UDC: 004.4. INFO M: str. 11-15

МОДЕЛ РАЧУНАРСКЕ МРЕЖЕ ЗА еУПРАВУ
MODEL OF THE COMPUTER NETWORK FOR eGOVERNMENT

Иван Нејгебауер, Милан Керац, Александар Сударевић, Зоран Војновић

РЕЗИМЕ: У раду је дат приказ решења рачунарских мрежа органа државне управе у земљама Европске Уније. Предложен је логички модел мреже органа државне управе који омогућује контролисано укључивање екстерних корисника у приватну мрежу органа управе.
КЉУЧНЕ РЕЧИ: еУправа, мрежа, виртуелно, IPsec, VPN.
ABSTRACT: This paper presents the summary of e-government network designs in the European Union member countries. It also proposes the logical model of the e-government network which facilitates controlled access of external users and organizations to the base private network.
KEY WORDS: e-government, network, virtual, private, IPsec, VPN.

1. Увод

Концепт еУправе подразумева умрежавање органа управе на свим нивоима, са хоризонталном и вертикалном комуникацијом између појединих целина. Пошто се обим умрежавања не може унапред сагледати, решење које омогућава контролисан и безбедан приступ екстерним корисницима мора бити прилагодљиво и подесиво уз минимално додатно административно оптерећење. Технологија виртуелних приватних мрежа пружа такво решење.

У наставку рада прво је дат преглед и кратак приказ технологија виртуелних приватних мрежа. Затим су сажето описана решења мрежа органа управе у земљама чланицама Европске уније. Следи опис најчешћих протокола за реализацију виртуелних приватних мрежа, и најзад логичка архитектура мреже еУправе која укључује ова мрежна решења.

2. Преглед технологије виртуелних приватних мрежа

Организације које су децентрализоване, или чије особље ради ван матичне локације, имају потребу да омогуће удаљени приступ локалним мрежним ресурсима. Иако је извесне захтеве (често и већину) за приступање и размену података могуће реализовати помоћу вишеслојних технологија у чијој је основи веб приступ, постоје случајеви када је погодније удаљеног корисника логички припојити интерном мрежном окружењу. Овај приступ захтева креирање *виртуелне мреже*, конструкта који удаљеном кориснику пружа илузију непосредне везе са матичном мрежом. Технички, виртуелне мреже се конструишу помоћу тунелирања, тј. транспортовања корисниковог саобраћаја привременом везом успостављеном преко мреже различите од матичне (нпр. глобалног Интернета.)

Овиме се решава проблем децентрализованог приступа, али се уводи нови: подаци који путују преко привремене везе потенцијално су видљиви другим корисницима, рачунајући и непријатељски настројене, на тачкама куда пролази саобраћај између корисника и приступног чворишта у матичној мрежи организације. Ово значи да је за успостављање везе предуслов сигурна аутентификација корисника, а да сама веза мора бити криптографски заштићена. Комбиновање виртуелне мреже са аутентификацијом и криптографском заштитом чини *виртуелну приватну мрежу* (VPN – *Virtual Private Network)*.

Са увођењем виртуелних приватних мрежа, безбедност интерне матичне мреже почиње критично да зависи од безбедности и поузданости VPN имплементације, што значи да планирање мрежне архитектуре мора узети у обзир ове параметре. Додатни потенцијални проблеми коришћења VPN технологија су:

– Кашњење у комуникацији. Иако са корисникове тачке гледишта веза са матичном мрежом изгледа као локална, она то реално није – сваки послати или примљени пакет са подацима мора да пређе дужи и детерминистички непредвидљив пут у односу на случај стварне локалне повезаности. За сервисе код којих су кашњење и/или варијација протока критични параметри (као што је нпр. пренос говора) ово може довести до деградације или неупотребљивости сервиса.

– Повећани захтеви за ресурсима. Криптографска заштита – шифровање и дешифровање токова података – захтева додатно процесорско време у односу на отворену комуникацију, што додатно доприноси кашњењу у комуникацији.

