

White Paper

Význam standardů pro řízení síťového přístupu



Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408.745.2000
1.888 JUNIPER
www.juniper.net

Obsah

Úvod	3
Standardní versus proprietární řízení síťového přístupu	3
Co je TNC (Trusted Network Connect)	5
Jak TNC funguje	5
Architektura TNC založená na standardech	6
Technologie UAC (Unified Access Control) od Juniper Network	8
UAC & TNC	9
Shrnutí	10

Úvod

Uživatelé dnes potřebují mít přístup do podnikové sítě odkudkoliv ve světě, v kteroukoliv denní dobu a přes bezpočet přístupových technologií a zařízení s nejrůznějšími operačními systémy, operačními prostředím a aplikacemi.

V tomto globálně dynamickém a odlišném světě obvykle síťoví administrátoři nemají ponětí, kde bylo řízené či neřízené zařízení nějakého uživatele předtím, než se uživatel pokusil dostat do podnikové sítě. Zařízení tohoto uživatele mohlo být nakaženo nějakou zákeřnou formou škodlivého softwaru – malwaru – produkovaného dnešními sofistikovanými a velmi dobře financovanými počítačovými hackery. Zařízení uživatele by tak mohlo sloužit jako zprostředkovatel pro transfer viru, spyware, adware, tzv. trojských koní, červů, rootkitů a dalších škodlivých aplikací do podnikové sítě nebo přímo do dalších nic netušících uživatelských zařízení.

A proto vstupuje na scénu řízení síťového přístupu. Neexistuje sice univerzálně schválená definice řízení síťového přístupu (Network Access Control), ale v zásadě se jedná o schopnost kontrolovat a řídit přístup do sítě na základě souladu s určitými síťovými politikami (pravidly, zásadami). Síťové politiky, se kterými je vyžadován soulad, mohou zahrnovat politiky založené na identitě uživatelů, identitě zařízení, stavu zařízení nebo umístění zařízení – abychom jmenovali alespoň některé. Řízení síťového přístupu umí zajistit, aby bylo navázáno odpovídající spojení do odpovídající sítě a odpovídajícím způsobem - jak z hlediska uživatele tak z hlediska zařízení. Dále lze pomocí řízení síťového přístupu zajistit, aby uživatelé vyhovovali určitým politikám (pravidlům, zásadám) autentizace, aby jejich zařízení splňovala požadavky autentizačních a bezpečnostních politik a aby uživatelé a zařízení byli v souladu i s dalšími politikami nastavenými v dané organizaci.

Vzhledem k šíři záběru funkcí řešení pro řízení síťového přístupu tato řešení často přesahují oddělení podnikové počítačové sítě a zasahují do řady interních podnikových jednotek a úseků. Implementace řízení síťového přístupu se týká jednak všech IT oborů, od správy uživatelských počítačů po bezpečnost uživatelských PC, od síťové infrastruktury po administraci sítě. Může také zahrnovat osoby a zdroje, které zajišťují pro organizaci soulad s legislativními požadavky, neboť řízení síťového přístupu úzce souvisí s některými problémy při zajištění souladu s právními normami a dalšími předpisy. Kromě různých organizačních oddělení a skupin zapojených do rozhodovacího procesu kolem řízení síťového přístupu existuje dále i řada uživatelských zařízení a hardwarových a softwarových komponent síťové infrastruktury, na které budou mít tato rozhodnutí významné dopady.

Vezmeme-li v úvahu, jak širokou oblastí je řízení síťového přístupu, od počtu a variantnosti uživatelských zařízení a infrastrukturních komponent přímo ovlivňovaných zavedením této technologie po počet úseků organizace zahrnutých do rozhodovacího procesu ohledně řízení síťového přístupu, je zřejmé, že rozhodnutí mezi standardním nebo proprietárním řešením řízení síťového přístupu má pro podnik kritický význam.

Standardní versus proprietární řízení síťového přístupu

Podle výkladového Merriam-Websterova slovníku je „standard“ definován jako „něco, co je zavedeno státní institucí, zvyklostmi nebo obecným souhlasem jako model nebo vzor.“ Slovo „proprietární“ je naopak definováno jako „něco, co je používáno, vyráběno nebo prodáváno v rámci výhradního zákonného práva vynálezce nebo výrobce.“ Tyto definice platí také pro svět síťových technologií.

