Nätverkssäkerhet – Remote Access VPN med pfSense

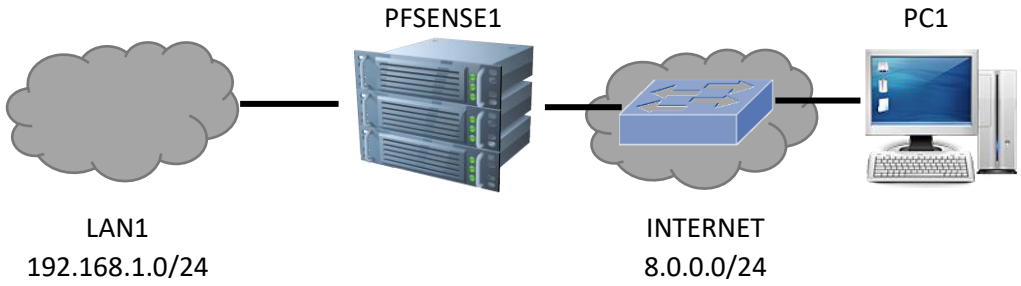
I denna laboration kommer vi att skapa en så kallad *Remote Access* VPN åtkomst (baserad på OpenVPN) så att klienter utifrån det oskyddade nätverket (Internet) kan komma åt det inre skyddade nätverket och på så sätt komma åt skyddade tjänster som om klienten var ansluten till det lokala nätverket.

Antal: Enskilt eller i grupp om två.

Material: En maskin som kör pfSense och en maskin som agerar klient. 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

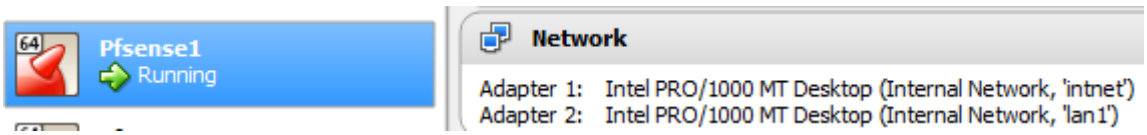
Topologi



Enhet	Gränssnitt	IP-adress	Nätmask	Default-Gateway	Switch port
PC1	Fa0	8.0.0.10	255.255.255.0	-	-
PFSENSE1	Fa0	8.0.0.1	255.255.255.0	8.0.0.254	-
	Fa1	192.168.1.1	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 en maskin med pfSense installerad. Denna maskin måste ha två nätverkskort. Vi använder oss av 2 "Internal Networks" som vi kallar *LAN1* och *Intnet* och ansluter enligt följande: (se bild)



Har vi två maskiner som kan agera klienter så är det bra men det räcker med en maskin, *PC1* som vi kommer att använda både för att konfigurera *PfSense1* via *LAN1* samt agera klient ute på "Internet".

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

```
WAN (wan)       -> em0        ->
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 webC
3) Reset WebConfigurator password    12) PHP shell +
```

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 **8.0.0.1**
5. Ange **24** som subnätmask (antal bitar 24 = 255.255.255.0)
6. Ange IP-adressen **8.0.0.254** 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).

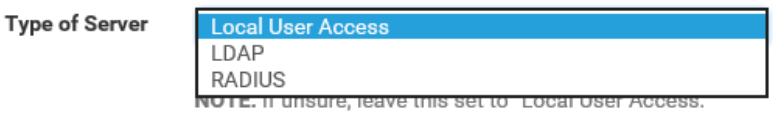
```
WAN (wan)       -> em0        -> v4:  8.0.0.1/24
LAN (lan)       -> em1        -> v4: 192.168.1.1/24
```

Observera att LAN nätverket automatiskt tilldelas adressen **192.168.1.1** samt kör en DHCP-server (ifall vi installerat pfSense med express-inställningar).

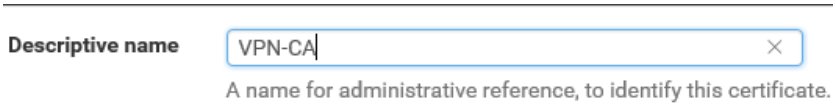
12. Anslut en klient (**PC1**) till **LAN1** och kontrollera så att klienten får korrekta IP-inställningar från **PfSense1**

```
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
```

