Lietuvos mokslo ir studijų institucijų kompiuterių tinklas LITNET

Kauno technologijos universitetas

Virtualių ugniasienių paslauga

Virtualios ugniasienės įdiegimo ir konfigūravimo bei administravimo-stebėjimo aprašas

Paslauga sukurta vykdant Europos socialinio fondo finansuojamą projektą „Mokslo ir studijų institucijoms LITNET teikiamų IT paslaugų plėtra“ Nr. 09.3.3-ESFA-V-711-01-0003

Kuriame Lietuvos ateitį

2014–2020 metų Europos Sąjungos fondų investicijų veiksmų programa

Kaunas, 2019 m.

Turinys

Įvadas

Projekte yra numatyta sukurti ir įdiegti kaip prototipą - Virtualios ugniasienės paslaugą, kuri būtų skirta LITNET informacinių resursų, pasiekiamų per LITNET teikiamas paslaugas, IT apsaugai užtikrinti.

Paslaugą numatoma įdiegti ir taikyti daliai esamų LITNET informacinių resursų esančių LITNET duomenų centruose Kauno ir Vilniaus miestuose. Sudaryti galimybes LITNET institucijoms pasinaudoti centralizuotais LITNET IT saugos resursais, įgalinant tam tikras IT saugos politikas konkrečios LITNET institucijos informaciniams srautams ar resursams esantiems Kauno ir/ar Vilniaus LITNET duomenų infrastruktūroje.

Virtualios ugniasienės taikymo koncepcija

Šiuo dokumentu yra siekiama pateikti esmines strategines kryptis, formuojant bendrą ir tęstinę IT saugos priemonių koncepciją Vilniaus ir Kauno miestuose teikiamų LITNET paslaugų IT Saugos stiprinimui. LITNET paslaugos šiuo atveju yra suprantamos kaip duomenų srautai (tinklo infrastruktūra) bei LITNET klientams teikiamos prieinamos IS paslaugos - Web portalai, e-pašto sistemos, autorizacijos sistemos, failų saugyklos, duomenų bazės ir pan. Įvardintų LITNET paslaugų tiekimui tiesiogiai naudojami tam tikri tinko, fizinių ir virtualizuotų aplikacijų serverių ir saugyklų resursai, bei LITNET techninių centrų lokalių tinklų ir juose esančių pagalbinių techninių priemonių skirtų užtikrinti LITNET paslaugų tiekimą resursai, įskaitant kompiuterizuotas darbo vietas ir jose esančius resursus.

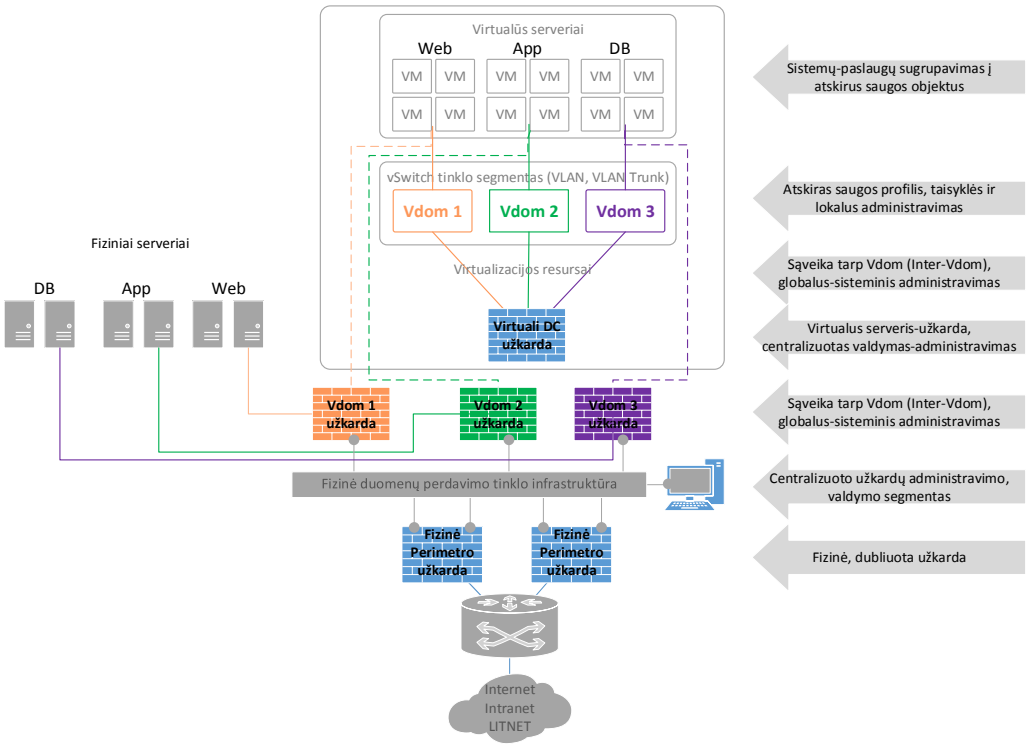
Toliau, šiame etape, (bei išeinant iš aukščiau įvardintų LITNET paslaugų ir su paslaugų užtikrinimu ir priežiūra susijusiais procesais) išskiriame 2 stambius IT saugos objektus-grupes: Duomenų centro resursai (1); ir Administraciniai tinklo resursai (2). Toliau pateikiami koncepciniai IT Saugos sprendimų siūlymai kiekvienai iš įvardintų IT saugos grupių.

