

```

/*
* C:\fritzbox.cfg
* Thu Jun 07 10:49:09 2007
*/

vpncfg {
    connections {
        enabled = yes;
        conn_type = conn_type_lan;
        name = "bintec";
        always_renew = no;
        reject_not_encrypted = no;
        dont_filter_netbios = yes;
        localip = 0.0.0.0;
        local_virtualip = 169.254.1.1;
        remoteip = 0.0.0.0;
        remote_virtualip = 0.0.0.0;
        remotehostname = "vpn-test.bintec.de";
        localid {
            user_fqdn = "vpn-test@bintec.de";
        }
        mode = phase1_mode_aggressive;
        phase1ss = "all/all/all";
        keytype = connkeytype_pre_shared;
        key = "supersecretgeheimkey";
        cert_do_server_auth = no;
        use_nat_t = no;
        use_xauth = no;
        use_cfgmode = no;
        phase2ss = " esp-all-all/ah-none/comp-all/pfs ";
        accesslist = "permit ip any 192.168.100.0 255.255.255.0";
    }
    ike_forward_rules = "udp 0.0.0.0:500 0.0.0.0:500",
                        "udp 0.0.0.0:4500 0.0.0.0:4500";
}

// EOF

```

| Name der Verbindung (keine Zugangsdaten)

| Internetnutzung während VPN verbieten
| Sämtliches NetBIOS ausgehend Filtern

| Eigene virtuelle IP-Adresse

| DynDNS-Name der Gegenstelle

| Eigene Identität IKE-Phase 1

| Modus der IKE-Phase 1 (Aggressive)
| Sicherheitsstrategie IKE-Phase 1

| Preshared Key (Kennwort)

| Sicherheitsstrategie IKE-Phase 2 (IPSEC)
| Erlaubte Netzwerke bzw. Hosts