

**Nettverkskommunikasjon over ulike nettverkssoner**

<b>Målgruppe</b> Dette temaarket er spesielt relevant for:	<input checked="" type="checkbox"/> Leverandør <input checked="" type="checkbox"/> IKT-ansvarlig <input type="checkbox"/> Prosjektleder	<input checked="" type="checkbox"/> Sikkerhetsleder/koordinator <input type="checkbox"/> Virksomhetens leder/ledelse <input type="checkbox"/> Medarbeider/ansatt	<input checked="" type="checkbox"/> Databehandler <input type="checkbox"/> Personvernombud <input type="checkbox"/> Annet, spesifiser .....
<b>Ansvar</b>	IKT-Ansvarlig		
<b>Når</b>	Under etablering av et informasjonssystem eller ved endringer		
<b>Formål</b>	Beskrive behovet for å kontrollere nettverkskommunikasjon mellom soner for autentisering		
<b>Omfang</b>	Omfatter all nettverkskommunikasjon innenfor et informasjonssystem		
<b>Hjemmel</b>	Personopplysningsforskriften § 2-11		
<b>Referanser</b>	Veileder i sikkerhetsarkitektur: Systemteknisk sikkerhet – Sikkerhetsbarrierer Systemteknisk sikkerhet - Datakommunikasjon		

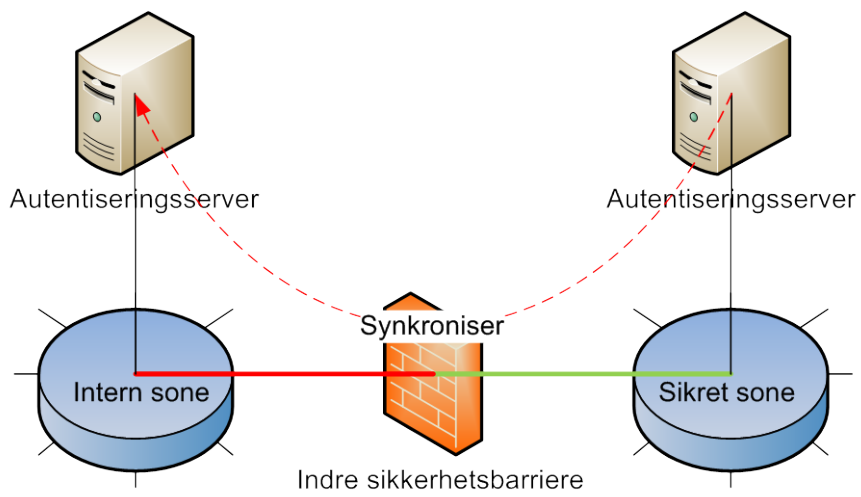
**Bakgrunn**

Autentiseringsløsninger benytter ulike kommunikasjonsporter for å kommunisere seg i mellom. Dette er nærmere forklart i sikkerhetsveilederen under kapittelet systemteknisk sikkerhet. Eksempelvis bruker LDAP i Active Directory port 389 i tillegg til en hel del andre porter for å kommunisere<sup>1</sup>.

For å kommunisere mellom ulike nettverkssoner må slik trafikk normal gå igjennom sikkerhetsbarrierer eller annet nettverksutstyr som sslvpn, rutere og svitsjer. Det er en forutsetning at minimum en sikkerhetsbarriere står imellom nettverkssoner med ulikt sikkerhetsnivå. Sikkerhetsbarrierene vil ikke fungere som forutsatt dersom alle påkrevde kommunikasjonsporter for autentiseringsmekanismer er åpne til enhver tid.

Nr.	Aktivitet/Beskrivelse
<b>1</b>	<b>Kommunikasjon gjennom sikkerhetsbarrierer</b> <ul style="list-style-type: none"> <li>• Antall kommunikasjonsporter i sikkerhetsbarrierer må holdes til et minimum</li> <li>• Active Directory autentisering eller andre autentiseringsmekanismer kan ikke brukes mellom ulike soner uten å begrense antallet åpne kommunikasjonsporter.</li> <li>• Datakommunikasjonen må initieres fra sikre soner for å hindre uautorisert trafikk inn i slike soner.</li> <li>• Det anbefales å bruke autentiseringsservere i "read-only mode" i sikre soner. Grunnen til dette er enveis oppdatering, som vil minimere nettverkstrafikken mellom sonene</li> </ul>
<b>2</b>	<b>Mulige metoder</b> <ul style="list-style-type: none"> <li>• Bruk av IP/VPN – Trunkere nettverkstrafikk</li> <li>• Omkonfigurere nettverksporter for autentiseringsmekanismer og annen nettverkstrafikk i serverkonfigurasjonen.</li> <li>• Styre trafikken gjennom SSLVPN, "reverse" Proxy eller andre tekniske hjelpemidler i DMZ</li> </ul>

<sup>1</sup> [http://technet.microsoft.com/en-us/library/dd772723\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd772723(WS.10).aspx)



Figur 1: Autentiseringsløsning mellom to soner med ulikt sikkerhetsnivå