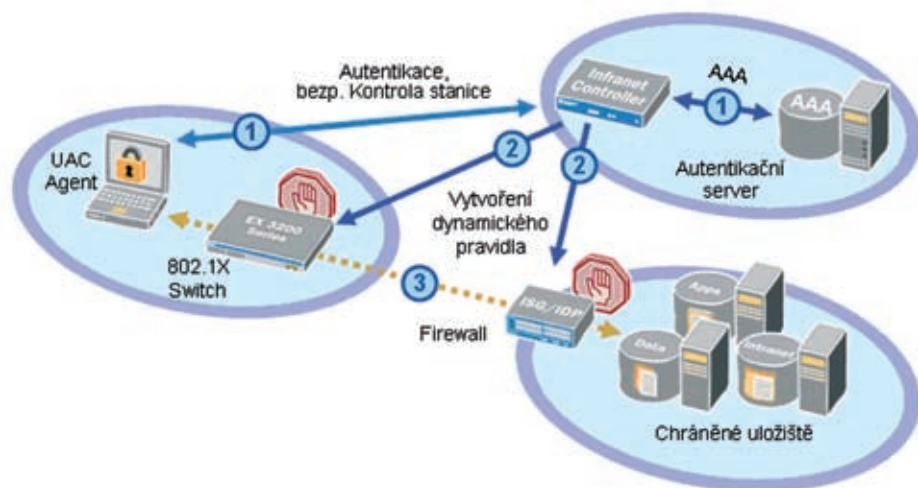


Unified Access Control

Bezpečné řízení přístupu v prostředí LAN

Magická slovíčka NAC (Network Access Control) už možná slyšel ne jeden z Vás. Tato třípísmenná zkratka jednoduše označuje řízení přístupu na úrovni lokální sítě pomocí specializovaného centrálního zařízení. U Juniper Networks k tomuto účelu používáme produkt Infranet Controller, který dokáže na základě autentikace koncové stanice a výsledku bezpečnostní kontroly odemknout porty na přístupových switchích. Společnost Juniper Networks jde jako jediná v této technologii ještě dál a začlenila do řízení přístupu také dynamické zadávání pravidel na lokálních firewallech, čímž ještě zvýšila úroveň bezpečnosti síťových zdrojů.



V dnešní době je již problematika ochrany sítě z internetu často vyřešena, proto je potřeba zaměřit se také na síť uvnitř. Výše zmíněné zařízení vyšlo z každodenních potřeb chránit nejenom síťová data, ale i lokální počítače mezi sebou proti nejrůznějším druhům škodlivého kódu. Jednoduchý příklad z každodenního života může být následující:

Spousta uživatelů stále více využívá místo pracovních stanic laptopy. Zaměstnanci na nich pracují nejenom v prostředí korporace, ale častěji i doma. Zcela bez obav na laptotech nechávají hrát hry a brouzdat po internetu své děti, které nevědomky stáhnou do počítače spoustu škodlivého kódu. Zejména tím zcela reálně vystavují korporátní síť nebezpečí v momentě, kdy uživatelé přinesou laptop zpět a zapojí jej do segmentu korporátní sítě. V tu chvíli může dojít k rozšíření nákazy v podobě trojských koňů, červů, virů atd. Že vám tato situace přijde povědomá? Může být...

Juniper Networks je společnost, která bezpečnost nikdy nebrala na lehkou váhu. Když v roce 2006 provedla akvizici společnosti Funk software, bylo jen otázkou času, kdy se jejich produkty řady Steel Belted Radius (SBR) objeví jako jeden ze stavebních kamenů právě

v technologii NAC. Tak se stalo v roce 2007 a od té doby nabízí NAC technologie kontrolu přístupu na L2 až L7.

Popis celé technologie je na dlouhé povídání, proto bych rád objasnil princip činnosti založený na prvcích Juniper Networks a také výhody tohoto řešení.

