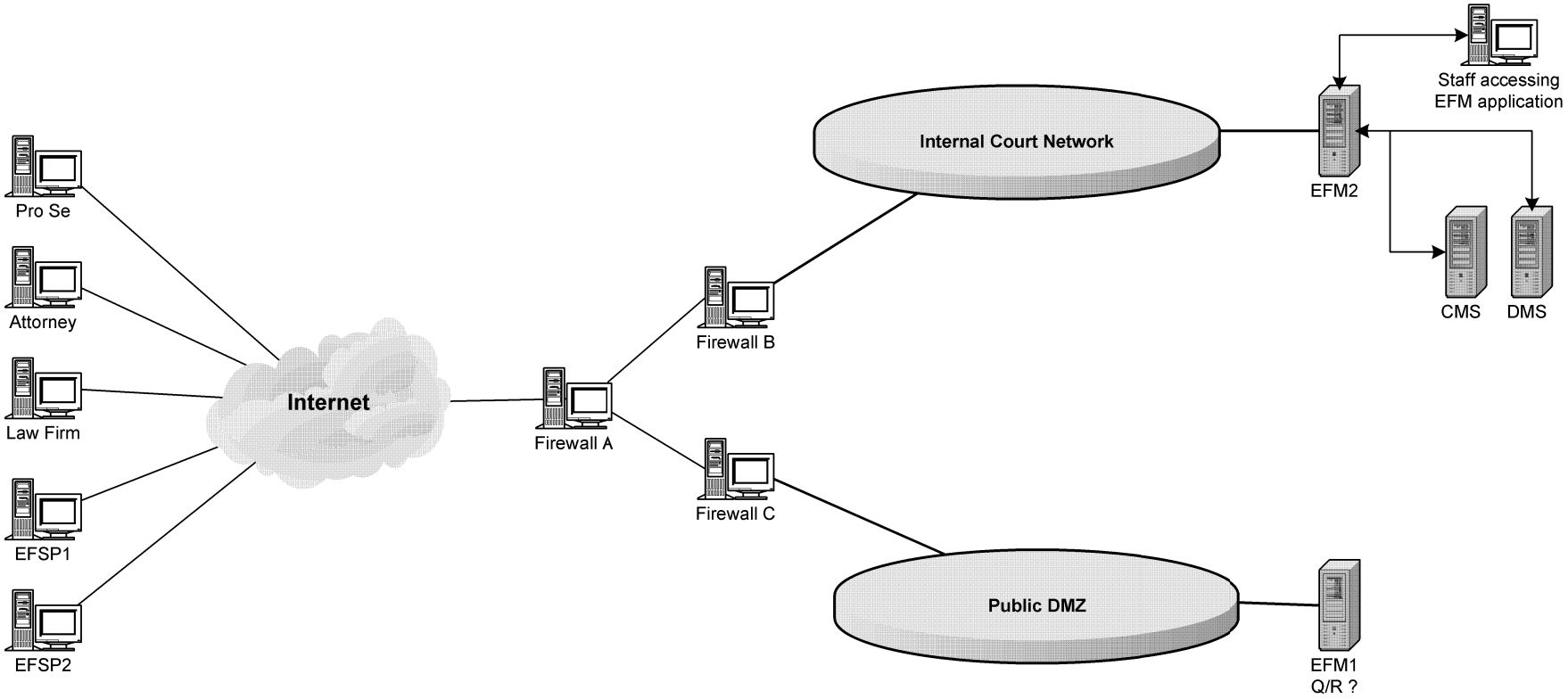
EFSP to EFM
Network Security
Recommendation



Since Network Security Rules would prohibit access to the Internal Court Network from anything outside Firewall B:

1 - EFSP submits IP address and Court assigns User ID and Password.
2 - EFSP IP address coded into ACL on Firewalls A and C.
3 - EFSPs send Filings to EFM1
4 - Firewalls A and B contain ACLs for EFSP IP#, which are the only authorized IP#s to access EFM1.
5 - EFM1 stores Filings temporarily and sends ACK for Filing Received back to EFSP.
6 - EFM2 periodically PULLs Filings from EFM1*. (EFM1 cannot initiate communication to EFM2)
7 - EFM2 processes other EFM activities as described by OXCI documentation.

* Some Security Administrators may allow EFM1 to PUSH data inside Court Network, but many will require EFM2 to initiate the communication as a PULL from the Inside network to the Public DMZ. This is the only way to protect the Internal network from vulnerabilities or attacks.

02/20/04 Allen Jensen
Orange County Superior Court
(949) 476-4984