Duomenų centro resursų apsaugos sprendimas

Duomenų centro resursų apsaugai siūloma naudoti UTM/NGFW tipo funkcijų įrenginį, kuris būtų konfigūruojamas Skaidriu („Transparent“) arba NAT/Maršrutizavimo („Route“) režimu. Aptarnaujamų sąsajų prasme, gali būti aptarnaujami fiziniai, VLAN Trunk, VLAN sąsajos. Darbo režimo ir aptarnaujamų sąsajų tipas priklauso nuo duomenų tinklo infrastruktūros ar srautų kontrolės galimybių ir tikslus parinkimas priklauso nuo konkretaus duomenų centro esamos situacijos, ir šiame dokumente nėra

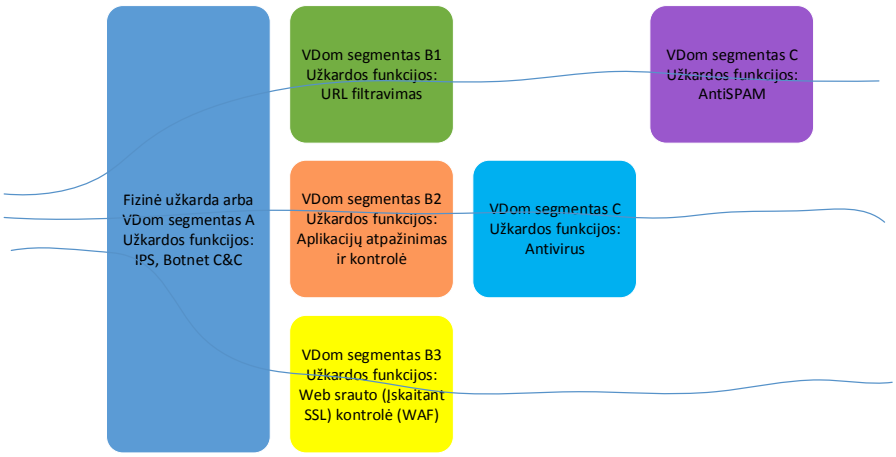
aptariamas, tačiau šiuo dokumentu siekiama pateikti esmines funkcines galimybes, ir įvardinti skirtumus tarp galimų darbo režimų.

Žemiau pateikiamuose paveikslėliuose yra iliustruojama galima ir siūloma LITNET duomenų centro resursų infrastruktūros segmentavimo saugos požiūriu schema (pav.1)



Pav. 1 Segmentavimo schema

ir iliustruojami IT saugos profilių ir politikų galimi scenarijai (pav.2).



Pav. 2 IT saugos profilių ir politikų galimi scenarijai

Toliau pateikiamos minimalios-pradinės rekomendacijos, kurios pareikalautų minimalių esamų duomenų centrų srautų ir architektūros pakeitimų-pertvarkymų. Siūlomos sudiegti Saugos politikos ir/ar taisyklės duomenų centro resursų apsaugai būtų tokios:

1. Įeinančio duomenų centro apribojimas ir kontrolė pagal TCP/UDP prievadus ir/ar Aplikacijas. Pavyzdžiui, jeigu saugomas duomenų centras ar jo segmentas teikia Web paslaugas skirtas ir prieinamas viešai iš Internet, formuojamos įeinančio srauto taisyklės uždraudžiančios kreipimąsi į bet kurį TCP/UDP ar Aplikacijos prievadą išskyrus TCP 80 ir 443
2. Įeinančio duomenų centro apribojimas iš tam tikrų pasaulio vietovių/šalių. Taisyklė prasminga tais atvejais jeigu teikiamam duomenų centre ar jo segmente nėra ir negali būti aplikacijų kurios prasmingos pasiekti. Pavyzdžiui plačiau nei iš Lietuvos ar Europos šalių ir pan. Tokia taisyklė atmeta bet kokį srauto kreipinį į bet tokią aplikaciją iš tam tikro šalių/regionų sąrašo.
3. Įeinančio srauto kontrolė draudžiant bet kokius kreipinius iš Botnet sistemoje dalyvaujančių IP/DNS įrašų. Tam naudojama dinamiškai-nuolatos atnaujinama IP/DNS įrašų duomenų bazė, kurioje yra ~ 50.000 įrašų ir kurie yra pripažinti kaip Botnet ir Botnet C&C dalyvaujantys veikloje ir bet kokie paketai iš tokių šaltinių būtų neaptarnaujami.
4. Įeinančio srauto kontrolė, leistiniems įėjimo kryptis aptarnauti, prievadams ir aplikacijoms būtų kontroliuojama atliekant gilesnę protokolo lygio analizę ir taikant tokias papildomas funkcijas kaip IPS ir Antivirus. Pavyzdžiui, bendru atveju kalba daugiausia eina apie HTTP/HTTPS srautą, taigi, tokiu atveju būtų ženkliai sumažintas SQL Injection, PHP bei įvairiausias žalingo kodo tipo atakų kiekis orientuotas į bendrinį Web aplikacijų pažeidžiamumą.
5. Būtų rekomenduojama perimetre, užkardos pagalba, atlikinėti SSL nukrovimą („Off-Load“) įeinančiam srautui į duomenų centrą. Toks funkcijos įdiegimas suteiktų galimybę analizuoti HTTP/SSL/SSH protokolus, aptikti juose esančius žinomus (identifikuotus) pažeidžiamumus, taikyti tai srauto daliai kitus patikros mechanizmus ir/ar funkcijas, t. y. HTTP tipo srautas gali būti nukreiptas į Web aplikacijų užkardą ir pan. Tačiau šiame punkte reikia pateikti tokius pastebėjimus - UTM/NGFW užkardoje būtų reikalinga patalpinti (perkelti) duomenų centre esančių ir naudojančių SSL protokolą resursų (serverių) sertifikatus su privačiu raktu, o tai galimai gali kelti tam tikrų aptarnavimo procesų ir atsakomybių peržiūrą ir perskirstymą nes įprasta praktika kad SSL sertifikatus įkelia, valdo ir tvarko pačios sistemos administratorius-savininkas konkrečiame serveryje arba Proxy. Be to, tokiuose duomenų centro taškuose, kur yra naudojamas didelis kiekis sertifikatų ar sertifikatų