– Двоструки пренос података. Ако је корисников рачунар подешен тако да све комуникационе захтеве упућује преко виртуелне везе (што је са безбедносне тачке гледишта препоручљиво), саобраћај ван матичне мреже прелазиће двоструки пут: прво од захтеваног извора до матичног комуникациог чворишта, па од њега до

корисника. Ово још више доприноси кашњењу, и може захтевати посебна мрежна и безбедносна подешавања уколико корисник мора да приступа временски осетљивим сервисима ван матичне мреже.

– Фрагментација. Тунелирање подразумева енкапсулацију крајњег корисничког саобраћаја у најмање један спољашњи пакет, што неизбежно смањује максималну величину пакета за корисничке податке. Повећана фрагментација токова података смањује и пропусни опсег корисничких веза због повећаног фиксног оптерећења везе додатним пакетским заглављима.

3. Преглед мрежне инфраструктуре органа управе у земљама чланицама Европске уније

Мрежне инфраструктуре можемо сврстати у два типа, по томе како су реализоване:

– Приватне – Уколико организација, која је корисник мрежне инфраструктуре, реализује и управља најмање њеном логичком топологијом (од трећег, мрежног, нивоа ISO OSI модела, па навише). Физичка топологија (први и други ниво ISO OSI модела), односно, преносни путеви могу да припадају организацији-кориснику, али су најчешће изнајмљени од провајдера телекомуникационих услуга.

– Јавне – Уколико се за реализацију мрежне инфраструктуре користе услуге интернет провајдера. У овом случају се комуникација одвија преко Инернета, најчешће уз ослонац на виртуалне приватне мреже.

У земљама чланицама ЕУ мрежна инфраструктура која је подршка сервисима управе је најчешће реализована као приватна, али постоје изузеци. У наставку текста дат је преглед карактеристичних решења по чланицама ЕУ.

Аустрија. *Corporate Network Austria* (CNA) је приватна, протеже се на читавој територији Аустрије. Држава је власник инфраструктуре којом управља из једног центра (*Federal Data Processing Center*). Повезује сва владина одељења и агенције, агенције социјалног осигурања и девет регионалних управа. Свака регија има своју мрежу која је повезана на *CNA*.

Белгија. FedMAN је приватна MAN (*Metropolitan Area Network*) мрежа (на широј територији Брисела). Повезује управе 15 федералних министарстава и владине зграде у Бриселу, и опслужује око 60000 корисника. Пропусни опсег јој је 155 *Mb/s* и функционише од 2002. године.

Кипар. *Government Data Network* (GDN) са *Government Internet/Intranet/Extranet* (GIN) је приватна, реализована је помоћу ATM и *Frame Relay* технологија. Повезује владине системе (локалне мреже институција), а *Government Internet Node* (GIN) је тачка везе са Интернетом.

Чешка. *Public Administration Intranet* (IVS ‡ *Intranet Verejne Spravy*) је приватна мрежна инфраструктура која је тренутно у развоју. Треба да повеже сва јавна административна тела (њихове локалне мреже) и обезбеди сигуран и економичан пренос података и гласа. Користи преносну инфраструктуру провајдера телекомуникационих услуга (*Czech Telecom*). Пружиће сигуран и поуздан приступ Интернету, заштићен *е-маил* систем и сигурну размену података свим владиним институтцијама на територији целе државе.

Данска. Тренутно не постоји мрежна инфраструктура која повезује све институције управе.

Естонија. *EEBone* је приватна мрежна инфраструктура која повезује владине институције (њихове локалне мреже) од 1998. године. Све институције државне и локалне управе имају право, али не и обавезу, да је користе. Коришћење *backbone* мреже је бесплатно за све организације које је користе, финансира се из државног буџета. Организација корисник мора да обезбеди приступни линк и сноси трошкове његовог одржавања. Тренутно повезује више од 21000 рачунара у више од 1300 институција државне и локалне управе. Приступ Интернету је омогућен 2000. године.

Финска. Senaattori је приватна мрежна инфраструктура свих финских министарстава, парламента и канцеларије председника. У функцији је од 1998. године.

