Nätverkssäkerhet – Site-to-site VPN med pfSense

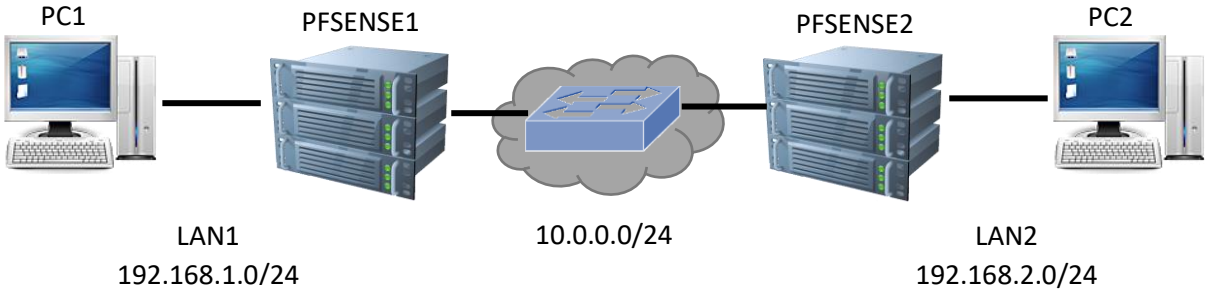
I denna laboration kommer vi att skapa en så kallad Site-to-site VPN tunnel (baserad på IPSec) mellan två brandväggar som kör pfSense. Detta ska simulera att vi har två siter som är anslutna till "Internet" där vi vill att datorerna på respektive skyddade LAN ska kunna kommunicera med varandra och använda tjänster mm. som bara tillåts på de skyddade lokala nätverken utan att obehöriga ska kunna se informationen som utbyts.

Antal: Enskilt eller i större grupp ifall fysisk labbutrustning används. Görs laborationen i virtuell miljö så kan man med fördel jobba enskilt, annars kan det vara enklast att samarbete med en annan grupp.

Material: Två maskiner som kör pfSense och två maskiner som agerar klienter. Eventuellt en switch för att koppla samman datorerna med men det går bra att koppla ihop dem direkt, gränssnitt till gränssnitt.

Tips: Dokumentation hittar ni på https://doc.pfsense.org

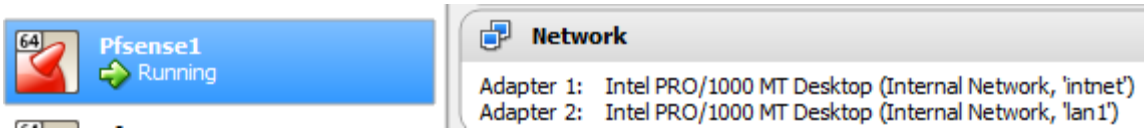
Topologi

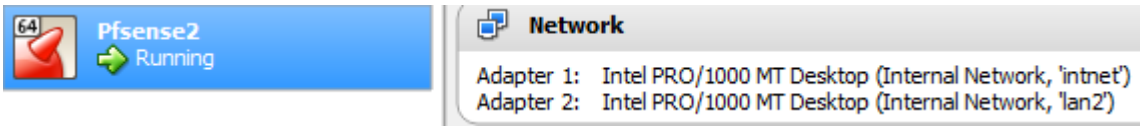


Enhet	Gränssnitt	IP-adress	Nätmask	Default-Gateway	Switch port
PC1	Fa0	Via DHCP	255.255.255.0	192.168.1.1	-
PC2	Fa0	Via DHCP	255.255.255.0	192.168.2.1	-
PFSENSE1	Fa0	10.0.0.1	255.255.255.0	10.0.0.254	-
	Fa1	192.168.1.1	255.255.255.0	-	-
PFSENSE2	Fa0	10.0.0.2	255.255.255.0	10.0.0.254	-
	Fa1	192.168.2.1	255.255.255.0	-	-

