

pfsense firewall



מבוא

בתחילת עידן המחשבים מידע בין מחשבים הועבר באמצעים פיזיים שהועברו ביניהם. תקשורת מחשבים נועדה בכדי להימנע מהעברת מידע באמצעים הפיזיים ולבצע העברת מידע באמצעות תווך תקשורת כל שהוא (כבלים קואקסיאליים, סיבים אופטיים וכו'). רשתות מחשבים נפוצות כיום בכל העולם והמוכרת בהם היא רשת האינטרנט. רשת מחשבים משמשת להעברת מידע, אחסון קבצים, שיתוף קבצים, עבודה משותפת על מסמכים, הדפסה וכו'.

קיימות מספר רשתות:
LAN- רשת מקומית. מתפרשת על אזורים קטנים כמו בית ספר, משרד וכו'. קיים סמיכות של רכיבי המחשוב אחד לשני.
WAN-רשת רחבה. מתפרשת על אזורים גדולים כמו סניפים של ארגון, שימוש של צרכנים (בנקים חנויות וכו'). משמשת לחיבור בין רשתות מקומיות. אשר מורכבת ממספר רשתות LAN ומקשרת בניהן.
לצורך הגנה על המידע ואופן העברתו בתוך הרשת ובין רשתות שונות הקימו תוכנות שיסייעו לכך, אחת מהן היא מערכת ה FIREWALL.

בעבודה זו נתמקד ב.Pfsense FireWall

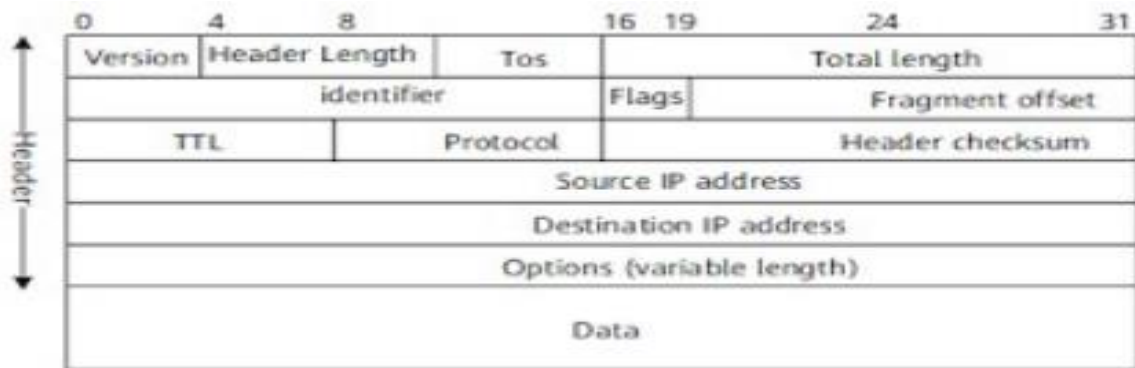
אופן העברת הנתונים:

קיימים מספר מודלים להעברת נתונים בתוך רשתות, אחד מהם הוא מודל OSI המתאר את אופן העברה באמצעות 7 שכבות.



העברת המידע מתבצעת באמצעות חבילת מידע (פאקט) המועברת ברשת ממקום למקום. היא מורכבת מ header and payload מתייחס ליחידת מידע בשכבה השלישית, שכבת רשת.

header - פורט הוא נשלח, מהו באיזה, המעידים על מקור שליחת הפאקט יופיעו נתונים יעדו של הפאקט ואיזה פורט הוא נשלח.
payload - החלק בפאקט שבו מועבר המידע.



כמו כן ישנן שכבות נוספות הרלוונטיות במודול זה עבור FIREWALL הם: השכבה הפיזית (physical) - תפקידה של שכבה זו הוא להעביר את הביטים מנקודה אחת לנקודה שניה באמצעות 0 או 1. מייצגת את הפעולות הרכיבים הפיזיים שלוקחים חלק בתהליך התקשורת.

שכבת הקו (Data link) - אחראית על מעבר הסיביות בין שתי תחנות של הרשת. שכבת הקו אחראית על העברת המידע.

נהוג לחלק את שכבה זו לשני שכבות:

llc (logical link control) - מהשכבות העליוניות אחראית על חלוקת הנתונים שמגיעים למסגרות, ועל טיפול בכל מסגרת בנפרד, מקשרת בין שכבת הקו לשכבת הרשת.
mac ((media access control address) ה mac - מזהה ייחודי המוטבע על כל רכיב תקשורת בעת הייצור ואינה ניתנת לשינוי.

שכבת הרשת (Network) - מאפשרת תקשורת באמצעות כתובות IP ומכאן היא גם מאפשרת ניתוב התקשורת ע"פ האינטרנט. בשכבה זו מתבצעות כל ההחלטות הנוגעות לדרך בה יועברו הנתונים על גבי הרשת, היא זו שתקבע האם קיים קשר בין המקור ליעד.

מה זה FIREWALL?

מערכת להפרדת אזורים ברשת ובין רשתות שונות, ניטור וחסומה של תקשורות בלתי רצויות בכדי לסנן את המידע הנכנס והיוצא מהמחשבים דרך האינטרנט. ניתן להשתמש במערכת בתור משתמש פרטי וגם בתור ארגון גדול.

תפקידה היעודי של חומת האש לנהל בקרת גישה, לשלוט על תעבורה יוצאת ונכנסת. בקרת גישה הינו סדר חוקים אשר נקבע עפ"י צרכי המערכת לאילו גורמים מותר להגיע למקומות מסוימים ברשת, קביעת שימוש בפרוטוקולים שונים.

במידה ותגיע לחומת האש פאקטה שאינה עומדת בתנאי המעבר היא תיחסם וימנע ממנה כניסה/יציאה לרשת המחשבים ולרשת הפרטית.

רשימת החוקים שמוגדרת תבדוק כל פאקטה שמנסה לצאת או להיכנס מרשת אחת לאחרת נבדקת ומוחל עליה החוק הראשון

החוקים בחומת האש מתבצעים באמצעות שיטת white list משמע אנו קובעים אילו תקשורות אנו מאפשרים ברשת שלנו, במידה ולא הגדרנו חוק המאפשר פעולה כל שהיא ברשת ישנו חוק (שלא נראה ויזואלית) שנקרא implicit deny שאומר כי הכל מהכל חסום והוא נמצא בתחתית טבלת החוקים וזאת מכיוון שחומת האש עובדת לפי first match.

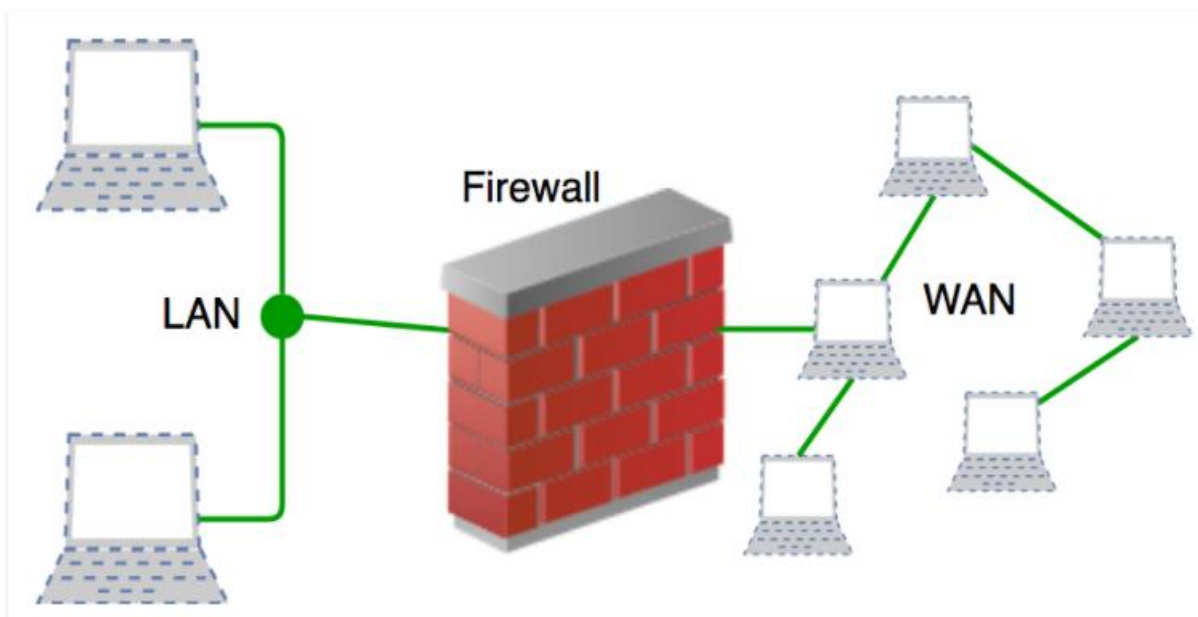
כאשר מתקבלת בקשה מתבצעת בדיקה בחוקים שהגדרנו העובדת לפי סדר מלמעלה למטה כאשר אין חוק המאשר את הבקשה שהתקבלה הבקשה תיתקל בחוק האחרון implicit deny והבקשה תדחה.

חוק זה קיים על מנת לכסות את כל אפשרויות שלא ניתנות לפניה ע"י מנהל חומת האש.

חומת האש מסתכל על צד הHEADER בפאקט ועפ"י קריאה של הנתונים כגון SRC,DST,SERVICE

חומת האש יכולה לזהות כאשר משתמש הוציא syn ואז לאפשר לקבל חזרה syn ack חזרה.

אם לא נראה כי יצא syn ורק יתקבל syn ack לפיירוול אז הפאקטה לא תעבור ותדחה מצב זה נקרא statefull inspection.



תוכן עניינים










2 - 4	תקציר
6-14	התקנת המערכת
	<u>תפריט מערכת</u>
15-19	SYSTEM
20	INTERFACES
21-24	FIREWALL
25-26	SERVICES
27	VPN
28	STATUS
29-33	DIAGNOSTICS

PFSense FIREWALL

מדובר על open source FIREWALL בנוי על מערכת הפעלה מסוג FreeBSD. ל-FIREWALL זה יש יכולות נוספות כגון IDS\IPS, DLP, VPN ועוד.

