby u povolovacího pravidla. K této chybě dochází zejména ve chvíli, kdy je nedostatečně definovaný požadavek na prostup. Použití tohoto objektu téměř vždy znamená přílišné otevření firewallu. Zároveň použití „Any“ nenutí autora požadavku a pravidla, aby se zamysleli nad tím, zda nelze prostup více omezit.

Součástí procesů na úpravy firewallové politiky by mělo být omezení na používání obecného objektu u povolovacích pravidel. Správně definovaný koncept firewallové politiky navíc už sám o sobě ztěžuje použití tohoto objektu, protože administrátor potřebuje pravidlo umístit do správné sekce, což znamená blíže specifikovat jeho zdroj a cíl. Omezit množství pravidel s obecným objektem je obvykle o něco snazší u zónového firewallu, protože bývá jednodušší si uvědomit, mezi kterými zónami má komunikace probíhat, než přesně určit skupiny objektů, jichž se týká.

Riziková pravidla

Často se při práci v různých prostředích a při auditech setkáváme s pravidly, která jsou na první pohled příliš otevřená nebo zjevně představují bezpečnostní riziko. Někdy je i bez podrobné znalosti prostředí vidět, že dané pravidlo není vytvořené z hlediska bezpečnosti správně. Obvykle jde o povolení málo specifikované komunikace mezi serverovými a uživatelskými sítěmi.

Do procesu úprav firewallové politiky je vhodné zavést krok, v jehož rámci dojde k validaci změny z hlediska bezpečnosti. Tuto validaci by měl provádět někdo nezávislý (obvykle oddělení bezpečnosti ve společnosti), protože administrátor může raději upřednostnit jednoduchost před bezpečností. Jednou z nejdůležitějších částí procesu je nastavení výjimek a především dočasných výjimek. Všechny výjimky by měly být vždy posouzeny z bezpečnostního hlediska. U dočasných výjimek je navíc třeba jasně specifikovat dobu jejich platnosti, hlídat ji a striktně dodržovat. Dočasné podmínky jsou obvykle největší zdroj bezpečnostních chyb. Často vznikají ve spěchu, například v době migrace, kdy jediným cílem je, aby vše fungovalo. Jen málo kdy pak ale dojde k omezení povoleného prostupu jen na nezbytné porty.

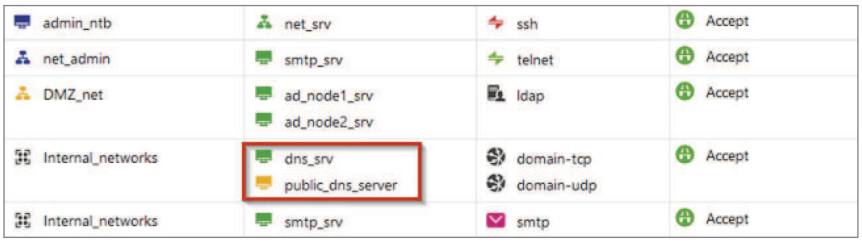
Praxe nám také ukazuje, že je vhodné používat barvy objektů k odlišení různých bezpečnostních zón (pokud nám to samozřejmě grafické rozhraní dané technologie umožňuje). Díky barvám je pak na první pohled vidět bezpečnostní chyba. Zároveň se vyrýsují odchylky ze struktury politiky, takže administrátor či auditor ihned zjistí, kde je třeba zjednat nápravu.

Závěrečná pravidla

Na konci každé politiky, každé vrstvy nebo samostatné tabulky je pravidlo, které určí, co se stane se zbývajícím provozem. Ten by se měl ve standardní firewallové politice vždy zahodit a zalogovat. V reálu se tak obvykle skutečně děje. Někdy ale narážíme i na to, že

Obr. 2: Omezení používání „Any“ u povolovacích pravidel. Legenda: ❶ Nahrazení obecného objektu „Any“ za konkrétní sítě, ❷ Specifikace skupiny portů místo obecného objektu

No.	Name	Source	Destination	Services & Applications
Firewall access (1)				
Special rules (2-5)				
To DMZ (6)				
6	To DMZ zone	Any	DMZ_Zone	Any
6.1	to web srv	Internet, Internal_networks ❶	web_srv	web_srv_grp ❷
6.2	Cleanup rule	Any	Any	Any



Obr. 3: Odlišné barvy poukazují na chybu v politice.

po implementaci zůstalo závěrečné pravidlo nastavené na povolení komunikace. Toto je ale obrovská chyba, která by neměla nikdy nastat. Ani v průběhu samotné migrace by nemělo dojít k úplnému otevření firewallu, rozhodně ale nesmí být veškerý provoz povolen, když skončí servisní okno.

