KAUNO TECHNOLOGIJOS UNIVERSITETAS

KOMPIUTERIŲ KATEDRA

Valstybinių institucijų tinklų saugos nustatymas

Elektroninių paslaugų sauga

Laboratorinis darbas Nr. 4

Atliko: IFM-1/3 gr. stud.

Eligijus Kiudys

Vadovas: doc. G. Činčikas

Kaunas 2022

Valstybinių institucijų tinklų saugos nustatymas

1. **Darbo tikslas:**

Susipažinti su Valstybinių institucijų tinklų realizavimo principais bei jų saugos įvertinimu

2. **Teorinė dalis:**

Valstybinių institucijų tinklų saugai naudojama įvairių tipų ugniasienės, paprasti paketų filtrai, įsimenančius paketų filtrai, taikomųjų programų įgaliotieji serveriai, filtrų sudarymo algoritmai, transportinio lygmens tuneliai, duomenų šifravimas, slaptažodžiai. Dažniausiai tai nulemia ekonominiai faktoriai.

Valstybinių institucijų tinklų saugos grėsmės:

- *Kompiuteriniai virusai bei interneto kirminai.* Tai yra piktavališkos programos, sugebančios save platinti. Dažnai virusai bei kirminai atlieka žalingus veiksmus: sunaikina informaciją, atlieka kompiuterines atakas prieš kitus kompiuterius, kompiuteriai ir tinklai patiria perkrovas bei pan.
- *Pavojus prarasti informaciją.* Įsilaužėliai, gavę nesankcionuotą priėjimą prie kompiuterio, gali sunaikinti arba pavogti (perimti) privačią, svarbią informaciją. Dažnai įsilaužėlių tikslas - perimti vartotojų slaptažodžius, banko (mokėjimo kortelių) informaciją, el. pašto adresus ir kt.
- *Kompiuterio valdymą* perėmę įsilaužėliai, gali panaudoti jį kitokiems piktavališkiems tikslams, pavyzdžiui, kompiuteris gali būti paverstas naujų atakų poligonu ar piratinės programinės įrangos saugykla. Pažeistas kompiuteris patirs perkrovas, gali būti sugadinta programinė įranga, dėl padarytų nuostolių kompiuterio savininkas gali susilaukti sankcijų iš interneto paslaugų teikėjo ar iš teisėsaugos institucijų. Norint atstatyti kompiuterio normalų veikimą, visada prarandama daug laiko ir lėšų.

Galima išvardinti priežastis, dėl kurių pažeidžiami kompiuteriai:

- vartotojams dažnai trūksta žinių apie interneto pavojus;
- parduodami nauji kompiuteriai dažnai nėra pakankamai apsaugoti nuo interneto grėsmių;
- vartotojai nesinaudoja (dėl žinių, laiko ar noro trūkumo) pigiomis ar nemokamomis techninėmis priemonėmis, skirtomis padidinti kompiuterio saugumą, pamiršta atlikti programų atnaujinimus.

Užkarda

Užkarda (ugniasienė) – tai įranga (aparatinė arba programinė), sukurianti apsauginę sieną tarp kompiuterio ir interneto. Ji gali apsaugoti kompiuterį nuo daugelio įsilaužėlių bei kompiuterinių virusų ir kirminų.

Užkarda gali:

- apsaugoti nuo interneto virusų, kirminų, bandančių įsiskverbti į kompiuterį iš interneto;
- apsaugoti nuo įsilaužėlių, atakuojančių kompiuterį;
- neleisti nepageidautinoms programoms išsiųsti informacijos iš jūsų kompiuterio.

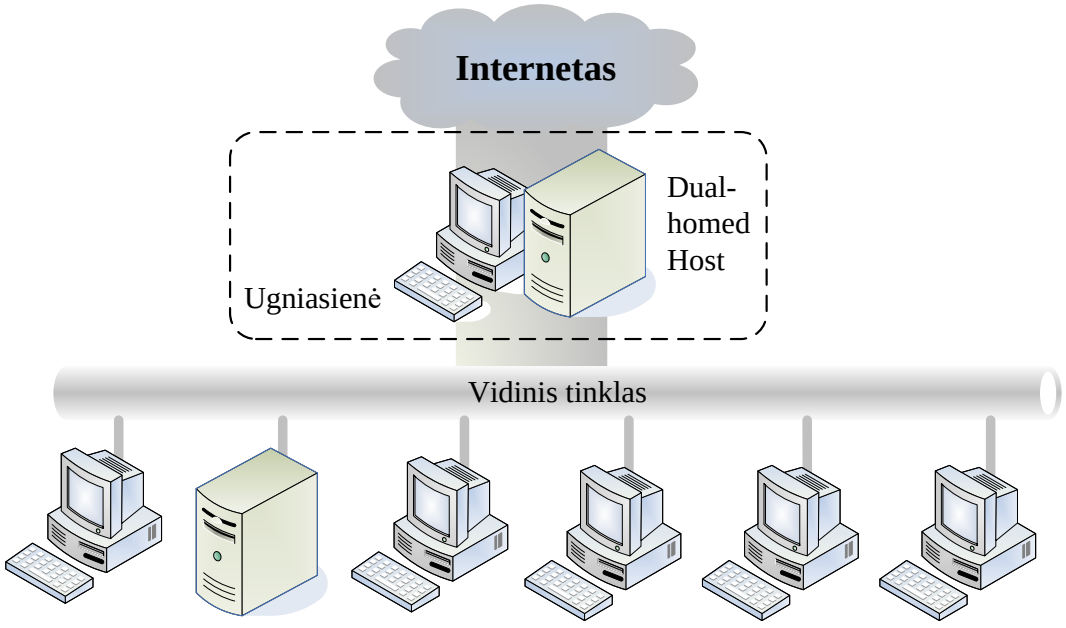
Užkarda negali:

- *apsaugoti nuo kompiuterių, kuriuos jūs laikote patikimais (pvz. kaimyninis vietinio tinklo kompiuteris);*
- *apsaugoti nuo interneto virusų, kirminų, kuriuos gaunate elektroniniu paštu, per naršykle ar kitų programų pagalba.*

Aparatinė užkarda

Vietinį tinklą rekomenduojama apsaugoti specialiu įrenginiu – aparatine užkarda (1 pav.). Toks įrenginys turėtų uždrausti bet kokius prisijungimus iš interneto tinklo prie darbo kompiuterių. Tokią funkciją gali atlikti:

- specializuotas įrenginys, atliekantis tik užkardos funkcijas;
- tinklo maršrutizatorius ar bevielės prieigos taškas su galimybe filtruoti tinklo srautus;
- įrenginys (serveris), atliekantis vidinio tinklo adresų transliavimo funkcijas (NAT).



