Complete SRX220H Cluster with Radius authentication and IP assignment based Dynamic VPN and Shrewsoft VPN client

SRX side:

```
version 10.4R1.9;
groups {
    node0 {
        system {
            host-name BARACK_1;
        }
        interfaces {
            fxp0 {
                unit 0 {
                    family inet {
                        address 10.10.10.254/24;
                    }
                }
            }
        }
    }
    node1 {
        system {
            host-name BARACK_2;
        }
        interfaces {
            fxp0 {
                unit 0 {
                    family inet {
                        address 10.10.10.253/24;
                    }
                }
            }
        }
    }
    global {
        system {
            backup-router destination 0.0.0.0/0;
        }
    }
}
apply-groups "${node}";
system {
    time-zone Europe/Budapest;
    authentication-order [ radius password ];
    root-authentication {
        encrypted-password #######    }
    name-server {
        192.168.29.2;
        192.168.20.4;
    }
    radius-server {
        192.168.29.2 {
            port 1812;
            secret #######
        }
    }
```

```
radius-options {
    password-protocol mschap-v2;
    attributes {
        nas-ip-address 10.0.1.1;
    }
}
login {
    user network-ro-users {
        uid 2002;
        class read-only;
    }
    user network-rw-users {
        uid 2003;
        class super-user;
    }
}
services {
    ssh;
    telnet;
    xnm-clear-text;
    dns {
        forwarders {
            152.66.115.1;
        }
    }
    web-management {
        https {
            system-generated-certificate;
            interface [ reth0.1000 reth0.29 ];
        }
    }
}
syslog {
    archive size 100k files 3;
    user * {
        any emergency;
    }
    file messages {
        any critical;
        authorization info;
    }
    file interactive-commands {
        interactive-commands error;
    }
    file traffic-log {
        any any;
        match RT_FLOW_SESSION;
    }
}
max-configurations-on-flash 5;
max-configuration-rollbacks 5;
license {
    autoupdate {
        url https://ae1.juniper.net/junos/key_retrieval;
    }
}
processes {
    general-authentication-service {
```

```
            traceoptions {
                file auth-debug;
                flag all;
            }
        }
    }
    ntp {
        server 148.6.0.1;
    }
}
chassis {
    cluster {
        control-link-recovery;
        reth-count 3;
        redundancy-group 1 {
            node 0 priority 1;
            node 1 priority 100;
            preempt;
            interface-monitor {
                ge-0/0/0 weight 255;
                ge-0/0/2 weight 255;
                ge-3/0/2 weight 255;
                ge-3/0/0 weight 255;
                ge-0/0/3 weight 255;
                ge-3/0/3 weight 255;
            }
        }
        redundancy-group 0 {
            node 0 priority 1;
            node 1 priority 100;
        }
    }
}
interfaces {