V technickém kontextu je „standard“ obvykle definován jako soubor specifikací nebo směrnic ohledně interoperability (vzájemné spolupráce a fungování výrobku či technologie), které byly dohodnuty, přijaty či schváleny všeobecně (univerzálně), anebo velkou skupinou zainteresovaných stran. „Otevřenými standardy“ jsou pak ty sady směrnic pro interoperabilitu, které jsou veřejně dostupné a mohou být použity kýmkoliv, kdo se takto rozhodne. Standardy obsahují parametry konkrétních produktů, ale také koncepty kompatibility, interoperability a dohod.

V oblasti řízení síťového přístupu je k dispozici řada řešení, ale většina řešení pro řízení síťového přístupu je buď zcela nebo zčásti proprietární. Přestože z krátkodobého hlediska se mohou proprietární řešení řízení síťového přístupu jevit jako atraktivní, z dlouhodobého hlediska bývají pro podnik velmi nákladná.

Prakticky každá skupina nebo organizace může prohlásit, že její specifikace nebo směrnice jsou „standardem“. Avšak pokud tyto specifikace či směrnice nebyly dány k dispozici veřejnosti pro všeobecné použití a přijetí, bez nějakých omezení nebo limitů v podobě licenčních podmínek či uživatelských poplatků, pak nemohou představovat skutečný „standard“. Uživatelé by si měli dávat pozor na specifikace, které se zdají být standardem, nebo jsou jako standard deklarovány, ale ve skutečnosti se jedná o proprietární technologie. Omezení přitom může spočívat v použití těchto specifikací, které slouží spíše zájmům tvůrce specifikace, nikoliv uživatele.

Obdobně může nějaký výrobce úspěšně nalákat velký počet společností, aby přijaly určitou jeho privátní specifikaci, ale tím se z této specifikace nestává otevřený standard. Pokud není specifikace otevřeně publikována za účelem veřejného použití a revize, pokud nebyla všeobecně přijata a odsouhlasena skupinou podobně zaměřených zúčastněných stran a pokud není její použití nijak omezeno, nemůže se nazývat standardem. Je vlastněna a kontrolována privátně, a tudíž je podle definice proprietární.

Existuje spousta pádných důvodů, proč by měla organizace při svém rozhodování o tom, jaké řešení pro řízení přístupu do své sítě použije, uvažovat o řešení založeném na standardech. Standard zdůrazňuje interoperabilitu mezi komponentami. Standard dále poskytuje interoperabilitu s jinými technologiemi a produkty, a tak umožňuje, aby si organizace zvolila ty produkty a řešení, které jsou pro ni nejvhodnější, a přitom bude mít zaručeno, že budou vzájemně spolupracovat. Zavedení proprietárního řešení naopak může snížit tuto flexibilitu a zvýšit celkové náklady na vlastnictví systému (TCO), neboť organizace má omezený výběr produktů a nemůže vytvářet heterogenní prostředí založené na těch nejlepších technologiích.

U většiny organizací se rozhodování o tom, zda zvolit a implementovat standardní nebo proprietární řešení, soustředí do několika klíčových faktorů:

1. Organizace potřebuje určit, jakou hodnotu přinese daná technologie – ať proprietární nebo založená na standardech – jejímu podnikání. Jedním z faktorů je, zda řešení poskytne okamžitou úsporu nákladů. Standardy jsou životně důležité pro organizace, které se chtějí vyhnout tomu, že budou závislé pouze na technologii, produktech či podpoře jediného výrobce (dodavatele). Pokud organizace zvolí technologii založenou na standardech, nemusí se obávat nepřiměřeného zvyšování cen nebo jiných jednostranných nátlakových akcí, které může dodavatel podniknout.
2. Dalším důležitým faktorem je doba, práce a náklady potřebné na integraci, otestování a zavedení zvoleného řešení, a dále to, zda standardní nebo proprietární řešení pomáhá při snížení těchto nákladů. Díky standardům mohou být technologie otevřené a všeobecně přístupné a typicky poskytují organizacím, které standardní technologie implementují, možnost vybrat si z různých dodavatelů. Přínosy plynoucí z této výhody se pochopitelně zvyšují s tím, jak se zvyšuje počet interoperabilních prvků v rámci celkového řešení. Řešení založená na standardech mohou snížit celkové náklady na vlastnictví (TCO) a současně organizaci poskytují svobodu zvolit si technologie, které chtějí používat a integrovat. Použití a implementace standardů se rovná hodnotě a svobodě volby.
3. Řešení pro řízení síťového přístupu v sobě integrují řadu uživatelů, zařízení a technologií týkajících se bezpečnosti a kontroly síťového provozu. Zejména k nim patří tzv. oblast AAA (Authentication, Authorization, Accounting) tj. technologie autentizace, autorizace a účtování přístupů, dále technologie pro integritu koncových bodů, prosazování a řízení síťových politik, pro realizaci karantén a nápravy. Řešení řízení přístupu na bázi standardů tyto technologie hladce integruje, a propojuje tak i různé organizační úseky zodpovědné za kontrolu nad implementací těchto technologií, jako je provoz a administrace sítě, bezpečnostní operace, správa uživatelských počítačů, správa RADIUS serverů neboli identit a soulad s právními normami. Volbou řešení řízení síťového provozu založeného na standardech může organizace současně integrovat několik technologií a zároveň skupiny a úseky kritické pro úspěšnou implementaci a zavedení těchto technologií.

4. Řízení přístupu má rovněž svůj díl standardů a protokolů, které zajišťují kompatibilitu a interoperabilitu. K těmto standardům a protokolům patří protokol RADIUS, protokol EAP (Extensible Authentication Protocol) a protokol 802.1X. Standard 802.1X, což je IEEE standard pro řízení síťového přístupu na bázi portů přizpůsobený pro prostředí velkých podniků, poskytuje silný základ pro autentizaci, řízení přístupu a zajištění privátnosti dat. Standard 802.1X sám o sobě využívá také další standardy, jako je např. protokol RADIUS (Remote Dial-In User Service), což je standardní bezpečnostní protokol pro prostředí klient/server od IETF a typicky se používá v autentizačních serverech v prostředích na bázi 802.1X. Standard 802.1X také využívá standardní protokol EAP, který pracuje v různých autentizačních systémech a poskytuje standardní autentizační rámec u klasických i bezdrátových sítí. (Význam standardu 802.1X a souvisejících protokolů a standardů pro řízení přístupu bude předmětem jiného analytického materiálu).

Jedinou otevřenou architekturou pro řízení síťového přístupu založenou na standardech, která vyhovuje prakticky všem aspektům definice „standardu“, je technologie TNC (Trusted Network Connect), sada otevřených specifikací založených na standardech, jejíž základní filosofie je propojený ideál integrity a identity.

Co je TNC (Trusted Network Connect)

Trusted Network Connect neboli TNC je název divize organizace Trusted Computing Group (TCG). Je to také název architektury řízení síťového přístupu založené na otevřených standardech.

The Trusted Computing Group (TCG) je nezisková organizace založená v roce 2003 s cílem vyvíjet, definovat a podporovat otevřené standardy pro důvěryhodné počítačové a bezpečnostní technologie napříč platformami, periferiemi a zařízeními. Skupina TCG má přibližně 140 členů, ke kterým patří výrobci komponent, vývojáři softwaru, systémoví integrátoři a síťové a infrastrukturní společnosti, z nichž 70 se aktivně podílí na definici a specifikaci otevřené architektury TNC pro řízení síťového přístupu založené na standardech.

Řešení TNC vyvíjené uskupením Trusted Computing Group je otevřená architektura, která definuje několik standardních rozhraní, jež naznačují tečkované čáry na obr. 2. Tato standardní rozhraní umožňují, aby komponenty od různých výrobců spolu bezpečně spolupracovaly, a vytvářely tak z existujících instalovaných zařízení a heterogenních sítí řešení pro integritu koncových bodů a řízení síťového přístupu. Architektura TNC je vytvořena tak, aby stavěla na zavedených standardech a technologiích, jako jsou protokoly 802.1X, RADIUS, IPsec, EAP nebo TLS/SSL.