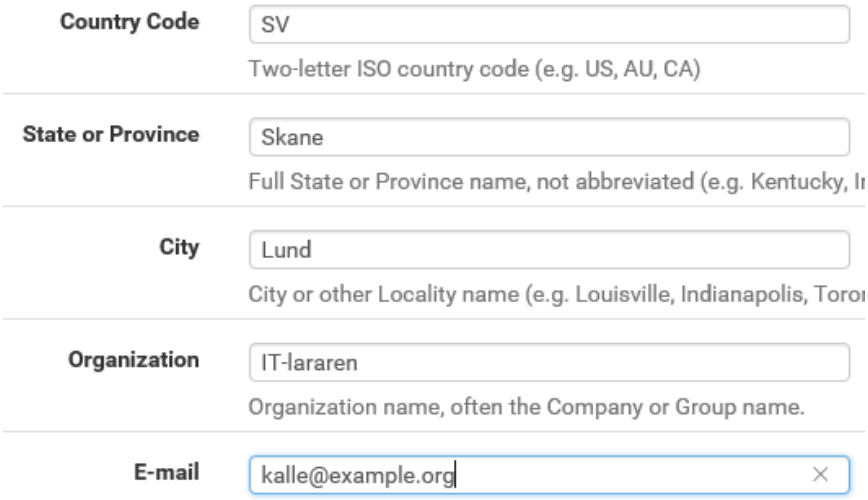
13. På **PC1**, öppna en webbläsare och anslut till **192.168.1.1**. Ni kan behöva ange protokollet i adressfältet, **https://192.168.1.1**
14. Logga in med användarnamn **admin** och lösenordet **pfsense**
15. Är det första gången ni loggar in på en pfsense-installation så kommer den automatiska installationsguiden att starta. Om så är fallet så avslutas den enklast genom att klicka på pfsense-loggan.
16. Klicka på **VPN** – **OpenVPN** och sedan på fliken **Wizard** som startar den automatiska guiden för att skapa en OpenVPN Remote Access Server.
17. Välj autentiserings typ **Local User Access**. Observera att man kan autentisera via både LDAP och RADIUS.



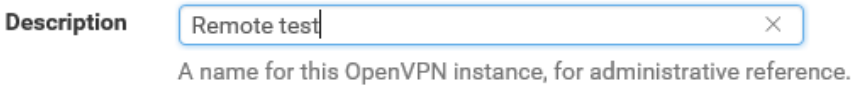
18. Nästa steg är att skapa en *CA* (Certificate Authority) som kan utfärda certifikat. Ange valfritt beskrivande namn i fältet **Descriptive Name**. Vi använder här **VPN-CA**



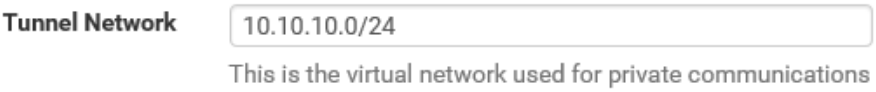
19. Observera nyckellängd och livstid för certifikaten. Vi använder standardinställningar här men i produktion så är rekommendationen att öka nyckellängden. I övrigt så fyller vi i följande (se bild):



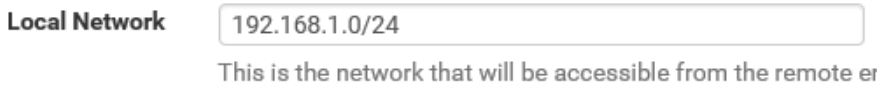
20. Nästa steg är generell information såsom vilket gränssnitt som ska användas för inkommande anslutningar (WAN) samt protokoll (UDP) och portnummer. Notera dessa inställningar och använd standardinställningarna. Ange valfri **Description**. Vi väljer här **VPN test**.



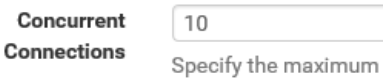
21. Notera inställningarna för kryptering och behåll standardinställningarna.
22. Ange ett nytt unikt nätverk som *Tunnel Network*. Detta är ett virtuellt nätverk som används mellan servern och klienter. Ange **Tunnel Network** till **10.10.10.0/24**



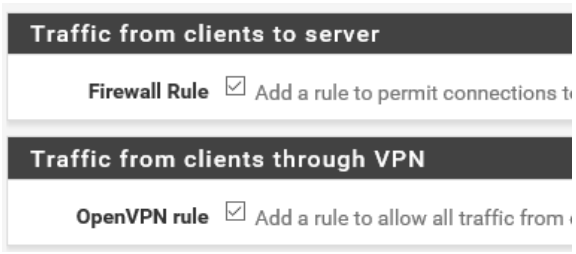
23. Ange **Local Network** till **192.168.1.0/24**. Detta är det inre nätverk som anslutande klienter ska komma åt.



