**SSG5 Config** (Using MIP to access the second segment 192.168.2.#)

unset key protection enable

set clock timezone 0

set vrouter trust-vr sharable

set vrouter "untrust-vr"

exit

set vrouter "trust-vr"

unset auto-route-export

exit

set service "RDP\_custom" protocol tcp src-port 0-65535 dst-port 3389-3389

set alg appleichat enable

unset alg appleichat re-assembly enable

set alg sctp enable

set auth-server "Local" id 0

set auth-server "Local" server-name "Local"

set auth default auth server "Local"

set auth radius accounting port 1646

set admin name "admin"

set admin password "<admin password here>"

set admin auth web timeout 10

set admin auth dial-in timeout 3

set admin auth server "Local"

set admin format dos

set zone "Trust" vrouter "trust-vr"

set zone "Untrust" vrouter "trust-vr"

set zone "DMZ" vrouter "trust-vr"

set zone "VLAN" vrouter "trust-vr"

set zone "Untrust-Tun" vrouter "trust-vr"

set zone "Trust" tcp-rst

set zone "Untrust" block

unset zone "Untrust" tcp-rst

set zone "MGT" block

unset zone "V1-Trust" tcp-rst

unset zone "V1-Untrust" tcp-rst

set zone "DMZ" tcp-rst

unset zone "V1-DMZ" tcp-rst

unset zone "VLAN" tcp-rst

set zone "Untrust" screen tear-drop

set zone "Untrust" screen syn-flood

set zone "Untrust" screen ping-death

set zone "Untrust" screen ip-filter-src

set zone "Untrust" screen land

set zone "V1-Untrust" screen tear-drop

set zone "V1-Untrust" screen syn-flood

set zone "V1-Untrust" screen ping-death

set zone "V1-Untrust" screen ip-filter-src

set zone "V1-Untrust" screen land

set interface "ethernet0/0" zone "Null"

set interface "ethernet0/1" zone "DMZ"

set interface "ethernet0/2" zone "Untrust"

set interface "ethernet0/3" zone "Trust"

set interface "bgroup0" zone "Trust"

set interface bgroup0 port ethernet0/4

set interface bgroup0 port ethernet0/5

set interface bgroup0 port ethernet0/6

unset interface vlan1 ip

set interface ethernet0/2 ip 192.168.1.91/24

set interface ethernet0/2 route

set interface ethernet0/3 ip 192.168.3.1/24

set interface ethernet0/3 nat

set interface bgroup0 ip 192.168.2.1/24

set interface bgroup0 nat

unset interface vlan1 bypass-others-ipsec

unset interface vlan1 bypass-non-ip

set interface ethernet0/2 ip manageable

set interface ethernet0/3 ip manageable

set interface bgroup0 ip manageable

set interface ethernet0/2 manage ping

set interface ethernet0/2 manage ssh

set interface ethernet0/2 manage ssl

set interface ethernet0/2 manage web

unset interface ethernet0/3 manage telnet

unset interface ethernet0/3 manage snmp

unset interface bgroup0 manage telnet

unset interface bgroup0 manage snmp

set interface ethernet0/3 dhcp server service

set interface bgroup0 dhcp server service

set interface ethernet0/3 dhcp server enable

set interface bgroup0 dhcp server enable

set interface ethernet0/3 dhcp server option lease 1440000

set interface ethernet0/3 dhcp server option gateway 192.168.3.1

set interface ethernet0/3 dhcp server option domainname MyDomain

set interface ethernet0/3 dhcp server option dns1 192.168.1.1

set interface bgroup0 dhcp server option lease 1440000

set interface bgroup0 dhcp server option gateway 192.168.2.1

set interface bgroup0 dhcp server option domainname MyDomain

set interface bgroup0 dhcp server option dns1 192.168.1.1

set interface ethernet0/3 dhcp server ip 192.168.3.33 to 192.168.3.44

set interface bgroup0 dhcp server ip 192.168.2.130 to 192.168.2.135

unset interface ethernet0/3 dhcp server config next-server-ip

unset interface bgroup0 dhcp server config next-server-ip

set interface "ethernet0/2" mip 192.168.1.130 host 192.168.2.130 netmask 255.255.255.248 vr "trust-vr"

set interface "serial0/0" modem settings "USR" init "AT&F"

set interface "serial0/0" modem settings "USR" active

set interface "serial0/0" modem speed 115200

set interface "serial0/0" modem retry 3

set interface "serial0/0" modem interval 10

set interface "serial0/0" modem idle-time 10

set flow tcp-mss

unset flow no-tcp-seq-check

set flow tcp-syn-check

unset flow tcp-syn-bit-check

set flow reverse-route clear-text prefer

set flow reverse-route tunnel always

set domain MyDomain

set pki authority default scep mode "auto"

set pki x509 default cert-path partial

set dns host dns1 192.168.1.1

set dns host dns2 0.0.0.0

set dns host dns3 0.0.0.0

set address "Trust" "192.168.3.0/24" 192.168.3.0 255.255.255.0

set ippool "vpnclient" 10.10.1.100 10.10.1.120

set user "<Your\_user\_name>" uid 2

set user "<Your\_user\_name>" type xauth

set user "<Your\_user\_name>" password "<Your\_user\_name\_ password here>"