1 pav. Ugniasienės vieta tinkle

Programinė užkarda

Net jei jūsų vietinis tinklas apsaugotas aparatine užkarda, nereikia pamiršti pavojų, kylančių iš to paties vietinio tinklo. Tai gali būti tiek priešiškai nusiteikęs kaimynas, kolega, tiek kompiuterinis virusas. Nuo tokių problemų gali apsaugoti programinė užkarda, įdiegta į jūsų kompiuterį. Žemiau išvardintos kelios tokios programinės sistemos, turinčios taip pat ir nemokamas versijas (gali būti apribotos naudojimo galimybės):

- Operacinė sistema MS Windows XP turi savo vidinę užkardą MS Windows XP „Internet Connection Firewall“. Įdiegus pataisų paketą SP2, užkarda įjungiama automatiškai. Ankstesnėms MS Windows versijoms galima naudoti žemiau išvardintas programines užkardas;
- ZoneAlarm (nemokama versija namų vartotojams bei nepelno organizacijoms, išskyrus valstybines bei mokslo organizacijas);
- Kerio Personal Firewall (nemokamas namų vartotojams);
- Outpost Firewall 1,0 (nemokamas);
- Sygate Personal Firewall (nemokamas asmeniniam naudojimui).

Antivirusinė programinė įranga

Internetu keliauja daugybė įvairių piktybinių programų – internetinių virusų bei kirminų. Jų galima sulaukti tiek elektroniniu paštu, tiek interneto pokalbių kanaluose, tiek per kitas elektroninio bendravimo priemones. Užkardos neapsaugo nuo virusų, atkeliaujančių elektroniniu paštu ar gaunamų naršant internetą. Viena tinkamiausių priemonių tam – antivirusinė programinė įranga su nuolat atnaujinama virusų duomenų baze. Žemiau išvardintos kelios tokios sistemos:

- Dr.Web. nemokamas Lietuvos valstybinėms mokymo įstaigoms.
- Avast! AntiVirus, Avast! 4home– nemokama versija namų vartotojams.
- AVG Anti-Virus .
- Windows Defender. Microsoft priemonė, skirta piktybinėms programoms aptikti ir užtikrinti nuolatinę kompiuterio apsaugą. Skirta operacinėms sistemoms Windows 2000, Windows XP ir Windows Server 2003, 2008, 2010.
- Lavasoft Ad-aware, skirta aptikti ir išnaikinti piktybines reklamines, šnipinėjimo ir panašias programas. Ad-aware Standard Edition – nemokama nekomerciniam naudojimui.
- McAfee VirusScan .
- BitDefender .
- Nod32
- Norton Antivirus .
- Comodo Antivirus.

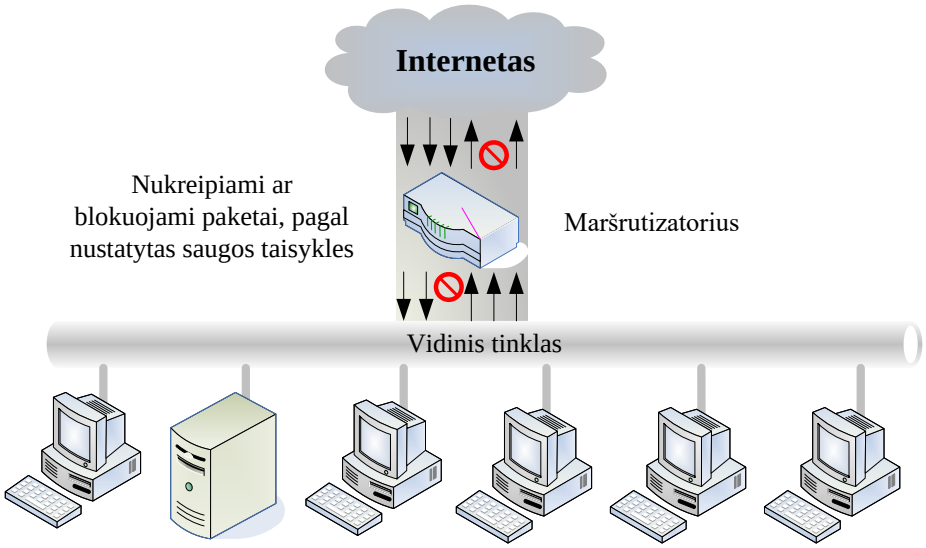
Pavojų keliantys failai

Kita didelė problema yra pačių interneto vartotojų pernelyg didelis patiklumas. Internetas nėra saugi vieta, nes kartu su jums reikalinga informacija, čia jūs galite gauti ir piktybinių programų, virusų.

Siekdami piktavališkų tikslų, įsilaužėliai bei virusai specialiai suformuoja žinutes, kurios įtikina nieko neįtariantį vartotoją pažiūrėti prisegtus laiško priedus, įvykdyti atsiųstą programą. Dažnai tokių atakų aukos patiki suklastotu atgaliniu adresu (laiško laukas „Nuo:“), žinutės tema, specialiai parinktu žinutės tekstu (pvz. pasiūlymas įdiegti atsiųstas saugumo pataisas) ar kitais žinutės požymiais. Toks puolimo metodas vadinamas socialine inžinerija.