התקנה, הקצאת משאבים וחלוקה לרשתות :

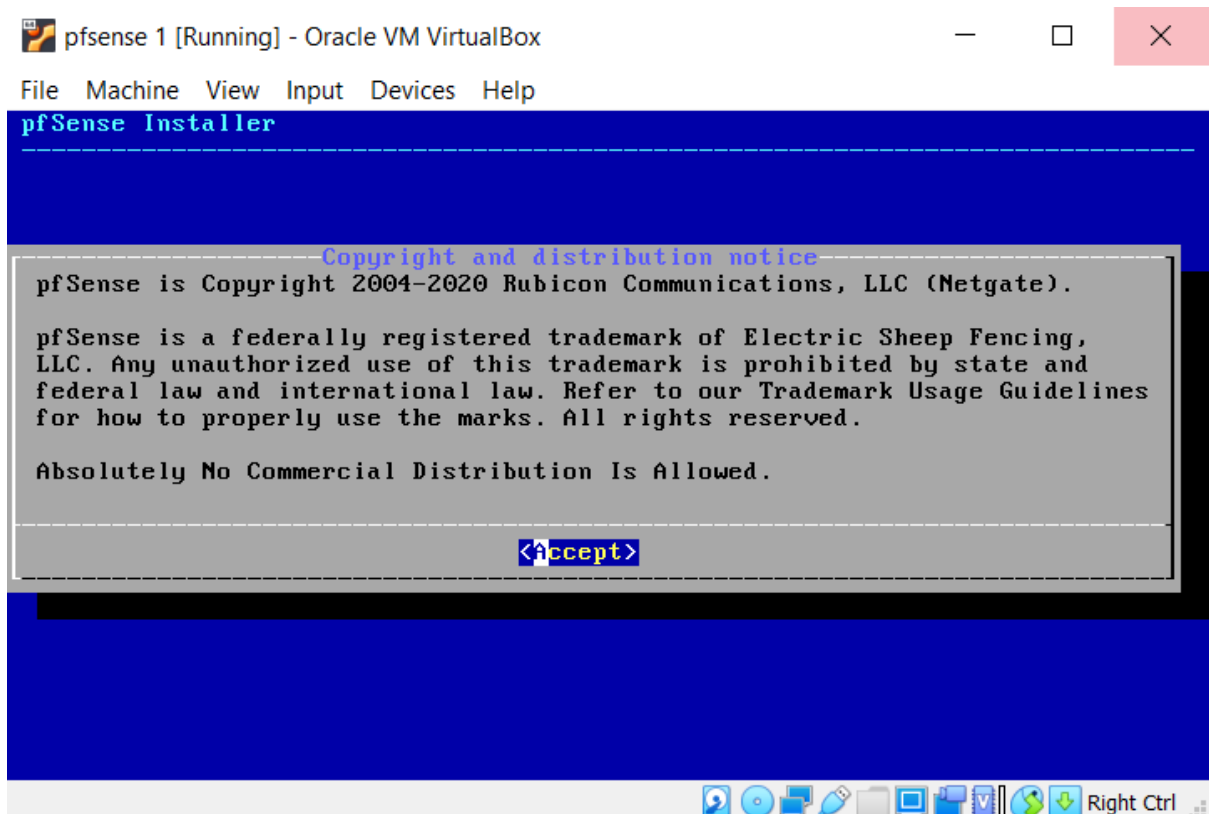
ההתקנה תתבצע בהתאם לצורך שלי ושל הארגון שלי.
משאבים שהוקצו ב-oracle virtualbox לצורך התקנת ה-FW:

	General
Name:	pfsense
Operating System:	Ubuntu (64-bit)
	System
Base Memory:	2048 MB
Boot Order:	Floppy, Optical, Hard Disk
Acceleration:	VT-x/AMD-V, Nested Paging, KVM Paravirtualization
	Display
Video Memory:	16 MB
Graphics Controller:	VMSVGA
Remote Desktop Server:	Disabled
Recording:	Disabled
	Storage
Controller:	IDE
IDE Secondary Master:	[Optical Drive] pfSense-CE-2.4.5-RELEASE-p1-amd64.iso (717.65 MB)
Controller:	SATA
SATA Port 0:	pfsense.vdi (Normal, 50.00 GB)
	Audio
Host Driver:	Windows DirectSound
Controller:	ICH AC97
	Network
Adapter 1:	Intel PRO/1000 MT Desktop (Bridged Adapter, Realtek PCIe GbE Family Controller)
Adapter 2:	Intel PRO/1000 MT Desktop (Internal Network, 'LAN')
Adapter 3:	Intel PRO/1000 MT Desktop (Internal Network, 'SERVERS')
Adapter 4:	Intel PRO/1000 MT Desktop (Internal Network, 'DMZ')
	USB
USB Controller:	OHCI
Device Filters:	0 (0 active)
	Shared folders
	None
	Description
	None

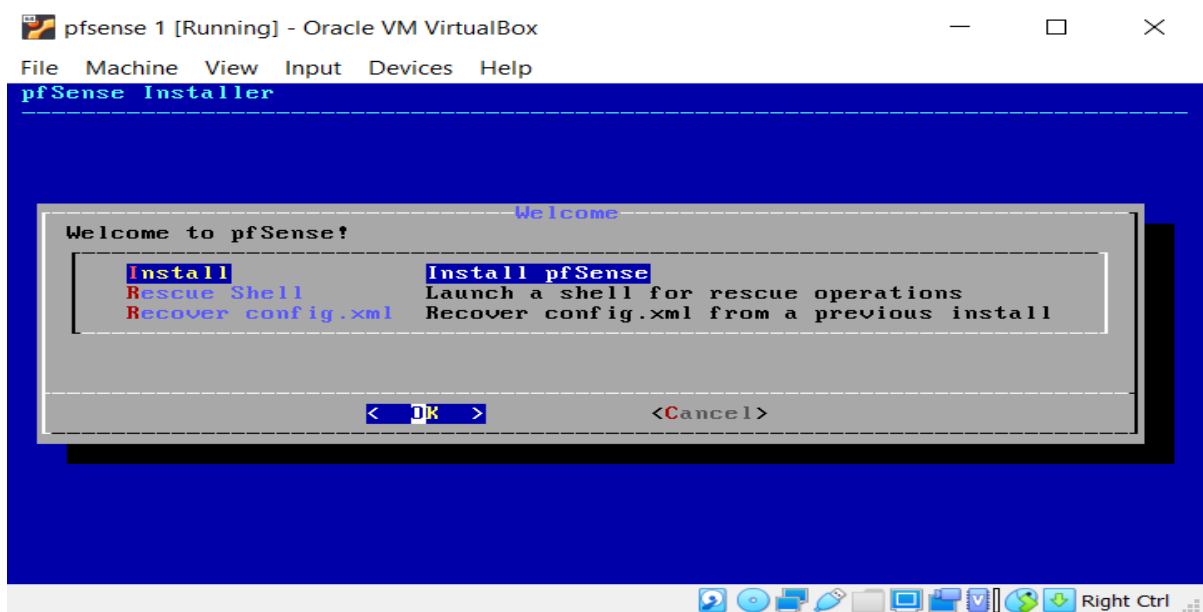
כרטיס 1 : מוגדר כ- BRIDGED ADAPTER המערכת הוירטואלית חולקת את אותו כרטיס רשת עם מערכת ההפעלה.

שאר הכרטיסים : מוגדרים כ- INTERNAL NETWORK המערכות הוירטואליות תקבל כרטיס רשת וירטואלי ואת כתובות ה IP תקבל באופן אוט' במידה וישנו DHCP על המחשב במידה ואין תקבל כתובת סטטית.

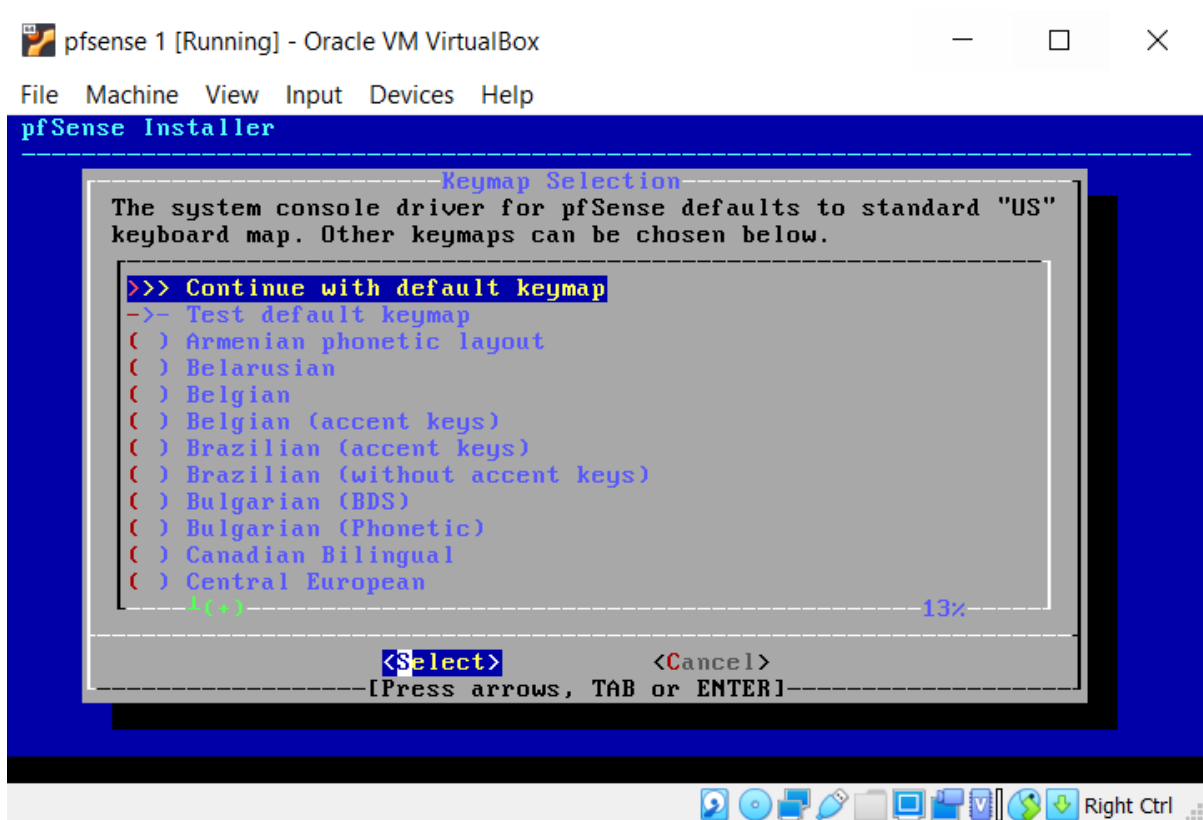
לאחר שבחרנו רשתות והקצנו משאבים נטעין את קובץ ה ISO ונתחיל בהתקנה.



