



Vienota bezvadu tīkla izveide ar Microsoft rīkiem

Microsoft
GOLD CERTIFIED
Partner

Learning Solutions
Information Worker Solutions
Microsoft Business Solutions
Advanced Infrastructure Solutions

Projekta apraksts

**Projekta pasūtītājs: LATVIJAS
REPUBLIKAS ZEMKOPIBAS MINISTRIJA**

Sagatavoja:

SIA „DPA”

www.dpa.lv

Tālr. 67509900

e-pasts: dpa@dpa.lv

VIENOTA BEZVADU TĪKLA IEVIEŠANA AR MICROSOFT RĪKIEM LATVIJAS REPUBLIKAS ZEMKOPĪBAS MINISTRIJĀ

Mērķis: Latvijas Republikas Zemkopības ministrijas (ZM) bezvadu tīkla pārveide, lai vienkāršotu administrēšanu un uzlabotu drošību.

ZM vienotā bezvadu tīkla ieviešana ar *Microsoft Network Policy Server* (NPS) apvieno bezvadu tīkla piekļuves punktu kopu, automatizē lietotāju pieslēgumu bezvadu tīklam, būtiski uzlabo tīkla drošību, kā arī samazina nepieciešamās administratīvās darbības.

Kopsavilkums

Valsts:	Latvijas Republika, Rīga
Nozare:	Valsts pārvalde, lauksaimniecība
Klienta profils:	ZM ir vadošā valsts pārvaldes iestāde lauksaimniecības, meža un zivsaimniecības nozarēs. Ministrijas misija ir izstrādāt, organizēt un koordinēt lauksaimniecības, meža nozares un zivsaimniecības politikas īstenošanu, kā arī rūpēties par vispārēju šo nozaru attīstību.
Situācija:	Novecojusi, neautomatizēta, decentralizēta un nedroša bezvadu tīkla infrastruktūra, ko bija nepieciešams modernizēt.
Risinājums:	Bezvadu tīkla modernizācija ir veikta, izmantojot <i>Microsoft Windows Server 2008 Network Policy Server</i> un bezvadu tīkla piekļuves punktu iespējas. Šī risinājuma ietvaros ir uzlabota tīkla drošība, izmantojot jaunāko WPA2 drošības protokolu un AES šifrēšanas algoritmu, automatizēta lietotāju pieslēgšanās ar RADIUS autentifikāciju, izveidota sistēma, kas ir noturīga pret bojājumiem un spējīga nodrošināt nepārtrauktu bezvadu tīkla darbību.
Ieguvumi:	Pilnībā pārveidota bezvadu tīkla infrastruktūra, izmantojot jaunākās Microsoft tehnoloģijas. Izveidota sistēma, kurai nav nepieciešama regulāra manuāla apkope. Vienots bezvadu tīkls ar vienu tīkla profilu. Lietotājiem - pilnībā automatizēts pieslēgums bezvadu tīklam bez koplietošanas atslēgām. Augsta sistēmas drošība pret ielaušanos un bojājumiem.

Situācija

ZM bezvadu tīkla struktūra sastāvēja no 14 piekļuves punktiem, kas bija izvietoti 6 stāvos. Katrs no piekļuves punktiem raidīja divus tīkla profilus ar atšķirīgiem bezvadu tīkla standartiem – 802.11a un 802.11g. Kopā tas veidoja 28 bezvadu tīkla profilus (SSID). Visi piekļuves punkti tika konfigurēti, izmantojot WPA drošības tipu ar TKIP šifrēšanu. Visiem piekļuves punktiem bija vienota koplietošanas atslēga (*preshared-key*). Izmantotie drošības protokoli, šifrēšana un tehnoloģija bija novecojusi un bezvadu tīkla struktūra sarežģīta. Lai nodrošinātu esošās konfigurācijas drošību, bija nepieciešama regulāra administratora iejaukšanās. Tas prasīja lielus laika resursus un radīja neērtības bezvadu tīkla lietotājiem.

