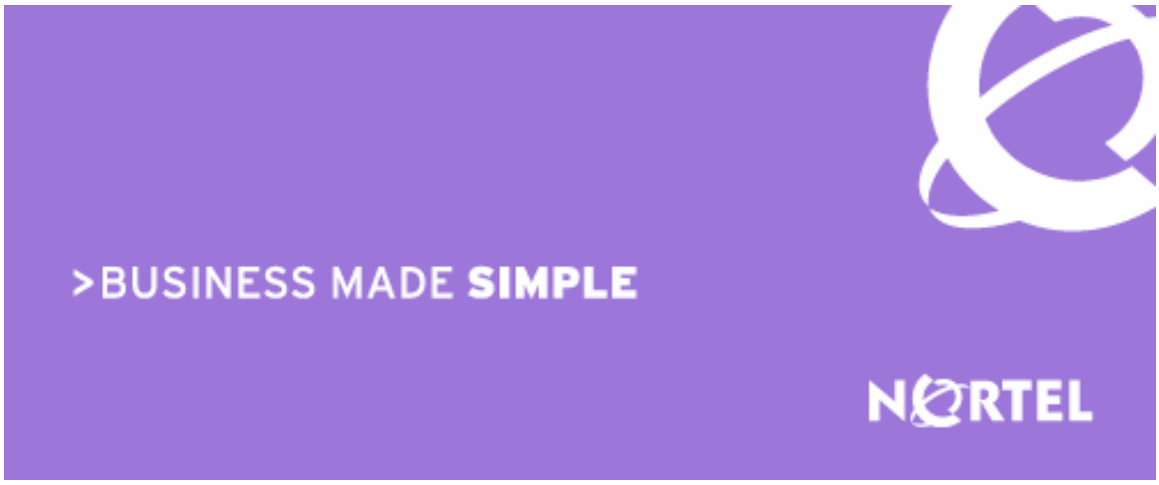


Nortel Secure Network Access
Release 1.5 - NSNA
Engineering

> Technical Configuration Guide for Network Access with NSNA and TunnelGuard for Non-SSCP Switches

Enterprise Solutions Engineering
Document Date: March, 2007
Document Version: 2.0

Nortel is a recognized leader in delivering communications capabilities that enhance the human experience, ignite and power global commerce, and secure and protect the world's most critical information. Serving both service provider and enterprise customers, Nortel delivers innovative technology solutions encompassing end-to-end broadband, Voice over IP, multimedia services and applications, and wireless broadband designed to help people solve the world's greatest challenges. Nortel does business in more than 150 countries. For more information, visit Nortel on the Web at nortel.com.

Disclaimer

This engineering document contains the best information available at the time of publication in terms of supporting the application and engineering of Nortel products in the customer environment. They are solely for use by Nortel customers and meant as a guide for network engineers and planners from a network engineering perspective. All information is subject to interpretation based on internal Nortel test methodologies which were used to derive the various capacity and equipment performance criteria and should be reviewed with Nortel engineering primes prior to implementation in a live environment.

Abstract

The purpose of this Technical Configuration Guide is to provide an example of setting up NSNA to allow wired and wireless users to gain access to the corporate network, but limit what applications they are allowed to use and what part of the corporate network they are allowed access. Any switch, access or core, could be used for this solution however it is recommended to use a switch that supports filtering at layer 2 and 3.

This document references the following products:

- Nortel Secure Network Access Switch (NSNA) software release 1.5.x.
- Nortel Ethernet Routing Switch 5500 (ERS5500)
- Nortel Ethernet Switch 470 (ES470)
- Nortel Ethernet Routing Switch 8600 (ERS8600)
- Nortel WLAN 2300 Series software release 5.0
- Legacy Cisco switches

Table of Contents

1. Overview: Non-SNAS Switch with TunnelGuard Authentication

The Nortel Secure Network Access Switch (SNAS) in the 1.5 release is capable of authenticating users from a non-Secure Switch Control Protocol (SSCP) switch, AP or hub using TunnelGuard with DHCP. Presently, only the ERS5500 and ERS8300 switches support SSCP. With the 1.5 release, SNAS is now capable of providing TunnelGuard authentication to users or devices connected to a non-SSCP switch, AP, or hub when configured in DHCP hub mode. DHCP hub mode can be used to extend NSNA functionality to third-party switches, other current Nortel products such as WLAN 2300 series or ES470 switches, or legacy devices.

The SNAS, when configured in DHCP hub mode, is assigned a single IP subnet where you assign a Red, Yellow, and Green IP address range from this single IP subnet. For non-registered devices – any device that has not performed authentication for TunnelGuard (TG) compliance checking – they will be allocated an IP address from the SNAS DHCP Red range. A small TTL value for the DHCP renewal process should be configured for the devices in the RED range. Once a client has authenticated, the device will be assigned a new IP address from either the Yellow or Green DHCP range. Please note that VLAN switching is not used. In other words, the non-SSCP switch will use the same VLAN so the Red, Yellow, and Red DHCP ranges must come from the same subnet.

1.1 Configuring SNAS for DHCP Hub Mode

When configuring DHCP on SNAS, it should be set up for hub mode for this application.

SNAS DHCP Hub Mode:

- Used with non-SSCP switches
- Uses a single IP subnet with a separate IP range within this subnet for the Red, Yellow, and Green NSNA access states
- The DNS return attribute for the Red DHCP range must point the virtual IP (VIP) address of the SNAS. This will forward all DNS queries to SNAS.
- The DNS return attribute for the Green DHCP range should use a valid DNS address or addresses. This will allow a device, once authenticated by TunnelGuard, to use valid DNS addressing.

1.2 Configuring the Non-SSCP Switch

For this application, any switch or hub can be used for this application. However, it is recommended that the access, wire-closet, or core switch supports the following security features:

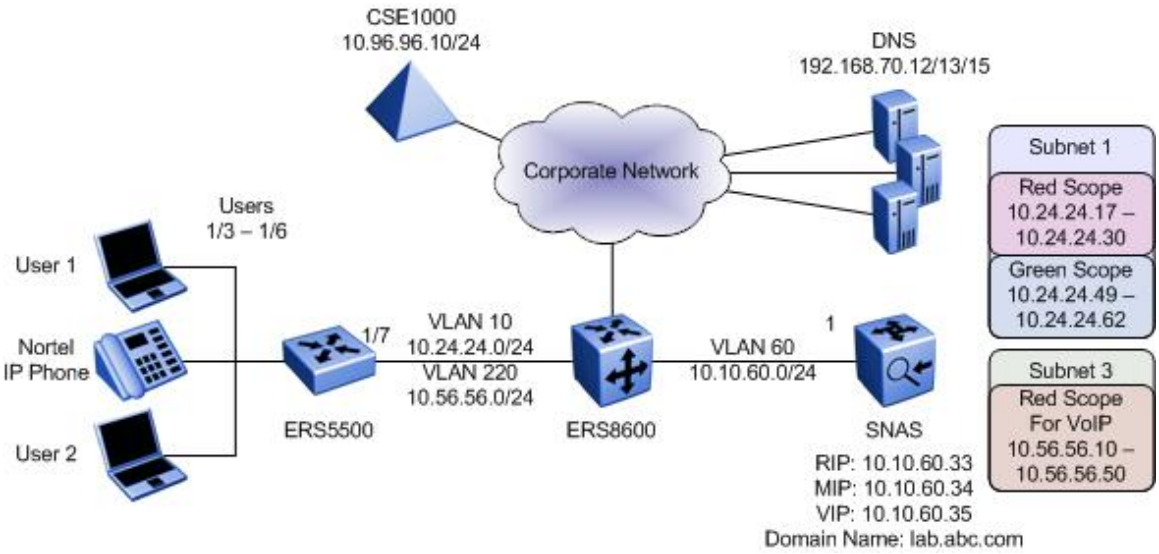
- Support filters or ACL’s to only forward DNS requests from a device within the SNAS Red DHCP range to the SNAS virtual IP (VIP). This will provide a DNS portal when a user first opens a browser, where the DNS query goes to SNAS to open up a TunnelGuard session to the end user.
- Setup additional filters or ACL’s on within the SNAS Red or Yellow DHCP range to only allow http to SNAS subnet, https to SNAS subnet, icmp, and dhcp traffic. All other traffic should be denied.

For additional security, DHCP Snooping and ARP inspection should be used if the access switch supports these features.

- DHCP Snooping with ARP inspection prevents a device from spoofing another IP address or changing to a static IP address within the Red, Yellow, or Green SNAS DHCP ranges.

2. Applying Non-SNAS Switch Filters at Access Layer

2.1 Configuration Example: ERS5520 using SNAS Hub Mode with Red and Green DHCP Range and Red Range for VoIP



For this configuration example, we wish to configure SNAS in DHCP Hub mode to supply a Red and Green DHCP range for the data users and another Red DHCP range for the Nortel IP Phone sets. The Red DHCP range for VLAN 10, the data VLAN, will also be configured with DHCP Option 191 to inform the Nortel IP Phone sets to use the Voice VLAN 220. This simply allows for TunnelGuard authentication for the data users to get to the core network via the SNAS Green DHCP range. Otherwise, via the Red DHCP range only, a user is only allowed DHCP, DNS to SNAS, ICMP, and HTTP/HTTPS to the SNAS subnet. In Section 3, we will add a remediation Yellow DHCP range to allow TunnelGuard to check for any number of attributes such as Antivirus revision level prior to letting a use onto the Green SNAS DHCP range.