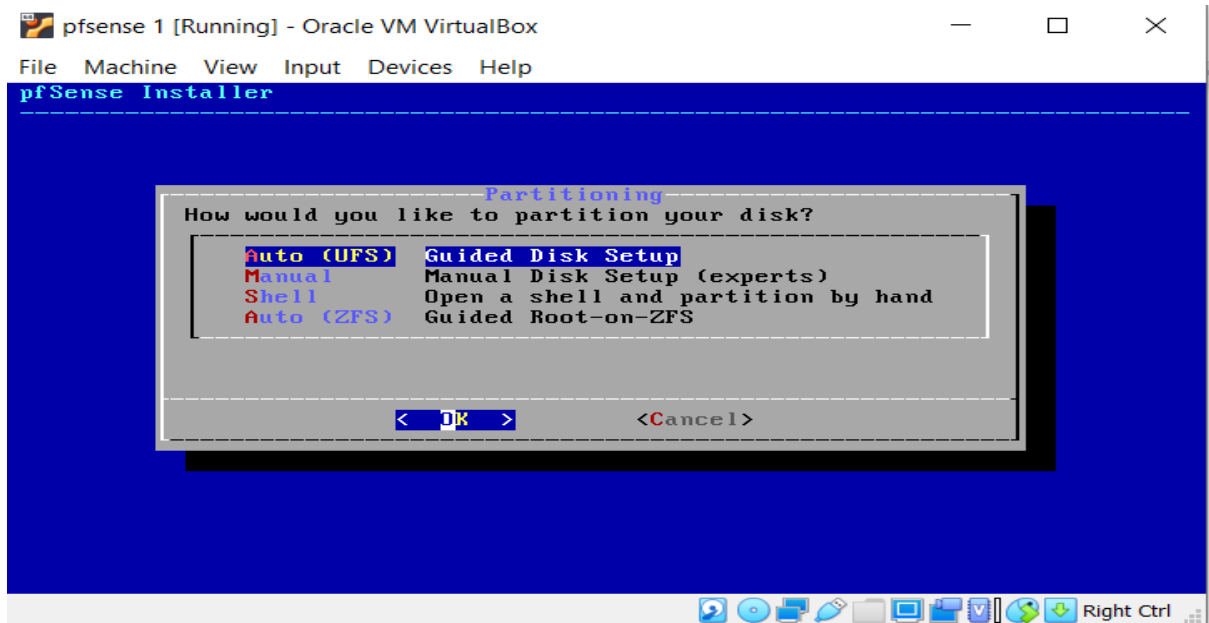
ok



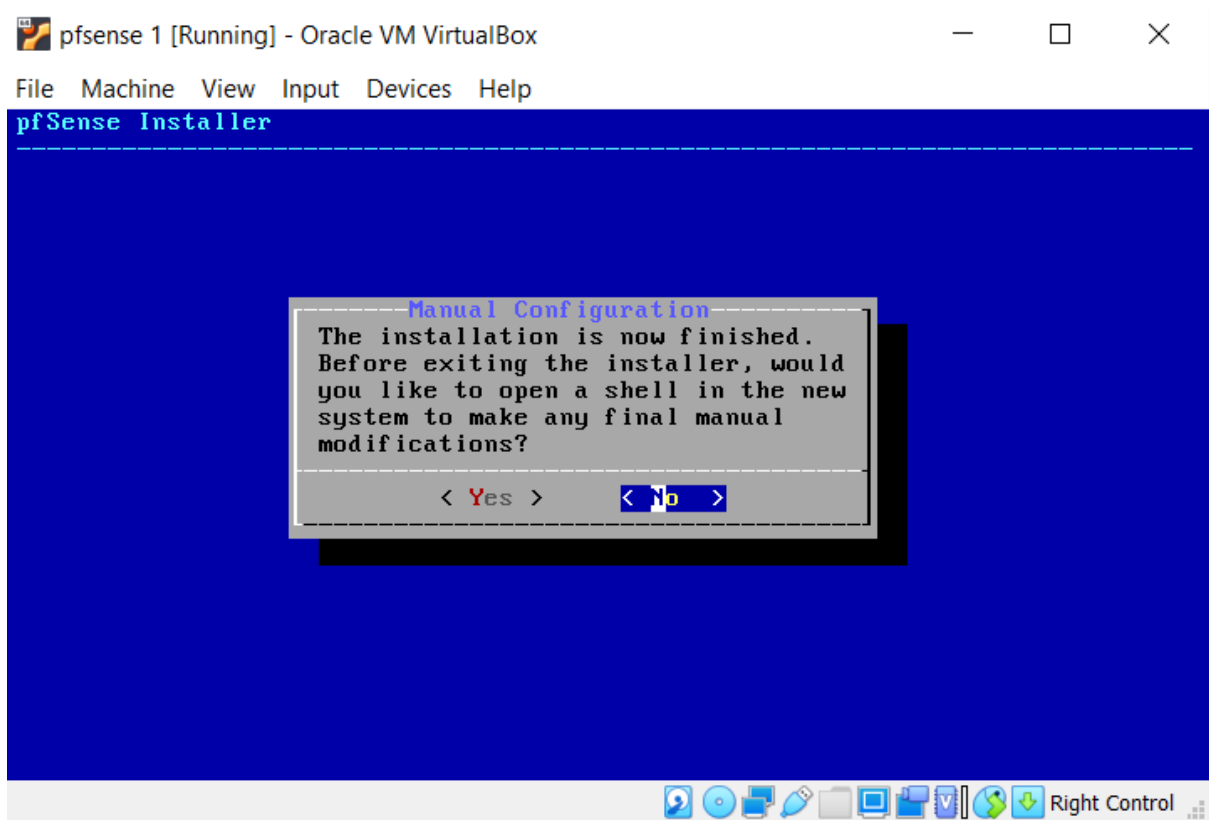
continue with default keymap
select



ok

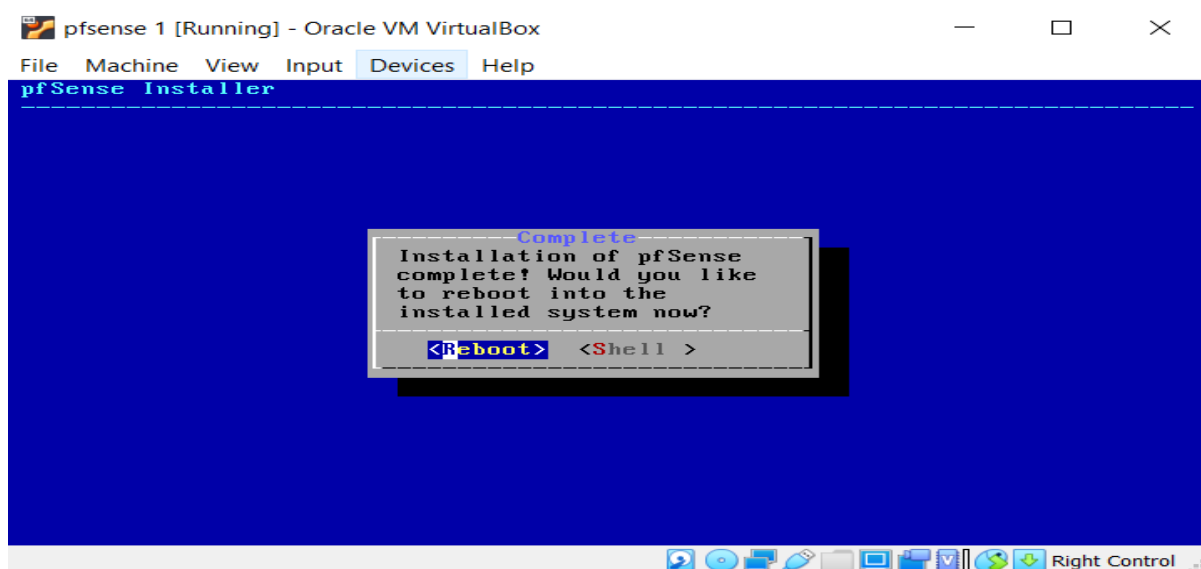


לאחר סיום ההתקנה נלחץ על NO כיוון שאין צורך בפתיחת SHELL

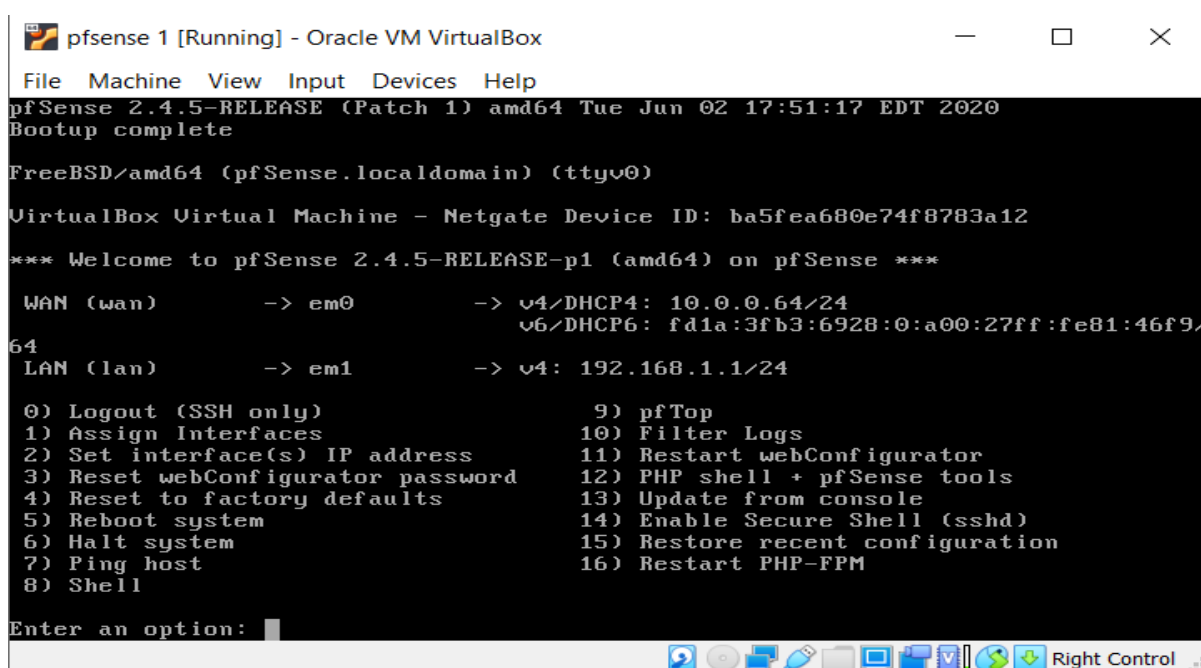


נוציא את הדיסק ובבחר ב REBOOT מכיוון שאם לא נעשה זאת הדיסק יעלה בשנית כהתקנה.

נלחץ מקש ימני על הדיסק נלחץ על remove disk from virtual drive לאחר מכן force unmount ולבסוף נלחץ על reboot .



מסך הפתיחה



נתחבר לכתובת wan שקיבלנו 10.0.0.64 בכדי לגשת לממשק הניהול ומתן המשך הגדרות למערכת אך לא לפני שנשבית את המערכת זמנית זאת מכיוון שחומת האש חוסמת באופן אוטומטית גישה לממשק הניהול. נבצע זאת באמצעות פקודה pfctl -d

```
pfSense 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
exit
VirtualBox Virtual Machine - Netgate Device ID: ba5fea680e74f8783a12
*** Welcome to pfSense 2.4.5-RELEASE-p1 (amd64) on pfSense ***

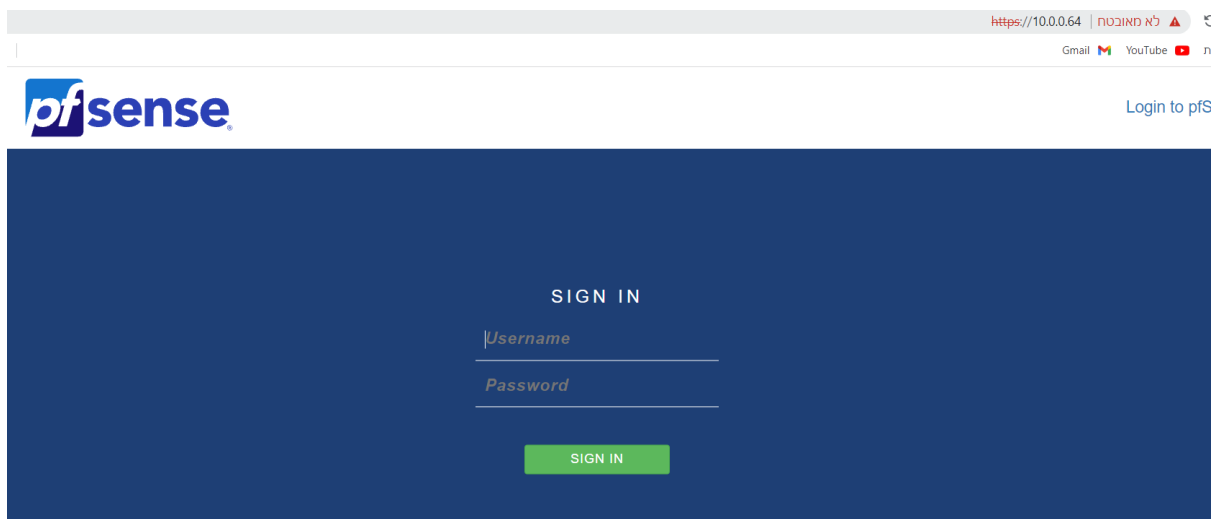
WAN (wan)      -> em0      -> v4/DHCP4: 10.0.0.64/24
                v6/DHCP6: fd1a:3fb3:6928:0:a00:27ff:fe81:46f9/64
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell


Enter an option: 8

[2.4.5-RELEASE][root@pfSense.localdomain]/root: pfctl -d
pf disabled
[2.4.5-RELEASE][root@pfSense.localdomain]/root: 
```

לאחר שביצענו זאת נוכל לגשת לממשק הניהול.



שם משתמש : admin



System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Wizard / pfSense Setup /

Step 1

pfSense Setup

Welcome to pfSense® software!

This wizard will provide guidance through the initial configuration of pfSense.

The wizard may be stopped at any time by clicking the logo image at the top of the screen.

pfSense® software is developed and maintained by Netgate®

Learn more

Next

נבחר ב 8.8.8.8 (גוגל) בכדי שמערכת תדע איך לתרגם כתובות רשת.

General Information

On this screen the general pfSense parameters will be set.

Hostname

pfSense

EXAMPLE: myserver

Domain

localdomain

EXAMPLE: mydomain.com