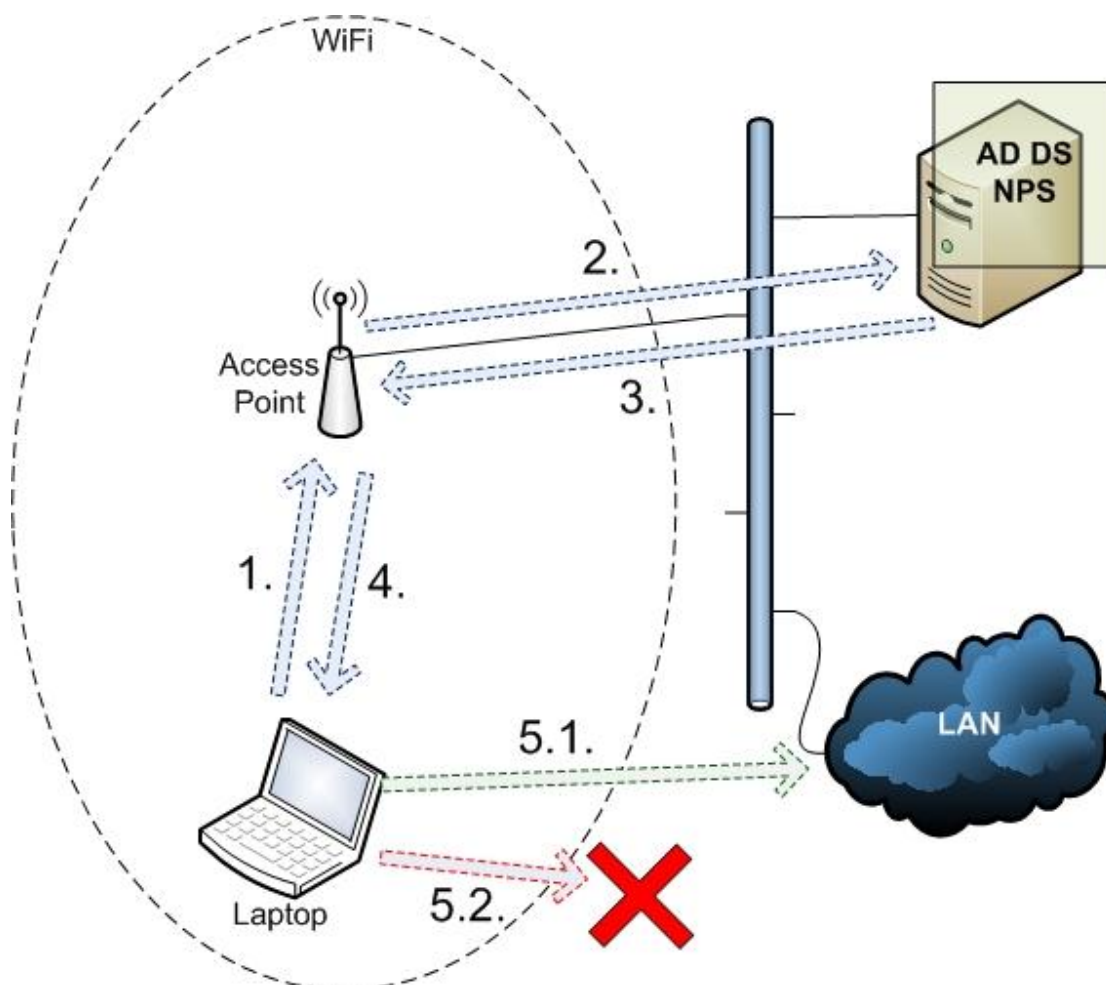
Lai sākotnējo bezvadu tīkla struktūru uzturētu drošu, bija nepieciešams pārāk liels administratoru laika resurss. Šāda struktūra ir droša tikai tādā gadījumā, ja koplietošanas

atslēgas tīkla piekļuvei tiek mainītas regulāri, turklāt tām būtu jābūt vismaz 22 simbolus garām. Tā kā ZM struktūrā bija 28 tīkla profili, tad regulāri mainīt atslēgas būtu bijis ārkārtīgi laikietilpīgi. Šādā risinājumā arī lietotājiem rodas sarežģījumi, jo regulāri nepieciešams nomainīt tīkla piekļuves atslēgas. Tīkla profilu pieslēguma informācija tiek glabāta uz lietotāju datoriem, un tie nespēj atšķirt, kad parole ir nomainīta. Tas nozīmē, ka lietotāji ir jāinstruē par to, kā nomainīt saglabātam tīkla profilam atslēgu. Drošas atslēgas ievadīšana (vismaz 22 simboli) ir ārkārtīgi sarežģīta mobilajos telefonos, jo tā jāievada pa vienam simbolam manuāli. Sākotnējā bezvadu tīkla drošības uzturēšanā tika izmantots novecojis drošības protokols (WAP) un šifrēšanas mehānisms (TKIP), kura drošības trūkumi ir identificēti jau pirms vairākiem gadiem. Izmantojot koplietošanas atslēgas, tās var viegli nodot trešajām personām, kuras varētu piekļūt ZM datiem.

Risinājums

Laikā no 2009. gada novembra līdz 2010. gada martam notika ZM bezvadu tīkla infrastruktūras restrukturizācija. Šajā laikā tika pilnībā pārveidota bezvadu tīkla struktūra, panākot pilnīgu lietotāju automatizētu pieslēgšanos tīklam. Tika ieviesti jaunākie Microsoft tehnoloģiskie risinājumi un izmantoti jaunākie drošības protokoli, kā arī šifrēšana. Šāds risinājums rada augstu tīkla drošības pakāpi, izmantojot sarežģītu šifrēšanas mehānismu un dinamisku atslēgas maiņu, tādā veidā novēršot jebkādu iespēju ielauzties tīklā no ārpuses. Izmantojot *Microsoft Network Policy Server (NPS)* serveri ar *Remote Authentication Dial In Service (RADIUS)* implementāciju, tiek panākta automatizēta lietotāju autentifikācija, balstoties uz noteiktām prasībām (piemēram, lietotājam jābūt domēna lietotājam), novēršot vajadzību pēc koplietošanas atslēgām. Šāds risinājums būtiski samazina nepieciešamību pēc administratīvas iejaukšanās. Ieviešot divus NPS serverus, tika panākta nepārtraukta bezvadu tīkla pieeja kāda NPS servera atteices gadījumā.

