```
## Last changed: 2016-05-27 18:55:49 GMT-8
version 12.1X46-D45.4;
groups {
    global {
        system {
            root-authentication {
                encrypted-password ...; ## SECRET-DATA
            }
        }
    }
}
system {
    host-name mrp-srx220;
    time-zone GMT-8;
    root-authentication {
        encrypted-password ...; ## SECRET-DATA
    }
    name-server {
        208.201.224.11;
        208.201.224.33;
        208.67.222.222;
        208.67.220.220;
    }
    name-resolution {
        no-resolve-on-input;
    }

    /* SSH User login */
    login {
        user admin {
            uid 2002;
            class super-user;
            authentication {
                ssh-rsa "ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAQEAogMU0RSBz8B1/xNSp7fkasjgSOB8MWxxHxH0owny3+jI3YunYWpCdX
XD4//l6/k007xSFb0QDb/Mjjz71Pe78CTAaYAjjETrk1lj56yktojqXi7eBayK8hYqVTV9UTirzOZNr5UGZh5EwMih617
Tytd8UApvPuEHhj2dsYzX2FtPaiNmLTKbC+g5HrY7E/9UYxBh1e2zWoDyjy9CtbNBHYMge6C2TXX2YzFSoCL2l
OdlBeoF8KYzJD1IZq2lNMU5CNeehZpYe2zQE+HPZ5Ah1IxQ/MIL/g9DutOx5lDpgadKr0cskcDRFPC0ooy29uwMU
9t674X3fHmIgb5UBEIxbw== admin@mrp-srx220"; ## SECRET-DATA
            }
        }
    }
    services {

        /* Prevent root from using SSH */
        ssh {
            root-login deny;
        }

        web-management {
            https {
                system-generated-certificate;
```

```
            interface [ ge-0/0/0.0 vlan.0 ];
        }

        session {
            idle-timeout 60;
        }
    }
}

syslog {
    archive size 100k files 3;
    user * {
        any emergency;
    }
    file messages {
        any critical;
        authorization info;
    }
    file interactive-commands {
        interactive-commands error;
    }
}
max-configurations-on-flash 5;
max-configuration-rollbacks 5;
license {
    autoupdate {
        url https://ae1.juniper.net/junos/key_retrieval;
    }
}
ntp {
    server us.ntp.pool.org;
}
}

interfaces {

/* Untrust Interface */

ge-0/0/0 {
    unit 0 {
        family inet {
            filter {
                /* This is for VOIP CoS */
                output voice-term;
            }
            address 198.27.134.230/28;
        }
    }
}

ge-0/0/1 {
    unit 0 {
        family ethernet-switching {
            vlan {
```

```
            members vlan0;
        }
    }
  }
}

ge-0/0/2 {
  unit 0 {
    family ethernet-switching {
      vlan {
        members vlan0;
      }
    }
  }
}

ge-0/0/3 {
  unit 0 {
    family ethernet-switching {
      vlan {
        members vlan0;
      }
    }
  }
}

/* Trust interface */

ge-0/0/4 {
  unit 0 {
    family ethernet-switching {
      vlan {
        members vlan0;
      }
    }
  }
}

ge-0/0/5 {
  unit 0 {
    family ethernet-switching {
      vlan {
        members vlan0;
      }
    }
  }
}

ge-0/0/6 {
  unit 0 {
    family ethernet-switching {
      vlan {
        members vlan0;
      }
```

```
        }
      }
    }

    ge-0/0/7 {
      unit 0 {
        family ethernet-switching {
          vlan {
            members vlan0;
          }
        }
      }
    }

    /* Loopback interface */

    lo0 {
      unit 0 {
        family inet {
          filter {

            /* This is to restrict management access to SRX */
            input lo-filter;
          }
        }
      }
    }

    vlan {
      unit 0 {
        family inet {
          address 192.168.254.254/24;
        }
      }
    }
  }

  routing-options {

    /* Static route to our gateway */
    static {
      route 0.0.0.0/0 next-hop 198.27.134.225;
    }
  }
  protocols {
    stp;
  }
  policy-options {
    prefix-list manager-ip {
      192.168.254.0/24;
    }
  }

  /* This is for VOIP CoS */
```

```
class-of-service {
    classifiers {
        inet-precedence corp-traffic {
            forwarding-class voice-class {
                loss-priority low code-points 101;
            }
            forwarding-class data-class {
                loss-priority high code-points 000;
            }
        }
    }
    forwarding-classes {
        queue 0 voice-class;
        queue 1 data-class;
    }
    interfaces {
        ge-0/0/0 {
            scheduler-map corp-map;
        }
        ge-0/0/4 {
            unit 0 {
                classifiers {
                    inet-precedence corp-traffic;
                }
            }
        }
    }
    scheduler-maps {
        corp-map {
            forwarding-class voice-class scheduler voice-sched;
            forwarding-class data-class scheduler data-sched;
        }
    }
    schedulers {
        voice-sched {
            buffer-size temporal 50;
            priority strict-high;
        }
        data-sched {
            priority low;
        }
    }
}


security {

    /* Phase 1 */
    ike {
        proposal Dynamic-VPN-P1-Proposal {
            description "Dynamic P1 Proposal";
            authentication-method pre-shared-keys;
            dh-group group2;
            authentication-algorithm sha1;
```

```
        encryption-algorithm 3des-cbc;
        lifetime-seconds 1200;
    }
    policy Dynamic-VPN-P2-Policy {
        mode aggressive;
        description "Dynamic P2 Policy";
        proposals Dynamic-VPN-P1-Proposal;
        pre-shared-key ascii-text ...; ## SECRET-DATA
    }
    gateway Dynamic-VPN-P1-Gateway {
        ike-policy Dynamic-VPN-P2-Policy;
        dynamic {
            hostname pacificmortgagecompany.com;
            connections-limit 5;
            ike-user-type shared-ike-id;
        }
        external-interface ge-0/0/0.0;
        xauth access-profile Dynamic-XAuth;
    }
}

/* Phase 2 */

ipsec {
    proposal Dynamic-P2-Proposal {
        description Dynamic-VPN-P2-Proposal;
        protocol esp;
        authentication-algorithm hmac-sha1-96;
        encryption-algorithm aes-256-cbc;
        lifetime-seconds 3600;
    }
    policy Dynamic-P2-Policy {
        perfect-forward-secrecy {