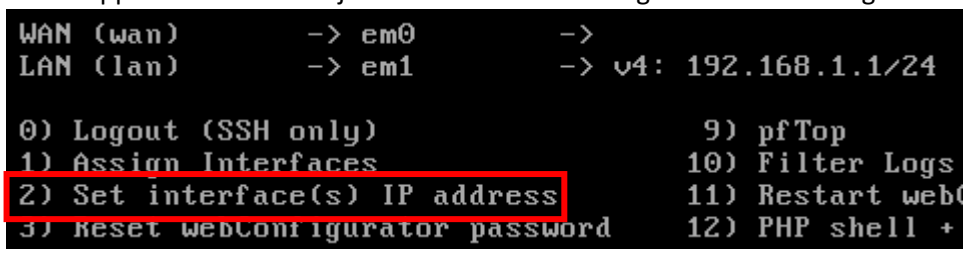
Utförande: I exemplet så kommer vi att utgå från att man gör laborationen i en Virtuell miljö (Virtualbox).

Koppla samman enheterna enligt topologin. Vi förutsätter här att vi har två maskiner med pfSense installerade. Dessa maskiner måste ha två nätverkskort var. Vi använder oss av 3 "Internal Networks" som vi kallar *LAN1, Intnet* och *LAN2* och ansluter dem till pfsense1 och pfsense 2 enligt följande: (se bild)





1. Starta upp **PfSense1** och välj alternativ **2** för att konfigurera IP-inställningar.



2. Välj interface **1** (kallat **WAN**). Detta är som standard konfigurerat till automatisk tilldelning via DHCP men vi ska nu sätta en fast statisk adress.
3. Välj **n** (no) som svar på frågan ifall vi vill använda DHCP
4. Ange IP-adressen **10.0.0.1**
5. Ange **24** som subnätmask (antal bitar 24 = 255.255.255.0)
6. Ange IP-adressen **10.0.0.254** som "upstream gateway address". Denna adress kommer vi ej att använda och fyller egentligen ingen funktion i detta scenario.
7. Välj **n** (no) som svar på frågan ifall vi vill använda DHCPv6
8. Tryck på **ENTER** för att inte ange någon IPv6-adress.
9. Välj **n** (no) som svar på frågan ifall vi vill använda http istället för HTTPS
10. Tryck på **ENTER**
11. Kontrollera så att IP-inställningarna för nätverkskorten är korrekt (se bild).

Observera att LAN nätverket automatiskt tilldelas adressen **192.168.1.1** samt kör en DHCP-server (ifall vi installerat pfSense med express-inställningar). Detta passar bra för pfsense1 men är något vi måste ändra på för pfsense2.

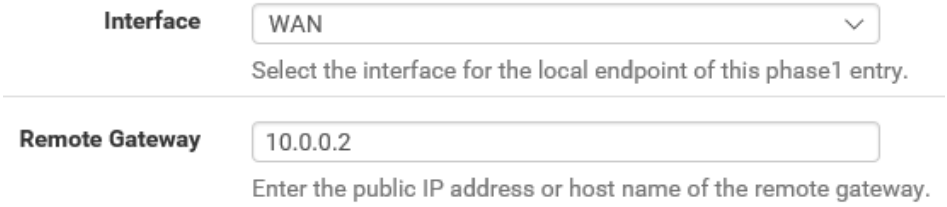
12. Starta **PfSense2** och upprepa steg 1 till 10. Konfigurera WAN-gränssnittet för pfsense2 med IP-adressen **10.0.0.2** (steg 6).
13. På **PfSense2** välj alternativ **2** (Set Interface IP address)
14. Välj alternativ **2** (LAN)
15. Ange IP-adressen **192.168.2.1**
16. Ange **24** som nätmask
17. Klicka på **ENTER** (för ingen upstream gateway address)
18. Klicka på **ENTER** (för ingen IPv6-adress)
19. Ange **Y** (Yes) för att aktivera DHCP-server på LAN-gränssnittet
20. Ange lämplig startadress som DHCP-servern ska dela ut, t.ex. **192.168.2.50**
21. Ange lämplig slutadress som DHCP-servern ska dela ut, t.ex. **192.168.2.200**
22. Välj **n** (no) som svar på frågan ifall vi vill använda http istället för HTTPS
23. Tryck på **ENTER**
24. Kontrollera så att IP-inställningarna för nätverkskorten är korrekt (se bild).