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

Primary DNS Server

8.8.8.8

Secondary DNS Server

Override DNS

☒

Allow DNS servers to be overridden by DHCP/PPP on WAN

נוריד את ה ✓ מכיוון שאם נשאיר אותם תיחסם הגישה לכתובות הפרטיות שמגיעות מה wan . הביטול נעשה מכיוון שאנו בסביבת מעבדה ובמעבדה כתובת ה wan שלנו היא באותו BD של הכתובת הפרטית במחשב.

RFC1918 Networks

Block RFC1918 Private Networks

☐ Block private networks from entering via WAN

When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.

Block bogon networks

Block bogon networks

☐ Block non-Internet routed networks from entering via WAN

When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets received.

» Next

נקצה כתובת LAN

Configure LAN Interface

On this screen the Local Area Network information will be configured.

LAN IP Address

192.168.1.1

Type dhcp if this interface uses DHCP to obtain its IP address.

Subnet Mask

24

» Next

Wizard / pfSense Setup / Wizard completed. ?

Step 9 of 9

Wizard completed.

Congratulations! pfSense is now configured.

We recommend that you check to see if there are any software updates available. Keeping your software up to date is one of the most important things you can do to maintain the security of your network.

[Check for updates](#)

Remember, we're here to help.

[Click here](#) to learn about Netgate 24/7/365 support services.

User survey

Please help all the people involved in improving and expanding pfSense software by taking a moment to answer this short survey (all answers are anonymous)

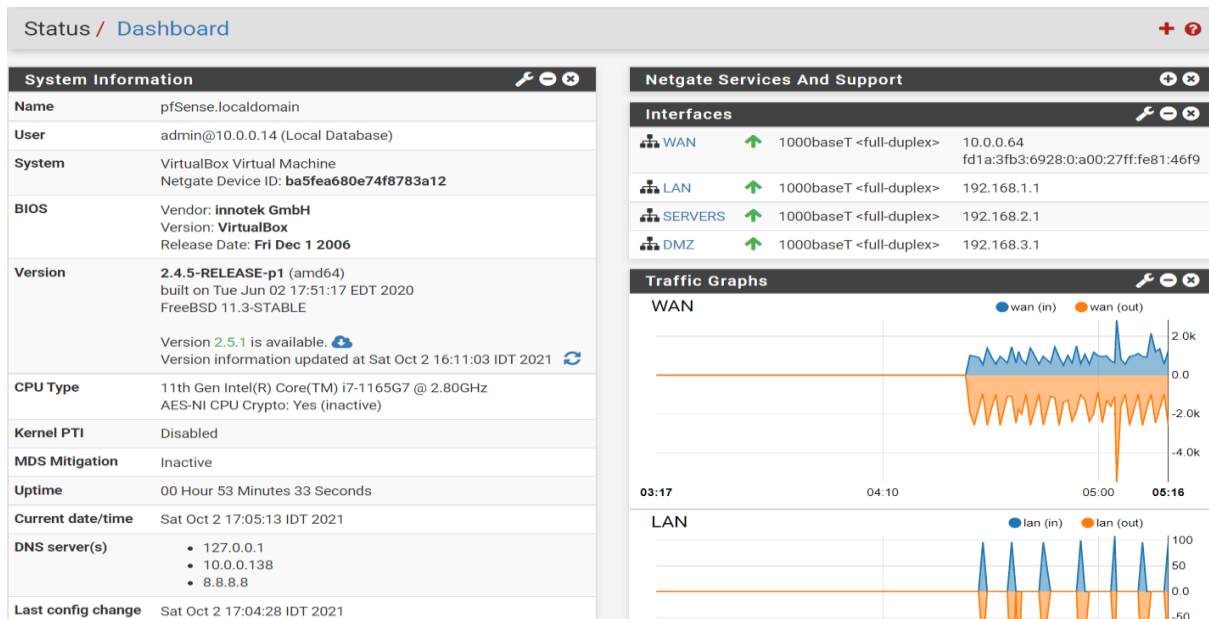
[Anonymous User Survey](#)

Useful resources.

- Learn more about Netgate's product line, services, and pfSense software from our [website](#)
- To learn about Netgate appliances and other offers, [visit our store](#)
- Become part of the pfSense community. Visit our [forum](#)
- Subscribe to our [newsletter](#) for ongoing product information, software announcements and special offers.