Základní kameny

Celá infrastruktura je rozdělena do třech částí:

- Infranet Controller (IC) – prvek jenž ověřuje uživatele proti SBR a dokáže řídit přístupové switche a firewally
- Infranet Enforcer (IF) – přístupový switch EX řady s podporou 802.1x, popř. firewall řady NS, SSG, ISG
- Infranet Agent (IA) – suplicant nainstalovaný na koncové stanici

V praxi pak řízení přístupu vypadá tak, že uživatel zapojí laptop nebo svůj desktop do lokální sítě, kde si nainstalovaný suplicant vyhledá nejbližší Infranet Controller a pokusí se na něm autentikovat. To vše zatím probíhá na druhé síťové vrstvě bez přidělení IP adresy za pomoci EAP-JUAC protokolu. Jakmile IC ověří jeho identitu, provede na koncové stanici kontrolu bezpečnosti tzv. HOST CHECK

a na základě jejího výsledku pak rozhodne, do jaké VLAN nebo části sítě dotyčnou stanicí vypustí. Tento mechanismus má obrovskou výhodu v tom, že v případě, kdy uživatel nesplní některou z podmínek nadefinovanou administrátorem UAC, má možnost dostat přidělenou VLAN, ve které může napravit nedostatky své stanice, např. provést patch operačního systému, nainstalovat si novou antivirovou bázi apod. Podmínky pro kontrolu jsou naprosto flexibilní bez ohledu na použití operačního systému stanice. Juniper IC podporuje všechny dostupné verze Windows (včetně 64-bitové Visty), Linux, Solaris a Mac OS. Úspěšná bezpečnostní kontrola pak díky radius atributům odemkne port, přidělí IP adresu z DHCP serveru a dovolí přistoupit stanicí do lokální sítě.

U Juniper Networks je výše popsán postup velmi podobný konkurenčním řešením. Nicméně Juniper jde ještě dál a k řízení přístupu na druhé síťové vrstvě přidává ovládání také vrstvy třetí, kterou je ovládání firewallů. Praxe je opět taková, že tyto firewally mohou být jako druhá nebo chcete-li třetí vrstva obrany. První vrstvou je bezpečnostní kontrola koncového bodu (včetně kontroly na Malware), druhou pak řízení druhé síťové vrstvy pomocí 802.1x na přístupových bodech a třetí pak řízení firewallů na L3 třeba s nánástavbou až do sedmé síťové vrstvy L7. Tato třetí vrstva je také ovládána IC, který

na základě ověření uživatele zjistí jeho zdrojovou IP adresu, dále pak do kterých částí sítě mu administrátor povolí přístup a konečně na jakých portech. Tím se vytvoří dočasné pravidlo a uživatel může komunikovat do požadované destinace. Není nereálný příklad, kdy na hranici demilitarizované zóny a internetu může být použit firewall zcela bez jediného pravidla. Tento pak řídí IC a pomocí SSH tak dynamicky pravidla vytváří. Po skončení session je pak okamžitě smaže.

Výhody řešení Juniper Networks

- Veškeré rozhodování a kontroly koncových stanic zajišťuje jedno zařízení Infranet Controller
- Možnost naimportovat radius knihovny také ostatních výrobců 802.1x zařízení
- Možnost autentikovat na základě MAC adresy také neříditelná zařízení (telefony, tiskárny)
- Podpora všech běžných operačních systémů
- Bezpečnostní kontrola koncových bodů již na druhé síťové vrstvě
- Integrovaný radius server
- Rozšířená sada EAP autentikačních metod
- Kooperace s IPS sondami
- Podpora kontrolních mechanismů třetích stran
- Segmentace uživatelů do oblastí (realm) a rolí (roles)

- Podpora Shavlik NetCheck patch manageru
- Jednotný centrální management Network and Security Manager 2008
- Podpora roamingu
- Autentikace pomocí certifikátu

Úplně nakonec jsem si nechal jednu velmi důležitou vlastnost a to je centrální management software Network and Security Manager 2008. Tento jedinečný nástroj dokáže spravovat až 6000 Juniper zařízení současně. Z jednoho místa pak můžete provádět nastavování, reporting, vyšetřování logu, korelaci apod. Více o tomto ojedinělém nástroji, jenž spojuje svět networkingu a bezpečnosti, se dozvíte na jiném místě tohoto magazínu.

Více informací naleznete na www.soft-tronik.cz