Sigurnost mreže i komunikacije

11. PREDAVANJE

Algebra
visoka škola za
primijenjeno računarstvo

Sadržaj

- Upravljanje Windows vatrozidom
- Konfiguracija IPsec postavki i pravila sigurne veze
- Implementacija izolacijskih zona

Upravljanje Windows vatrozidom

- Što je to Windows vatrozid?
- Što su profili lokacija mreže?
- Preporuke za konfiguraciju
- Kako implementirati pravila vatrozida
- Planiranje strategije vatrozida

Što je to Windows vatrozid?

Windows vatrozid je host-based vatrozid koji je uključen u Windows Server 2012. Sastoji se od:

- Inbound i outbound pravila
- Pravila sigurne veze (engl. Connection security rules)

Vatrozid možemo administrirati pomoću:

- Upravljačke konzole
- Group Policy
- Netsh komande
- Windows PowerShell

Što su profili lokacija mreže?

Profili vatrozida su skup konfiguracijskih postavki koji se primjenjuju na određeni tip mreže

Profili koji su nam na raspolaganju su:

- Public
- Private
- Domain

Windows Server 2012 ima mogućnost da više profila bude aktivno istovremeno

Preporuke za konfiguraciju

Imajmo na umu sljedeće preporuke:

- Pojednostavimo konfiguraciju korištenjem pravila baziranih na aplikacijama
- Pravila bazirana na portovima koristimo kada ne možemo kreirati ona bazirana na aplikacijama
- Odaberimo odgovarajući profil za pravila
- Obučimo korisnike da prilikom spajanja na mrežu odaberu ispravni profil
- Koristimo opcije raspona da pravila ograničimo na pojedine IP adrese ili raspone IP adresa
- Koristimo tipove sućelja da bi pravila primjenili samo na bežične veze ili an veze za udaljeni pristup

Kako implementirati pravila vatrozida

Pravila vatrozida možemo implementirati:

- Ručnom konfiguracijom na svakom poslužitelju
- Pomoću Group Policy postavki
- Eksportiranjem i importiranjem pravila vatrozida

Planiranje strategije vatrozida

Kada implementiramo vatrozid napravimo sljedeće:

- Blokirajmo sve inbound veze
- Kreirajmo iznimke za inbound veze za pojedine aplikacije prema potrebi
- Pomoću outbound pravila kontrolirajmo komunikaciju aplikacija s drugim servisima
- Onemogućimo outbound veze
- Razmislimo o implementaciji connection security pravila

Konfiguracija IPsec postavki i pravila sigurne veze

- Što je IPsec?
- Što su IPsec modovi rada?
- IPsec opcije autentifikacije
- Što su pravila sigurne veze?
- Preporuke za implementaciju

Što je IPsec?