Nastavení povolení na konci politiky naštěstí není příliš častý úkaz. Běžnější je situace, kdy je povolovací pravidlo na konci části politiky (například vrstvy nebo tabulky). Do této vrstvy se dostane jen část provozu, která odpovídá nadřazenému pravidlu. Takováto vrstva či tabulka se pak chová jako samostatná politika, která se ale týká jen oné části komunikace. Běžně by v tomto případě na konci mělo být zakazovací pravidlo. Tentokrát to ale nelze říci obecně, protože záleží na funkci, kterou má daná vrstva či tabulka vykonávat. K filtraci na úrovni FW už mohlo dojít v rámci nadřazeného pravidla a zmíněná část politiky může sloužit například pro aplikační kontrolu nebo pro definici výjimek z nadřazeného pravidla. Zde záleží na tom, jakým způsobem je celá politika koncipována. Z hlediska přehlednosti je lepší, aby všechny vrstvy nebo tabulky fungovaly jako samostatná firewallová politika a končily zakazovacím pravidlem.

Další doporučení pro řízení firewallových procesů

Výše uvedené tipy by měly při sestavování firewallových procesů pomoct omezit ty nejčastější chyby, které se při správě firewallů obvykle dělají. Kromě nich jsou v tomto článku uvedena další praxí ověřená doporučení.

Pravidelná revize pravidel

Dobře nastavené procesy jsou jedna věc, jejich dodržování je věc druhá. Aby vše fungovalo tak, jak to bylo plánované, je třeba provádět pravidelné kontroly. Je vhodné provádět pravidelnou kontrolu báze pravidel a ověřit, že je vytvořena podle stanoveného konceptu. Je třeba ověřit, že v politice nejsou žádné neschválené výjimky, že jsou pravidla umístěna do sekcí, ve kterých mají být. Dále je dobré zkontrolovat, že se dodržují jmenné konvence, že v politice nejsou zastaralá, (dlouho) disablovaná či nepoužívaná pravidla a objekty. Také je třeba vyhodnotit, zda politika neobsahuje nová riziková pravidla či neschválené výjimky. V rámci revize je pak také vhodné ověřit validitu zavedených pravidel, jak již bylo zmíněno v předchozí části tohoto článku.

Takovou to revizi by měli několikrát do roka provádět sami administrátoři. Alespoň jednou ročně by ji pak měl provést nezávislý auditor. Pokud se při revizi najdou chyby, měla by se naplánovat jejich brzká náprava. Případně je také vhodné zjistit, jak a proč chyba vznikla. Na základě toho je pak třeba vyhodnotit, zda jsou procesy nastavené správně a není třeba je pozměnit.

Využívání možností dané technologie

Autor firemních postupů pro správu firewallů by se měl nejprve co nejdůkladněji seznámit s možnostmi technologie, která bude v organizace použita. Různé produkty nabízejí dobré funkcionality, které je vhodné zakomponovat i do procesů. Nevýhodou samozřejmě je, že při výměně technologie bude třeba postupy upravit. Na druhou stranu se ale díky tomu daná technologie využije naplno se všemi svými možnostmi. S výhodou je možné používat například výše zmíněné barvy objektů, vrstvy či oddělené tabulky, větší množství politik či například modul pro ověření compliance s obecnými standardy.

Využívání komunikačních matic

Aby bylo možné pravidelně revidovat bázi pravidel a změny v ní, je potřeba mít k dispozici nějaký strukturovaný záznam o požadovaných prostupech. Jedním z praktických typů záznamu těchto požadavků jsou například komunikační matice. Ty popisují požadované prostupy v podobě jednoduché tabulky. Aby dokumentace pomocí těchto matic fungovala, je třeba, aby ji udržoval vlastník každé aplikace či systému, jenž potřebuje vytvořit prostupy na firewallu. Matice je pak třeba aktualizovat při každé změně a udržovat je jak jako součást dokumentace daného systému, tak jako podklad pro vytváření prostupů. Komunikační matice zjednodušují práci oddělení bezpečnosti, které může přímo z matice vyhodnocovat rizika požadované komunikace daného systému. Z matice jsou také patrné podsystémy, které daný systém využívá a na kterých je závislý, což usnadňuje analýzu dopadů při výpadku některého z nich.