Paketų filtravimas

Paketų filtravimo sistemos , nukreipia paketus tarp vidinių ir išorinių kompiuterių, bet jie tai daro atrankos būdu. Jie leidžia arba blokuoja tam tikrus paketų tipus tam, kad atspindėti vietos saugumo politiką, kaip parodyta 2 pav. Maršrutizatoriaus tipas, naudojamas paketų filtravimo ugniasienėje, yra žinomas kaip *patikrinimo maršrutizatorius*.



2 pav. Paketų filtravimas tarp vidinio tinklo ir interneto

Paketų filtravimas yra tinklo saugumo mechanizmas, kuris kontroliuoja duomenis tinkle. Pagrindinis įrenginys, kuris jungia IP tinklus, vadinamas *maršrutizatoriumi*. Maršrutizatorius gali būti aparatinės įrangos dalis, kuri neturi jokios kitos paskirties arba jis gali būti programinės įrangos dalis, kuri veikia bendros paskirties kompiuteryje paleidus Unix, Windows ar kitą operacinę sistemą (MS-DOS, Macintosh ar kitą).

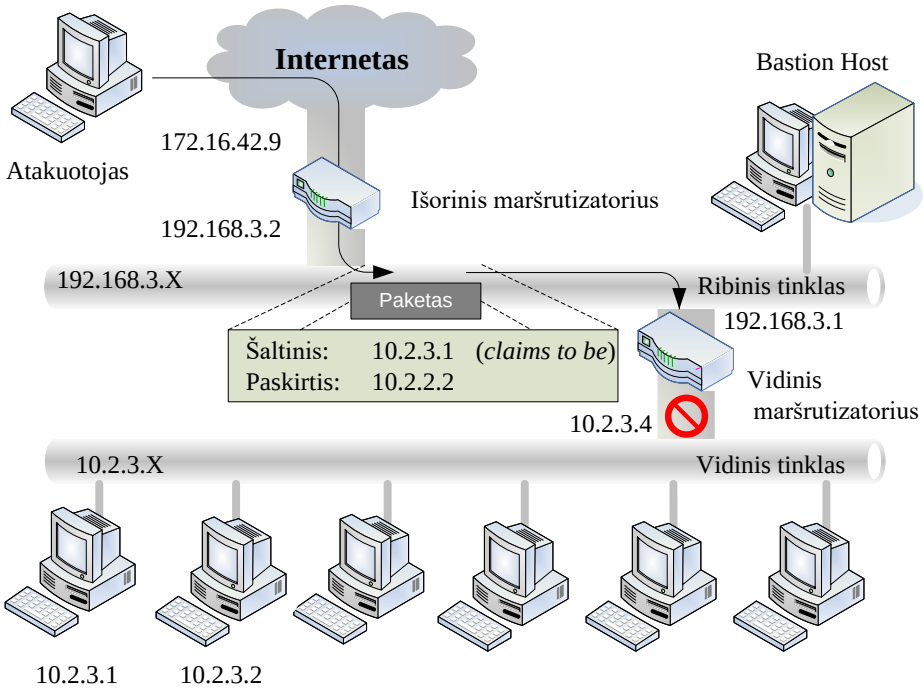
Maršrutizatorius turi nuspręsti kaip nusiųsti kiekvieną paketą, kurį jis gana, į jo galutinę paskyrimo vietą. Pakete yra tik galutinės paskyrimo vietos IP adresas, bet neturi informacijos kaip į tą vietą patekti. Maršrutizatoriai bendrauja vienas su kitu naudodami siuntimo protokolus, tokius kaip informacijos apie maršrutą protokolas (angl. Routing Information Protocol“ (RIP)) ir pirmo laisvo trumpiausio kelio (angl. Open Shortest Path First (OSPF) parinkimo protokolas, kad sudaryti siuntimo maršruto lenteles. Kai siunčiamas paketas, maršrutizatorius palygina paketo paskyrimo vietos adresą su siuntimo lentelėje esančia informacija ir siunčia paketą siuntimo lentelėje nurodytu adresu. Paprastai, maršrutizatoriuje nėra saugomi maršrutai apie paskyrimo vietas. Todėl maršrutizatorius, pagal nutylėjimą, paketą nukreipia į greitesnių ar geriau sujungtų maršrutizatorių pusę. Paprastas maršrutizatorius patikrina tik paketų paskyrimo vietų adresą, o paketų filtravimo maršrutizatorius, pagal paketų filtravimo taisykles, patikrina ar paketas gali būti nukreiptas į konkretų adresą, ar ne. Kai

kurie įrenginiai atlieka paketų filtravimą be maršruto sudarymo; t.y. jie gali priimti arba atmesti paketus, kol jie atliks tolesnį apdorojimą.

Paketų filtravimo rezultatai

Paprastos, greitai ir kiekvienam paketui atskirai vykdomos operacijos lengviau atliekamos paketų filtravimo sistemose. Pagrindinis paketų filtravimo privalumas yra svertų sistema, kuri leidžia apsirūpinti tam tikromis apsaugomis visame tinkle.

Tik tuo atveju, kai filtravimo maršrutizatoriai išdėstyti tam tikrose tinklo vietose, gali būti suteikta neabejotina apsauga. Pavyzdžiui, jei laukiamas paketas su vidinio tinklo adresais, o pasirodo paketai iš išorinio tinklo, gera idėja juos atmesti, nes paketai paprastai turi netikrus adresus ir bando praeiti kaip iš vidinio tinklo (3 pav.). Taip pat reikia atmesti visus vidinius paketus, kurie turi išorinių šaltinių adresus. Sprendimą gali priimti tik vidinio tinklo paketų filtravimo maršrutizatorius.



