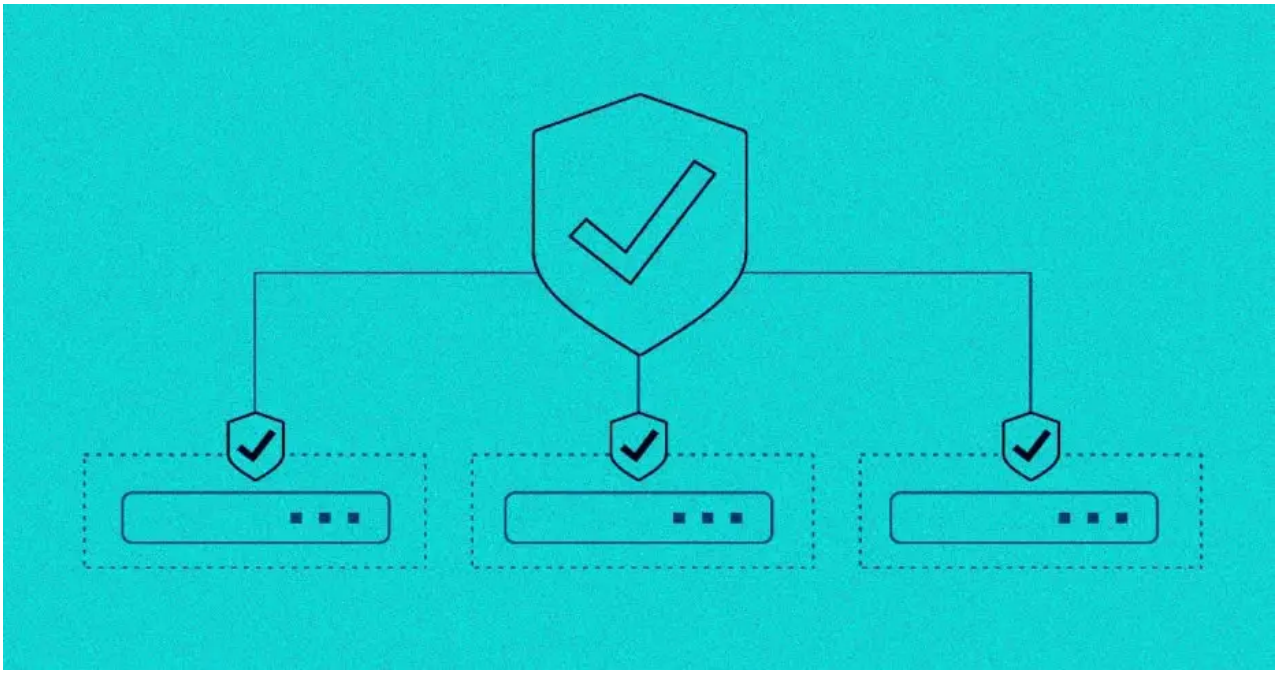
Mikrosegmentace sítí: Proč jsou bezpečnější

itigic.com/cs/microsegmentation-of-networks-why-safer

Matt Mills April 20, 2020

Síťové architektury a jejich tradiční modely řízení pozvolna zaostávají. Tato příručka vám ukáže základy **mikrosegmentace** a jak se přizpůsobuje těmto novým síťovým architekturám, které pracují s více cloudovými službami a virtualizací. Jedním z jeho nejvýznamnějších rysů je mnohem vyšší úroveň zabezpečení.

Co je to mikrosegmentace?



Jedná se o typ segmentace sítě, který je konkrétně zaměřen na řešení kritických problémů, s nimiž se musí zabývat **ochrana sítě** . Hlavním cílem je snížit rizika útoků a přizpůsobit bezpečnostní opatření požadavkům použití. Mikrosegmentace je moderní přístup, který poskytuje sítím vyšší zabezpečení, do značné míry v souladu s dynamickými prostředími informačních technologií.

Síť bezpečnost již není v jeho řízení volitelnou záležitostí, tento segmentační model je praktičtější a snadnější způsob, jak začít přijímat **Nulová důvěra** model v sítích. Nezapomeňte, že posledně

jmenované spočívá v aplikaci všech řízení přístupu, autentizace a dalších, na všechny uživatele stejně, bez rozlišení rolí a funkcí v organizaci.