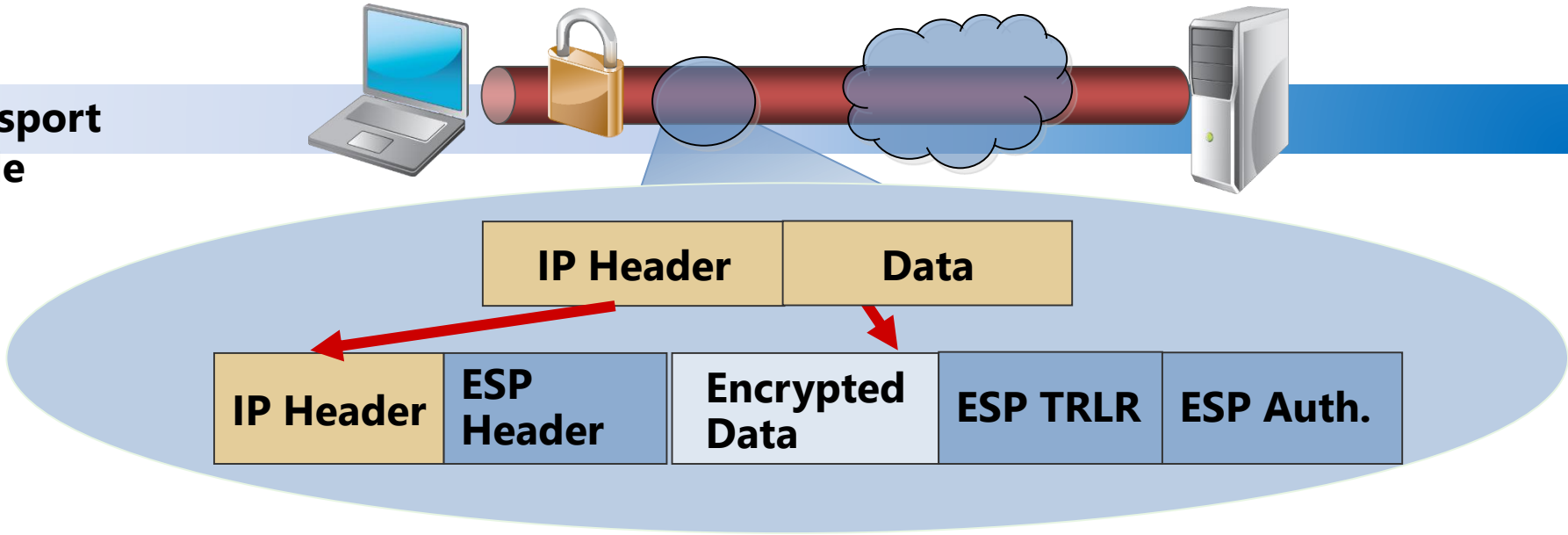
IPsec je skup protokola koji omogućava sigurnu, enkriptiranu komunikaciju između dva ili više računala kroz nesigurnu mrežu

Preporučeni scenariji korištenja:

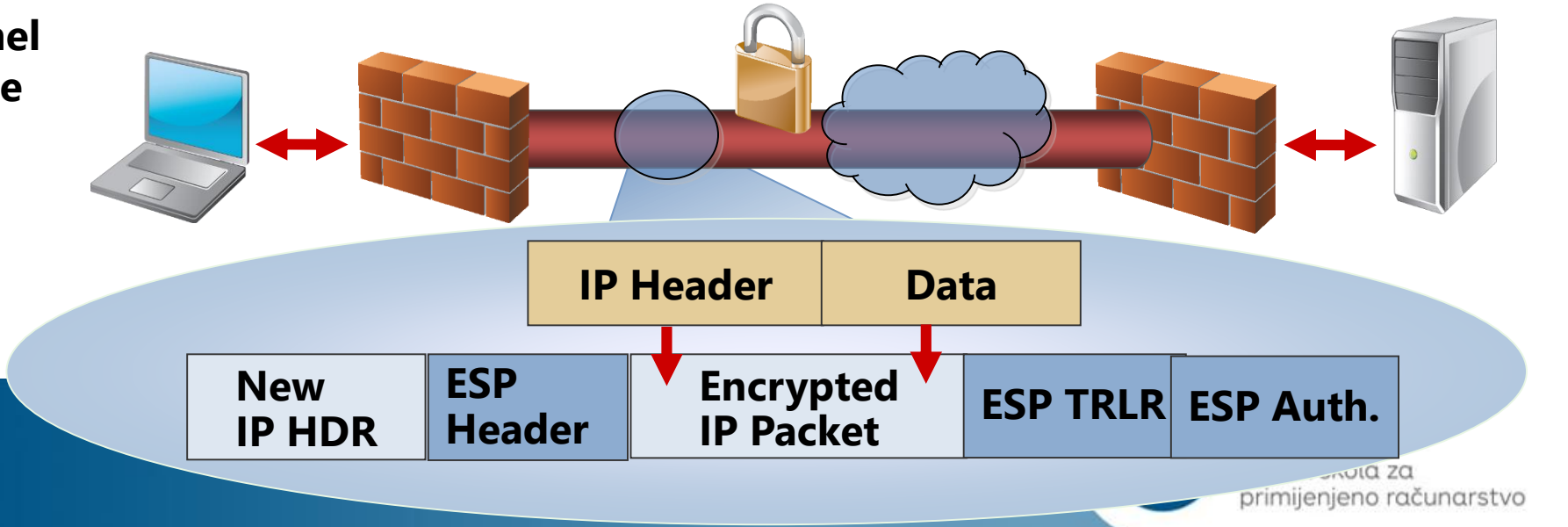
- Filtriranje paketa
- Autentifikacija i enkripcija prometa u mreži
- Autentifikacija i enkripcija prometa između točno određenih računala
- L2TP/IPsec za VPN veze
- Site-to-site tuneliranje
- Kreiranje logičkih mreža