Jak TNC funguje

Architektura TNC byla vytvořena s tím záměrem, aby organizacím pomáhala chránit jejich podnikové sítě před viry, červy, útoky typu DoS (odmítnutí služby), a dalšími škodlivými aplikacemi, a to tak, že budou moci kontrolovat konfigurace připojujících se zařízení a uplatňovat určité bezpečnostní politiky předtím, než bude přístup do sítí poskytnut. Architektura TNC staví na existujících oborových standardech a podle potřeby definuje nové otevřené standardy, s cílem umožnit neproprietárním a interoperabilním řešením vzájemně spolupracovat v rámci heterogenních prostředí.

Otevřené specifikace TNC obsahují definici softwarových rozhraní a protokolů pro komunikaci mezi komponentami bezpečnosti koncových bodů a mezi servery koncových bodů a síťovými prvky. Rámec architektury TNC umožňuje realizovat interoperabilní řešení zahrnující produkty od různých výrobců a nabízí větší výběr při volbě komponent, které by nejlépe splňovaly požadavky podniku na integritu koncových bodů a řízení síťového přístupu.

Standardy 802.1X, EAP, IPsec a RADIUS řeší otázky bezpečné síťové konektivity. Tyto standardy poskytují robustní základnu pro rozšíření procesu síťového přístupu tak, aby zahrnoval i bezpečnostní konfigurační informace týkající se hostitelského systému, a jsou proto široce podporovány výrobci síťových zařízení. Všeobecné rozšíření a implementace těchto bezpečnostních standardů a protokolů umožňuje zákazníkům začleňovat do svých systémů technologii TNC, a tak využívat investice do existující infrastruktury, aniž by museli slevit z výhod interoperability a svobody volby.

Architektura TNC popisuje interakci různých síťových entit, jejímž výsledkem je zjištění stavu klientského systému nebo zařízení, které se pokouší připojit do sítě, a sdělení tohoto stavu dalším síťovým entitám jako jsou systémy, síťová zařízení nebo servery. To umožňuje vyhodnotit klientské zařízení vůči stanoveným minimálním požadavkům bezpečnostní politiky organizace a určit reakci sítě na žádost o přístup.

Řešení založená na otevřených specifikacích TNC zajišťují přítomnost, stav a bezpečnostní úroveň bezpečnostních aplikací stejně jako dalších aplikací specifikovaných organizací. Řešení na bázi TNC zajišťují dodržování přístupových politik organizace tak, že ověřují autentizaci zařízení nebo uživatele a předtím, než povolí připojení do sítě, vyžadují vytvoření určité úrovně důvěry. Tato řešení také poskytují možnost realizace karantény a nápravy u zařízení, která nesplňují minimální požadavky bezpečnostní politiky, jak jsou definovány organizací. Toto se realizuje tak, že se problematické zařízení izoluje a pak se u něj provedou, je-li to možné, příslušné nápravné procedury, aby zařízení vyhovovalo stanovené bezpečnostní politice organizace a získalo nárok na přístup do podnikové sítě.

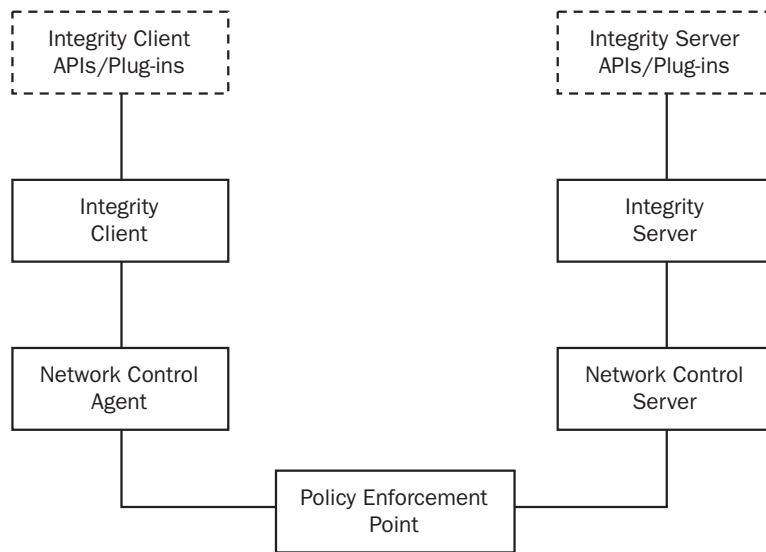
Architektura TNC založená na standardech