valdymo procedūros yra automatizuotos, bei sertifikatų galiojimas yra labai ribotas ir reikalaujantis atnaujinimo, tokiose taškuose sertifikatų įkėlimas ir veiksmai su jais užkardoje būtų probleminiai.

6. Įeinančio HTTP srauto (labiau kodo) detalizuotai-precizinei analizei ir užkardinimo funkcijų taikymui būtų rekomenduojama diegti specializuotą Web aplikacijų/turinio užkartą (WAF), tačiau šiame dokumente tai nėra aptarinėjama.
7. Įeinančiam srautui į duomenų centro resursus ir jame esant santykinai dideliam HTTP/HTTPS srautui būtų prasminga užkardą įrengti kaip HTTP ir HTTPS apkrovos paskirstymo įrenginį, aišku jeigu esama klasterizuotų HTTP/HTTPS aplikacijų-serverių. Pravartu pastebėti, kad UTM/NGFW tipo užkardos sistemos nėra specializuotos apkrovos balansavimo sistemos, jos yra ribotos savo protokolų ir mechanizmų palaikymu, tačiau gali būti efektyviai pritaikomos esant momentiniam Web srauto intensyvumui ir poreikiui jį išbalansuoti tarp kelių serverių. Pavyzdžiui, tai gali būti – didelis Web srautas studentų priėmimo ar pan. metu.
8. Analogiška funkcija aprašytai p. 3 būtų diegiama ir išeinančiam srautui, tikslu užkardinti komunikaciją su Botnet C&C (botnet komandų ir valdymo įrenginiais, valdančiai kenkėjiška programa užkrėstų sistemų tinklą) tuo atveju jeigu dėl kažkokių priežasčių duomenų centro įrenginiai buvo pažeisti Botnet-o.
9. Analogiška funkcija aprašytai p. 4 būtų diegiama ir išeinančiam srautui išnaudojant IPS ir Antivirus funkcionalumą.
10. Išeinančiam srautui būtų tikslinga taikyti Aplikacijų („Application“) požymio kontrolės funkcijas, kai pagal požymius/parašus yra nustatoma ta ar kita aplikacija ir galimai drausti tos ar kitos aplikacijos srautą iš vidaus į išorę. Pavyzdžiui, tai gali būti RDP, Telnet, SMTP ir pan. aplikacijų atpažinimas ir draudimas bendriniame lygyje.
11. Priklausomai nuo to kaip būtų atlikta duomenų centro segmentacija, t. y. ar būtų išskaidymas į tam tikras paslaugų-sistemų grupes ir jų talpinimas į tam tikrą segmentą ar ne, (Pavyzdžiui, vienas segmentas su Web svetainių FrontEnd-ais, Web svetainių DB; kitas segmentas su Autorizacijos paslaugomis (LDAP, MS-AD, RADIUS ir t.t.), atlikus srauto stebėjimą tam tikram periodui ir pasidarius tam tikrą „apkrovimo charakteristikos bruožą:, būtų prasminga suformuoti tam tikrą, segmentui būdingą, įeinančių sesijų ribojimą (pagal įvairius L2/L3 kriterijus) – tai leistų preventyviai užkardyti DDoS tipo atakas.

Administraciniai tinklo resursai

Po administraciniais tinklo resursais yra suprantami duomenų centruose esančių aplikacijų naudojami resursai (pvz.: LDAP/AD, Duomenų bazės, File saugyklos ir pan.), kurie sąveikauja aplikacijų lygmeniu ir užtikrina paslaugas LITNET naudotojams; tinklo valdymo, administravimo ir adresavimo resursai (pvz.: RADIUS, DNS, DHCP ir pan.); bei administratorių, sistemas prižiūrinčių darbuotojų, kompiuterinės darbo vietos, kurios jungiasi prie bei valdo ir administruoja aplikacinius bei administracinius resursus.

