

**DATORTĪKLA DROŠĪBAS SISTĒMA  
“UGUNSSIENA”**

**ADMINISTRATORA  
ROKASGRĀMATA**

v. 3.3.4



# Saturs

<b>1. Ievads</b> .....	<b>5</b>
<b>2. Iespējas</b> .....	<b>5</b>
<b>3. Terminoloģija</b> .....	<b>5</b>
<b>4. Sistēmas vadība</b> .....	<b>6</b>
<b>5. Konfigurācijas servera instalēšana</b> .....	<b>6</b>
<b>6. Pieslēgšanās konfigurācijas serverim</b> .....	<b>10</b>
<b>7. Sistēmas galvenā komandkarte (Start)</b> .....	<b>11</b>
<b>8. Ugunssienas instalēšana no konfigurācijas servera</b> .....	<b>12</b>
<b>9. Ugunssienas programmas atjaunināšana (Upgrade)</b> .....	<b>13</b>
9.1. Atjauninājumu failu augšupielādēšana.....	13
9.2. Atjauninājumu instalēšana .....	13
<b>10. Konfigurēšana</b> .....	<b>14</b>
10.1. Grupas .....	14
10.2. Adrešu grupas (Address groups) .....	14
10.3. Tīkla protokolu grupas (Protocol groups) .....	15
10.4. E-pasta adrešu grupas (E-mail groups).....	15
10.5. Ugunssiena (Host).....	16
10.6. Ugunssienas komponentu lapa .....	17
10.7. Tīkla interfeiss (Network interface) .....	17
10.7.1 Tīkla interfeisa pamat konfigurācijas parametri .....	18
10.7.2 Virtuālie interfeisi (Vlan).....	18
10.7.3 Virtuālais rezervēšanas interfeiss (VRRP) .....	18
10.8. Maršrutētājs (Router) .....	18
10.9. Sertifikātu serveris (CA) .....	19
10.9.1 Informācija par sertifikātu.....	20
10.9.2 Sertifikātu servera konfigurēšana.....	20
10.9.3 Jauna sertifikāta pievienošana .....	20
10.9.4 Sertifikāta pieprasījuma augšupielādēšana .....	21
10.9.5 Ģenerēt sertifikāta pieprasījumu un privāto atslēgu .....	21
10.9.6 Lietotāju pieprasītie sertifikāti .....	21
10.10. Virtuālais privātais tīkls (VPN).....	21
10.10.1 Tunelis uz specifisku IP adresi .....	22
10.10.2 Tunelis starp diviem konfigurācijas servera hostiem .....	24
10.10.3 Tunelis ar nenoteiktu otrā gala adresi.....	24
10.10.4 CIPE VPN tunelis .....	24
10.11. Ugunsmūris (Firewall) .....	24
10.11.1 Ugunsmūra filtri .....	25
10.11.2 Lietotāju autorizācija .....	27
10.11.3 Rezerves kopijas .....	27
10.11.4 Drošības uzraudzības žurnāls (Security monitoring) .....	27
10.11.5 Uzbrukumu detektors (Intrusion detection) .....	27
10.12. Tīkla adrešu tulkošana (Network address translation - NAT) .....	29
10.13. HTTP starpniekserveris (HTTP proxy).....	31
10.14. Datu plūsmas uzskaitē (Traffic accounting) .....	32
10.15. E-pasta serveris (E-mail server) .....	33
10.15.1 E-pasta servera globālie konfigurācijas parametri .....	33
10.15.2 Lietotāju kontu konfigurēšana .....	34
10.15.3 Lietotāju meklēšana.....	34
10.15.4 Lietotāju pievienošana.....	34
10.15.5 Sistēmas statusa informācija (System information).....	36
10.15.6 Vēstuļu statistika („Mail statistics”) .....	36
10.15.7 Lietotāju statistika („User statistics”).....	36
10.16. E-pasta kontroles sistēma (E-proxy) – centrālā konfigurācija.....	36
10.16.1 Vispārīgie E-proxy konfigurācijas parametri.....	36
10.16.2 SMTP un e-pasta apstrādes filtri .....	37

10.16.3	SMTP filtri .....	38
10.16.4	E-pasta apstrādes filtri – kopīgā konfigurācija .....	38
10.16.5	E-pasta apstrādes filtri – specifiskā konfigurācija .....	40
10.16.6	E-pasta izejošie filtri .....	40
10.16.7	E-proxy caurspīdīgais režīms .....	40
10.16.8	E-proxy paziņojumu sagataves .....	41
10.17.	E-pasta kontroles sistēma (E-proxy) – lokālā konfigurācija .....	42
10.17.1	E-pasta vēstules apstrādes rindā .....	42
10.17.2	Aizturētās e-pasta vēstules .....	43
10.17.3	Pretvīrusu programmu vīrusu bāzes .....	43
10.17.4	Spam filtra datubāze .....	44
10.17.5	Izaicinājuma/atbildes filtra datubāze (Challenge/response) .....	44
10.17.6	E-proxy statistika .....	44
10.17.7	E-pasta vēstules apskatīšana pēc viņas ID vērtības .....	44
10.18.	Datu plūsmas pārbaude (Net check) .....	45
10.19.	DHCP serveris .....	46
10.20.	DNS buferserveris (DNS cache) .....	47
<b>11.</b>	<b>Administrēšanas logs (Administrative) .....</b>	<b>48</b>
11.1.	Jauns sistēmas lietotājs .....	49
<b>12.</b>	<b>„Tools” .....</b>	<b>49</b>
12.1.	Log faili .....	49
12.1.1	Vispārējā statistika .....	50
12.1.2	Log failu izvēles un apskates forma .....	50
12.2.	Address info .....	51
12.3.	Ping .....	51
12.4.	Traceroute .....	52
12.5.	ARP .....	52
12.6.	Process List .....	52
12.7.	Disk space .....	52
12.8.	Upgrade manager .....	52
12.9.	Iekārtu bojājumu noteikšanas sistēma (Host status monitor) .....	52
<b>13.</b>	<b>Noslēgums .....</b>	<b>52</b>
<b>14.</b>	<b>Pielikumi .....</b>	<b>53</b>
14.1.	VPN tunelis uz Windows 2000/XP .....	53
14.2.	Glosārijs .....	54

## 1. Ievads

„UGUNSSIENA” ir datortīkla drošības sistēma (turpmāk tekstā – ugunssiena) ar tās pamat komplektā integrētu tīkla vadības un kontroles aprīkojumu. Sistēma nodrošina datortīklu aizsardzību no nesankcionētas lietošanas, kā arī dod iespēju veikt interneta pieejas kontroli.

Sistēma atkarībā no konkrētās komplektācijas var sastāvēt no šādiem servisiem:

- uguns mūris (*firewall*),
- tīkla adrešu tulkošana (*NAT*),
- trafika uzskaitē (*Accounting*),
- tīkla pārbaude (*NetCheck*),
- virtuālais privātais tīkls (*VPN*),
- sertifikātu serveris (*CA*),
- Datu plūsmas satura analīze (*SPY*),
- e-pasta serveris,
- domēna vārdu serveris (*DNS server*),
- maršrutētājs (*router*),
- e-pasta kontroles sistēma (*E-proxy*),
- HTTP starpniekserveris (*HTTP proxy*)

## 2. Iespējas

Ugunssiena pieļauj attālinātu sistēmas kontroli un vadību, kas garantē, ka attiecīgais tīkla speciālists vienmēr varēs piekļūt sistēmai un vajadzības gadījumā veikt nepieciešamās konfigurācijas izmaiņas. Sistēma piedāvā netikai attālinātu vadību, bet arī centralizētu vadību. Kas nozīmē, ka vairākus attālinātus tīkla punktus, kuros uzstādīta ugunssiena, iespējams konfigurēt no viena punkta (vadības serveris). Šāda centralizēta vadība vēl jo vairāk atvieglo sarežģītu tīklu konfigurēšanu, jo daudzi konfigurācijas parametri ir vienādi visiem punktiem, attiecīgi jākonfigurē tikai vienreiz.

## 3. Terminoloģija

Latviešu valodā ne visiem datorterminiem ir atbilstošie tulkojumi, un lielai daļai no tiem, kam tomēr ir latviskotais variants, tas tomēr ir pārāk neveikls lai to izmantotu aprakstot vienu vai otru terminu. Lai nu, kā arī nebūtu ar tiem latviskotajiem terminiem, šajā rokasgrāmatā tie ir lietoti diezgan plaši, tādēļ lai nerastos nesaprašanas tiem, kas labi pārzina angļiskos terminus, aiz latviskā termina parasti ir norādīts angļiskais, *italic* šriftā:

ugunsmūris (*firewall*).

Rokasgrāmatas tekstā īpaši ir apzīmēti ekrānformu parametri.

WEB norādes (saites) ir pasvītrotas underline šriftā

**[Ekrānformu pogas ir bold šriftā un kvadrātiekvās]**

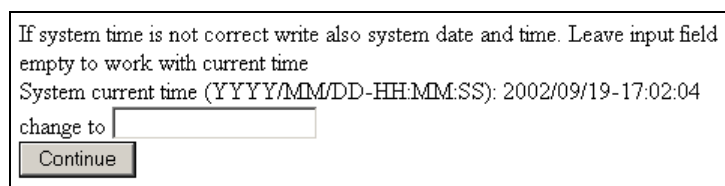
Rokasgrāmatā izmantotās specifiskās terminoloģijas tulkojumi un skaidrojumi latviešu valodā, doti šī dokumenta pielikumā „Glosārijs”.

## 4. Sistēmas vadība

Administratora datorā nav nepieciešams instalēt speciālu programmu darbam ar sistēmu. Konfigurēšana notiek izmantojot vadības serveri, pie kura var piekļūt attālināti caur WEB interfeisu ar jebkuru interneta pārlūkprogrammu, kura atbalsta HTTPS protokolu un uztur X.509 digitālo sertifikātu izmantošanu. Šīm prasībām atbilst gan Microsoft Internet Explorer 5.0, gan Netscape Navigator 4.7 pārlūkprogrammas un jaunākas to versijas. Gadījumā, ja sistēma uzstāda ar īpaši garu (8192 bitu un garāka) šifrēšanas atslēgu tad prasības pret pārlūkprogrammu palielinās, bet visbiežāk prasībām atbildīs administratora iecienītā interneta pārlūkprogramma.

## 5. Konfigurācijas servera instalēšana.

1. Nepieciešamā komplektācija:
  - Minimālās prasības: CPU Intel Pentium I, HDD 1GB, RAM 64MB, CD-ROM (tikai instalēšanas laikā), tīkla karte
  - rekomendētās prasības: CPU Intel Celeron/AMD Duron, HDD 20GB, RAM 128MB CD-ROM, PCI tīkla karte(s)
  - Ugunssienas instalācijas disks (CD)
  - Kāda darbstacija, no kuras kontrolēt instalēšanas gaitu
2. Instalējamā mašīnā CD-ROM iekārtā ieliek instalācijas disku un to pārstartē. Mašīna sāks lādēties no CD diska (tā ir jābūt uzstādītam datora BIOSā). Gaida līdz vairs netiek lasīti dati no CD (CD-ROM lampiņa vairs nemirgo, parasti 1 - 5 minūtes).
3. Atver interneta pārlūkprogrammu, no kāda cita datora kam ir pieeja ugunssienas datoram caur tīklu (lokālais vai internets), un pārlūkprogrammas adresi logā raksta:  
*https://adrese/us*  
kur "adrese" ir vēlamā ugunssienas konfigurācijas servera IP adrese, var izmantot arī vārdisko adresi (firewal.uznemums.lv). Adresei jābūt pareizai (tādai kāda ir iespējama ugunssienas apakštīklā). Konfigurācijas serveris uzskata, ka viņa adrese ir tā, kuru tīklā kāds pieprasa, bet neviens uz to neatbild. Šī iemesla dēļ būtu jāizvairās no konfigurācijas servera instalēšanas atrodoties lielā apakštīklā, jo ugunssiena var paņemt adresi kas nav domāta tai. Kad serveris adresi atradis, tas atbild uz interneta pārlūka sūtīto pieprasījumu, pārlūkprogramma ielādē pirmo lapu jau drošajā, jeb šifrētajā režīmā (https). Tajā klikšķina uz saites „*Press here to start!*”, lai turpinātu instalēšanas procesu.
4. Ielādējas pirmā instalēšanas palīga lapa:



If system time is not correct write also system date and time. Leave input field empty to work with current time  
System current time (YYYY/MM/DD-HH:MM:SS): 2002/09/19-17:02:04  
change to

- Šī lapa ir lai uzstādītu konfigurācijas serverim pareizu laiku, kas ir obligāts un absolūti nepieciešams pasākums. Lapā parādās pašreizējais sistēmas laiks, ja tas nav precīzs, tad precīzu laiku ieraksta ailītē (tā kā norādīts paraugā) un spiež pogu [**Continue**]. Ja laiks nav jāmaina tad ailīti atstāj tukšu.
5. Ielādējas nākamā lapa, pamata (*root*) sertifikāta ģenerēšana.

System need root certificate. Specifie method of making key and certificate:

**Private key**

generate 4096  password

upload file  Choose

**Certificate**

make request to CA

self sign

upload  Choose

certificate is in key file

**Host private key length**

Default value: 4096

Ok

Šajā lapā izvēlas kāds būs pamata sertifikāts (atslēga). Šis būs tas sertifikāts, kas glabāsies uz konfigurācijas servera un ar šo tiks parakstīti visu šim serverim pieslēgto ugunszienu sertifikāti. Ir iespējami vairāki varianti kā iegūt atslēgu un sertifikātu. Ja nav kādas speciālas prasības no sertifikātiem, tad šos standarta uzstādījumus nav vajadzības mainīt, un droši var pāriet uzreiz uz nākamo soli spiežot pogu **[OK]**. Standarta konfigurācija nekādā veidā nav mazāk droša.

- ģenerēt (*Private key generate*) vai augšupielādēt (*Private key upload file*) atslēgu un sūtīt pieprasījumu uz kādu kantori, lai tas paraksta sertifikātu (*Certificate make request to CA*)
- ģenerēt (*Private key generate*) vai augšupielādēt (*Private key upload file*) atslēgu un sertifikātu parakstīt ar to pašu atslēgu (*Certificate self sign*). Šis ir rekomendētais variants.
- augšupielādēt atslēgu (*Private key upload file*) un augšupielādēt atbilstošo sertifikātu (*Certificate upload*)
- augšupielādēt atslēgu un sertifikātu kas atrodas vienā failā (*Private key upload file*), attiecīgi pie „*Certificate*” norāda izvēlni „*certificate is in key file*”

Pēc visām izvēlnēm, zemāk ir sadaļa (*Host private key lenght*) kas norāda ugunszienu noklusēto atslēgu garumu. Šī ir tikai noklusētā vērtība, kuru būs iespējams nomainīt ģenerējot konkrētas ugunszienu sertifikātu.

Kad izvēle izdarīta spiež pogu **[ OK ]**. Pēc pogas nospiešanas sākas atslēgas ģenerēšana, ja tāda opcija izvēlēta. Atkarībā no atslēgas garuma tā var ģenerēties no dažām sekundēm līdz dažām stundām.

Mašīnai ir nepieciešams *root* sertifikāts, tādēļ ja tiek izmantots sertifikāts, kas nav parakstīts ar Ugunszienu *root* sertifikātu, nepieciešams augšupielādēt visus sertifikātus līdz konkrētajam *root* sertifikātam.

- Kad atslēga uzģenerēta ielādējas sertifikāta informācijas lapa.

Write certificate information:

Your name

E-mail

Organization name

Valid time  years (1-30)

Ok

Te ievada kontaktpersonas vārdu, uzvārdu, e-pasta adresi, uzņēmuma nosaukumu, un izvēlas sertifikāta derīguma termiņu gados. Kad tas darīts spiež pogu **[ OK ]**.

Pēc pogas nospiešanas uz ekrāna tiek izdota informācija par konkrēto sertifikātu. Ja informācija ir pareiza tad instalēšanu turpina klikšķinot uz saites „*next*”.

- Informācija par konkrētu ugunszienu, ne vairs kā par konfigurācijas serveri.

Configure host information	
Name	<input type="text" value="install"/>
Private key length	4096
Name server	<input type="text" value="192.168.0.1"/>
Domain	<input type="text" value="firewall.lv"/>
Mode	router
CD-key	<input type="text"/>
<input type="button" value="Ok"/>	

Izvēlas ugunssienas vārdu („Name”), privātās atslēgas / sertifikāta garumu („Private key length”), vārdu serveri DNS („Name Server”), ieraksta domēna nosaukumu („Domain”), izvēlas ugunssienas darbības principu „router” vai „bridge” („Mode”), visbiežāk rūterta darbības modelis ir labākais. Beigu beigās jāievada CD atslēga („CD-key”), šo atslēgu var atrast instalācijas CD vāciņa aizmugurē.

Obligāti aizpildāmie lauki ir ugunssienas vārds un CD atslēga. Kad tie aizpildīti instalēšanu turpina nospiežot [OK] pogu.

8. Instalēšana turpinās.

Installing new "Ugunssiena" host: install
Make certificates to secure installation actions and next configurations:
1) <a href="#">Install host certificate</a>
2) <a href="#">Upload server certificate</a>
<a href="#">Next</a>

Tagad vajag izpildīt abus soliņus.

- a) Klikšķina uz saites „[Install host certificate](#)” lai uzģenerētu un uzinstalētu sertifikātu ko izmantos konfigurācijas servera ugunssiena kontaktējoties ar citām ugunssienām. Atveras mazs pārlūkprogrammas logs, kas piedāvā instalēt sertifikātu. Lai sāktu instalēšanu klikšķina uz saites „[Start](#)”. Sākas sertifikāta ģenerēšana. Kad tas darīts logā ielādējas sekojoša lapa:

Updating host: <b>install</b> 13:17:21 (0)
New configuration is active.
Click to confirm new configuration. System will wait 60 seconds for confirmation.
<a href="#">Accept</a> <a href="#">Decline</a> <a href="#">Close</a>

Lai apstiprinātu jauno sertifikātu, 60 sekunžu laikā pēc lapas ielādēšanās jānoklikšķina uz saites „[Accept](#)”. Pēc tam mazo logu var vērt ciet.

- b) Galvenajā logā klikšķina uz saites „[Upload server certificate](#)”. Šeit ugunssiena saņems konfigurācijas servera atslēgas publisko daļu. Atkal atveras mazs pārlūka logs un tajā jāklikšķina uz saites „[Start](#)”. Kad lādēšanās beigusies, ielādējas jauna lapa. Tajā klikšķina uz saites „[Accept](#)”, lai apstiprinātu aizsūtīto sertifikātu. Kad tas padarīts mazo logu var vērt ciet.

Tagad galvenajā logā var klikšķināt uz saites „[Next](#)”, lai pārietu pie nākošā soļa.

9. Ielādējas jaunas ugunssienas instalēšanas lapa.



**Installing new "Ugunssiena" host: install**

Devices:

slot	vendor	device	status
pci0:13:0:	Realtek Semiconductor	RT8139 (A/B/C/8130) Fast Ethernet Adapter	active
pci0:18:0:	Realtek Semiconductor	RT8139 (A/B/C/8130) Fast Ethernet Adapter	no carrier

Existing interfaces:

IP address	netmask	name	slot	action
127.0.0.1	255.0.0.0	Loopback	loopback0:	<a href="#">Edit interface</a>

Detected addresses:

IP address	netmask	gateway	status	action
10.10.10.123	255.255.255.128	10.10.10.19	3	<a href="#">Add interface</a>

[Edit routing configuration](#)

[Add administrator](#)

[Update configuration](#)

Šajā lapā, pirmajā tabulīnā (*Devices:*) ir redzamas visas tīkla kartes, kas ir ugunssienas mašīnā. Jāpievērš uzmanība slotam (*Slot*) un statusam, tas būs vajadzīgs nākošajā solī.

- 1) Pie „*Existing interfaces:*” klikšķina uz saites „*Edit interface*”, lai sāktu tīkla karšu konfigurēšanu. Ielādējas jauna lapa. Te var nomainīt tīkla kartes vārdu (*Name*), norāda kuru tīkla karti izmantot (*Interface*) un norāda tīkla kartes izmantojamās adreses (*Address, Netmask*). Beigās spiež pogu **[Save & Back]**.
- 2) Ja vajag pievienot vēl kādu tīkla interfeisu (tīkla karte fiziski jau atrodas ugunssienas mašīnā), tad ugunssienas instalēšanas lapā, tabulīnā „*Detected addresses:*” klikšķina uz saites „*Add interface*” un tāpat kā iepriekšējā apakšpunktā norāda vārdu, fizisko tīkla karti un adreses.
- 3) Tagad pievieno jaunu „rūti”, parasti sāk ar standarta rūti. Ugunssienas instalēšanas lapā klikšķina uz saites „*Edit routing configuration*”. Ielādējas jauna lapa. Pirmās rindas lodziņus atstāj tukšus. Otrās rindas pirmajā lodziņā („*Network address*”) izvēlas „*any*” un otrajā („*Gateway*”) ieraksta rūtera adresi. Spiež uz pogas **[Save & Back]**.
- 4) Nākošais solis ir pievienot sistēmas administratoru. Klikšķina uz saites „*Add administrator*”. Jaunajā lapā ailitēs ieraksta sistēmas lietotāja vārdu (*Username*), paroli (*Password*), vēlreiz ievada paroli lai to apstiprinātu (*Password (confirm)*), pilnu vārdu, organizāciju, e-pasta adresi, telefona numuru. Lauciņā „*Timeout*” norāda lietotāja sesijas noilguma laiku, pēc cik sekundēm lietotāja sesija tiks slēgta dīkstāves gadījumā. Vismaz vienam sistēmas lietotājam jābūt ar tiesību līmeni „*Supervisor*”, to norāda attiecīgajā rūtiņā ieliekot ķeksīti. „*Account locked*”, te var norādīt lietotāja konts ir bloķēts vai nav (gadījumā ja ir bloķēts lietotāja konts tad izņemot ķeksīti no rūtiņas, to var atbloķēt). Nākošajā lodziņā (*Lock after incorrect logins more than*) var norādīt pēc cik neveiksmīgiem autorizēšanās mēģinājumiem lietotāja konts tiks bloķēts. Un kā beidzamo var izvēlēties lietotāja tiesības uz darbību (*Rights*), te izvēlas starp „*view*” (tikai skatīt) un „*edit*” (skatīt un izmainīt). Visu beidzot spiež uz pogas **[Save & Back]**.
- 5) Tagad spiež uz saites „*Update configuration*”. Atvēršies mazs pārlūka logs, tajā klikšķina uz saites „*Start*”, lai sāktu datu atjaunināšanu. Kad atjaunināšana būs pabeigta, tad būs iespēja to apstiprināt spiežot uz saites „*Accept*”. Kad tas darīts jāspiež uz saites „*Close*”. Ja logā lapa ar „*Accept*” neparādās vai arī šo saiti nospiežot, sistēma parāda kļūdu, tad jaunā konfigurācija ir darboties nespējīga. Izmainiet to. Ja viss noritējis kā tam jābūt, klikšķina uz saites „*Next*”, lai sāktu datu rakstīšanu uz ugunssienas diska.

10. Ielādējas lapa, kas parāda kādi cietie diski ir mašīnai.

**Installing new "Ugunssiena" host: install**

Detected hard disks:  
 Number: 1  
 ide:1, master  
 size: 40982151168  
 sectors: 63, tracks: 16, cylinders: 79408  
 partition: 165; size: 25600000

Choose disk on which install  
 Enter number:

Izvēlas uz kura diska instalēt, un izvēlētā diska numuriņu ieraksta ailītē. Tad spiež pogu **[Format]**. Sāksies diska formatēšana, un pēc tam failu kopēšana no CD diska uz cieto disku. Par darba gaitu informē lapa, kas ik pēc desmit sekundēm atjaunojas.

Kopēšana pabeigta, tad kad ielādējas lapa, kas informē par padarītu darbu „Done”. Klikšķina uz saites „Next”, lai pārietu pie nākamā soļa.

11. Nepieciešams pārstartēt Ugunssienas konfigurācijas serveri. No šī brīža vairs nav vajadzīga CD-ROM iekārta, to var ņemt nost.

Lai izslēgtu sistēmu klikšķina uz saites „Shutdown”. Sistēma izslēgsies, pašu mašīnu var atvienot no strāvas. Lai pārstartētu klikšķina uz saites „Restart”, vienīgi der atcerēties, ka sistēma pārstartējoties atkal iestartēsies no CD-ROM diska, tādēļ to vajag izņemt.

12. Apsveicu, Konfigurācijas serveris ir uzinstalēts!

## 6. Pieslēgšanās konfigurācijas serverim

Tā kā visa ugunssienas vadība tiek organizēta attālināti (caur tīklu), tad ir nepieciešams pieslēgties konfigurācijas serverim. Interneta pārlūkprogrammas adresu logā ieraksta konfigurācijas servera adresi, ja adrese ir 128.128.128.1, tad pēc parauga:

<https://128.128.128.1/us>

Ja tīklā darbojas DNS serveris, tad cipariskās adreses vietā var izmantot vārdisko adresi. Ja vārdiskā adrese ir firewall.uznemums.lv, tad pārlūkprogrammas adresu logā raksta:

<https://firewall.domain.com/us>

Prefikss <https://> ir nepieciešams, lai interneta pārlūkprogrammai norādītu, ka datu apmaiņa notiks drošajā, jeb šifrētajā režīmā. Pēc adreses ievadīšanas, atvērsies lietotāja sesijas reģistrācijas ekrānforma:

Username

Password

Language

- *Username* – lietotāja vārds ar kādu tas reģistrēts sistēmā,
- *Password* – lietotāja parole pieejai sistēmai,

Ievadītos datus apstiprina spiežot pogu **[Login]**, vairumam pārlūkprogrammu pietiks, ja pēc datu ievadīšanas nospiedīs „Enter” taustiņu uz klaviatūras.