Typická architektura řešení pro řízení síťového přístupu se podobá standardní architektuře bezpečnosti přístupu jako je RADIUS nebo 802.1X. V architektuře řízení síťového přístupu je podniková síť hlídána tzv. bodem vynucení (policy enforcement point – „vynucuje“ definovanou politiku), který poskytuje uživatelům nebo zařízením přístup pouze tehdy, pokud byli schváleni serverem pro řízení sítě. Jako bod vynucení může fungovat mnoho různých síťových zařízení: např. přístupový bod 802.1X, přepínač nebo směrovač, firewall, VPN gateway nebo specializované zařízení pro integritu koncového bodu.

Na uživatelském zařízení je agent, buď předinstalovaný nebo ho lze stáhnout. Tento agent obvykle pomocí nějakého API nebo zásuvného modulu (plug-in) shromažďuje informace o bezpečnostním stavu zařízení uživatele a stavu bezpečnostních produktů, které jsou na něm nainstalované, a určuje, zda zařízení neobsahuje nějaký malware nebo jiné škodlivé aplikace.

Uživatel nebo zařízení je pak autentizováno vůči podnikové síti, aby se ověřilo, že mu bylo schváleno přistupovat do sítě. Jakmile je autentizováno, informace shromážděné o bezpečnostním stavu uživatelského zařízení a stavu jeho bezpečnostního softwaru se porovnají vůči definovaným politikám organizace pro bezpečnost sítě a přístupů. Když se profil uživatelského zařízení zkontroluje vůči politikám organizace a ověří se, že vyhovuje, uživateli a jeho zařízení může být poskytnut přístup do podnikové sítě.

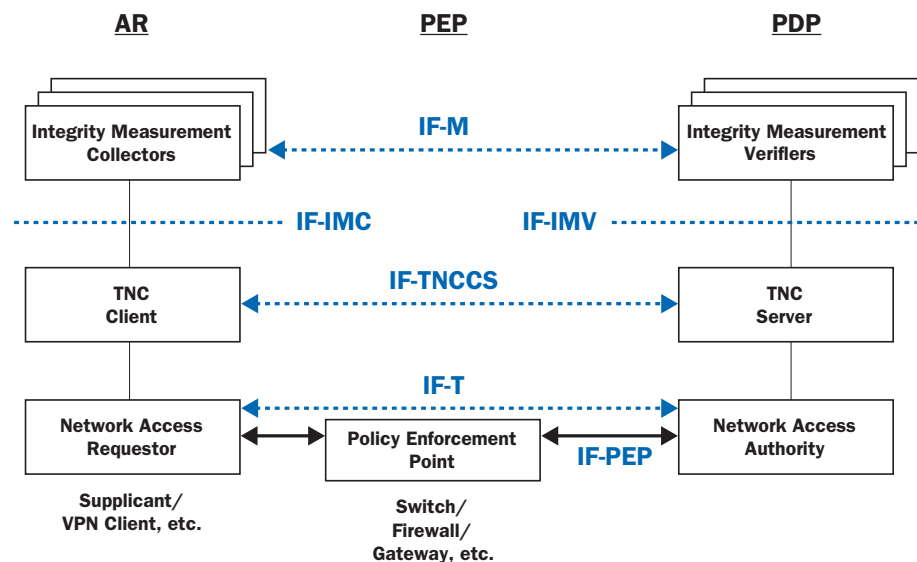
Autentizace uživatele, bezpečnostní stav zařízení, stav bezpečnostního softwaru zařízení, soulad s bezpečnostními politikami a politikami síťového přístupu a autorizace uživatele nebo zařízení – to vše bude určovat, zda uživateli a zařízení bude poskytnut přístup do podnikové sítě, anebo zda se provede jiný typ akce – např. zamítnutí přístupu do sítě, karanténa nebo náprava zařízení.



Obr. 1 – Typická architektura a komponenty řízení síťového přístupu

Otevřená architektura TNC založená na standardech se řídí podobným modelem. V řešení na bázi TNC obsahuje strana klienta tzv. integrity klienta, který se jmenuje TNC Client. TNC Client spolupracuje s plug-inem IMC (Integrity Measurement Collector), který shromažďuje stavové informace ohledně bezpečnosti klientského zařízení a stavu bezpečnostního případně dalšího softwaru na tomto zařízení. TNC Client dále spolupracuje s komponentou Network Access Requestor, která řídí základové protokoly pro požadavky na síťový přístup (802.1X, Ipsec, TLS/SSL, DHCP).