Overall, we will configure the following:

- SNAS
  - Setup SNAS for DHCP Hub mode
  - Setup two data DHCP ranges, a Red range using a range of 10.24.24.16/28 with DHCP Option 191 and a Green range using a range of 10.24.24.48/28
  - Setup another DHCP range, a Red range using a range of 10.56.56.10-50 with DHCP Option 128 for the Nortel IP Phone sets
  - Set the DHCP lease time to 1 day
  - For this example, we will use local SNAS authentication and create two users named user1 and user2
- ERS5500
  - Setup the ERS5500 for Layer 2 operation using VLAN 10 and VLAN 220

- Configure the appropriate filters for the Red SNAS range to only allow DNS to the SNAS VIP
- Configure additional Red SNAS range filters to only allow HTTP and HTTPS to SNAS subnet, ICMP, and DHCP traffic. Deny all other traffic for the Red range
- Meter all Red Subnet HTTP/HTTPS traffic to 1000Kbps

NOTE: The Site Specific Option #191 pertains to the VLAN ID information that the IP Phone set will require for the voice VLAN. The format for the String pertaining to Option 128 is shown below. Note that the string always begins with 'VLAN-A' where 'A' refers to the revision of the Nortel DHCP/VLAN specification. The string must also end with a period (.).

VLAN-A:vvvv.

Where: "VLAN-A" = Option #191 begins with this string for all Nortel IP Phone Sets
"vvvv" = The VLAN ID in Decimal

For this example, enter the following:

- **VLAN-A:220.**

NOTE: The format of the String for Option #128 is as shown below. Note that the string always begins with 'Nortel-i2004-A' where 'A' refers to the revision of the Nortel DHCP/VLAN specification.

Nortel-i2004-A,iii.iii.iii.iii:ppppp,aaa,rrr;iii.iii.iii.iii:ppppp,aaa,rrr.

Where
"Nortel-i2004-A" = Option #128 begins with this string for all Nortel IP phone sets
"iii.iii.iii.iii" = the IP Address of the Call Server (S1 or S2)
"ppppp" = port number for the Call Server
"aaa" = the Action for the Server
"rrr" = the Retry Count for the Server

The IP Address must be separated from the port number by a colon (:). The parameters for the Primary (S1) and the Secondary (S2) Call Servers are separated by a semicolon (;). The string must end a period (.).

For this example, enter the following:

- **Nortel-i2004-A,10.96.96.10:5000,1,5.**

NOTE: Since the ERS5500 is configured for Layer 2, the ERS8600 must be configured with DHCP relay via VLAN 10 and VLAN 220. Configure a DHCP relay agent on ERS8600 pointing to SNAS MIP address of 10.10.60.34.

2.1.1 SNAS

Please follow the steps below to configure DHCP hub mode on SNAS as per the requirements listed above. An example of the complete configuration is provided in Appendix C.

1. Create subnet 1 using SNAS DHCP hub mode to be used for VLAN 10.

```
>> Main# /cfg/domain 1/dhcp/subnet 1
Creating Subnet 1
Select one of hub, filter and standard: hub
Set the subnet name: Subnet_1
Enter subnet network address: 10.24.24.0
Enter subnet network mask: 255.255.255.0

------------------------------------------------------------
[Subnet 1 Menu]
```

```
      type        - Set type
      name        - Set name
      address     - Set network address
      netmask     - Set network mask
      red         - Red vlan Settings menu
      yellow      - Yellow vlan Settings menu
      green       - Green vlan Settings menu
      ena         - Enable subnet
      dis         - Disable subnet
      del         - Remove Subnet

>> Subnet 1#

>> Subnet 1# ena
```

NOTE: If you try to apply the changes now, you will be notified with the following error message:

Invalid setting for AAA/Xnet/1/SAC/DHCP/StdOpts. Required standard options not configured: [3,6,15,51]

This is indicating that you must at minimum set the following DHCP options:

- DHCP Option 3: Default Router
- DHCP Option 6: Domain Name Server
- DHCP Option 15: Domain Name
- DHCP Option 51: Lease time

2. Create the Global DHCP standard options.

NOTE: These options will be applied to all SNAS ranges by default. You can still override these default settings by setting up the DHCP options under Red/Yellow/Green ranges.

NOTE: The DHCP lease time, standard option 51, is expressed in seconds. For this example, we will set DHCP option 51 to 86,400 seconds which translates to 1 day.

```
>> DHCP# /cfg/domain 1/dhcp

------------------------------------------------------------
[DHCP Menu]
      subnet      - DHCP subnet menu
      stdopts     - Standard options menu
      vendopts    - Vendor options menu

>> DHCP#

>> DHCP# stdopts 3
Creating Standard Options 3
Set the standard option value: 10.24.24.1

------------------------------------------------------------
[Standard Options 3 Menu]
      name        - Name
      value       - Set value
      del         - Remove Standard Options

>> Standard Options 3# ..
```

```
------------------------------------------------------------
[DHCP Menu]
      subnet      - DHCP subnet menu
      stdopts     - Standard options menu
      vendopts    - Vendor options menu

>> DHCP# stdopts 6
Creating Standard Options 6
Set the standard option value: 10.10.60.35

------------------------------------------------------------
[Standard Options 6 Menu]
      name        - Name
      value       - Set value
      del         - Remove Standard Options

>> Standard Options 6# ..

>> DHCP# stdopts 15
Creating Standard Options 15
Set the standard option value: lab.abc.com

------------------------------------------------------------
[Standard Options 15 Menu]
      name        - Name
      value       - Set value
      del         - Remove Standard Options

>> Standard Options 15# ..

------------------------------------------------------------
[DHCP Menu]
      subnet      - DHCP subnet menu
      stdopts     - Standard options menu
      vendopts    - Vendor options menu

>> DHCP# stdopts 51
Creating Standard Options 51
Set the standard option value: 86400

------------------------------------------------------------
[Standard Options 51 Menu]
      name        - Name
      value       - Set value
      del         - Remove Standard Options

>> Standard Options 51# ..

------------------------------------------------------------
[DHCP Menu]
      subnet      - DHCP subnet menu
      stdopts     - Standard options menu
      vendopts    - Vendor options menu

>> DHCP#
```

3. Create the SNAS DHCP Red Range for VLAN 10 and add DHCP Option 191 for Subnet 1.

```
>> Main# /cfg/domain 1/dhcp/subnet 1/red/ranges

------------------------------------------------------------
[Ranges Menu]
      list        - List all values
      del         - Delete a value by number
      add         - Add a new value
      insert      - Insert a new value
      move        - Move a value by number

>> Ranges#

>> Ranges# add
Enter lower address: 10.24.24.17
Enter upper address: 10.24.24.30

>> Ranges# ..

------------------------------------------------------------
[DHCP Settings Menu]
      ranges      - Ranges menu
      stdopts     - Standard options menu
      vendopts    - Vendor options menu

>> Red DHCP settings# stdopts 191

------------------------------------------
[Standard Options 191 Menu]
      name        - Name
      value       - Set value
      del         - Remove Standard Options

>> Standard Options 191# value VLAN-A:220.
>> Standard Options 191# ..

------------------------------------------
[Red DHCP settings Menu]
      ranges      - Ranges menu
      stdopts     - Standard options menu
      vendopts    - Vendor options menu

>> DHCP Settings# stdopts 6
Creating Standard Options 6
Set the standard option value: 10.10.60.35

------------------------------------------------------------
[Standard Options 6 Menu]
      name        - Name
      value       - Set value
      del         - Remove Standard Options
```

4. Create the SNAS DHCP Green Range. For this example, we will set the upper green IP address to 10.24.24.61 so that we can assign the ERS5500 10.24.24.62.

```
>> Main# /cfg/domain 1/dhcp/subnet 1/green/ranges

------------------------------------------------------------
[Ranges Menu]
      list        - List all values
      del         - Delete a value by number
      add         - Add a new value
      insert      - Insert a new value
      move        - Move a value by number

>> Ranges# add
Enter lower address: 10.24.24.49
Enter upper address: 10.24.24.61

>> Ranges# ..

------------------------------------------------------------
[DHCP Settings Menu]
      ranges      - Ranges menu
      stdopts     - Standard options menu
      vendopts    - Vendor options menu

>> DHCP Settings# stdopts 6
Creating Standard Options 6
Set the standard option value: 192.168.70.12,192.168.70.13,
192.168.70.15

------------------------------------------------------------
[Standard Options 6 Menu]
      name        - Name
      value       - Set value
      del         - Remove Standard Options
```

5. Apply Changes

```
>> Main# apply
Changes applied successfully.
```

6. Create subnet 3 using SNAS DHCP hub mode to be used for VLAN 220.

```
>> Main# /cfg/domain 1/dhcp/subnet 3
Creating Subnet 3
Select one of hub, filter and standard: hub
Set the subnet name: VoIP
Enter subnet network address: 10.56.56.0
Enter subnet network mask: 255.255.255.0

------------------------------------------------------------
[Subnet 3 Menu]
      type        - Set type
      name        - Set name
      address     - Set network address
      netmask     - Set network mask
      red         - Red vlan Settings menu
      yellow      - Yellow vlan Settings menu
      green       - Green vlan Settings menu
      ena         - Enable subnet
      dis         - Disable subnet
      del         - Remove Subnet

>> Subnet 3# ena
```