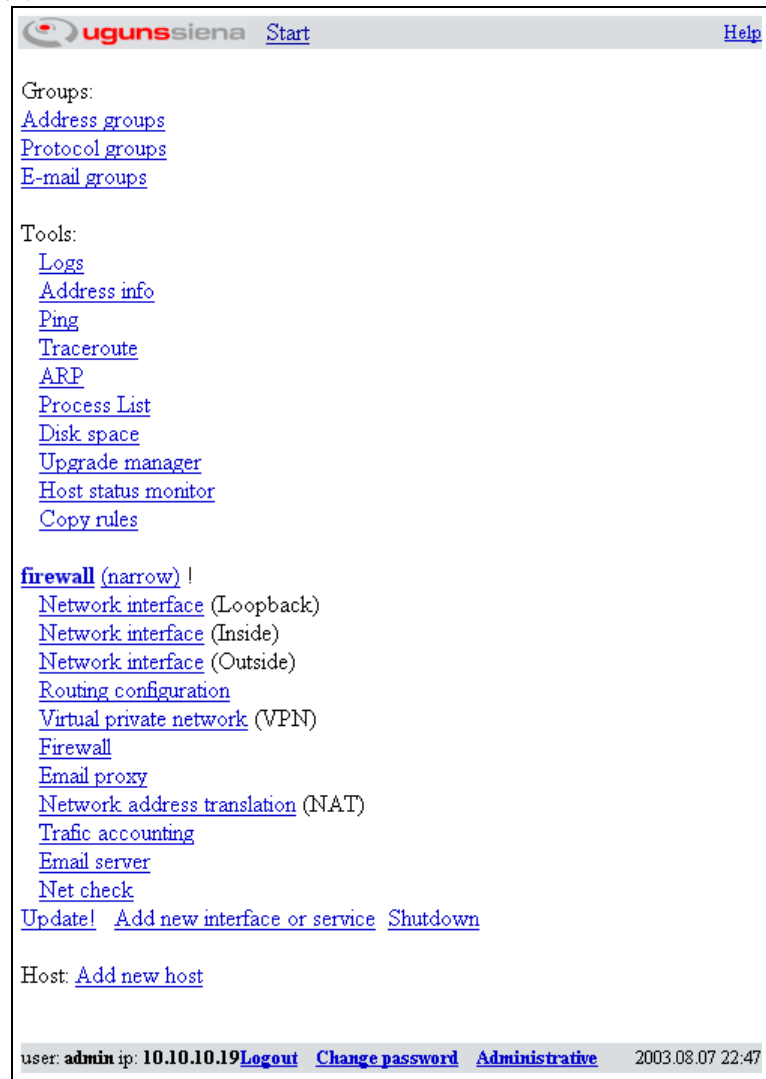
Sekmīgas pieslēgšanās gadījumā uz ekrāna tiks izvadīta sistēmas galvenā komandkarte (Start). Nesekmīgas lietotāja autorizācijas gadījumā, uz ekrāna parādīsies paziņojums „*Incorrect login!*” un zem tā, tāda pati kā iepriekš, lietotāja sesijas reģistrācijas ekrānforma.

Sistēmas audita uzskaites tabulās, tiek pierakstīti visi mēģinājumi pieslēgties (gan sekmīgie, gan nesekmīgie), precīzi fiksējot datumu, laiku, ievadītos parametrus un datora tīkla IP adresi. Audita žurnālu var apskatīt ugunssienas sadaļā „*Administrative*”. Vairākkārtīgu nesekmīgu pieslēgšanās mēģinājumu gadījumā (ja lietotāja vārds ir pareizs) lietotāja konts (*account*) tiek bloķēts (šāda iespēja jānorāda katram lietotājam atsevišķi). Atbloķēt kontu var tikai lietotāji ar „*Supervisor*” tiesību līmeni. Ja visiem sistēmā reģistrētajiem lietotājiem ar tiesību līmeni „*Supervisor*” (tādus var ieviest vairākus), tiek bloķēti konti, tai skaitā, konts tiek nobloķēts arī sākotnējam lietotājam „*admin*”, tādā gadījumā vienīgā iespēja atjaunot pieeju drošības sistēmas ugunssienas vadības sistēmai, ir kontaktēties ar uzņēmuma “UGUNSSIENA” tehnisko apkalpošanas dienestu.

Pēc šāda principa bloķējas lietotāju konti ja tas ir speciāli aktivizēts, neveiksmīgo mēģinājumu pieļaujamo skaitu, pirms bloķēšanās, var uzstādīt pēc vajadzības.

## 7. Sistēmas galvenā komandkarte (Start)

Pēc tam kad lietotājs veiksmīgi autorizējies ugunssienas konfigurācijas serverī, uz ekrāna tiek izvadīta komandkarte „Start”.



Šajā komandkartē ir viss, kas nepieciešams, lai varētu uzstādīt un administrēt ugunssieni. Ir pāris galvenās komandu kartes sastāvdaļas. Pirmā ir virsrakstu josla:



Tajā ir redzams pašreizējā atrašanās vieta sistēmā, kas noder arī ērtākai navigācijai pa sadaļām. Paraugā ir redzams, ka ir atvērta sadaļa adrešu grupas (*Address groups*) un tālākā sadaļa, grupa „Latvia”. Noklikšķinot uz kādu no saitēm (*Start*, *Address groups* vai *Latvia*), var nonākt attiecīgajā sadaļā.

Virsraksta joslas labajā malā vienmēr ir saite *Help*. Uz tās noklikšķinot var saņemt paskaidrojošu materiālu par konkrēto komandkarti. „*Help*” labākā īpašība ir, ka palīdzība vienmēr ir tur, kur tā ir vajadzīga.

Aiz virsraksta joslas seko sadaļa „*Groups*”. Grupas dod iespēju nodefinēt elementu kopas un dot tām vārdiskus apzīmējumus, kurus var izmantot tālākā ugunssienas konfigurēšanā.

Tālāk seko papildus instrumentus saturoša daļa – „*Tools*”. Rīki, kas ir šajā daļā nekādā veidā neietekmē ugunssienas darbību, bet palīdz darbā ar to.

Ugunssienas (*Host*) ir galvenā komandkartes „*Start*” sadaļa. Zem katras ugunssienas ir redzams, kas tai pievienots (servisi un komponentes). Piemēram, pie ugunssienas „*SIENA*”, ir trīs tīkla kartes (*Network interface*), uz tās darbojas virtuālā privātā tīkla serviss (*Virtual private network*), ugunsmūris (*Firewall*), un vēl vairāki citi servisi. Visus šos servisi un iekārtas var pilnībā konfigurēt un uzraudzīt no konfigurācijas servera.

Pašā apakšā ir josla, kas parāda ar kādu lietotāja vārdu ir reģistrēta sesija, un kāda ir lietotāja datora tīkla IP adrese. Tālāk ir saite „*Logout*” (beigt darbu), uz tās ir jāklikšķina lai beigtu darbu ar sistēmu. Vienmēr ir rekomendēts darbu ar sistēmu beigt tieši šādā veidā, jo tad tūlītēji tiek slēgta lietotāja sesija.

Tālāk seko saite „*Change password*”, šajā sadaļā lietotājs var nomainīt piekļuves paroli. Beidzamā saite ir „*Administrative*”, sīkāk par šo sadaļu skatīt rokasgrāmatas beigās, pie sadaļas ar tādu pašu nosaukumu.

## 8. Ugunssienas instalēšana no konfigurācijas servera

- Nepieciešamā komplektācija:
  - dators (jābūt iespējai iestartēties no CD)
  - minimālās prasības: CPU 486, HDD 1GB, RAM 32MB, CD-ROM (tikai instalēšanas laikā), PCI tīkla karte
  - rekomendētās prasības: CPU Intel Celeron/AMD Duron, HDD 20GB, RAM 128MB CD-ROM, PCI tīkla karte(s)
  - Ugunssienas instalācijas disks (CD)
  - strādājošs ugunssienas konfigurācijas serveris (jābūt pieejamam caur tīklu).
- Instalējamā mašīnā ievieto programmas instalācijas disku, un parūpējas lai mašīna no šī CD iestartētos.
- Ielogojas konfigurācijas serverī.
- Lai pievienotu jaunu ugunssieni konfigurācijā, lapas apakšējā daļā jāsameklē saite „Host: Add new host”, uz tās arī jāklikšķina.
- Jānorāda:
  - ugunssienas vārdu (*Name*) – obligāts,
  - privātās atslēgas garumu (*Private key length*). Šī ir konkrētās ugunssienas atslēga. Ar šīs atslēgas publisko daļu tiks šifrēti visi dati, kas nāk no konfigurācijas servera un ir domāti šai ugunssienai. Šī atslēga tiek parakstīta ar konfigurācijas servera root sertifikātu.
  - DNS servera adresi (*Name server*) – rekomendējam 127.0.0.1,
  - „Domain” – tīkla domains, var atstāt tukšu,
  - nepieciešamais ugunssienas darba režīms (*Mode*),
  - konfigurācijas servera adrese (*Management server IP*).
- Spiež pogu [**Save**]. Kad tas izdarīts, tad zemāk parādās jauna saite – pievienot tīkla adapteri (Add network interface), uz tās noklikšķina.
- Ieraksta tīkla kartes vārdu (tikai pašu zināšanai), IP adresi (*Address*) un netmasku (*Netmask*). Spiež uz pogas – [**Save & Back**].
- Pie „Primary IP” izvēlas IP adresi un spiež pogu [**Save**].
- Klikšķina uz saites „Install host”.
- Jaunajā lapā izvēlas pirmo punktu – instalēt ugunssienas sertifikātu (Install host certificate) uz tā noklikšķinot.
- Atveras jauns pārlūka (mazs) logs, kas piedāvā instalēt sertifikātu, spiež „Start” un ugunssienas daturs sāk privātās atslēgas ģenerēšanu (garums tika norādīts iepriekš). Tas var aizņemt vairākas minūtes laika, atkarībā no jaunās ugunssienas ātrdarbības un izvēlēta atslēgas garuma. Siena uzģenerēs atslēgu, to aizsūtīs parakstīt uz konfigurācijas serveri, un tad tam nosūtīs atslēgas publisko daļu. Kad tas izdarīts, atslēga jāapstiprina spiežot uz „Accept” (60 sekundžu laikā). Uzraksts „*Configuration accepted*” liecina, ka sertifikāts ir apstiprināts un tas darbojas. Mazo logu var vērt ciet.
- Līdzīgi izpildiet arī otro punktu „Upload server certificate”. Te siena tiek pie konfigurācijas servera publiskās atslēgas. Kad atslēga veiksmīgi saņemta, tad no tā brīža konfigurācijas serveris un siena ar datiem savā starpā apmainās tikai droši šifrētājā režīmā.
- Galvenajā logā jāspiež uz „Next”.
- Jaunajā lapā parādās informācija par tīkla adapteriem uz ugunssienas mašīnas. Jāpievērš uzmanība slotam (*Slot*) un statusam, tas būs vajadzīgs nākošajā solī. Pie „*Existing interfaces*” jāklikšķina uz saites (iepriekš iedotais tīkla kartes vārds).
- Jaunajā lapā ir redzama informācija par attiecīgo tīkla karti. Pie „*Interface*” norāda tīkla kartes slotu (tas bija redzams iepriekšējā lapā) un spiež pogu [**Save & Back**].
- Tagad lapas apakšā spiež uz saites „Edit routing configuration”. Jaunajā lapā pievieno jaunu rūti (*route*). Pirmās rindas lodziņos neraksta neko. Otrās rindas pirmajā lodziņā (*Network address*) izvēlas „any” un otrajā (*Gateway*) ieraksta maršrutētāja(*router*) adresi. Spiež uz pogas [**Save & Back**].
- Tagad spiež uz saites „Update configuration”. Atvērsies mazs pārlūka logs, tajā klikšķina uz saites „Start”, lai sāktu datu atjaunināšanu. Kad atjaunināšana būs pabeigta, tad būs iespēja to apstiprināt spiežot uz saites „Accept”. Kad tas darīts jāspiež uz saites „Close”. Ja logs ar „Accept” neparādās vai arī šo saiti nospiežot, sistēma parāda kļūdu, tad jaunā konfigurācija ir darboties nespējīga. Izmainiet to.
- Vecajā logā var klikšķināt uz saites „Next” lai pārietu pie nākamā soļa.
- Jaunajā lapā parādās informācija pa ugunssienas cietajiem diskiem (*HDD*), kā arī šeit jāizvēlas uz kura diska instalēt sistēmu, to norāda ierakstot attiecīgā diska numuru ailītē. Spiež uz pogas blakus [**Format**].
- Sākas diska sagatavošana instalēšanai un failu kopēšana (lapa ik pa 10 sekundēm atjaunojas dodot iespējams sekot līdz instalēšanas gaitai). Uzraksts „*Done*” liecina, ka instalēšana pabeigta.
- Jāspiež uz saites „Next”, jaunā lapa informē, ka instalēšana ir pabeigta. Jāizslēdz ugunssienas daturs klikšķinot uz saites „Shutdown” (fiziski neizslēgsies). Tagad var ņemt ārā instalācijas disku (CD). No šī brīža, vairs nebūs vajadzīga pati CD-ROM iekārta, tā kā arī to var ņemt nost, iepriekš izslēdzot ugunssienas datoru un atvienojot no strāvas.

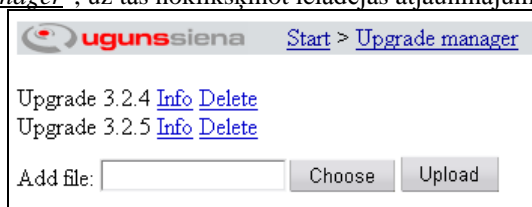
22. Ugunssienas datoram BIOSā norāda lai tas sistēmu ielādē no instalēšanas procesā norādītā diska. Iestartē ugunssieni.
23. Apsveicu, instalēšana ir pabeigta.

## 9. Ugunssienas programmas atjaunināšana (Upgrade)

Ugunssieni sākot no versijas 3.1.0 iespējams atjaunināt uz jaunāku izmantojot atjauninājumu failus. Par katras ugunssienas versiju var pārliecināties konfigurācijas servera lapā „Start” noklikšķinot uz ugunssienas vārda. Apakšdaļā zem galvenajām navigācijas pogām ir redzama ugunssienas versija. Šajā pat vietā parādīsies pieejamie ugunssienas atjauninājumi. Atjauninājumu failus iespējams lejupielādēt no Ugunssienas interneta mājas lapas (<http://www.ugunssiena.lv/>), vai tie var tikt saņemti pa e-pastu pēc pieprasījuma saņemšanas.

### 9.1. Atjauninājumu failu augšupielādēšana

Lai uzsāktu ugunssienas atjaunināšanu, nepieciešams uz konfigurācijas servera augšupielādēt atjauninājuma failu. Šim nolūka ugunssienas konfigurācijas servera galvenajā komandkartē „Start” pie „Tools” ir saite „[Upgrade manager](#)”, uz tās noklikšķinot ielādējas atjauninājumu augšupielādēšanas forma.

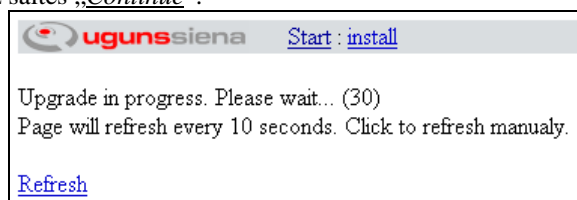


Šajā lapā redzami visi jau augšupielādētie atjauninājumi, iespējams apskatīt to aprakstus („[Info](#)”) vai izdzēst neaktuālus atjauninājumus („[Delete](#)”).

Izvēlas atjauninājumu failu un spiež pogu [**Upload**]. Augšupielādēšanas laiks var ietilgt uz vairākām minūtēm, šis laiks ir tieši atkarīgs no atjauninājumu faila izmēra.

### 9.2. Atjauninājumu instalēšana

Kad atjauninājumi veiksmīgi augšupielādēti pie katra konfigurācijas servera hosta (ugunssienas), ir redzami šim hostam aktuālie atjauninājumi. Lai uzstādītu atjauninājumu uz ugunssienas, klikšķina uz tā versijas, piemēram, „Version 3.2.5”. Ielādējas lapa, kas parāda atjauninājuma faila aprakstu. Obligāti jāizlasa šis apraksts, jo tajā ir informācija kādi soļi ir noteikti jāizpilda pēc instalācijas pabeigšanas. Ja aprakstā minētie noteikumi atbilst konkrētajai ugunssienai, apakšā klikšķina uz saites „[Start upgrade!](#)” lai pārietu pie atjauninājuma uzstādīšanas. Nākamā lapā redzama statusa informācija par atjauninājumu, vai izdevies to palaist, ja nē tad parādās kļūdas paziņojums. Ja paziņojuma teksts ziņo, ka atjauninājums palaists, tad turpina atjaunināšanu klikšķinot uz saites „[Continue](#)”.



Lapa ik pa 10 sekundēm pārlādēsies, līdz atjauninājuma instalācija būs pabeigta, par to liecina paziņojuma teksts „[Upgrade successful](#)”. Šajā brīdī ir vērts atcerēties, kas bija teikts atjauninājuma aprakstā, ja obligāta prasība bija pārstārtēt ugunssieni, tad to ir vēlams izdarīt nekavējoties, galvenajā konfigurācijas servera lapā „Start” izpildot konkrētās ugunssienas „[Shutdown](#)” operāciju.

## 10. Konfigurēšana

Lai pilnvērtīgi varētu nokonfigurēt ugunssienu, būtu nepieciešamas labas zināšanas par datortīklu uzbūves principiem, tīklu protokoliem, datu pakešu apstrādes principiem un Interneta servisiem, kas nodrošina DNS adresāciju, e-pasta servisu un citus. Tas gan nenozīmē, ka to visu labi nepārzinot nav iespējams pieņemtami nokonfigurēt ugunssienu.

### 10.1. Grupas

Pie grupām var nodefinēt elementu kopas un tām dot vārdiskus apzīmējumus, kas tālāk būs izmantojami ugunssienas konfigurēšanā. Piemēram, ir ļoti ērti, ja var izveidot adresu grupu kur ir tikai Latvijas interneta adreses, un tālāk šo grupu var izmantot lai ierobežotu vai atļautu kādu darbību Latvijas interneta tīklā. Tāpat nokonfigurējot iekšējā tīkla adresu grupu, visai grupai var piešķirt lielākas privilēģijas kontaktējoties savā starpā.

### 10.2. Adrešu grupas (Address groups)

Pie adrešu grupām nodēfinē IP adreses un to kopas. Pēc noklusēšanas jau ir vairākas adrešu grupas. Automātiskās adrešu grupas neparādās šajā adrešu grupu sarakstā.

Uzklīkšķinot uz attiecīgo grupas nosaukumu, ir iespējams veikt tajā izmaiņas, nomainīt grupas nosaukumu, pievienot vai noņemt adresi, vai adrešu apgabalu. Kā arī ir iespēja izdzēst nevajadzīgu adrešu grupu. Apakšējā ailītē ir saite „[Add new group](#)”, noklikšķinot uz tās, var izveidot jaunu adrešu grupu.

The screenshot shows the 'Remote' address group configuration page. At the top, the breadcrumb trail is 'Start > Address groups > Remote'. The 'Address group name' field contains 'Remote'. Below is a table with columns 'Address list' and 'Comments'. The table contains four rows of IP addresses and their corresponding comments: '192.168.0.0:255.255.255.0' (NYC office), '10.10.12.144:255.255.255.240' (London office), '-10.10.12.148:255.255.255.255' (London office exception), and '159.148.75.28' (Boss). Below the table are 'Save', 'Save & Back', and 'Cancel' buttons. Further down, there is a 'Link, which contains addresses' field and an 'Import addresses' button. At the bottom, there are 'Delete' and 'Show' buttons with labels 'Click here to remove address group:' and 'Click here to show data in textarea:' respectively.

Address list	Comments
192.168.0.0:255.255.255.0	NYC office
10.10.12.144:255.255.255.240	London office
-10.10.12.148:255.255.255.255	London office exception
159.148.75.28	Boss

*Address group name* – adrešu grupas nosaukums. Nākamajā ailītē (*Address list ip or ip:subnet*) ieraksta attiecīgi IP adresi, vai arī IP adresi ar attiecīgo apakštīkla adresi (*subnet mask*) (tādā veidā definē apakštīkla adrešu grupu). Katrs ieraksts var sākties ar „+” vai „-” zīmi. „+” nozīmē, ka adrese ietilpst grupā, savukārt „-” ka neietilpst. Plusus var nelikt.

Ir iespēja pievienot adreses no saites, ailīte „*Link, which contains addresses*”, te var ierakstīt web adresi un ielādēt no tās datus nospiežot pogu **[Import addresses]**.

Nospiežot pogu **[Show]**, iespējams apskatīt un/vai labot adrešu grupu tekstuālā veidā.

Runājot par adrešu grupām. Eksistē vēl tādas automātiskās adrešu grupas. Tās ir grupas, kuras ir iespējams izveidot pie katras „sienas” tīkla kartes (*network interface*). Lietotājs pats var izvēlēties vai vajag un ja vajag tad kāda tipa grupas veidot. Grupas tiek veidotas pēc parauga, ja sienai ar doto nosaukumu „Firewall” tiek pieviesta tīkla karte „Test” ar adresi 128.128.128.128:255.255.255.0, tad ir iespēja izveidot trīs dažādas automātiskās adrešu grupas:

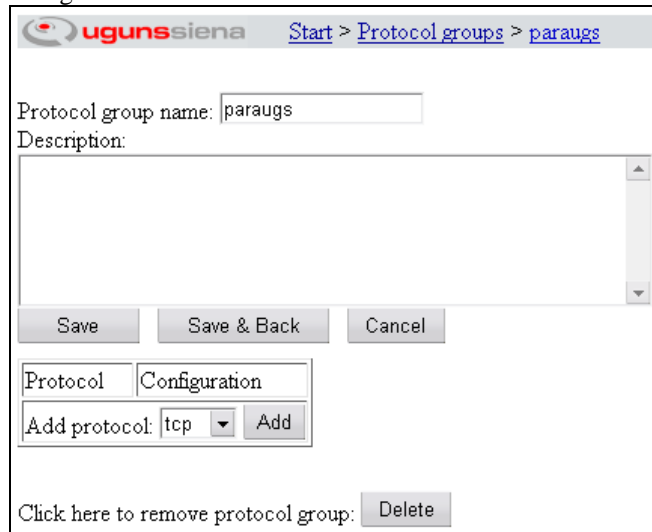
- ~Firewall/Test/broadcast, ar adresi 128.128.128.255:255.255.255.0
- ~Firewall/Test/host, ar adresi 128.128.128.128:255.255.255.255
- ~Firewall/Test/subnet, ar adresi 128.128.128.0:255.255.255.0

Šīs grupas nav redzamas pie pārējām adrešu grupām, bet tās ir redzamas un izmantojamas konfigurējot ugunssienu (ugunsmūris, VPN, trafika uzskaitē, u.t.t).

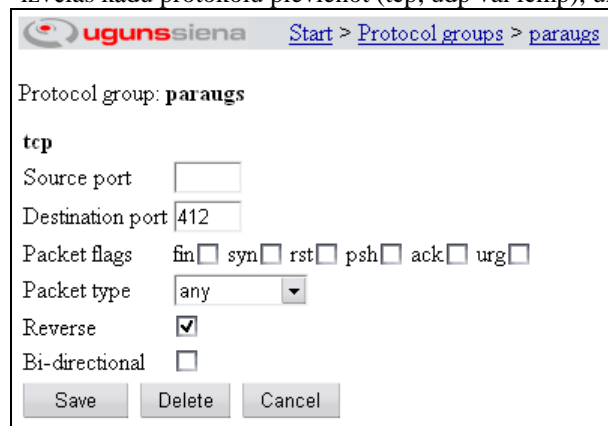
### 10.3. Tīkla protokolu grupas (Protocol groups)

Protokolu grupas (*Protocol groups*), šeit var nedefinēt interneta protokolus un attiecīgos portus. Pēc noklusēšanas ugunsšienas nainstalējot jau ir nedefinēti standarta protokoli (*ftp, http, https, smtp u.t.t.*).

