Stavíme firewallové řešení

Lukáš Solil

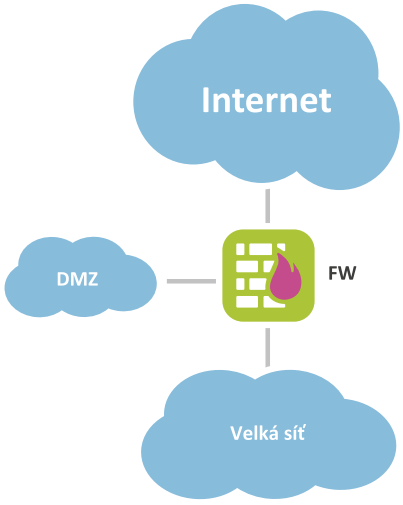
Jsou různé situace v životě lidském, kdy je třeba zabývat se pořízením nového firewallu. Možná je to proto, že se firma rozrostla a jeden linuxový administrátor s open-source stavovým firewallem (iptables) už nezvládá obsluhovat požadavky uživatelů. Nebo možná proto, že staré řešení už nestačí a bylo by lepší nějaké s novými funkcemi. Nebo se vedení společnosti rozhodlo investovat do bezpečnosti a implementace firewallu vypadá jako vhodný první krok. Ať tak nebo tak, někdy se stane, že je potřeba firewall pořídit. Co když jste ten úkol dostali zrovna vy? Jak to udělat, aby investice do firewallu nebyly jen vyhozené peníze? Jak probíhá implementace firewallu?

Architektura sítě

V ideálním případě je ve společnosti připravený plán rozvoje IT. Plán je stanovený na několik let dopředu a schválený vedením společnosti, takže není problém sehnat potřebné zdroje. Firewall vybíráte proto, že přišel na řadu podle tohoto plánu. Architektura celého řešení je jasná, opět se jen stačí podívat do plánu. Zde je architektura jasně popsaná v kombinaci s ostatními prvky, jak s těmi, které již v síti jsou, tak s těmi, které v ní teprve mají být.

Jenže výskyt ideálních případů se limitně blíží nule a firem je na světě opravdu hodně, takže je dost pravděpodobné, že pořádný plán rozvoje k dispozici nemáte a architekturu celého řešení budete muset řešit vy.

Obrázek 1: Síť bez segmentace



Nejprve se zamysleme nad tím, co především by měl firewall dělat. Měl by od sebe oddělovat různé části sítě a filtrovat komunikaci tak, aby mezi jednotlivými částmi neprocházelo nic, co tam být nemá. Moderní firewally navíc obvykle nabízejí další užitečné funkce, jako například VPN, IPS, síťový antivirus, aplikační firewall a další. A samozřejmě od firewallu očekáváme, že to bude všechno stíhat zpracovávat tak, abychom nepocítili zpoždění. Je zajímavé, kolika lidem vadí, když se jim seká video a stahování obrázků trvá přes hodinu...

V první řadě se zaměřme na segmentaci sítě. To je hlavní úloha firewallu. Není dobré, aby byla společnost na jedné velké síti. Pokud se totiž do ní dostane případný útočník, může se v ní volně pohybovat. Může v ní zkoušet prolomit bezpečnost všech zařízení bez nutnosti obcházet další zábrany. Proto je třeba síť rozdělit na menší podsítě (segmentovat). Pokud je síť rozdělená na menší celky, útočníkovi se hůře napadají zařízení v jejích jednotlivých částech. I když se dostane do jedné části, firewall mu brání v tom, aby se snadno dostal do ostatních. V podstatě se dá říci, že čím jsou podsítě menší, tím lepší bezpečnost, protože případný útočník musí překonávat tím více překážek.