Na straně serveru funguje TNC Server jako Integrity Server. Spolupracuje s plug-inem IMV (Integrity Measurement Verifier), který ohodnocuje bezpečnost koncových bodů na základě informací přijatých od plug-inu IMC a předdefinovaných nebo dynamicky uplatňovaných bezpečnostních politik zavedených organizací. TNC Server dále spolupracuje se síťovou autorizační autoritou (Network Access Authority), kterou je typicky AAA/RADIUS server, který realizuje rozhodnutí TNC Serveru ohledně přístupu a povoluje nebo zamítá koncovému bodu přístup do chráněné sítě v závislosti na tom, zda vyhovuje bezpečnostním síťovým politikám.



Obr. 2 – Architektura a komponenty řízení síťového přístupu TNC (Trusted Network Connect)

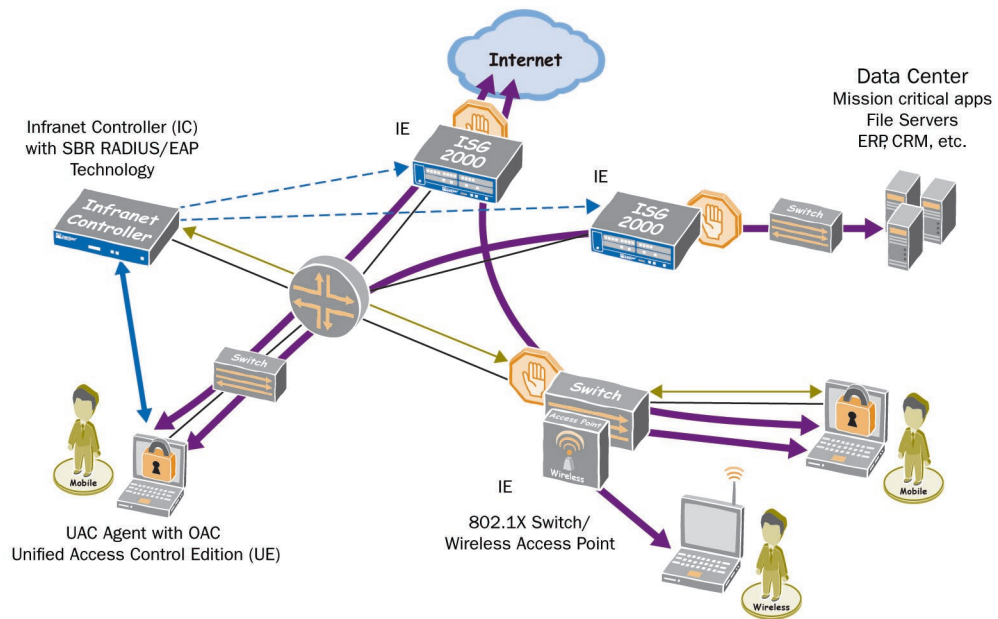
Otevřená architektura TNC také poskytuje solidní základ pro budoucí rozšíření řízení přístupu, neboť poskytuje volitelnou podporu pro další standardní komponentu TCG – modul TPM (Trusted Platform Module). TPM je hardwarový modul začleněný do zařízení, které umožňuje vzdálenou verifikaci integrity hardwaru a softwaru tohoto zařízení. Nejedná se sice o vyžadovanou komponentu TNC, ale integrováním TNC architektury s modulem TPM lze vytvořit integritu koncového bodu ještě důvěryhodnějším způsobem, který je naprosto imunní vůči jakémukoliv škodlivému softwaru.

Existuje tedy způsob jak integrovat zavedené oborové standardy a je definována otevřená architektura založená na standardech. Nyní tedy vše, co podnik potřebuje, je řešení od důvěryhodného dodavatele, respektovaného v daném oboru, který by spojil standardy a otevřenou architekturu dohromady a vytvořil řešení integrity koncových bodů a řízení přístupu do sítě, které by bylo možno použít ve smíšeném, heterogenním síťovém prostředí a které by chránilo celou podnikovou síť a různorodá uživatelská zařízení pokoušející se o přístup do ní. Všechno toto a ještě mnohem více je nyní k dispozici od společnosti Juniper Networks v jejím řešení UAC (Unified Access Control).