3 pav. Paketų filtravimo pavyzdys

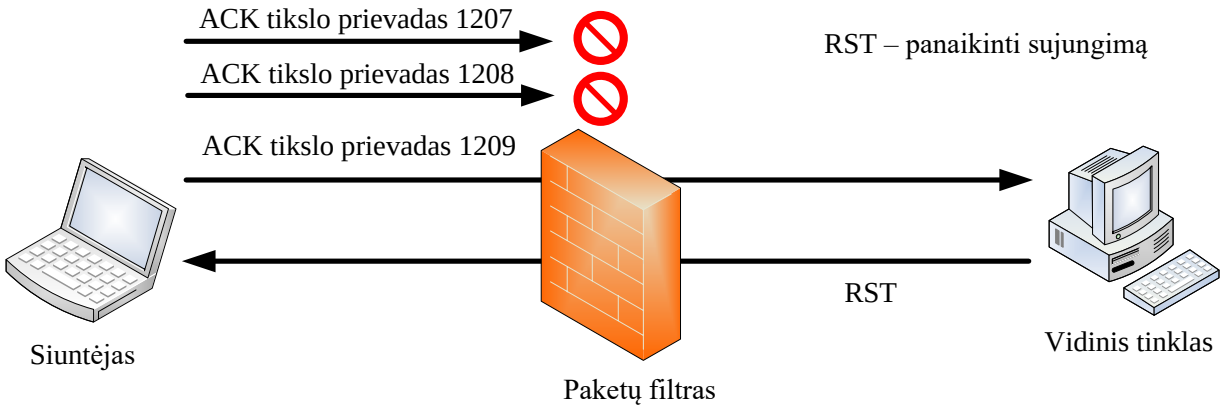
Maršrutizatoriai yra labai patikimi TCP/IP realizavimuose (jie yra nepažeidžiami pasitaikius aukščiau pateiktų puolimų atveju).

Įsimenantis ar dinaminis paketų filtravimas

Įsimenantis (angl. stateful) paketų filtravimas. Kaip matyti iš pavadinimo, įsimenančio paketų filtravimo metu prie paketų filtravimo ugniasienės pridedama būsena, kuri išsaugo TCP jungimosi maršrutą ir atsimena UDP „sujungimus“. Įsimenantis paketų filtravimas veikia transporto lygyje. Šis procesas pavaizduotas 4 pav.

Pagrindinis įsimenančio paketų filtravimo pranašumas yra išeinančių sujungimų maršruto išsaugojimas. Tai apsaugo nuo atakų, tokių kaip veikiančių TCP patvirtinimo numerių (ACK) peržiūra

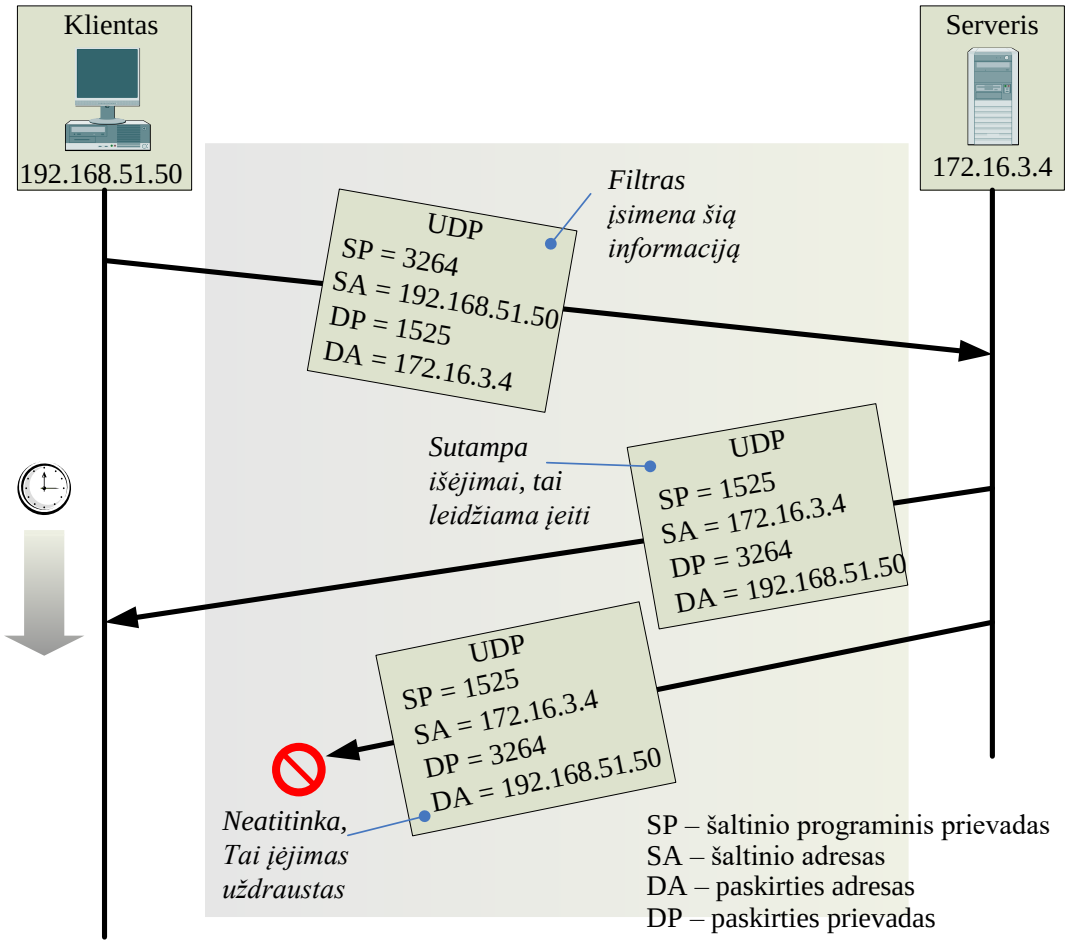
(**4** pav.). Įsimenančio paketų filtravimo trūkumas yra tas, kad negalima patikrinti ar sutampa taikomosios programos duomenys.