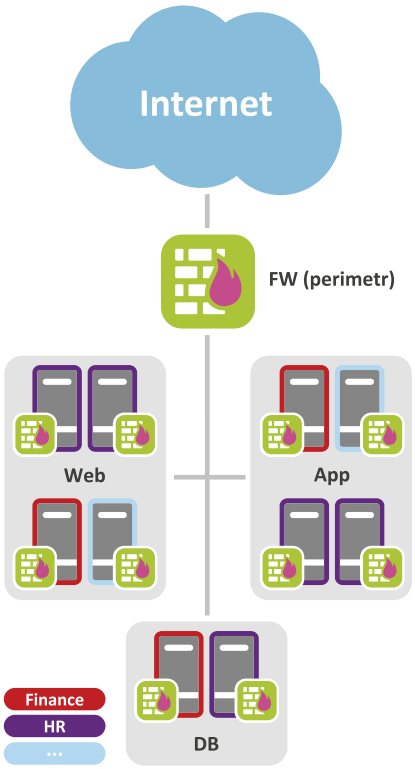
Z hlediska bezpečnosti je nejlepší variantou, když v každé části sítě je jen velmi málo zařízení (někdy i jen jedno). Jenže jak už to tak bývá, čím větší bezpečnost, tím více práce pro administrátory. Jednotlivé podsítě je nejprve potřeba navrhnout, pak vytvořit a nakonec mezi nimi udělat prostupy. A pak to všechno neustále udržovat v chodu a pořádku i přes druhý zákon termodynamiky*, který se vám v tom očividně snaží zabránit.

*Druhý zákon termodynamiky v podstatě říká, že v izolovaném systému se nikdy samo neuklidí, zato tam sám od sebe může vznikat nepořádek. (pozn. autora)

V dnešní době existují technologie, které umožňují dosáhnout tzv. mikrosegmentace. Tedy naprosto granulárního oddělení síťových prvků až na úroveň jednotlivých síťových rozhraní. Mikrosegmentace neslouží k ochraně perimetru, je ale výborným bezpečnostním řešením pro rozčlenění vnitřních sítí, zejména datacenter. Vhodně zvolená virtualizační technologie může mikrosegmentaci plně podporovat. V takovém případě v podstatě není uvnitř datacentra potřeba firewall, protože jej zastoupí virtualizace. Ta jakoby vytvořila malý firewall před každým jednotlivým prvkem, čímž případnému útočníkovi znesnadňuje pohyb z jednoho zařízení na druhé.

K mikrosegmentaci je vhodné navíc pořídit externí firewall, který ochraňuje perimetr

Obrázek 2: Datacentrum s mikrosegmentací



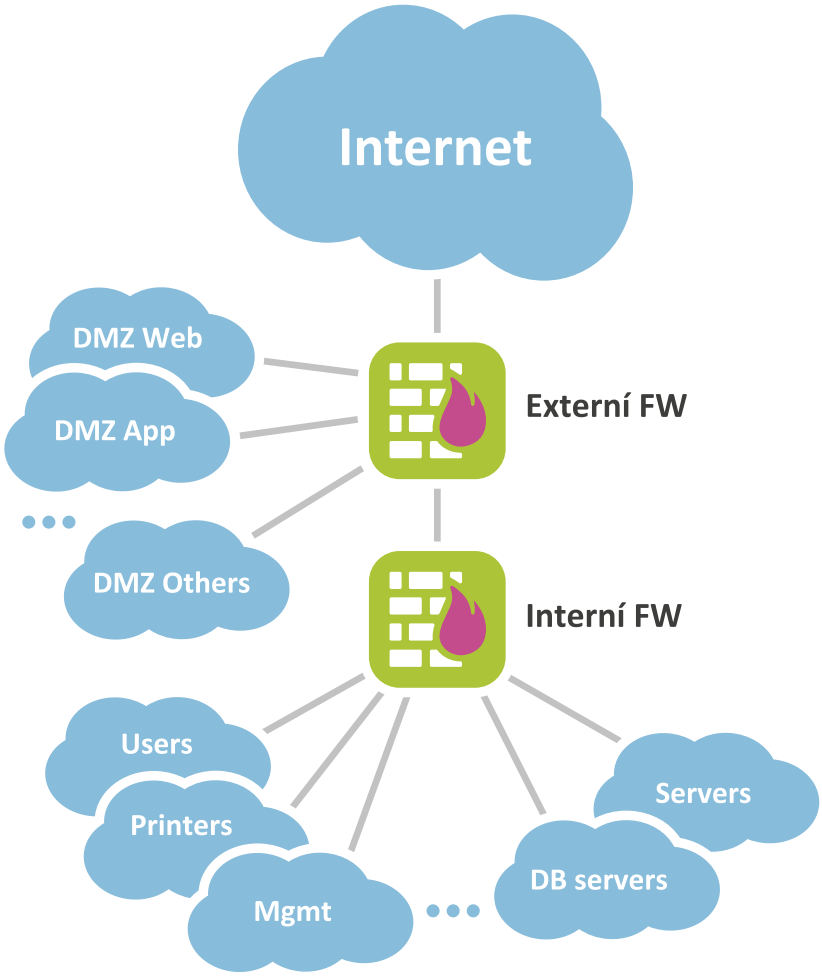
a zároveň zahrnuje řešení pro snadné centrální řízení prostupů (jak na virtualizaci, tak na firewallu). Celkově to ale obvykle vyjde poměrně draho, takže společný výskyt těchto technologií není v naší geografické oblasti moc častý.

