

## BlueTeam 2 Ohje

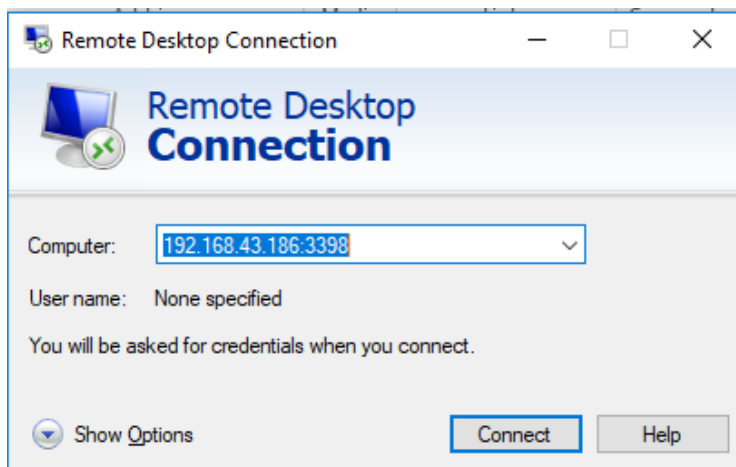
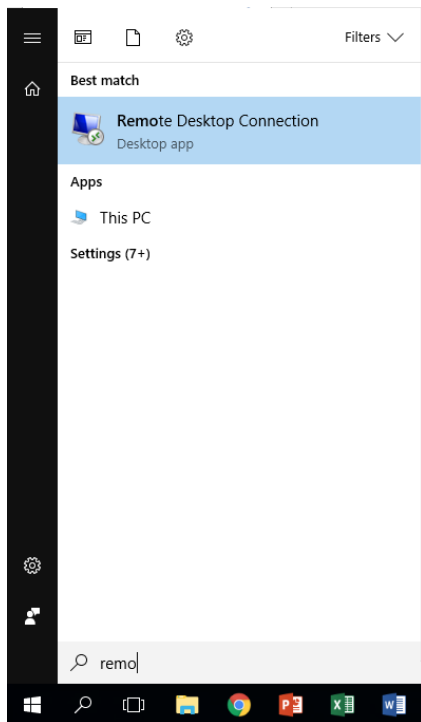
### Viestintä

Liittyy blue tiimin Mattermostiin osoitteessa mattermost.masiina.com (Tunnus:blueteam2 salasana: blueteam2). Liittyy blue team private channeliin.

### Etäyhteys

Harjoittelevat joukot ottavat etäyöpöytäyhteyden tiettyyn IP-osoitteeseen ja porttiin. Älkää kokeilko muita portteja. **IP-osoite ilmoitetaan ennen pelin alkua.**

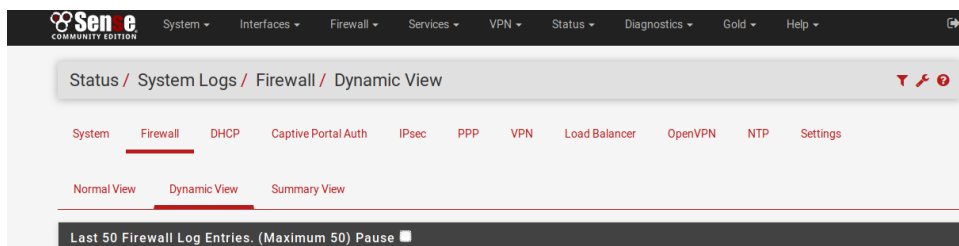
Remote Host Name	Käyttö	Port
Masiina Workstation	Palomuurin hallinta	3398
BT2 Mattermost	Mattermost / tiketinhallinta	3416



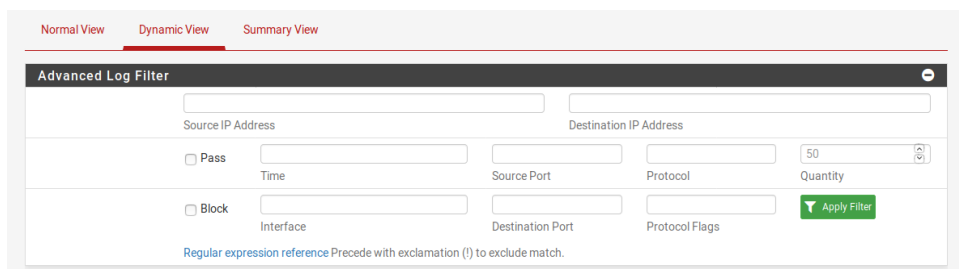
## Palomuuuri

Palomuuuriin päästään palomuuuri koneelta kiinni selaimesta IP-osoitteesta 192.168.1.1 ja kirjautumalla tunnuksilla admin/pfsense