4 pav. Veikiančių TCP patvirtinimo numerių (ACK) peržiūra

Dinaminis paketų filtravimas reiškia, kad priklausomai nuo srauto keičiasi sistemos elgesys. Pavyzdžiui, jei naudojame įsimenančio paketų filtravimo taisyklę, negalime peržiūrėti įeinančio UDP paketo ir sakyti, kad visada jis bus priimtas ar atmestas.

Žemiau pateiktas 5 pav. iliustruoja dinaminį paketų filtravimą UDP sluoksnyje.



5 pav. Dinaminis paketų filtravimas UDP sluoksnyje

Būsenos maršruto stebėjimas suteikia daugiau filtravimo galimybių, bet čia yra ir keblumų. Pirma, maršrutizatorius turi išsaugoti būsenos maršrutą; tai papildoma apkrova maršrutizatoriui. Jei paketas gali eiti per likusius be darbo maršrutizatorius, jie taip pat turi turėti tą pačią būsenos informaciją. Yra protokolai šios informacijos keitimui. Ne problema jei dauguma srautų nuolat naudoja tą patį maršrutizatorių, o jų yra ne vienas ir jie likę be darbo. Jei tuo pačiu metu naudojate likusius be darbo maršrutizatorius, būsenos informaciją kiekvienam maršrutizatoriui reikia perduoti nuolat, priešingu atveju atsako paketas gali ateiti anksčiau už būsenos atnaujinimą.

Antra, maršrutizatorius saugo būsenos kelią be jokios garantijos, kad bus atsako paketas. Ne visi UDP paketai turi atsakus. Jei maršrutizatorius neatsako - jis atmeta paketus, kurie turėjo būti priimti. Keletas protokolų specifikacijų pateikia nurodymus, bet nevisada teisingus. Pavyzdžiui, DNS atsakas numatytas 5 sekundžių ribose, bet atsako laikas, po DNS užklausos per Internetą, gali būti ilgesnis nei 15 sekundžių.

Ši filtravimo rūšis taip pat apsaugo nuo adresų suklastojimo; ji patvirtina, kad paketai yra atsakai, pagrįsti jų šaltinių adresais, todėl puolėjas, kuris perima išeinantį paketą, gali suklastoti atitinkamą šaltinio adresą ir grąžinti priimtą „atsakymą“ (ar, priklausomai nuo realizavimo, visą pluoštą paketų, kurie bus priimti kaip atsakymai). Vis dėlto, tai suteikia gana didelį saugumą keletui UDP protokolų, kurie kitais atžvilgiais būtų nepaprastai sunkiai apsaugomi.

Taikomųjų programų įgaliotasis serveris

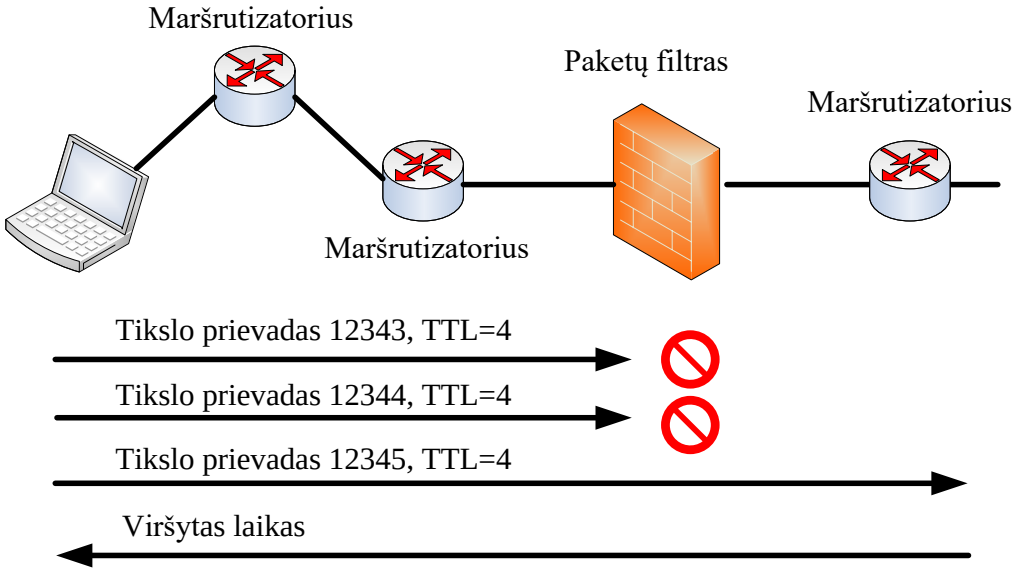
Įgaliotasis serveris (toliau proxy) - tai priemonė, kuri veikia vartotojo naudai. Proxy ugniasienės taikomoji programa visais būdais iki taikomojo lygio sulaiko įeinančius paketus. Vartotojo pusėje ugniasienė patikrina ar paketai teisingi (kaip įsimenančio paketų filtravimo atveju) ir ar pakete esantys duomenys nekelia grėsmės.

Pagrindinis taikomųjų programų proxy privalumas yra pilna sujungimų ir taikomųjų programų duomenų peržiūra. Kaip rezultatas, taikomosios programos proxy gali nufiltruoti blogus duomenis (tokius kaip virusai) taikomajame lygyje, transporto lygyje filtruojami blogi paketai. Taikomosios programos proxy trūkumas yra greitis arba, tiksliau greičio trūkumas. Čia sugaištama daugiau laiko negu paprastame paketų filtravime, kol ugniasienė perdirba paketus į taikymo lygį ir patikrina gautus duomenis.

Įdomi taikomųjų programų proxy savybė yra ta, kad įeinantys paketai sunaikinami, o nauji paketai sukuriami, kai duomenys perleidžiami per ugniasienę. Net jei ši savybė atrodo nereikšminga, ji yra svarbi kaip saugumo savybė. Šios savybės privalumai gerai matomi panaudojus „Firewalk“ įrenginį , kuris suprojektuotas stebėti ugniasienės programinius prievadus.

