

monitoring



context

Dit document toont hoe je monitoring uitvoert op pfsense, zodat je netwerk verkeer kunt volgen.

pftop

geeft een overzicht (cfr Linux top commando) van de state table van de firewall (pf)
maw: alle openstaande verbindingen die de firewall heeft tussen netwerken.

Diagnostics > pftop

- filter: laat toe om te filteren op protocol, source, destination, port, ...
 - voorbeelden:
 - filter: port 3389 toont alle RDP verkeer op Windows servers
 - filter: dst <ip adres> toont alle verkeer dat met een bepaald IP is/wordt opgezet.
 - filter: port 902: toont alle verkeer dat op poort 902 (VM restore) wordt opgezet.
- Zo kan je de file transfer zien passeren

Output									
pftop: Up State 1-2/2 (105), View: default, Order: bytes									
PR	DIR	SRC	DEST	STATE	AGE	EXP	PKTS	BYTES	
tcp	In	10.11.115.26:51983	10.11.12.16:902	ESTABLISHED:ESTABLISHED	00:11:46	24:00:00	17749131	15661M	
tcp	Out	10.11.115.26:51983	10.11.12.16:902	ESTABLISHED:ESTABLISHED	00:11:46	24:00:00	17749131	15661M	

Warning: Verkeer dat niet wordt opgebouwd (blocked, bv) zal je hier **niet** zien

states

geeft een overzicht van de state table van de firewall

Diagnostics > States

- State Filter: laat toe om te filteren op interface en een bijkomende regex in te geven (ipadres, poort, ...)
- voorbeelden:
 - filter: LAN, ESTABLISHED: toont alle verbindingen op interface LAN

State Filter

Interface

LAN

Filter expression

ESTABLISHED

Filter

States						
Interface	Protocol	Source (Original Source) -> Destination (Original Destination)	State	Packets	Bytes	
LAN	tcp	10.11.12.16:752 -> 10.11.25.20:2049	ESTABLISHED:ESTABLISHED	16.42 M / 59.017 M	969.06 MiB / 81.11 GiB	
LAN	tcp	10.11.12.16:14472 -> 10.11.50.20:3260	ESTABLISHED:ESTABLISHED	160.693 M / 35.334 M	217.93 GiB / 13.08 GiB	
LAN	tcp	10.11.12.20:58187 -> 10.11.50.20:3260	ESTABLISHED:ESTABLISHED	190.743 M / 35.769 M	261.39 GiB / 7.26 GiB	
LAN	tcp	10.11.12.20:852 -> 10.11.25.20:2049	ESTABLISHED:ESTABLISHED	267.716 K / 301.489 K	20.31 MiB / 201.33 MiB	
LAN	tcp	10.11.12.16:48796 -> 10.11.50.20:3260	ESTABLISHED:ESTABLISHED	60.54 M / 10.609 M	83.13 GiB / 2.02 GiB	

Note: Wordt al snel één van je meestgebruikte diagnonses als je over meerdere interfaces beschikt

logboek

- ga naar:**Status > System > Logs: Firewall**
- 3 weergaves:
 - **Normal** View: standaard view van alle verkeer, met inbegrip van een omschrijving van de rule die van toepassing was
 - **Dynamic** View: dynamische weergave waarbij nieuwe logs worden aangevuld.
 - **Summary** View: grafisch overzicht van verkeer dat werd verwerkt, gerangschikt per poort, protocol, ...
- hier zie je meteen of verkeer al dan niet doorgelaten wordt;
- maak er een goede gewoonte **elke** firewall regel van logging te voorzien.

From:

<https://louslab.be/> - **Lou's lab**

Permanent link:

<https://louslab.be/doku.php?id=pfsense:monitoring>

Last update:

2024/11/16 18:14