Další možností, jak dosáhnout mikrosegmentace, je využití vhodné cloudové technologie. U cloudu je někdy také problém s cenou, ale po propočítání nákladů na jeho alternativy, může nakonec vyjít nejlevněji. Přesto čeká poskytovatele cloudových řešení ještě spousta práce, aby přesvědčili společnosti k tomu, že se vzdají plné kontroly nad svými daty a začnou věřit nějaké třetí straně. Hodně lidí stále na přesun do mraku reaguje klasickým Mrakoplašovským: „To nemůže nikdy fungovat“. Často opravdu ani není možné přesunout celou infrastrukturu do cloudu. Proto se zatím jako nejpravděpodobnější scénář jeví to, že společnosti sice budou mít část infrastruktury v cloudu, ale podstatnější služby a data si ponechají raději u sebe. Ty části sítě, které se do cloudu už podařilo dostat, je možné poměrně dobře segmentovat s pomocí jeho nativních funkcí.

Nyní bych se ale chtěl vrátit k tomu, jak segmentaci dělat, když nemáte prostředky na vhodné technické řešení pro mikrosegmentaci. V tomto případě bude třeba sítě navrhnout rozumně tak, aby ještě bylo možné se v nich vyznat a vytvářet mezi nimi správné prostupy, ale aby nebyly příliš velké, čímž by se snížila bezpečnost.

Většina společností, i když jinak nemá dobře vyřešenou segmentaci, má oddělenou část serverů přístupnou z internetu (DMZ). To je samozřejmě nutnost. Dále je třeba oddělit do samostatných sítí uživatele, IP telefonii, databázové servery, terminálové servery, atd... U každé společnosti je to trochu jiné. Cílem je, aby zařízení v jednom segmentu byla z bezpečnostního hlediska podobná. Tedy aby byl případný útok na ně přibližně stejně náročný, a aby dopady na podařený útok na různá zařízení v rámci jednoho segmentu měla přibližně stejný dopad. Zároveň by zařízení v jednom segmentu měla mít podobná oprávnění v přístupu do ostatních částí sítě, čímž se zjednoduší tvorba bezpečnostní politiky na firewallu.

Častou chybou v segmentaci, se kterou se setkáváme při auditech, je, že společnosti používají třívrstvé modely aplikací (protože si někdo přečetl, že je to tak správné), ale už od sebe tyto vrstvy neoddělují firewallem (to už tam nepsali). Každá část má být ve své podsíti, jinak zaniká velká část bezpečnostních výhod třívrstvého modelu.



Obrázek 3: Segmentovaná síť

Při návrhu celé architektury se také bude potřeba zamyslet nad tím, mezi kterými částmi sítě mají probíhat pokročilé kontroly (IPS a spol.) a kde bude stačit obyčejný stavový firewall. Toto rozhodnutí následně bude důležité pro určení správné výpočetní síly vybíraného řešení. Je dobré počítat také s tím, že firewallů může být v síti více než jeden. Rozdělení úkolů mezi více nezávislých firewallů je vhodné, protože se tím sníží riziko, že jakákoliv chyba na jednom zařízení způsobí kompletní výpadek sítě. Samozřejmostí by mělo být zajištění vysoké dostupnosti pro všechny podstatnější firewallové uzly v síti.