7. Create the SNAS DHCP Red Range for VLAN 220 and add DHCP Option 128 for Subnet 3.

```
>> Main# /cfg/domain 1/dhcp/subnet 3/red/ranges

------------------------------------------------------------
[Ranges Menu]
      list        - List all values
      del         - Delete a value by number
      add         - Add a new value
      insert      - Insert a new value
      move        - Move a value by number

>> Ranges#

>> Ranges# add
Enter lower address: 10.56.56.10
Enter upper address: 10.56.56.50

>> Ranges# ..

------------------------------------------------------------
[DHCP Settings Menu]
      ranges      - Ranges menu
      stdopts     - Standard options menu
      vendopts    - Vendor options menu

>> Red DHCP settings# stdopts 128

------------------------------------------
[Standard Options 128 Menu]
      name        - Name
      value       - Set value
```

```
      del         - Remove Standard Options

>> Standard Options 128# value Nortel-i2004-A,10.96.96.10:5000,1,5.
>> Standard Options 128# ..

----------------------------------------
[Red DHCP settings Menu]
      ranges      - Ranges menu
      stdopts     - Standard options menu
      vendopts    - Vendor options menu

>> DHCP Settings# stdopts 3
Creating Standard Options 3
Set the standard option value: 10.56.56.1

------------------------------------------------------------
[Standard Options 3 Menu]
      name        - Name
      value       - Set value
      del         - Remove Standard Options

>> Standard Options 3# apply
```

8. Add additional TunnelGuard users. Assuming you have setup a TunnelGuard group named 'tunnelguard', use the following commands to create additional users. If a group has not been defined, go to "*/cfg/domain 1/aaa/group 1*" to create one.

```
>> Main# /cfg/domain 1/aaa/auth/local
Enter auth id: (1-63) 1

------------------------------------------------------------
[Local database Menu]
      add         - Add user in local database
      passwd      - Change user's password in local database
      groups      - Change user's groups in local database
      del         - Delete user from local database
      list        - List users in local database
      import      - Import database from TFTP/FTP/SCP/SFTP server
      export      - Export database to TFTP/FTP/SCP/SFTP server

>> Local database# add
Enter user name: user1
Enter passwd: user1
Enter group names (comma separated): tunnelguard

>> Local database# add
Enter user name: user2
Enter passwd: user2
Enter group names (comma separated): tunnelguard

>> Local database# apply
Changes applied successfully.

>> Local database# list
tg      <encrypted>     tunnelguard
user1   <encrypted>     tunnelguard
```

```
user2    <encrypted>      tunnelguard
```

NOTE: If you have setup SNAS to use the default TunnelGuard "tunnelguard" group, it will check the end user device for the file "c:\tunnelguard\tg.txt". Please use SREM (Security & Routing Element Manager) to change this setting if required.

9. Make sure http redirect is enabled. This is required to redirect the http session from a user to SREM

```
>> Main# /cfg/domain 1/httpredir
------------------------------------------------------------
[Http Redir Menu]
      port        - Set Http Server port
      redir       - Enable/Disable Http to Https redirection

>> Http Redir# redir on

>> Http Redir# apply
```

2.1.2 ERS5500 Configuration

From a default configuration, create the management interface, VLAN 10, and all the appropriate SNAS Red DHCP Range filters.

1. Enter configuration mode
   - 5510-48T>***enable***
   - 5510-48T#***config terminal***
2. Enable autopvid VLAN configuration
   - 5510-48T(config)# ***vlan configcontrol autopvid***
3. Create the data and voice VLANs.
   - 5510-48T(config)# ***vlan create 10 name snas type port***
   - 5510-48T(config)# ***vlan create 220 name VoIP type port***
4. Remove all port members from the default VLAN. Enable tagging on trunk port to the ERS8600, setup the user ports for untagged data and tagged voice and set the default VLAN to 10 on the user ports.
   - 5510-48T(config)# ***vlan members remove 1 ALL***
   - 5510-48T(config)# ***vlan ports 7 tagging tagall***
   - 5510-48T(config)# ***vlan ports 3-6 tagging unTagPvidOnly***
   - 5510-48T(config)# ***vlan members 10 3-7***
   - 5510-48T(config)# ***vlan members 220 3-7***
   - 5510-48T(config)# ***vlan ports 3-6 pvid 10***
5. Create the management IP address and assign VLAN 10 as the management VLAN.
   - 5510-48T(config)# ***vlan mgmt 10***
   - 5510-48T(config)# ***ip address 10.24.24.62 netmask 255.255.255.0 default-gateway 10.24.24.1***
6. Create a new interface group and add port member 3 to 6.
   - 5510-48T(config)# ***qos if-group name vlan_10 class untrusted***
   - 5510-48T(config)# ***qos if-assign port 3-6 name vlan_10***

7. Create a meter to be used to police all HTTP/HTTPS traffic to 1000 Kbps with an in-profile action of standard traffic and dropping excess traffic.

   - 5510-48T(config)# ***qos meter 1 name "meter_1" committed-rate 1000 max-burst-rate 2000 max-burst-duration 32 in-profile-action 2 out-profile-action 1***

8. Create Elements to be used when setting up the policies. IP Element 1 will be used to allow DNS traffic only from SNAS red DHCP range to SNAS VIP and will be added to policy 1. IP Element 2 will be used to allow DHCP traffic and will be added to policy 2. IP Element 3 will be used to allow ICMP traffic and will be added to policy 3. IP Element 4 and IP element 5 will be combined in classifier block 1 and applied to policy 4 used to allow HTTP/HTTPS traffic to SNAS subnet. IP Element 6 and L2 element 1 plus IP Element 3 and L2 element 1 will be combined in classifier block 2 and applied to policy 5 to allow UDP and ICMP traffic for the for the Voice VLAN 220. Element 7 (classifier 9) will be used to allow all traffic from SNAS green DHCP range and will be added to policy 6. Element 8 will be used to deny all traffic that does not match IP elements 1 to 7 and will be added to policy 7.

   - 5510-48T(config)# ***qos ip-element 1 src-ip 10.24.24.16/28 dst-ip 10.10.60.35/32 protocol 17 dst-port-min 53 dst-port-max 53***
   - 5510-48T(config)# ***qos ip-element 2 protocol 17 dst-port-min 67 dst-port-max 67***
   - 5510-48T(config)# ***qos ip-element 3 protocol 1***
   - 5510-48T(config)# ***qos ip-element 4 dst-ip 10.10.60.0/24 protocol 6 dst-port-min 80 dst-port-max 80***
   - 5510-48T(config)# ***qos ip-element 5 dst-ip 10.10.60.0/24 protocol 6 dst-port-min 443 dst-port-max 443***
   - 5510-48T(config)# ***qos ip-element 6 protocol 17***
   - 5510-48T(config)# ***qos ip-element 7 src-ip 10.24.24.48/28***
   - 5510-48T(config)# ***qos ip-element 8***
   - 5510-48T(config)# ***qos l2-element 1 vlan-min 220 vlan-max 220 ethertype 0x800***

9. Create a classifier for each of the IP elements created above. Please note that Classifiers 6 is a combination of IP element 6 and L2 element 1 which will be used to allow UDP traffic for the Voice VLAN 220. Classifier 7 is a combination of IP element 3 and L2 element 1 which will be used to allow ICMP traffic for the Voice VLAN 220.

   - 5510-48T(config)# ***qos classifier 1 set-id 1 name red_dns element-type ip element-id 1***
   - 5510-48T(config)# ***qos classifier 2 set-id 2 name dhcp element-type ip element-id 2***
   - 5510-48T(config)# ***qos classifier 3 set-id 3 name icmp element-type ip element-id 3***
   - 5510-48T(config)# ***qos classifier 4 set-id 4 name http element-type ip element-id 4***
   - 5510-48T(config)# ***qos classifier 5 set-id 5 name https element-type ip element-id 5***
   - 5510-48T(config)# ***qos classifier 6 set-id 6 name "UDP_VoIP" element-type ip element-id 6***
   - 5510-48T(config)# ***qos classifier 7 set-id 6 name "UDP_VoIP" element-type l2 element-id 1***
   - 5510-48T(config)# ***qos classifier 8 set-id 7 name "ICMP_VoIP" element-type ip element-id 3***
   - 5510-48T(config)# ***qos classifier 9 set-id 7 name "ICMP_VoIP" element-type l2 element-id 1***
   - 5510-48T(config)# ***qos classifier 10 set-id 8 name "drop_all" element-type ip element-id 8***
   - 5510-48T(config)# ***qos classifier 11 set-id 9 name green element-type ip element-id 7***

10. Create Classifier block 1 and 2. Block 1 will combine the HTTP and HTTPS IP elements and combined with meter 1 created in step 7 above. Block 2 will combine the Voice UDP and ICMP IP and L2 elements and set the QoS level to Premium.

    - 5510-48T(config)# ***qos classifier-block 1 block-number 1 name web set-id 4 meter 1***
    - 5510-48T(config)# ***qos classifier-block 2 block-number 1 name web set-id 5 meter 1***
    - 5510-48T(config)# ***qos classifier-block 3 block-number 2 name VoIP set-id 6 in-profile-action 6***
    - 5510-48T(config)# ***qos classifier-block 4 block-number 2 name VoIP set-id 7 in-profile-action 6***

11. Configure the policies required and apply them to the interface group configured in step 5 above. For this example, we will track statistics for each policy; add “track-statistics individual” to the end of each policy as shown below.

    - 5510-48T(config)# ***qos policy 1 name "red_dns" if-group "vlan_10" clfr-type classifier clfr-id 1 in-profile-action 2 precedence 14 track-statistics individual***
    - 5510-48T(config)# ***qos policy 2 name dhcp if-group "vlan_10" clfr-type classifier clfr-id 2 in-profile-action 2 precedence 13 track-statistics individual***
    - 5510-48T(config)# ***qos policy 3 name icmp if-group "vlan_10" clfr-type classifier clfr-id 3 in-profile-action 2 precedence 11 track-statistics individual***
    - 5510-48T(config)# ***qos policy 4 name web if-group "vlan_10" clfr-type block clfr-id 1 precedence 10 track-statistics individual***
    - 5510-48T(config)# ***qos policy 5 name VoIP if-group "vlan_10" clfr-type block clfr-id 2 precedence 9 track-statistics individual***
    - 5510-48T(config)# ***qos policy 6 name green if-group "vlan_10" clfr-type classifier clfr-id 9 in-profile-action 2 precedence 8 track-statistics individual***
    - 5510-48T(config)# ***qos policy 7 name "drop_all" if-group "vlan_10" clfr-type classifier clfr-id 8 in-profile-action 1 precedence 7 track-statistics individual***

    You can use the command “show qos action” to view the ID to action correlation.