Što su IPsec modovi rada?

ESP Transport Mode



ESP Tunnel Mode



IPsec opcije autentifikacije

Metoda	Ključne mogućnosti
Default	Koristi autentifikacijsku metodu koja je konfigurirana na IPsec Settings kartici.
Computer and User (Kerberos V5)	Request ili require da se i korisnik i računalo autentificiraju prije nego započne komunikacija. Potrebno je članstvo u domeni.
Computer (Kerberos V5)	Request ili require da se računalo autentificira putem Kerberos verzije 5 autentifikacijskim protokolom. Potrebno je članstvo u domeni.
User (Kerberos V5)	Request ili require da se korisnik autentificira putem Kerberos verzije 5 autentifikacijskim protokolom. Potrebno je članstvo u domeni.
Computer certificate	Request ili require ispravan računalni certifikat, nužno je da postoji barem jedan CA. Prihvaća samo zdravstvene certifikate: request ili require ispravan zdravstveni certifikat za autentifikaciju; nužno je postojanje IPsec NAP.
Advanced	Konfiguracija bilo koje dostupne metode. Možemo definirati metode za prvu i drugu autentifikaciju.

Što su pravila sigurne veze?

Pravila sigurne veze:

- Autentificiraju dva računala prije nego počne komunikacija
- Osigurava i štiti podatke koji putuju između računala
- Koristi razmjenu ključeva, autentifikaciju, integritet podataka, i enkripciju (opcija)

Kako su povezana pravila vatrozida i sigurne veze:

- Pravila vatrozida propuštaju ili brane promet ali ne štite podatke
- Pravila sigurne veze štite promet ali taj promet mora biti propušten kroz vatrozid

Preporuke za implementaciju

Neke od preporuka za implementaciju pravila sigurne veze:

- Da bi se ostvarila IPsec veza na računalima moraju postojati kompatibilna pravila sigurne veze
- Kada kreiramo pravilo sigurne veze druga pravila se mogu primjenjivati na korisnika ili računalo
- Koristimo Kerberos V5 autentifikaciju da bi i računalima i korisnicima omogućili autentifikaciju
- Izbjegavajmo primjenu IPsec pravila i pravial sigurne veze na ista računala
- Prije implementacije testirajmo
- Koristimo IPsec samo kada je potrebno
- Group Policy koristimo za primjenu pravila na više računala
- Windows PowerShell ili Netsh možemo koristiti za kreiranje skripti i upravljanje pravilima

Implementacija izolacijskih zona

- Kako rade zone izolacije
- Planiranje domenske izolacijske zone
- Preporuke za implementaciju