    ge-0/0/0 {
        gigether-options {
            redundant-parent reth0;
        }
    }
    ge-0/0/2 {
        gigether-options {
            redundant-parent reth1;
        }
    }
    ge-0/0/3 {
        gigether-options {
            redundant-parent reth2;
        }
    }
    ge-3/0/0 {
        gigether-options {
            redundant-parent reth0;
        }
    }
    ge-3/0/2 {
        gigether-options {
            redundant-parent reth1;
        }
```

```
}
ge-3/0/3 {
    gigether-options {
        redundant-parent reth2;
    }
}
fab0 {
    description "Cluster fabric communications ONLY!";
    fabric-options {
        member-interfaces {
            ge-0/0/1;
        }
    }
}
fab1 {
    description "Cluster fabric communications ONLY!";
    fabric-options {
        member-interfaces {
            ge-3/0/1;
        }
    }
}
reth0 {
    description "Redundant TRUST trunk";
    vlan-tagging;
    mtu 1492;
    redundant-ether-options {
        redundancy-group 1;
    }
    unit 29 {
        description "VLAN_29 network";
        vlan-id 29;
        family inet {
            address 192.168.29.1/24;
        }
    }
    unit 1000 {
        description "Management network";
        vlan-id 1000;
        family inet {
            address 10.0.1.1/24;
        }
    }
}
reth1 {
    description "Redundant UNTRUST trunk";
    vlan-tagging;
    mtu 1492;
    redundant-ether-options {
        redundancy-group 1;
    }
    unit 3 {
        description "Internet_2 network";
        vlan-id 3;
    }
    unit 50 {
        description "Internet_1 network";
        vlan-id 50;
```

```
            family inet {
                address 1.1.1.234/27 {
                    primary;
                    preferred;
                }
            }
        }
    }
    reth2 {
        description "Redundant DMZ trunk";
        vlan-tagging;
        mtu 1492;
        redundant-ether-options {
            redundancy-group 1;
        }
        unit 1002 {
            description "VLAN_1002 DMZ";
            vlan-id 1002;
            family inet {
                address 10.0.2.1/24;
            }
        }

        unit 1003 {
            vlan-id 1003;
            family inet {
                address 10.0.3.1/24;
            }
        }
    }
    st0 {
        unit 0 {
            family inet;
        }
        unit 1 {
            family inet;
        }
        unit 2 {
            family inet;
        }
    }
}
forwarding-options {
    helpers {
        bootp {
            relay-agent-option;
            description "dhcp relay to dhcp server";
            server 10.0.3.2;
            maximum-hop-count 5;
            interface {
                reth2.1003;
            }
        }
    }
}
routing-options {
    interface-routes {
        rib-group inet default;
```

```
    }
    static {
        rib-group default;
        route 192.168.20.0/24 next-hop st0.0;
        route 0.0.0.0/0 next-hop 1.1.1.225;
        route 192.168.3.0/24 next-hop st0.0;
    }
    rib-groups {
        default {