12. Enable DHCP Snooping for VLAN 10 and set port 7 for trusted.

    - 5510-48T(config)# ***ip dhcp-snooping vlan 10***
    - 5510-48T(config)# ***ip dhcp-snooping enable***
    - 5510-48T(config)# ***interface fastEthernet 7***
    - 5510-48T(config-if)# ***ip dhcp-snooping trusted***
    - 5510-48T(config-if)# ***exit***
    - 5510-48T(config)#

13. Enable ARP Inspection for VLAN 10 and set port 7 for trusted.

    - 5510-48T(config)# ***ip arp-inspection vlan 10***
    - 5510-48T(config)# ***interface fastEthernet 7***
    - 5510-48T(config-if)# ***ip arp-inspection trusted***
    - 5510-48T(config-if)# ***exit***

Use the following commands to verify operations:

- 5510-48T# ***show vlan***
- 5510-48T# ***show vlan interface <info|vid>***
- 5510-48T# ***show ip dhcp-snooping***
- 5510-48T# ***show ip dhcp-snooping interface***
- 5510-48T# ***show ip dhcp-snooping binding***
- 5510-48T# ***show ip arp-inspection***
- 5510-48T# ***show ip arp-inspection interface***
- 5510-48T# ***show qos ip-element***

- 5510-48T# ***show qos classifier***
- 5510-48T# ***show qos if-group***
- 5510-48T# ***show qos if-assign***
- 5510-48T# ***show qos policy***
- 5510-48T# ***show qos statistics <1|2>***

2.2 Verify Operations

2.2.1 End Device Verification

2.2.1.1 Verify IP address via user. It should have an IP address from the SNAS Red DHCP range and the DNS setting should be pointing to the SNAS VIP

C:\>***ipconfig /all***

```
Ethernet adapter Lab:

        Description . . . . . . . . . . . : Compaq NC3163 Fast Ethernet NIC #2
        Physical Address. . . . . . . . . : 00-50-8B-E1-58-E8
        DHCP Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 10.24.24.17
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.24.24.1
        DHCP Server . . . . . . . . . . . : 10.10.60.34
        DNS Servers . . . . . . . . . . . : 10.10.60.35
        Lease Obtained. . . . . . . . . . : Tuesday, May 30, 2006 11:41:47 AM
         Lease Expires . . . . . . . . . . : Tuesday, May 30, 2006 12:21:47 PM
```

2.2.1.2 Open up a browser connection and authenticate using TunnelGuard. If everything goes well, you should get a new IP address belonging to the Green DHCP range and the DNS setting should also change.

C:\>***ipconfig /all***

```
Ethernet adapter Lab:

        Description . . . . . . . . . . . : Compaq NC3163 Fast Ethernet NIC #2
        Physical Address. . . . . . . . . : 00-50-8B-E1-58-E8
        DHCP Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 10.24.24.49
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.24.24.1
        DHCP Server . . . . . . . . . . . : 10.10.60.34
        DNS Servers . . . . . . . . . . . : 192.168.70.12
                                            192.168.70.13
                                            192.168.70.15
        Lease Obtained. . . . . . . . . . : Tuesday, May 30, 2006 11:48:40 AM
        Lease Expires . . . . . . . . . . : Tuesday, May 30, 2006 12:28:40 PM
```

2.2.2 SNAS Verification

2.2.2.1 Verify DHCP address and user sessions via SNAS prior to a user authentication. There should be no user sessions and the user should have an IP address within the Red DHCP range

```
>> Main# /info/dhcp/list/all
Client Id            Status     Ip               Time Left
-----------------------------------------------------------------
00:50:8b:e1:58:e8    allocated  10.24.24.17      113608

>> Main# /info/sessions
 Number of currently active sessions: 0

Domain  Switch  Port    User                Source IP        Source Mac
        Login   Type    Vlan                Portal IP
------- ------- ------- ------------------- ---------------- -----------------

>> Information#
```

2.2.2.2 After the user has successfully authenticated via TunnelGuard, the IP should change and a session should be logged.

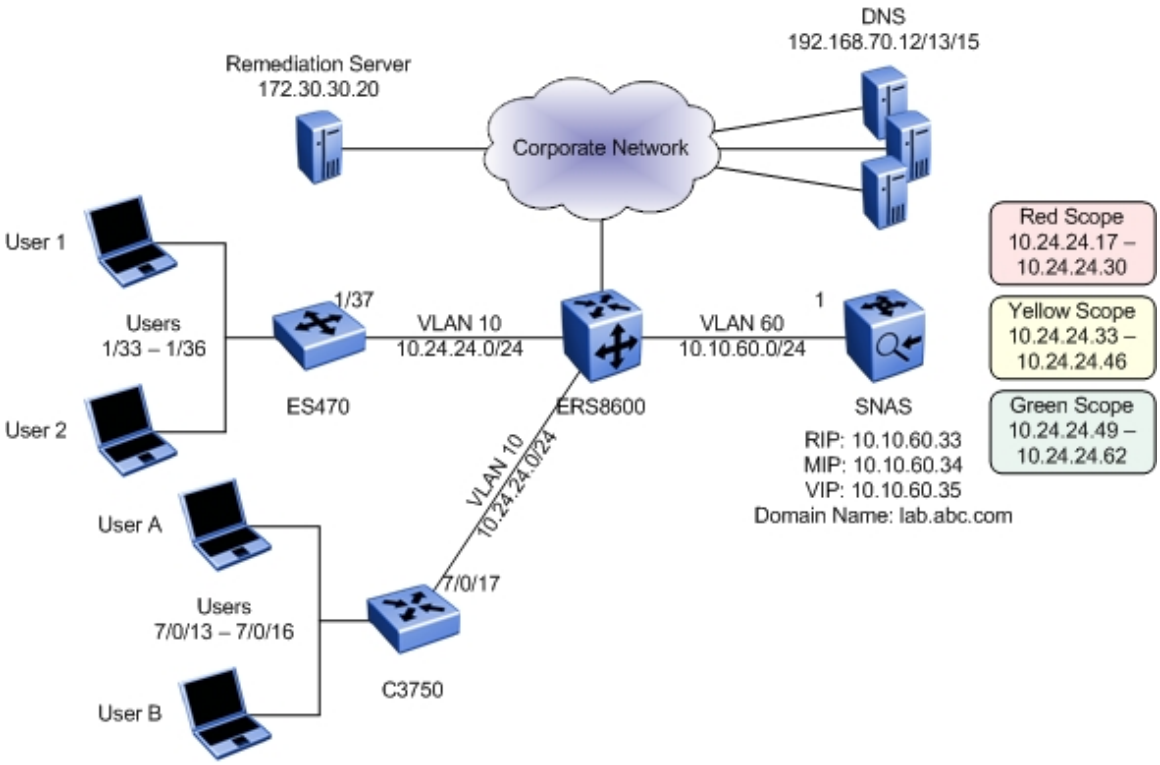
```
>> Main# /info/dhcp/list/all
Client Id            Status     Ip               Time Left
-----------------------------------------------------------------
00:50:8b:e1:58:e8    allocated  10.24.24.49      113717

>> Main# /info/sessions

 Number of currently active sessions: 1

Domain  Switch  Port    User                Source IP        Source Mac
        Login   Type    Vlan                Portal IP
------- ------- ------- ------------------- ---------------- -----------------
      1       0      -- user1               10.24.24.49      00:50:8b:e1:58:e8
```

2.3 Configuration Example: ES470 and Cisco 3750 using SNAS Hub Mode with Red, Yellow, and Green DHCP Range without Voice



Continued from example 2.1 above now using an ES470 as the access switch, we will add a remediation Yellow DHCP range to SNAS assuming the remediation server is 172.30.30.20. In addition, we will add a Cisco 3750 and provide the necessary access-map filters to allow operation as a non-snas switch.

For this example, we will configure TunnelGuard to check for Symantec Anti-virus and also to check for the file c:\tunnelguard\tg.txt. The file c:\tunnelguard\tg.txt is setup automatically when initially setting up TunnelGuard. This file would normally not be used, and is only used for demonstration purposes for this example to show how to setup TunnelGuard using two rules.

Overall, we will setup up the following DHCP ranges via SNAS:

- Red DHCP range: 10.24.24.16/28
- Yellow DHCP range: 10.24.24.32/28
- Green DHCP range: 10.24.24.48/28

2.3.1 ES470 Setup

From a default configuration, create the management interface, VLAN 10, and all the appropriate SNAS Red and Yellow DHCP Range filters.