24. Vi anger **Concurrent Connections** till **10**. Anger vi inget så tillåtes (antagligen) hur mångga anslutningar som helst (oklart i dokumentationen).

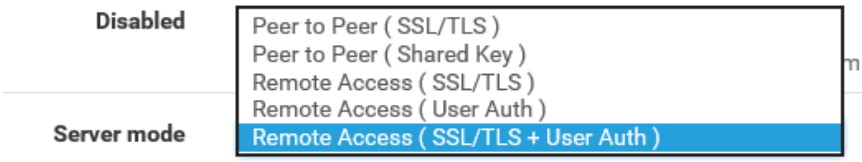


25. Vi behåller standardinställningarna. Vissa inställningar är extra intressanta såsom *Inter-Client Communication* som tillåter kommunikation mellan anslutna klienter samt DNS-inställningar mm. Bläddra ner och klicka på **Next**
26. Klicka i **Firewall Rule** och **OpenVPN rule** för att lägga till brandväggsregler så att klienter kan kommunicera med VPN-servern samt tillåta trafik från klienterna genom VPN-tunneln.

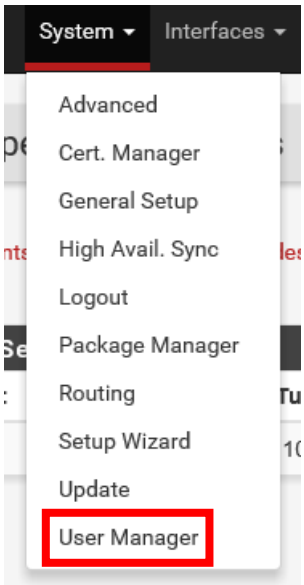


27. Guiden är nu klar. Klicka på **Finish**
28. Det finns inställningar som vi kan ändra som ej presenterades vid den automatiska guiden. För att göra detta så klickar vi på **Edit Server (OBS frivilligt)**.

29. Intressantas av inställningar är **Server Mode** som kan konfigureras till olika typer (Se bild).



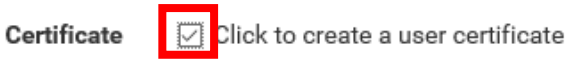
Standard är **Remote Access (SSL/TLS + User Auth)**. Vilket innebär att anslutna klienter behöver både ett *certifikat* samt autentisera sig men *användarnamn/lösenord* för att ansluta (säkrast). Vill vi göra det enkelt för oss så kan vi ändra till enbart certifikat eller enbart användarautentisering (finns olika fördelar med dessa konfigurationer men vi använder standardinställningar).



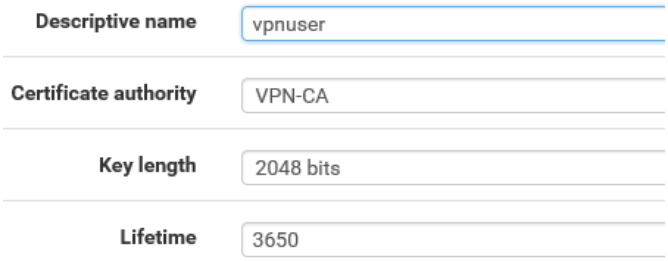
30. Avbryt ändringar genom att t.ex. klicka på **Servers** i övre menyn eller på något i övre menyn.
31. Nästa steg är nu att skapa en lokal användare samt ett certifikat så att vi kan ansluta. Gå till **System – User Manager**
32. Klicka på **Add** för att skapa en ny användare

33. Vi fyller i **Username test** och **Password 1qaz!QAZ** samt fullständigt namn.

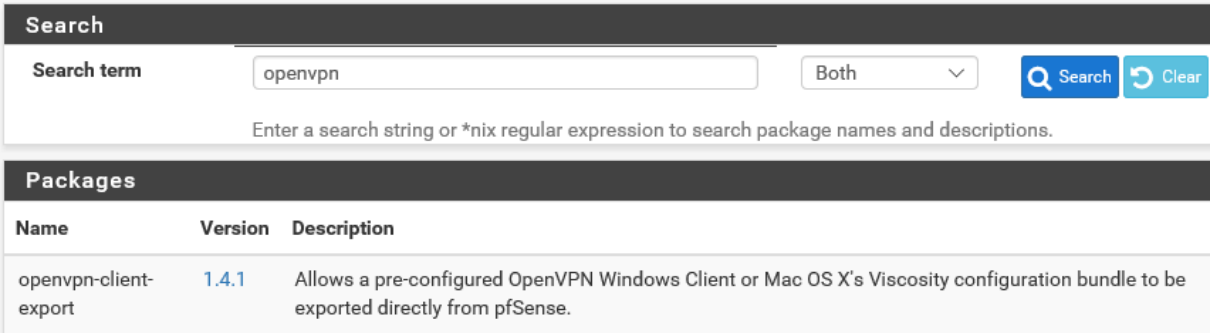
34. Bocka i rutan vid **Certificate** för att skapa ett certifikat åt användaren.