Příprava poptávky

Poté, co dokončíte návrh segmentace sítě, bude potřeba odhadnout, jaký bude mezi jednotlivými segmenty přibližně provoz. Následně bude třeba zvolit vhodný koeficient, kterým tento odhad vynásobit, aby vznikla rezerva. Pak ještě vynásobit předpokládaným růstem společnosti a toto naprosto přesně matematicky vypočítané číslo ještě vhodně upravit tak, aby se vám líbilo.

Pokud už segmenty sítě existují, je vhodné první odhad udělat na základě nějakých měření. Buďto provedete měření na aktivních prvcích, které již v síti máte nebo si půjčíte nějaký firewall a měření provedete na něm. Druhá možnost se může více přiblížit finálnímu zapojení a většinou je proto přesnější. A dá se jí většinou říkat Proove of Concept (PoC), což je výhoda, protože část práce za vás udělá partner nebo výrobce. Pokud máte k dispozici dobrého partnera, firewall vám rád zapůjčí, protože bude mít přesnější data pro následné přesné stanovení výkonnostních parametrů firewallů - sizing. Pokud žádného partnera nemáte, zvažte výhody spolupráce s ním. Půjčí vám firewall a pomůže i v dalších fázích.

Když už máte nějaká čísla, můžete skoro začít poptávat výrobce firewallů a hledat vhodné řešení pro vaši společnost. Ale ještě předtím bude potřeba dát dohromady, co vlastně od výrobku očekáváte. Kromě propustnosti bude potřeba popsat celou řadu parametrů, které musí řešení splňovat, aby vám k něčemu bylo. Například budete muset rozhodnout, zda má řešení poskytovat také

aplikační kontrolu, síťový antivirus, uživatelské VPN, IPS, kontrolu SSL komunikace, vysokou dostupnost a další funkce. Pokud nevíte, jaké funkce potřebujete, opět je dobré to probrat s partnerem nebo výrobcem.

Výběr vhodného řešení

Jakmile poptáte různé dodavatele, aby vám připravili nabídku a návrh zapojení firewallu, můžete si dát nohy na stůl a čekat. Za chvíli vám budou prezentovat svoje řešení. Zjistíte, že každé z nich je nejlepší, zatímco ty ostatní nejlepší zdaleka nejsou. Což je zvláštní paradox, který se v podobných situacích vyskytuje velmi často.

Jak se tedy rozhodnout, když jsou všechna řešení nejlepší, a přitom ta ostatní jsou celkem špatná? Není to jednoduché, ale mělo by to jít. Většina administrátorů si uvědomuje, že důležitá je propustnost a latence firewallu, proto se výrobci předhánějí v tom, aby oni měli tu nejlepší. Z mého pohledu ale zrovna tato vlastnost tak moc vypovídající není. Každé řešení se totiž ukáže za nějakých podmínek jako jedno z nejlepších. Problém je v tom, že udané podmínky pravděpodobně v praxi nebudou splněny a tím pádem hodnoty propustnosti a latence mohou být ve skutečnosti úplně jiné.

Někteří výrobci uvádí mimo jiné i hodnoty pro „skutečný svět“, jenže i ty se mezi výrobci špatně srovnávají, protože metodika, podle které se skutečný svět definuje, může být různá. Výrobce totiž při měření hodnot neví, jak bude vypadat provoz na vaší síti. Jaká část provozu bude webová komunikace? Kolik z provozu bude šifrováno? Jaká část provozu bude tvořena malými pakety a jaká naopak velkými? Někteří výrobci vycházejí ze statistiky. Jenže proti statistice se vždycky dají použít Murphyho zákony, které způsobí, že zrovna u vás to bude jinak. To znamená, že hodnoty nemusí být na vaši síť příliš aplikovatelné. A pak jsou zde ještě různé finty, díky kterým někteří výrobci mají lepší výsledky než jiní. Jde například o to, že mají při měření vypnuté něco, co by ale mělo být ve skutečnosti zapnuté. Nebo možná má výrobek výjimečně dobré hodnoty při samotném „firewallování“, ale jakmile zapnete jakoukoli pokročilejší funkci, tak se výhoda ztratí a naopak je výsledek horší než u ostatních řešení.