Gyvavimo laikas, arba TTL (angl. time to live), yra laukas IP pakete, kur įrašytas šuolių kiekis, kuris yra informacija apie paketo nueitą kelią, kol jis baigėsi. Kai paketo kelias nutrauktas interneto kontrolės žinučių protokolas ICMP (angl. Internet Control Message Protocol) šaltiniui siunčia „viršyto laiko“ klaidos pranešimą.

Darome prielaidą, kad siuntėjas žino ugniasienės IP adresą, vienos sistemos IP adresą ugniasienėje ir šuolių kiekį iki ugniasienės. Tuomet siuntėjas siunčia paketą ugniasienei žinomu centrinio kompiuterio IP adresu, o TTL lauke nustatomas šuolių kiekis iki ugniasienės. Darome prielaidą, kad siuntėjas paskirties vietos programinį prievadą nustato į *p*. Jei ugniasienė nepraleidžia duomenų per programinį prievadą *p*, nebus jokio atsako. Jei ugniasienė praleidžia duomenis per programinį prievadą *p*, siuntėjas gaus „viršyto laiko“ klaidos pranešimą iš pirmo maršrutizatoriaus ugniasienės, priėmusios paketą. Siuntėjas gali pakartoti šį procesą skirtingais programiniais prievadais *p* tam, kad nustatyti, kuris prievadas ugniasienėje atviras. Tokių atakų pavyzdys pateiktas 6 pav.



6 pav. „Firewalk“ veikimo pavyzdys

„Firewalk“ negali dirbti per taikomosios programos proxy ir kiekvienas paketas, kuris yra nukreiptas per ugniasienę, yra naujas paketas. Ypač, turi būti nustatytas iš naujo į numatytąją reikšmę, o pagrindinis kompiuteris, kuris priima paketą, neišsiųs „viršyto laiko“ klaidos pranešimo.

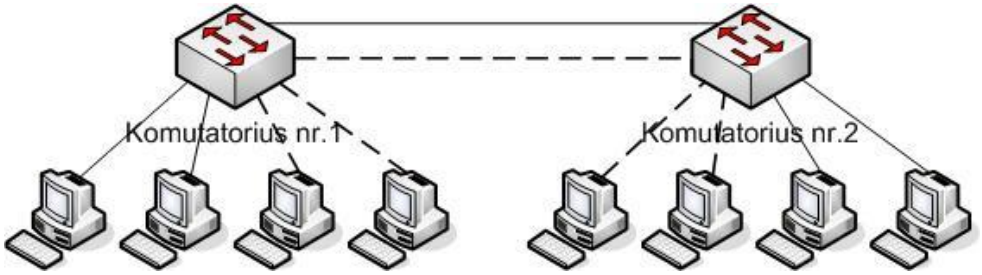
Virtualūs tinklai, sukurti viename komutatoriuje jungčių grupavimo pagalba

Tai racionalu, nes virtualūs tinklai, sukurti vieno komutatoriaus pagrindu, negali būti didesni, nei yra jungčių. Jei prie vienos jungties prijungtas segmentas, sukurtas kartotuvo pagrindu, tai tokių segmentų mazgus nėra prasmės įtraukti į įvairius virtualius tinklus, nes duomenų srautas vis vien nepasikeis.

Virtualių tinklų sudarymas jungčių grupavimo metodu nereikalauja iš administratoriaus daug rankų darbo – reikia kiekvieną jungtį prirašyti keliems skirtingų vardų tinklams. Paprastai tokia operacija atliekama pele perkėlus jungčių grafinius simbolius į tinklo grafinius simbolius.

VLAN tinklas MAC adresų grupavimo metodu

Antras būdas, kuris naudojamas virtualių tinklų kūrimui, yra MAC adresų grupavimas. Tinkle esant daugybei mazgų šis metodas reikalauja daug administratoriaus rankų darbo. Tačiau, jis tampa daug lankstesniu metodu nei jungčių grupavimas, kuriant virtualius tinklus kelių komutatorių pagrindu.



7 pav. Virtualių tinklų kūrimas keliuose komutatoriuose esant jungčių grupavimui

Aukščiau pateiktame 7 pav. vaizduojama problema, kuri iškyla kuriant virtualius tinklus kelių komutatorių, palaikančių jungčių grupavimo techniką, pagrindu. Jei kokie nors virtualaus tinklo mazgai prijungti prie skirtingų komutatorių, tai kiekvieno tokio tinklo komutatorių sujungimui turi būt išskirta sava jungčių pora. Priešingu atveju, jei komutatoriai bus susieti tik viena jungčių pora, informacija apie kadro priklausomybę vieno ar kito virtualaus tinklo, dar prieš perduodant ją iš komutatoriaus, jau bus prarasta. Tokiu būdu, komutatorių su jungčių sugrupavimu susijungimui reikia tiek jungčių, kiek jie palaiko virtualių tinklų. Jungtys ir kabeliai tokiam metodui naudojami labai išlaidžiai. Be to, sujungiant virtualius tinklus per maršrutizatorių, kiekvienam virtualiam tinklui išskiriamas atskiras kabelis, o tai apsunkina vertikalų išskyrimą, ypač jei virtualaus tinklo mazgai išdėstyti keliuose namo aukštuose.

Tinklo MAC adresų grupavimas kiekviename komutatoriuje išvaduoja nuo kelių jungčių ryšio būtinybės, tačiau reikalauja daug rankinio darbo ženklinant MAC adresus kiekviename tinklo komutatoriuje.