            import-rib [ inet.0 Internet1-vlan50.inet.0 Internet2-
vlan3.inet.0 ];
        }
    }
}
protocols {
    stp;
}
security {
    ike {
        traceoptions {
            file ikelog files 5;
            flag all;
        }
        respond-bad-spi;
        proposal pre-g2-aes128-md5 {
            authentication-method pre-shared-keys;
            dh-group group2;
            authentication-algorithm md5;
            encryption-algorithm aes-128-cbc;
            lifetime-seconds 28800;
        }
        proposal pre-g2-3des-md5 {
            authentication-method pre-shared-keys;
            dh-group group2;
            authentication-algorithm md5;
            encryption-algorithm 3des-cbc;
            lifetime-seconds 28800;
        }

     ##shrew proposal

           proposal shrewsoft-psk {
            authentication-method pre-shared-keys;
            dh-group group5;
            authentication-algorithm sha1;
            encryption-algorithm aes-256-cbc;
            lifetime-seconds 180;
        }
        policy ike_HQ_MGMT {
            mode main;
            description "HQ_MGMT";
            proposals pre-g2-3des-md5;
            pre-shared-key ascii-text #####
        }
     ## UserVPN policy

     policy ike_UserVPN {
           mode aggressive;
```

```
            proposals shrewsoft-psk;
            pre-shared-key ascii-text #####
        }
        gateway gw_HQ_MGMT {
            ike-policy ike_HQ_MGMT;
            address 6.6.6.6;
            no-nat-traversal;
            local-identity hostname host.domain.com;
            external-interface reth1.50;
        }
      ## UserVPN gateway

        gateway gw_UserVPN {
            ike-policy ike_UserVPN;
            dynamic {
                hostname vpn.domain.com;
                connections-limit 50;
                ike-user-type shared-ike-id;
            }
            no-nat-traversal;
            external-interface reth1.50;
            xauth access-profile prof_UserVPN;
        }
    }
    ipsec {
        traceoptions {
            flag all;
        }
        proposal g2-esp-aes128-md5 {
            protocol esp;
            authentication-algorithm hmac-md5-96;
            encryption-algorithm aes-128-cbc;
            lifetime-seconds 3600;
            lifetime-kilobytes 32768;
        }

## Phase2 shrewsoft proposal

        proposal shrewsoft {
            protocol esp;
            authentication-algorithm hmac-sha1-96;
            encryption-algorithm aes-256-cbc;
            lifetime-seconds 3600;
        }
        policy ipsec_VLAN_29_MGMT {
            perfect-forward-secrecy {
                keys group2;
            }
            proposals g2-esp-aes128-md5;
        }
        policy ipsec_USERVPN {
            perfect-forward-secrecy {
                keys group5;
            }
            proposals shrewsoft;
        }
        vpn HQ_VLAN_29 {
            bind-interface st0.0;
```

```
        vpn-monitor {
            optimized;
        }
        ike {