25. Anslut en klient (**PC1**) till **LAN1** och kontrollera så att klienten får korrekta IP-inställningar från **PfSense1**

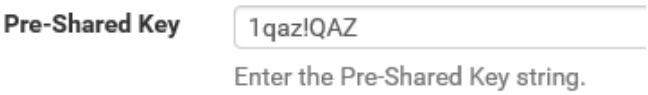
```
Connection-specific DNS Suffix  . : localdomain
Link-local IPv6 Address . . . . . : fe80::5d08:aa7d:9106:c483%8
IPv4 Address. . . . . . . . . . . : 192.168.1.100
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : fe80::1:1%8
                                    192.168.1.1
```

26. På **PC1**, öppna en webbläsare och anslut till **192.168.1.1**. Ni kan behöva ange protokollet i adressfältet, **https://192.168.1.1**
27. Logga in med användarnamn **admin** och lösenordet **pfsense**
28. Är det första gången ni loggar in på en pfsense-installation så kommer den automatiska installationsguiden att starta. Om så är fallet så avslutas den enklast genom att klicka på pfsense-loggan.
    Klicka på **VPN** – **IPSec**
29. Klicka på **Add P1**

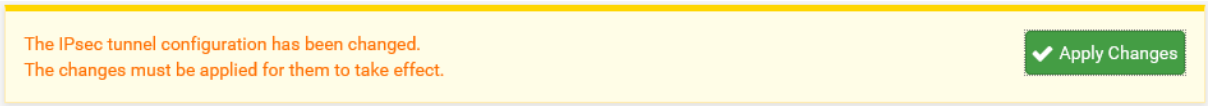
30. Vi går nu in i **VPN – IPSec – Tunnels – Edit Phase 1** och ska skapa en IPSec VPN-tunnel. Vi behåller standardinställningarna i stort sett. Bläddra ner och ange IP-adressen **10.0.0.2** (adressen till PfSense2) som **Remote Gateway**. Kontrollera även att **interface** är **WAN** (se bild).



31. Bläddra ner (notera standardinställningarna för de olika faserna). Ange en lämplig **Pre-shared Key** vi väljer **1qaz!QAZ** (i produktion bör nyckeln vara betydligt längre)



32. Bläddra ner (notera standardinställningarna för de olika faserna) och klicka på **Save** längst ner för att spara.
33. Vid ändringar visas en notifiering

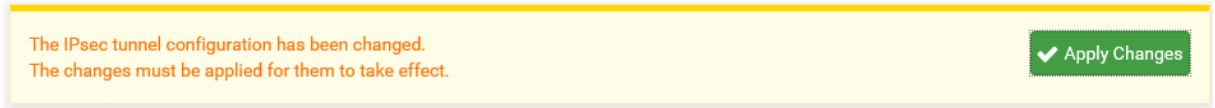


    Klicka på **Apply Changes**
34. Vi måste nu definiera vilken trafik som är "intressant" d.v.s. den trafik som ska skickas genom vår VPN-tunnel. Klicka på **Show Phase 2 Enteries**

    Klicka på **Add P2**

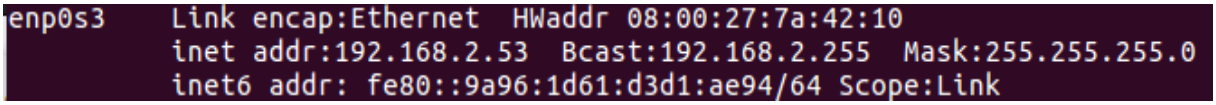
35. Vi går nu in i **VPN – IPSec – Tunnels – Edit Phase 2** och ska definiera vilken trafik som ska skickas genom VPN-.tunneln
    Vi använder standardinställningar som i stort sett säger att tunneln ansluter till vårt lokala (LAN) IPv4-nätverk (notera inställningarna).
    Bläddra ner och ange **Remote Network** till **192.168.2.0/24** (Interna nätverket för PfSSense2 LAN2)

36. Bläddra ner och klicka på **Save** för att spara konfigurationen
37. Vid ändringar visas en notifiering



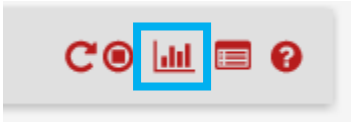
Klicka på **Apply Changes**

38. Anslut en klient (**PC2**) till **LAN2** och kontrollera så att klienten får korrekta IP-inställningar från **PfSense2**