Sprendžiant šio segmento saugą būtų pirmiausia būtų rekomenduojama atlikti papildomą esamų resursų segmentavimą į VLAN-us ir sukurti tam tikras saugos politikas tarp šių administracinių VLAN-ų bei sukurti saugos politikas šiems VLAN-ams bendravimui su kitais VLAN-ais ir išoriniais resursais. Pagrindinis šios segmento saugos uždavinio ir tuo pačiu saugos politikos formavimo skirtumas lyginant su duomenų centro resursų apsaugos atveju yra tas, kad į šį segmentą neturi būti galimybės jungtis iš orinių ir/ar bet kurių kitų vidaus tinklų, nes jame esantys resursai tiesiogiai neteikia jokių paslaugų. Vertinant išvardintas sąlygas šis segmentas turi būti suformuojamas naudojant arba NAT ir/arba „Router“ užkardos darbo režimus. Skaidrus („Transparent“) režimas yra netinkamas saugos politikų efektyviam užtikrinimui šiame segmente.

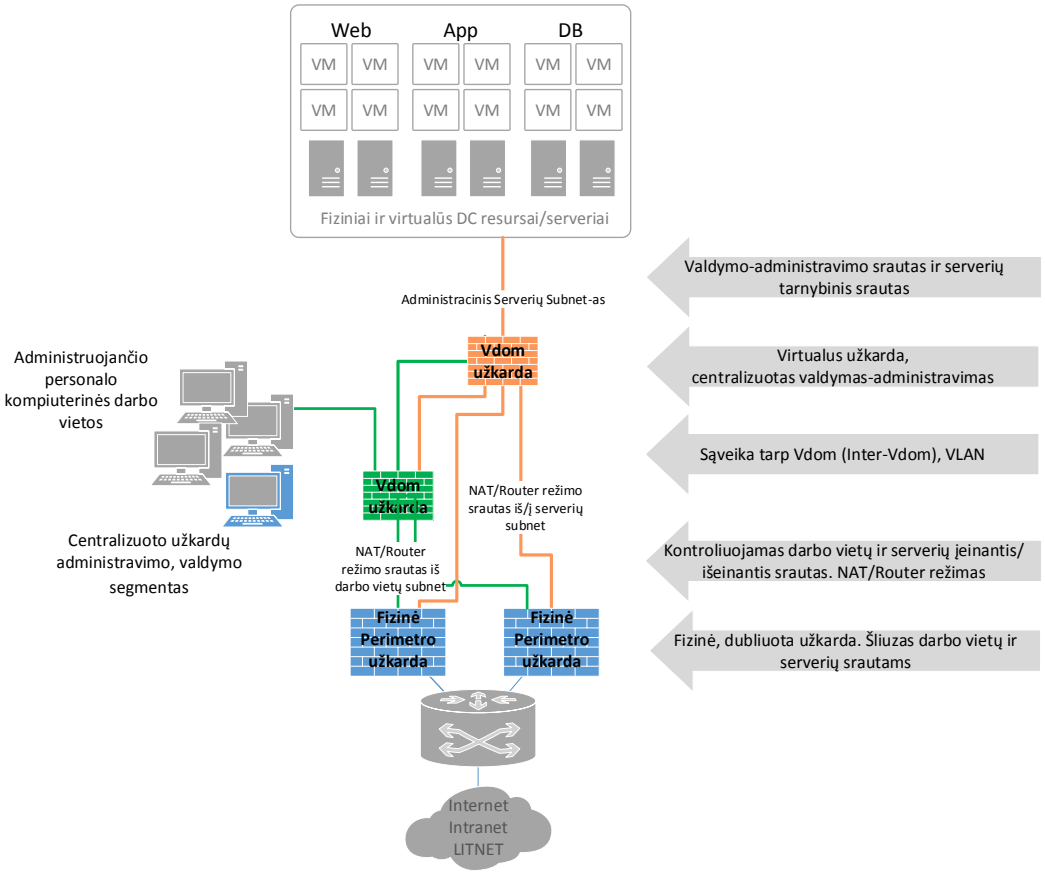
Šiame segmente (Pav. 3) siūlome sudiegti tokias *Saugos politikas* ir/ar *taisykles*:

1. Administruojančio personalo kompiuterinės darbo vietos ryšiui su viešais ir/ar bet kuriais kitais LITNET/KTU tinklais privalo naudoti NAT darbo režimą. NAT atliekamas naudojant vieną ar kelis išorinius IP adresus. Užkarda yra įrengiama kaip šliuzas visam išeinančiam srautui.
2. Bet koks įeinančio srauto iniciavimas į administruojančio personalo kompiuterinių darbo vietų VLAN ar IP adresus yra draudžiamas ir atmetamas.
3. Esant netipiniam ir išskirtiniam poreikiui jungtis į administruojančio užkarda gali atlikti VPN šliuzo vaidmenį; tokiu atveju užkarda sudaro SSL/TLS tipo VPN tunelius. Tunelių pagalba galima prisijungti prie individualizuoto resurso-aplikacijos arba tiesiog įsijungti į segmentą. Tunelio sudarymas atliekamas naudojant administruojančio personalo ir/ar KTU personalo duomenų bazes, naudojant naudotojo ir naudotojo grupės autentikavimą.
4. Išeinantis iš administruojančio personalo darbo vietų srautas nėra filtruojamas ar ribojamas išskyrus bet kurio pobūdžio srautą kurio adresatai yra įtraukti į Botnet ar Botnet C&C dinamines duomenų bazes.
5. Išeinantis iš administruojančio personalo darbo vietų srautas yra stebimas specializuotų saugos profilių (taisyklių), inspektuojant išeinantį duomenų srautą nuo galimo žalingo kodo, virusų, nuorodų

į žalingo ar kenkėjiško kodo svetaines/nuorodas. (IPS, „Antivirus“, DNS, Web URL, „Malware“ funkcijos).