Tyto důvody jsou podle mě dostatečné k tomu, abychom se při výběru firewallových řešení zaměřili na jiné vlastnosti výrobků, než je propustnost a latence. Ty sice ze zřetele úplně pustit nemůžeme, ale nejsou zase tolik podstatné. Nejlepší bude si nechat nějaký sizing doporučit, vyzkoušet jej, a pokud nebude splňovat požadavky, vrátit ho dodavateli jako nevyhovující.

Při výběru firewallu je naopak dobré se zaměřit na to, jestli řešení splňuje všechny požadavky na různé funkce, které jste si na začátku vydefinovali. A tím nemyslím ty, jež píše, že splňuje, ale ty, které opravdu splňuje. Ideální je, nechat si udělat demo, při kterém si ty nejdůležitější věci vyzkoušíte nebo necháte předvést.

Výše zmíněné funkce jsou důležité, ale stejně vás nejspíše moc nepřiblíží k tomu, jaké řešení si vybrat. Důvod je ten, že velcí výrobci spolu drží krok a zásadní vlastnosti produktů mají nějakým způsobem integrované všichni.

Tím se dostáváme k tomu, co považuji za nejdůležitější kritérium výběru - to, jak se vám s celým produktem pracuje. Opět doporučuji, nechat si udělat demo, na kterém ověříte, jak se produkt ovládá. Nechte jej otestovat co nejvíce lidmi, kteří s ním poté budou pracovat. Zaměřte se na to, jak dlouho vám trvají základní úkony, které se provádí stále dokola. Uvažte, jak dobře se vám pracuje s firewallovými logy. Jak snadné nebo složité je vrátit se k předchozím verzím politiky. Jak je možné pracovat s uživatelskými identitami místo IP adres. Jak moc granulárně lze všechno řídit. Jak intuitivní pro vás prostředí je. Jak hodně se vám při ovládání produktu chce prohodit klávesnici monitorem. Nechte si od partnera nebo výrobce ukázat to, jakým způsobem se provádějí běžné úkony. Podle mě by se do popředí vašeho výběru mělo dostat takové řešení, se kterým se vám pracuje dobře. Pokud se totiž řešení dobře ovládá, stráví administrátoři kratší čas učením, děláním chyb a celkově prací s firewallem.

Jestliže stále ještě váháte mezi několika řešeními, můžete se rozhodnout podle jejich bezpečnosti. Jde o bezpečnostní řešení, takže by nemělo být samo o sobě děravé jako cedník. Pokud jste horko těžko rozsegmentovali síť a oddělili jednotlivé segmenty firewally, veškerá vaše práce přijde vniveč, když ty firewally někdo úspěšně napadne a dostane se z nich do všech částí sítě. Jak ale poznat, které řešení je bezpečnější? Všechny výrobky mají nebo měly nějaké zranitelnosti. Můžeme se ale podívat na to, kolik se jich našlo. Pokud jich má nějaké řešení významně jiný počet než všechna ostatní, už to něco vypovídá o tom, jakým způsobem je vyvíjeno. Co by dále mohla být zajímavá informace, je, jak rychle jsou u daného výrobku nalezené zranitelnosti opravovány. Pokud se chyby opravují jednou za půl roku, výrobce asi bezpečnosti nedává vysokou prioritu a výrobek lze jen těžko považovat za bezpečný.