	INET	DMZ	LAN	SRV_COMM	SRV_DB	SRV_APP
INET	0	1	0	0	0	0
DMZ	1	1	1	0	0	1
LAN	1	1	1	1	0	1
SRV_COMM	0	1	0	1	0	0
SRV_DB	0	0	0	1	1	0
SRV_APP	0	0	0	1	1	1

Tabulka 1: Příklad binární komunikační matice

Pro výše zmíněné účely je vhodná matice, která ve sloupcích i řádcích obsahuje jednotlivé servery systému či sítě systému a v buňkách porty, jež je třeba mezi nimi povolit. Kromě tohoto typu tabulky je praktická také binární komunikační matice. Ta slouží zejména k high-level pohledu na celou firewallovou politiku. V jejích sloupcích a řádcích jsou uvedené bezpečnostní zóny (či jiné rozumné celky, agregaci lze zvolit libovolně). V buňkách tabulky jsou pak jen jedničky nebo nuly, podle toho, zda mezi těmito zónami existuje nějaký prostup nebo ne. Tato matice je vhodná pro rychlou kontrolu firewallu – pokud je například hodnota jedna v buňce pro provoz mezi méně a více zabezpečenou zónou, je třeba zjistit, proč zde probíhá provoz a jakého je typu. Pravděpodobně pak bude třeba zjednat nápravu, aby tento prostup nebyl dále potřeba.

Efektivní řízení firewallové politiky

Dobré nastavení procesů je základ pro to, aby se dařilo firewallovou politiku udržet přehlednou a bezpečnou. S narůstajícím počtem firewallů, administrátorů a systémů je ale čím dál tím těžší procesy dodržovat a kontrolovat. Proto existují nástroje, které pomohou efektivně dodržovat zavedené postupy, automatizovaně kontrolovat a revidovat firewallová pravidla a reportovat souhrnně důležité informace. V této části článku jsou shrnuty hlavní funkcionality, kterými tyto nástroje mohou při řízení firewallových politik pomoct.

Vytvoření mapy sítě

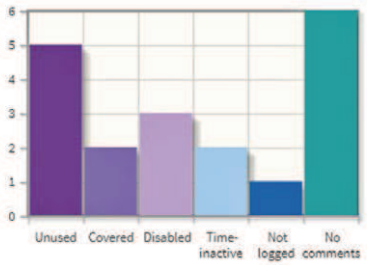
Nástroje pro řízení firewallů se napojí přímo na management servery jednotlivých produktů a vyčtou si z nich informaci o politikách a routingu. Dále je také možné je napojit na další aktivní prvky sítě, jakými jsou například routery. Díky tomu mohou tyto nástroje modelovat celé prostředí a zjistit, kde jsou umístěny které sítě. Administrátoři potom mají možnost vytvořené modely využít k vyhledávání cesty, kterou projde vybraný provoz. Zároveň lze automaticky zjistit, zda je provoz na některém z firewallů v cestě zablokován. Nástroj pak obvykle rovnou nabízí postup potřebný k povolení této komunikace.

Optimalizace politiky

Jednou z nejdůležitějších vlastností nástrojů na správu bezpečnostních politik je reporting možných optimalizací. Díky němu lze rychle a efektivně dosáhnout odstranění některých chyb uvedených v první části tohoto článku. Nástroj automaticky vyhodnotí nepoužívaná pravidla a objekty, ukáže, která pravidla se překrývají a která jsou duplicitní. Ještě zajímavější je možnost odhalení rizikových pravidel, kdy nástroj detekuje prostupy mezi více a méně zabezpečenými částmi sítě a vyhodnocuje rizikovost portů, které jsou mezi nimi otevřeny.

Nástroje si kromě politik a routingu vyčítají z firewallů také logy za vybrané období. Díky tomu mají možnost spočítat využívanost jednotlivých pravidel na úrovni jednotlivých objektů (zdrojů, cílů i portů). Tato informace například říká, že ze skupiny pěti počítačů využívají prostup jen tři. Nebo že je otevřený rozsah tisíce TCP portů, ale reálně se jich používá jen pár. S těmito vstupy lze snadno a bezpečně uzavřít příliš otevřené prostupy. Bez automatizovaných nástrojů přitom tyto informace téměř není možné získat.

Další pomocí při optimalizaci politiky je, že nástroje navrhují, jak napravit nalezené chyby a jak správně seřadit pravidla. Tato vlastnost zjednodušuje práci administrátorům, kteří by jinak museli zvážit, jak chybu napravit a vymyslet, jak to udělat a zároveň dodržet stanovený koncept.