6. Išeinantis HTTPS, SSH srautas (SSL/TLS) nėra inspektuojamas (nėra nešifruojamas) išskyrus paketo antraštės informaciją.
7. Aprašant paslaugas aptarnaujančių (serverių) resursų segmento duomenų srauto taisykles, pirmiausia yra nustatomi komunikacijos su išoriniais tinklais poreikiai (būtinumas) ir juos nustačius atskiriems paslaugų aptarnavimo serveriams (grupėms) sudaromos individualizuotos išeinančio srauto taisyklės, įvertinant galimus adresatus, prievadus, aplikacijos aprašus ir protokolus.
8. Išeinančiam iš paslaugas aptarnaujančių (tarnybinių stočių) resursų segmento duomenų srautui yra taikoma NAT funkcija. NAT transliavimui į išorinius tinklus yra naudojami kiti išoriniai IP adresai nei administruojančio personalo darbo vietoms.
9. Bet koks išorinio įeinančio srauto iniciavimas į paslaugų aptarnavimo segmentą yra draudžiamas ir atmetamas, išskyrus VPN tunelius ir srautus iš administruojančio personalo kompiuterinių darbo vietų.
10. Visam iš/į paslaugas aptarnaujančiam (įeinančiam ir išeinančiam) duomenų srautui yra taikomos srauto filtravimas ir inspektavimas pagal tam tikras taisykles, ribojant nenaudojamus paslaugos protokolus ir prievadus, bei galimai inspektuojant srautą pagal maksimalias užkardos galimybes.

Žemiau pateikiama bendrai iliustruojanti siūlomą administracinio ir duomenų srautų segmento saugos zonų saugumo ir darbo režimus, bei duomenų srautus.



Pav. 3 IT saugos politikos taikymas

Toks fizinės struktūros formavimas sprendžia tokius esminius duomenų srautų formavimo ir IT saugos politikos duomenų uždavinius:

- LITNET duomenų centrų resursai, esantys Vilniaus ir Kauno universitetuose – konkrečiai VU ir KTU yra išskiriami iš bendro VU ir KTU duomenų srauto ir nukreipiami per užkardas. Sprendimas pareikalaus duomenų srautų esamuose magistraliniuose ir/ar duomenų centrų lygmens maršrutizatoriuose (maršrutizuojančiuose komutatoriuose) tam tikrų (identifikuotų kaip LITNET DC) VLAN segmentų ir/ar IP tinklų/potinklių iškėlimo ir atidavimo aptarnauti įrengiamoms užkardoms. Užkardose veikiausiai reikės naudoti ir rekomenduojama naudoti tiek dinaminius maršrutizavimo (OSPF, BGP); tiek aukštą patikimą įgalinančius (VRRP) protokolus.
- VDU ir VGTU kaip LITNET partneriai šiuo metu neturi savo duomenų centruose unikalių LITNET paslaugų-resursų, tačiau pas šiuos partnerius yra duomenų centrų objektai, kuriems bendrame LITNET projekto kontekste yra taip pat būtina užtikrinti duomenų srautų ir IT saugos politikų įdiegimą. Detalesnė analizė parodė, kad šiuo metu būtų reikalinga suformuoti ir padidinti

IT saugą šių institucijų (VDU, VGTU), administraciniams ir mokslo bei studijų poreikiams tenkinti naudojamiems, serverių duomenų srautams apsaugoti.

- Formuoti naujus, loginiu ir administraciniu požiūriu paslaugų ar būsimų projektų segmentus į nepriklausomus segmentus-zonas duomenų srautų ir/ar paslaugų požiūriu , suteikiant stambios paslaugos ar projekto lygyje galimybę pilnai valdyti duomenų srautus ir diegti IT saugos politikas nepriklausomai.
- Sumažinti įsigytos įrangos našumo ir funkcionalumo rizikas nuo galimos grėsmės duomenų srautų arba funkcionalumo augimo poreikio ateityje, tam numatant architektūros ir funkcionalumo plėtrą.