Jak to funguje

Mikrosegmentace platí pro každého člena a **jedinečné a centralizované** síťová politika. To umožňuje implementaci síťových zásad, které přesahují to, kde jsou lidé. To znamená, že již nezávisí na tom, kde je uživatel připojen. Nyní záleží na tom, zda je uživatel skutečně připojen. Tento způsob uplatňování síťových zásad je nezbytný, protože cloudové služby jsou stále více přijímány a tyto samozřejmě samozřejmě přesahují hranice dané sítě.

I když je zřejmé, mikrosegmentace je zaměřena na konečné uživatele. Zejména kvůli skutečnosti, že velká část událostí, které ohrožují zabezpečení sítě, pochází ze zařízení uvedených koncových uživatelů. Jinými slovy, tento způsob správy sítí není omezen na obrovské podnikové infrastruktury, jako jsou datová centra.

Typy mikrosegmentace

Hostitelský agent

To je zaměřeno na koncové uživatele. Všechna data procházející sítí procházejí zařízením, které funguje jako **centrální manažer** . Jednou z hlavních výhod je, že nemusíte objevovat a dešifrovat algoritmy a / nebo šifrovací protokoly, které provoz má. Aby však tato strategie mikrosegmentace mohla naplno využít svůj potenciál, musí být na všech hostitelích v síti nainstalován specializovaný software. Je také důležité vědět, že použitím typu Host-agent bude možné zabránit událostem zabezpečení v síti ještě předtím, než hostitel vstoupí do samotné sítě.