[Finish](#)

במסך הראשי נוכל להבחין בפרטי המערכת, סוג גירסא, כתובת די אנ אס, אחוז הניצול של המשאבים וכן בכרטיסי הרשת כתובות.



תפריטי המערכת:

system - מכיל אפשרויות רבות בעלות אופי מתקדם אפשרויות אלה מתאימות את התנהגות חומת האש לסביבות מורכבות יותר.

advanced

admin access

קביעת אפשרויות שונות לניהול חומת האש, שימוש בפרוטוקולי התחברות לממשק (HTTP/HTTPS), ניתן להגדיר חיבור בSSH על מנת להתחבר לחומת האש ולנהל אותה מרחוק.

firewall and nat

ניתן להשבית את חומת האש על מנת שלא יתבצע ניתוח של תעבורת רשת. שימוש בפונקציה זו הינה לטובת בדיקה האם מתבצעת חסימה בחומת האש.

networking

שליטה וחסימה בשימוש כתובות IPV6 . אפשרות זו מוגדרת כברירת מחדל.

Miscellaneous

עמודה זו תציג כלים שונים כגון שימוש בפרוקסי, איזון עומסים על המערכת (חלוקת עבודה בין מספר מחשבים על מנת להקל על עומס העבודה), חיסכון במשאבים על סמך פעילות המערכת. אפשרות לקביעת חוק (Schedules) המגדיר לוחות זמנים על פי צרכי המערכת. לאחר הגדרתו נוכל לשייך אותו לחוק שהגדרנו ברשת שלנו והחוק יפעל בהתאם לזמנים שהוגדרו לו מראש (שימוש בפרוטוקולים בזמנים שונים, גישה למקומות מסוימים ברשת וכו'). כברירת מחדל כאשר יפוגו לוחות הזמנים, חיבורים המורשים לפי לוח הזמנים נסגרים. אפשרות זו מבטלת את ההתנהגות הזו.

notifications

חומת האש יכולה להתריע למנהל המערכת על אירועים ושגיאות חשובות על ידי הצגת התראה בסימן הפעמון בתפריט הראשי. בנוסף ניתן להגדיר שההתראות יישלחו לכתובת מייל או לטלגרם.

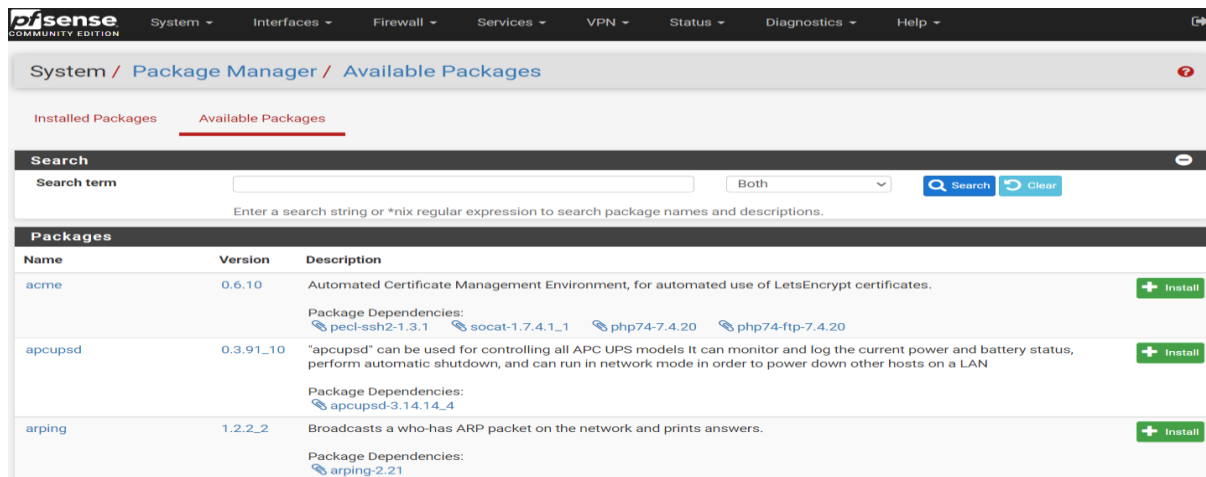
general setup

תפריט להגדרות כלליות, קביעת שם משתמש, דומיין, מיקום, שפת תפעול, איזור זמן

System / General Setup	
System	
Hostname	<input type="text" value="pfSense"/> Name of the firewall host, without domain part
Domain	<input type="text" value="localdomain"/> Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternative TLDs such as 'local.lan' or 'mylocal' are safe.
DNS Server Settings	
DNS Servers	<div><input type="text" value="9.9.9.9"/> Address Enter IP addresses to be used by the system for DNS resolution. These are also used for the DHCP service, DNS Forwarder and DNS Resolver when it has DNS Query Forwarding enabled.</div> <div><input type="text" value=""/> DNS Hostname Enter the DNS Server Hostname for TLS Verification in the DNS Resolver (optional).</div>
Add DNS Server	+ Add DNS Server
DNS Server Override	<input checked="" type="checkbox"/> Allow DNS server list to be overridden by DHCP/PPP on WAN If this option is set, pfSense will use DNS servers assigned by a DHCP/PPP server on WAN for its own purposes (including the DNS Forwarder/DNS Resolver). However, they will not be assigned to DHCP clients.
DNS Resolution Behavior	<div><input type="radio"/> Use local DNS (127.0.0.1), fall back to remote DNS Servers (Default)</div> <div>By default the firewall will use local DNS service (127.0.0.1, DNS Resolver or Forwarder) as the first DNS server when possible, and it will fall back to remote DNS servers otherwise. Use this option to choose alternate behaviors.</div>
Localization	
Timezone	<div><input type="text" value="Asia/Jerusalem"/> Select a geographic region name (Continent/Location) to determine the timezone for the firewall. Choose a special or 'Etc' zone only in cases where the geographic zones do not properly handle the clock offset required for this firewall.</div>
Timeservers	<div><input type="text" value="2.pfsense.pool.ntp.org"/> Use a space to separate multiple hosts (only one required). Remember to set up at least one DNS server if a host name is entered here!</div>

package manager

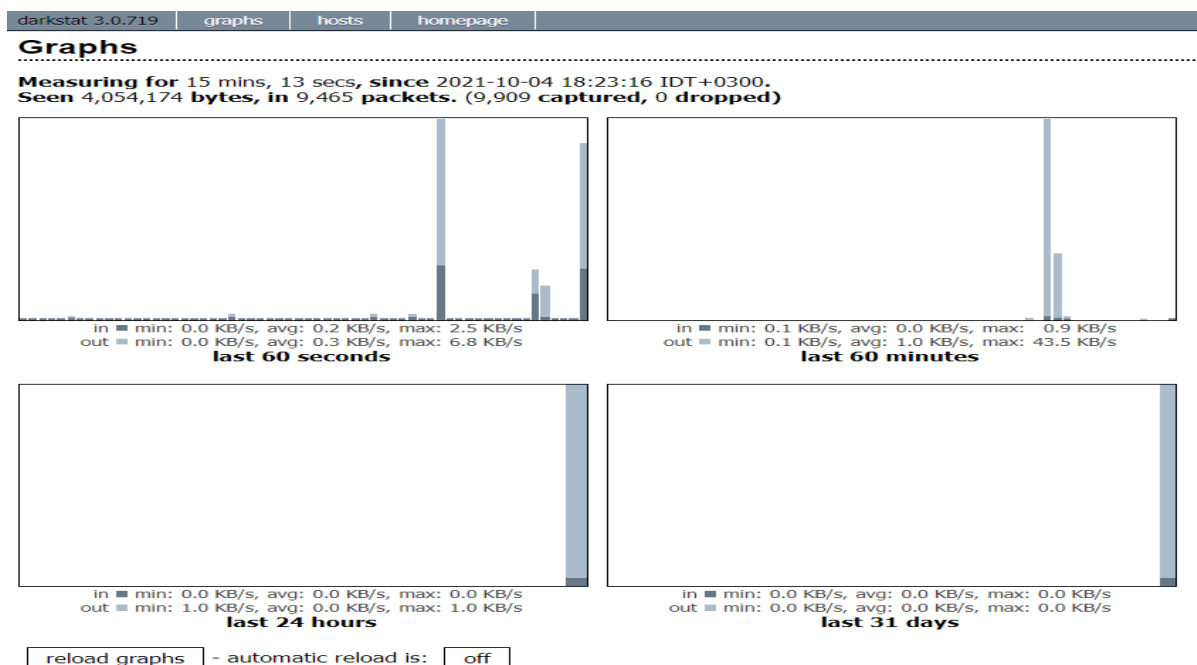
אחת היכולות של pfSense היא יכולת ההתאמה למצבים רבים ושונים באמצעות חבילות. פונקציה זו מאפשרת לנו להוריד מהאינטרנט כלים שיוכלו לסייע בהגנה על המערכת.



להלן כמה דוגמאות על חבילות פופולריות :

(1) Squid - הוא שרת פרוקסי המיועד לשמירת מטמון. הוא שומר מטמון של דפי אינטרנט, תמונות ועוד. אם הפריט המבוקש נמצא במטמון, Squid יכול להעביר אותו ישירות למשתמש המבקש במקום להשתמש בחיבור האינטרנט מה שיכול לשפר את ביצועי האינטרנט.

(2) Darkstat - הוא כלי לניתוח תעבורת רשת על מנת לייעל את ביצועים ולחפש בעיות אפשריות. ניתן לצפות בנתונים שנאספו בכדי לראות אילו פרוטוקולים ויציאות תופסים את רוב רוחב הפס ברשת שלך, התנהלות משתמשים וכו'. מכיוון שכלי פועל ע"י ממשק אינטרנטי נצטרך להגדיר חוק בחומת האש על מנת לאפשר גישה לממשק.