Bazinė ugniasienių IT saugos politika

MSI perimetro apsaugos politika

1. Duomenų srautas kompiuterių tinkle turi būti kontroliuojamas ugniasiene;
2. Ugniasienės tinklo sąsajų zonos yra pavaizduotos šiame dokumente "Ugniasienės tipai";
3. Ugniasienės taisyklių sąrašas yra atspausdinamas, pateikiamas MSI ir peržiūrimas ne rečiau kaip kartą per ketvirtį. IT apsaugos audito metu, jei toks būna, patikrinamas šio sąrašo atitikmuo realiai ugniasienės konfigūracijai;
4. Ugniasienė yra patalpinta virtualiai fiziškai apsaugotoje patalpoje;
5. Ugniasienės taisyklė pagal nutylėjimą – **deny all inbound and outbond packets**;
6. Ugniasienė valdoma naudojant saugaus šifruoto prisijungimo metodus;
7. Visos nenaudojamos ugniasienės sąsajos yra užblokuotos;
8. Kiek tai įmanoma, ugniasienės sisteminių įrašų žurnalai (angl. logs) yra persiunčiami į sisteminių įrašų centralizuotą tarnybinę stotį arba tam skirtą informacinę sistemą;
9. Ugniasienės sisteminiai įrašai yra saugomi ne mažiausiai kaip **6 mėn.**;
10. Ugniasienės vidinių adresų užmaskavimui yra panaudojama NAT technologija, nebent nustatytą kitaip;
11. Ugniasienės kritiniai klaidų ištaisymai yra sprendžiami per **24 darbo valandas**;
12. Ugniasienė parengta ir blokuoja šiuos srautus:
    a. Neautentifikuotų šaltinių įeinantį srautą, kai gavėjas – ugniasienė;
    b. Įeinantį srautą, kai šaltinio adresas – vienos iš ugniasienės sąsajų adresas;
    c. Įeinantį ICMP srautą;

d. Įeinantį ar išeinantį srautą su IP adresais 127.0.0.1 arba 0.0.0.0;
e. Įeinantį ar išeinantį srautą su transliuojamais (angl. „broadcast“) IP adresais.

13. Ugniasienės kontroliuojamų zonų schema ir aprašymas turi būti saugomi pas MSI elektroniniu pavidalu kaip failas **IPadr_conf.doc** ;
14. Ugniasienės konfigūracijos keitimas galimas tik užpildžius atitinkamą taisyklių keitimo formą, kurioje nurodomas užsakymo laikas, kiek laiko turi galioti taisyklė, kas ir ką užsako, kokie turėtų būti pakeitimai ir koks laukiamas bei gautas rezultatas.

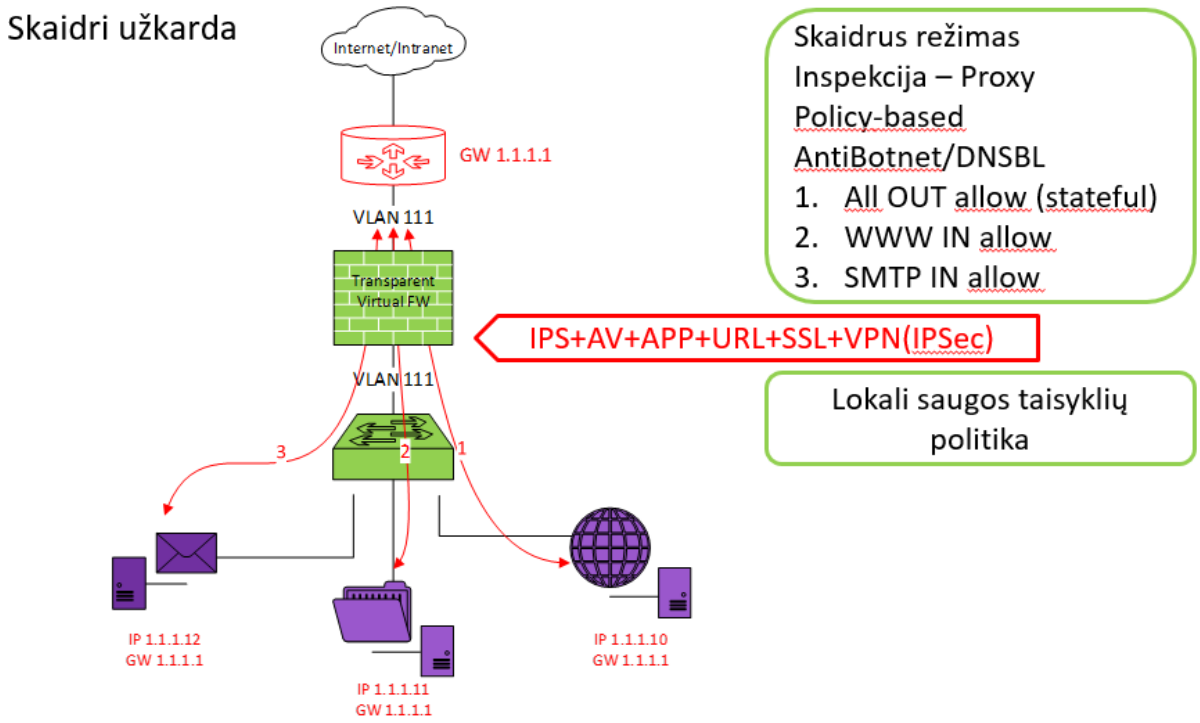
Ugniasienės priėjimo teisių suteikimo politika

1. Teisės turi būti suteikiamos rolių pagrindu, vartotojai turi būti priskirti rolėms. Draudžiama teises suteikti tiesiogiai darbuotojų prisijungimo vardams;
2. Svarbiems MSŠ informaciniams ištekliams turi būti paskirtas atsakingas asmuo (iš vadovų), kuris sprendžia priėjimo prie informacijos teisių suteikimo klausimą (t.y. prieigos teisių matricos pakeitimo klausimą);
3. Ne rečiau kaip kartą per **6 mėnesius** turi būti pasirinktinai patikrinama, kaip priėjimo teisių matrica atitinka realią būseną;
4. MSI pati turi parengti ir dokumentuota priėjimo teisių suteikimo, kontrolės ir panaikinimo vidaus procedūra.