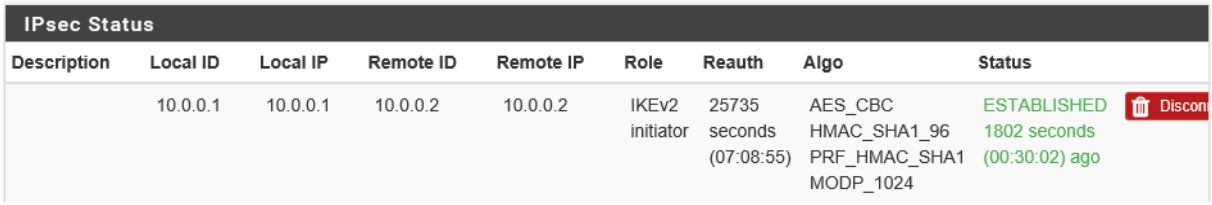


(bild från Ubuntu-klient)

39. Från **PC2** öppna kommandotolken (eller terminalen om ni kör Linux) och prova att pinga **192.168.1.1** och IP-adressen för **PC1**. Notera att det ej går att kommunicera med dessa.
40. På **PC2**, öppna en webbläsare och anslut till **192.168.2.1**. Ni kan behöva ange protokollet i adressfältet, **https://192.168.2.1**
41. Logga in med användarnamn **admin** och lösenordet **pfsense**
42. Upprepa nu steg **28** till **37** men ange **Remote Gateway 10.0.0.1** samma **Pre-Shared Key 1qaz!QAZ** samt **Remote Network 192.168.1.0/24**.
43. På **PfSense1** klicka på **VPN – IPSec** och sedan på **Related Status**

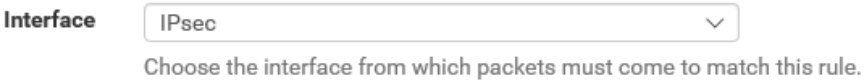


44. Vi ser nu IPSec statusen. Om tunneln ej är ansluten så klicka på **Connect**. Ni kan behöva göra samma sak på **PfSense2**. Om allt fungerar så ska status vara *ESTABLISHED* (se bild).

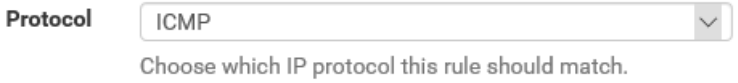


45. Nu är tunneln etablerad men brandväggarna blockerar fortfarande trafiken så vi måste lägga regler som anger vilken trafik som ska tillåtas genom vår VPN-tunnel.
46. På **PfSense1** klicka på **Firewall – Rules**
47. Klicka på **Add** för att skapa en ny regel.

48. Välj **Interface IPSec**



49. Välj **Protocol ICMP** för att tillåta ICMP-trafik på vår IPSec-tunnel så att vi kan pinga enheter.



50. Bläddra ner och klicka på **Save**
51. Vid ändringar visas en notifiering

Klicka på **Apply Changes**

52. Upprepa steg **47** till **51** men ange **Protocol TCP** för att tillåta all TCP-trafik.
53. Vi måste lägga samma regler på **PfSense2** så upprepa steg **47** till **52** på **PfSense2**
54. Kontrollera så att allt fungerar genom att från **PC1** pinga **192.168.2.1** (PfSense 2 interna gränssnitt) och pinga **PC2**. Prova även att ansluta med webbläsaren till PfSense2 på IP-adressen **192.168.2.1**

```
C:\Users\Itlararen>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time=1ms TTL=63
Reply from 192.168.2.1: bytes=32 time<1ms TTL=63
Reply from 192.168.2.1: bytes=32 time=1ms TTL=63
Reply from 192.168.2.1: bytes=32 time=1ms TTL=63
```

55. **Extrauppgift:** Vid tid över kan ni prova att skapa en VPN-tunnel som använder OpenVPN istället för IPSec. Titta i pfSense dokumentation vid behov. Ni bör ta bort befintlig VPN-tunnel först i så fall.

Detta skall du kunna efter genomförd labb:

✓ Skapa en Site-to-site VPN-tunnel baserad på IPSec med PfSense