3) snort - היא מערכת לאיתור/מניעת חדירה. תפקידה לקרוא את הPAYLOAD בפאקטה, מזהה את חתימתו של הקובץ המועבר ופי כך פועלת בהתאם. התקנת חבילה זו מאפשרת לנתח תעבורת רשת לאיתור בדיקות, התקפות, סריקות, יציאות ועוד.

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

WAN Settings WAN Categories **WAN Rules** WAN Variables WAN Preprocs WAN IP Rep WAN Logs

Available Rule Categories

Category Selection: ▼
Select the rule category to view and manage.

Defined Custom Rules

```
alert tcp any any -> any any (msg:"executable transmitted over ip"; content:"|4D 5A|");
```

routing

זוהי אחת הפונקציות העיקריות של חומת האש והיא עוסקת בניתוב תעבורת רשת כגון פרוטוקולי ניתוב, ניתוב כתובת IP ציבוריות והצגת פרטי ניתוב.

gateway

הנתב שדרכו מגיעים לרשת

static routes





ניתובים סטטים משמשים כאשר ניתן להגיע לרשתות דרך נתב שאינו מוגדר כברירת מחדל. ניתן לבחור באופציה זו ולהגדיר כתובת ידנית על פי הצורך. הנתב יודע להעביר את בקשת הניתוב על פי הטבלה שברשותו.



user manager

יצירת משתמש חדש בחומת האש אשר יקבל הרשאות בהתאם להחלטת מנהל הממשק. ניתן יהיה לשייכו לקבוצה אשר הוגדר לה הרשאות מראש (כגון צפיה, ביצוע פעולות במערכת וכו'). ישנה אפשרות להגדרת session timeout לממשק הניהול וביצוע הגדרות נוספות.

System / [User Manager](#) / [Users](#) ?

Users Groups Settings Authentication Servers

Users					
	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	 ITAMAR	itamar ashkenazi	✓		 
<input type="checkbox"/>	admin	System Administrator	✓	admins	

 Add  Delete

interfaces

הגדרת והוספת רשתות, ניתן לבצע שינויים בסיסיים של תצורת הממשק בזמן ההתקנה וגם לאחר ההתקנה הראשונית על ידי כניסה לעמודה ושינוי ההגדרות. ישנה אפשרות לערוך כל רשת, לדוגמא חסימה של גישה רשתות מסויימות, אין סיבה שתהייה גישה של רשתות פנימיות מהרשת החיצונית.

interface assignments

כרטיסיה זו תציג את הרשתות הקיימות בחומת האש ניתן לבצע הוספה של רשתות קביעת סוג התצורה ומתן כתובת IP.

interface groups





שיטה המאפשרת להציב כללים במספר ממשקים בו זמנית לדוגמא קבוצה עשויה לשמש כלל ל VLAN DMZ LAN.


wireless

הינו כרטיס אלחוטי שמריצה חומת האש, יכול לשמש כממשק WAN או כממשק OPT - מתייחס לכל הממשקים הנוספים מלבד LAN ו-WAN.

vlan

הגדרת מקטע וירטואלי במקום פיזי אשר מבצע חלוקת רשתות

Interface	Network port
WAN	em0 (08:00:27:4a:6d:32)
LAN	em1 (08:00:27:2e:b3:31) 
SERVERS	em2 (08:00:27:d0:a4:74) 
DMZ	em3 (08:00:27:c6:ce:bd) 
vlanitamartest	VLAN 50 on em1 - lan (Vlan) 

 Save

firewall

נגדיר חוקים בפרוטוקולים שונים האש בו המרכזי בחומת הפיצ'ר בהתאם לצרכי המערכת.

Aliases

קבוצות חוקים בפרוטוקולים, פורטים ו הגדרתURLs ושיוך לחוק שנתאים לצרכי המערכת.

Firewall / Aliases / Edit

Properties

Name

web_servers

The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".

Description

web server port

A description may be entered here for administrative reference (not parsed).

Type

Port(s)

Port(s)

Hint

Enter ports as desired, with a single port or port range per entry. Port ranges can be expressed by separating with a colon.

Port

80

HTTP

Delete

443

HTTPS

Delete

Firewall / NAT / Port Forward

The changes have been applied successfully. The firewall rules are now reloading in the background.
[Monitor](#) the filter reload progress.

Port Forward 1:1 Outbound NAT

Rules

	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Actions
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	web_servers	192.168.10.8	web_servers	

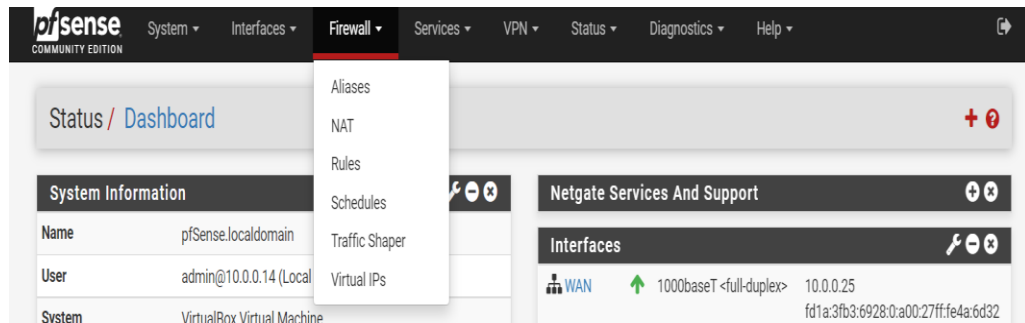
Alias details

Value	Description
80	HTTP
443	HTTPS

Add Add Delete Separator

NAT

חוקים המאפשרים המרה בין כתובות איי פי חיצוניות לפנימיות ללא חשיפת הכתובת הפנימית



NAT Network Address Translation

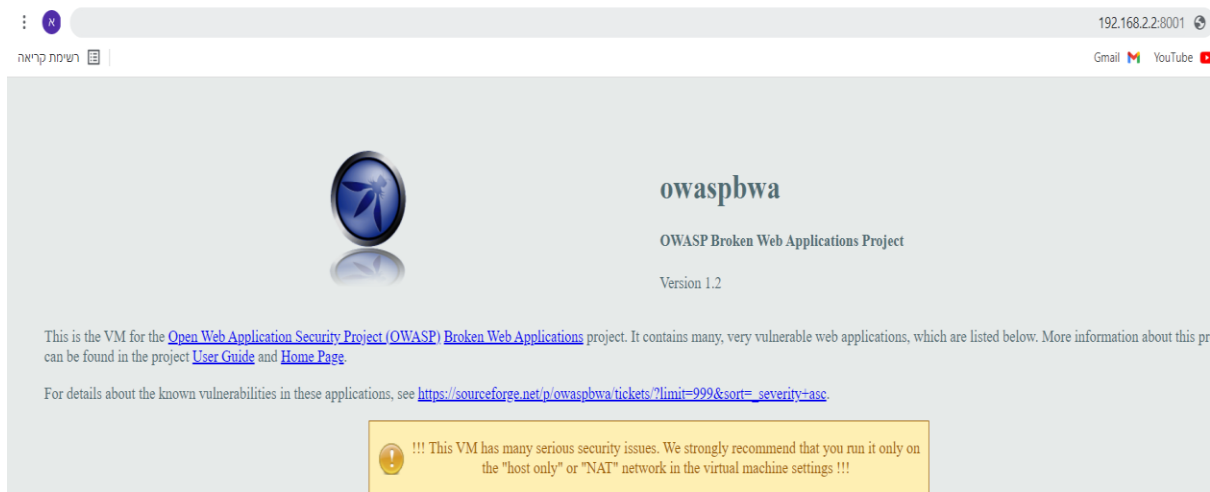
חיבור מחשבים רבים הנמצאים באותה הרשת המקומית לרשת האינטרנט באמצעות כתובת IP אחת בלבד.

יישום זה שימושי לצורך שמירה על הסודיות של הרשת הפנימית ולצורך צמצום כתובות אייפי

<u>Destination</u>	<input type="checkbox"/> Invert match.	WAN address		/	
		Type	Address/mask		
<u>Destination port range</u>	Other	8001	Other	8001	
	From port	Custom	To port	Custom	
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.					
<u>Redirect target IP</u>	192.168.2.2				
	Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12				
<u>Redirect target port</u>	HTTPS				
	Port	Custom			
	Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically). This is usually identical to the "From port" above.				
<u>Description</u>	web access to BWAP				
	A description may be entered here for administrative reference (not parsed).				

במעבדה שלי הגדרתי שכל השרתים שלי תחת כתובת 192.168.2.0/24 הקמתי מערכת הפעלה BWAPP שהיא מבוססת לינוקס והגדרתי חוק NAT על מנת לגשת לממשק המערכת.

החוק הוגדר שכל הפונה לכתובת ה WAN (הכתובת של ה FW) בפורט 8001 יופנה ישירות לכתובת "שמסתתרת" מאחורי כתובת ה FW שהיא בעצם הכתובת של ה BWAPP.



RULES

חוקי גישה, מתן חוקי גישה לפי כתובת מקור וכתובת יעד בפרוטוקולים מסוימים ובפורטים ספציפיים

לדוגמא: בסביבת המעבדה שלי פתחתי גישה מהמחשב שלי לכתובת ה WAN בפורט 443 (HTTPS) באופן קבוע על מנת שתהיה לי גישה לממשק ויתאפשר לי עבודה נוחה יותר.

Source			
Source	<input type="checkbox"/> Invert match	any	Source Address
Display Advanced			
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any .			
Destination			
Destination	<input type="checkbox"/> Invert match	WAN address	Destination Address
Destination Port Range	<input type="text" value="HTTPS (443)"/>	<input type="text" value="HTTPS (443)"/>	<input type="text" value="Custom"/>
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.			
Extra Options			
Log	<input type="checkbox"/> Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).		
Description	<input type="text" value="web admin access from wan"/> A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.		
Advanced Options	Display Advanced		

כעת לאחר ביצוע חוק זה יש גישה חופשית לממשק ניהול.