Pievienot jaunu protokolu grupu, var klikšķinot uz saites „*Add new group*” tabulas apakšā. Jaunā lapā būs ailīte kur ierakstīt protokola grupas vārdu un ja nepieciešams arī aprakstu. Kad tas darīts, jāspiež uz pogas [Save]. Lapa atjaunojas un tagad izskatās tā:



Pie „*Add protocol:*” izvēlas kādu protokolu pievienot (*tcp, udp vai icmp*), un spiež uz pogas [Add]



Jaunajā lapā ievada datus:

- „*Source port*” – sūtītāja ports (parasti atstāj tukšu).
- „*Destination port*” saņēmēja ports (servisa ports).
- „*Packet flags*” – paketes karodziņi (nav ieteicams izmantot ja nav skaidrības par šiem karodziņiem).
- „*Packet type*” – pakešu tips, jebkāds (*any*), savienojumu atverošā pakete (*setup*) un nodibināta savienojuma pakete (*established*).
- „*Reverse*” – nodrošina apgrieztu savienojumu iespēju. Piemērs ir ftp protokols, kad veicot savienojumu ftp klients dod pieprasījumu uz servera 21 portu, serveris atbild, bet brīdī kad tiek pieprasīts no servera nolādēt failu, tad ftp serveris griežas pie klienta un jautā pēc kāda porta uz kuru sūtīt faila saturu. Tas arī ir apgrieztais savienojums. No sākuma klients serverim, pēc tam serveris klientam.
- „*Bi-directional*” – abos virzienos. Respektīvi, no „*Source port*” uz „*Destination port*” un otrādi. Iesakāms lietot UDP servisiem.

Kad vajadzīgās vērtības iestādītas, spiež uz pogas [Save]. Parādās iepriekšējā lapa, kurā ir pievienots viens protokols. Ja ir vajadzīgs, tad pievieno vēl citus protokolus, ja nē, tad spiež uz pogas [Save & Back].

### 10.4. E-pasta adrešu grupas (E-mail groups)

E-pasta grupas (*E-mail groups*). Tieši tāpat kā pie iepriekšējām grupām, arī šeit var definēt grupas. E-pasta grupas izmanto e-pasta kontroles sistēmā.

## 10.5. Ugunsiena (Host)

Noklikšķinot uz attiecīgās ugunsienas vārda var izmainīt tās parametrus:

- Pirmais lauks ir ugunsienas vārds, vēlams izvēlēties tādu kas kaut ko izsaka par konkrēto mašīnu (atrasšanās vietas nosaukums vai kā tamlīdzīgi).
- *Private key length* – norāda ugunsienas privātās atslēgas garumu.
- Laukā „vārdu serveris” (*Name server*), ja tas ir nepieciešams, ieraksta attiecīgā tīkla domēna vārda servera adresi (DNS).
- Nākošajā laukā ieraksta tīkla domēnu (*Domain*), kādā atrodas ugunsiena.
- Pie „*Mode*” izvēlas ugunsienas darba režīmu, starp maršrutētāju (*router*) jeb tiltu (*bridge*), parasti izmanto maršrutētāja konfigurāciju. Maršrutētāja konfigurācijā katrai ugunsienas tīkla kartei jābūt citā tīklā (piemēram, viena uz lokālo tīklu, otra uz internetu). Tiltas konfigurācijā visām tīkla kartēm ir vienādas adreses.
- „*NTP server*” norāda NTP servera adresi ar kuru sinhronizēt ugunsienas pulksteni. Ja tas nav nepieciešams ailiiti atstāj tukšu.
- „*Throughput limit*” datu caurplūdes limits, megabiti sekundē. Noderīga opcija ja ugunsienas slodze neatbilst aparatūras spējām. Vairumā gadījumu šī opcija jāatstāj tukša.
- „*SNMP comunity*” - SNMP tīkla diagnostikas protokola "parole".
- Ailītē „*CD-key*” jābūt ierakstītam instalācijas diska numuram (tas pats, kas bija vajadzīgs lai uzinstalētu ugunsieni).
- Ailē „*Management server ip*”, izvēlas kādu no piedāvātajām konfigurācijas serveru adresēm (ir iespējamās vairākas adreses, ja ir pieinstalēti vairāki konfigurācijas serveri).
- „*Primary IP*” ailē ir iespēja izvēlēties, kura no ugunsienas adresēm tiks izmantota kā galvenā (adreses ir vairākas, ja ugunsienai ir vairākas nokonfigurētas tīkla kartes).
- Beidzamā ailītē „*Description*”, gadījumā ja tas nepieciešams, te ieraksta aprakstu par konkrēto ugunsieni.

The screenshot shows the Mikrotik WinBox configuration window for a firewall host. The window title is "ugunsiena Start: firewall". The "Host" section contains the following fields:

- Name: firewall
- Private key length: 4096
- Name server: 127.0.0.1
- Domain: us.lv
- Mode: router
- NTP server: 10.10.10.111
- Throughput limit: 100 Mb/s
- CD-key: (empty)
- Management server ip: 127.0.0.1 (Loopback)
- Primary ip: 127.0.0.1 (Loopback)
- Description: (empty)

At the bottom, there are buttons for "Save", "Save & Back", and "Cancel". The software version is 3.1.1. There are also links for "Reinstall certificate" and "Custom configuration".

Zemāk seko pogu rinda, kuras piespiežot var saglabāt izmaiņas, saglabāt un atgriezties iepriekšējā lapā, izdzēst ugunsieni no konfigurācijas servera vai atcelt veiktās izmaiņas. Izdzēšanas opcija nav pieejama ja ugunsiena, kas tiek apskatīta pati ir konfigurācijas serveris.

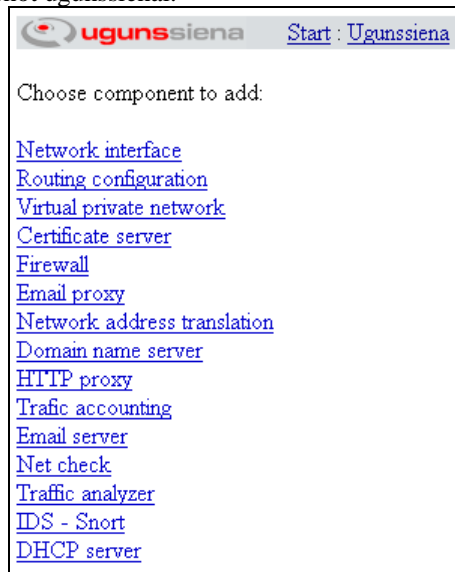
Tālāk ir saite „*Reinstall certificate*”, šī opcija būs jāizmanto, ja ir mainījies konfigurācijas servera *ROOT* sertifikāts, lai attālinātajai ugunsienai nomainītu sertifikātus.

Beidzamā saite, kas attiecas uz ugunsieni ir „*Custom configuration*”, šī ir opcija ko var izmanto pieredzējuši ugunsienas administratori, kas zina ko dara, lai izveidotu īpašu konfigurāciju testu nolūkiem. Ja nav pārliecības par to ko rakstīt šajā konfigurācijā, tad noteikti labāk tur neko nerakstīt.



## 10.6. Ugunssienas komponentu lapa

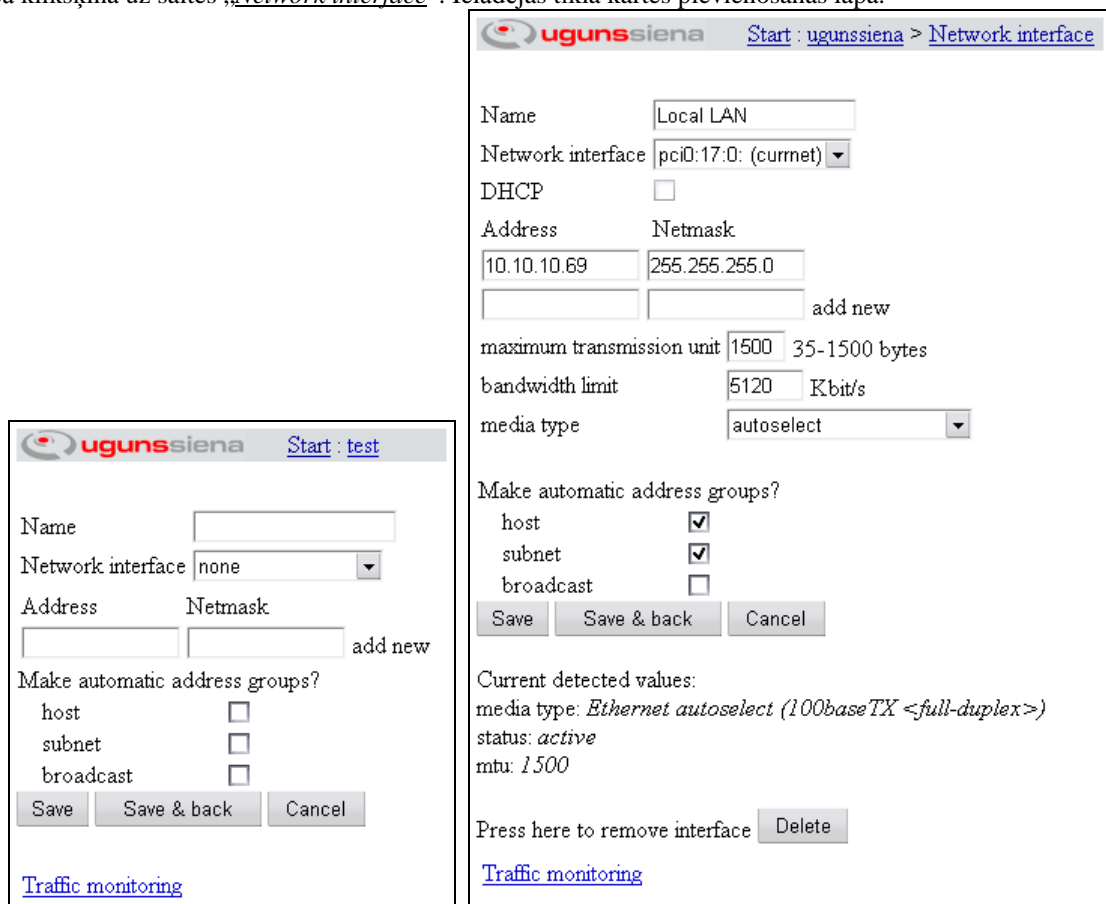
Lai ugunssienai pievienotu jaunu iekārtu vai servisu, tad galvenajā komandu kartē zem ugunssienas (*Host*), klikšķina uz saites „*Add new interface or service*”. Ielādēties ugunssienas komponentu lapa ar iekārtu un servisu sarakstu, ko var pievienot ugunssienai.



Lai pieinstalētu servisu vai komponentu, klikšķina uz attiecīgās saites.

## 10.7. Tīkla interfeiss (Network interface)

Galvenajā „Start” lapā pie katras ugunssienas (*Host*), ir jau pievienotās tīkla kartes (*Network interface*) ar iekāvās norādītu iepriekš izvēlēto tīkla kartes vārdu, uz to noklikšķinot var tikt klāt pie tīkla kartes uzstādījumiem (nosaukums, adreses, u.t.t.). Ja vajag pielikt vēl kādu tīkla karti, tad ugunssienas komponentu lapā klikšķina uz saites „*Network interface*”. Ielādējas tīkla kartes pievienošanas lapa.



### 10.7.1 Tīkla interfeisa pamat konfigurācijas parametri

Pēc labpatikas izvēlas tīkla kartes vārdu (*Name*), bet vēlams tādu kas kaut ko izsaka par tīklu pie kura tā pieslēgta, piemēram, „*Local LAN*” lokālajai tīkla kartei. Pie „*Interface*” izvēlas uz kuras fiziskās tīkla kartes attiecas konkrētā konfigurācija.

*Network Interface*: Norāda tīkla interfeisu uz kuru attiecas konfigurācija. Tas var būt gan reāls fiziskais interfeiss, gan *Loopback* interfeiss, gan virtuālais interfeiss (*VLAN*), gan virtuālais rezervēšanas interfeiss (*VRRP*).

*DHCP*: atzīmējot norāda vai uz interfeisa darbosies DHCP klients. Ja ir atzīmēta šī izvēle, tad adrese šim interfeisam tiks pieprasīta no attiecīgā tīkla DHCP servera. Un tādā gadījumā zemāk norādītās IP adreses tiks izmantotas tikai automātisko adrešu grupu ģenerēšanai.

Ievada IP adresi (*Address*) un tīkla masku (*Netmask*). Ja uz karti nepieciešams pievienot vairākas adreses, tad pēc [**Save**] nospiešanas būs pieejama vēl viena tukša ailīte kur to ierakstīt.

Zemāk ir ailīte „*maximum transmission unit*”, maksimālais pieļaujamo interneta paketes izmērs uz šī interfeisa. Gadās kad lielas paketes (ar maksimālo pieļaujamo izmēru) ir pie vainas tīkla nekorektai funkcionēšanai, tad ierobežojot paketes maksimālo izmēru ir iespējams atrisināt šāda tipa problēmas.

„*bandwidth limit*” ja nepieciešams norāda maksimālo pieļaujamo datu plūsmas ātrumu caur šo interfeisu.

Ailītē „*media type*” var norādīt interfeisa ātruma parametrus. Šis parametrs jāmaina tikai tad, ja ar „*autoselect*” opciju tīkla karte nedarbojas korekti.

Automātiskās adrešu grupas (par to būtību tika aprakstīts pie adrešu grupām). Šādas automātiskās adrešu grupas ir ārkārtīgi ērti lietojamas konfigurējot uguns mūri un VPN tuneļus, kā arī ērti izmantojamas trafika uzskaites sistēmā. Lietotājs pats izvēlas kādu grupu veidot. Grupu kas satur tikai uguns sienas konkrētā interfeisa adreses (*host*), grupu kas satur visu apakštīklu (*subnet*) vai grupu kas satur apraides adreses (*broadcast*). Grupu izveido ieliekot ķeksīti attiecīgajā ailītē, izdzēs – izņemot. Nav iespējams izdzēst grupu, kas tiek lietota kādā no uguns sienas servisiem (*firewall*, *VPN*). Mēģinot izdzēst (izņemt ķeksīti) grupu, kas tiek lietota, par to parādīsies informējošs paziņojums ar norādēm uz filtriem kur adrese tiek lietota.

„*Traffic monitoring*” nodrošina iespēju apskatīt tīkla noslodzes statistiku grafiskā veidā.

### 10.7.2 Virtuālie interfeisi (Vlan)

Iespējams pievienot ne tikai reālus interfeisus, bet arī tā saucamos virtuālos interfeisus (*Vlan*). Nepieciešama lieta ja vajag veidot virtuālos tīklus. Lai pievienotu virtuālo interfeisu, ailītē „*Network interface*” norāda „*VLAN*”. Pēc [**Save**] pogas nospiešanas, parādīsies divas jaunas ailītes, „*Parent interface*” – reālais interfeiss, te jānorāda uz kura fiziskā (reālā) tīkla interfeisa attiecas šis virtuālais interfeiss un „*Vlan ID*” – virtuālā interfeisa numurs (0-255). Šāds virtuālais interfeiss tālākā uguns sienas konfigurācijā neatšķiras no parasta interfeisa.

### 10.7.3 Virtuālais rezervēšanas interfeiss (VRRP)

Uguns sienas atbalsta virtuālā rezervēšanas protokola darbību – *VRRP (Virtual Router Redundancy Protocol)*. Šis protokols piedāvā iespēju uz diviem vai vairāk hostiem uzkonfigurēt vienādas tīkla IP adreses tā, ka rezerves hosts („*backup*”) pārņem darbu, ja no ierindas izgājis primārais hosts.

Ailītē „*Network interface*” norāda „*VRRP*”, pēc [**Save**] pogas nospiešanas parādās jaunas konfigurācijas ailītes.

„*Parent interface*” – norāda uz kura fiziskā tīkla interfeisa darbosies šis protokols.

„*VRRP ID*” – vienā tīklā var darboties vairāki nesaistīt *VRRP* protokoli. Norāda vienu ID visiem viena *VRRP* protokola hostiem.

„*Priority*” – vienam hostam ir jābūt galvenajam, tam šajā laukā izvēlas „*master*”, pārējiem izvēlas „*backup*”.

„*VRRP password*” – drošības labad, lai izvairītos no ļaunprātīgām darbībām balstoties uz šo protokolu, tā komunikācijas starp „*master*” un „*backup*” hostiem var tikt aizsargātas ar paroli. To ieraksta šajā ailītē.

Šo protokolu var izmantot ne tikai lai nodrošinātu rezerves serveru darbību, bet arī lai nodrošinātu jaudas sadali („*load balancing*”) starp diviem hostiem. Šādā gadījumā katram hostam ir jābūt galvenajam („*master*”) uz kādu IP apgabalu un uz pārējo IP apgabalu tam jābūt kā „*backup*” hostam. Attiecīgi lietotāju tīkla interfeisu konfigurācijās norāda dažādas „*gateway*” adreses.

## 10.8. **Maršrutētājs (Router)**

Lai pievienotu maršrutētāja (*router*) servisu, uguns sienas komponentu lapā klikšķina uz saites „[Routing configuration](#)”.

Pirmajā ailītē norāda tīkla adresi, otrajā netmasku un trešajā vārteju (*Gateway*). Tikpat labi var izmantot iepriekš definēto adresu grupu, to izvēlas apakšējā ailītē, un attiecīgi pretī ieraksta vārtejas adresi. Kad tas darīts spiež pogu [**Save & Back**], vai arī [**Save**] ja ir doma pievienot vēl kādu maršrutu (*route*). Pievienotais maršruts parādās galvenajā komandu kartē zem ugunssienas kā jauna saite, attiecīgi uz to noklikšķinot var veikt izmaiņas maršrutētāja uzstādījumos.

## 10.9. Sertifikātu serveris (CA)

Sertifikātu serveris paredzēts digitālo sertifikātu izdošanai. Šie sertifikāti derīgi e-pasta aizsardzībai, autorizēšanās nolūkiem, datu šifrēšanai. Serveris piedāvā iespēju ģenerēt jaunus sertifikātus un tos parakstīt. Sertifikātu serveri iespējams pieinstalēt tikai pie konfigurācijas servera.

Sertifikātu servera servisu pievies gluži tāpat kā visus citus ugunssienas servissus, no ugunssienas komponentu lapas, tajā klikšķinot uz saites „*Certificate server*”.

	subject	serial	status
1	O=Uzņēmums/CN=Administrator	0	signed & active
2	O=SIĀ Ugunssiena/Email=ca@ugunssiena.lv	0	signed & active

Te redzami ugunssienai pieinstalētie sertifikāti. Visi sertifikāti sadalīti vairākās kategorijās pēc to mērķa. Uzsākot darbu tiek parādīti saucamie ROOT sertifikāti („*Certificate authority*”). Tie ir sertifikāti, kas izmantoti lai parakstītu citus sertifikātus. Ailītē „*Show*” norādot citas kategorijas nosaukumu iespējams apskatīt tās kategorijas sertifikātus. Pieejamās kategorijas ir:

- „*Certificate authority*” – sertifikāti, kas izmantojami citu sertifikātu parakstīšanai.
- „*Server*” – sertifikāti, kas paredzēti dažādu serveru lietošanai (https, ftps, u.t.l.).
- „*Person*” – sertifikāti, kas izsniegti personām, e-pasta šifrēšanai, dokumentu parakstīšanai, autorizācijai.
- „*Virtual private network*” – sertifikāti, kas paredzēti VPN savienojumu autorizācijai.
- „*Host*” – pie konfigurācijas servera pieslēgto ugunssienas sertifikāti.

Tabuliņā redzami dati no sertifikāta apraksta („*subject*”) daļas, seriālais numurs un sertifikāta statuss. Noklikšķinot uz ciparu pirmajā ailītē iespējams iegūt papildus informāciju par sertifikātu.

### 10.9.1 Informācija par sertifikātu

The screenshot shows a web browser window with the address bar displaying 'Start : ugunssiiena > Certificate server'. The main content area is titled 'Certificate information' and contains a table with the following data:

Purpose	Certificate authority
Status	signed & active
Serial	0
Subject	L=Ugunssiiena O=Uzņēmums OU=Uzņēmums CN=Administrator emailAddress=admin@firewall.lv
Issuer	L=Ugunssiiena O=Uzņēmums OU=Uzņēmums CN=Administrator emailAddress=admin@firewall.lv
Valid from	2004-03-25 15:27
Valid to	2009-02-07 15:27

Below the table, there is a 'Refresh' button. Under the heading 'Export certificate (public key)', there is an 'Export' button. A text block states: 'This certificate is exportable in PKCS12 format with private key. Use password to protect exported private key'. Below this is a text input field for 'password (optional)' and an 'Export' button. Further down, there is a 'Revoke' button under the heading 'You can revoke this certificate', and a 'Remove' button under the heading 'You can remove private key from server'.

Šajā logā redzama detalizēta informācija par sertifikātu. Ir vairākas darbības, kas iespējamas ar sertifikātu. Saglabāt sertifikāta publisko atslēgu („*Export certificate (public key)*”). Ja uz servera stāv sertifikāta privātā atslēga, to iespējams eksportēt, saglabāt kā failu. Lai aizsargātu privāto atslēgu, vēlams ievadīt paroli pirms eksportēšanas. Tāpat iespējams izdzēst privāto atslēgu no servera, to izdara spiežot pogu lapas apakšā [**Remove**]. Iepriekš gan būtu vēlams citur to noglabāt. Sertifikātu iespējams anulēt, atsaukt. To iespējams izdarīt spiežot pogu [**Revoke**].

### 10.9.2 Sertifikātu servera konfigurēšana

Uzstādīt sertifikātu servera parametrus iespējams klikšķinot uz saites „*Certificate server configuration*”. Pirmajā ailītē norāda kuru sertifikātu izmantot automatiskajai lietotāju sertifikātu parakstīšanai („*Default certificate for user request signing*”). Nākamajā ailē ar ķeksīti atzīmē vai atļaut automatisku lietotāju sertifikātu parakstīšanu („*Automatically sign user requests*”). Trešajā ailītē norāda automatiski parakstīto sertifikātu, noklusēto derīguma laiku dienās („*Default certificate valid time*”). Nākamajā laukā („*Show other certificates on user page*”) ar ķeksīšiem atzīmē kāda tipa sertifikātus rādīt autorizētajiem lietotājiem. Autorizētie lietotāji ir tie, kuriem izveidots lietotāja konts uz ugunssienas ar tiesību līmeni „*User*”. Šiem lietotājiem tipiski nepieciešami dažādi „*root*” sertifikāti („*Certificate authority*”), personu sertifikāti („*Person*”) un VPN tuneļu autorizācijas sertifikāti („*Virtual private network*”).

Sekojošajā laukā („*Show information from subject*”) atzīmē ko no sertifikāta apraksta („*Subject*”) datiem rādīt pie sertifikātu sarakstiem. Viss beidzot norāda par sertifikātu izdošanu atbildīgās personas e-pasta adresi. Uz šo adresi tiks sūtīti paziņojumi par pieprasījumiem parakstīt sertifikātus.

### 10.9.3 Jauna sertifikāta pievienošana

Jaunu sertifikātu sistēmai var pievienot klikšķinot uz saites „*Import certificate*”. Atveras forma sertifikāta augšupielādēšanai. Jānorāda sertifikāta veids, to izvēlas no piedāvātajiem ailītē „*Purpose*”. Sertifikātu norāda vai nu kā lokālu failu ailītē „*upload file*”, vai to iekopē, kā tekstu BASE64 kodējumā, ailītē

„paste as text field”. Ja sertifikāts bijis aizsargāts ar paroli, tad to ievada ailītē „password”. Sertifikātu iespējams augšupielādēt ja tas ir PKCS #7, PKCS #12 vai X.509 formātā.

#### 10.9.4 Sertifikāta pieprasījuma augšupielādēšana

Pieprasījumu parakstīt sertifikātu, iespējams augšupielādēt klikšķinot uz saites „[Upload certificate request](#)”. Ielādējas forma. Norāda sertifikāta veidu („Purpose”). Pieprasījumu norāda vai nu kā lokālu failu, vai iekopē ailītē „paste as text field” kā tekstu. Ja pieprasījums bijis aizsargāts ar paroli, tad paroli ievada ailītē „password”. Ja sertifikātu servera konfigurācijā aktivizēta automātiska sertifikātu parakstīšana, tad uzreiz pēc pieprasījuma augšupielādēšanas procedūras pabeigšanas, pieprasījums tiks parakstīts, ja vien tas ir iespējams.

#### 10.9.5 Ģenerēt sertifikāta pieprasījumu un privāto atslēgu

Sertifikātu serveris nodrošina iespēju uzģenerēt privāto atslēgu un nosūtīt pieprasījumu parakstīt sertifikātu. Šī opcija pieejama klikšķinot uz saites „[Generate new certificate request with private key](#)”.

Izvēlas atslēgas garumu („Private key length”), garāka atslēga nozīmē lielāku drošību, bet arī 1024 bitu gara atslēga ir pietiekami gara lai to ar mūsdienu tehnoloģijām nebūtu iespējams atlauzt. Izvēlas vienu no sertifikātu veidiem, kam atbildīs šis sertifikāts („Purpose”). Aizpilda sertifikāta informācijas laukus („Certificate information”). Vārds kam sertifikāts būs paredzēts („Name or host”), šis ir obligāti aizpildāmais lauks. E-pasta adrese, arī šī ir obligāti nepieciešamā informācija. Laukā „Organization” ieraksta uzņēmuma nosaukumu, ja tāds ir. „Organization unit” – uzņēmuma apakšvienības nosaukumu, ja ir. „Country” – divus simbolus garo valsts kodu (LV, UK, US, ...) šis ir obligāti aizpildāmais lauks. Lauki „Locality” un „State or province” ir neobligāti. Kad vajadzīgie lauki aizpildīti spiež pogu **[Generate]**. Sākas sertifikāta privātās atslēgas ģenerēšana. Kad tā uzģenerēta ielādējas nākamā ekrānforma. Sākumā ir tabuliņa, kurā redzama informācija par sertifikātu. Zemāk iespējams izvēlēties ar kuru sertifikātu parakstīt tikko uzģenerētās atslēgas pieprasījumu („Signer”). Iespējams izvēlēties vienu no sistēmai pieinstalētajiem ROOT sertifikātiem, vai izvēlēties „Self signed”, kas nozīmē, ka sertifikāts tiks parakstīts pats ar sevi. Kas parakstījis sertifikātu, nekādā veidā neietekmē drošību, bet nodrošina sertifikāta autentiskuma pārbaudi. Sekojošajā ailītē izvēlas sertifikāta derīguma termiņu dienās. Spiež pogu **[Sign]**, un sertifikāts tiks nolikts rindā uz parakstīšanu.