35. Vi anger **vpnuser** som beskrivande namn. Observera inställningar för nyckellängd och livstid (räknas i dagar, standard är 10 år). Kontrollera så att Certificate Authority är den som vi skapade tidigare.

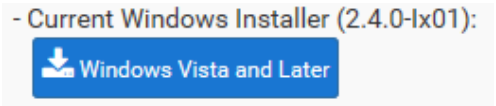


36. Bläddra ner och klicka på **Save**
37. För att underlätta anslutningen till vår VPN-server så ska vi nu installera ett programpaket till pfSense som heter **OpenVP-Client-Export**. Med detta verktyg kan vi enkelt exportera inställningar till våra klienter och till och med få en exekverbar installationsfil för Windows. Klicka på **System – Package Manager** (detta kräver att pfSense-maskinen har åtkomst till Internet, har den inte det så får vi tillfälligt ge den Internet-access genom att ansluta WAN-gränssnittet till NAT eller bryggat nätverk och ändra WAN-inställningarna)
38. Klicka på **Available Packages**
39. Enklast är att söka på **openvpn**



40. Klicka på **Install**

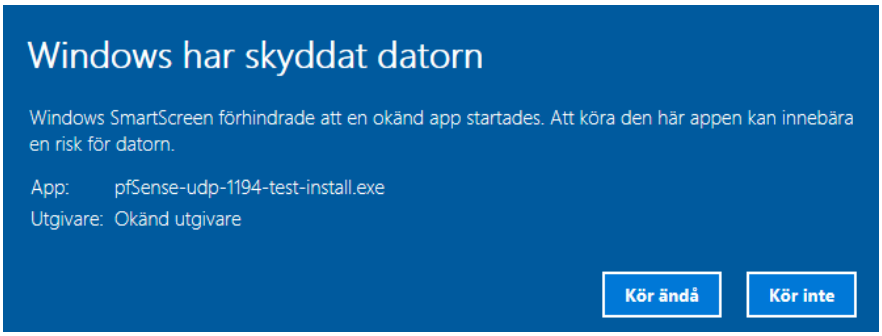
41. Klicka på **Confirm**
42. När installationen är slutförd så hittar man verktyget under **VPN – OpenVPN**
43. Innan vi går vidare så konfigurerar vi om WAN-gränssnittet på pfSense-maskinen till **8.0.0.1** om ändringar gjordes i steg 37.
44. Klicka på det nya menyalternativet **Client Export**
45. Observera inställningarna. Vi bläddrar längst ner och väljer aktuell användare **test** och klickar på knappen **Windows Vista and Later** för att ladda hem en installationsfil med *OpenVPN Community Client* med tillhörande certifikat för användaren test.



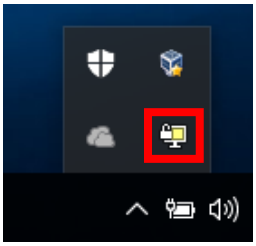
OBS i detta ögonblick så exporteras inställningar för att ansluta till pfSense-maskinens IP-adress på WAN-gränssnittet. När vi ska testa vår klient sedan så måste klienten kunna nå detta IP-nummer…

46. Spara filen på skrivbordet (eller valfri plats så länge vi vet var vi har den).
47. Anslut klientdatorn till samma nätverk som pfSense-maskinens WAN-gränssnitt är ansluten till. Se till så att klientdatorn har ett IP-nummer så att klienten har åtkomst till pfSense-maskinens WAN-gränssnitt via nätverket.
48. På klientdatorn. Kör installationsfilen som bör heta något i stil med *pfSense-udp-1194-test-install.exe*. En varning kommer upp ifall ni kör Windows 10 eftersom installationsfilen inte är

