

During implementation of FFIS it was suggested that IPSEC protocol be allowed on the firewall so that the VPN could be established. This protocol would allow any machine (from any IP address) running IPSEC to circumvent the Cisco PIX firewall. In order to limit access, specific changes were made so that only packets from 199.130.206.218 (NFC/FFIS) and 165.221.54.97 (FDW for Brio) can pass through the firewall.

Again, Marty Schneeman is running a Cisco PIX firewall which the syntax below is specific for. Other firewalls may have other ways to limit the IPSEC implementation. There is no known risk associated with IPSEC, but Marty tries to limit holes in the firewall.

----- For FFIS / Verspath

```
conduit permit esp any host 199.130.206.218
conduit permit ah any host 199.130.206.218
conduit permit udp any eq isakmp host 199.130.206.218
conduit permit tcp any eq 36865 host 199.130.206.218
conduit permit tcp any eq 22 host 199.130.206.218
```

----- For BRIO

```
conduit permit esp any host 165.221.54.97
conduit permit ah any host 165.221.54.97
conduit permit udp any eq isakmp host 165.221.54.97
conduit permit tcp any eq 22 host 165.221.54.97
```

esp- encapsulating security payload (RFC 1827)
ah- authentication header (RFC 2402)
isakmp- internet security association and key management protocol
22- secure shell

The 36865 port is necessary for VersaPath because that is a Kasten-Chase product

Mike Blum
ITS Beltsville
301-504-6182 X436