            gateway gw_HQ_MGMT;
            ipsec-policy ipsec_VLAN_29_MGMT;
        }
        establish-tunnels immediately;
    }
    vpn USERVPN {
        ike {
            gateway gw_UserVPN;
            ipsec-policy ipsec_USERVPN;
        }
    }
}
nat {
    source {
        rule-set trust-to-untrust {
            from zone trust;
            to zone untrust;
            rule allow_internet {
                match {
                    source-address 192.168.29.0/24;
                    destination-address 0.0.0.0/0;
                }
                then {
                    source-nat {
                        interface;
                    }
                }
            }
        }
    }
    destination {
        pool SERVER1 {
            address 192.168.29.4/32;
        }
        rule-set nat_to_SERVER1 {
            from interface reth1.50;
            rule nat_rule_to_SERVER1 {
                match {
                    destination-address 5.5.5.5/32;
                }
                then {
                    destination-nat pool SERVER1;
                }
            }
        }
    }
    proxy-arp {
        interface reth1.50 {
            address {
                5.5.5.5/32;
            }
        }
        interface reth2.1003 {
            address {
```

```
                10.0.3.100/24 to 10.0.3.200/24;
            }
        }
    }
}
screen {
    ids-option untrust-screen {
        icmp {
            ping-death;
        }
        ip {
            source-route-option;
            tear-drop;
        }
        tcp {
            syn-flood {
                alarm-threshold 1024;
                attack-threshold 200;
                source-threshold 1024;
                destination-threshold 2048;
                timeout 20;
            }
            land;
        }
    }
}
zones {
    security-zone trust {
        address-book {
            address VLAN_29 192.168.29.0/24;
            address SERVER1 192.168.29.4/32;
            address SERVER2 192.168.29.2/32;
            address MGMT 10.0.1.0/24;
        }
        host-inbound-traffic {
            system-services {
                all;
            }
            protocols {
                all;
            }
        }
        interfaces {
            reth0.1000;
            reth0.29;
        }
    }
    security-zone untrust {
        address-book {
            address BARACK_reth1.50 1.1.1.3/32;
            address INTERNET 0.0.0.0/0;
            address BARACK_REMOTE_HTTPS 1.1.1.3/32;
                     }

       screen untrust-screen;
        host-inbound-traffic {
            system-services {
                ike;
```

```
            }
        }
        interfaces {
            reth1.50 {
                host-inbound-traffic {
                    system-services {
                        ssh;
                        telnet;
                        ping;
                        https;
                        ike;
                    }
                }
            }
            reth1.3 {