Француска. AdER (*Administration En Réseau*) је јавна мрежна инфраструктура која повезује министарстава (њихове приватне мреже). Користи је око 450 000 рачунара (75% од укупног) и функционише од 2000. године. Њену основу чини SETI транспортни сервис који је реализован као VPN мрежа изнад инфраструктуре провајдера телекомуникационих услуга. AdER/SETI мрежа је повезана са европском административном мрежом TESTA (*Trans-European Administrative Network*).

Немачка. *Berlin-Bonn Information Network* (IVBB) је приватна мрежна инфраструктура која је развијена 1990-тих година. Пружа свим федералним управним телима централизован приступ Интернету, мрежне сервисе (WWW, FTP, *e-mail*, итд.) и приступ сервисима који чине IVBB Интранет (интерни сервиси који су доступни једино федералним управним телима). Тренутно се проширује у *Information Network of the Federal Administration* (IVBV) која ће повезати федерална управна тела у сигурну, затворену мрежу.

Грчка. *National Public Administration Network* (*SYZEFXIS*) је приватна мрежна инфраструктура која користи и VPN технологије. Пружа напредне телекомуникационе и информационе сервисе: пренос гласа (телефонија), аудио/видео материјала и података. Повезује више од 1700 јавних установа уз помоћ 4 VPN мреже. Проширена је са MAN оптичким инфраструктурама (оптички прстенови), у око 50 општина на територији Грчке, којим повезују јавне институције (зграде јавне управе, школе, пореске управе итд.).

Мађарска. *Electronic Government Backbone* (EGB) је приватна мрежна инфраструктура, која је у употреби

од 2004. године. Протеже се на територији читаве земље. Користи је јавни сектор (управа) као сигурну комуникациону ифраструктуру и подршку за владин интранет (интерне сервисе). EGB је повезана са TESTA мрежом.

Ирска. *Irish Government's Virtual Private Network* (GVPN) је јавна мрежна инфраструктура. Развила је Влада републике Ирске, уз ослонац на VPN. Користи се за комуникацију између владиних одељења и агенција.

Италија. *Unitary Network of the Public Administration* (RUPA – *Rete unitaria della Pubblica Amministrazione*) је приватна мрежна инфраструктура која повезује сва јавна управна тела у земљи. Треба да је замени *Public Connectivity System* (*Sistema Pubblico di Connettività*) мрежа, тренутно у развоју, која ће побољшати квалитета услуга и сигурносне стандарде.

Летонија. *State-Significant Data Transmission Network* (VNDPT) је приватна мрежна инфраструктура коју је развила, и њоме управља, *State Information Network Agency* (VITA) државна агенција. Повезује владине и општинске институције и организације у целој земљи. Чине је 32 мрежна чворишта. Обезбеђује инфраструктуру за пренос гласа и података, и омогућава динамичку промену пропусног опсега на приступним линијама у зависности од потреба локалних инфраструктура институција које је користе. Постоји и део VNDPT-а, задужен да обезбеди приступ споља, који служи за публикацију података који су од јавног интереса.

Литванија. *Secure State Data Communication Network* (SSDCN) је јавна мрежна инфраструктура. Користи услуге интернет провајдера "Infostruktûra", државног предузеће којим управља Министарство унутрашњих послова. Покрива територију Литваније и повезује око 100 јавних тела (Скупштину, Канцеларију председника, Канцеларију премијера, министраства, државна одељења, округе и локалне заједнице, Пореску управу, итд.). SSDCN је повезана са TESTA мрежом.

Луксембург. RACINE је приватна мрежна инфраструктура која повезује све државне институције у земљи. Развио је и са њом управља *Informatics Centre of the State*.

Малта. *Maltese Government Network* (MAGNET) је приватна мрежна инфраструктура. Повезује сва министарства, владина одељења и агенције, локална већа, школе, полицијске станице, библиотеке, болнице, домове здравља, канцеларије социјалне службе и амбасаде. Свим организацијама које је користе пружа приступ владиној интранет мрежи. MAGNET II мрежа, која је у употреби од 2005. године, ће потпуно заменити MAGNET. MAGNET II мрежа нуди повећан пропусни опсег, бољу поузданост (кроз механизам *Service Level Agreement* – SLA), повећану сигурност са енкрипцијом и VoIP саобраћај између свих корисника.