#### 10.9.6 Lietotāju pieprasītie sertifikāti

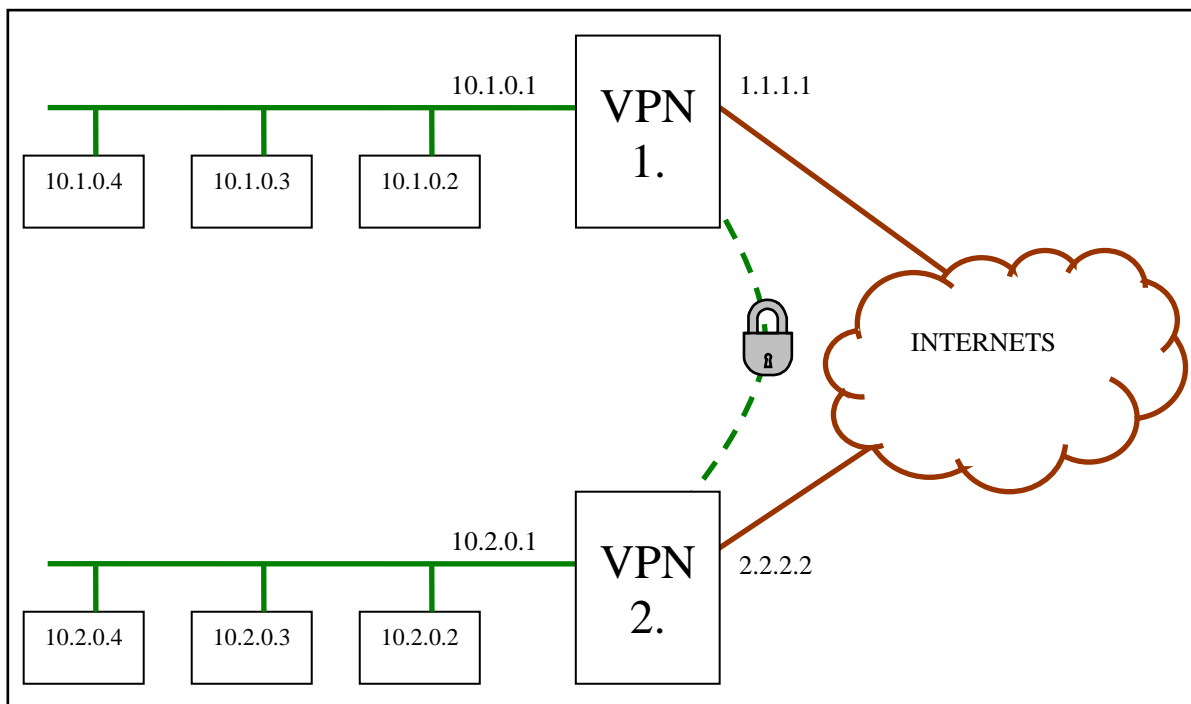
Šī ir sadaļa, kas pieejama sistēmas lietotājiem ar tiesību līmeni „User”. No šīs sadaļas iespējams paņemt citu lietotāju sertifikātu publiskās atslēgas (piemēram, e-pasta kriptēšanai), uzģenerēt lietotāja sertifikātu („[Request new certificate for person \(e-mail signing\)](#)”), tas automātiski nonāks kategorijā „Person”. Iespējams uzģenerēt sertifikātu VPN autorizācijas vajadzībām („[Request new certificate for computer \(vpn\)](#)”). Tāpat iespējams apskatīt un lietotāja operētājsistēmā ieinstalēt citus, uz sertifikātu servera pieejamus sertifikātus („[Other certificates](#)”). Šeit parādās sertifikāti no tām kategorijām, kuras tika atļautas sertifikātu servera konfigurācijā.

### 10.10. Virtuālais privātais tīkls (VPN)

VPN nodrošina drošu divu attālinātu tīklu savienošanu izmantojot interneta tīklu. Virtuālā privātā tīkla servisu pievieno no ugunssienas komponentu lapas. Klikšķina uz saites „[Virtual private network](#)”. Ielādējas nākamā izvēļu lapa, kas piedāvā izvēlēties VPN tipu (*Choose VPN type*:). Ir trīs iespējamie „ipsec” VPN konfigurācijas modeļi un viens CIPE konfigurācijas modelis:

- tunelis uz specifisku IP adresi (*VPN tunnel to specific IP*), izmantojams, lai izveidotu tuneli uz citu hostu kas atbalsta IPSEC VPN savienojumu, bet nav kāds no konfigurācijas servera hostiem. Piemērs varētu būt VPN uz kādu citu organizāciju, vai uz kāda cita ražotāja izstrādātu tīkla iekārtu.
- tunelis starp diviem konfigurācijas servera hostiem, saucamais spogulis (*Mirrored VPN with other host in management*), speciāli paredzēts lai nodrošinātu vienkāršotu VPN konfigurēšanu starp diviem konfigurācijas servera hostiem.
- tunelis ar nenoteiktu otrā gala adresi (*VPN tunnel with unspecified endpoint*), izmantojams gadījumos kad nav iespējams noteikt otra gala adresi. Piemēram, cilvēks ar portatīvo datoru, kurš izmanto iezvanpieeju, vai dators ar dinamisko (DHCP) adresi.
- CIPE VPN tunelis, kas realizē šifrētu IP datu pakešu enkapsulāciju UDP paketēs, CIPE VPN nodrošina trafika kriptēšanu ar „Blowfish” algoritmu, atbilstoši protokola specifikācijai ([http://sites.inka.de/bigred/devel/cipe-doc/cipe\\_6.html](http://sites.inka.de/bigred/devel/cipe-doc/cipe_6.html)). Kā pozitīvu īpašību var minēt, ka šāds tunelis vieglāk sakonfigurējams ja pa vidu ir tīkla adrešu translācija (NAT).

Attiecīgi noklikšķina uz nepieciešamo konfigurācijas modeli.



#### 10.10.1 Tunelis uz specifisku IP adresi

Visa konfigurācijas lapa ir sadalīta pa vairākām daļām. Pirmā ir „*Status*”, pie „*Name*” norāda konkrētā VPN nosaukumu, un ar ķeksīti atzīmē būs aktīvs vai nē. Nākamā sadaļa, ir tuneļa gali (***Tunnel endpoints***). Tās ir VPN interneta adreses (hostu ārējās adreses). Pie „*local ip*” norāda šī gala VPN adresi, pie „*remote ip*” – otra VPN tuneļa gala IP. Tālāk seko sadaļa „*Networks*”, kurā definē kādas adreses ies caur VPN tuneli. Pie „*local address*” norāda iekšējās adreses. Pēc parauga VPN1 galā tās būs 10.1.0.0:255.255.255.0 vai kā šajā gadījumā tīkls norādīts izmantojot automātisko adrešu grupu (~Ugunssienu/Local/subnet). Pie „*remote address*” norāda otra VPN gala iekšējās adreses. Šīs sadaļas konfigurācija abos tuneļa galos ir vienāda, tikai apgriezta otrādi.

Nākamā ir sadaļa „*IPSEC parameters*”. Vairumā gadījumu pietiek ar noklusētajiem uzstādījumiem. Ir svarīgi ievērot, ka **abos VPN galos parametriem jābūt vienādi uzstādītiem**. Atzīmējot pie „*keep alive*” norāda, ka VPN tunelis visu laiku tiks uzturēts aktīvs. Pretēji, tunelis tiks izveidots tikai brīdī, kad tiek sūtīti dati caur to.

Sadaļa „*IKE proposals*”, te jānorāda kādā veidā notiks apmaiņa ar kriptēšanas atslēgām. Vismaz vienam algoritmam jābūt atzīmētam, piedevām abos VPN galos jābūt atzīmētam vismaz vienam kopīgam algoritmam. Nu un beidzamais lauciņš ir apraksta ierakstīšanai (*description*). Te var pierakstīt svarīgu informāciju lai vēlāk būtu vieglāk atcerēties ko, uz kurieni, un kādām vajadzībām ir šis VPN. Gala beigās spiež pogu [Save].

ugunssiena Start : Ugunssiena > Virtual private network

### VPN tunnel to specific IP

**Status:**  
name   
enabled

**Tunnel endpoints:**  
local ip   
remote ip

**Networks:**  
local address  or   
remote address  or

**IPSEC parameters:**  
protocol   
encryption   
hash   
pfs group   
lifetime   
keep alive

**IKE proposals:**  
proposals  3des|sha1|modp768|key|3600  
 rijndael|md5|modp768|cert|3600

description

[Configure certificate authorization](#)  
[Configure preshared key](#)

Edit proposals:  
1 3des|sha1|modp768|key|3600  
2 rijndael|md5|modp768|cert|3600  
[Add new proposal](#)

[Download configuration for Windows XP](#)  
[Download configuration for Windows 2000](#)

Pēc datu saglabāšanas lapas apakšā būs parādījušās jaunas izvēles. Konfigurēt sertifikātu autorizāciju (*Configure certificate authorization*) un konfigurēt sarunāto atslēgu (*Configure preshared key*), zem šīm saitēm norāda viena un/vai otra veida VPN autorizēšanās metodes datus. Kuru no autorizēšanās metodēm konfigurēt (kura tiks izmantota) nosaka parametri, kas norādīti pie autentifikācijas metodēm (*Edit proposals*). Noklikšķinot uz saites [Configure certificate authorization](#) ielādēsies lapa, kas parāda pieejamos sertifikātus, ar kuriem ir iespējama autorizācija. Te parasti ir vismaz divi CA sertifikāti un vismaz viens katram hostam. Izvēlas sertifikātu un to atzīmē. Tabulas apakšā ir pogas. **[Add as trusted certificates]** nospiežot šo pogu atzīmētie sertifikāti tiks uzstādīti, kā autorizācijas sertifikāti, konkrēti ar šiem sertifikātiem varēs autorizēties VPN piekļuvei. **[Add as trusted signers]** nospiežot šo pogu atzīmētie sertifikāti tiks uzstādīti kā uzticamie sertifikāti, VPN piekļuvei varēs autorizēties ar sertifikātiem, kas parakstīti ar šiem, uzticamiem sertifikātiem. Sertifikāti, kas aktivēti parādās augšā, tabulīnā „Valid certs”.

Noklikšķinot uz saites „*Configure preshared key*” ielādējas lapa kur ailītē jāieraksta VPN sarunāta atslēga (kaut kas līdzīgs parolei, tikai tipiski tā ir garāka virkne). Iekš „*Edit proposals*” konfigurē VPN autorizācijas metodes. Var labot esošās autorizācijas metodes vai pievienot jaunas.

Apakšā atrodas saites uz Microsoft Windows XP un Windows 2000 automātiskās konfigurācijas failiem. Šie konfigurācijas faili ir izmantojami lai automātiski nokonfigurētu Windows operētājsistēmu,

kā dotā VPN otro galu. Sīkāk par šo failu izmantošanu skatīt pielikumā „VPN tunelis uz Windows 2000/XP”.

#### 10.10.2 Tunelis starp diviem konfigurācijas servera hostiem

Būtība ir tieši tāda pati kā konfigurējot tuneli uz noteiktu IP adresi. Atšķirība tikai tā, ka šajā gadījumā automātiski tiks nokonfigurēts arī otrs VPN gals. Šāda iespēja ir tikai tad ja veido VPN savienojumu starp diviem, viena konfigurācijas servera hostiem. Šo otro hostu norāda sadaļā tuneļa gali (**Tunnel endpoints**), ailītē „remote ip”. Kā redzams tad tajā var izvēlēties tikai kādu no esošajiem hostiem un to adresēm. Pārējā konfigurācija ir identiska, kā pie abu galu VPN konfigurācijas (10.10.1 punkts). Nedaudz var mulšināt fakts, ka pie otrā gala hosta nekur neparādās, ka tam ir VPN savienojums ar pirmo. Šo VPN konfigurē tikai vienā galā jo otrā galā konfigurācija ir tāda pati, tikai IP adreses ir pretēji.

#### 10.10.3 Tunelis ar nenoteiktu otrā gala adresi

Šāda VPN konfigurācija nepieciešama ja nav iespējams noteikt vienu VPN gala adresi. Šāda situācija var būt aktuāla, ja nepieciešams lai kāds lietotājs varētu piekļūt lokālajam tīklam no dažādiem ārējiem punktiem, vai ja otrajā galā ir dinamiskā IP adrese. Konfigurēšana atkal ir ārkārtīgi līdzīga abiem iepriekšējiem VPN modeļiem. Atšķirība tā, ka nevienā vietā nav jānorāda otrā VPN gala adreses.

#### 10.10.4 CIPE VPN tunelis

CIPE VPN pēc būtības ir vienkāršots standarta VPN gadījums. Un tomēr konfigurācija nedaudz atšķiras. CIPE VPN pievieno no ugunssienas komponentu lapas, tajā izvēloties „*Virtual private network*” un nākamajā izvēļu lapā izvēloties „*CIPE vpn tunnel*”.

The screenshot shows the configuration interface for a CIPE VPN tunnel. The window title is "ugunsiena Start: firewall > Virtual private network". The main title is "CIPE vpn tunnel". Under "Status:", the name is "CIPE VPN" and "enabled" is checked. Under "Tunnel endpoints:", the local ip is "127.1.1.1 (Internet)" with port "1010", and the remote ip is "192.168.11.1" with port "12000". Under "Networks:", the local address is "~firewall/Local LAN/subnet" and the remote address is "192.168.0.0:255.255.255.0". The preshared key is "5A38C9BA1F" with a note "up to 16 bytes (in hexadecimal)". There is a description field which is currently empty. At the bottom, there are three buttons: "Save", "Save & Back", and "Cancel".

Konfigurācijas lapā izskatās līdzīga parasta VPN gadījumam. „name” – nosaukums. „enabled” – vai aktivēt CIPE VPNu.

Sadaļā „**Tunnel endpoints**” norāda abu tuneļa galu mašīnu IP adreses un portus. Ports var būt jebkurš ugunssienas brīvais ports (0-65000).

Sadaļā „**Networks**” norāda kādi tīkli iet caur tuneli.

„preshared key” – atslēga, kaut kas līdzīgs parolei. Jāuzdod heksadecimālajā pierakstā un tā nevar būt garāka par 16 baitiem (32 hekso simboli).

Vēl atliek apraksts („description”) par konkrēto tuneli, kas nav obligāts, bet vēlams.

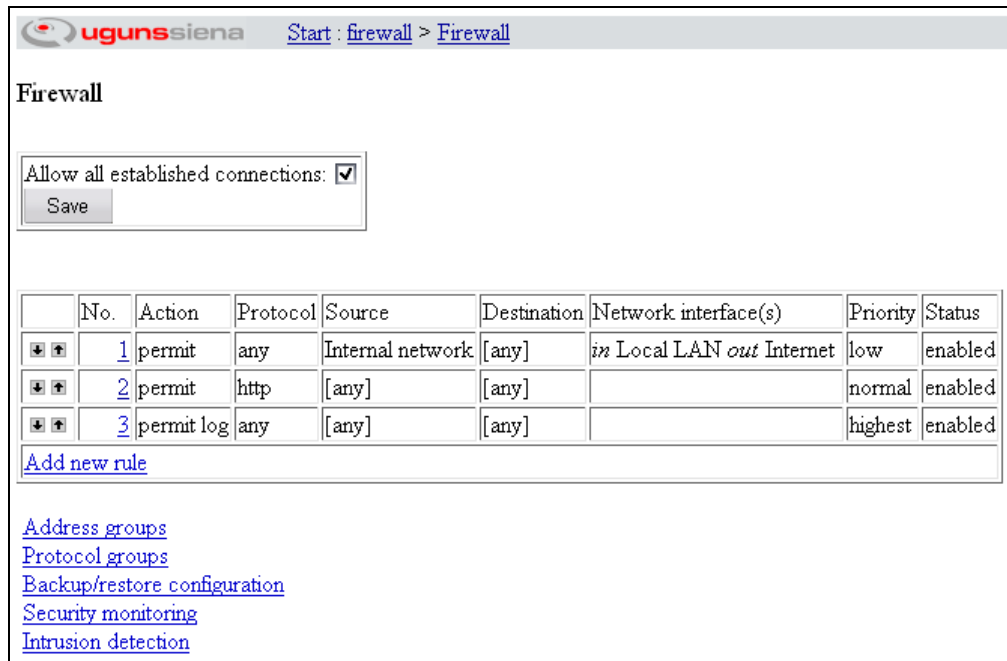
VPN tuneli ir iespējams nokonfigurēt starp ugunssienu un Microsoft Windows2000/XP izmantojot standarta Windows iespējas. Kā to realizēt skatīt pielikumā „VPN tunelis uz Windows2000/XP”.

### 10.11. Ugunsmūris (Firewall)

Ugunsmūris ir viena no galvenajām ugunssienas sastāvdaļām, kas nodrošina nepieciešamo drošības līmeni. vienīgi ugunsmūris ir pareizi jākonfigurē lai tas darbotos kā paredzējis lietotājs.



Lai pievienotu ugunsdmūri, uguns sienas komponentu lapā klikšķina uz saites „*Firewall*”, atveras jauna lapa.



Pirmajā tabulā ir iespēja norādīt kā darbosies ugunsdmūris. Ja ir atzīmēta rūtīņa „*Allow all established connections*”, tas nozīmē, ka ugunsdmūris pārbauda tikai savienojumu dibinošās datu paketes, un ja tās atbilst kritērijiem, tad ugunsdmūris atļauj nodibināt savienojumu, sekojošās paketes vairs nepārbaudot. Ja noteikti vajag lai ugunsdmūris pārbauda katru datu paketi, tad ķeksīti jāņem laukā. Tomēr no ātrdarbības viedokļa ieteicams ķeksīti atstāt, un ja tomēr vajag lai ugunsdmūris pārbauda dažos gadījumos visas paketes, tad tas jānorāda konkrētā filtra konfigurācijā.

#### 10.11.1 Ugunsdmūra filtri

Nākamā tabula rāda kādi filtri jau pievienoti. Par katru filtru ir nedaudz, bet pietiekoši informācijas lai saprastu ko apmēram tas dara. Filtru secību var mainīt klikšķinot uz bultiņām (uz augšu un uz leju). Labot esošu filtru var noklikšķinot uz tā numuriņu. Lai pievienotu jaunu ugunsdmūra filtru (*rule*), otrajā tabuliņā klikšķina uz saites „*Add new rule*”. Atveras ugunsdmūra filtra lapa.

„*Rule number*” – filtri izpildās pēc kārtas, pirmais, otrais, trešais u.t.t.. Datu pakete ienāk ugunsdmūrī un iet cauri visiem filtriem līdz atbilst kāda filtra nosacījumiem. Piemērs: filtrs 1 norāda, ka paketes, kas nāk no Latvijas, ir jāaizliedz; filtrs 2 atļauj paketēm no Latvijas iet tikai uz īpašām IP adresēm. No šādas konfigurācijas nav jēgas, jo neviena Latvijas pakete līdz filtram 2 nenokļūs. Šādā gadījumā ir jāmaina filtru secība. Filtra numuru var mainīt arī iepriekšējā logā, kur ir redzami visi definētie filtri. Blakus lodziņā var izvēlēties aktivizēt (*enabled*) vai atstāt izslēgtu (*disabled*) filtru.

Rīcība (*Action*). Šajā tabulas rindiņā norāda ko filtrs darīs, kad datu pakete tiks saņemta. Pirmajā lodziņā ir iespēja izvēlēties starp trīs darbībām: noliegt (*deny*), atļaut (*permit*) un noraidīt (*reject*) par to brīdinot sūtītāju. Noliegdošā darbība aizliedz pakešu plūsmu, ja izpildās filtra kritēriji, atļaujošā – atļauj pakešu plūsmu, ja izpildās kritēriji un noraidošā aizliedz pakešu plūsmu un dod par to ziņu paketes sūtītājam. Šajā rindā tālāk seko vairākas izvēles rūtīņas (*check box*), ieliekot ķeksīti attiecīgajā rūtīņā papildus tiks veiktas sekojošās darbības:

- „*Log*” – pieraksta visus gadījumus, uguns sienas drošības žurnālā, kad kāda pakete ir atbildusi filtra kritērijiem.
- „*Keep state*” – šis savienojuma variants nodrošina tā saukto dinamisko filtru. Dinamisks filtrs tiks izveidots tad, kad tiks saņemta savienojumu atverošā pakete un slēgts pēc savienojumu slēgdošās paketes saņemšanas, vai laika noilguma. Ieķeksējot šo rūtīņu tiek panākts, ka tiek pārbaudīta katra datu pakete, kas atbilsts filtra nosacījumiem, jāizvēlas šī opcija ja nepieciešams noteikt filtrēšanas prioritāti.
- „*Accept replies (bi-directional)*” – šis ir pēdējais no savienojumu veidošanas tipiem. Tas ir abējāda savienojums, no klienta uz serveri un no servera uz klientu.

ugunssiena Start: firewall > Firewall

Rule number	1	enabled
Action	permit	<input type="checkbox"/> Log <input checked="" type="checkbox"/> Keep state <input type="checkbox"/> Accept replies(bi-directional)
Groups		Custom values
Service	any	protocol: <input type="text"/> (only tcp, udp) source port: <input type="text"/> destination port: <input type="text"/>
Source address	Internal network	<input type="text"/> ip or ip:subnet
Destination address	[any]	<input type="text"/> ip or ip:subnet
Interfaces	in Local LAN	out Internet
Priority	low	
Custom rule	<input type="text"/>	
Description	No iekšējā tīkla uz ārpusi	

Save Save & Back Delete Cancel

Tabulas pelēkā daļā tiek uzstādīti filtra kritēriji. Kritēriju daļa ir sadalīta divos stabiņos, pirmais ir grupas (*Groups*) un otrs ir izvēles vērtības (*Custom values*). Tādas kritērijus var uzdot divos veidos, vai nu izmantojot nedefinētās grupas, vai ierakstīt attiecīgas kritēriju vērtības pie paša filtra. Izmantot nedefinētu grupu ir ļoti ērti ja grupa sastāv no vairākām vienībām, toties gadījumos kad filtrs attiecas tikai uz vienu tīkla adresi vai protokolu portu, tad definēt jaunu grupu varētu būt neērti. Vienmēr ir noderīgi meklēt optimālāko variantu. Definējot tīkla servisu un adreses katrā var izvēlēties tikai vienu definēšanas variantu. Teiksim tīkla servisu definē izmantojot tikai izvēles vērtības un adreses definē izmantojot tikai definētās adresu grupas. Nedrīkst servisu definēt gan ar grupām, gan izvēles vērtībām vienlaicīgi, tāpat tas attiecas arī uz adresēm.

Tīkla servisi (*Service*), norāda uz kādu tīkla servisu attieksies filtra kritēriji. Grupu ailītē var izvēlēties kādu no nedefinētajām protokolu grupām, vai arī pie „*Custom values*” ieraksta izmantojamo protokolu un portus (tieši tāpat kā konfigurē protokolu grupas).

Sūtītāja adrese (*Source address*). Norāda sūtītāju (no kurienes nāk datu paka) adreses uz kādām attiecas filtrs. Var adreses izvēlēties no definētajām adresu grupām vai ierakstīt konkrētu adresi vai adresu grupu pie izvēles vērtībām.

Saņēmēja adrese (*Destination address*), adrese, uz kuru tiek sūtīta datu pakete. Norāda izmantojot adresu grupu, konkrētu adresi vai adresu grupu.

Rindīnā „*Interfaces*” norāda caur kuru ugunssienas tīkla karti dati, kas attiecas uz filtru, ienāk (*in*) un caur kuru tīkla karti dati iziet (*out*). Ailītēs var izvēlēties kādu no pieinstalētajām tīkla kartēm vai norādīt jebkuru (*any*). Šāda opcija krietni paaugstina ugunsmūra drošību gadījumos kad vajag atdalīt iekšējo tīklu no ārējā. Iekšējais tīkls iet caur vienu tīkla karti, bet internets pieslēgts pie otras, līdz ar to tīklus var atdalīt ne tikai pēc IP adresēm, bet arī fiziski pēc tīkla kartēm.

„*Priority*” – filtra prioritātes noteikšana. Nosakot filtru prioritāti iespējams regulēt interneta trafika plūsmu attiecības. Vienam tīkla segmentam nosakot augstāku prioritāti pār citu tam datu plūsmas ātrums būs attiecīgi lielāks. Viens gan, lai prioritātes darbotos nepieciešams lai katra datu pakete tiek pārbaudīta. Tas nozīmē, ka vai nu nedrīkst atļaut jau nodibināto savienojumu pakešu plūsmu bez pārbaudes („*Allow all established connections*”), vai filtra konfigurācijā jānorāda „*Keep state*” filtrēšana. „*low*” prioritāte ir divreiz lielāka kā „*lowest*”, „*normal*” prioritāte ir divreiz lielāka kā „*low*” un četras reizes lielāka, kā „*lowest*”, un tā uz priekšu. Tādas „*highest*” prioritāte ir 16 reizes lielāka kā „*lowest*” prioritāte.