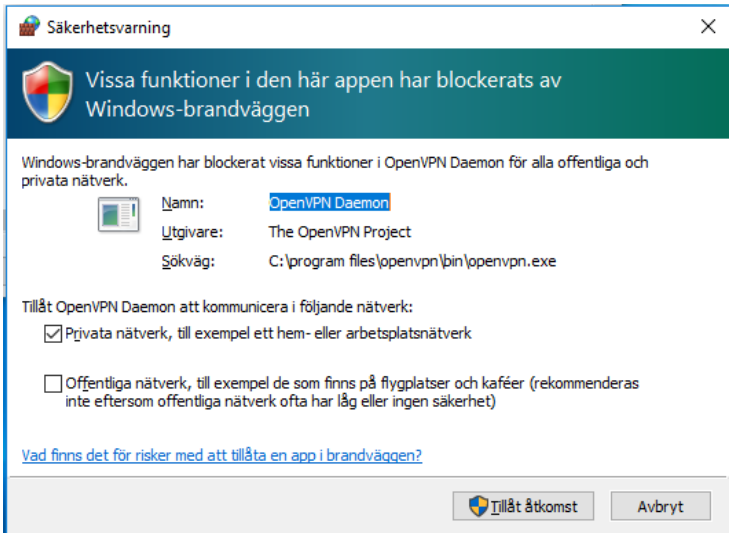
signerad av en betrodd källa. Klicka i så fall på **Mer information** och **Kör ändå** för att starta installationen.



49. Klicka på **Ja** i dialogrutan från User account Control.
50. Klicka på **Install**
51. Klicka på **Next**
52. Klicka på **I Agree** för att acceptera licensavtalet
53. Klicka på **Next**
54. Klicka på **Install**
55. Under installationen dyker det upp en dialogruta som undrar ifall vi vill installera ett nätverkskort. Klicka på **Installera**
56. Klicka på **Next**
57. Klicka på **Finish**
58. Klicka på **Close**
59. När allt är klart så ska OpenVPN-klienten ha installerats. Vi hittar den nere till höger i statusfältet. Klicka på ikonen.

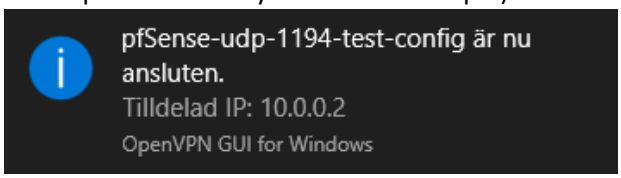


60. En dialogruta öppnas som frågar efter användarnamn och lösenord. Ange uppgifterna till den lokala användare vi skapade på pfSense-maskinen **test** med lösenordet **1qaz!QAZ**



61. Tillåt OpenVPN-klienten i Windowsbrandväggen.
62. Om allt fungerar som det ska så ansluts vi nu och kommer åt det skyddade interna nätverket. Vi felsökning, kontrollera alla inställningar, certifikat och användare. Kontrollera att

enheterna sitter på rätt nätverk samt IP-inställningar. Vissa användare hävdar att man alltid behöver köra OpenVPN som administratör. Kontrollera även brandväggen på klienten. Tänk även på att pfSense blockerar alla privata IP-adresser på WAN-gränssnittet som standard (därför använder vi en icke-privat adress-rymd i detta exempel).



63. Prova att starta kommandotolken (eller terminalen) på klientmaskinen och kontrollera IP-inställningar med **ipconfig** (eller ifconfig). Notera att det virtuella nätverkskortet tilldelats ett IP-nummer i det nätverk som angavs i steg 22 (10.0.10.0/24).
64. Prova att pinga pfSense-maskinens inre LAN-gränssnitt med kommandot **ping 192.168.1.1**
65. Prova även att ansluta med webbläsare till pfSense webbgränssnitt **https://192.168.1.1**
66. Extra utmaning: Det ska gå att skapa en Remote Access VPN som fungerar med Windows inbyggda VPN-klient. det har dock rapporterats om en hel del problem sedan Windows 10 Anniversary Update kom. Får ni tid över kan ni se ifall ni får igång ett sådant scenario. Glöm ej att ta bort befintligt OpenVPN-konfiguration först för säkerhetsskull. Mer information hittar man här: https://doc.pfsense.org/index.php/IKEv2_with_EAP-MSCHAPv2

Detta skall du kunna efter genomförd labb:

✓ Skapa en Remote-Access VPN-server baserad på OpenVPN med PfSense samt ansluta en klient