unset user "<Your\_user\_name>" type auth

set user "<Your\_user\_name>" "enable"

set user "User2" uid 3

set user "User2" type xauth

set user "User2" password "<User2\_ password here>"

unset user "User2" type auth

set user "User2" "enable"

set user "vpnclient\_ph1id" uid 1

set user "vpnclient\_ph1id" ike-id fqdn "client.DynName..org" share-limit 25

set user "vpnclient\_ph1id" type ike

set user "vpnclient\_ph1id" "enable"

set user-group "vpnclient\_group" id 1

set user-group "vpnclient\_group" user "vpnclient\_ph1id"

set crypto-policy

exit

set ike gateway "vpnclient\_gateway" dialup "vpnclient\_group" Aggr local-id "vpngw.DynName..org" outgoing-interface "ethernet0/2" preshare "<your\_Preshare\_key\_here>" proposal "pre-g2-3des-sha" "pre-g2-3des-md5" "pre-g2-aes128-sha" "pre-g2-aes128-md5"

set ike gateway "vpnclient\_gateway" dpd-liveness interval 30

unset ike gateway "vpnclient\_gateway" nat-traversal udp-checksum

set ike gateway "vpnclient\_gateway" nat-traversal keepalive-frequency 20

set ike gateway "vpnclient\_gateway" xauth server "Local"

unset ike gateway "vpnclient\_gateway" xauth do-edipi-auth

set ike respond-bad-spi 1

set ike ikev2 ike-sa-soft-lifetime 60

unset ike ikeid-enumeration

unset ike dos-protection

unset ipsec access-session enable

set ipsec access-session maximum 5000

set ipsec access-session upper-threshold 0

set ipsec access-session lower-threshold 0

set ipsec access-session dead-p2-sa-timeout 0

unset ipsec access-session log-error

unset ipsec access-session info-exch-connected

unset ipsec access-session use-error-log

set xauth default ippool "vpnclient"

set xauth default dns1 192.168.1.1

set xauth default dns2 4.2.2.2

set vpn "vpnclient\_tunnel" gateway "vpnclient\_gateway" replay tunnel idletime 0 proposal "nopfs-esp-3des-sha" "nopfs-esp-3des-md5" "nopfs-esp-aes128-sha" "nopfs-esp-aes128-md5"

set url protocol websense

exit

set policy id 1 from "Trust" to "Untrust" "Any" "Any" "ANY" permit log

set policy id 1

exit

set policy id 3 name "vpnclient\_inbound" from "Untrust" to "Trust" "Dial-Up VPN" "Any" "ANY" tunnel vpn "vpnclient\_tunnel" id 0x2 log

set policy id 3

exit

set policy id 5 from "Untrust" to "Trust" "Any" "MIP(192.168.1.130/29)" "ANY" permit log

set policy id 5

exit

set policy id 4 from "Untrust" to "Trust" "Any" "Any" "ANY" permit log

set policy id 4

exit

set nsmgmt bulkcli reboot-timeout 60

set ssh version v2

set ssh enable

set config lock timeout 5

unset license-key auto-update

set telnet client enable

set snmp port listen 161

set snmp port trap 162

set snmpv3 local-engine id "01621007003110"

set vrouter "untrust-vr"

exit

set vrouter "trust-vr"

unset add-default-route

set route 0.0.0.0/0 interface ethernet0/2 gateway 192.168.1.1

exit

set vrouter "untrust-vr"

exit

set vrouter "trust-vr"

exit

**ShrewSoft client config:**

n:version:2

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:1

n:client-banner-enable:1

n:network-notify-enable:1

n:client-wins-used:1

n:client-wins-auto:1

n:client-dns-used:1

n:client-dns-auto:1

n:client-splitdns-used:1

n:client-splitdns-auto:1

n:phase1-dhgroup:2

n:phase1-life-secs:86400

n:phase1-life-kbytes:0

n:vendor-chkpt-enable:0

n:phase2-life-secs:3600

n:phase2-life-kbytes:0

n:policy-nailed:1

n:policy-list-auto:1

s:network-host:DynName.dyndns.org

s:client-auto-mode:push

s:client-iface:virtual

s:network-natt-mode:enable

s:network-frag-mode:enable

s:auth-method:mutual-psk-xauth

s:ident-client-type:fqdn

s:ident-server-type:fqdn

s:ident-client-data:client.DynName.org

s:ident-server-data:vpngw.DynName.org

b:auth-mutual-psk:<your\_key\_Here>

s:phase1-exchange:aggressive

s:phase1-cipher:auto

s:phase1-hash:auto

s:phase2-transform:auto

s:phase2-hmac:auto

s:ipcomp-transform:disabled

n:phase2-pfsgroup:-1

s:policy-level:auto

s:client-saved-username:<Your\_user\_name>

Network:



MIP ip’s match from 192.168.1.130-135 to 192.138.2.130-135 automatically