ZM bezvadu tīkla restrukturizāciju laikā no 2009. gada novembra līdz 2010. gada martam veica Latvijas IT kompānija – SIA DPA. Projekta gaitā tika veikta vecās bezvadu tīkla infrastruktūras izpēte un dokumentēšana, plānošana, serveru lomu ieviešana un konfigurēšana, GPO izveide, testēšana, piekļuves punktu konfigurācija un projektējuma dokumenta izveide.



1. Piekļuves pieprasījums, lietotāja datu nosūtīšana.
2. Piekļuves pieprasījums, lietotāja datu nosūtīšana.
3. Piekļuves akceptēšana vai noraidīšana.
4. Piekļuves akceptēšana vai noraidīšana.
- 5.1. Piekļuves akceptēšana – lietotājs piekļūst tīkla resursiem.
- 5.2. Piekļuves noraidījums – lietotājs paliek ārpus tīkla.

Rezultāti

Projekta rezultātā ir **iegūts vienots bezvadu tīkls, aizvietojo 28 tīkla profilus (SSID) ar vienu.**

Bezvadu tīkla ieviešanā **izmantoti esošie serveru resursi**, uzliekot *Microsoft Network Policy Server* lomas.

WPA drošības tips ir aizvietots ar WPA2-Enterprise, kas ietver sevī AES šifrēšanu. Šie iestatījumi nodrošina grūti uzlaužamu tīklu, kas veic dinamisku piekļuves atslēgu maiņu un sarežģītu šifrēšanu algoritmu.

Lietotāju pieslēgums bezvadu tīklam ir pilnībā automatizēts arī uz iepriekš neizmantotiem datoriem. To nodrošina RADIUS implementācija NPS serverī, autentificējot

lietotājus, balstoties uz iepriekš norādītiem kritērijiem (piemēram, lietotājam jābūt kādā konkrētā drošības grupā, jābūt domēna lietotājam vai jālieto domēna dators).

Ieviešot divus NPS serverus, sinhronizējot konfigurāciju un izmantojot piekļuves punktu tehniskās iespējas, **panākta nepārtraukta bezvadu tīkla darbība viena NPS servera atteices gadījumā.**

Izveidota sistēma, kuras **uzturēšanā nav nepieciešama regulāra administratora iejaukšanās.**

Ir izveidota 14 piekļuves punktu kopa, kuru iespējams viegli papildināt.

Dati

Raksturojums	Pirms migrācijas	Pēc migrācijas
Bezvadu tīkla profili (SSID)	28	1
Drošības tips	WPA	WPA2
Šifrēšana	TKIP	AES
Autentifikācijas tips	Pre-shared key	Active Directory authentication
Autentifikācijas serveris	IAS	NPS

Par Microsoft® Network Policy Server

Network Policy Server (NPS) ir Remote Authentication Dial-in User Service (RADIUS) un vārtejas servera (proxy) implementācija Windows Server 2008 sistēmā. NPS ir aizvietotājs iepriekšējās paaudzes Windows Server 2003 autentifikācijas serverim Internet Authentication Service (IAS).

Pateicoties RADIUS implementācijai, NPS veic centralizētu pieslēguma autentifikāciju, autorizāciju un daudzu tīkla piekļuvju tipu uzskaiti, ieskaitot bezvadu un „virtual private network (VPN)” pieslēgumus. Izmantojot RADIUS vārtejas servera iespējas, NPS pārvirza autentifikācijas un uzskaites ziņojumus uz citiem RADIUS serveriem. NPS darbojas arī kā atbilstības izvērtēšanas (health evaluation) serveris priekš Network Access Protection (NAP).

Plašākai informācijai

Microsoft Windows Server 2008 Network Policy Server mājas lapa:
<http://technet.microsoft.com/en-us/network/bb629414.aspx>

Lai vairāk uzzinātu par Centrāleiropas un Austrumeiropas reģiona (CEE) Microsoft partneru gada balvas saņēmēju (2008., 2009.gads), Latvijas IT uzņēmumu SIA DPA (Datorprogrammu apgāds): www.dpa.lv

Lai iegūtu plašāku informāciju par Latvijas Republikas Zemkopības ministriju:
www.zm.gov.lv

Šī gadījuma izpēte paredzēta tikai informatīviem nolūkiem. *Microsoft Latvia* un *Microsoft Corporation* neuzņemas nekādas tiešas, netiešas vai ar likumu noteiktas garantijas saistībā ar šajā dokumentā pausto informāciju.

Publicēts 2010.gada martā.