Ailīte „*Custom rule*” ir tikai speciāliem gadījumiem, kad filtra vēlamā konfigurācija ir tik sarežģīta, ka to nevar izveidot ar ekrānformas līdzekļiem. Šī opcija paredzēta tikai īpaši zinošiem ugunssienas administratoriem.

Pēdējā ailītē (*Description*) ja nepieciešams, var ierakstīt paskaidrojumu par konkrēto filtru. Saglabā filtru spiežot pogu [Save & back].

Šajā pašā ugunsmūra lapā zem filtru tabuliņas ir vēl pāris noderīgas saites, uz adresu grupām (*Address groups*), protokolu grupām (*Protocol groups*).

### 10.11.2 Lietotāju autorizācija

Ugunssienas ugunsmūra papild iespēja ir nodrošināt piekļuvi interneta resursiem tikai autorizētiem lietotājiem. Konfigurējot ugunsmūri pie adrešu grupām ir tāda grupa „*[Authorized users]*”. Šī grupa ir dinamiska adrešu grupa, kas sastāv no autorizēto lietotāju IP adresēm. Kad lietotājs autorizējas uz ugunssienas viņa IP adrese nonāk šajā grupā, un atrodas tajā, kamēr vien lietotāja sesija ir aktīva. Lietotāji ir jāievieš tieši tāpat kā sistēmas administratori (skat. punktu 11.1), vienīgi viņu tiesību līmenis ir jāuzstāda kā „*User*”.

### 10.11.3 Rezerves kopijas

Lai izveidotu vai ielādētu ugunsmūra uzstādījumu rezerves kopiju, klikšķina uz saites „*Backup/restore configuration*”. Jaunā lapā būs redzamas visas pieejamās rezerves kopijas un to veidošanas datums. Jaunu kopiju var izveidot ailītē „*Backup name:*” ierakstot kopijas nosaukumu un atliek vien nospiegt pogu [OK].

Lai ielādētu rezerves kopiju, uz tās noklikšķina. Jaunā lapā izvēlas ko no visas rezerves kopijas atjaunot, ugunsmūra filtrus, protokolu grupas, vai adrešu grupas. Un spiež pogu [Restore]. Vecu vai nevajadzīgu rezerves kopiju izdzēs spiežot pogu [Delete backup].

### 10.11.4 Drošības uzraudzības žurnāls (Security monitoring)

Piedāvā apskatīt ugunsmūra log failu saturu, gan par konkrēto dienu, gan vecākus log failus no arhīva. Noklikšķinot uz saites „*Security monitoring*” ielādējas drošības uzraudzības žurnāls. Augšā ir trīs pogas, uz tām klikšķinot var tikt pie šīs dienas log faila un drošības grafikiem.

[Security graphs] grafiskā veidā parāda aizturēto datu pakešu skaitu, gan kopējo, gan pa protokoliem atsevišķi.

[Today's log] parāda visu konkrētās dienas aizturēto datu pakešu log failu.

[Today's log tail] parāda konkrētās dienas log faila beidzamās 20 rindiņas.

Zemāk var apskatīt log failus no arhīva, gan grafiskā veidā, gan teksta veidā. Visbeidzot iespējams log failus arī filtrēt. „*with in*” – rādīt tikai tās log rindiņas, kas satur konkrēto tekstu, „*with out*” rādīt tās rindiņas, kas nesatur konkrēto tekstu, teksts šajā gadījumā ir jebkāda simbolu virkne.

### 10.11.5 Uzbrukumu detektors (Intrusion detection)

Advancēts instruments, kas uzrauga ugunsmūra drošības log failus un ziņo ja ir sasniegts noteiktais pārkāpumu limits.

Galvenais darbības princips. Caur detektora filtra iziet katrs ugunsmūra drošības log faila ieraksts, ja ieraksts atbilst detektora filtra nosacījumiem, tad tiek iedarbināti detektora skaitītāji, kas pieskaita konkrēto gadījumu dažādos griezumos, pēc sūtītāja porta un adreses, pēc saņēmēja porta un adreses un pēc sūtītāja tīkla adreses. Kad skaitītājs saskaitījis noteikto skaitu pārkāpumu vai sasniedzis noteikto ierakstu skaitu, viņš ziņo uz norādīto e-pasta adresi.

Uzbrukumu detektors pieejams noklikšķinot uz saites „*Intrusion detection*”, ielādējas uzstādīto detektoru saraksta lapa.

Detector name	Description	Status
<a href="#">All</a>	10.5 to 10.69	enabled
<a href="#">Basic</a>	any -> any	enabled

Add new

Send warnings to:

Alert interval in seconds:

Save changes

Show log file for date:

Pirmā ir tabuļa, kas parāda visus uzstādītos detektorus, noklikšķinot uz detektora nosaukuma var pamainīt tā uzstādījumus. Lai pievienotu jaunu detektoru ir poga [Add new]. Tālāk seko daži pamat

uzstādījumi. „Send warnings to:” – e-pasta adreses, atdalītas ar komatiem, uz kurām detektora skaitītāji ziņos. „Alert interval in seconds:” – laika intervāls, kas norāda maksimālo ziņojumu sūtīšanas biežumu. Respektīvi, viena detektora viens skaitītājs nesūtīs brīdinājumus biežāk, kā norādīts. Ja skaitītājam būtu jānosūta 60 sekunžu laikā 4 ziņojumi, bet uzlikts laika intervāls ir 60 sekundes. Tad aizies pirmais ziņojums un pēc 60 sekundēm nākamais, kurš ziņos, ka pa šo laiku trīs reizes ir noticis ziņojamais gadījums.

Zemāk seko poga e-pasta adrešu un laika intervāla saglabāšanai [**Save changes**].

Beidzamā opcija ir apskatīt paša detektora log failus. Ailītē ieraksta datumu par interesējošo dienu un klikšķinot uz pogas [**OK**] apstiprina savu izvēli.

Pēc pogas [**Add new**] nospiešanas, pirmā ielādējas lapa, kas jautā pēc detektora nosaukuma. Kad tas ievadīts, pēc [**Save**] pogas nospiešanas ielādējas nākamā lapa, kas ir galvenā detektora konfigurācijas lapa.

Current detector: **Test** (enabled)

Disable   Rename   Delete   Back

Current filters:

	Nr	Action	Protocol	Source	Destination	Status
▼ ▲	1	include	any	Any	Any	enabled

[Add new filter](#)

Current counters:

Count	Interval	Type	Count per Type	Send mail	Message text	Status
10	60	any	-	<input checked="" type="checkbox"/>	type1	enabled
10	60	source port	10	<input checked="" type="checkbox"/>	type2	enabled
10	60	source address	10	<input checked="" type="checkbox"/>	type3	enabled
10	60	destination port	10	<input checked="" type="checkbox"/>	type4	enabled
10	60	destination address	10	<input checked="" type="checkbox"/>	type5	enabled
10	60	source network	10	<input checked="" type="checkbox"/>	type6	enabled

Send warnings to E-mail group: Test ▼

Alert interval in seconds: 10

Save

Augšā ir pamata vadības pogas. [**Enable**]/[**Disable**] – aktivēt/pasivēt detektoru, [**Rename**] – mainīt detektora nosaukumu, [**Delete**] – izdzēst detektoru un [**Back**] – atgriezties pievienot detektoru lapā.

Tabuliņa „Current filters”, te ir detektora filtri ar domu atrast paketes, kas varētu interesēt. Sākotnēji ir filtrs, kuram atbildis jebkurš log faila ieraksts. Lai mainītu filtra nosacījumus noklikšķina uz tā numuriņu.

Rule number: 1 ▼ enabled ▼

Action: include ▼

Groups: any ▼

Service: any ▼

Source address: any ▼

Destination address: any ▼

Custom values: protocol: ▼ (only tcp, udp) source port: destination port: ▼

Save   Save & Back   Delete   Cancel

Ja ir vairāki detektora filtri, tad pirmajā rindīnā („Rule number”) norāda filtra numuru un aiz tā vai aktivēt, vai neaktivēt filtru. Nākamā rindīņa „Action” norāda vai ieraksts, kas atbildis nosacījumiem tiek uzskatīts par vajadzīgo vai nevajadzīgo, „include” – iekļaujot, „exclude” – izņemot. Tālāk, „Service”,

norāda par kādiem interneta protokoliem un portiem ir interese šim filtram. „Source address” sūtītāja adrese, „Destination address” saņēmēja adrese. Protokolus un adreses var norādīt gan tieši gan izmantojot adrešu grupas. Filtru saglabā ar pogu [Save].

Detektora skaitītāju tabuliņa „Current counters”, pavisam ir seši skaitītāji.

- „any” skaita jebkuru gadījumu kad ugunsmūra log ieraksts ir atbildis detektora filtriem.
- „source port” skaita pēc sūtītāja portiem.
- „source address” skaita pēc sūtītāja adreses.
- „destination port” skaita pēc saņēmēja porta.
- „destination address” skaita pēc saņēmēja adreses.
- „source network” skaita pēc sūtītāja tīkla adreses.

Visiem skaitītājiem izņemot „any” ir trīs galvenie parametri.

- „Count per type” – maksimālais ierakstu skaits, par kuriem skaitīt gadījumus.
- „Min. count” – gadījumu skaits, kas skaitītājam jāsavāc lai viņš ziņotu.
- „Interval” – laika intervāls sekundēs pēc kura ieraksts vairs neskaitīsies.

Lai vieglāk būtu saprast skaitītāju darbības principu, sīkāk par sūtītāja adreses skaitītāju („Source address”). Pēc detektora filtra atrasts, ka ieraksts ar sūtītāja adresi x.x.x.x ir jāpieskaita. Skaitītājs atzīmē sūtītāja adresi x.x.x.x un tai skaita atzīmē ieliek 1. Ja tiek atrast nākamais ieraksts ar sūtītāja adresi x.x.x.x, tad tagad adresei x.x.x.x skaita atzīmē ieraksta 2. Ja atrod ierakstu ar adresi y.y.y.y tad arī to skaitītājs atceras un skaita atzīmē ieliek 1. Tātad „Count per type” ir cik tādas adreses skaitītājs spēs atcerēties. „Min. count” cik liels skaits pie vienas adreses jāsavāc lai par to ziņotu. Un „Interval” ir laiks, pēc kura sasniegšanas vairs neskaitās adreses atrašanas gadījums. Šāds darbības princips ir visiem filtriem, vienīgi filtrs „any” jebkuru gadījumu skaita tikai vienā skaita atzīmē.

Lai mainītu skaitītāja uzstādījumus noklikšķina uz tā nosaukuma. Jaunā lapā iespējams izvēlēties aktivēt vai pasivēt skaitītāju („Enable/disable counter”). Izmainīt trīs galvenos parametrus („Count per type”, „Min. count” un „Interval”), izvēlēties vai sūtīt ziņojumus uz e-pastu (ziņojums noteikti tiks ierakstīts detektora log failā), kā arī ierakstīt skaitītāja ziņojuma tekstu („Message text”).

## 10.12. Tīkla adrešu tulkošana (Network address translation - NAT)

Šis serviss nodrošina iespēju vairākus datorus pieslēgt internetam (jebkuram IP tīklam) caur vienu adresi vai arī slēpt iekšējā tīkla adreses no publiskā interneta tīkla. Kad apakštīkla dators sūta pieprasījumu uz kādu interneta serveri (destination address), tad NAT serveris, caur kuru iet savienojumi, datu paketē nomaina sūtītāja adresi (source address) uz savu vai norādīto, un to iesūta tīklā. Kad NAT serveris saņem atbildes paketi no prasītās adreses (destination address), tad viņš pārveido adresi atpakaļ uz apakštīkla datora adreses, un iesūta apakštīklā. Tādā veidā apakštīkla dators saņem atbildes paketi no prasītā servera.

Lai pieinstalētu NAT servisu, ugunssienas komponentu lapā klikšķina uz saites „[Network address translation](#)”.

Start : [firewall](#) > [Network address translation](#)

Name: NAT tests  
Interface: vlan Local LAN  
Default address for translation:   
Reverse:

[NAT filters](#)

Static translation rules

protocol	local address	port	public address	port	description
tcp	10.10.11.5	1024-1124	192.168.0.1	2024-2124	John server
tcp	10.10.11.6	986	192.168.0.1	120	Bank software
any					

Save Save & Back Cancel

Click here to remove NAT: Delete

Ieraksta NAT vārdu un izvēlas uz kuru tīkla karti (Interface) serviss darbosies (biežāk ārējā pieslēguma tīkla karte). Gadījumā ja tīkla karte darbojas uz vairākām IP adresēm tad ailītē „Default address for translation” norāda kura būs primārā adrese.

Atzīmē ailītē „Reverse”, ja nepieciešams veidot reverso tīkla adrešu tulkošanu. Šāds NATs nepieciešams gadījumos, ja to konfigurē uz iekšējā tīkla adreses, nevis kā pierasts uz ārējās adreses. Šāds NATs darbojas principā tieši tāpat, vienīgi apgriezti – tīkla paketē, tai izejot caur NAT serveri tiks nomainīta nevis *source*, bet *destination* adrese.

Apakšējos lodziņos (*Static translation rules*) var norādīt tā saucamos statiskos tulkojumus. Tie ir izmantojami gadījumos kad iekšējā tīklā darbojas kāds serveris kam jābūt pieejamam no „ār pasaules”. Ailītē „*protocol*” izvēlas kāds protokols izmantojams. Pie „*local address*” norāda iekšējā tīkla datora adresi un pie „*port*” norāda portu vai portu apgabalu, kuru izmantot. Tālāk norāda publisko adresi (*public address*) un publisko portu vai portu apgabalu. Ailītē „*description*” var norādīt aprakstu par konkrētā ieraksta nozīmi.

Ir vērts ievērot, ka portu apgabalu izmēriem ir jāsakrīt. Tāpat jāievēro lai starp šiem statistiskajiem tulkojumiem nebūtu ierakstu starp kuriem sakrīt adrešu un portu apgabali.

Rezultāts būs tāds, griežoties no ār pasaules pie norādītās publiskās adreses ar attiecīgo portu, NAT serveris automātiski visas paketes pārsūtīs pie datora ar norādīto lokālo adresi un norādīto lokālo portu. Līdz ar to lokālā servera serviss būs pieejams, tā it kā tas darbotos uz uguns sienas ārējā interfeisa.

Kad dati ievadīti spiež uz pogas [Save] tādā veidā apstiprinot izmaiņas. Parādīsies jauna saite „*Routing rules*”, uz tās noklikšķinot atveras maršrutēšanas filtru lapa.

ugunsiena Start : firewall > Network address translation > Filters						
In						
Nr	Action	Protocol	Source	Destination	Status	
1	translate	any	[any]	Public network	enabled	
<a href="#">Add new rule</a>						
Out						
Nr	Action	Protocol	Source	Destination	Status	
1	translate	any	Internal network	[any]	enabled	
<a href="#">Add new rule</a>						

Konfigurēšanu veic skatoties no NAT servera tīkla kartes viedokļa. „*Out*” filtri būs tie, kas laidīs datus no iekšējām adresēm uz ār pasauli. „*In*” filtri savukārt laidīs datus atpakaļ no ār pasaules pie prasītājiem (iekšējā tīkla adresēm).

Loģiskāk konfigurēšanu sākt ar izejošo daļu, „*Out*” tabulā klikšķina uz saites „*Add new rule*”. Ielādējas jauna lapa.

ugunsiena Start : firewall > Network address translation > Filters	
Rule number	1 enabled
Action	translate
Groups Custom values	
Service	any protocol: (only tcp, udp) source port destination port
Source address	Internal network ip or ip.subnet
Destination address	[any] ip or ip.subnet
Save Save & Back Delete Cancel	

„*Rule number*” – norāda filtra numuru un vai aktivēt (*enabled*), vai neaktivēt (*disabled*). Lai darbotos, filtru vajag aktivēt (*enabled*).

„*Action*” – norāda NAT darbību, tulkot (*translate*), vai izsūtīt uzreiz (*direct*). Norāda tulkot (*translate*).

Pie „*Service*” norāda ar kādu protokolu un portu notiks darbība (izvēlas no definētajiem protokoliem, vai ieraksta vajadzīgās vērtības ar roku. Lai internets būtu pieejams pilnā apmērā tad izvēlas grupu kur ir visi protokoli (*any*)).

„*Source address*” – adreses, no kurām nāk pieprasījumi. Dotajā gadījumā tās ir visas iekšējā tīkla adreses, ja vajadzīgs, lai visi no iekšējā tīkla tiek klāt internetam.

„*Destination address*” – adrese, uz kuru no iekšējā tīkla tiek sūtīts pieprasījums. Tātad tās būs visas adreses, kuras nav iekšējā tīklā. Tā kā lokālajā tīklā šo uzdevumu veic pašas tīkla kartes, un pa lokālo tīklu darbojas lokālie maršrutētāji, tad tās, kas pienāks pie NAT servera, būs tikai ārējās adreses, kuras vajag tulkot. Parasti izvēlas grupu, kura satur visas interneta adreses (*any*).

Tādat NAT serveris tulkos (NATos) visu kas nāk no iekšējā tīkla un ir adresēts uz jebkuru interneta adresi (lokālās adreses atkrīt pašas par sevi). Spiež uz pogas **[Save & Back]**.

Kad nokonfigurēta izejošā daļa var sākt konfigurēt ienākošo daļu. „In” tabulā klikšķina uz saites „*Add new rule*”.

The screenshot shows the 'Filters' configuration page in the ugunssiena interface. The breadcrumb path is 'Start : firewall > Network address translation > Filters'. The configuration form includes:

- Rule number: 1, enabled
- Action: translate
- Service: any
- Source address: [any]
- Destination address: Public network
- Custom values: protocol (dropdown), source port, destination port

Buttons at the bottom: Save, Save & Back, Delete, Cancel.

Te viss ir tieši tāpat kā pie „Out” filtra konfigurēšanas. Vajadzīgs, lai tulkotas tiktu adreses, kas ienāk no ārpusaules. Tādat tulko jebkuru protokolu un portu (*Service*), kas nāk no jebkuras (*any*) interneta adreses (*Source address*) un ir adresēts uz (*Destination address*) tīkla ārējām adresēm (parasti viena adrese, kas nāk no interneta pakalpojumu sniedzēja). Tādat NAT serverim pieder ārējā adrese, un viss, kas tiek sūtīts uz viņa ārējo adresi, tiek tulkots uz kādu no iekšējām adresēm. NAT serveris zina, no kuras iekšējās adreses bija pieprasījums uz konkrētu interneta adresi, tādēļ atbildi no tās interneta adreses, viņš pārsūta konkrētajai iekšējai adresei. Ja pie NAT servera pienāk savienojums no kādas interneta adreses, bet neviena iekšējā tīkla adrese nav pieprasījusi informāciju no tās adreses, tad NAT serveris uzskata, ka tas savienojums ir domāts viņam pašam.

Kad lauciņi aizpildīti spiež uz pogas **[Save & Back]**.

### 10.13. HTTP starpniekserveris (HTTP proxy)

HTTP starpniekserveris (*proxy*) ir labs līdzeklis, kā vienkāršā veidā ierobežot lietotāju piekļuvi HTTP resursiem. Šo servisu pievieno no ugunssienas komponentu lapas klikšķinot uz saites „*HTTP proxy*”. Ir jāievēro lai starpniekserveris varētu darboties, ugunssienai ir jābūt pieejai pie DNS servera, vai uz tās jābūt palaistam DNS bufferserverim.

The screenshot shows the 'HTTP proxy' configuration page in the ugunssiena interface. The breadcrumb path is 'Start : firewall > HTTP proxy'. The configuration form includes:

- Enabled:
- Port: 8080
- IP address (optional): 192.168.0.200 (Local LAN)
- Outgoing IP address (optional): 127.1.1.1 (Internet)
- Transparent:

Buttons: Save, Save & Back, Cancel.

No.	Action	From	To	Status
1	permit	[any]	domain: *.lv	enabled
2	permit	~firewall/Local LAN/subnet	domain: *	enabled

Buttons: Add new rule, Transparent mode filters, Show log (Access log, 20031203, Ok), Click here to remove HTTP proxy (Delete).

Pēc noklusēšanas HTTP starpniekserveris tiek uzstādīts uz 8080 porta. Portu, protams, iespējams nomainīt uz jebkuru citu, ja vien to „neklausās” kāds cits uguns sienas serviss. „IP address” ja nepieciešams norāda no kuras adrese šis serviss būs pieejams, pretējā gadījumā tas būs pieejams no jebkuras uguns sienas adrese. „Outgoing IP address” ja nepieciešams norāda adresi izejošajam trafikam, adrese, no kuras starpniekservera serviss veiks pieprasījumus uz interneta resursiem.

Starpniekserveris spēj darboties saucamajā caurspīdīgajā režīmā („Transparent”), tas nozīmē, ka lietotājiem nav nepieciešams speciāli pārkonfigurēt savas interneta pārlūkprogrammas. Viss interneta trafiks, kas atbilst sadaļā „Transparent mode filters” uzrādītajiem filtriem tiks automātiski padots caur šo starpniekserveri.

Ja konfigurēšanu šajā brīdī beidz, tad starpniekserveris ir gatavs darboties. No jebkuras adrese uz jebkuru iespējams nokļūt izmantojot šo serveri. Un tomēr bieži vajadzīgs dažādi ierobežot HTTP trafiku, šim gadījumam ir starpniekservera filtri. Jaunu filtru pievieno klikšķinot uz saites „Add new rule”.

Filtra pirmajā rindiņā izvēlas filtra numuru un aktivēt vai uzstādīt neaktivizētu filtru. Nākamā rindiņā „Action” norāda atļaut („permit”) vai aizliegt („deny”) filtram atbilstošus savienojumus. Rindiņā „Source address” pieprasītāja adreses, adreses, no kurām veic savienojumu uz starpniekserveri. Izvēlas no adrešu grupām, vai ieraksta konkrētu adresi ar netmasku. Visbeidzot izvēlas pieejamos resursus („Destination url”). Izvēlas kāds būs kritērijs, „url” – konkrēta adrese (http://www.ugunssiena.lv/klientiem/), „domain” – domēns (ugunssiena.lv) vai „path” – lapas apgabals (/eng/news/). Sekojošajā ailītē ieraksta vēlamu izteiksmi ar zvaigznīti apzīmējot neierobežotu skaitu patvaļīgu simbolu. Tālāk sekojošajā ailītē („Case sensitive”) aizņeksējot nozīmē, ka nosacījums ir jutīgs uz lielajiem un mazajiem burtiem. Ieliekot ķeksi beidzamajā ailītē („Regular expression”) nosacījums tiek uzvertts kā loģiskā izteiksme, šajā gadījumā ir krietni lielākas iespējas nedefinēt kādu konkrētu nosacījumu, bet ir jāzina kā raksta loģiskās izteiksmes, teiksim lai izteiktu to pašu ko normāli ar „\*” nepieciešama šāda izteiksme : „\.\*”.

Piezīme. Ja nav neviena filtra starpniekserveris apkalpo visus pieprasījumus, ja ir kaut viens filtrs, tad tikai tos kas ir definēti.

Pašā apakšā ir dažī formas elementi („Show log”) kuru mērķis parādīt sakrātos log failus. Pirmajā ailītē izvēlas piekļuves log failu („Access log”) vai aktivitāšu log failu („Event log”), otrajā ailītē ieraksta datumu par kuru interesē log failus apskatīt. Spiežot uz pogas [OK] apstiprina izvēli.

#### 10.14. Datu plūsmas uzskaitē (Traffic accounting)

Ugunssiena ietver arī datu plūsmas uzskaites sistēmu. Lai pievienotu šo servisu, uguns sienas komponentu lapā klikšķina uz saites „Traffic accounting”.



Lai saņemtu vēlamu informāciju, tad sāk ar to, ka izvēlas laika periodu (*Date interval*) no – līdz, datuma formāts ir ggggMMDD. gggg – pilns gads, MM – mēneša numurs izteikts ar diviem cipariem un DD – mēneša diena izteikta ar diviem cipariem.

Tālāk obligāti jāizvēlas par kādu tīkla karti veikt uzskaiti. (*Choose interface*), norāda kādu no pieinstalētajām tīkla kartēm. Nākošajā sadaļā izvēlas no adrešu grupām par kurām rādīt statistiku, attiecīgi to atzīmējot izvēles rūtiņā.

Kad tas darīts spiež uz pogas **[Make groups report]**, un tad ielādēsies tabula, kurā būs atskaite. Gadījumā ja ir izvēlēts liels laika intervāls un datu plūsma ir bijusi liela, tad uz datu tabulas parādīšanos būs ilgāk jāpagaida.

Ir iespējams skatīt atskaiti pēc IP adresēm (*Statistic by ip address*). Tad pirmajā lodziņā norāda adreses no grupas (*Address from group*) un otrajā – adreses uz grupu (*Traffic to group*). Tādā veidā statistika tiks parādīta no vienas grupas uz otru. Apakšā izvēles rūtiņa nozīmē, ka otrā grupa tiks sadalīta pa konkrētām IP adresēm. Lai apskatītos atskaiti spiež uz pogas **[Make ip addresses report]**.