                host-inbound-traffic {
                    system-services {
                        ssh;
                        telnet;
                        ping;
                        https;
                        ike;
                    }
                }
            }
        }
    }
    security-zone VPN {
        address-book {
            address HQ 192.168.20.0/24;
                    }
        host-inbound-traffic {
            system-services {
                all;
            }
            protocols {
                all;
            }
        }
        interfaces {
            st0.1;
            st0.2;
            st0.0;
        }
    }
    security-zone DMZ {
        interfaces {
            reth2.1002;
        }
    }
##dedicated zone for user vpn
    security-zone USERVPN {
        host-inbound-traffic {
            system-services {
                any-service;
            }
        }
        interfaces {
```

```
            reth2.1003;
        }
    }
}
policies {
    traceoptions {
        file policy;
        flag all;
    }
    from-zone VPN to-zone trust {
        policy from_HQ_to_MGMT {
            match {
                source-address HQ;
                destination-address MGMT;
                application any;
            }
            then {
                permit;
                log {
                    session-init;
                }
                count;
            }
        }
        policy from_HQ_to_VLAN_29 {
            match {
                source-address HQ;
                destination-address VLAN_29;
                application any;
            }
            then {
                permit;
                log {
                    session-init;
                }
                count;
            }
        }
    }
    from-zone trust to-zone VPN {
        policy from_MGMT_to_HQ {
            match {
                source-address MGMT;
                destination-address HQ;
                application ICMP;
            }
            then {
                permit;
            }
        }
        policy from_VLAN_29_to_HQ {
            match {
                source-address VLAN_29;
                destination-address HQ;
                application any;
            }
            then {
                permit;
```

```
                log {
                    session-init;
                }
                count;
            }
        }
            }
        }
    }
    from-zone trust to-zone untrust {
        policy from_VLAN29_to_Internet {
            match {
                source-address VLAN_29;
                destination-address any;
                application any;
            }
            then {
                permit;
            }
        }
        policy any-permit {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit;
            }
        }
    }
    from-zone trust to-zone trust {
        policy from_VLAN_29_to_PAC-MGMT {
            match {
                source-address VLAN_29;