Kako rade zone izolacije

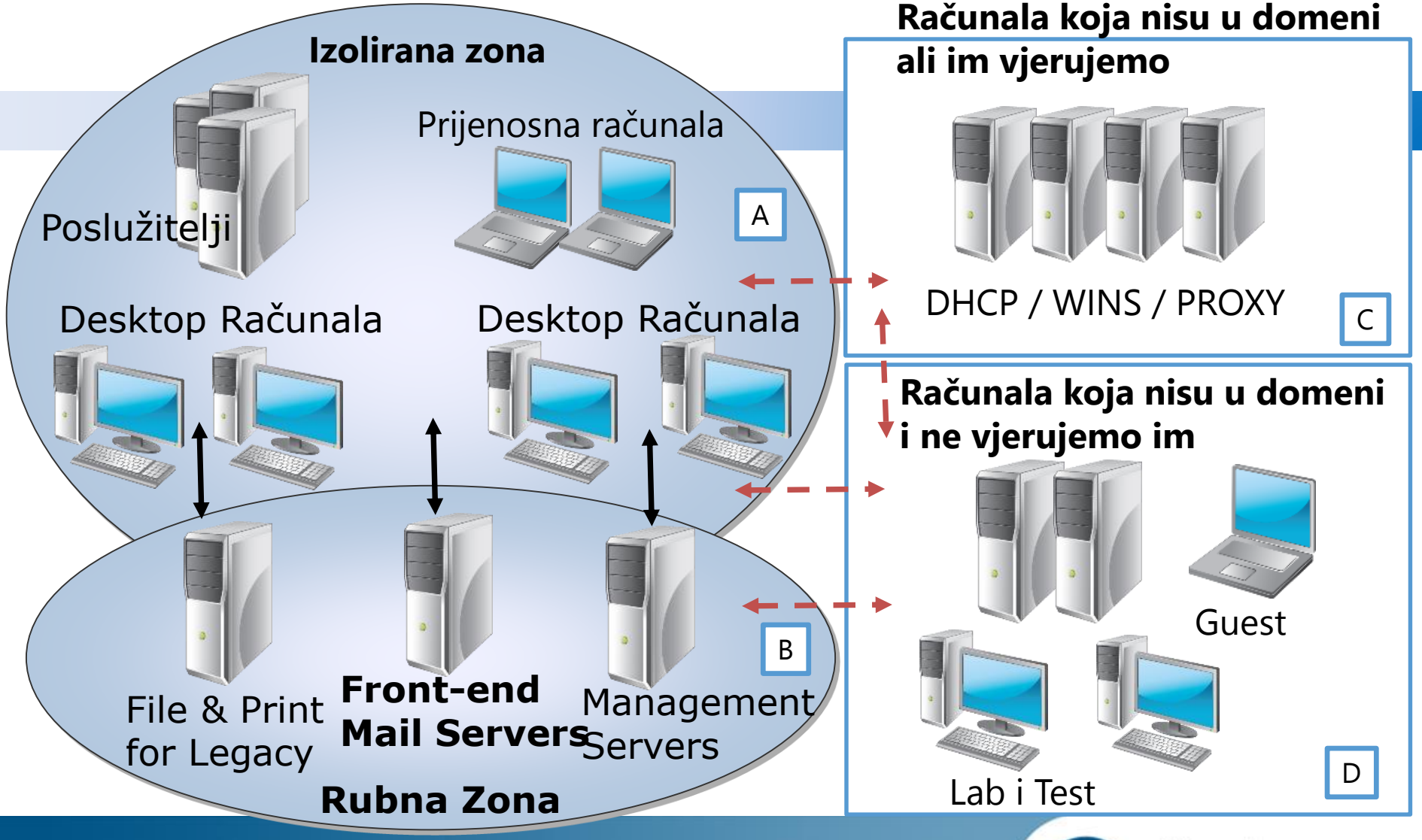
Sljedeći faktori su primijenjeni na zone izolacije:

- Računala u izoliranoj zoni mogu komunicirati sa svim drugim računalima
- Računala koja nisu u izoliranoj mreži ne mogu započeti komunicirati s računalima u izoliranoj mreži

Domenska izolacija je situacija kada su računala domene izolirana od onih računala koja nisu članovi domene.