PFSense palomuuria kannattaa katsoa Dynamic View – tilassa, jossa näkee uusimmat tapahtumat. Tilana pääsee valitsemalla ylhäältä valikosta Status -> System Logs -> Firewall -> Dynamic View



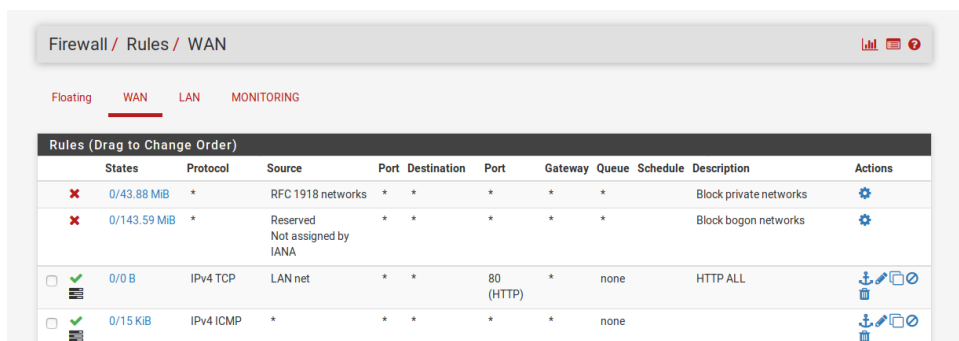
Kyseistä tilaa voi suodattaa, esimerkiksi jos haluaa nähdä vain tietystä IP-osoitteesta lokeja. Suodattimeen pääsee klikkaamalla suppilon kuvaa oikeasta yläreunasta.



Lokista voi myös lisätä helposti sääntöjä, joilla estää tai sallia liikenne. Tämä onnistuu, kun painaa osoitteen vieressä olevaa laatikkoa.

✗	Nov 16 13:45:47	► LAN	Easy Rule: Add to Block List	192.168.1.1	ICMPv6
✓	Nov 16 13:45:48	WAN	194.154.65.11:54734	192.168.2.20:8888	TCP:S

Palomuuuriin voi lisätä sääntöjä Firewall -> Rules valikosta. Rajapinta valitaan sen mukaan, halutaanko estää liikenne ulkoisesta tai sisäverkosta.



Uuden säännön voi lisätä alhaalta Add – painikkeesta. Action kohdasta määritetään, halutaanko säännöllä estää vai sallia liikenne. Protocol kohdasta valitaan, mitä protokollaa liikenne noudattaa. Jos halutaan esim. Estää yksi osoite, laitetaan Source kohtaan Single host or alias valikosta ja kirjoitetaan seuraavaan kenttään IP-osoite.

Edit Firewall Rule	
<b>Action</b>	<div>Block</div> <p>Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.</p>
<b>Disabled</b>	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
<b>Interface</b>	<div>WAN</div> <p>Choose the interface from which packets must come to match this rule.</p>
<b>Address Family</b>	<div>IPv4</div> <p>Select the Internet Protocol version this rule applies to.</p>
<b>Protocol</b>	<div>TCP</div> <p>Choose which IP protocol this rule should match.</p>
Source	
<b>Source</b>	<input type="checkbox"/> Invert match. <div>Single host or alias</div> <div>193.52.231.125 / </div>
<b>Display Advanced</b>	<input checked="" type="button" value="Display Advanced"/>
Destination	