1. Enter configuration mode
   - 470-48T>***enable***
   - 470-48T#***config terminal***
2. Create the management VLAN and assign an IP address to it.
   - 470-48T(config)# ***vlan create 10 name VLAN-10_nsna type port***
3. Enable tagging on trunk port to the ERS8600 and add port members
   - 470-48T(config)# ***vlan ports 37 tagging tagall***
   - 470-48T(config)# ***vlan members 10 33-37***
4. Assign VLAN 10 as the management VLAN and assign the switch a management IP address.
   - 470-48T(config)# ***vlan mgmt 10***
   - 470-48T(config)# ***ip address 10.24.24.62 netmask 255.255.255.0 default-gateway 10.24.24.1***
5. Create a new interface group and add port member 3 to 6.
   - 470-48T(config)#***qos if-assign-list del portlist 33-36***
   - 470-48T(config)# ***qos if-group name vlan_10 create class untrusted***
   - 470-48T(config)# ***qos if-assign-list add portlist 33-36 name vlan_10***
6. Create IP filters to be used when setting up the policies. IP filter 1 will be used to allow DNS traffic only from SNAS red DHCP range to SNAS VIP. IP filter 2 will be used to allow DNS traffic only from SNAS yellow DHCP range to SNAS VIP. IP filter 3 will be used to allow traffic to the remediation server. IP filter 4 will be used to allow DHCP traffic. IP filter 5 will be used to allow ICMP. IP filter 6 will be used to allow all DHCP traffic. IP filter 7 will be used to allow HTTPS traffic. IP filter 8 will be used to allow all traffic from the SNAS Green DHCP Range. IP filter 9 will be used to deny all other traffic.

   a) Add DNS filters for Red and Yellow SNAS DHCP range to allow DNS only to SNAS
   - 470-48T(config)# ***qos ip-filter 1 create src-ip 10.24.24.16 255.255.255.240 dst-ip 10.10.60.35 255.255.255.255 protocol udp dst-port 53***
   - 470-48T(config)# ***qos ip-filter 2 create src-ip 10.24.24.32 255.255.255.240 dst-ip 10.10.60.35 255.255.255.255 protocol udp dst-port 53***

   b) Add filter to allow Yellow SNAS DHCP range to remediation server
   - 470-48T(config)# ***qos ip-filter 3 create src-ip 10.24.24.32 255.255.255.240 dst-ip 172.30.30.20 255.255.255.255***

   c) Add filter to allow DHCP
   - 470-48T(config)# ***qos ip-filter 4 create protocol udp dst-port 67***

   d) Add filter to allow ICMP
   - 470-48T(config)# ***qos ip-filter 5 protocol icmp***

   e) Add filters to allow http and https only to SNAS subnet
   - 470-48T(config)# ***qos ip-filter 6 create dst-ip 10.10.60.0 255.255.255.0 protocol tcp dst-port 80***
   - 470-48T(config)# ***qos ip-filter 7 create dst-ip 10.10.60.0 255.255.255.0 protocol tcp dst-port 443***

   f) Add filter to allow all traffic for Green DHCP SNAS range

- 470-48T(config)# ***qos ip-filter 8 create src-ip 10.24.24.48 255.255.255.240 dst-ip 0.0.0.0 0.0.0.0***

g) Add filter to deny all other traffic

- 470-48T(config)# ***qos ip-filter 9 create***

7. Create two IP filter sets, one with IP filters 1 to 8 to allow traffic and another to deny all other traffic using IP filter 2.

a) Add IP filter set 1 and add filters 1 to 8 to be used with a policy with an action of allow

- 470-48T(config)# ***qos ip-filter-set 1 create set 1 name fGrp1 filter 1 filter-prec 1***
- 470-48T(config)# ***qos ip-filter-set 2 create set 1 name fGrp1 filter 2 filter-prec 2***
- 470-48T(config)# ***qos ip-filter-set 3 create set 1 name fGrp1 filter 3 filter-prec 3***
- 470-48T(config)# ***qos ip-filter-set 4 create set 1 name fGrp1 filter 4 filter-prec 4***
- 470-48T(config)# ***qos ip-filter-set 5 create set 1 name fGrp1 filter 5 filter-prec 5***
- 470-48T(config)# ***qos ip-filter-set 6 create set 1 name fGrp1 filter 6 filter-prec 6***
- 470-48T(config)# ***qos ip-filter-set 7 create set 1 name fGrp1 filter 7 filter-prec 7***
- 470-48T(config)# ***qos ip-filter-set 8 create set 1 name fGrp1 filter 8 filter-prec 8***

b) Add a second IP filter set and add filter 9 to be used with a policy with an action of deny.

- 470-48T(config)# ***qos ip-filter-set 9 create set 2 name fGrp2 filter 9 filter-prec 1***

8. Configure the policies required and apply them to the IP filter sets group configured in step 6 above. Note that an action of 65527 allow traffic while 65526 drops traffic – please use the "show qos actions" command to view the qos actions.

- 470-48T(config)# ***qos policy 1 create name p1 if-group vlan_10 filter-set-type ip filter-set 1 in-profile-action 65527 order 1***
- 470-48T(config)# ***qos policy 2 create name p2 if-group vlan_10 filter-set-type ip filter-set 2 in-profile-action 65526 order 2***

9. Use the following commands to verify operations:

- 470-48T# ***show vlan***
- 470-48T# ***show vlan interface <info|vid>***
- 470-48T# ***show qos if-group***
- 470-48T# ***show qos if-assign-list***
- 470-48T# ***show qos ip-filters***
- 470-48T# ***show qos ip-filter-sets***
- 470-48T# ***show qos statistics***

2.3.2 SNAS Configuration

The configuration for SNAS is the same as used above with the addition of the Yellow DHCP range. List below is the SNAS configuration with addition high-lighted in blue.

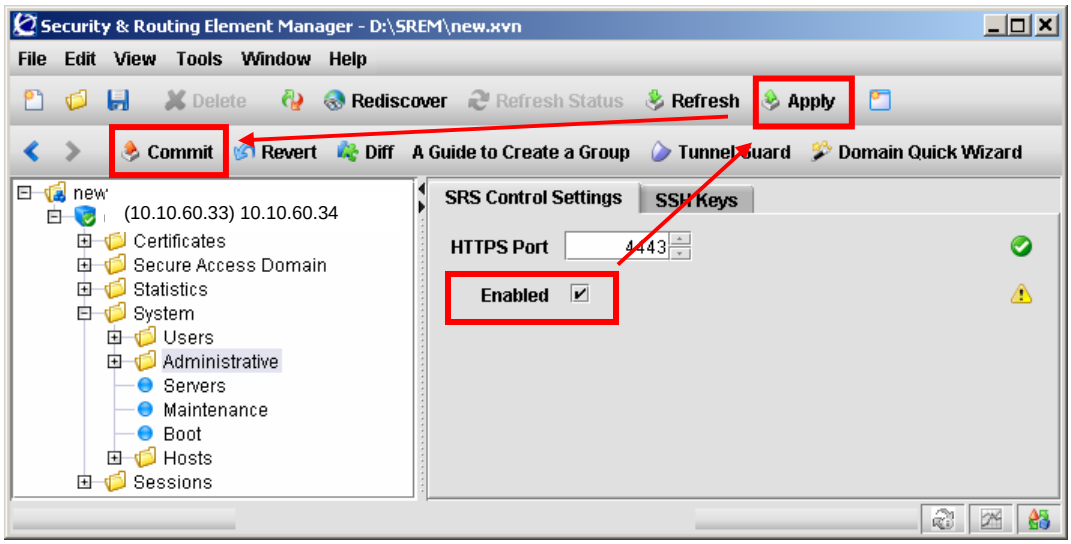
```
/cfg/domain 1/dhcp/.
/cfg/domain 1/dhcp/subnet 1/.
        type hub
        name Subnet_1
        address 10.24.24.0
        netmask 255.255.255.0
        ena enabled
/cfg/domain 1/dhcp/subnet 1/red/.
/cfg/domain 1/dhcp/subnet 1/red/ranges/.
        add 10.24.24.17 10.24.24.30
/cfg/domain 1/dhcp/subnet 1/red/stdopts 6/.
        value 10.10.60.35
/cfg/domain 1/dhcp/subnet 1/red/stdopts 51/.
        value 10
/cfg/domain 1/dhcp/subnet 1/yellow/.
/cfg/domain 1/dhcp/subnet 1/yellow/ranges/.
        add 10.24.24.33 10.24.24.46
```

```
/cfg/domain 1/dhcp/subnet 1/green/.
/cfg/domain 1/dhcp/subnet 1/green/ranges/.
        add 10.24.24.49 10.24.24.61
/cfg/domain 1/dhcp/subnet 1/green/stdopts 6/.
        value 192.168.70.12, 192.168.70.13, 192.168.70.15
/cfg/domain 1/dhcp/stdopts 3/.
        value 10.24.24.1
/cfg/domain 1/dhcp/stdopts 6/.
        value 10.10.60.35
/cfg/domain 1/dhcp/stdopts 15/.
        value lab.abc.com
/cfg/domain 1/dhcp/stdopts 51/.
        value 2400
/cfg/domain 1/sshkey/.
```

2.3.3 TunnelGuard Configuration

- TunnelGuard for this example will be setup to check for c:/tunnelguard/tg.txt and for the lasted Symantec Antivirus update. TunnelGuard can also check for running processes, digital certificates, registry entries, program-version and date checks, etc.

In order to use the TunnelGuard configuration tool, the SRS administration must be enabled using the SREM or via the CLI.