Další velmi důležitou vlastností je stabilita řešení. Jak často se stane, že se najde nějaká chyba, kterou musí řešit support výrobce? Jak často dojde k tomu, že se firewall zachová nějak nepředvídatelně? Toto je velmi důležité. Bohužel tyto informace nelze od výrobců zjistit. Je lepší se obrátit spíše na ostatní uživatele firewallů a na internet. I když v obou případech mohou být informace dost zkreslené kvůli nějakým náhodným incidentům, které se někomu staly. Je třeba brát v úvahu, že o dobrých věcech se většinou moc nemluví a nepíše. Zato jakmile je někde nějaká chyba, najdete o ní zmínku téměř všude. Případně vám opět může pomoci partner, který typicky spolupracuje s více výrobci a dobře je zná. Samozřejmě i zde mohou být informace zkreslené, protože partner může mít také své vlastní zájmy. Toto nebezpečí ale není tak vysoké, protože dobrý partner se snaží zákazníkovi skutečně pomáhat, aby s ním mohl navázat dlouhodobější spolupráci, což by se nepodařilo, pokud by mu od začátku špatně radil.

Zatím jsme mluvili jen o tom, jak zvolit řešení od nějakého výrobce. Je ale třeba zmínit i to, že stejný výrobek je možné použít různými způsoby. Je možné navrhnout použití appliance či virtuální appliance od výrobce nebo například serveru, na který se instaluje firewallový software. Případně může být navržena virtualizace na úrovni daného řešení místo na hypervizoru třetí strany. V tomto článku se nedozvíte, jaká varianta je nejlepší, protože to je velmi závislé jak na situaci, tak na zvoleném firewallovém řešení. Celkově lze jen doporučit to, že pokud hodláte využít virtualizaci pro bezpečnostní brány, měly by mít pro sebe vyhrazené samostatné servery.

Implementace

Řekněme, že se vám po různých peripetiích podařilo nakonec nějaké řešení vybrat. Nyní zjistíte, že až doteď to bylo v podstatě jednoduché, protože teď přichází implementace. Jenže jak ji naplánovat? Co k tomu bude potřeba? Jak dlouho to asi bude trvat?

Ať už provádíte výměnu firewallu nebo instalaci na čisté louce, je potřeba si uvědomit, že se bude pravděpodobně jednat o poměrně náročný projekt. Každý projekt je totiž náročný, nebo je aspoň dobré to o něm říkat. Samozřejmě, pokud se instaluje jen malý firewall na pobočku, nebude to tak složité jako instalace centrálního clusteru.

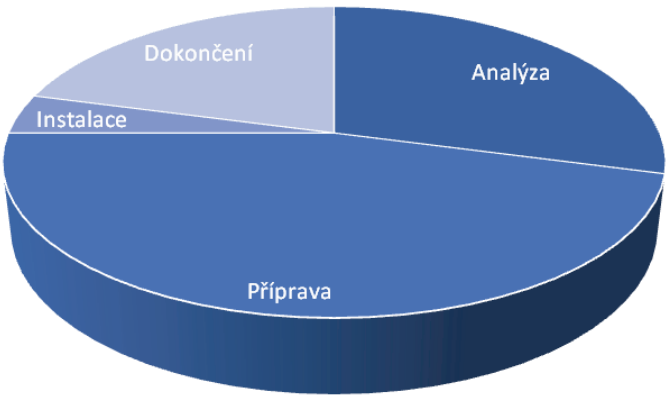
Obrázek 4: Implementace firewallového řešení

U větších implementací bude potřeba nejprve vše dobře naplánovat. Bude potřeba popsat stávající síť a úplně přesně naplánovat, jak má vypadat na konci projektu. Bude potřeba zajistit vše od místa v racku, přes adresní plán a routing, až po konfiguraci všech připojených VPN. Bude nutné naplánovat co největší část celé operace. I v případě, že si necháte od někoho implementaci udělat, připravte se na to, že vás čeká spoustu práce s dodáváním různých vstupních informací.

Pokud nemáte před implementací v ruce plán celé implementace, kterému rozumíte, tak ji raději odložte nebo zrušte. V takovém případě se totiž můžete podívat k obzoru. To co tam uvidíte, jsou blížící se problémy.