Řešení UAC (Unified Access Control) od Juniper Network

Unified Access Control (UAC) je komplexní řešení pro řízení síťového přístupu, které v sobě kombinuje výkonnou uživatelskou autentizaci a autorizaci založenou na standardech, řízení a správu politik na bázi identit a bezpečnost a inteligenci koncových bodů, a výsledkem je rozšíření řízení přístupu v rámci celé podnikové sítě.

Díky začlenění oborových standardů a zavedených, ověřených a všeobecně přijímaných síťových a bezpečnostních produktů poskytuje řešení UAC od Juniper Networks organizacím spolehlivý prostředek pro realizaci jejich bezpečnostních politik, a to jak před vlastním poskytnutím přístupu uživateli do sítě, tak během trvání relace. Tento model pomáhá organizaci dosáhnout komplexní jednotné bezpečnostní politiky a účinně funguje v boji proti současným síťovým hrozbám.



Obr. 3 – Řešení Unified Access Control (UAC) od Juniper Networks

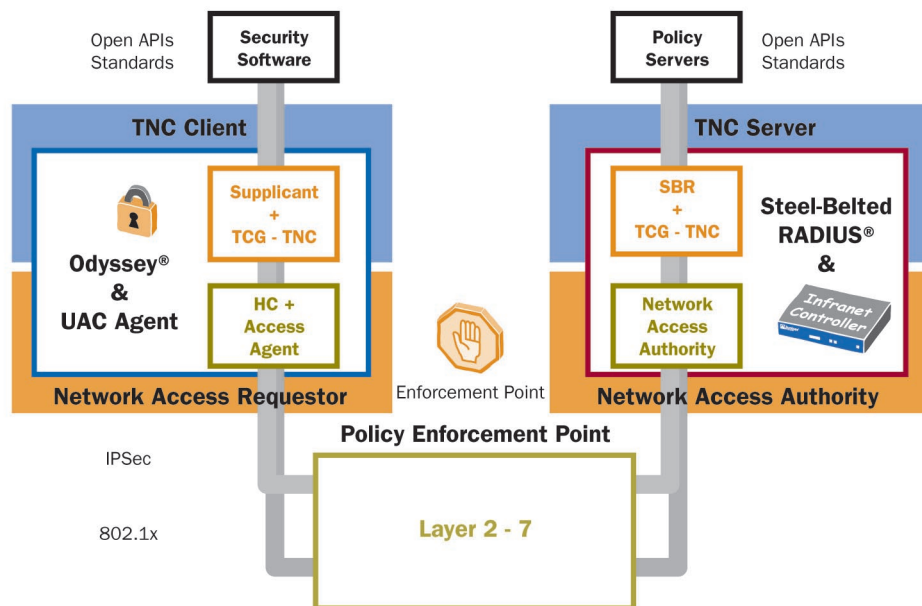
UAC & TNC

Nová verze řešení Unified Access Control (UAC) od Juniper Networks – UAC verze 2.0 – umožňuje řízení bezpečného přístupu na bázi standardů v rámci podnikových LAN. UAC v. 2.0 podporuje otevřené specifikace TNC (Trusted Network Connect) pro aplikační prosazování bezpečnostních požadavků u koncových bodů pokoušejících se o připojení do podnikové sítě.

Díky podpoře otevřených specifikací architektury TNC umožňuje řešení UAC organizacím využít jejich dosavadní investice do heterogenních síťových zařízení a softwaru. Podpora specifikací architektury pro řízení síťového přístupu na bázi standardů dále zjednodušuje schopnost řešení UAC začlenit se do existujícího síťového prostředí, takže může rychle a cenově efektivně začít zabezpečovat síť a síťová zařízení, což poskytuje podniku maximální flexibilitu při implementaci a velmi vysokou návratnost investic (ROI).