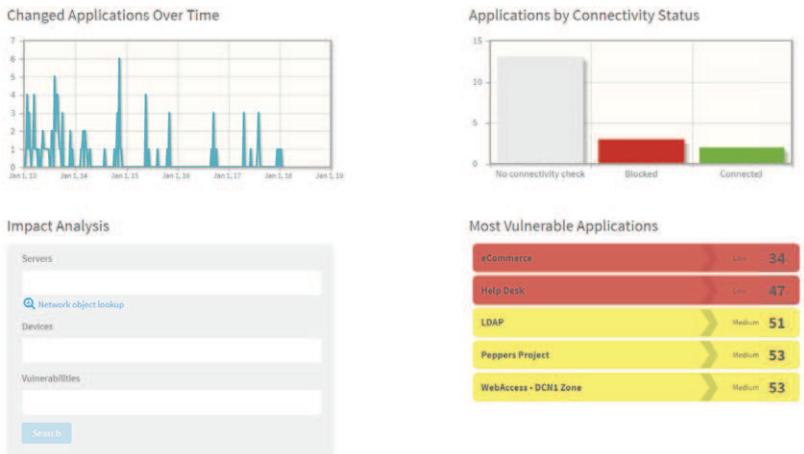
Obr. 4: Příklad grafu z reportu pro optimalizaci pravidel.

Workflow

Nástroje pro management firewallových politik obvykle obsahují také možnost využít automatizované workflow pro správu životního cyklu změn v politice. Workflow se může libovolně přizpůsobit potřebám společnosti, standardně ale zahrnuje obvyklé kroky, jako jsou vytvoření požadavku na úpravu, návrh implementace změny, zvážení bezpečnostních rizik, samotná implementace, validace správnosti zavedených změn, atd.

V tomto případě nástroj opět pomáhá v zamezení chyb zmíněných na začátku tohoto článku jednak tím, že vynucuje vytvoření požadavku na změnu, ale také tím, že umožňuje vložit do workflow bezpečnostní kontrolu implementované změny. Díky tomu, že každý požadavek na změnu musí projít nástrojem, je k dispozici dokumentace vzniku celé politiky. To umožňuje mimo jiné snazší validaci aktuálnosti požadavků na prostupy.

Obr. 5: Ukázka reportu o spravovaných aplikacích.



Správa firewallu a business požadavky

Některé nástroje nabízí možnost přiblížení správy firewallů ještě více k vlastníkům, správcům či projektovým manažerům aplikací a systémů. Ti mají možnost v nástroji spravovat zdroje a informace o komunikaci svých aplikací. Díky tomu nástroj může vykreslit graf komunikace, vytvořit komunikační matici a založit všechny potřebné požadavky na prostupy. Další výhodou je pak možnost zjistit, jaký dopad bude mít na systémy výpadek některého serveru či firewallu. Při integraci s vulnerability managementem zároveň uživatelé získají informace o známých zranitelnostech týkajících se daného systému a o dalších rizicích s ním spojených.

Vzhledem k tomu, že jsou tyto produkty přímo určené ke správě firewallových politik, dokážou velmi zjednodušit a zefektivnit práci. Kromě výše zmíněných výhod poskytují například centrální správu pro různé výrobce firewallů nebo porovnání politik s různými standardy a doporučeními. Výhod těchto systémů je více a liší se mezi jednotlivými produkty.

Závěr

Aby správa firewallových politik fungovala bez problémů a bezpečně, je třeba mít správně nastavené procesy a postupy, kterými se lze v praxi řídit. Se zvyšujícím se počtem pravidel a firewallů je řízení správy firewallu stále těžší a vyžaduje častější kontroly správného nastavení. Pro efektivní řízení firewallových politik je vhodné zvážit využití automatizovaných nástrojů, které pomohou v dodržování nastavených procesů a celkově pomohou udržovat bezpečnostní politiky firewallů. V každém případě je ale potřeba se řízením firewallových politik zabývat a nenechat je rozvíjet samovolně. Jinak v brzké době dojde k situaci, kdy se v nich nikdo nevyzná. Začnou se vytvářet výjimky, které budou pokaždé výše a výše v politice, pro jistotu na všech firewallech, které by mohly provoz omezit. Budou stále vznikat nové prostupy, které nikdo nebude schopen kontrolovat, až nakonec nebude firewall kontrolovat o moc více než obyčejný router. ■

Lukáš Solil

Autor článku působí jako Security Specialist ve společnosti AEC a.s.