Když máte v ruce plán, začíná konfigurační část projektu. Většina konfigurace se dá připravit ještě před tím, než se zmigruje na nový firewall. A když říkám většina, tak myslím naprostá většina až skoro všechno. To znamená, že část přípravy je nejdelší a nejpracnější. Ale nebývá ani zdaleka tou nejdůležitější ani nejtěžší. To nejtěžší už totiž máte za sebou, pokud držíte v ruce dobře připravený plán celé implementace. Pokud jej stále nemáte, tak jste se do této fáze vůbec neměli dostat, viz předchozí odstavec. Plán by mimo jiné měl obsahovat i informace pro přípravu, takže ta je více méně jen jednoduché postupování podle návodu.

Obrázek 5: Poměrná doba částí implementace



Po přípravě už následuje samotná instalace nového firewallu. Odteď budete fungovat na novém řešení. Ale před tím vás čeká ještě jeden či více pracovních víkendů. Nezapomeňte si na instalaci připravit svačinu. Přes to, že instalace bývá ta nejkratší část celého projektu, je to obvykle ta nejnepříjemnější a pocitově se jako nejdelší může jevit. Ovšem v případě, že máte k dispozici špičkový catering, může tomu být přesně naopak.

Poté, co se do sítě nasadí nový firewall, můžete očekávat pár dní, kdy vám bude neustále vyzvánět telefon, pokud si ovšem moudře nevypnete vyzvánění. Nikdo nemůže očekávat, že se po instalaci nevyskytnou žádné problémy. Za prvé je tu pořád ten Murphy a za druhé tentokrát statistika mluví v jeho prospěch, takže k problémům prostě dojít musí. Je potřeba mít připravené kapacity, které problémy vyřeší. V ideálním případě by to neměl být ten samý člověk, který strávil celý víkend v práci. Na druhou stranu je potřeba, aby kapacity byly o průběhu akce patřičně informovány, aby měly od čeho se při řešení problémů odrazit.

Jakmile se situace trochu uklidní, zbývá ještě nastavit pokročilé funkce, které jsou po migraci buďto přepnuté jen na detekci nebo úplně vypnuté. Toto již nebývá tak složité, ale obvykle to trvá neúměrně dlouho. Důvod je ten, že účastníci projektu ztrácí ten správný drive a přestanou tlačit na jeho dokončení. Jakmile se ale dodělají i tyto detaily, je v podstatě hotovo. V síti máte nový firewall a můžete sklízet ovoce své práce.

Ještě jste se vlastně ptali, jak dlouho to celé bude trvat. Samozřejmě není možné na to dát jednoznačnou odpověď. Je ale dobré počítat s delší dobou, než jakou na první pohled odhadujete. Typicky se podceňuje náročnost první fáze, kdy je potřeba všechno naplánovat. Jenže to je ta nejdůležitější a nejtěžší část celé operace, takže je potřeba si na to vyhradit dost času. Pokud implementaci neděláte sami, ale máte partnera, který vám s ní pomůže, uvědomte si, že stejně bude potřeba spousta vaší práce. Celkový čas projektu je závislý i na tom, jak rychle budete dodávat potřebné informace. Abyste měli přibližný odhad, jak dlouho může implementace firewallového řešení trvat, jde podle mého názoru přibližně o 2-3 měsíce na jeden firewallový cluster s management serverem. Opět je zde spoustu proměnných, takže se odhad může velmi změnit.

I když se implementace firewallu může zdát jako náročná záležitost, věřte, že jí také skutečně je. Ale není třeba se obávat. Tak po sedmém osmém pokusu se do toho dostanete a budete firewally stavět jak na běžícím páse. Oproti jiným technologiím je firewall nepříjemný v tom, že jeho výpadek obvykle znamená výpadek značného množství síťových služeb, ne-li přímo všech. A to zase znamená, že se zastaví většina aktivity ve firmě, což je často poměrně drahá záležitost. Proto je dobré mít někoho, kdo implementaci správně připraví a provede. Pokud nikoho takového ve firmě nemáte, nebojte se sáhnout po externích zdrojích. Ať už implementaci firewallů budete provádět sami nebo s někým, přeji vám, ať se úspěšně podaří. Je to vždy příjemný pocit dokončit úspěšně takový náročný projekt. ■

Lukáš Solil

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