## Työtehtävä

- Seurata tikettijärjestelmää
- Tiketeissä määritellyn ongelman mukaan tehdä palomuuuri asetukset sekä muut tekniset toimenpiteet häiriötilanteissa
- Kaikista tehdyistä muutoksista täytyy tehdä tiketti (esim. Palomuurista estetty x.x.x.x - osoite)
- Lisätietoja tiketeistä voidaan kysellä Blue Team ykköseltä Mattermostissa.
- Blue tiimien johtajan (eli Masiinan toimitusjohtajan) tehtävänä seurata twitter.fi sekä iltajutku.fi sivustoja uusien tapahtumien varalta ja varmistaa yrityksen toiminnan jatkuvuus.
- Jos palomuurissa aiotaan estää liikenne jostain osoitteesta, siihen täytyy kysyä Masiinan toimitusjohtajalta lupa.
- Operaattorilta voi kysyä lisätietoa tuntemattomista IP-osoitteista Mattermostissa.
- Jos hissi ei lähetä dataa valvomoon, selvitä hissin IP, pingaa osoitteeseen. Jos ei vastaa, ota yhteyttä huoltomiehiin Huolto - kanavassa Mattermostissa.
- Virhetilanteissa yhteys huoltomieheen.

## HTTP-sivustot

Sivusto	Käyttö	Tunnus / Salasana
Masiina.com	Masiinan kotisivut	-
Iltajutku.fi	Iltapäivälehti	-
Twitter.fi	Sosiaalinen media	-
Operaattori.fi	Operaattorin sivustot	-
Support.masiina.com Huom! Admin käyttäjä	Tikettijärjestelmä	masiina/root66
Mattermost.masiina.com	Viestintäkanava	blueteam2/blueteam2

## Tikettijärjestelmä

Tikettijärjestelmään päästään kirjautumaan admin käyttäjällä painamalla Sign In - sivulta "I'm an agent – sign in here" kohdasta johon sitten syöttämällä tiedot päästään sisään. Tunnukset masiina/root66

**SUPPORT CENTER**  
Support Ticket System


Guest User | [Sign In](#)

[Support Center Home](#) [Open a New Ticket](#) [Check Ticket Status](#)


**Sign in to Masiina Support**

To better serve you, we encourage our Clients to register for an account.

Not yet registered? [Create an account](#)  
**I'm an agent – [sign in here](#)**



Tickets-välilehden alta löytyy kaikki tehdyt tiketit



Welcome, **Masiina**. | [Admin Panel](#) | [My Preferences](#) | [Log Out](#)

[Dashboard](#)
[Users](#)
[Tickets](#)
[Knowledgebase](#)

[Open \(1\)](#)
[Closed \(5\)](#)
[New Ticket](#)

[\[advanced\]](#)

[Open Tickets](#) — Showing 1 - 1 of 1


	Ticket	Date	Subject	From	Priority	Assigned To
<input type="checkbox"/>	<a href="#">910620</a>	11/16/2017 6:18 am	MIKÄÄN EI TOIMI	blueteam1	Normal	

Select: [All](#) [None](#) [Toggle](#)

Page: **[1]** [Export](#)

Copyright © 2006-2017 Masiina Support All Rights Reserved.

Kun tiketti on avattu voidaan sieltä antaa kommenttia tilanteesta sekä voidaan muuttaa tiketin tilaa yms. Huom! Admin käyttäjällä ei poisteta tikettejä



[Dashboard](#)
[Users](#)
[Tickets](#)
[Knowledgebase](#)

[Open \(1\)](#)
[Closed \(5\)](#)
[New Ticket](#)

[Ticket #910620](#)

<b>Status:</b> Open	<b>User:</b> <a href="#">blueteam1 (4)</a>
<b>Priority:</b> Normal	<b>Email:</b> blueteam1@masiina.com
<b>Department:</b> Support	<b>Phone:</b>
<b>Create Date:</b> 11/16/2017 6:18 am	<b>Source:</b> Web (62.106.8.5)

<b>Assigned To:</b> — Unassigned —	<b>Help Topic:</b> Report a Problem
<b>SLA Plan:</b> Default SLA	<b>Last Message:</b> 11/16/2017 6:18 am
<b>Due Date:</b> 11/18/2017 6:18 am	<b>Last Response:</b>

**MIKÄÄN EI TOIMI**

<b>11/16/2017 6:18 am</b>	blueteam1
EI TOIMI	

[Post Reply](#)
[Post Internal Note](#)
[Department Transfer](#)
[Assign Ticket](#)

**To:**

**Collaborators:** [Add Recipients](#)

**Response:**

<>

Start writing your response here. Use canned responses from the drop-down above