CLI command:

```
>> /cfg/sys/adm/srsadmin/ena/apply
```

- Please see Appendix A regarding setting up TunnelGuard

2.3.4 Cisco 3750 Setup

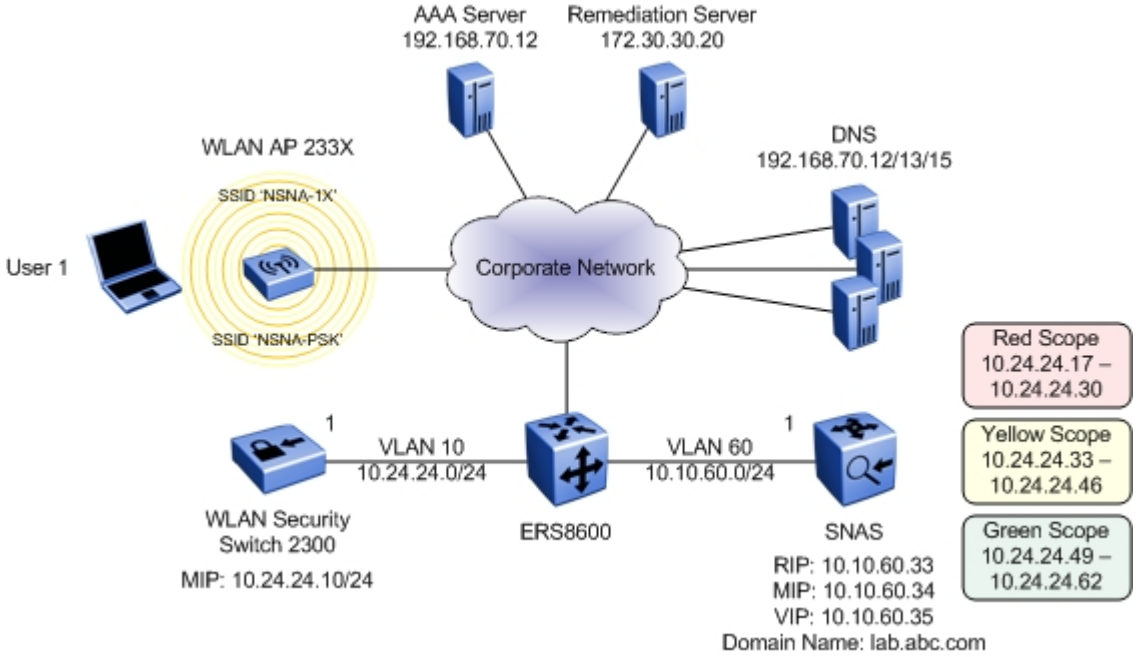
The following configuration will perform the following:

- Create VLAN 10 with port members 13 to 17 with port 17 being a tagged port
- Enable DHCP Snooping and ARP Inspection for VLAN 10
- Create an Access List for the SNAS filters and add the list to access port members 13 to 16.

```
!
no aaa new-model
switch 7 provision ws-c3750g-24t
ip subnet-zero
!
ip dhcp snooping vlan 10
ip dhcp snooping
ip arp inspection vlan 10
ip arp inspection validate ip
!
!
vlan access-map map1 10
 action forward
 match ip address non_snas
vlan internal allocation policy ascending
!
interface GigabitEthernet7/0/13
 switchport access vlan 10
 switchport mode access
 ip access-group non_snas in
 no mdix auto
!
interface GigabitEthernet7/0/14
 switchport access vlan 10
 switchport mode access
 ip access-group non_snas in
 no mdix auto
!
interface GigabitEthernet7/0/15
 switchport access vlan 10
 switchport mode access
 ip access-group non_snas in
 no mdix auto
!
interface GigabitEthernet7/0/16
 switchport access vlan 10
 switchport mode access
 ip access-group non_snas in
 no mdix auto
!
interface GigabitEthernet7/0/17
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10
 switchport mode trunk
 ip arp inspection trust
 no mdix auto
```

```
 ip dhcp snooping trust
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 no ip address
!
ip access-list extended match_all
 permit ip any any
ip access-list extended non_snas
 permit udp 10.24.24.16 0.0.0.15 host 10.10.60.35 eq domain
 permit udp 10.24.24.32 0.0.0.15 host 10.10.60.35 eq domain
 permit ip 10.24.24.32 0.0.0.15 host 172.30.30.20
 permit udp any any eq bootps
 permit udp any any eq bootpc
 permit icmp any any
 permit tcp any 10.10.60.0 0.0.0.255 eq www
 permit tcp any 10.10.60.0 0.0.0.255 eq 443
 permit ip 10.24.24.48 0.0.0.15 any
!
```

2.4 Configuration Example: Wireless LAN 2300 using SNAS Hub Mode with Red, Yellow, and Green DHCP Range



In this example, we will now introduce a WLAN Security Switch 2300 as an access switch. The WLAN Security Switch 2300 should be running software version 5.0 to take advantage of the new DHCP Restrict feature which makes the solution much more secure. DHCP Restrict prevents a user from assigning himself a static address from the green range and bypassing the TunnelGuard check. This feature in combination with ACLs based on green/red/yellow subnet ranges provides good user segmentation and protection against users deliberately trying to circumvent the TunnelGuard authentication process.

The WLAN Security Switch 2300 will provide WPA Enterprise (802.1X) and WPA SOHO (PSK) wireless services and map the wireless users to VLAN 10. We will also create the necessary ACLs and enable the DHCP Restrict and keep-initial VLAN features.

This example configuration will use the same DHCP ranges and TunnelGuard rules on the SNAS as defined in example 2.3:

- Red DHCP range: 10.24.24.16/28
- Yellow DHCP range: 10.24.24.32/28
- Green DHCP range: 10.24.24.48/28

2.4.1 Wireless LAN Security Switch 2300 Setup

The following configuration will be performed:

- Use Quickstart to define the base switch configuration.
- Create an Access Control List called NSNA to restrict access to users based on Red, Yellow and Green address ranges.
- Create an 802.1X service-profile called NSNA-1X using TKIP encryption.
    - Define default VLAN 10 and NSNA filter-id attributes. This will place all users in VLAN 10 as well as assign the NSNA ACLs.

      Note: Users may be assigned to VLAN and filter-id attributes from the AAA server using RADIUS return attributes.
    - If different VLAN IDs are assigned to service-profiles on other switches in the mobility domain, enable the keep-initial VLAN feature which will ensure that VLAN 10 membership is maintained as the client roams.

      Note: If VLAN and filter-id attributes are being assigned by the AAA server the keep-initial VLAN feature is not required.
    - Enable DHCP Restrict to enforce IP addressing from the SNAS. This will block access to statically addressed users as well as users who attempt to change from dynamic to static addressing.
    - Map the service profile to the default radio-profile.
    - Define authentication rule for pass-through to the external AAA server group.
- Define an AAA server and AAA server group for 802.1X authentication.
- Create a PSK service-profile called NSNA-PSK using TKIP encryption.
    - Define a pass-phrase for authentication
    - Define default VLAN 10 and NSNA filter-id attributes. This will place all users in VLAN 10 as well as assign the NSNA ACLs
    - If different VLAN IDs are assigned to service-profiles on other switches in the mobility domain, enable the keep-initial VLAN feature which will ensure that VLAN 10 membership is maintained as the client roams.
    - Enable DHCP Restrict to enforce IP addressing from the SNAS. This will block access to statically addressed users as well as users who attempt to change from dynamic to static addressing.
    - Map the service profile to the default radio-profile
- Add a Distributed Access Point
    - Specify the Access Point model and serial number
    - Specify the 802.11a/b/g channel and power settings
    - Assign the 802.11a/b/g radios to the default radio-profile
    - Note: DHCP or DNS services must be configured so that the Distributed Access Point can locate the WLAN Security Switch 2300.

1. Enter configuration mode and the Quickstart wizard.
   - NT2360-30E114> ***enable***
   - NT2360-30E114# ***quickstart***
2. In the Quickstart wizard define the switch name, IP addressing, VLAN and passwords.
   - This will erase any existing config. Continue? [n]: ***yes***
   - System Name [2360]: ***WSS2360-1***
   - Country Code [US]: ***US***
   - System IP address []: ***10.24.24.10***
   - System IP address netmask []: ***255.255.255.0***
   - Default route []: ***10.24.24.1***
   - Do you need to use 802.1Q tagged ports for connectivity on the default VLAN? [n]: ***N***
   - Enable Webview [y]: ***Y***
   - Admin username [admin]: ***admin***
   - Admin password [mandatory]: ***<admin-password>***
   - Enable password [optional]: ***<enable-password>***
   - Do you wish to set the time? [y]: ***N***
   - Do you wish to configure wireless? [y]: ***N***

1. Rename the default VLAN to VLAN10.
   - WSS2360-1# ***set vlan 1 name VLAN10***
2. Create a Access Control List (ACL) called NSNA with the following Access Control Entries (ACEs):

   a) Add ACE for Red, Yellow and Green ranges to allow communication with the VLAN 10 default gateway.
   - WSS2360-1# ***set security acl ip NSNA permit ip 10.24.24.0 0.0.0.255 10.24.24.1 0.0.0.0***

   b) Add ACE for Red, Yellow and Green ranges to allow DHCP.
   - WSS2360-1# ***set security acl ip NSNA permit udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 range 67 68***

   c) Add ACE for Green range to allow DNS only to SNAS
   - WSS2360-1# ***set security acl ip NSNA permit udp 10.24.24.16 0.0.0.15 10.10.60.35 0.0.0.0 eq 53***

   d) Add ACE for Red range to allow HTTP & HTTPS only to SNAS
   - WSS2360-1# ***set security acl ip NSNA permit tcp 10.24.24.16 0.0.0.15 10.10.60.35 0.0.0.0 eq 80***
   - WSS2360-1# ***set security acl ip NSNA permit tcp 10.24.24.16 0.0.0.15 10.10.60.35 0.0.0.0 eq 443***

e) Add ACE for Yellow range to allow DNS only to SNAS

- WSS2360-1# ***set security acl ip NSNA permit udp 10.24.24.32 0.0.0.15 10.10.60.35 0.0.0.0 eq 53***

f) Add ACE for Yellow range to allow HTTPS only to SNAS

- WSS2360-1# ***set security acl ip NSNA permit tcp 10.24.24.32 0.0.0.15 10.10.60.35 0.0.0.0 eq 443***

g) Add ACE for Yellow range to allow HTTP access to the remediation server

- WSS2360-1# ***set security acl ip NSNA permit tcp 10.24.24.32 0.0.0.15 172.30.30.20 0.0.0.0 eq 80***