Холандија. *Rijksoverheidsintranet* (RYX) је приватна мрежна инфраструктура која пружа приступ интранет сервисима холандске владе. Усклађена је са локалним мрежним инфраструктурама у различитим одељењима. Повезује 150 000 запослених у 14 министарстава. Хашки прстен (*Hague Ring*) је приватна мрежна инфраструктура која повезује (главне) зграде владиних одељења. У употреби је од 2006. године. Канцеларија генералног секретара за одбрану је развила инфраструктуру на основу иницијативе Савета генералних секретара.

Пољска. Тренутно се развија мрежна инфраструктура која ће повезати владина одељења, канцеларије и агенције, и локалну управу.

Португалија. Реализације *intranet*-а који ће користити државна администрација је предвиђена за 2005. годину.

Словачка. GovNet је приватна мрежна инфраструктура чији је развој започет 1990-тих година. Од 1993. године је почела да функционише мрежна инфраструктура базирана на изнајмљеним аналогним линијама (*Small* GovNet фаза). 2002. године почела реализација пројекта са циљем да обезбеди сигурну везу на Интернет и прошири сервисе на регионалну и локалну управу. Пројекат је стопиран и тренутно се одличује о томе да ли да се реализује као државна мрежна инфраструктура (приватна) или коришћењем услуга једног или више провајдера (јавна).

Словенија. HKOM (*Fast Communications Network*) је приватна мрежна инфраструктура која повезује владина тела, односно њихове постојеће интернет/интранет инфраструктуре (више од 1600 локалних мрежних инфраструктура) у јединствену мрежу.

Шпанија. Владин *intranet* је приватна мрежна инфраструктура која повезује 16 министарстава, 17 регионалних влада и одређени број локалних управа. Инфраструктуром управља Министарство за јавну управу (*Ministry of Public Administrations*). Архитектура, технологије, сервиси и сигурносни механизми који су имплементирани су веома слични онима који се користе у *TESTA* мрежи Европске уније. Главни пројекат мреже је био спреман 2000. године, а реализација је започета 2002. године.

Шведска. Тренутно не постоји мрежна инфраструктура, али шведска Агенција за јавну управу (*Swedish Agency for Public Management*) је урадила студију изводљивости и очекује се да предложи реализацију владиног сигурног *интранет*-а.

Велика Британија. *Government Secure Intranet* (GSI) је приватна мрежна инфраструктура која повезује владина одељења и агенције. Пружа сигурну и поуздану везу на Интернет (*web*, пренос фајлова, претраживање, публиковање докумената), интерни и екстерни *e-mail*. Побољшана верзија *GSI* мреже је почела да ради 2004. године, карактерише је употреба VPN технологија, могућност преноса гласа и аудио/видео садржаја и могућност креирања VPN мрежа за затворене групе корисника. Имплементацијом нове

инфраструктуре повезани су органи локалних управа и тренутно повезује више од 350 000 корисника. Ову инфраструктуру је могуће проширити и на здравство (*National Health Service*) и Министарство одбране (*Ministry of Defence*), тада ће имати више од милион корисника.

4. ВПН протоколи

Први широко коришћен протокол за виртуелне приватне мреже био је *PPTP* (*Point to Point Tunneling Protocol)* у имплементацији за Мицрософт фамилију оперативних система [1]. Овај протокол се и данас често користи због једноставности конфигурисања и прилагођавања мрежним архитектурама које користе превођење адреса (NAT – *Network Address Translation.)* Основне карактеристике овог протокола су:

- Два канала за пренос података: управљачки и комуникациони. Успостављање и раскидање виртуелне везе најављују се на управљачком каналу, док се поступак аутентификације корисника и пренос података одвијају на комуникационом каналу.
- Кориснички подаци имају двоструку додатну енкапсулацију пре слања од корисничког рачунара до приступног чворишта и обратно: прво у PPP *(Point to Point Protocol)*, па у GRE *(Generic Routing Encapsulation).*
- Под извесним условима, неке врсте PPP пакета су криптографски заштићене.

