

Vejledning i UNI•Sikkerhed-routerens indbyggede firewall

UNI•C er en styrelse under Undervisningsministeriet, der leverer et bredt spektrum af it-tjenester til uddannelses- og forskningsverdenen. Mere end en million brugere er jævnligt i berøring med UNI•Cs it-tjenester og produkter.

Læs mere på www.uni-c.dk

Konvertering af åbent og ubeskyttet O-ben

UNI•C anbefaler skoler med et åbent og ubeskyttet O-ben i deres UNI•Sikkerhed at få nettet beskyttet ved hjælp af Sektornet-routerens indbyggede firewall. Firewallen tages i brug ved at konvertere O-benet til et beskyttet ben af typen P eller X.

Denne vejledning gennemgår en række punkter, der er relevante at overveje i forbindelse med en konvertering.

P- eller X-ben?

For det første skal det fastlægges, om det nye ben skal være af typen P eller X.

Såvel P- som X-benet er som udgangspunkt lukket af i forhold til adgang fra maskiner på internettet. Der er dog adgang til P-benet fra skolens eget A-ben. I det store hele er beskyttelsen af de to ben i standardkonfigurationen derfor identisk. Forskellene ligger i de muligheder, der er for at tilpasse de to typer ben efter egne ønsker og behov.

P-ben

P-benet indgår på linie med A-benet i skolens sikkerhedsgruppe og er dermed underlagt gruppens beslutninger. Hvis skolen derfor ønsker en ændring af P-benet, der sænker sikkerheden, vil det kun være muligt, hvis ændringen er godkendt af sikkerhedsgruppen. Fordelen ved P-benet er, at det er nemt og ligetil at åbne for trafik fra andre P-ben i samme sikkerhedsgruppe.

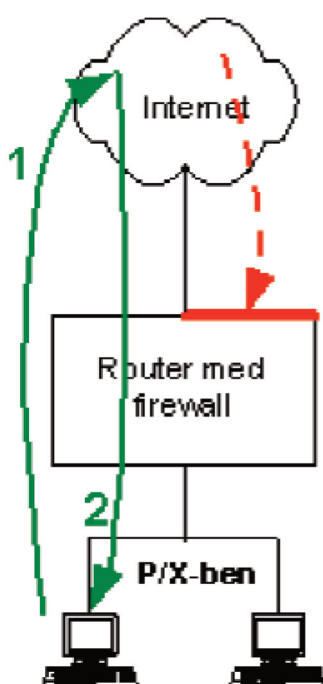
X-ben

X-benet indgår i modsætning til P-benet ikke i en sikkerhedsgruppe. Det betyder, at skolen kan få foretaget ændringer af opsætningen uden at de først skal godkendes. X-benet er derimod ikke velegnet, hvis skolen har stort behov for kommunikation med andre skoler i samme sikkerhedsgruppe.

Forskel mellem P-ben og X-ben

Skemaet herunder illustrerer hvilke forskelle der er mellem et P-ben og et X-ben.

	P-ben	X-ben
Indgår i sikkerhedsgruppen og er dermed underlagt gruppens beslutninger	x	
Skolen har selv fuld beslutningsret over benet		x
Adgang fra skolens A-ben	x	
Beskyttet af routerens firewall	x	x
Velegnet som undervisningsben hvis der er behov for kommunikation med andre skoler i sikkerhedsgruppen	x	
Velegnet som undervisningsben, hvis der ikke er behov for kommunikation med andre skoler i samme sikkerhedsgruppe		x
Velegnet som DMZ-ben til skolens offentlige servere som fx web- og mailserver		x



Portåbninger

Inden en konvertering til P- eller X-ben finder sted, bør det overvejes, om der er behov for statiske åbninger fra internettet mod det nye ben. Bemærk at sådanne åbninger normalt kun være mulige at få foretaget mod X-benet, men afhængig af sikkerhedsgruppens beslutninger kan de også være mulige for P-benet.

Firewallen der beskytter P- og X-benet sørger automatisk for at al almindelig trafik, der initieres fra skolen mod internettet fortsat vil fungere efter konverteringen. Det gælder adgang til webservere, mailservere, newsservere og alle andre gængse internettjenester.

På figuren initierer maskinen til venstre en forbindelse og firewallen tillader derfor automatisk returtrafikken.

Beskyttelsen og begrænsningen kommer ind i det tilfælde hvor det forsøges at initiere trafik fra internettet mod X/P-benet som illustreret med rødt på figuren nedenfor. Firewallen vil som udgangspunkt spærre for denne trafik, helt i overensstemmelse med tankegangen om at nettet skal beskyttes.

Hvis skolen har enkelte servere/tjenester, der fortsat skal være adgang til fra internettet, skal de lokaliseres, så der i forbindelse med konverteringen kan laves særlige åbninger, der netop tillader trafik til den/de udvalgte tjenester. I forbindelse med bestilling af konverteringen specificeres servertypen og maskinens IP-adresse.

De mest almindelige offentlige servere med tilhørende portnumre fremgår af følgende tabel:

Server	Protokol	Portnummer
Webserver	http	80/tcp
Webserver (https)	https	443/tcp
Mailserv	smtp	25/tcp
Windows Terminal Server (fjernskrivebord)	rdp	3389/tcp
Citrix	ica	1494/tcp
FTP-server	ftp	21/tcp
Windows NT/2000	NetBT	139/tcp

Hvis der i stedet er tale om egentlig lokalnetservere, der kun skal bruges af skolens egne brugere, bør der laves en løsning, der sikrer, at ikke alle på hele internettet har adgang. I den forbindelse anbefales Sektornet VPN, en meget sikker og fleksibel løsning, der sikrer at kun udvalgte brugere får adgang til skolens lokalnet.

Mere generel information om sikkerheden i Sektornet-routeren kan findes på www.uni-c.dk/basisabonnement.