## 10.15. E-pasta serveris (E-mail server)

E-pasta servera administrācijas rīki ir sadalīti divās daļās. Ir globālie konfigurācijas parametri, kas pieejami no konfigurācijas servera un ir lietotāju kontu konfigurācijas sistēma, kas pieejama lokāli uz katra e-pasta servera atsevišķi. Globālā konfigurācija pieejama konfigurācijas serverī zem attiecīgā hosta klikšķinot uz saites „[Email server](#)”. Lietotāju kontu konfigurācija pieejama pēc adreses: „<https://host/local/email/>” kur „*host*” ir attiecīgā hosta adrese (IP vai vārdiskā).

### 10.15.1 E-pasta servera globālie konfigurācijas parametri.

The screenshot shows a web browser window with the title "ugunssiena" and a breadcrumb "Start : testgw > Email server". The main content is titled "Email server configuration". It contains several input fields and checkboxes:

- Domains:** A text box containing "example.com".
- POP3 enabled:** A checked checkbox followed by "on port" and a text box containing "110".
- Specific IP (optional):** An empty text box.
- Server e-mail:** A text box containing "mail@example.com".
- Add signature filter:** An unchecked checkbox.
- Add 'local mail' filter:** An unchecked checkbox.
- Translations:** A section with two columns: "alias" and "target". The "alias" column has a text box with "exs.com" and the "target" column has a text box with "exapmle.com".

At the bottom of the form are three buttons: "Save", "Save & Back", and "Cancel". Below these buttons is a link "Click here to remove Email server:" followed by a "Delete" button. At the very bottom is a blue link "User account configuration".

„*Domains*” – norāda kādus domēnus serveris apkalpos. Brīvajā ailītē ieraksta pirmo domēnu un pēc **[Save]** pogas nospiešanas parādīsies vēl viena tukša ailīte nākamā domēna ievadīšanai.

„*POP3 enabled*” – atzīmē ar ķeksīti un norāda portu, ja nepieciešams aktivēt POP3 pieeju serverim.

„*Specific IP*” – norāda uz kuras no ugunssienas adresēm tiks pieņemti POP3 savienojumi.

„*Server e-mail*” – e-pasta adrese, no kuras tiks izsūtīti visi servera paziņojumi.

„*Add signature filter*” – atzīmē ar ķeksīti, ja lietotājiem nepieciešama iespēja saņemt tikai parakstītas e-pasta vēstules.

„*Add 'local mail' filter*” – atzīmē ar ķeksīti, ja ir lietotāji, kuriem nepieciešama iespēja saņemt tikai lokālā domēna e-pasta vēstules.

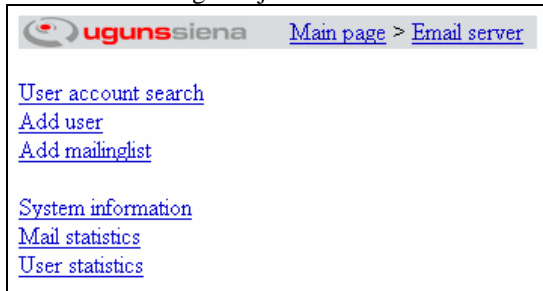
„*Translations*” – būtībā norāda e-pasta pseidonīmus („*alias*”). Piemērā redzams, ka e-pasta adreses, kurām hosta daļa sastāv no *exs.com* tiks translētas uz *example.com*. Tādejādi e-pasta vēstules, kas nāk uz adresi *user@exs.com* tiks pārtranslētas uz *user@example.com*.

Viss beidzot, apakšā pieejamas standarta vadības pogas.

Vēl pie šīs konfigurācijas formas pieder saite lapas apakšā „[User account configuration](#)”. Šī saite aizved līdz lokālo lietotāju kontu konfigurācijas rīkiem. Tie ir atrodas atsevišķi uz katras ugunssienas uz kuras uzstādīts e-pasta serveris.

### 10.15.2 Lietotāju kontu konfigurēšana

Lietotāju kontu konfigurācijas rīki pieejami lokāli uz katra ugunssienas e-pasta servera (ne uz konfigurācijas servera). Pieslēgties ugunssienas e-pasta servera lokālajiem konfigurācijas rīkiem iespējams pēc adreses: „<https://host/local/email/>” kur „host” ir attiecīgās ugunssienas adrese (IP vai vārdiskā), vai no konfigurācijas servera pie e-pasta servera konfigurācijas ir saite uz lokālo lietotāju kontu konfigurāciju.



### 10.15.3 Lietotāju meklēšana

Izvēlnē („*User account search*”), te ir iespēja meklēt sistēmā reģistrētos lietotājus.



The screenshot shows a search form with the following fields and controls:

- full name:
- e-mail:
- type:  (dropdown menu)
- order by:  (dropdown menu)
- Buttons: Search, Back

Below the form, there is a table with the following content:

name	e-mail
<a href="#">Admin</a>	<a href="mailto:admin@ugunssiena.lv">admin@ugunssiena.lv</a>

Meklēt iespējams pēc lietotāja norādītā pilnā vārda („*full name*”), vai pēc e-pasta adreses („*e-mail*”). Atrasti tiek tie ieraksti, kuros ietilpst uzdotā meklēšanas atslēga. Ailītē „*type*” norāda meklēt tikai lietotāju adreses („*users*”), vai tikai adresātu sarakstus („*mailinglists*”), vai abos tipos („*any*”). Ailītē „*order by*” norāda rezultātus kārtot pēc vārda vai e-pasta adreses. Kad kritēriji uzstādīti, spiežot pogu **[Search]**, tiek sameklēti atbilstošie lietotāju kontu ieraksti.

Rezultātos klikšķinot uz vārda iespējams labot lietotāja uzstādījumus. Klikšķinot uz e-pasta adreses iespējams apskatīt lietotāja pastkastītes saturu.

### 10.15.4 Lietotāju pievienošana

Jaunu lietotāju vai adresātu sarakstu („*mailing list*”) pievieno klikšķinot uz saites „*Add user*” vai „*Add mailinglist*” attiecīgi. Konfigurācija starp parastu lietotāju vai adresātu sarakstu atšķiras tikai ar vienu ķeksīti („*mailinglist*”) konfigurācijas formā.

ugunssiena [Main page](#) > [Email server](#)

### User information

full name	<input type="text" value="User User"/>
e-mail	<input type="text" value="user@example.com"/>
pop3 username (blank - same as email name)	<input type="text"/>
password (blank - leave old)	<input type="password" value="*****"/>
screen name in webmail	<input type="text" value="User"/>
mail box size	<input type="text" value="2000"/> K.B; 0-unlimited
delete mail from Inbox after	<input type="text" value="0"/> days; 0-unlimited
other email	<input type="text"/>
enable account	<input checked="" type="checkbox"/>
enable forward	<input type="checkbox"/>
forward addresses	<div style="border: 1px solid gray; height: 100px; width: 100%;"></div>
accept only local mails	<input type="checkbox"/>
accept only signed mails	<input type="checkbox"/>
use trash folder	<input checked="" type="checkbox"/>
use sent folder	<input checked="" type="checkbox"/>
mailinglist	<input type="checkbox"/>
admin notes	<input type="text" value="test user"/>

Pilnais vārds („*full name*”), obligāti aizpildāmais lauks. Lietotāja vai adresātu saraksta nosaukums.

E-pasta adrese („*e-mail*”), obligāti aizpildāmais lauks. Pilna lietotāja e-pasta adrese ar visu domēna daļu. Ugunssienas e-pasta serveris var apkalpot vairāku domēnu e-pasta kastītes, tādēļ arī jānorāda e-pasta adreses domēna daļa.

POP3 pieejas lietotāja vārds. Šo var atstāt tukšu, tādā gadījumā par POP3 lietotāja vārdu kalpos e-pasta adreses lokālā daļa.

Parole („*password*”), lietotāju gadījumā - obligāti aizpildāms lauks, adresātu saraksta gadījumā var atstāt tukšu, tādā veidā nodrošinot, ka nav iespējams pieslēgties e-pasta serverim ar listes lietotāja vārdu. Lietotājs šo parametru var mainīt pats pieslēdzoties webmail sistēmai.

Ekrāna vārds („*screen name in webmail*”), ja lietotājs izmantos e-pasta servera webmail iespējas, tad šis būs vārds ko redzēs citi saņemot vēstuli no šī lietotāja ("*User*" <*user@example.com*>). Lietotājs šo parametru var mainīt pieslēdzoties webmail sistēmai.

Pastkastītes izmērs („*mail box size*”), maksimālais pieejamais diska vietas daudzums lietotāja e-pasta vēstuļu glabāšanai uz servera, izmērs kilobaitos. Vērtība 0 (nulle), nozīmē virtuāli neierobežotu pastkastītes izmēru (kopējais ierobežojums visiem lietotājiem, ir pieejamais ugunssienas cietā diska lielums).

Automātiska veco vēstuļu dzēšana („*delete mail from Inbox after*”). Vēstules, kas vecākas par norādīto dienu skaitu, tiks automātiski dzēstas no ienākošo („*Inbox*”) vēstuļu mapes. Vērtība 0 (nulle), nozīmē, ka automātiska vēstuļu dzēšana ir atslēgta. Lietotājs šo opciju var mainīt pieslēdzoties webmail sistēmai.

Cita e-pasta adrese („*other email*”), kāda cita lietotāja e-pasta adrese, kontaktinformācija sistēmas administratora vajadzībām.

Lietotāja konta aktivēšana („*enable account*”), atzīmējot ar ķeksīti norāda, ka šis lietotāja konts aktīvs. Tikai aktīva konta lietotāji var autorizēties webmail un POP3 pieejai.

Aktivēt e-pasta pārsūtīšanu („*enable forward*”). Šo izvēlni atzīmējot, viss ienākošais pasts tiks pārsūtīts uz zemāk norādītajām adresēm. Lietotājs šo opciju var mainīt pieslēdzoties webmail sistēmai.

Pārsūtīšanas adreses („*forward addresses*”), norāda e-pasta adreses, uz kurām pārsūtīt visas ienākošā pasta vēstules. E-pasta adreses katra jāraksta savā rindā (jāatdala ar [enter] simbolu). Ienākošā pasta vēstule netiek saglabāta ienākošo vēstuļu mapītē pēc pārsūtīšanas, bet ja tas tomēr nepieciešams, tad pārsūtāmo

adrešu sarakstā jānorāda paša saņēmēja adrese. Pārsūtīšana uz norādītajām adresēm ir spēkā tikai tad, ja ir aktivēta e-pasta pārsūtīšanas opcija.

Pieņemt pastu tikai no lokālā servera („*accept only local mails*”). Atzīmējot šo opciju, lietotājs saņems e-pasta vēstules tikai no lietotājiem tajā pašā domēnā. Lietotājs šo opciju var mainīt pieslēdzoties webmail sistēmai.

Pieņemt tikai parakstītas e-pasta vēstules („*accept only signed mails*”). Tiek pieņemtas tikai tās e-pasta vēstules, kuras ir parakstītas ar sūtītāja publisko atslēgu („*digital signature*”). Lietotājs šo opciju var mainīt pieslēdzoties webmail sistēmai.

Lietot miskastes mapīti („*use trash folder*”), atzīmējot šo opciju, dzēstās vēstules tiks pārvietotas miskastes mapītē. Lietotājs šo opciju var mainīt pieslēdzoties webmail sistēmai.

Lietot izsūtīto vēstuļu mapīti („*use sent folder*”), atzīmējot šo opciju, visas izsūtītās vēstules automātiski tiks saglabātas izsūtīto vēstuļu mapītē. Lietotājs šo opciju var mainīt pieslēdzoties webmail sistēmai.

Adresātu saraksts („*mailing list*”). Šī opcija ir tikai kā pazīme sistēmā, lai vieglāk atšķirtu adresātu sarakstus no parastu lietotāju pasta kastītēm.

Administratora piezīmes („*admin notes*”), ailīte piezīmju saglabāšanai pie lietotāja konta.

#### 10.15.5 Sistēmas statusa informācija (*System information*)

Šajā sadaļā iespējams iepazīties ar dažiem sistēmas stāvokli raksturojošiem lielumiem. Informācija par failu sistēmām („*Filesystem information*”), disku partīciju izmēri un aizpildījums.

Sistēmā reģistrēto lietotāju skaits („*Registered users*”), webmail aktīvo sesiju skaits („*Active sessions*”), sistēmā saglabāto e-pasta ziņojumu skaits („*Mails in system*”) un visu saglabāto e-pasta vēstuļu kopējais izmērs („*All mail size*”).

#### 10.15.6 Vēstuļu statistika (*Mail statistics*)

Iespējams apskatīt vēstuļu skaita statistiku gan par kādu e-pasta lietotāju atsevišķi, gan kopīgi par visiem lietotājiem. Atlasīšanai tiek izmantota lietotāja e-pasta adrese. Iespējams norādīt par kādu laika intervālu ir interese.

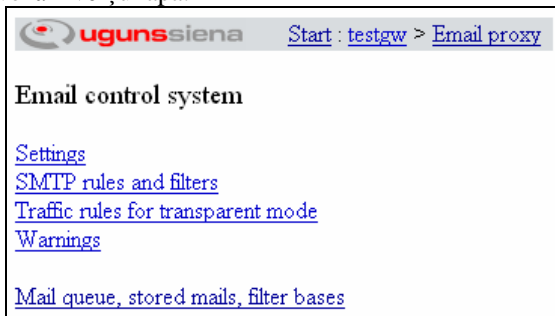
#### 10.15.7 Lietotāju statistika (*User statistics*)

Šajā sadaļā iespējams apskatīt statistisku informāciju par kādu sistēmas lietotāju. Tabuliņā redzami visi sistēmas lietotāji. Tabuliņu var sakārtot gan pēc lietotāja e-pasta adreses gan pēc aktivitāšu laika. Noklikšķinot uz lietotāja e-pasta adreses tiek parādīta informācija par lietotāja aktivitātēm sistēmā.

### 10.16. E-pasta kontroles sistēma (E-proxy) – centrālā konfigurācija

E-pasta kontroles sistēma (E-proxy) ir e-pasta aizsardzības un satura menedžmenta sistēma. Sistēma nodrošina visa veida e-pasta sūtījumu filtrēšanu, pēc izmēra, pēc satura, pēc pielikumiem, pēc sūtītājiem un saņēmējiem.

E-proxy konfigurācija pieejama no konfigurācijas servera pie attiecīgā hosta klikšķinot uz saites „*Email proxy*”. Ielādējas galvenā izvēlņu lapa.



#### 10.16.1 Vispārīgie E-proxy konfigurācijas parametri

Sadaļā „*Settings*” uzstāda vispārīgus E-proxy konfigurācijas parametrus.

„IP-address” un „port” – uzstāda uz kādas adreses un porta E-proxy klausīsies pēc ienākošajiem SMTP sūtījumiem. Šīs ailītes var atstāt tukšas, kas nozīmē uz jebkuras IP adreses 25 porta.

„Max-connections” – maksimālais pieļaujamais ienākošo SMTP konekciju skaits.

„Idle-timeout” – laiks sekundēs cik ilgi tiks turēta atvērta SMTP sesija, pēc pēdējo datu saņemšanas brīža.

„Timeout” – kopējais laiks sekundēs cik ilgi var notikt viena SMTP sūtījuma saņemšana. Ja e-pasta vēstule nav atnākusi šajā laikā, savienojums tiek pārtraukts.

„Max-size” – maksimāli pieļaujamais SMTP sūtījuma izmērs megabaitos (MB).

„Max-recv” – maksimāli pieļaujamais vienas e-pasta vēstules saņēmēju skaits.

„Server-email” – e-pasta adrese, no kuras tiks izsūtīti servera paziņojumi.

„Server-name” – servera DNS vārds, nepieciešams izsūtīt e-pasta vēstules, jo daži e-pasta serveri pārbauda vai vēstule nāk no „pareiza” hosta.

„Max-processes” – skaits cik e-pasta sūtījumi var tikt apstrādāti vienlaicīgi (paralēli). Apstrādājot e-pasta vēstules paralēli iegūst ātrdarbības uzlabojumus. Tomēr pārāk liels paralēlo procesu skaits var krasi samazināt kopējo ātrdarbību.

„Max-CPU-time” – norāda cik sekundes procesora laika tiek dotas vienas e-pasta vēstules apstrādei. Pirmajā ailītē norāda cik sekundes dotas uz vienu vēstuli, un otrajā norāda cik papildus sekundes procesora laika nāk klāt par katru e-pasta vēstules megabaitu (lielas e-pasta vēstules ir atļauts apstrādāt ilgāk).

„Transparent” – ja atzīmēts, tad E-pasta kontroles sistēma strādās „caurspīdīgajā” režīmā, respektīvi, caur E-pasta kontroles sistēmu ies visi tie e-pasta sūtījumi, kuri atbilst caurspīdīgā režīma filtriem.

„Report language” – izvēlas kādā valodā sūtīt paziņojumus lietotājiem no e-pasta kontroles sistēmas.

„Report week days” – nedēļas dienas, kurās sūtīt paziņojumus lietotājiem. Pirmais ķeksītis pirmdienai, līdz beidzamais – svētdienai.

„Report times” – norāda laiku cikos tiks izsūtīti paziņojumi.

#### 10.16.2 SMTP un e-pasta apstrādes filtri

Sadaļā „SMTP rules and filters” uzstāda SMTP saņemšanas noteikumus un saņemto e-pasta vēstuļu apstrādes filtrus.

ugunsiena Start: testgw > Email proxy

### E-proxy rules

#### SMTP rules

	Nr	Action	Source Address	Source Email	Destination Email	Status
⬇ ⬆	1	permit	is [any]	is [any]	is *@example.com	enabled
⬇ ⬆	2	permit	is Local net	is *@example.com	is [any]	enabled
⬇ ⬆	3	deny	is [any]	is [any]	is [any]	enabled

[Add new rule](#)

#### Filter rules

	Nr	Action	Source Address	Source Email	Destination Email	Prog	Status
⬇ ⬆	1	deny	is [any]	is [any]	is [any]	do-tasks	enabled
⬇ ⬆	2	deny	is [any]	is [any]	is [any]	attach-filter	enabled
⬇ ⬆	3	permit	is [any]	is [any]	is [any]	vscan-sophos	enabled

[Add new rule](#)

### 10.16.3 SMTP filtri

Sadaļā „SMTP rules” nedefinē noteikumus, kas nosaka e-pasta vēstuļu saņemšanu. Jaunu noteikumu pievieno tabulā, klikšķinot uz saites „Add new rule”.

ugunsiena Start: testgw > Email proxy

#### SMTP rules

Rule number: 1 enabled

Action: permit

Source address: is  group Group: [any]  ip IP or IP:subnet

Source email: is  group Group: [any]  email Email

Destination email: is  group Group:  email Email: \*@example.com

Save Save & Back Delete Cancel

„Action” – darbība ja ienākošais SMTP savienojums atbilst nedefinētajiem noteikumiem. „permit” – atļauj, „deny” – aizliedz savienojumu un „check” – nodod savienojumu pie nākamā filtra.

„Source address” – izsūtītāja IP adrese, ir („is”) vai nav („is not”) vienāda ar norādīto. IP adreses var norādīt vai nu kā adrešu grupu, vai kā atsevišķu adresi ar netmasku.

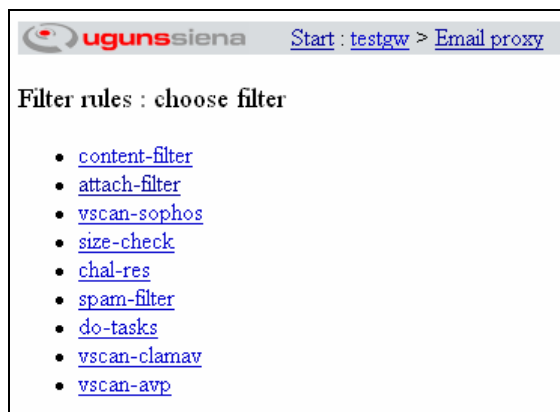
„Source email” – izsūtītāja e-pasta adrese, ir („is”) vai nav („is not”) vienāda ar norādīto. E-pasta adresi var norādīt vai nu kā adrešu grupu, vai kā atsevišķu adresi.

„Destination email” – saņēmēja e-pasta adrese, ir („is”) vai nav („is not”) vienāda ar norādīto. E-pasta adresi norāda vai nu kā adrešu grupu, vai kā atsevišķu adresi.

### 10.16.4 E-pasta apstrādes filtri – kopīgā konfigurācija

Sadaļā „Filter rules” nedefinē filtrus, kas tiek izpildīti uz saņemtajām e-pasta vēstulēm. Visu filtru konfigurācijas parametri ir ārkārtīgi līdzīgi. Vispirms kopīgās lietas.

Jaunu filtru pievieno klikšķinot uz saites „Add new rule”.



Ielādējas sarakstiņš ar iespējamajiem e-pasta filtriem. Izvēlas nepieciešamo filtru, noklikšķinot uz viņa nosaukuma. Kādi filtri ir iespējami, skatīt tālāk.

Filtru darbības shēma ir sekojoša. Ja e-pasta vēstule atbilst filtrā norādītajiem kritērijiem, tad pašai vēstulei tiek piemērota viena no darbībām, kas ir norādīta sadaļā „Action” un tiek izpildīts filtra uzdevums, kas norādīts sadaļā „Task”.

„Action” – darbība, kas jā dara ar e-pasta vēstuli, ja tā atbilst filtra kritērijiem. „permit” – atļaut, vēstule tiek nosūtīta saņēmējam. „deny” – aizliegt, vēstule tālāk netiek sūtīta (saņēmējs nesaņems). „check” – tikai pārbaude, šajā gadījumā filtrs neietekmē vēstules saņemšanu vai nesaņemšanu toties tiek izpildīts filtra uzdevums („task”).

„Rule timeout” – norāda cik reizes atkārtot filtru („Number of tries”), ja tas nav spējis atvēlētājā laikā izpildīties. Un ko darīt ja tā arī neizdodas vēstuli „izdzīt” cauri filtram. Darbības ir, „match rule” – tiek uzskatīts, ka vēstule atbilda filtra kritērijiem, vai „do task” – tiek uzskatīts, ka vēstule filtra nosacījumiem neatbilst, bet filtra uzdevums tomēr tiek izpildīts.

„Source address” – izsūtītāja IP adrese, ir vienāda vai nav vienāda ar adresi no adrešu grupas vai atsevišķi norādītu adresi.

„Source email” – izsūtītāja e-pasta adrese.

„Destination email” – saņēmēja e-pasta adrese.

„Send email to” – ja vēstule atbilst kritērijiem, tad tā tiks aizsūtīta uz norādītu adresi vai adrešu grupu.

„Send warning to” – ja vēstule atbilst kritērijiem, tad par to tiek aizsūtīts norādītais brīdinājums („Warnings”) uz e-pasta adresi vai adrešu grupu.

„Warn sender” – brīdinājums tiks aizsūtīts vēstules sūtītājam. Brīdinājuma vēstuli izvēlas pie „Warnings”.

„Warn recipient” – brīdinājums tiks aizsūtīts vēstules saņēmējam.

„Save” – vēstule tiek saglabāta uz E-proxy servera.

#### 10.16.5 E-pasta apstrādes filtri – specifiskā konfigurācija

Filtra konfigurācijā pašā apakšā ir katra filtra specifiskie konfigurācijas parametri.

„Content-filter” – e-pasta satura filtrs. Konfigurācijā norāda „regular expression” izteiksmi, kurai jāatbilst e-pasta sūtījumiem.

„Attach-filter” – e-pasta pielikumu filtrs. „pattern” – uzskaita e-pasta pielikumu failu kritērijus. Kritēriji jāraksta katrs jaunā rindīnā.

„Vscan-xxx” – vīrusu ķērāja filtrs. Beidzamie simboli („xxx”) ir antivīrusu programmas nosaukums. Vīrusu ķērājam nav specifisko konfigurācijas parametru. E-proxy vienlaicīgi var izmantot vairākus pretvīrusu filtrus. Piemēram, katru e-pasta sūtījumu pārbaudīt ar divu ražotāju vīrusu ķērāju. Tādā veidā samazinot risku, ka kāds vīrus tomēr izspruks cauri.

„Size-check” – e-pasta vēstules maksimālā izmēra filtrs. Maksimālo izmēru var norādīt kilobaitos („KB”) vai megabaitos („MB”).

„Chal-res” – Pieprasījuma-atbildes filtrs. Principā šis ir efektīvākais veids kā cīnīties ar spamu. Darbības princips ir sekojošs, iekšējām e-pasta adresēm ir piekārtots tā saucamais „balto” sūtītāju saraksts. Sūtītāji no „baltā” saraksta bez problēmām var nosūtīt vēstules uz iekšējām e-pasta adresēm. Sūtītāji, kuri nav baltajā sarakstā arī var nosūtīt vēstuli saņēmējam, bet viņiem vēstules sūtīšana būs jāapstiprina (jāielādē interneta lapa, kuras adrese saņemta automātiskajā atbildē). Pēc apstiprināšanas, viņu e-pasta adrese automātiski tiks pievienota „baltajam” sarakstam. Filtra specifiskā konfigurācija. „Host name or IP address” – ieraksta IP vai vārdisko adresi, kuru izmantot vēstules apstiprināšanas interneta lapas adresei. „Internal mails” – norāda e-pasta adrešu grupu, kuras adreses tiek aizsargātas ar šo filtru (iekšējās adreses). „Use accepted email address for any internal users” – ja atzīmēts tad visām iekšējām adresēm tiek uzturēta viena kopīga „balto” adrešu grupa. „Challenge recipient” – ja atzīmēts tad e-pasta adreses apstiprināšanas automātiskā atbilde tiek sūtīta nevis e-pasta izsūtītājam, bet gan saņēmējam.