                destination-address MGMT;
                application [ junos-ssh junos-https junos-icmp-ping
];
            }
            then {
                permit;
            }
        }
    }
    from-zone untrust to-zone trust {
        policy from_INTERNET_to_SERVER1 {
            match {
                source-address any;
                destination-address PAC_BIX_SERVER1;
                application any;
            }
            then {
                permit;
            }
        }
        policy from_INTERNET_to_SERVER1-SMTP {
            match {
                source-address [ INTERNET ];
```

```
                    destination-address SERVER1;
                    application junos-smtp;
                }
                then {
                    permit;
                }
            }
        }
##tunnel to uservpn zone

        from-zone untrust to-zone USERVPN {
            policy tun_UserVPN {
                match {
                    source-address any;
                    destination-address any;
                    application any;
                }
                then {
                    permit {
                        tunnel {
                            ipsec-vpn USERVPN;
                        }
                    }
                }
            }
        }
##allow traffic from uservpn to another nets

        from-zone USERVPN to-zone VPN {
            policy from_UserVPN_to_HQ {
                match {
                    source-address any;
                    destination-address any;
                    application any;
                }
                then {
                    permit;
                }
            }
        }
        default-policy {
            deny-all;
        }
    }

      #reduce mss to avoid large packets
      flow {
        tcp-mss {
            all-tcp {
                mss 1350;
            }
            ipsec-vpn {
                mss 1350;
            }
        }
    }
##dynamic vpn profile
```

```
    dynamic-vpn {
        force-upgrade;
        access-profile prof_UserVPN;
        clients {
            USERVPN-Group {
                remote-protected-resources {
                    192.168.20.0/24;
                    192.168.29.0/24;
                }
                ipsec-vpn USERVPN;
                user {
           ## Usernames must EXACTLY the same as in Active Directory pre-
win2k name
                    user1;
                    user2;
                    user3;
                    user4;
                    user5;
                }
            }
        }
    }
}
firewall {
    family inet {
        filter ISP-filter {
            term to_Internet1-vlan50 {
                from {
                    source-address {
                        1.1.1.234/32;
                    }
                }
                then {
                    routing-instance Internet1-vlan50;
                }
            }
            term to_Internet2-vlan3 {
                from {
                    source-address {