Tinklų sauga

Vidinis tinklo ryšys

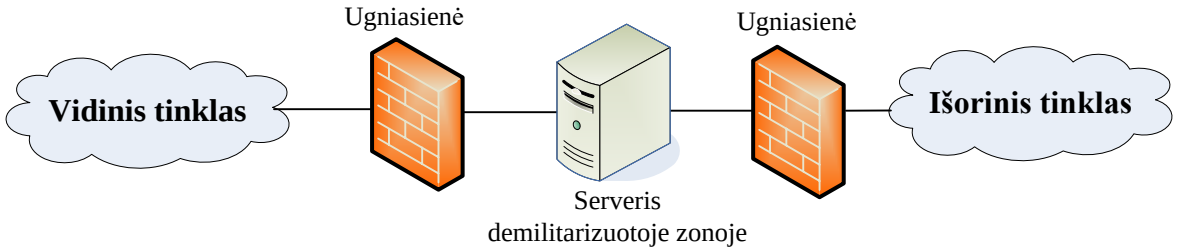
Visuose organizacijos kompiuteriuose, kuriuose saugoma svarbi informacija, privalo būti naudojama informacijos saugumo administratoriaus patvirtinta prieigos kontrolės sistema, t.y. jie turi būti apsaugoti slaptažodžiu. Visi kiti kompiuteriai turi būti apsaugoti ekrano užsklandos (angl. screen

saver) slaptažodžiu. Daugiavartotojiškose IS, naudojamose organizacijoje, privalo būti naudojamos automatinio atjungimo priemonės, leidžiančios automatiškai atjungti prie sistemos prisijungusį, tačiau tam tikrą nustatytą laiką neaktyvų vartotoją.

Išorinis tinklo ryšys

Visi išorinio tinklo prijungimai prie organizacijos vidinio kompiuterinio tinklo privalo būti apsaugoti dinaminių slaptažodžių prieigos kontrolės sistema. Dinaminiai slaptažodžiai – tai kiekvieną kartą jungiantis sugeneruojami nauji slaptažodžiai, kurie užkerta kelią neautorizuotam pakartotinam prisijungimui naudojant tą patį slaptažodį. Vartotojams, kurių kompiuteriai yra prisijungę prie išorinio tinklo, yra draudžiama palikti kompiuterius be priežiūros, išskyrus atvejus, kuomet yra naudojama dinaminių slaptažodžių prieigos kontrolės sistema. Vartotojams, naudojantiems organizacijos kompiuterius, draudžiama užmezginėti ryšius su išoriniais tinklais, įskaitant ir interneto tiekėjus, išskyrus atvejus, kuomet yra gautas Informacijos saugumo administratoriaus leidimas.

Vidinis tinklas nuo išorės turi būti atskirtas ugniasiene. Viešąsias paslaugas tiekiantys serveriai turi būti pajungti demilitarizuotoje zonoje. Demilitarizuota zona – tai speciali saugumo konfigūracija, kai tiek išorinis, tiek vidinis prisijungimas prie serverio yra saugomas ugniasiene (8 pav.).



8 pav. Serveris demilitarizuotoje zonoje, apsaugotas ugniasienėmis iš dviejų pusių

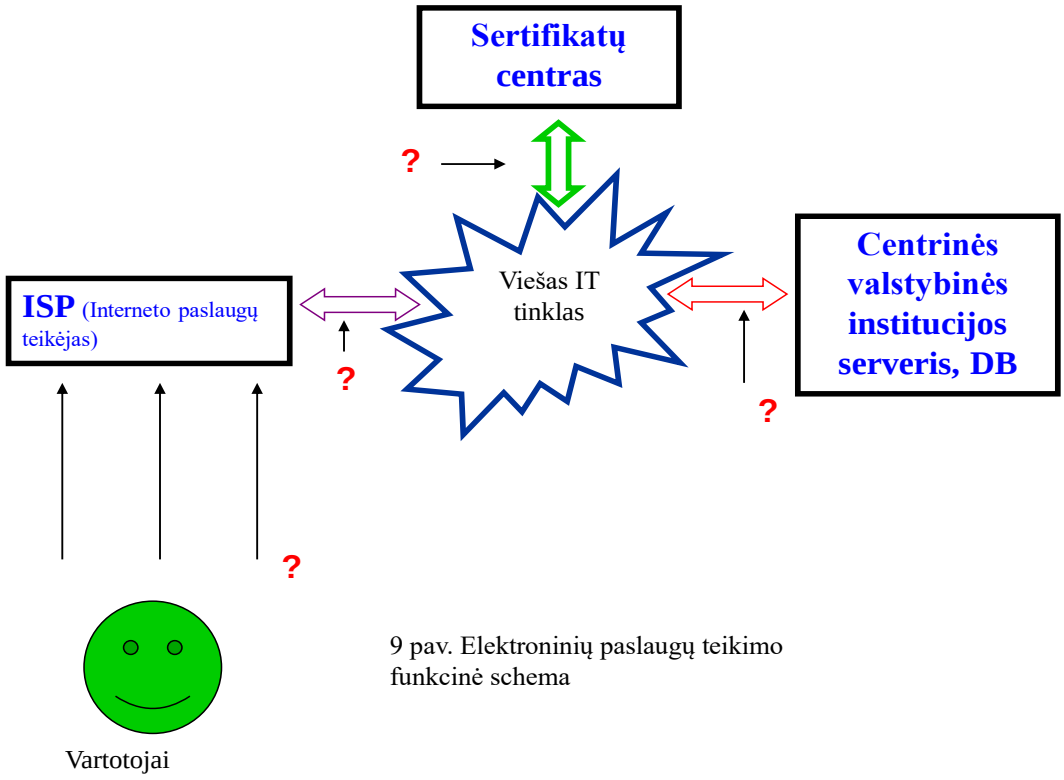
3. Darbo užduotis:

Naudojant IT tinklo įrenginius ***„Fortinet 100“*** , ***„Fortinet 60“***, ***„CR100iNG”*** atlikti tinklo sujungimus pagal schemas, pateiktas 9 ir 10 pav.

Naudoti visas įrenginių funkcines savybes, kurios reikalingos elektroninių paslaugų saugumo užtikrinimui

Naudojantis pateiktais [2] literatūroje pavyzdžiais, nustatyti schemose *„silpnąsias“* saugos grandis, įvertinant ***žmogiškąjį faktorių***, (administratorių gebėjimus, kvalifikaciją, ISP tinklų personalo bei vartotojų kvalifikaciją).