„Spam-filter” – apmācāms antispama filtrs. Ailītē „Settings” norāda vai lietotājiem būs dota iespēja „apmācīt” spam filtra datubāzi. Ailītē „Host name or ip address” norāda hosta vārdu uz kura lietotāji varēs apskatīt spam filtra aizturētās vēstules. Ailītē „Send reports to” norāda e-pasta adrešu grupu, kurai sūtīt atskaites par visām aizturētajām e-pasta vēstulēm. Atskaites saņems katrs grupas lietotājs par vēstulēm, kuras aizturētas balstoties uz šī filtra darbību.

„Do-tasks” – pavisam vienkāršs filtrs bez papildus konfigurēšanas iespējām. Lietojams ja nepieciešams nosūtīt e-pastu vai kādu brīdinājumu pēc noteiktiem kritērijiem.

#### 10.16.6 E-pasta izejošie filtri

Ar šiem filtriem norāda kā jāizsūta e-pasta sūtījumi. Tipiski lokālie sūtījumi iet uz kādu lokālo serveri, pārējie, kur nu tiem jāiet. Konfigurācijas parametri ir ārkārtīgi līdzīgi tiem kas pie e-pasta apstrādes filtriem. Būtiskākā atšķirība ir beidzamā ailīte „Server IP”, ja šajā ailītē norāda saņēmēja SMTP servera adresi, tad e-pasta sūtījumi, kas atbilst filtram, tiks sūtīti uz šo serveri, nevis uz serveriem no e-pasta adrešu domēna daļas.

#### 10.16.7 E-proxy caurspīdīgais režīms

Strādājot „caurspīdīgajā” režīmā E-proxy pārtver visus tīkla savienojumus kas atbilst filtros uzstādītajiem noteikumiem. Tipiski izveido filtru kur visas SMTP konekcijas tiek pārtvertas un e-pasta sūtījumi tiek apstrādāti uz E-proxy. Šādā veidā var izvairīties no vīrusu un citu nevēlamu failu iekļūšanas un izkļūšanas no uzņēmuma iekšējā tīkla caur e-pasta sūtījumiem.

E-proxy galvenajā izvēlņu lapā klikšķina uz saites „Traffic rules for transparent mode” lai aktivētu saucamo „caurspīdīgo” režīmu. Jaunajā lapā, pašā augšā ar ķeksīti atzīmē vai aktivēt „caurspīdīgo” režīmu. Spiežot pogu [Save], izvēli apstiprina.

Jaunu interneta savienojumu pārtveršanas filtru pievieno klikšķinot uz saites „Add new rule”. Ielādējas filtra veidošanas forma.

„Action” – izvēlas vai savienojumi, kas atbilst filtra kritērijiem tiks pārtverti un apstrādāti („proxy”), vai arī savienojums netiks aiztikts („direct”).

„Service” – norāda kāds savienojuma protokols un ports tiek skatīts. To var norādīt ar protokolu grupu, vai ievadot izvēles vērtības.

„Source address” – sūtītāja IP adrese. Norāda kā adrešu grupu vai ievada izvēles vērtības.

„Destination address” – saņēmēja IP adrese. Norāda kā adrešu grupu vai ievada izvēles vērtības.



### 10.16.8 E-proxy paziņojumu sagataves

Veidojot E-proxy e-pasta apstrādes filtrus, konfigurācijā tiek izmantotas paziņojumu sagataves. Šīs sagataves var būt gan pilnībā statiski paziņojumi gan var tikt dinamiski ģenerētas pēc speciāliem noteikumiem filtra izpildes laikā.

Paziņojumu sagataves pieejamas no E-proxy galvenās izvēlņu lapas, klikšķinot uz saites „Warnings”.

ugunsiena Start : eproxy\_sm > Email proxy

#### Defined E-proxy warnings

- [attach admin](#)
- [attach recip](#)
- [attach sender](#)
- [chall-res recip](#)
- [chall-res sender](#)
- [content admin](#)
- [content recip](#)
- [content sender](#)
- [default](#)
- [spam black list sender](#)
- [spam claim](#)
- [spam recipient](#)
- [spam sender](#)
- [vscan admin](#)
- [vscan recip](#)
- [vscan sender](#)

Add

---

#### Default E-proxy filter warnings

	Admin warning	Sender warning	Recipient warning
content-filter	content admin	content sender	content recip
attach-filter	attach admin	attach sender	attach recip
vscan-sophos	vscan admin	vscan sender	vscan recip
size-check			
chal-res		chall-res sender	chall-res recip
spam-filter		spam sender	spam recipient
do-tasks			
Default warning	default	default	default

Set

Augšā redzamas iepriekš nedefinētās paziņojumu sagataves („Defined E-proxy warnings”). Noklikšķinot uz nosaukuma iespējams veikt izmaiņas tajā. Jaunu paziņojumu sagatavi pievieno spiežot pogu [Add]. Zemāk („Default E-proxy filter warnings”) var norādīt standarta paziņojumus pie dažādiem E-proxy filtriem.

ugunsiena Start: testgw > Email proxy

### Defined E-proxy warnings

Current warning: **default**

Name:

Head:

```
From: %SM
To: <>
Subject: the email was stopped
```

Body:

```
The email message sent from %S to %R was stopped.
The id of the email is %ID
Please contact %SM for further info.
```

**Warning variables**

- %SM server email
- %S sender
- %R recipients
- %SZ size
- %ID id
- %WT warning text
- %HD header
- %SB subject
- %DT date
- %IP ip
- %RN rule number
- %RI rule id
- %PN filter name

Buttons: Save, Save & Back, Delete, Cancel

Paziņojuma sagataves veidošanai izmanto dinamiskos mainīgos, kas filtra izpildes laikā tiks aizstāti ar atbilstošām vērtībām. Labajā pusē ir doti visi mainīgie un paskaidrojums kāda tipa vērtība viņa vietā tiks ielikta izpildoties filtram. Paziņojumam atsevišķi ir jāizveido galvenes daļa („*Head*”) un satura daļa („*Body*”).

### 10.17. E-pasta kontroles sistēma (E-proxy) – lokālā konfigurācija

E-proxy lokālā konfigurācija pieejama uz katra hosta pie tā tieši pieslēdzoties. Pieslēgties lokālās administrācijas rīkiem iespējams no E-proxy galvenās izvēlņu lapas (konfigurācijas serverī), tajā klikšķinot uz saites „*Mail queue, stored mails, filter bases*”, vai pieslēdzoties pie adreses: „*https://host-address/local/eproxy/*”, kur „*host-address*” ir hosta IP vai vārdiskā adrese.

ugunsiena Main page > Eproxy

- [Mails in processing](#)
- [Stored mails](#)
- [Anti-virus bases](#)
- [Upload email for antispam filter](#)
- [Statistic](#)

View mail with internal ID :

Lokālā konfigurācija piedāvā apskatīt dažāda veida informāciju par e-pasta vēstulēm, kuras dotajā brīdī atrodas uz servera.

#### 10.17.1 E-pasta vēstules apstrādes rindā

„*Mails in processing*” – klikšķinot uz šīs saites iespējams apskatīt kādas e-pasta vēstules dotajā brīdī tiek apstrādātas uz E-proxy servera. Rezultātus var atfiltrēt un kārtot izmantojot vēstuļu atlasē filtru.

ugunsiena [Main page](#) > [Eproxy](#) > [Stored mails](#)

**Show only mails where**

From address is  To address is

IP is  Filter is

Received after - (ddmmyyyy-hhmm) Received before - (ddmmyyyy-hhmm)

**Actions for emails**

Action:   Perform action for all found mails

Send to custom recipient:

**View**

Mails in page

[Show page as plain text](#)

Atlasīt rezultātus iespējams pēc „From”, „To” un IP adresēm, pēc E-proxy filtra un pēc saņemšanas datuma.

Zemāk iespējams norādīt darbību priekš atzīmētajām e-pasta vēstulēm. Ailītē „Action” izvēlas vienu no piedāvātajām darbībām.

„Send immediately” – e-pasta vēstule tiks aizsūtīta saņēmējam bez tālākas to apstrādes caur E-proxy filtriem.

„Process” – atzīmētajām e-pasta vēstulē tiek uzstādīts, ka tās tūlīt tiek apstrādātas.

„Delete” – atzīmētās e-pasta vēstules tiek dzēstas.

„Mark as spam and delete” – atzīmētās vēstules antispaama filtram tiek norādītas kā spam vēstuļu paraugs un tiek dzēstas.

„Mark as spam” – atzīmētās e-pasta vēstules antispaama filtram tiek norādītas kā spam vēstuļu paraugs.

„Mark as no spam” – atzīmētās e-pasta vēstules antispaama filtram tiek norādītas kā derīgās vēstules, ne spams.

Ir iespējams atzīmētās vēstules arī pārsūtīt kādam saņēmējam, Tādā gadījumā ailītē „Send to custom recipient” ieraksta saņēmēja e-pasta adresi un piespiež pogu **[OK]**.

Visbeidzot atlasē sadaļa, kas atbild par datu parādīšanu („View”). Ailītē „Mails in page” norāda cik vēstules rādīt uz ekrāna vienā lapā. Klikšķinot uz saites „[Show page as plain text](#)” rezultāti tiek parādīti tīra teksta veidā.

### 10.17.2 Aizturētās e-pasta vēstules

Aizturētās e-pasta vēstules („*Stored mails*”) iespējams atfiltrēt gluži tāpat kā vēstules apstrādes rindā. Arī darbības ar šīm vēstulēm ir stipri līdzīgas. Jauna opcija ir „Send to original recipients” – e-pasta vēstule tiks aizsūtīta oriģinālajiem saņēmējiem.

Ķeksītis „Perform action for all found mails” – nozīmē, ka nav nepieciešams atzīmēt katru e-pasta vēstuli atsevišķi lai ar visām izpildītu vienu darbību. Atzīmējot ar ķeksīti darbība tiks piemērota visām vēstulēm kas atlasītas pēc augstāk definētajiem filtrēšanas kritērijiem (arī tad ja visas vēstules nav redzamas uz ekrāna). Drošības labad, pēc **[OK]** pogas nospiešanas, vēlreiz būs jāatzīmē ķeksītis un jānospiež poga lai darbība tiktu izdarīta ar visām atlasītajām vēstulēm.

### 10.17.3 Pretvīrusu programmu vīrusu bāzes

Apskatīt pretvīrusu programmatūras vīrusu bāzes var klikšķinot uz saites „[Anti-virus bases](#)”. Tā kā E-proxy var izmanto vairākus pretvīrusu moduļus tad sākotnēji jāizvēlas kurš modulis interesē.

ugunsiena [Main page](#) > [Eproxy](#)

[Update anti-virus bases now](#)

file	date
main.cvd	2004.12.21 13:52
daily.cvd	2004.12.21 13:52

Tabuliņā redzamas jaunākās vīrusu definīcijas un kad tās atjaunotas. Pašā augšā ir saite „[Update anti-virus bases now](#)”, uz tās noklikšķinot tiek palaista antivīrusa atjaunināšanas procedūra.

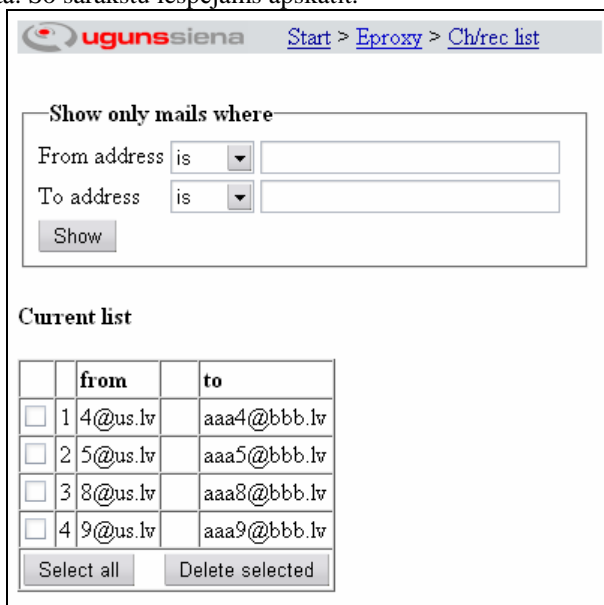
#### 10.17.4 Spam filtra datubāze

Antispama filtrs ir „jāapmāca”, viņam ir jāparāda kādas vēstules ir uzskatāmas kā spams un kādas ir atļaujamas. „Iebarot” tam vēstuli var klikšķinot uz saites „[Upload email for antispam filter](#)”. Ielādējas vienkārša forma. Pirmajā ailītē izvēlas vai vēstule, kura tiks augšupielādēta ir spams („spam”), vai uzskatāma par atļautu („not spam”). Pašu vēstuli var augšupielādēt divējādi, vai nu augšupielādējot vēstules failu (plain-text), vai ielīmēt („paste”) e-pasta tekstu lielajā teksta laukā. Šajā gadījumā vajag norādīt kā konvertēt jaunu rindu taustiņus („Convert newlines in text to:”).

Zem svītras ir saraksts ar spam filtra datubāzes rezerves kopijām. Rezerves kopijas tiek veidotas automātiski, bet ir iespējams izveidot papildus rezerves kopiju, spiežot uz saites „[Make backup now!](#)”. Rezerves kopiju iespējams lejupielādēt, kā arī augšupielādēt. Tas ir noderīgi ja jau „apmācīta” spam filtra datubāze jāpārnes uz citu hostu, vai ja kļūdas rezultātā ir sabojāta spam filtra datubāze.

#### 10.17.5 Izaicinājuma/atbildes filtra datubāze (Challenge/response)

Šis filtrs darbojas tā, ka aizsargātās pasta kastītes saņem vēstules tikai no tiem sūtītājiem, kuru e-pasta adreses ir „baltajā” sarakstā. Šo sarakstu iespējams apskatīt.



The screenshot shows a web interface for 'ugunsiena'. At the top, there are navigation links: 'Start > Eproxy > Ch/rec list'. Below this is a search filter section titled 'Show only mails where'. It contains two dropdown menus: 'From address' and 'To address', both currently set to 'is'. There are empty input fields next to each dropdown and a 'Show' button below them. Below the search section is a section titled 'Current list' containing a table with the following data:

	from	to
<input type="checkbox"/>	1 4@us.lv	aaa4@bbb.lv
<input type="checkbox"/>	2 5@us.lv	aaa5@bbb.lv
<input type="checkbox"/>	3 8@us.lv	aaa8@bbb.lv
<input type="checkbox"/>	4 9@us.lv	aaa9@bbb.lv

Below the table are two buttons: 'Select all' and 'Delete selected'.

Augšā ir ailītes lai būtu iespējams atfiltrēt rezultātus gan pēc sūtītāja adreses, gan saņēmēja. Zemāk ir pats e-pasta adrešu saraksts. Ja kāds ieraksts ir zaudējis savu aktualitāti, to iespējams atzīmēt un izdzēst.

#### 10.17.6 E-proxy statistika

„[Statistic](#)” – iespējams apskatīt vispārīgu statistiku par E-proxy darbību.

„[Mails in system](#)” – skaitliska informācija par e-pastu skaitu sistēmā kopumā, pēdējās 7 dienās, un pašreizējā dienā. Statistika par e-pasta vēstulēm kas dotajā brīdī tiek apstrādātas. Un statistika par aizturētajām e-pasta vēstulēm.

„[Top IP addresses](#)” – statistika par aktīvākajām IP adresēm. Tās ir adreses, no kurām ienākušas visvairāk e-pasta vēstules. Kopējā statistika, beidzamajās 7 dienās un tekošajā dienā.

#### 10.17.7 E-pasta vēstules apskatīšana pēc viņas ID vērtības

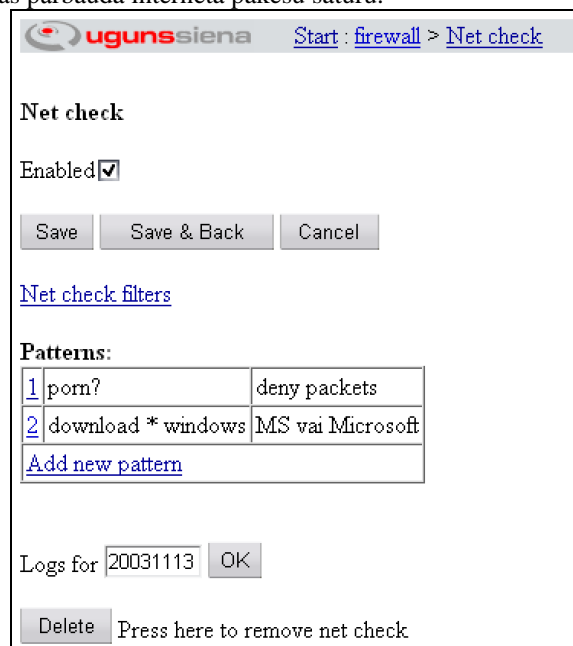
Katrai e-pasta vēstulei, kura iziet caur E-proxy sistēmu, ir savs unikāls ID kods. Šo kodu ierakstot ailītē „[View mail with internal ID](#)”, iespējams vēstuli apskatīt. Ielādējas vēstules apskates forma.



Augšā ir vispārīga informācija par vēstuli, zemāk redzams kāds filtrs bijis par iemeslu vēstules aizturēšanai. Tālāk seko e-pasta vēstules struktūra („Mail structure”). Pēc tam, divas saites, apskatīt vēstules galveni („View mail header”) un apskatīt visu vēstules kodu („View mail source”). Un pašā apakšā divas saites, ar kurām vēstuli pievieno antispama filtram vai nu kā spam vēstuli („This is a spam”), vai kā atļautu vēstuli („This is not a spam”).

### 10.18. Datu plūsmas pārbaude (Net check)

Šis ir instruments, kas pārbauda interneta pakešu saturu.

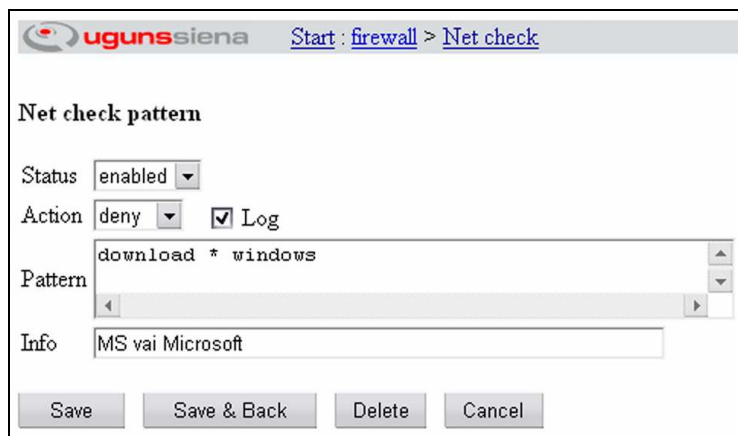


To kāda trafika paketes pārbaudīt norāda NetCheck filtros (*Net check filters*). Šie filtri veidojas gluži tāpat, kā ugunsmūra filtri. Filtriem atbilstošais interneta trafiks tiks pārbaudīts uz sadaļā „Patterns” norādītajām meklēšanas izteiksmēm.

Jau nedefinētās meklēšanas izteiksmes redzamas zem uzraksta „Patterns”. Numuri katras izteiksmes sākumā parāda meklēšanas secību un kalpo kā saites lai varētu pamainīt izteiksmi. Tālāk seko pati meklēšanas izteiksme un visbeidzot apraksts par izteiksmi.

Zemāk ir ailīte, kurā ierakstot datumu var apskatīt NetCheck log failu par konkrēto dienu.

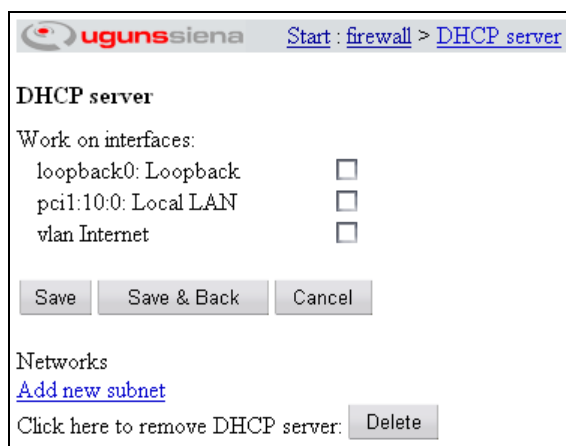
Jaunu izteiksmi pievienot klikšķinot uz saites „Add new pattern”.



Norāda vai izteiksme ir aktīva („*Status*”), darbību ko izpildīt ja datu pakete atbilst nosacījumam („*Action*”). „*deny*” – aizliegt, abiem savienojuma „galiem” tiek nosūtīta savienojumu aizverošā paka. „*permit*” – atļaut. Tālāk ar ķeksīti („*Log*”) atzīmē vai gadījumu pierakstīt log failā. Meklējamo izteiksmi norāda ailītē „*Pattern*”. Meklējamā izteiksme sastāv no interesējošā atslēgvārda kur vienu mainīgu simbolu var aizstāt ar „?” (jautājuma zīmi) un neierobežoti daudz patvaļīgu simbolu var apzīmēt ar „\*” (zvaigznīti). Piemēram, izteiksmei „j??is” atbilst gan „juris”, gan „janis”, gan visi citi vārdi kur starp „j” un „is” ir jebkuri citi simboli. Kā var manīt paraugā tad tāda izteiksme atbildīs gan „download microsoft windows”, gan „download MS windows”, gan visiem citiem tekstiem kur pieminēti vārdi „download ” un „ windows” vienlaicīgi, piedevām tieši šādā secībā. Beidzamā ailīte „*Info*”, tas ir neliels apraksts par izteiksmi, kas ar to ir domāts. Apakšā ir standarta darbību pogas, kuras izmantojot var saglabāt izteiksmi un / vai izdzēst izteiksmi.

## 10.19. DHCP serveris

Lai pievienotu DHCP servera servisu ugunssienai, ugunssienas komponentu lapā klikšķina uz saites „[DHCP server](#)”.



Pirmais jāizvēlas uz kuriem tīkla interfeisiem darboties serverim. To dara ieliekot ķeksīti pretī attiecīgās tīkla kartes nosaukumam. Kad interfeiss izvēlēts, saglabā konfigurāciju ar [**Save**].

Ailītē „*Freetext configuration*” iespējams norādīt papildus DHCP servera konfigurācijas parametrus. Par tiem skatīt zemāk.

Nākamais solis ir pievienot DHCP tīklus, to dara klikšķinot uz saites „Add new subnet”. DHCP tīkla konfigurācija sastāv no vairākām daļām. „*Network address*” un „*Netmask*”, šajās ailītēs ieraksta kādā adrešu apgabalā atradīsies DHCP klientu adreses, tīkla adrese un maska. Nākamā ir informācija DHCP klientam, „*Gateway*” maršrutētāja (rūtera) adrese, „*Domain name server*” vārda servera adrese (DNS).

Arī šeit ir ailīte „*Freetext config*”, tajā norāda papildus DHCP servera konfigurācijas parametrus. Piemēram Microsoft Windows darbustacijām varētu būt nepieciešams WINS servera adrese, to norāda šādi: `option netbios-name-servers 192.168.1.1`; Iespējams norādīt domēna adresi, to norāda šādi: `option domain-name "mydomain.org"`; Par papildus konfigurācijas parametriem iespējams uzzināt šajā interneta adresē: <http://isc.org/sw/dhcp/>

Norāda adrešu apgabalu („*IP address pool ranges*”) no kura klienti varēs saņemt adreses, norāda vai nu atsevišķas IP adreses vai adrešu apgabalu – galapunkti ietilpst apgabalā. Adrešu apgabalu norāda tikai ar adresēm nevis ar maskām.

Iespējams sasaistīt IP adreses un MAC adreses, lai konkrēti klienti vienmēr saņemtu noteiktu IP adresi.

Visbeidzot iespējams norādīt, ka šis DHCP servera tīkls būs kāda cita DHCP servera rezerves serveris. Normāli šo ailīti atstāj tukšu. Šis nepieciešams VRRP gadījumā.

## 10.20. DNS buferserveris (DNS cache)

DNS buferserveris nodrošina domēna vārdu atšifrēšanu. Šis serveris sūta pieprasījumus uz DNS serveri un izveido pats savu pagaidu DNS ierakstu tabulu, lai varētu apkalpot savus klientus. DNS buferserveri pievieš no uguns sienas komponentu lapas, klikšķinot uz saites „DNS cache”.

„Source address” – izvēlas no kuras interfeisa adreses griezties pie DNS serveriem.

„Forward mode” – izvēlas kādu no DNS buferservera darbības modeļiem, „none” – dati DNS ierakstu veidošanai tiks prasīti tikai no „DNS root” serveriem (daži starptautiskie lieli serveri), „first” – pirmām kārtām tiks apjautāti zemāk norādītie DNS serveri, un tikai tad starptautiskie „DNS root” serveri, vai „only” DNS tabula tiks veidota tikai balstoties uz informāciju no norādītajiem DNS serveriem.

„forwarders ip addresses” – norāda DNS serverus, kuriem sūtīt DNS pieprasījumus. Šie serveri tiks ņemti vērā tikai gadījumā, ja DNS buferservera darbības modelis būs vai nu „first”, vai „only”.