Прва верзија овог протокола је имала низ слабости [4], укључујући:

- Слање криптографски слабе трансформације корисничке лозинке у току фазе аутентификације, што је могло да доведе до једноставне реконструкције лозинке.
- Извођење кључа за симетрично шифровање саобраћаја непосредно из лозинке, за коју се може претпоставити низак ниво ентропије.
- Коришћење идентичног кључа за оба смера комуникације, што је због специфичног алгоритма за шифровање (RC4) могло да се употреби за реконструкцију кључа.

Наредна верзија је променом алгоритма за аутентификацију и другим модификацијама исправила основне слабости прве, мада опасност речничког испитивања и реконструкције лозинки и даље остаје. Због тога се PPTP не препоручује у ситуацијама где је безбедност битан захтев архитектуре.

Други, такође често коришћен, али са становишта безбедности боље пројектован и испитан скуп протокола је комбинација IPsec и L2TP (стандардизована као комбиновани протокол L2TP/IPsec. [3]). Ова комбинација је сложенија за конфигурисање у односу на PPTP, али поседује већу флексибилност и боља безбедносна својства. Основне карактеристике овог протокола су:

- Криптографска заштита читавог тока комуникације, пошто је спољашњи ниво енкапсулације IPsec у ESP *(Encapsulation Security Payload)* режиму, који пружа и интегритет и поверљивост саобраћаја.
- Могућност коришћења инфраструктуре јавних кључева за аутентификацију крајњих тачака комуникације. Систем је могуће користити и са дељеним тајним кључевима, али ограничења различитих имплементација чине ову варијанту нефлексибилном.
- Додатна енкапсулација: најмање три нивоа – *PPP, L2TP* и *IPsec*, што смањује максималну величину пакета за кориснички саобраћај. У случају да се било која од крајњих тачака тунела налази иза уређаја за превођење адреса, мора се употребити још један ниво енкапсулације – UDP енкапсулација за NAT-T *(NAT Traversal)* механизам [2].

У Microsoft фамилији оперативних система, L2TP/IPsec клијенти су саставни део 2000/XP Professional серије, док за раније верзије постоји посебна, додатна имплементација.

5. Логичка архитектура мреже еУправе

Мрежа еУправе треба да буде логички организована тако да својим корисницима омогући експлоатацију ресурса у складу са правима дефинисаним од стране органа управе. Корисницима се постављају ограничења чије би заобилажење утицало на перформансе, безбедност или интегритет целокупне мреже. Логичка архитектура се имплементира применом:

- Хијерархијског приватног адресирања у складу с адресним планом органа еУправе.
- Дефинисањем хијерархије ДНС имена која прати организацију адресног простора.
- Технологије виртуелних локалних рачунарских мрежа (VLAN) у оквиру матичне мреже.
- Рутирањем између ВЛАН-ова на уређајима у чворишту мреже.

Увођење виртуелних приватних мрежа као начина приступа појединим ресурсима доступним на централној мрежи еУправе је оптимално решење за потребу комуникације између издвојених локација и матичне мреже, које може униформно да се искористи и за друге сценарије приступа, као што су рад мобилних корисника или интеграција бежичних мрежа са матичном мрежом. Изабрани протокол за реализацију виртуелних приватних мрежа је L2TP/IPsec.

Додатна два елемента логичке инфраструктуре која су неопходна да би се омогућио приступ екстерним корисницима уз минимално административно оптерећење, а

уз задржавање безбедносних карактеристика матичне мреже, јесу:

– Систем за подршку инфраструктури јавних кључева, којима се постиже међусобна аутентификација крајњих тачака у обезбеђеном VPN тунелу.
– Систем за централизовану аутентификацију и ауторизацију корисника ресурса, којима се додатно регулишу корисничке привилегије.