UAC dále rozšiřuje své hodnotící schopnosti koncových bodů tak, že začleňuje do svého systému integrity koncových bodů řešení pro antivirus, správu souladu s normami a správu softwarových oprav odpovídající TNC. Poskytuje také podporu pro generická TNC bezpečnostní řešení třetích stran, která tak lze snadno integrovat v rámci soustavy řešení UAC. UAC také rozšiřuje své schopnosti kontroly hostitelského systému, takže podporuje kontroly koncových zařízení podle norem TNC týkající se MAC adres a NetBios systémů.

Organizace nyní mohou implementovat řízení přístupů na bázi standardů flexibilním a cenově efektivním způsobem, a to na základě využití UAC podpory pro různé typy prvků pro prosazování politik a schopnosti tohoto řešení zabezpečovat přístup bez nutnosti nákladných síťových upgradů nebo masivních aktualizací softwaru či firmwaru v její síťové infrastruktuře.



Obr. 4 Řešení UAC v. 2.0 od Juniper Network na architektuře TNC

Řešení UAC v. 2 od Juniper Networks poskytuje komplexní bezpečnost sítě a koncových bodů od síťové vrstvy 2 až po vrstvu 7. Řešení lze snadno a rychle implementovat v rámci zavedených, existujících sítí, a je flexibilní i v rámci měnících se síťových prostředí. Vzhledem k tomu, že UAC je řešení založené na standardech, které využívá a podporuje otevřené specifikace TNC a oborové standardy pro řízení síťového přístupu a integritu koncových bodů, zajišťuje organizaci interoperabilitu a kompatibilitu různých zařízení, a tak organizaci nabízí možnost svobodně volit síťová zařízení a komponenty a vyhnout se potenciálně nákladným, omezujícím závislostem na jediném dodavateli.

Shrnutí

Výhody a nevýhody proprietárních řešení pro řízení síťového přístupu by měly organizace přesvědčit o tom, aby se vyhýbaly řešením, která jsou proprietární nebo jsou založená na „proprietárních standardech“, a orientovaly se na řešení důsledně založená na otevřených standardech. Řešení pro řízení síťového přístupu na bázi standardů přináší organizacím snadnou implementaci, interoperabilitu, vysokou návratnost investic a svobodnou volbu. Poskytují organizaci možnost vybrat si takovou síťovou infrastrukturu a software, které nejlépe vyhovují a přizpůsobují se jejich neustále se měnícím sítím, a přitom se nemusejí obávat, že se stanou závislými na jednom výrobci či dodavateli. Standardní architekturní specifikace pro řízení síťového přístupu TNC (Trusted Network Connect) jsou veřejné, otevřené a dostupné online každému výrobcí – a to poskytuje vynikající úroveň bezpečnosti a jistoty.

Začleněním robustních prověřených oborových standardů, jako je 802.1X, RADIUS a EAP, do svých otevřených architekturních specifikací TNC nabízí nejvyšší úroveň ochrany, která je v dnešních dynamicky se měnících tržních podmínkách nezbytná. Totéž realizuje Juniper Networks prostřednictvím přijetí a použití otevřených specifikací TNC ve svém řešení UAC (Unified Access Control).

Díky použití architektury TNC založené na standardech jako jednoho z pilířů svého řešení umožňuje řešení UAC od Juniper Networks organizacím realizovat řízení síťového přístupu v rámci podnikových LAN flexibilním a cenově efektivním způsobem. Využitím podpory UAC pro různé typy prvků pro prosazování politik a díky schopnosti zabezpečovat přístup bez nutnosti nákladného předělávání sítě nebo kompletních aktualizací softwaru či firmwaru síťové infrastruktury umožňuje UAC organizacím využívat jejich existující investice do různorodých síťových zařízení a softwaru pro řízení přístupu. Otevřený přístup UAC založený na standardech prostřednictvím architektury TNC a jeho začlenění dalších oborových standardů jako je protokol 802.1X poskytuje organizacím interoperabilitu nezávislou na výrobcích a tím možnost volby i v případech, kdy byla organizace dříve vázána na použití proprietárních řešení. S řešením UAC od Juniper Networks si organizace může svobodně vybrat kterékoliv z nejlepších síťových komponent a softwaru tak, aby co nejlépe vyhovovaly jejím obchodním potřebám – což představuje významné přínosy ve smyslu flexibility, nákladů a hodnoty.