                        3.3.3.4/32;
                    }
                }
                then {
                    routing-instance Internet2-vlan3;
                }
            }
            term default {
                then accept;
            }
        }
    }
}
##Radius authentication

access {
    profile prof_UserVPN {
        authentication-order radius;
        address-assignment {
```

```
            pool pool_UserVPN;
        }
        radius-server {
            192.168.29.2 secret ##### SECRET-DATA
        }
    }
    address-assignment {
        pool pool_UserVPN {
            family inet {
                network 10.0.3.0/24;
                range xauthip_UserVPN {
                    low 10.0.3.100;
                    high 10.0.3.200;
                }
                xauth-attributes {
                    primary-dns 192.168.29.2/32;
                    primary-wins 192.168.29.2/32;
                }
            }
        }
    }
    firewall-authentication {
        web-authentication {
            default-profile PACUserVPN;
        }
    }
}
routing-instances {
    Internet2-vlan3 {
        routing-options {
            static {
                route 0.0.0.0/0 next-hop 3.3.3.1;
            }
        }
    }
    Internet1-vlan50 {
        routing-options {
            static {
                route 0.0.0.0/0 next-hop 1.1.1.225;
            }
        }
    }
}
applications {
    application ICMP protocol icmp;
    application HTTPS {
        protocol ipip;
        destination-port https;
    }
    application HTTP {
        protocol ipip;
        destination-port http;
    }
    application SSH_22 {
        protocol ipip;
        destination-port ssh;
    }
    application-set MGMT_protocols {
```

```
        application HTTPS;
        application HTTP;
        application SSH_22;
        application ICMP;
    }
}
```

Shrew profile export:

Some notes:

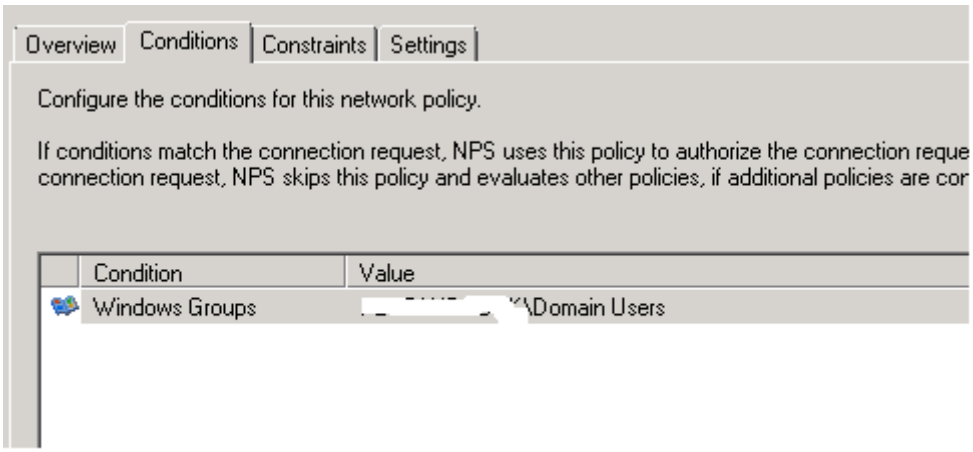
- use IKE config push method,
- use radius for IP assignment
- use 180 sec IKE phase1 key life-time
- use 2.2 alpha11 version

```
n:version:4
n:network-ike-port:500
n:network-mtu-size:1380
n:client-addr-auto:1
n:network-natt-port:4500
n:network-natt-rate:15
n:network-frag-size:540
n:network-dpd-enable:0
n:client-banner-enable:1
n:network-notify-enable:1
n:client-wins-used:0
n:client-wins-auto:1
n:client-dns-used:1
n:client-dns-auto:0
n:client-splitdns-used:1
n:client-splitdns-auto:0
n:phase1-dhgroup:5
n:phase1-keylen:256
n:phase1-life-secs:180
n:phase1-life-kbytes:0
n:vendor-chkpt-enable:0
n:phase2-keylen:256
n:phase2-life-secs:3600
n:phase2-life-kbytes:0
n:policy-nailed:0
n:policy-list-auto:0
n:client-dns-suffix-auto:0
s:network-host:1.1.1.234
s:client-auto-mode:push
s:client-iface:virtual
s:network-natt-mode:enable
s:network-frag-mode:enable
s:client-dns-addr:192.168.29.2
s:client-dns-suffix:domain.com
s:client-splitdns-list:domain.com
s:auth-method:mutual-psk-xauth
s:ident-client-type:fqdn
s:ident-server-type:any
