Firewall migratie: Sophos naar pfsense

doelstelling

deze werkinstructie beschrijft hoe ik mijn Sophos firewall omzette naar PFsense.

configuratie bestanden ophalen

swich

- meld aan als admin
- maak een backup van de switch. XML bestand bevat oa alle VLANs (inclusief de naam)

Sophos

1. meld aan als admin
2. ga naar: **System > Backup & Firmware > Import export > Export: Export Selective configuration, Add new item**
    1. **BackupRestore**:backup methode (inclusief credentials)
    2. **DHCPServer**: dhcp configuratie per interface
    3. **FirewallRule**: firewall regels
    4. **FirewallRuleGroup**: firewall regels indeling (appliance, netwerk, windows, linux, ...)
    5. **Interface**: fysieke interfaces (inclusief PPoE details)
    6. **IPHost**: host, netwerk (h_ad1, nw_installatie, bv)
    7. **IPHostGroup**: (hg_bigjack_nfs, bv)
    8. **Services**: service_tcp/udp:poort (NFS, s_qcenter, bv)
    9. **ServiceGroup**: groep met services (sg_AD_authentication, bv)
    10. **VLAN**: alle vlans, inclusief netwerk configuratie.
3. **Export**
4. **Download**
5. pack het TAR-bestand uit met **7zip**
6. **hernoem** naar betekenisvolle naam (interfaces, vlan, ...)

Note: Je kan alles in 1 tarball downloaden maar **afzonderlijke** bestanden zijn handiger om in Visual Studio Code te laden en ivv checklist af te werken

pfsense

1. meld aan als admin
2. ga naar: **Diagnostics > Backup & Restore**
3. **Backup Area**:
    1. DHCP Server
    2. Aliases
    3. Interfaces
    4. VLANS
4. **Download configuration as XML**

Note: Als je pfsense bovenstaande configuraties nog niet heeft, dien je er mogelijk een dummy aan te maken zodat je de xml syntax hebt.

configuratie bestanden maken

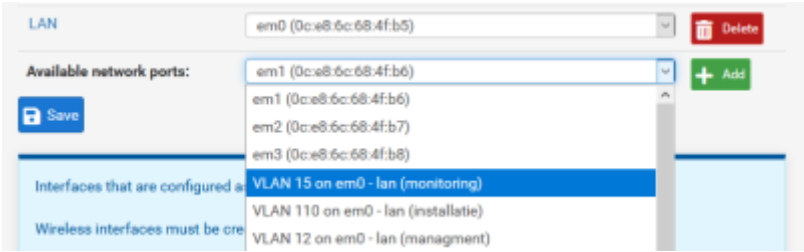
Warning: Gebruik enkel **underscores** in je naamgeving, geen spacties, haakjes, ...
Dat leidt tot fouten bij het laden van je fw regels!

VLAN

- open **Visual Studio Code**
- open pfsense VLAN bestand
- selecteer Sophos VLAN bestand, rechter-klik: **Open to the Side**
- maak de VLANs aan in pfsense VLAN.xml
- kijk het bestand na op syntax fouten en **bewaar** het.
- open **Diagnostics > Backup & Restore: Restore Backup**
- **Restore area**: **VLANS**
- **configuration file**: blader naar het bestand dat je maakte
- kies **Restore Configuration**

Interfaces

- ga naar **Interfaces > Assignments**
- **Available network ports**:selecteer de VLAN en kies **+Add**



- dubbelklik op **OPT**
    - **Description**: vervang door naam van VLAN

    - IPv4: **Static IPv4**
    - **IPv4 Address**: geef subnet in dat je voor die interface terugvindt in Sophos VLAN.xml. Kies voor IP = IP Sophos -1 (dus: .253 ipv .254). Dit voorkomt dat je gelijke adressen hebt als beide fw aan staan.
    - **Enable**: vink aan
    - **Save**, **Apply Changes**
- voer bovenstaande stappen uit voor de overige VLANs.

aliases

Nu je interfaces hebt, kan je firewall regels aanmaken tussen die verschillende netwerken.
Daarvoor gebruik je volgende aliassen:

- **ip host**: individuele host met IP adres of ip netwerk.
- **hostgroup**: groep met ip host en/of ip netwerk die toegang krijgen
- **service group**: groep met netwerkppoorten waarop toegang verleend wordt.

ip host

- ga op dezelfde manier tewerk als bij VLAN maar open IPHostGroup.xml
- zoek naar: `<HostType>IP</HostType>`

```
<Name>h_freebsd</Name>
<IPFamily>IPv4</IPFamily>
<HostType>IP</HostType>
<IPAddress>10.11.110.75</IPAddress>
</IPHost>
```

- voeg alle hosts toe
- restore in pfsense

Note: Als het bestand niet correct restored wordt, controleer dan je syntax op typo's
syntax highlighting is een grote hulp om opening en closing tags op te sporen!

ip hostgroup

* ga op dezelfde manier tewerk als bij ip host maar open dit keer IPHostGroup.xml

- zoek naar: `<IPHostGroup`

```
<IPHostGroup transactionid="">
<Name>hg_dns_transfer_ad1</Name>
<Description/>
<HostList>
<Host>h_ad3</Host>
<Host>h_ad5</Host>
</HostList>
```

```
<IPFamily>IPv4</IPFamily>
</IPHostGroup>
```