SCHEDULES

ניתן להוסיף חוקים זמניים, לא תמיד צריך לאפשר גישה קבועה. לדוגמא: אם עובד צריך גישה לשרת כספים לצורך הוצאת דוח רבעוני ניתן להגדיר שהגישה מהעמדה שלו לשרת











תהייה פתוחה בימים א-ה בין השעות 8:00-17:00 בחודש אוקטובר בלבד ובצורה הזו למנוע גישה מעבר לשעות הפעילות של העובד.

Firewall / Schedules

Schedules

Name	Range: Date / Times / Name	Description	Actions
money_server	Mon - Thur Sun / 7:00-16:59 /	SERVERS	 

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	 0/0 B	IPv4 TCP	*	*	*	*	*	none	money_server		   
<input type="checkbox"/>	 0/185 KiB	IPv4 TCP	*	*	WAN address	443 (HTTPS)	*	none		web admin access from wan	   

VIRTUAL IP ADDRESS

הגדרת כתובת וירטואלית ולא פיזית. בFIREWALL זה ישנן 4 סוגים של כתובות IP וירטואליות: IP ALIAS, CARP, PROXY ARP ו OTHER. כל אחד מהם שימושי במצב שונה.

SERVICES

ישנם מספר SERVICES שניתנים לבחירה, מצב מספר דוגמאות:

DHCP SERVER

פרוטוקול תקשורת להקצאת כתובות IP, במסך זה ב FIREWALL ניתן לבחור את הטווח כתובות אשר נרצה שיוקצו, בוחרים את הסביבה הרצויה ובה מגדירים את ההגדרות. מעבר לכתובות IP, ניתן להקצות גם כתובת SUBNET MASK ו SUBNET, שם הדומיין, STATIC ARP וכדומה.

General Options	
Enable	<input checked="" type="checkbox"/> Enable DHCP server on LAN interface
BOOTP	<input type="checkbox"/> Ignore BOOTP queries
Deny unknown clients	<input type="checkbox"/> Only the clients defined below will get DHCP leases from this server.
Ignore denied clients	<input type="checkbox"/> Denied clients will be ignored rather than rejected. This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
Ignore client identifiers	<input type="checkbox"/> If a client includes a unique identifier in its DHCP request, that UID will not be recorded in its lease. This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.
Subnet	10.10.0.0
Subnet mask	255.255.255.0
Available range	10.10.0.1 - 10.10.0.254
Range	<div>From: 10.10.0.10 To: 10.10.0.245</div>

NTP

פרוטוקול המאשר סנכרון עם השעון המרכזי, זאת על מנת שכל הרכיבים ברשת שלי היו בעלי אותה שעה ותאריך. נושא זה חשוב מכיוון שבמידה ובחלק מהשרתים\ תחנות\ ציוד אחר תהייה שעה או תאריך שונה, הלוגים רשמו עם השעון של אותו שרת ובעת תחקור יהיה קושי לדעת את התאריך המדויק בו הפעולה קרתה.

NTP Status	
Server Time	19:08:34 IDT
Sync Source	162.159.200.1 (stratum 3)

SNMP

פרוטוקול המאפשר ניהול התקני רשת מרחוק. מאפשר ניטור של מספר פרמטרים בניהם:
ניטור תעבורת הרשת, מעבד, זיכרון ושימוש בדיסק.
ניתן להגדיר את המודולים עליהם נרצה להפעיל את ה SNMP

SNMP Daemon	
Enable	<input checked="" type="checkbox"/> Enable the SNMP Daemon and its controls
SNMP Daemon Settings	
Polling Port	<input type="text" value="161"/> Enter the port to accept polling events on (default 161).
System Location	<input type="text"/>
System Contact	<input type="text"/>
Read Community String	<input type="text" value="public"/> The community string is like a password, restricting access to querying SNMP to hosts knowing the community string. Use a strong value here to protect from unauthorized information disclosure.
SNMP Traps Enable	
Enable	<input type="checkbox"/> Enable the SNMP Trap and its controls
SNMP Modules	
SNMP modules	<input checked="" type="checkbox"/> MibII <input checked="" type="checkbox"/> Netgraph <input checked="" type="checkbox"/> PF <input checked="" type="checkbox"/> Host Resources <input checked="" type="checkbox"/> UCD <input checked="" type="checkbox"/> Regex
Interface Binding	

VPN







IPSEC TUNNELS

פרוטוקול מבוסס VPN שמקים TUNNELS בין תחנות\ נתבים \ FIREWALL
ניתן להקים ב2 תצורות:

AH - חותם על המידע ומאמת את היוזר

ESP - מבצע הצפנה של המידע

בFIREWALL PFSENSE נתמך בIKEv1 וIKEv2, ניתן לבחור את סוגי ההצפנה

IPsec Tunnels								
	IKE	Remote Gateway	Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
<input type="checkbox"/> 		V2	WAN 10.10.55.30	AES256-GCM (128 bits)	SHA384	14 (2048 bit)		  
								

ישנה אפשרות ליישם L2TP

L2TP Users		
Username	IP address	Actions
ITAMATASH	192.168.15.20	 

OPENVPN

נותן פתרון ליצירת תווך SSL שמאפשר גישה מרחוק לאתר. תומך במספר רב של מערכות הפעלה כגון: LINUX, ANDROID, MAC, SOLARIS, IOS וכדומה.

מורכב מ SERVER ו CLIENT כאשר הגישה היא בין אתר לאתר חומת אש אחת פועלת כשרת והשנייה כלקוח.

STATUS

מציג סטטוס של כל פיצ'ר שהפעלנו ב FIREWALL
בלשונית filter reload ניתן לבחון אם יש שגיאות כלשהן בפיצ'רים שהתקנו

Status / Filter Reload

Filter Reload

[Reload Filter](#)





































[Queue Status](#)

Reload status

```

Initializing
Creating aliases
Creating gateway group item...
Generating Limiter rules
Generating NAT rules
Creating 1:1 rules...
Creating outbound NAT rules
Creating automatic outbound rules
Setting up TFTP helper
Creating NAT rule SSH access to ELK
Creating NAT rule SSH access to HAProxy
Creating NAT rule SSH access to BWAP
Creating NAT rule web access to BWAP
Creating NAT rule web access to xvwa
Creating NAT rule web access to kibana
Generating filter rules
Creating default rules
Pre-caching ...
Creating filter rule ...
Creating filter rules ...
Setting up pass/block rules
Setting up pass/block rules
  
```

בדיקת ה SERVICES שמותקנים

Services			
Service	Description	Status	Actions
bsnmpd	SNMP Service	✓	  
dhcpcd	DHCP Service	✓	    
dpinger	Gateway Monitoring Daemon	✓	    
ipsec	IPsec VPN	✓	    
ntpd	NTP clock sync	✓	    
radvd	Router Advertisement Daemon	✓	 
snort	Snort IDS/IPS Daemon	✓	 
syslogd	System Logger Daemon	✓	   
unbound	DNS Resolver	✓	    

בנוסף ניתן לראות את הלוגים, איזה חוקים לא עבדו כמו שצריך ובאמצעותם לנתח תקלות.
את הלוגים ניתן לראות על כל אחד מהמודולים שהגדרנו: FIREWALL, IPSEC, VPN וכו'

Status / System Logs / Firewall / Normal View

System

Firewall

DHCP

Captive Portal Auth

IPsec

PPP

VPN

Load Balancer

OpenVPN

NTP

Settings

Normal View

Dynamic View

Summary View

Last 50 Firewall Log Entries. (Maximum 50)

Action	Time	Interface	Rule	Source	Destination	Protocol
✖	Oct 9 16:52:33	WAN	Default deny rule IPv4 (1000000103)	📶 192.168.1.10:1900	📶 239.255.255.250:1900	UDP
✖	Oct 9 16:52:33	WAN	Default deny rule IPv4 (1000000103)	📶 192.168.1.10:1900	📶 239.255.255.250:1900	UDP
✖	Oct 9 16:52:33	WAN	Default deny rule IPv4 (1000000103)	📶 192.168.1.12:43754	📶 239.255.255.250:1900	UDP
✖	Oct 9 16:52:33	WAN	Default deny rule IPv4 (1000000103)	📶 192.168.1.10:1900	📶 239.255.255.250:1900	UDP
✖	Oct 9 16:52:33	WAN	Default deny rule IPv4 (1000000103)	📶 192.168.1.10:1900	📶 239.255.255.250:1900	UDP
✖	Oct 9 16:52:33	WAN	Default deny rule IPv4 (1000000103)	📶 192.168.1.12:43754	📶 239.255.255.250:1900	UDP

diagnostics

backup & restore

שרת גיבוי ושחזור הגדרות.

command prompt

פונקציה זו מאפשרת גישה לSHELL, ביצוע פקודות PHP, יכולות יכולת להוריד או להעלות קבצים.

Diagnostics / Command Prompt

Shell Output - netstat

Active Internet connections

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	(state)
tcp4	0	0	192.168.1.34.https	192.168.1.28.59970	ESTABLISHED
udp4	0	0	192.168.1.34.snmp	*,*	
udp6	0	0	pfSense.ntp	*,*	
udp4	0	0	10.10.2.1.12f	*,*	
udp4	0	0	localhost.ntp	*,*	
udp6	0	0	localhost.ntp	*,*	
udp4	0	0	192.168.19.33.ntp	*,*	
udp6	0	0	fe80::1:1%em1.ntp	*,*	
udp4	0	0	pfSense.ntp	*,*	
icm4	0	0	192.168.1.34.*	*,*	
icm4	18450	0	192.168.1.34.*	*,*	
icm6	0	0	fe80::a00:27ff:f.*	*,*	
icm6	77911	0	fe80::a00:27ff:f.*	*,*	

dns lookup

ביצוע שאילתות DNS. שאילתות אלה משיגות כתובות IP או שם DOMAIN

Diagnostics / DNS Lookup

DNS Lookup

Hostname

Results

Result	Record type
74.6.231.20	A
74.6.143.26	A
74.6.231.21	A
74.6.143.25	A
98.137.11.164	A
98.137.11.163	A
2001:4998:44:3507::8000	AAAA
2001:4998:44:3507::8001	AAAA
2001:4998:124:1507::f001	AAAA
2001:4998:24:120d::1:0	AAAA
2001:4998:24:120d::1:1	AAAA
2001:4998:124:1507::f000	AAAA

Timings

Name server	Query time
127.0.0.1	1 msec
192.117.235.235	12 msec
62.219.186.7	10 msec
8.8.8.8	54 msec

בנוסף קיימת שיטה traceroute המאפשרת מציאת דרך שבה עוברות חבילות מידע. תוכנה זו מייצרת פלט של רשימת כתובות ה IP של ממשקי הנתבים אשר קיימים בדרך אל היעד החל מנקודת המוצא ממנה יצאה הבקשה.