s:ident-client-data:vpn.domain.com
b:auth-mutual-psk:xxxx
s:phase1-exchange:aggressive
```

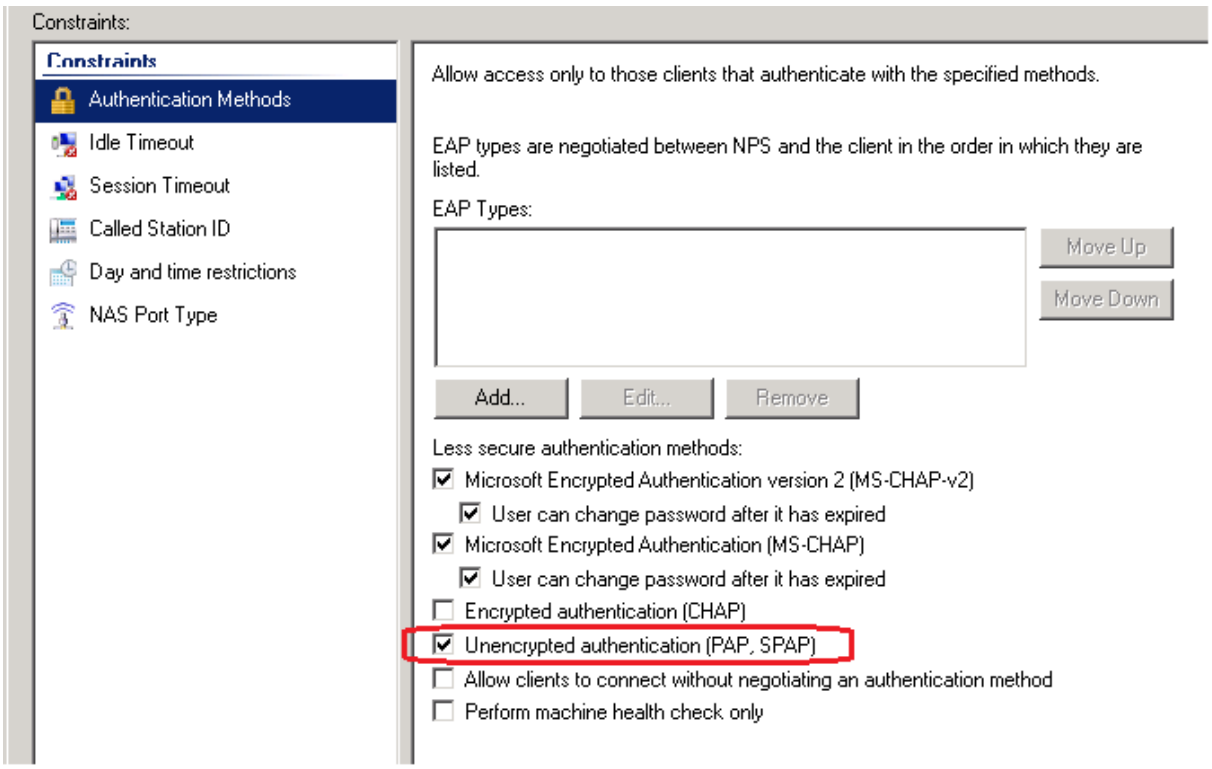
```
s:phase1-cipher:aes
s:phase1-hash:sha1
s:phase2-transform:esp-aes
s:phase2-hmac:sha1
s:ipcomp-transform:disabled
n:phase2-pfsgroup:5
s:policy-level:auto
s:policy-list-include:192.168.0.0 / 255.255.0.0
```

Windows 2k8 NPS settings:

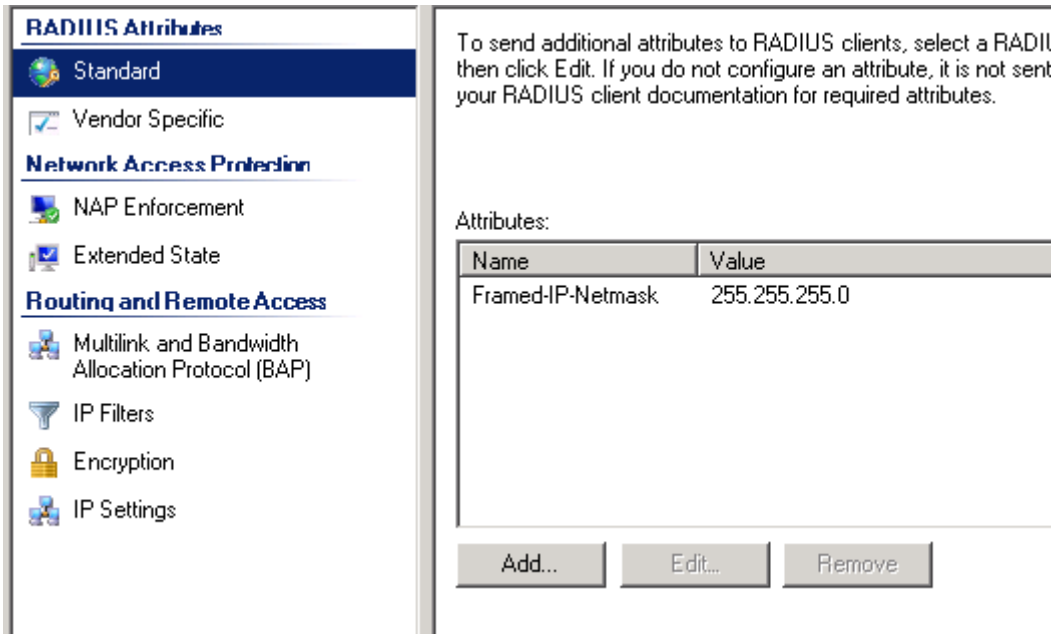
match to a windows group:



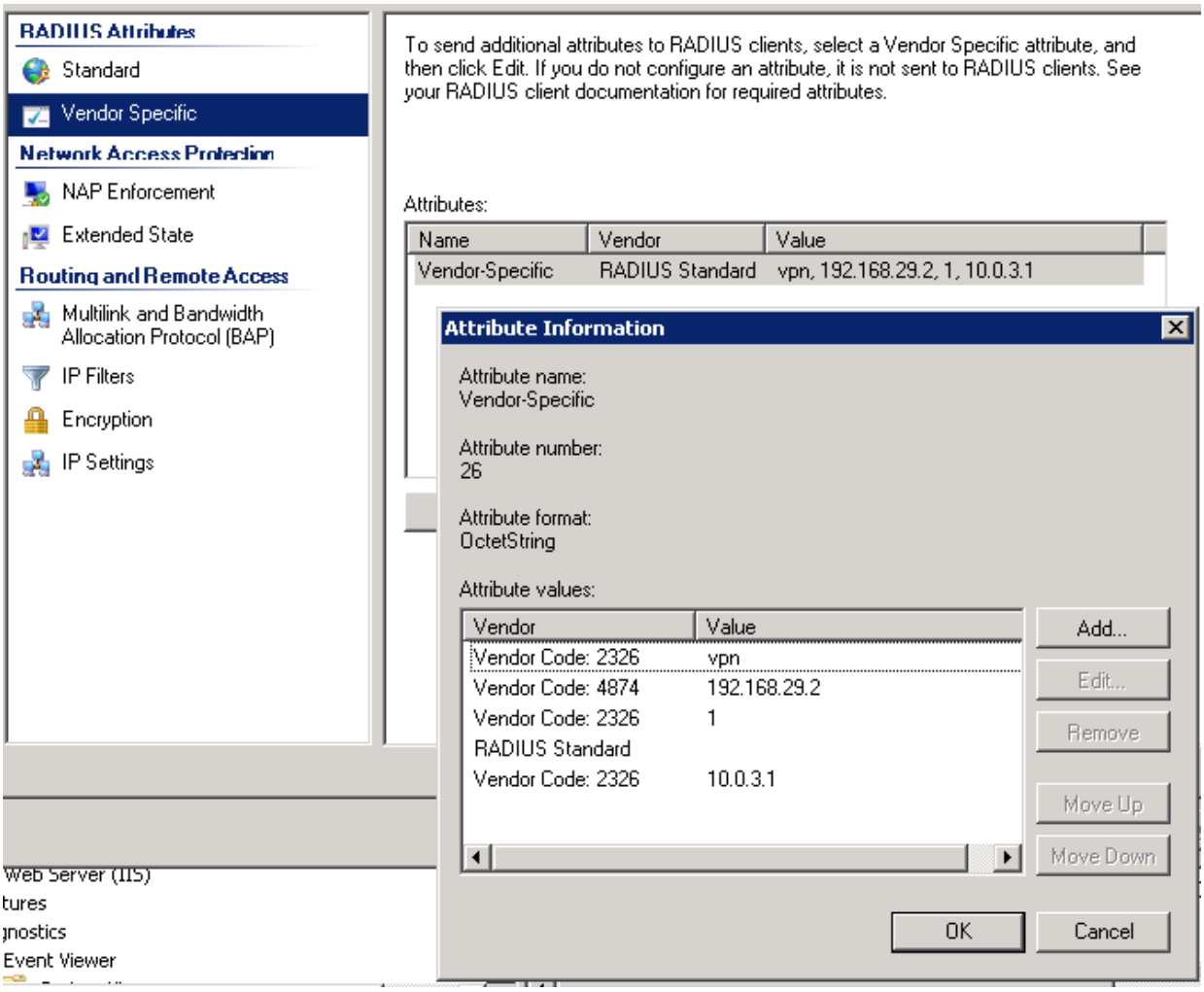
MUST use PAP:



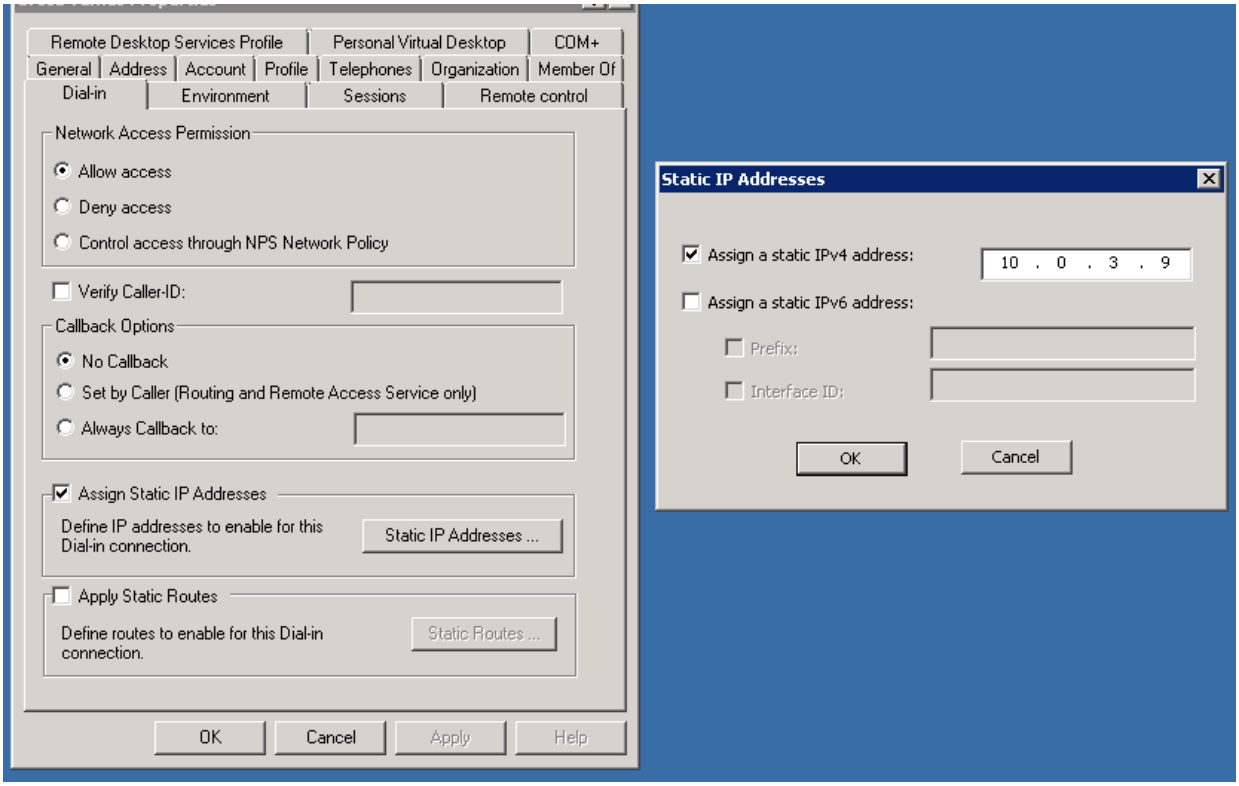
Framed pool assignment:



Custom RADIUS attributes (attribute definitions here: http://www.juniper.net/techpubs/software/junos/junos90/swconfig-system-basics/configuringradius-attributes-for-l2tp.html



Use ADUC dial-in properties of user to assign IP address:



And verifications:

```
root@BARACK_1> show security ike security-associations index 40 detail
node0:
--------------------------------------------------------------------------
-
IKE peer x.x.x.x, Index 40,
  Role: Responder, State: UP
  Initiator cookie: 890ffa91e2c5e13e, Responder cookie: 51d2b5bb15aa73ed
  Exchange type: Aggressive, Authentication method: Pre shared keys with
XAuth (initiator)
  Local: 1.1.1.234:500, Remote: x.x.x.x:55004
  Lifetime: Expires in 115 seconds
  Peer ike-id: vpn.domain.com
  Xauth user-name: user1
  Xauth assigned IP: 10.0.3.9
  Algorithms:
   Authentication        : sha1
   Encryption            : aes-cbc (256 bits)
   Pseudo random function: hmac-sha1
  Traffic statistics:
   Input  bytes  :                850
   Output bytes  :                896
   Input  packets:                  5
   Output packets:                  7
  Flags: Caller notification sent
  IPSec security associations: 0 created, 0 deleted
  Phase 2 negotiations in progress: 2
```

```
    Flags: Caller notification sent, Waiting for done

root@BARACK_1> show security ipsec security-associations detail
node0:

  Virtual-system: root
  Local Gateway: 1.1.1.225, Remote Gateway: x.x.x.x
  Local Identity: ipv4_subnet(any:0,[0..7]=192.168.0.0/16)
  Remote Identity: ipv4(any:0,[0..3]=10.0.3.9)
    DF-bit: clear
    Policy-name: tun_UserVPN

    Direction: inbound, SPI: 371a40d, AUX-SPI: 0
                              , VPN Monitoring: -
    Hard lifetime: Expires in 2885 seconds
    Lifesize Remaining:  Unlimited
    Soft lifetime: Expires in 2328 seconds
    Mode: tunnel, Type: dynamic, State: installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: aes-cbc (256
bits)
    Anti-replay service: counter-based enabled, Replay window size: 64

    Direction: outbound, SPI: 4a5eb22d, AUX-SPI: 0
                              , VPN Monitoring: -
    Hard lifetime: Expires in 2885 seconds
    Lifesize Remaining:  Unlimited
    Soft lifetime: Expires in 2328 seconds
    Mode: tunnel, Type: dynamic, State: installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: aes-cbc (256
bits)
    Anti-replay service: counter-based enabled, Replay window size: 64
```

Good luck! by pingTomi 15/01/2011