h) Add ACE for Green range to allow unrestricted access to the network

- WSS2360-1# ***set security acl ip NSNA permit 10.24.24.48 0.0.0.15***

i) Commit ACEs for the NSNA ACL and apply changes

- WSS2360-1# ***commit security acl NSNA***

3. Add 172.30.30.20 as a AAA server with the name W3KServer1 and define add it to a AAA server group called IAS
   - WSS2360-1# ***set radius server W3KServer address 172.30.30.20 key <sharedkey>***
   - WSS2360-1# ***set server group IAS members W3KServer***
4. Create an 802.1X service-profile called NSNA-1X that supports 802.1X authentication and TKIP encryption and define options.
   - WSS2360-1# **set service-profile NSNA-1X ssid-name NSNA-1X**
   - WSS2360-1# **set service-profile NSNA-1X wpa-ie enable**
   - WSS2360-1# **set service-profile NSNA-1X attr vlan-name VLAN10**
   - WSS2360-1# **set service-profile NSNA-1X attr filter-id NSNA.in**
   - WSS2360-1# **set service-profile NSNA-1X keep-initial-vlan enable**
   - WSS2360-1# **set service-profile NSNA-1X dhcp-restrict enable**
   - WSS2360-1# **set radio-profile default service-profile NSNA-1X**
5. Create a 802.1X access rule that will authenticate all 802.1X users to the AAA server group called IAS
   - WSS2360-1# **set authentication dot1x ssid NSNA-1X ** pass-through IAS**
6. Create a PSK service-profile called NSNA-PSK that supports PSK authentication and TKIP encryption and define options.
   - WSS2360-1# **set service-profile NSNA-PSK ssid-name NSNA-PSK**
   - WSS2360-1# ***set service-profile NSNA-PSK auth-fallthru last-resort***
   - WSS2360-1# **set service-profile NSNA-PSK wpa-ie enable**
   - WSS2360-1# **set service-profile NSNA-PSK auth-psk enable**
   - WSS2360-1# **set service-profile NSNA-PSK psk-phrase <wpa-pass-phrase>**
   - WSS2360-1# **set service-profile NSNA-PSK dhcp-restrict enable**
   - WSS2360-1# **set service-profile NSNA-PSK keep-initial-vlan enable**

- WSS2360-1# **set service-profile NSNA-PSK attr vlan-name VLAN10**
- WSS2360-1# **set service-profile NSNA-PSK attr filter-id NSNA.in**
- WSS2360-1# **set radio-profile default service-profile NSNA-PSK**

7. Add a Distributed Access Point and specify the 802.11a/g channel and power settings as well as add the 802.11a/g radios to the default radio-profile.
   - WSS2360-1# **set dap 1 serial-id stp1w20kc3 model 2330**
   - WSS2360-1# **set dap 1 radio 1 channel 1 tx-power 10 radio-profile default mode enable**
   - WSS2360-1# **set dap 1 radio 2 channel 44 tx-power 10 radio-profile default mode enable**
8. Use the following commands to verify operations:
   - WSS2360-1# **show vlan**
   - WSS2360-1# **show service-profile <service-profile-name>**
   - WSS2360-1# **show radio-profile <radio-profile-name>**
   - WSS2360-1# ***show security acl info NSNA***
   - WSS2360-1# ***show dap status***
   - WSS2360-1# ***show sessions network ssid <ssid-name> verbose***

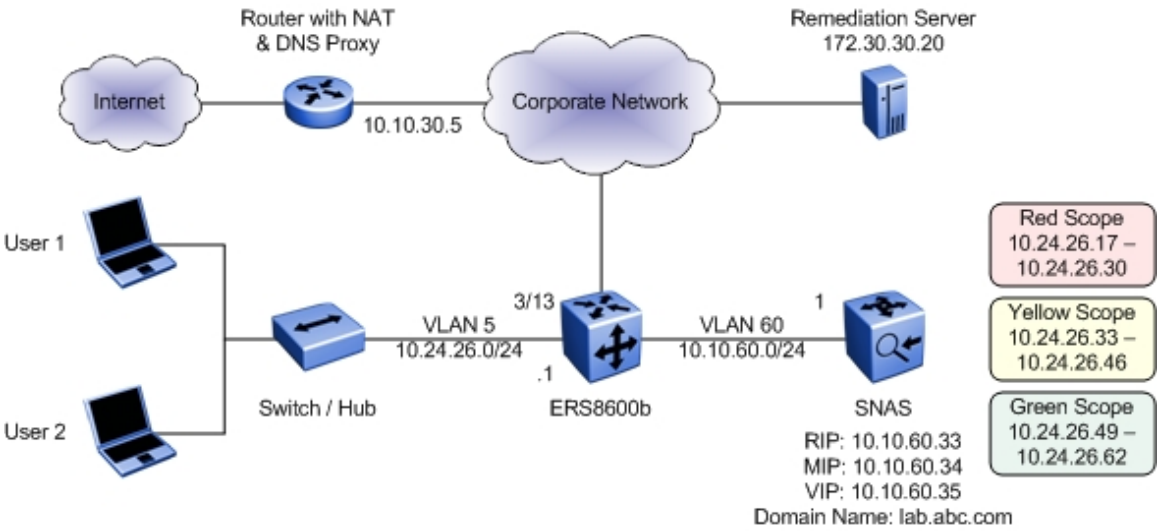
For an example of the completed WLAN Security Switch 2300 configuration please refer to Appendix C.

2.4.2 SNAS Configuration

The configuration for SNAS is the same as used in example 2.3. For an example of the completed SNAS configuration please refer to Appendix C.

3. Applying Non-SNAS Switch Filters at the Core

3.1 Configuration Example: ERS8600 with R-modules using SNAS Hub Mode with Red, Yellow, and Green DHCP Ranges



For this configuration example, we will configure SNAS in DHCP Hub mode to supply a Red, Yellow, and Green DHCP range for the access switch shown in the diagram above. We wish to allow Internet access only via the DHCP Green range. Once a user passes TunnelGuard authentication and passes any TunnelGuard policy configured, the user will be allowed to access the internet. Please see Appendix A in regards to setting up a TunnelGuard policy. We will configure the ERS8600b switch with ACL's such that the Red or Yellow DHCP range is only allowed DHCP, DNS to SNAS, ICMP, HTTP/HTTPS to SNAS subnet, and access to the remediation server only if the user's IP address is within the Yellow DHCP range.

Overall, we will configure the following:

- SNAS
  - Setup SNAS for DHCP Hub mode
  - Setup three DHCP ranges, a Red Range using a range of 10.24.26.16/28, a Yellow Range using a range of 10.24.26.32/28 and a Green Range using a range of 10.24.26.48/28
- ERS8600b
  - Configure VLAN 5 with OSPF and DHCP Relay
  - Configure the appropriate ACL's to only allow the Red or Yellow Range access to ICMP, DHCP, HTTP/HTTPs to the SNAS subnet, and DNS to SNAS only
  - Configure ACL's to allow the Yellow Range access to the remediation server

NOTE: The ERS8600 R-modules only should only be used for non-snas filtering. This is because the R-module supports filtering on ARP operations and VLAN id. The ERS8600 legacy modules do not support filtering on ARP nor VLAN id.

3.1.1 ERS8600 Configuration

From a default configuration, create the management interfaces, the user VLAN 10, and all the appropriate SNAS Red DHCP Range filters.

1. Create VLAN 5, add port members, add IP address, enable DHCP, and enable OSPF passive.

   - ERS8610-B:5# ***config vlan 5 create byport 1 name VLAN-5_non_snas***
   - ERS8610-B:5# ***config vlan 5 ports add 3/13***
   - ERS8610-B:5# ***config vlan 5 ip create 10.24.26.1/24***
   - ERS8610-B:5# ***config vlan 5 ip dhcp-relay enable***
   - ERS8610-B:5# ***config vlan 5 ip ospf interface-type passive***
   - ERS8610-B:5# ***config vlan 5 ip ospf enable***

2. Enable DHCP agent.

   - ERS8610-B:5# ***config ip dhcp-relay create-fwd-path agent 10.24.26.1 server 10.10.60.34 mode dhcp state enable***

3. Enable OSPF

   - ERS8610-B:5# ***config ip ospf admin-state enable***

4. Create ACT 1. Configure the ACT to enable filtering on VLAN, src-ip, dst-ip, TCP destination port, UDP destination port, ICMP, and ARP.

   - ERS8610-B:5# ***config filter act 1 create name ACT-1_non_snas***
   - ERS8610-B:5# ***config filter act 1 ethernet vlan***
   - ERS8610-B:5# ***config filter act 1 ip srcIp,dstIp,ipProtoType***
   - ERS8610-B:5# ***config filter act 1 protocol tcpDstPort,udpDstPort,icmpMsgType***
   - ERS8610-B:5# ***config filter act 1 arp operation***
   - ERS8610-B:5# ***config filter act 1 apply***

5. Create ACL 1. Configure the ACL to use ACT 1 and set the type to port with port 3/13 as the port member. For this example, we will enable the global action to count to allow us to view the filter statistics.