У случају фиксних екстерних локација које имају потребу за повременом комуникацијом са матичном мрежом, неопходно је да се:

– На корисничком рачунару на екстерној локацији инсталира ланац сертификата за аутентификацију самог рачунара и приступног чворишта у матичној мрежи еУправе.
– На истом том рачунару подеси повремена веза која отвара виртуелни тунел ка чворишту матичне мреже, и то посредством посебног уређаја на локацији екстерног корисника (у случају да локација користи приватну везу ка матичној мрежи) или посредством глобалног Интернета (уколико локација користи јавну везу).

Веза мора бити подешена тако да се избегне раздвојено тунелирање, тј. сав екстерни саобраћај мора да прелази преко виртуелне приватне мреже.

Под претпоставком да екстерна локација већ има локалну рачунарску мрежу која може, а не мора, бити повезана на глобални Интернет, једини услов за несметано повезивање на матичну мрежу еУправе јесте одсуство колизије локалног приватног адресног простора и адресног блока чији се део постаје активирањем виртуелне приватне мреже. Уколико колизија постоји, приватни адресни простор екстерне локације мора да се промени.

Важно је напоменути да евентуалне грешке у конфигурисању адресног простора, нехотичне или злонамерне, не могу послужити за остваривање приступа интерним ресурсима матичне мреже. Виртуелна веза не може да се успостави без остваривања IPsec асоцијације, а она зависи од *међусобне* аутентификације екстерног рачунара и приступног чворишта. Ово искључује покушај подметања лажног приступног чворишта. С друге стране, колизија адресног простора се детектује приликом PPP фазе конфигурисања адреса крајњих тачака, што доводи до неуспеха у успостављању VPN тунела.

Бежичне мреже активне на одређеном простору у оквиру матичне мреже могу се третирати као посебан случај фиксних екстерних локација. Овакав третман ублажава бројне безбедносне проблеме природене бежичним мрежама. До колизије адресног простора не може доћи јер је он цео под административном контролом матичне мреже.

Мобилни корисници такође морају бити регистровани и у инфраструктури јавних кључева (тј. имати одговарајући ланац сертификата на свом рачунару), и у централном регистру корисника. Разлика у односу на фиксне екстерне локације јесте непредвидивост IP адресе мобилног корисника, осим чињенице да се са стране матичне мреже мора видети као јавна. Ово значи да приступно чвориште мора бити доступно на глобалном Интернету, без могућности селективног ограничавања доступности.

6. Закључак

Приказана логичка архитектура мреже еУправе обједињује стандардне логичке елементе, као што су адресирање, именовање и изолација мрежних домена, са додатним елементима који су потребни за несметано логичко проширење мреже екстерним корисницима. Администрација екстерног приступа је централизована, што смањује административно оптерећење, а безбедносни захтеви могу бити очувани. Приказани модел је довољно флексибилан да може, уз мале измене, да послужи за прикључивање различитих категорија екстерних корисника.

Литература

[1] Hamzeh, K. et al, *Point-to-Point Tunneling Protocol (PPTP)*, RFC 2637, July 1999.

[2] Kivinen, T. et al, *Negotiation of NAT-Traversal in the IKE*, RFC 3947, January 2005.

[3] Patel, B. et al, *Securing L2TP using IPsec*, RFC 3193, November 2001.

[4] Schneier, Bruce and Mudge, *Cryptanalysis of Microsoft's Point-to-Point Tunneling protocol (PPTP)*, Proceedings of the 5th ACM Conference on Computer and Communications Security, pp. 132-141, 1998.

Милан Керац дипл. инж., Академска рачунарска мрежа Универзитета у Новом Саду. Област: рачунарске мреже.

Иван Нејгебауер дипл. инж., Академска рачунарска мрежа Универзитета у Новом Саду. Област: рачунарске мреже.

Зоран Војновић дипл. инж., Академска рачунарска мрежа Универзитета у Новом Саду. Област: рачунарске мреже.

Александар Сударевић дипл. инж., Академска рачунарска мрежа Универзитета у Новом Саду. Област: рачунарске мреже.