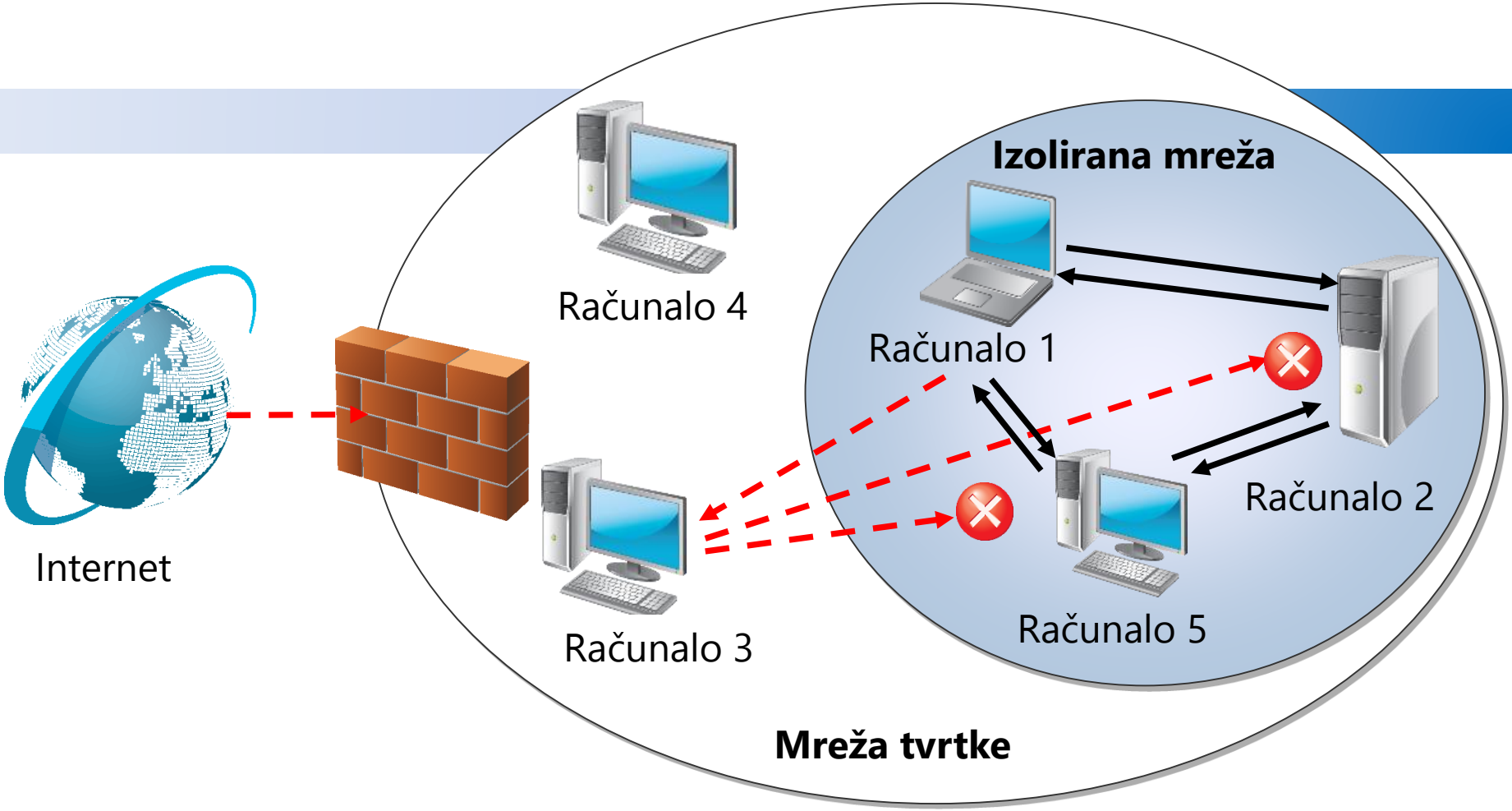
Izolacija poslužitelja izolira pojedine poslužitelje od računala koji nisu članovi domene.

Planiranje domenske izolacijske zone



Algebra
visoka škola za primijenjeno računarstvo

Preporuke za implementaciju



Pokrenuta neautentificirana komunikacija

Pokrenuta autentificirana komunikacija