## 11. Administrēšanas logs (Administrative)

Pēc ielogošanās konfigurācijas serverī, katras lapas apakšā atrodas pelēka josla.

user: **Paraugs** ip: **10.10.10.11** [Logout](#) [Change password](#) [Administrative](#)

Uz šīs joslas ir saite uz sadaļu „Administrative”, vieta, no kuras var pievienot jaunus sistēmas lietotājus un apskatīt audita žurnālu, kurā fiksētas visas sistēmas lietotāju darbības sistēmā. Kad uz šīs saites noklikšķina, atveras lapa:

Administrators :  
[Paraugs](#)  
[Administrator](#)  
[adm](#)  
[Add new administrator](#)  
  
[Audit](#)  
[Make full backup](#)

Ir redzami visi sistēmā reģistrētie lietotāji. Lietotāji ar „Supervisor” tiesību līmeni var nomainīt citu lietotāju paroles, kā arī izveidot jaunus vai izdzēst esošos lietotājus no sistēmas. Lai pievienotu jaunu lietotāju, klikšķina uz saites „Add new administrator”.



## 11.1. Jauns sistēmas lietotājs

<b>Administrator profile</b>		
Username	<input type="text" value="user"/>	
Password	<input type="password" value="*****"/>	
Password (confirm)	<input type="password" value="*****"/>	
Full name	<input type="text" value="User"/>	
Organization	<input type="text" value="SIA Uzņēmums"/>	
E-mail	<input type="text" value="user@uznemums.lv"/>	
Phone	<input type="text" value="9696969"/>	
Timeout	<input type="text" value="600"/> seconds	
Supervisor	<input checked="" type="checkbox"/>	
Account locked	<input type="checkbox"/>	
Lock after incorrect logins more than	<input type="text" value="3"/>	
<b>Rights</b>		
edit	SIENA	
<input type="button" value="Save"/>	<input type="button" value="Save &amp; Back"/>	<input type="button" value="Cancel"/>

Lapā obligāti aizpildāmie lauciņi ir lietotāja vārds (*Username*) un parole (*Password*). Jāpiezīmē, ka lietotāja vārdā un lietotāja pilnajā vārdā nedrīkst izmantot latviešu burtus. Ailītē „*Timeout*” norāda dīkstāves laiku sekundēs, kuru pārsniedzot lietotājam būs atkārtoti jāautorizējas. Norāda lietotāja tipu, respektīvi, ir iespējams norādīt vai lietotājam būs „*Supervisor*” tiesību līmenis (šie lietotāji var pievienot jaunus, vai izdzēst un labot esošo lietotāju kontus). „*Account locked*” norāda vai šis lietotāja konts ir bloķēts. Lietotājs ar bloķētu kontu nevar autorizēties sistēmā. Nākamajā ailītē norāda pēc cik neveiksmīgiem autorizēšanās mēģinājumiem lietotāja konts tiks bloķēts. Atbloķēt kādu kontu var tikai lietotājs ar „*Supervisor*” tiesību līmeni. Ja lietotājam nav „*Supervisor*” tiesību līmenis, tad beidzamajā daļā norāda lietotāja tiesības uz atsevišķām sienām (hostiem). Tās var būt nekādas, (atstājot ailīti tukšu), tikai apskatīties (*view*) vai skatīt un labot (*edit*).

Sadaļā „*Administrative*” ir izvēle „*Audit*”. Audits parāda visas darbības, kas notikušas konfigurācijas serverī (kādi lietotāji apmeklējuši un kādas darbības veikuši).

Ir vēl viena sadaļa – „*Make full backup*”, klikšķinot uz šīs saites ir iespēja lejupielādēt visu ugunssienu uzstādījumu rezerves kopijas. Izmantojot datus no šī arhīva faila, ir iespējams atjaunot pilnīgi visu ugunssienu uzstādījumus, tādā stāvoklī kā tie bija rezerves kopijas veidošanas brīdī.

## 12. „Tools”

Šī sadaļa iekļauj sevī papildus instrumentus, kas nekādā veidā neietekmē ugunssienas darbību, bet palīdz darbā ar ugunssienu.

### 12.1. Log faili

Katra ugunssiena raksta daudz dažādus log failus. Visus šos log failus vienuviet var apskatīt no konfigurācijas servera. Sadaļā „Tools” izvēloties saiti „*Logs*”. Log failus var apskatīt arī lokāli, pieslēdzoties attiecīgajam hostam uz adresi: „*http://host-address/local/*” kur „*host-address*” ir hosta IP vai vārdiskā adrese.

ugunssiena Start > Logs

Choose host: remote Ok

system	files	size	exact size	today
<a href="#">audit</a>	16	6 KB	6 438	<a href="#">1 709</a>
<a href="#">messages</a>	16	72 KB	74 216	<a href="#">52 880</a>
<a href="#">runproc</a>	16	78 KB	79 536	<a href="#">37 515</a>
<a href="#">sperman</a>	16	5 KB	4 906	<a href="#">1 184</a>
<a href="#">sfire</a>	16	24 KB	25 046	<a href="#">19 349</a>
<a href="#">svntaler</a>	16	1 KB	1 024	<a href="#">0</a>

dhcp	files	size	exact size	today
<a href="#">dhcp</a>	1	47 KB	48 102	<a href="#">47 078</a>

**Disk information for log partition**

Total size	478 KB	489 501
Disk size	27 GB	28 931 223 552
Free disk	25 GB	26 394 116 096

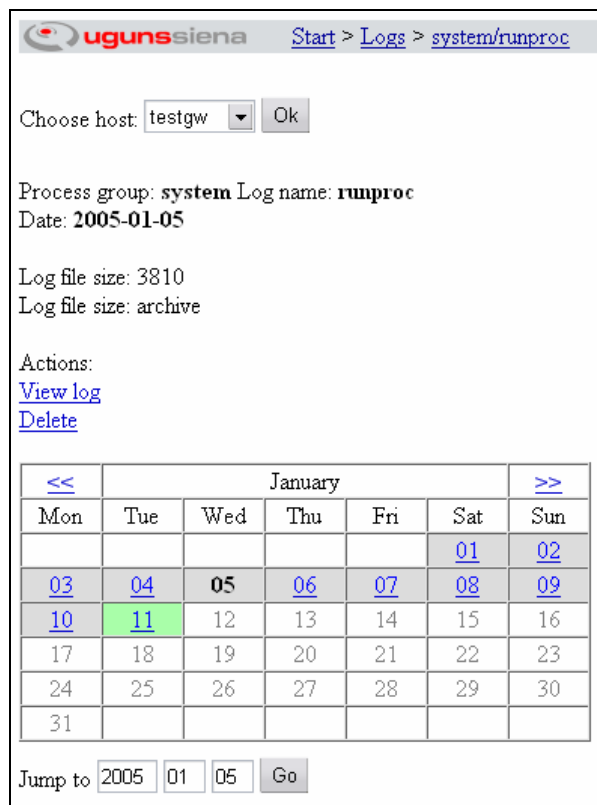
### 12.1.1 Vispārējā statistika

Pašā augšā izvēlas par kuru konfigurācijas servera hostu ir interese („Choose host”). Attiecīgi tabuliņā tiek parādīti visi log faili, kurus raksta konkrētā ugunssiena. Tabuliņā redzama pamat informācija par katru log failu. Pirmajā stabiņā – log faila nosaukums, otrajā („files”) – failu skaits (vienai dienai viens fails), trešajā stabiņā („size”) – kopējais failu izmērs norādīts cilvēkam viegli uztveramā formā, ceturtajā stabiņā („exact size”) – precīzs failu izmērs norādīts baitos un piektajā stabiņā („today”) – norādīts tekošās dienas faila izmērs.

Noklikšķinot uz log faila nosaukuma ielādēja log faila izvēles un apskates forma. Noklikšķinot uz beidzamajā ailītē redzamā šīsdienas log faila izmēra, iespējams to uzreiz apskatīt.

### 12.1.2 Log failu izvēles un apskates forma

No šīs formas iespējams apskatīt un / vai izdzēst jebkuru log failu.



Pirmajā ailītē „Choose host” izvēlas par kuru hostu ir interese. Zemāk seko informācija pie kādas grupas pieder konkrētais log fails un kā tas saucas, kā arī izvēlētais dienas datums. Pēc tam seko log faila izmērs un viņa tips, kas var būt arhivēts („archive”) vai parasts („plain”). Nākamā ir darbību sadaļa. Tajā ir divas saites, skatīt log failu („View log”) un dzēst log failu („Delete”). Viss beidzot ir navigācijas kalendārs, tajā ar pelēku krāsu atzīmētas tās dienas, par kurām ir log fails. Kalendārā noklikšķinot uz attiecīgās dienas var apskatīt tās dienas log failu. Pašā apakšā ir iespēja uzreiz ierakstīt interesējošās dienas datumu.

## 12.2. Address info

Šis ir viens no svarīgākajiem palīginstrumentiem pie ugunsienas ugunsmūra (*firewall*) konfigurēšanas.

*Address info* pārbauda IP adreses, un izdod datus:

- kādās adrešu grupās ietilpst konkrētā adrese
- kādi ugunsmūra (*firewall*) filtri (*rules*) attiecas uz adresi, ir iespējams norādīt kuras ugunsienas filtrus apskatīt (*Select Host:*)
- ja to norāda (*Look for DNS name*), tad meklē kāds DNS vārds ir piekārtots adresei
- ja norāda, tad meklē datus par adresi arī „WhoIs” serveros

Informācija par adrešu grupām palīdzēs noskaidrot vai konkrētā adrese ietilpst vajadzīgā adrešu grupā, vai kuras grupas tad īsti attiecas uz adresi.

Informācija par ugunsmūra filtriem kas darbojas uz IP adresi, palīdzēs gadījumos kad īsti nav skaidrs kādēļ adrese, netiek caur ugunsieni, vai taisni otrādi, tiek cauri. Tā kā ugunsmūra filtrus konfigurē uz katru ugunsieni atsevišķi, tad noderīgi ir izvēlēties lai informācija par ugunsmūra filtriem tiek meklēta tikai konkrētai ugunsienai. To var norādīt lauciņā „Select Host:”.

Ar ugunsieni nesaistīta iespēja ir atrast adresei piekārtoto DNS vārdu (*Look for DNS name*). Var gan minēt, ka vairumam adrešu DNS vārds nav piekārtots, bet tas neliedz pameklēt. Meklēt nav jēgas, ja ugunsienai nav pieejams DNS serveris.

Ļoti detalizētu informāciju par IP adresi var iegūt no *WhoIs* serveriem. It īpaši Eiropas adresēm, var atrast smalku informāciju, kam ir reģistrēta adrese, cik liels ir apakštīkls un pat kontaktinformāciju, kā sadabūt rokā tīkla administratoru. Viens gan, parasti uz atbildi no *WhoIs* serveriem ir nedaudz jāuzgaida.

## 12.3. Ping

„Ping” ir pats parastākais pings. Pingošana notiek no konfigurācijas servera mašīnas. Jānorāda adrese, kuru pingot (*Address:*), skaits (*Count:*) un ja nepieciešams ir iespējams norādīt konkrēti no kuras konfigurācijas servera IP adreses pingošanu izveikt.

#### 12.4. Traceroute

*Traceroute* ir instruments, kas atrod visus rūterus (maršrutētājus) starp konfigurācijas serveri un konkrētu interneta adresi. Ja ir nepieciešams, tad ir iespējams norādīt no kuras konfigurācijas servera adreses (*From IP*) skatīties pēc rūteriem.

Ailītē „*Hops max:*” norāda līdz cik rūteriem izsekot, maksimālā vērtība ir 255.

Ja ir nepieciešams uzzināt rūteriem dotos vārdus, tad aktivizē izvēli „*Resolve host names:*”, šī izvēle prasa lai būtu pieejams DNS serveris.

#### 12.5. ARP

ARP tabula parāda IP adreses un tām atbilstošās makadreses, katrai tīkla kartei uz ugunssienas.

#### 12.6. Process List

Instruments, kas tabulas veidā parāda procesus, kas palaisti uz kādu no ugunssienām.

#### 12.7. Disk space

Parāda ugunssienas cieto disku stāvokli, failu sistēmu, partīcijas izmēru, aizņemto un brīvo vietu un kur partīcija piemontēta.

#### 12.8. Upgrade manager

Šī ir tā vieta, no kuras augšupielādē ugunssienas atjauninājumu failus. Tepat redzami jau augšupielādētie atjauninājumu faili, kā arī iespējams izlasīt aprakstu (*Info*) par konkrēto atjauninājumu vai izdzēst neaktuālu atjauninājumu failu. Sīkāk par ugunssienas atjaunināšanu lasīt nodaļā 9.

#### 12.9. Iekārtu bojājumu noteikšanas sistēma (Host status monitor)

Neviens nevar būt pasargāts no visām problēmām. Bet ja tādas gadās tad labāk par tām uzzināt ātrāk. Šis instruments uzrauga visus konfigurācijas servera hostus, un ziņo ja ir izmaiņas viņu statusā. Par hosta statusa izmaiņām var tik nosūtīta e-pasta vēstule un norādīto adresi. Katram hostam jānorāda uz kādu e-pasta adresi sūtīt statusa ziņojumus.

Tiek uzraudzīts:

- vai hosts ir pieejams,
- tīkla interfeisu status (vai ir fizisks savienojums),
- diska vieta un vai pieejamas visas diska partīcijas.

Pārbaude notiek reizi piecās minūtēs. E-pasta vēstule tiek sūtīta katru reizi kad mainās status. Un reizi diennaktī ja problēma nav novērsta.

Visas statusa izmaiņas tiek rakstītas log failā.

## 13. Noslēgums

Par visiem jautājumiem šīs rokasgrāmatas sakarā lūdzu zvanīt:

Tel. 7807025 vai 9479905

SIA Ugunssiena  
Nometņu iela 21 korpuss 1.  
Rīga

Tehniskais atbalsts \*

tel.: 7807026

tel.: 9151830

e-mail: support@ugunssiena.lv

\* tiek garantēts saskaņā ar apkalpošanas vai garantijas līgumu.

## 14. Pielikumi

### 14.1. VPN tunelis uz Windows 2000/XP

Ugunssienas sistēma nodrošina iespēju izveidot kriptētu VPN tuneli uz Microsoft Windows 2000 un Windows XP sistēmu. Par VPN konfigurēšanu uz ugunssienas skatīt šīs rokasgrāmatas punktā 10.10 - „Virtuālais privātais tīkls (VPN)”.

Lai darbotos automātiskā VPN tuneļu konfigurēšana:

- Windows 2000 sistēmai jāpieinstalē „*IPSEC Policy Configuration Tool*”, to lejupielādēt iespējams Microsoft interneta mājas lapā (<http://www.microsoft.com/downloads/details.aspx?familyid=7d40460c-a069-412e-a015-a2ab904b7361&displaylang=en>).
- Windows XP sistēmai jāpieinstalē „*Windows Support Tools for Microsoft Windows XP Professional*”. Šī instalācijas pakotne atrodama Windows XP instalācijas diskā ([CDROM]:\SUPPORT\TOOLS\SETUP.EXE), Windows XP ar Service Pack 2 gadījumā šos „Support Tools” lejupielādēt no Microsoft mājaslapas (<http://www.microsoft.com/downloads/details.aspx?amp;displaylang=en&familyid=49ae8576-9bb9-4126-9761-ba8011fabf38&displaylang=en>)

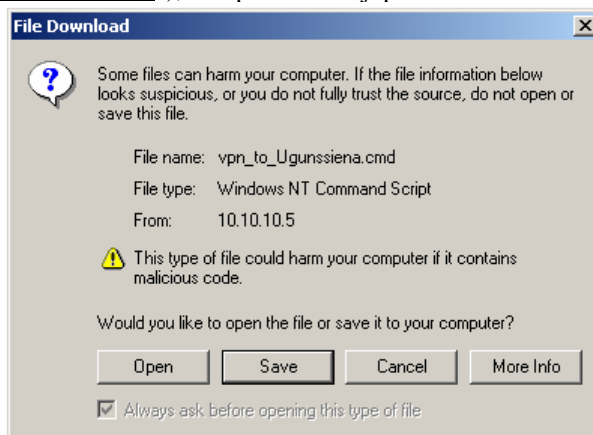
Uz ugunssienas konfigurē VPN tuneli, kā tas aprakstīts šīs rokasgrāmatas punktā 10.10. Konfigurējot, pie „*Tunnel endpoints*” -> „*remote ip*” norāda Windows mašīnas ārējo IP adresi un pie „*Networks*” -> „*remote address*” norāda Windows gala iekšējās adreses.

Veidojot VPN tuneli uz Windows sistēmu pastāv vairāki ierobežojumi. Pie „*IPSEC parameters*” Windows atbalstītie protokoli („*protocol*”) ir „ESP”, kriptēšanas algoritmi („*encryption*”) – „DES” un „3DES”, hash algoritmi – „SH1” un „MD5”, „*psf group*” – „MODP768” un „MODP1024”. Visi šie paši ierobežojumi attiecas arī uz „*IPE proposals*”.

VPN autorizēšanās iespējama divos veidos, ar digitālajiem sertifikātiem („*certificate authorization*”), vai sarunāto atslēgu („*preshared key*”).

- Autorizēšanās ar sarunāto atslēgu („*preshared key*”) – Konfigurējot VPN uz ugunssienas pie „*Configure preshared key*” norāda kaut kādu simbolu virkni, kura tiks izmantota autorizācijas nolūkiem. Saglabā VPN konfigurāciju ar [Save] pogu.
- Autorizēšanās ar digitālajiem sertifikātiem („*certificate authorization*”) – Klikšķina uz saites „*Configure certificate authorization*”. Ielādējas lapa, kurā redzami visi sistēmā pieejamie sertifikāti. Kā pievienot sistēmai sertifikātu skatīt šīs rokasgrāmatas punktā 10.9 – „Sertifikātu serveris (CA)”. Ir divi autorizēšanās modeļi. Atļaut autorizēties tikai ar konkrētu sertifikātu, šādā gadījumā atzīmē vēlamo sertifikātu un spiež pogu [Add as trusted certificates]. Otrs modelis ir atļaut autorizēties ar jebkuru sertifikātu, kurš parakstīts ar norādīto. Tādā gadījumā atzīmē sertifikātu un spiež pogu [Add as trusted signers]. Lai arī kāds sertifikātu autorizācijas modelis tiktu izvēlēts, lai autorizācija būtu iespējama, Windows sistēmai ir jābūt ieinstalētiem visiem sertifikātiem līdz pirmajam izdevējam („*root certificate*”).

Automātiskās konfigurācijas faili Windows sistēmām pieejami ugunssienas VPN konfigurācijas lapas apakšā. Klikšķinot uz operētājsistēmai atbilstošās saites („*Download configuration for Windows XP*” vai „*Download configuration for Windows 2000*”), tiek piedāvāts lejupielādēt Windows izpildāmu failu.



To var tūlīt palaist klikšķinot uz pogas [Open], vai saglabāt uz diska, lai palaistu vēlāk. Palaižot šo failu, automātiski tiks sakonfigurēts Windows IPSEC klients un nodibināts VPN tunelis uz ugunssienu.

## 14.2. Glosārijs

Ugunssienas izstrādāto sistēmu aprakstā tiek izmantoti virkne latviešu valodas termini, kuru tulkojums no angļu valodas uz latviešu valodu ir salīdzinoši mazpazīstams vai neierasts. Šis glosārijs ir domāts Ugunssienas produktu (US) lietotājiem vai interesentiem, un mēs ceram, ka tas varētu atvieglot mūsu piedāvāto tīkla drošības risinājumu izpratni.

- Lietotājs** (*User*) – persona, kurai ir reģistrēti lietotāja vārds, parole un personas dati US sistēmā
- Ugunssienu** – dators ar uzstādītu SIA Ugunssienu produktu.
- Hostdators** (*Host*) – dators, uz kura darbojas US produkti
- Tīkls** (*Network*) – vienā tīklā savienota datoru grupa
- Tīkla interfeiss** (*Network Interface*) – hostdatora pieslēgums tīklam (fiziskā vai virtuālā tīkla karte)
- IP maršrutētājs** (*IP Router*) – IP pakešu maršruta izvēles funkcija
- Pakešu filtrs** (*Packet Filter*) – pakešu filtrēšanas funkcija
- Tīkla adrešu translācija** (*Network Address Translation (NAT)*) – tīkla adrešu translācijas funkcija
- Virtuālais privātais tīkls** (*VPN*) – funkcija, kas nodrošina virtuālu šifrētu savienojumu (tuneli) starp diviem hostdatoriem, izmantojot citu tīklu
- Domēns** (*Domain*) – vārds, ko izmanto, lai identificētu tīkla adrešu kopu atbilstoši Interneta tīklā pieņemtajiem standartiem (RFC)
- IP adrese** – cipariska Interneta tīkla adrese (RFC)
- Tīkla maska** (*Netmask*) – cipariskās IP adreses maska (RFC)
- Vārteja** (*Gateway*) – IP adrese, uz kuru tiek pārsūtītas uzdotajam kritērijam atbilstošas datu paketes
- Serviss** (*Service*) – datu pakešu apmaiņas noteikumu kopums konkrētam pielietojumam, TCP/IP pielietojumu protokolu kopa (ftp, http, pop3 u.c.)
- Protokols** (*Protocol*) – jebkurš protokols atbilstoši OSI level 3 vai 4 standartam
- Ports** (*Port*) – servisa identifikācijas numurs protokolā (RFC)
- IP adrešu grupa** – ar vārdisku identifikatoru apzīmēts IP adrešu vai IP adrešu apgabalu kopums US sistēmā
- E-pasta starpniekserveris** (*e-mail proxy*) – E-pasta starpniekservera funkcija

\*\*\*

Glosārijā izmantoti šādi starptautisko standartu saīsinājumi:

**RFC** (*Request for Comments*) - dokumentu sērija, kas apraksta Interneta standartus un protokolus, ko publicē starptautiska organizācija *Internet Engineering Task Force* (IETF - sk. mājas lapu <http://www.ietf.org/>). Īsumā galvenie protokoli ir šādi:

- POP** (*Post Office Protocol*) - serveris e-pasta lasīšanai, arī *POP3* protokols
- SMTP** (*Simple Mail Transfer Protocol*) - serveris e-pasta sūtīšanai
- HTTP** (*Hyper Text Transport Protocol*) - WEB protokols, URL sastāvdaļa
- DNS** (*Domain Name Server*) - Jūsu Internet domēnu adrešu serveris
- TELNET** (*Telnet Protocol*) - termināla pieejas protokols
- FTP** (*File Transfer Protocol*) - failu pārsūtīšanas protokols
- ICMP** (*Internet Control Message Protocol*) - Interneta kontroles paziņojuma protokols
- IGMP** (*Internet Group Management Protocol*) - Interneta grupu vadības protokols
- TCP** (*Transmission Control Protocol*) - no hostdatora uz hostdatoru
- UDP** (*User Datagram Protocol*) - lietotāju datu kadru protokols
- IP** (*Internet Protocol*) - Interneta protokols
- SNMP** (*Simple Network Management Protocol*) - tīkla vadības protokols
- OSPF** (*Open Shortest Path First Protocol*) - īsākā ceļa maršrutēšanas protokols
- RIP** (*Routing Information Protocol*) - maršrutēšanas protokols
- ARP** (*Address Resolution Protocol*) - adreses noskaidrošanas protokols
- EGP** (*Exterior Gateway Protocol*) - ārējās vārtejas maršrutēšanas protokols
- DES** (*Unclassified Data Encryption Protocol*) - standarta datu šifrēšanas protokols
- RSA** (*RSA encryption*) - Patentēts publiskās atslēgšifrēšanas algoritms, ko izstrādājuši RSA Data Security
- SSL** (*Secure Sockets Layer*) - WEB sūtījumu šifrēšanas protokols
- IMAP** (*Internet Mail Access Protocol*) - vēlāks papildinājums *POP3* protokolam
- SSH** (*Secure Shell Protocol*) - drošās čaulas protokols, ko izmanto šifrētai pieteikšanās (*login*) procedūrai
- OSI** (*Open System Interconnection*) - tīklu savienojumu standartu modelis sadalījumam pēc pielietojuma līmeņiem (sīkākai informācijai sk. labu atsauces materiālu - <http://www.arnatech.com/cons5.html>). Īsumā šie līmeņi ir šādi:
  - OSI level 1** – fiziskais līmenis (interfeisa karte datora ligzdā)
  - OSI level 2** – datu savienojuma līmenis - Ethernet vai TokenRing (CSMA/CD, fizisko mēdiņu pieejas metode, pakešu kadra (*frame*) formāts).

**OSI level 3** – tīkla līmenis - datu pakešu maršrutējamie protokoli starp *software* adresēm, no tīkla uz tīklu savienojumi (TCP/IP, kā arī ražotāju specifiskie Novell IPX, IBM SNA, Apple AppleTalk u.c.)

**OSI level 4** – transporta jeb nogādes līmenis - sadala datus pa paketēm/savāc kopā galapunktā

**OSI level 5** - sesijas līmenis - kontrolē iepakojumu, piemēram, nodrošina kļūdu kontroli

**OSI level 6** - prezentācijas līmenis - veic faila vai parolu sūtīšanu, kriptēšanu, dekriptēšanu, datu formātu konversiju.

**OSI level 7** - aplikācijas līmenis - lietotāju interfeiss (teksts/grafika, e-pasta interfeiss)