Galimi virtualių ugniasienių diegimo režimai

Skaidrus („Transparent“) ugniasienės režimas

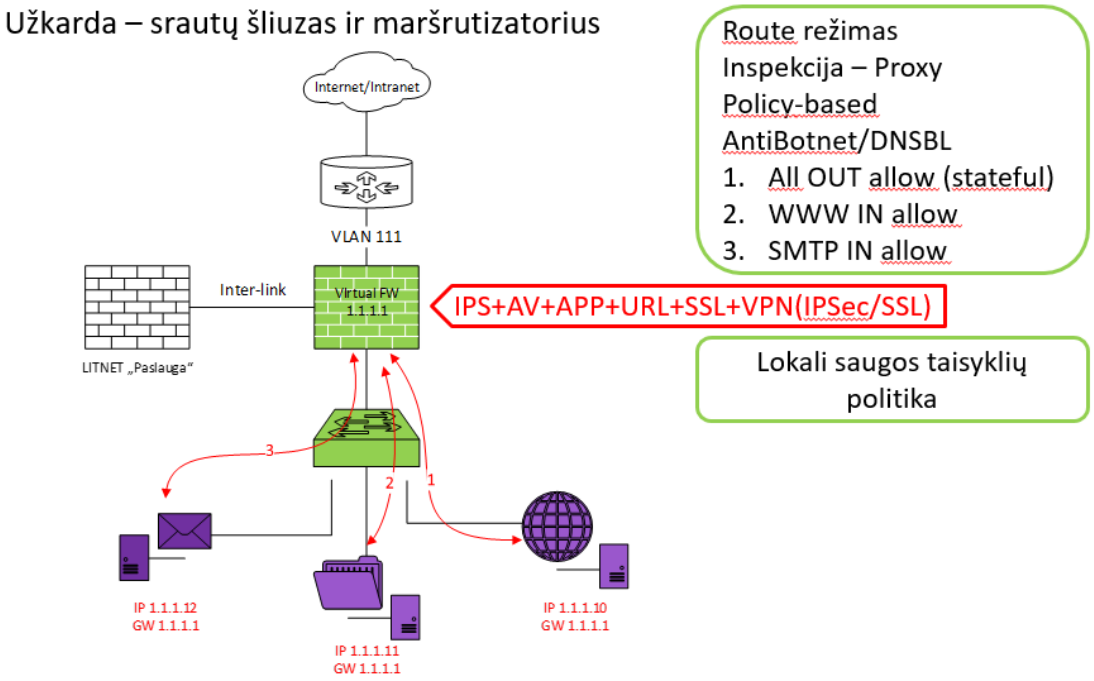
Skaidrus režimas (angl. „transparent“) – įrenginys jungiamas į tinklą skaidriai neįtakojant esamos IP adresacijos ir elektroninio pašto srautų.