            keys group5;
        }
        proposals Dynamic-P2-Proposal;
    }
    vpn Dynamic-VPN {
        df-bit copy;
        ike {
            gateway Dynamic-VPN-P1-Gateway;
            ipsec-policy Dynamic-P2-Policy;
        }
        establish-tunnels immediately;
    }
}
alg {
    h323 disable;
    mgcp disable;
    sccp disable;
    sip disable;
    ike-esp-nat {
        enable;
    }
```

```
}

/* Dynamic VPN */

dynamic-vpn {
    force-upgrade;
    access-profile Dynamic-XAuth;
    clients {
        all {
            remote-protected-resources {
                192.168.254.0/24;
            }
            remote-exceptions {
                0.0.0.0/0;
            }
            ipsec-vpn Dynamic-VPN;
            user {
                jklein;
                mikem;
            }
        }
    }
}

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;
        }
    }
}
nat {
    source {
        rule-set nsw_srcnat {
            from zone Trust;
            to zone Internet;
            rule nsw-src-interface {
                match {
                    source-address 0.0.0.0/0;
                    destination-address 0.0.0.0/0;
```

```
            }
            then {
               source-nat {
                  interface;
               }
            }
         }
      }
   }
}

/* Policies */

policies {

   /* Trust to Internet */

   from-zone Trust to-zone Internet {
      policy All_Trust_Internet {
         match {
            source-address any;
            destination-address any;
            application any;
         }
         then {
            permit;
         }
      }
      policy NextivaOutbound {
         match {
            source-address any;
            destination-address [ NextivaInbound NextivaInbound2 ];
            application any;
         }
         then {
            permit;
         }
      }
   }

   /*Internet to Trust */

   from-zone Internet to-zone Trust {
      policy NextivaInbound {
         match {
            source-address [ NextivaInbound NextivaInbound2 ];
            destination-address any;
            application any;
         }
         then {
            permit;
         }
      }
      policy Dynamic-VPN {
```

```
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit {
                    tunnel {
                        ipsec-vpn Dynamic-VPN;
                    }
                }
            }
        }
    }
}

/* Zones */

zones {

    /* Trust */

    security-zone Trust {
        address-book {
            address Michael 192.168.254.0/24;
        }
        host-inbound-traffic {
            system-services {
                ping;
                http;
                https;
                ike;
            }
        }
        interfaces {
            vlan.0 {
                host-inbound-traffic {
                    system-services {
                        ping;
                        https;
                        ssh;
                        http;
                        ike;
                    }
                }
            }
        }
    }

    /* Internet */

    security-zone Internet {
        address-book {
            address Nextiva {
```

```
                range-address 208.73.144.1 {
                    to {
                        208.73.151.254;
                    }
                }
            }
            address NextivaInbound 208.73.144.0/21;
            address NextivaInbound2 208.89.108.0/22;
            address Untrust_interface 198.27.134.0/28;
        }
        host-inbound-traffic {
            system-services {
                ping;
                http;
                https;
                ike;
            }
        }
        interfaces {
            ge-0/0/0.0 {
                host-inbound-traffic {
                    system-services {
                        ping;
                        http;
                        https;
                        ike;
                    }
                }
            }
        }
    }

    /* Loopback Interface */
    security-zone lo0 {
        host-inbound-traffic {
            system-services {
                ping;
            }
        }
    }

    /* Junos-Host */

    security-zone junos-host;
  }
}

firewall {

  /* This is more QoS configuration */

  policer voice-excess {
    if-exceeding {
      bandwidth-limit 8m;
```

```
            burst-size-limit 1600000;
        }
        then out-of-profile;
    }
    filter voice-term {
        term 01 {
            from {
                forwarding-class voice-class;
            }
            then policer voice-excess;
        }
        term 02 {
            then accept;
        }
    }
    filter lo-filter {
        term limited-ip {
            from {
                source-prefix-list {
                    manager-ip;
                }
            }
            then accept;
        }
    }
}

/*Access Profiles */

access {

    /* Dynamic-XAuth is used for Dynamic VPN */

    profile Dynamic-XAuth {
        authentication-order password;
        client jklein {
            firewall-user {
                password ...; ## SECRET-DATA
            }
        }
        client mikem {
            firewall-user {
                password ...; ## SECRET-DATA
            }
        }
        address-assignment {
            pool Dynamic-VPN-Pool;
        }
    }

    /* Dynamic VPN address pool */

    address-assignment {
        pool Dynamic-VPN-Pool {
```

```
            family inet {
                network 192.168.254.0/24;
                xauth-attributes {
                    primary-dns 192.168.254.221/24;
                }
            }
        }
    }
    firewall-authentication {
        web-authentication {
            default-profile Dynamic-XAuth;
        }
    }
}
vlans {
    vlan0 {
        vlan-id 2;
        l3-interface vlan.0;
    }
}
```