Diagnostics / Traceroute

Traceroute

Hostname

IP Protocol

IPv4

Select the protocol to use.

Source Address

Any

Select source address for the trace.

Maximum number of hops

18

Select the maximum number of network hops to trace.

Reverse Address Lookup

☐

When checked, traceroute will attempt to perform a PTR lookup to locate hostnames for hops along the path. This will slow down the process as it has to wait for DNS replies.

Use ICMP

☐

By default, traceroute uses UDP but that may be blocked by some routers. Check this box to use ICMP instead, which may succeed.

Traceroute

Results

```

1 192.168.1.1 5.716 ms 1.639 ms 1.026 ms
2 10.190.128.1 33.144 ms 10.623 ms *
3 * * *
4 212.25.116.153 15.609 ms 13.228 ms 10.618 ms
5 10.25.18.250 10.170 ms 14.255 ms 9.651 ms
6 10.25.19.10 9.162 ms 8.497 ms 16.654 ms
7 212.25.77.14 49.962 ms 9.340 ms 10.347 ms
8 62.219.189.21 62.068 ms
  212.179.124.85 10.395 ms 9.527 ms
9 212.179.124.38 62.136 ms
  80.81.193.115 61.238 ms 62.762 ms
10 209.191.112.25 74.316 ms
   80.81.193.115 58.589 ms 59.765 ms
11 209.191.64.24 150.387 ms
   209.191.112.25 70.098 ms 71.811 ms
12 209.191.64.24 219.025 ms
   209.191.112.7 74.079 ms
   209.191.64.24 143.232 ms
13 209.191.64.39 218.839 ms
   209.191.64.24 205.625 ms
   209.191.112.25 75.405 ms
14 209.191.64.39 231.496 ms
   209.191.64.24 204.718 ms
   216.115.105.29 204.356 ms

```

halt system

סגירת המערכת בבטחה על ידי פונקציית halt. פעולה זו מכבה את כלל השירותים הפעילים ובך חומת האש נסגרת ללא סיכון בפגיעה בשירותים.

Diagnostics / Halt System

The system is halting now. This may take one minute or so.

Stopping package pfBlockerNG...done.

Stopping package snort...done.

Stopping package squid3...done.

Stopping package squidGuard...done.

Stopping package darkstat...done.

Stopping /usr/local/etc/rc.d/dnsbl.sh...done.

Stopping /usr/local/etc/rc.d/sq_monitor.sh...done.

30

packet capture

בדיקה וניתוח של חבילת נתונים. ניתן לבחור כתובת IP כדי לקבל עליה מידע על חיבורים שימושים בפרוטוקולים שונים ועוד'

Diagnostics / Packet Capture

Packet Capture Options

Interface

SERVERS

Select the interface on which to capture traffic.

Promiscuous

☐ Enable promiscuous mode

Non-promiscuous mode captures only traffic that is directly relevant to the host (sent by it, sent or broadcast to it, or routed through it) and does not show packets that are ignored at network adapter level.
Promiscuous mode ("sniffing") captures all data seen by the adapter, whether or not it is valid or related to the host, but in some cases may have undesirable side effects and not all adapters support this option. Click Info for details

Address Family

Any

Select the type of traffic to be captured.

Protocol

Any

Select the protocol to capture, or 'Any'.

Host Address

10.10.1.4

This value is either the Source or Destination IP address, subnet in CIDR notation, or MAC address.
Matching can be negated by preceding the value with '!'. Multiple IP addresses or CIDR subnets may be specified. Comma (",") separated values perform a boolean 'AND'. Separating with a pipe ("|") performs a boolean 'OR'.
MAC addresses must be entered in colon-separated format, such as xx:xx:xx:xx:xx:xx or a partial address consisting of one (xx), two (xx:xx), or four (xx:xx:xx:xx) segments.
If this field is left blank, all packets on the specified interface will be captured.

Port

The port can be either the source or destination port. The packet capture will look for this port in either field. Matching can be negated by preceding the value with '!'. Multiple ports may be specified. Comma (",") separated values perform a boolean 'AND'. Separating with a pipe ("|") performs a boolean 'OR'. Leave blank if not filtering by port.

Packet Length

0

The Packet length is the number of bytes of each packet that will be captured. Default value is 0, which will capture the entire frame regardless of its size.

Count

100

This is the number of packets the packet capture will grab. Default value is 100.
Enter 0 (zero) for no count limit.

Level of detail

Normal

This is the level of detail that will be displayed after hitting "Stop" when the packets have been captured.
This option does not affect the level of detail when downloading the packet capture.

Reverse DNS Lookup

☐ Do reverse DNS lookup

The packet capture will perform a reverse DNS lookup associated with all IP addresses.
This option can cause delays for large packet captures.

Last capture start

October 10th, 2021 7:37:23 pm.

Last capture stop

October 10th, 2021 7:38:10 pm.

Start

View Capture

Download Capture

Packets Captured

19:37:38.983340 ARP, Request who-has 10.10.1.1 tell 10.10.1.4, length 46
19:37:38.983362 ARP, Reply 10.10.1.1 is-at 08:00:27:1a:c9:fs, length 28
19:37:38.983727 IP 10.10.1.4 > 8.8.8.8: ICMP echo request, id 38935, seq 1, length 64
19:37:39.036901 IP 8.8.8.8 > 10.10.1.4: ICMP echo reply, id 38935, seq 1, length 64
19:37:39.982251 IP 10.10.1.4 > 8.8.8.8: ICMP echo request, id 38935, seq 2, length 64
19:37:40.037448 IP 8.8.8.8 > 10.10.1.4: ICMP echo reply, id 38935, seq 2, length 64
19:37:40.983965 IP 10.10.1.4 > 8.8.8.8: ICMP echo request, id 38935, seq 3, length 64
19:37:41.037055 IP 8.8.8.8 > 10.10.1.4: ICMP echo reply, id 38935, seq 3, length 64
19:37:41.985896 IP 10.10.1.4 > 8.8.8.8: ICMP echo request, id 38935, seq 4, length 64
19:37:42.039303 IP 8.8.8.8 > 10.10.1.4: ICMP echo reply, id 38935, seq 4, length 64

pftop

31

יציג את כלל התהליכים בחומת האש.מכן ניתן יהיה לגזור חיבורים של משתמשים לממשקים, יציאה לרשת ולרשתות שונות.

Diagnostics / pfTop

pfTop Configuration

View: default

Filter expression: e.g. tcp, ip6 or dst net 208.123.73.0/24
click for filter help

Sort by: Bytes

Maximum # of States: 100

Output

pfTop: Up State 1-10/10, View: default, Order: bytes

PR	DIR	SRC	DEST	STATE	AGE	EXP	PKTS	BYTES
tcp	In	192.168.1.28:57023	192.168.1.34:443	ESTABLISHED:ESTABLISHED	00:08:48	24:00:00	2915	1783503
icmp	Out	192.168.1.34:58739	192.168.1.1:58739	0:0	00:09:28	00:00:09	2131	61799
tcp	Out	192.168.1.34:52380	192.5.5.241:53	FIN_WAIT_2:ESTABLISHED	00:07:20	00:07:40	9	1197
tcp	Out	192.168.1.34:46881	192.203.230.10:53	FIN_WAIT_2:ESTABLISHED	00:09:13	00:05:47	9	1142
udp	Out	:::1[41215]	:::1[123]	MULTIPLE:SINGLE	00:00:03	00:00:27	2	508
udp	In	:::1[41215]	:::1[123]	SINGLE:MULTIPLE	00:00:03	00:00:27	2	508
ipv6-icmp	In	fe80::1:1[16576]	ff02::1[16576]	NO_TRAFFIC:NO_TRAFFIC	00:00:16	00:00:00	2	352
ipv6-icmp	Out	fe80::1:1[16576]	ff02::1[16576]	NO_TRAFFIC:NO_TRAFFIC	00:00:16	00:00:00	2	352
ipv6-icmp	In	fe80::e2ce:c3ff:fe8c:698[1644]	ff02::1[16448]	NO_TRAFFIC:NO_TRAFFIC	00:00:24	00:00:02	2	320
ipv6-icmp	Out	fe80::1:1[0]	ff02::16[0]	NO_TRAFFIC:NO_TRAFFIC	00:00:16	00:00:00	2	152

ICMP-ping

תפקידו הוא לבדוק האם תקשורת מסוגלת להגיע ממקור אל היעד וחזרה .

התשובה נקבל 3 נתונים:

bytes -גודל חבילת המידע

time -כמה זמן במילי שניות

ttl -כמות הצעדים שחבילת המידע עוברת עד ליעד ובחזרה

socket

מציג רשימה של חיבורים פעילים ב tcp/udp .

פונקציה זו שימושית על מנת לצפות בכתובות ip ויציאות בשימוש בתהליכי מערכת או חבילות שונות.

Diagnostics / Sockets

Show all socket connections

IPv4 System Socket Information

USER	COMMAND	PID	FD	PROTO	LOCAL	FOREIGN
nobody	darkstat	32355	8	tcp4	192.168.1.35:666	*:*
root	syslogd	53970	8	udp4	*:514	*:*
root	ntpd	94711	21	udp4	*:123	*:*
root	ntpd	94711	23	udp4	192.168.1.35:123	*:*
root	ntpd	94711	26	udp4	192.168.4.1:123	*:*