Pav. 4 Skaidrus ugniasienės režimas

Maršrutizavimo režimas

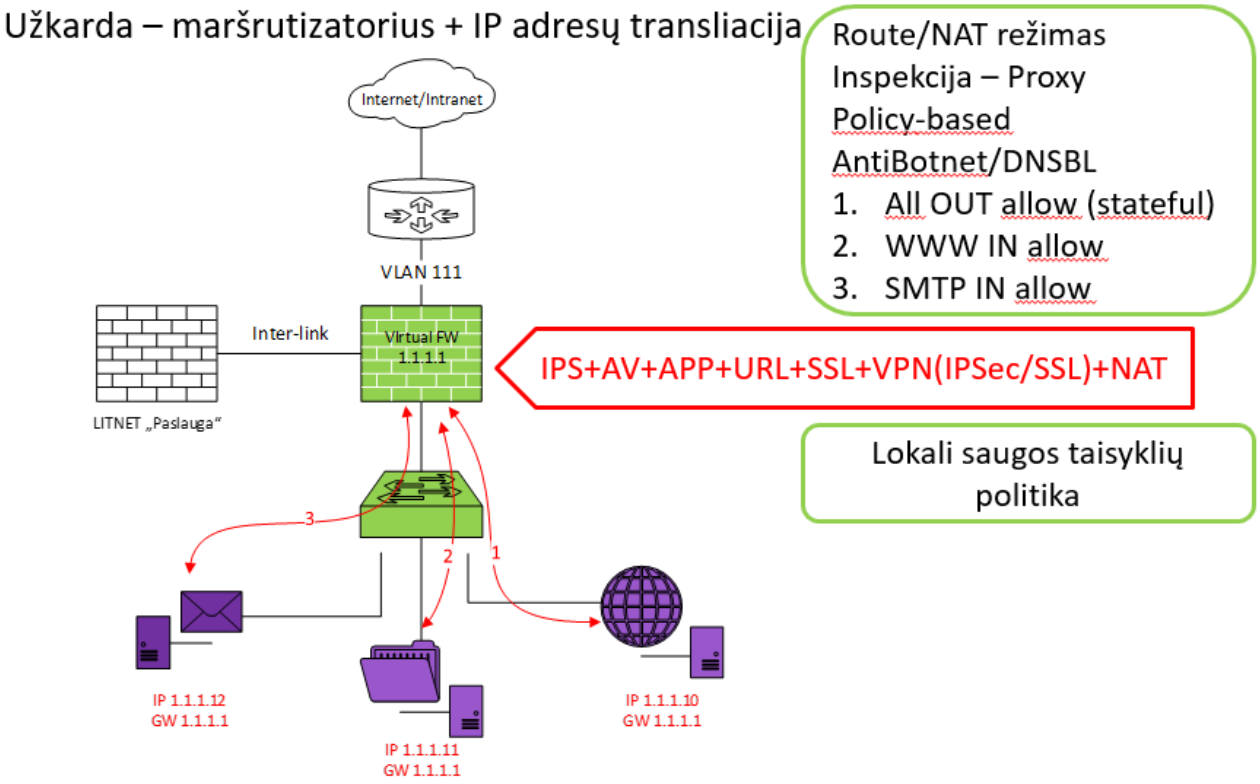
Maršrutizavimo režimas – įrenginys jungiamas į tinklą taip, kad priimtų gaunamus ir siunčiamus laiškus vietoj esamo elektroninio pašto serverio ir tik po patikrinimo perduotų tolimesniam transportavimui.



Pav. 5 Maršrutizavimo režimas

IP adresų transliacijos režimas

IP adresų transliacijos režimas (angl. NAT) – įrenginys jungiamas į tinklą ir jo sąsajose, naudojančiose IP adreso informaciją, vykdoma esančiame už NAT tinko mazge programa turi žinoti tikslų išorinį NAT maršrutizatoriaus adresą.



Pav. 6 Maršrutizavimo/IP adresų transliacijos režimas

Inspektavimo režimai

Pasirinkus tiek Skaidrų (angl. „Transparent“) tiek Maršrutizavimo/IP adresų transliacijos („Route“/ NAT) režimus galimi „Flow-based“ ir „Proxy-based“ inspektavimo režimai. „Flow-based“ inspektavimas – identifikuoja galimas saugumo grėsmes ir atakas, naudojant tiesioginio filtro metodą (angl. „DFA - Direct Filter Approach“) ir blokuoja realiu laiku. „Proxy-based“ inspektavimas apima „flow-based“ inspektavimo režimą – ištraukia ir saugo turinį (pvz.: failus ir tinklapius), toliau atlieka išsaugoto turinio inspektavimą nuo grėsmių. „Flow-based“ ir „Proxy-based“ inspektavimo funkcionalumas palyginamas lentelėje 1.

1 Lentelė "Flow-based" ir " Proxy-based" funkcionalumo palyginimas

Funkcija	**Flow-based inspekcija**	**Proxy-based inspekcija**
Anti-virus	✓	✓
Web filtravimas	✓	✓
DNS/Botnet filtravimas	✓	✓

Aplikacijų kontrolė	✓	✓
IPS	✓	✓
Anti-Spam	×	✓
DLP	×	✓
VoIP	×	✓
ICAP	×	✓
WAF	×	✓
Proxy opcijos	✓	✓
SSL inspekcija	✓	✓
SSH inspekcija	×	✓
IPSec GW	✓ tik Policy-based	✓
SSL GW	✓ tik Route/NAT	✓ tik Route/ANT

Tinklų saugumo didinimas

Tinklų saugumas yra pasiekiamas, naudojant įvairius įrankius, įskaitant ugniasienes. Ugniasienė yra vienas iš bazinių tinklo saugumo įrankių. Ugniasienės yra statomos tarp vidinio tinklo ir interneto. Jos suteikia centralizuotą tašką, per kurį eis visas duomenų srautas. Šiame taške labai patogu vykdyti stebėjimą ir žurnalizavimą. Tik vykdant visų šių saugumo užtikrinimo priemonių auditą galima pakelti sistemos saugumo lygį. Dažniausiai visi išvardyti aukščiau įrankiai turi žurnalizavimo mechanizmus ir auditavimo priemones. Viena iš efektyvių priemonių yra srautų žurnalizavimas ugniasienės lygmenyje tam, kad vėliau būtų galima atlikti analizę (prevencija, istorija). Analitikams lieka tik iš visų dalių surinkti duomenis ir agreguoti juos į bendrą ataskaitą. Taip pat verta paminėti, kad tokio tipo paketai, kurie integruoja skirtingus saugumo užtikrinimo įrankius ir pateikia bendrą valdymo panelę ir bendrus stebėjimo rezultatus yra naudojame ir šio projekto rėmuose. Todėl LITNET specialistai galės pateikti statistinę, bei analitinę apžvalgą pagal individualų poreikį.