- **Pastaba:** dėl laboratoriniams darbams skirto laiko limito, siūloma laboratorinio darbo užduotį atlikti teoriniame lygmenyje, pildant lenteles Nr1, Nr2.

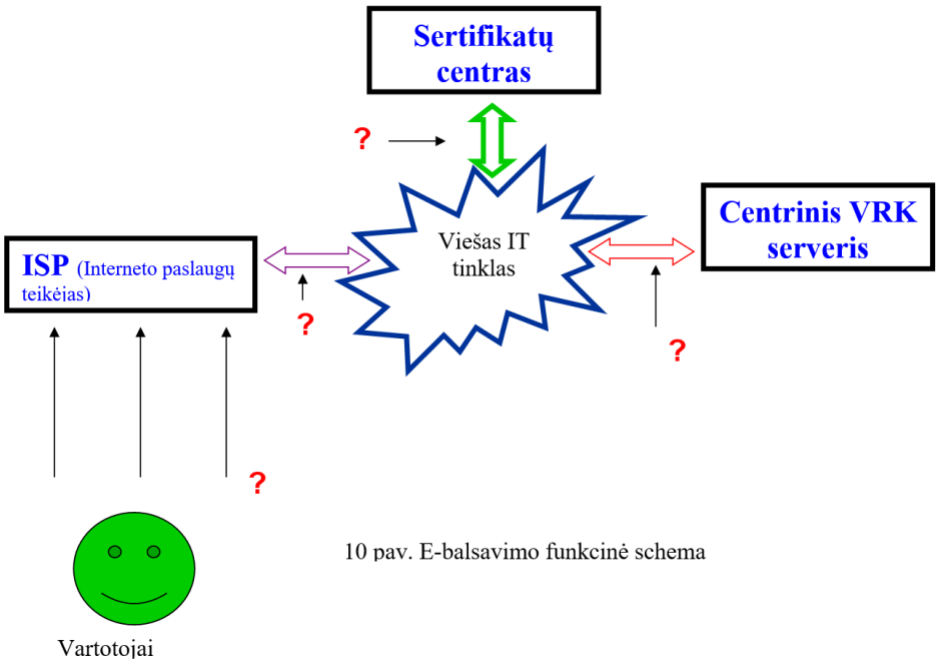


9 pav. Elektroninių paslaugų teikimo funkcinė schema

Lentelė **Nr1**.

Objektai		**Galimos grėsmės**	**Būdai ir priemonės saugos užtikrinimui**
Vartotojai	ISP	• Kenkėjiški failai. • Laužimasis į sistemą	• Antivirusinė • Ugniasienė • Protokolai, kurie yra saugūs • Saugiai sukonfigūruota sistema
ISP	Viešas IT tinklas	• DDOS atakos • Laužimasis Į sistemas, norint gauti prieigą prie tinklo • Virusai	• Šifruoti duomenis • Saugumo politikų taikymas • Atnaujinta programinė įranga

		• Fizinė prieiga prie kompiuterių	
Sertifikatų centras	Viešas IT tinklas	• Atakos kaip DDOS arba MITM • Duomenų nusisavinimas • Netikri sertifikatai • Spragų išnaudojimas	• Saugūs protokolai • Ugniasienės • Antivirusinė • Atnaujinta programinė įranga
CVI serveris, DB	Viešas IT tinklas	• Atakos (DOS, DDOS) • Duomenų klastojimas • Vidinės atakos • Serverio užgrobimas	• Ugniasienė • Saugumo politikos • Atnaujinta programinė įranga.



10 pav. E-balsavimo funkcinė schema

Lentelė **Nr2**.

Objektai		Galimos grėsmės	Būdai ir priemonės saugos užtikrinimui
Vartotojai	ISP	• Kenkėjiški failai (virusai), • Įsilaužimas	• Antivirusinė • Ugniasienė • Aparatinė užkarda • Tinkama konfigūracija
ISP	Viešas IT tinklas	• Tinklo atakos • Virusai	• Ugniasienė • Saugumo taisyklės
Sertifikatų centras	Viešas IT tinklas	• Atakos (DDOS, MITM) • Duomenų klastojimas	• Saugūs protokolai • Ugniasienės

		• Fizinė prieiga	• Saugumo politikos
VRK serveris, DB	Viešas IT tinklas	• Atakos (DOS, DDOS) • Duomenų klastojimas • „Brute Force“ atakos • Serverio perėmimas	• Ugniasienė • Saugumo politikos • Aparatinė ugniasienė • Sisteminiai atnaujinimai

4. Savikontrolės klausimai

a. Pagristi protokolų pasirinkimą
b. Pagristi sertifikatų centro svarbą
c. Pagristi centrinių serverių apsaugą, metodus
d. Aprašyti aptarnaujančiam personalui keliamus reikalavimus
e. Pagristi saugos užtikrinimui naudojamas priemones
f. Nusakyti pateiktų schemų *„silpnas“* grandis
g. Kokios labiausiai tikėtinos atakos e-balsavimo schemos atveju

.

5. Literatūra

1. http://www.ijcttjournal.org/2016/Volume36/number-1/IJCTT-V36P101.pdf
2. RAFAY BALOCH. ETHICAL HACKING AND PENETRATION TESTING GUIDE. ISBN 978-1-4822-3161-8 , © 2015 by Taylor & Francis Group, LLC. 532 pages.
3. Antanas Čenys, Jonas Juknius. Saugumo patikros ir etiško įsilaužimo technologijos. ISBN 978-609-433-071-1. © UAB „TEV“, 2011 . 130 psl.
4. CEHv9 Module 11 Hacking Webservers www.ethicalhackx.com
5. CEHv9 Module 12 Hacking Web Applications www.ethicalhackx.com