- voeg alle hosts toe
- restore in pfsense

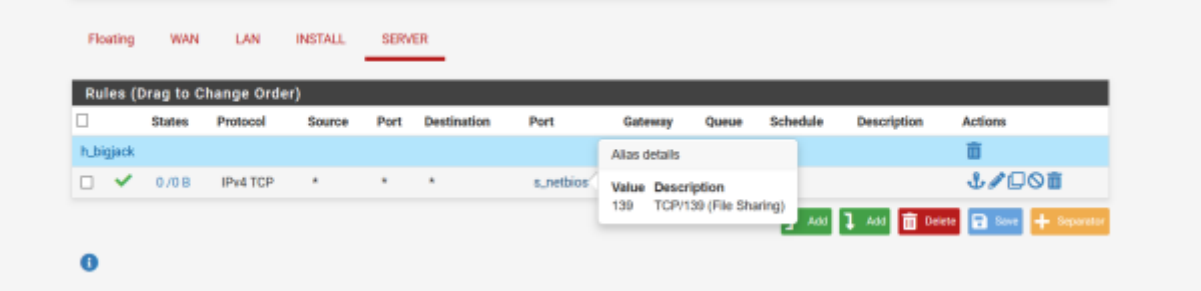
services

* ga op dezelfde manier tewerk als bij ip host maar open dit keer Services.xml

- zoek naar: <Name>s

```
<Name>S_RDP</Name>
<Type>TCPorUDP</Type>
<ServiceDetails>
<ServiceDetail>
<SourcePort>1:65535</SourcePort>
<DestinationPort>3389</DestinationPort>
<Protocol>TCP</Protocol>
```

- voeg alle services (ports) toe
- **description**: TCP/port
  die kan je dan later in je fw regels als je erover hovert



- restore in pfsense

servicegroups

* ga op dezelfde manier tewerk als bij services maar open dit keer ServiceGroup.xml

- zoek naar: <ServiceGroup transactionid=“”>

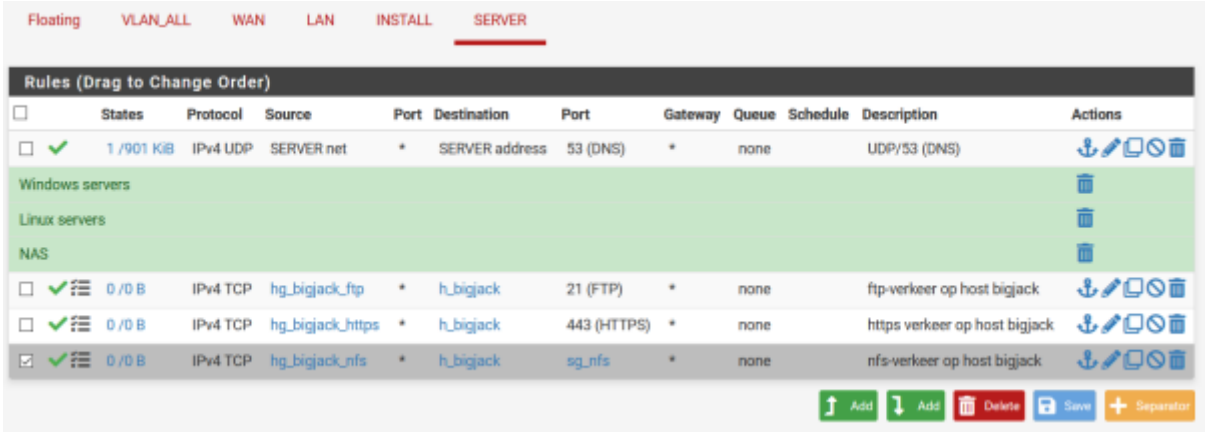
```
<Name>sg_synthing</Name>
<Description>services nodig om syncthing remote te
benaderen</Description>
<ServiceList>
<Service>HTTPS</Service>
<Service>s_syncthing</Service>
<Service>s_syncthing2</Service>
<Service>samba (137)</Service>
</ServiceList>
</ServiceGroup>
```

- voeg alle services (ports) toe aan de group
- **description**: geef een betekenisvolle omschrijving van de group
- restore in pfsense

Note: Beloon uzelf! Copy'n Paste is eentonig werk.
Alles wat nu volgt, is spannender werk:

firewall regels maken

- open **FirewallRuleGroup**.xml voor een overzicht van je fw-regels.
  Waar deze in Sophos op 1 pagina staan, zal je die moeten verdelen over de interfaces in pfsense.
  Regels die op een host van toepassing zijn zet je dus bij de interface waar die host achter zit. Het subnet, dus.
- voorbeeld: **h_bigjack_ftp** bepaalt de toegang op de FTP service op host bigjack die deel uitmaakt van het server netwerk.
  De firewall regel maak je dus aan op de interface server in pfsense.
- maak volgende **separator** aan:
  - Windows servers
  - Linux servers
  - NAS
- maak de fw regel aan uit **FirewallRuleGroup.xml**
- zoek de details rond de regel op in **FirewallRuleGroup.xml** en zet die over op de pfsense fw regel
- maak de volgende regel aan door een **duplicate** te nemen van de bestaande en pas aan waar nodig.



meer info

firewall, sophos, pfsense, werkinstructies, netwerking