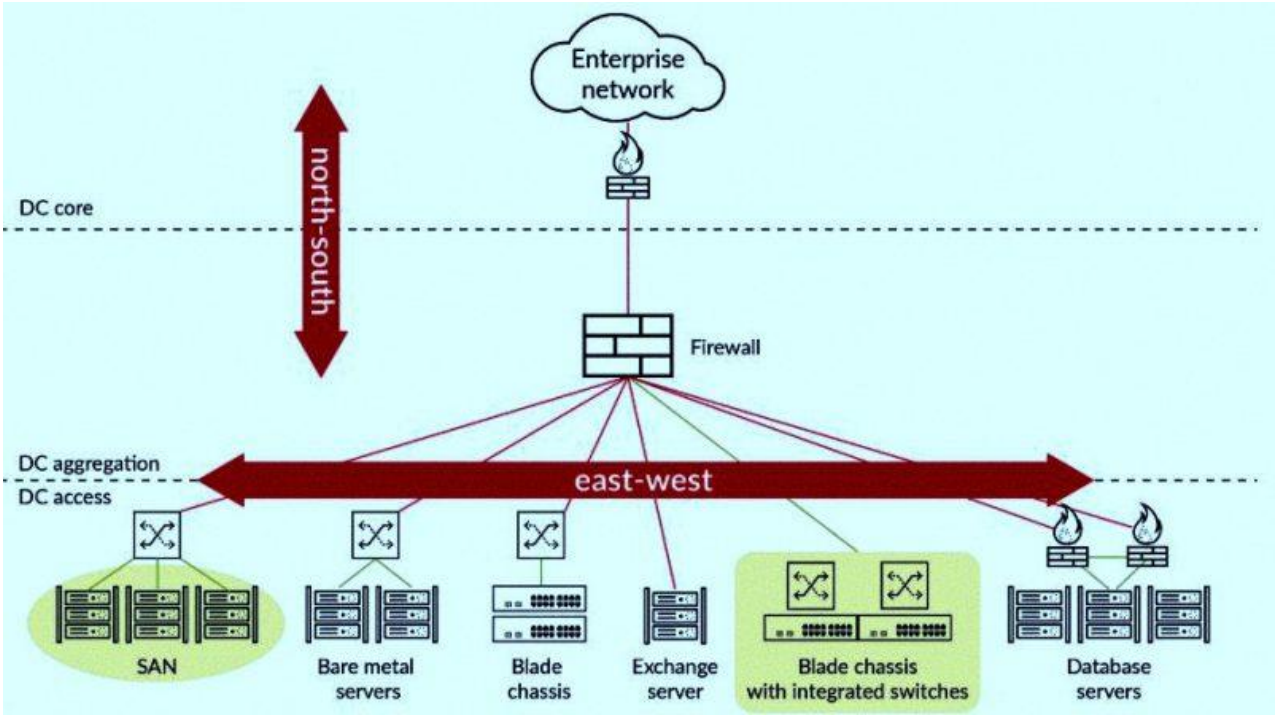
Na základě hypervizorů

Co je hypervisor? Je jádrem mnoha technologií virtualizace hardwaru. Zodpovídají za nasazení a správu hostovaného operačního systému, tj. Virtualizovaného. Výhodou implementace mikrosegmentace s hypervizory je to, že již lze použít již implementované brány firewall, kromě migrace stávajících síťových zásad na stejné hypervizory nebo jiné, v závislosti na tom, jak síťová aktivita migruje na tento model řízení.

Tento model však není nejvíce doporučován. Protože to nefunguje úplně v cloudových prostředích, kontejnerech nebo holých kovových hypervizorech (těch, které jsou nainstalovány na samotném počítačovém hardwaru a odtud, je virtualizace prováděna).

Můžeme také uvést jiný model, který je považován za **rozšíření tradičního řízení sítě** . Která například zahrnuje segmentaci na základě **Seznamy řízení přístupu** a další metody. Podle odborníků je to nejjednodušší model pro přijetí, protože se nejedná o „náhlou“ změnu ve způsobu řízení sítě. Problémy však mohou začít od okamžiku, kdy chcete přijmout mikrosegmentaci do velmi velkých segmentů sítě. Je tomu tak proto, že při řízení a poskytování podpory událostí je vyžadováno mnoho finančních zdrojů a specializovaný personál.

Proč je mikrosegmentace bezpečnější?



Palo Alto Networks vysvětluje význam mikrosegmentace v kontextu síťového provozu „sever-jih“ **(Sever-Jih v grafu)** a „východ-západ“ **(East-West v grafu)** . Segmentace sítě, jak ji známe, funguje nejlépe, pokud jde o provoz sever-jih, který zahrnuje komunikaci typu server-klient v celé síti. Dnes jsou síťové architektury obecně obnovovány díky cloudovým službám a jejich kombinace je známá jako **hybridní architektura** . Ten má větší síťový provoz z východu na západ, tj. Komunikaci mezi servery.

Graf, který jsme sdíleli výše, ukazuje, jak **velká část síťového provozu** dochází s rychlostí východ-západ. Vidíme servery věnované sítím Storage Area Networks (sítě SAN) a serverům Exchange (nebo jiným vyhrazeným pro e-maily). Můžeme také vidět servery věnované fungování jako databáze, které jsou obklopeny firewally.

Dalším bodem ve prospěch mikrosegmentace je rostoucí využívání virtuálních strojů a dalších virtualizačních metod. Pamatujte, že je možné, že jediný server může hostit více virtualizací, z nichž každá má odpovídající pracovní vytížení a požadavky na zabezpečení. Tento obnovený způsob segmentace zlepšuje bezpečnostní opatření na granulární úrovni, tj. Podle každé složky sítě.

Úvahy před provedením

Před provedením investice do implementace mikrosegmentace sítě jsou nezbytné. Doporučuje se mít **ovládání s vysokou úrovní detailů** ve vztahu ke které síťové architektuře se používá, kromě toho, které systémy a aplikace se používají. Na druhé straně musíte vědět, jak systémy spolu komunikují.

K tomu je třeba provést analýzu se všemi zúčastněnými stranami. Zejména pokud mluvíme o velké síti, která má kritické operace, které jsou prováděny denně. Je dokonce možné provést tuto analýzu s podporou poskytovatele. Tímto způsobem bude mnohem snazší identifikovat body, kde budou mikrosegmenty nainstalovány. Zde je nejdůležitější vyhnout se, pokud je to možné, aby nedocházelo k poklesu funkčnosti sítě.