   - ERS8610-B:5# ***config filter acl 1 create inPort act 1***
   - ERS8610-B:5# ***config filter acl 1 set global-action count***
   - ERS8610-B:5# ***config filter acl 1 port add 3/13***

6. Create the various ACE's. For this example, we will set the last ACE to deny all traffic to keep statistics for all dropped traffic. Otherwise, we can set the ACL default action to drop.

   a) Allow ICMP.
   - ERS8610-B:5# ***config filter acl 1 ace 1 create name icmp***
   - ERS8610-B:5# ***config filter acl 1 ace 1 action permit***
   - ERS8610-B:5# ***config filter acl 1 ace 1 ethernet vlan-id eq 5***
   - ERS8610-B:5# ***config filter acl 1 ace 1 ip ip-protocol-type eq icmp***
   - ERS8610-B:5# ***config filter acl 1 ace 1 enable***

   b) Allow DHCP.
   - ERS8610-B:5# ***config filter acl 1 ace 2 create name "dhcp"***
   - ERS8610-B:5# ***config filter acl 1 ace 2 action permit***
   - ERS8610-B:5# ***config filter acl 1 ace 2 ethernet vlan-id eq 5***
   - ERS8610-B:5# ***config filter acl 1 ace 2 protocol udp-dst-port eq 67***
   - ERS8610-B:5# ***config filter acl 1 ace 2 enable***

   c) Allow DNS from Red and Yellow DHCP range only to SNAS.

- ERS8610-B:5# ***config filter acl 1 ace 3 create name "red_yellow_dns"***
- ERS8610-B:5# ***config filter acl 1 ace 3 action permit***
- ERS8610-B:5# ***config filter acl 1 ace 3 ethernet vlan-id eq 5***
- ERS8610-B:5# ***config filter acl 1 ace 3 ip src-ip eq 10.24.26.17-10.24.26.46***
- ERS8610-B:5# ***config filter acl 1 ace 3 ip dst-ip eq 10.10.60.35***
- ERS8610-B:5# ***config filter acl 1 ace 3 protocol udp-dst-port eq dns***
- ERS8610-B:5# ***config filter acl 1 ace 3 enable***

d) Allow Yellow DHCP Range to allow access to remediation server.

- ERS8610-B:5# ***config filter acl 1 ace 4 create name "yellow_redem"***
- ERS8610-B:5# ***config filter acl 1 ace 4 action permit***
- ERS8610-B:5# ***config filter acl 1 ace 4 ethernet vlan-id eq 5***
- ERS8610-B:5# ***config filter acl 1 ace 4 ip src-ip eq 10.24.26.33-10.24.26.46***
- ERS8610-B:5# ***config filter acl 1 ace 4 ip dst-ip eq 172.30.30.20***
- ERS8610-B:5# ***config filter acl 1 ace 4 enable***

e) Allow HTTP and HTTPs traffic to SNAS subnet only***.***

- ERS8610-B:5# ***config filter acl 1 ace 5 create name "http"***
- ERS8610-B:5# ***config filter acl 1 ace 5 action permit***
- ERS8610-B:5# ***config filter acl 1 ace 5 ethernet vlan-id eq 5***
- ERS8610-B:5# ***config filter acl 1 ace 5 ip dst-ip eq 10.10.60.1-10.10.60.255***
- ERS8610-B:5# ***config filter acl 1 ace 5 protocol tcp-dst-port eq 80***
- ERS8610-B:5# ***config filter acl 1 ace 5 enable***
- ERS8610-B:5# ***config filter acl 1 ace 6 create name "https"***
- ERS8610-B:5# ***config filter acl 1 ace 6 action permit***
- ERS8610-B:5# ***config filter acl 1 ace 6 ethernet vlan-id eq 5***
- ERS8610-B:5# ***config filter acl 1 ace 6 ip dst-ip eq 10.10.60.1-10.10.60.255***
- ERS8610-B:5# ***config filter acl 1 ace 6 protocol tcp-dst-port eq 443***
- ERS8610-B:5# ***config filter acl 1 ace 6 enable***

f) Allow all traffic from Green DHCP Range.

- ERS8610-B:5# ***config filter acl 1 ace 7 create name "green"***
- ERS8610-B:5# ***config filter acl 1 ace 7 action permit***
- ERS8610-B:5# ***config filter acl 1 ace 7 ethernet vlan-id eq 5***
- ERS8610-B:5# ***config filter acl 1 ace 7 ip src-ip eq 10.24.26.49-10.24.26.62***
- ERS8610-B:5# ***config filter acl 1 ace 7 enable***

g) Allow ARP request and response.

- ERS8610-B:5# ***config filter acl 1 ace 8 create name "arp_req"***
- ERS8610-B:5# ***config filter acl 1 ace 8 action permit***
- ERS8610-B:5# ***config filter acl 1 ace 8 ethernet vlan-id eq 5***
- ERS8610-B:5# ***config filter acl 1 ace 8 arp operation eq arprequest***
- ERS8610-B:5# ***config filter acl 1 ace 8 enable***
- ERS8610-B:5# ***config filter acl 1 ace 9 create name "arp_rpse"***
- ERS8610-B:5# ***config filter acl 1 ace 9 action permit***
- ERS8610-B:5# ***config filter acl 1 ace 9 ethernet vlan-id eq 5***
- ERS8610-B:5# ***config filter acl 1 ace 9 arp operation eq arpresponse***
- ERS8610-B:5# ***config filter acl 1 ace 9 enable***

h) Deny all other traffic.

- ERS8610-B:5# ***config filter acl 1 ace 10 create name "deny_all"***
- ERS8610-B:5# ***config filter acl 1 ace 10 action deny***
- ERS8610-B:5# ***config filter acl 1 ace 10 ethernet vlan-id eq 5***
- ERS8610-B:5# ***config filter acl 1 ace 10 enable***

3.1.2 SNAS

Continued from example 2 above, we will create subnet 2 for this example. Overall, we can use the DHCP standard options created from example 2 and will only need to configure the default router for all subnet 2 ranges and configure the DNS setting for the Green range

1. Create subnet 1 using SNAS DHCP hub mode

```
>> Main# /cfg/domain 1/dhcp/subnet 2
Creating Subnet 1
Select one of hub, filter and standard: hub
Set the subnet name: non_snas_8600b
Enter subnet network address: 10.24.26.0
Enter subnet network mask: 255.255.255.0

------------------------------------------------------------
[Subnet 1 Menu]
      type        - Set type
      name        - Set name
      address     - Set network address
      netmask     - Set network mask
      red         - Red vlan Settings menu
      yellow      - Yellow vlan Settings menu
      green       - Green vlan Settings menu
      ena         - Enable subnet
      dis         - Disable subnet
      del         - Remove Subnet

>> Subnet 2#

>> Subnet 2# ena
```

2. Create the SNAS DHCP Red Range for subnet 2

```
>> Main# /cfg/domain 1/dhcp/subnet 2/red/ranges

------------------------------------------------------------
[Ranges Menu]
      list        - List all values
      del         - Delete a value by number
      add         - Add a new value
      insert      - Insert a new value
      move        - Move a value by number

>> Ranges#

>> Ranges# add
Enter lower address: 10.24.26.17
Enter upper address: 10.24.26.30

>> Ranges# ..

------------------------------------------------------------
[DHCP Settings Menu]
      ranges      - Ranges menu
      stdopts     - Standard options menu
      vendopts    - Vendor options menu
```

```
>> DHCP Settings# stdopts 3
Creating Standard Options 3
Set the standard option value: 10.24.26.1

------------------------------------------------------------
[Standard Options 3 Menu]
      name        - Name
      value       - Set value
      del         - Remove Standard Options

>> Standard Options 3# ..

------------------------------------------------------------
[DHCP Settings Menu]
      ranges      - Ranges menu
      stdopts     - Standard options menu
      vendopts    - Vendor options menu
```

3. Create the SNAS DHCP Yellow Range

```
>> Main# /cfg/domain 1/dhcp/subnet 1/yellow/ranges

------------------------------------------------------------
[Ranges Menu]
      list        - List all values
      del         - Delete a value by number
      add         - Add a new value
      insert      - Insert a new value
      move        - Move a value by number

>> Ranges# add
Enter lower address: 10.24.26.33
Enter upper address: 10.24.26.33

>> Ranges# ..

------------------------------------------------------------
[DHCP Settings Menu]
      ranges      - Ranges menu
      stdopts     - Standard options menu
      vendopts    - Vendor options menu

>> DHCP Settings# stdopts 3
Creating Standard Options 3
Set the standard option value: 10.24.26.1

------------------------------------------------------------
[Standard Options 3 Menu]
      name        - Name
      value       - Set value
      del         - Remove Standard Options
```

4. Create the SNAS DHCP Green Range

```
>> Main# /cfg/domain 1/dhcp/subnet 1/green/ranges

------------------------------------------------------------
[Ranges Menu]
      list        - List all values
      del         - Delete a value by number
      add         - Add a new value
      insert      - Insert a new value
      move        - Move a value by number

>> Ranges# add
Enter lower address: 10.24.26.49
Enter upper address: 10.24.26.61

>> Ranges# ..

------------------------------------------------------------
[DHCP Settings Menu]
      ranges      - Ranges menu
      stdopts     - Standard options menu
      vendopts    - Vendor options menu
```

```
>> DHCP Settings# stdopts 3
Creating Standard Options 3
Set the standard option value: 10.24.26.1

------------------------------------------------------------
[Standard Options 3 Menu]
      name        - Name
      value       - Set value
      del         - Remove Standard Options
>> Standard Options 3# ..

>> DHCP# stdopts 6
Creating Standard Options 6
Set the standard option value: 10.10.30.5

------------------------------------------------------------
[Standard Options 15 Menu]
      name        - Name
      value       - Set value
      del         - Remove Standard Options
```

5. Apply Changes

```
>> Main# apply
Changes applied successfully.
```

4. Appendix A: TunnelGuard Rule Definition

Configuring TunnelGuard to Check for Anti-Virus

In this example, a TunnelGuard SRS policy is being created to check that all PCs that log into the NSNAS domain have the Symantec Antivirus software running. A TunnelGuard policy can be configured to check for any number of items, but for this example, we will show how to setup TunnelGuard to check that Symantec AntiVirus is running and is up-to-date.

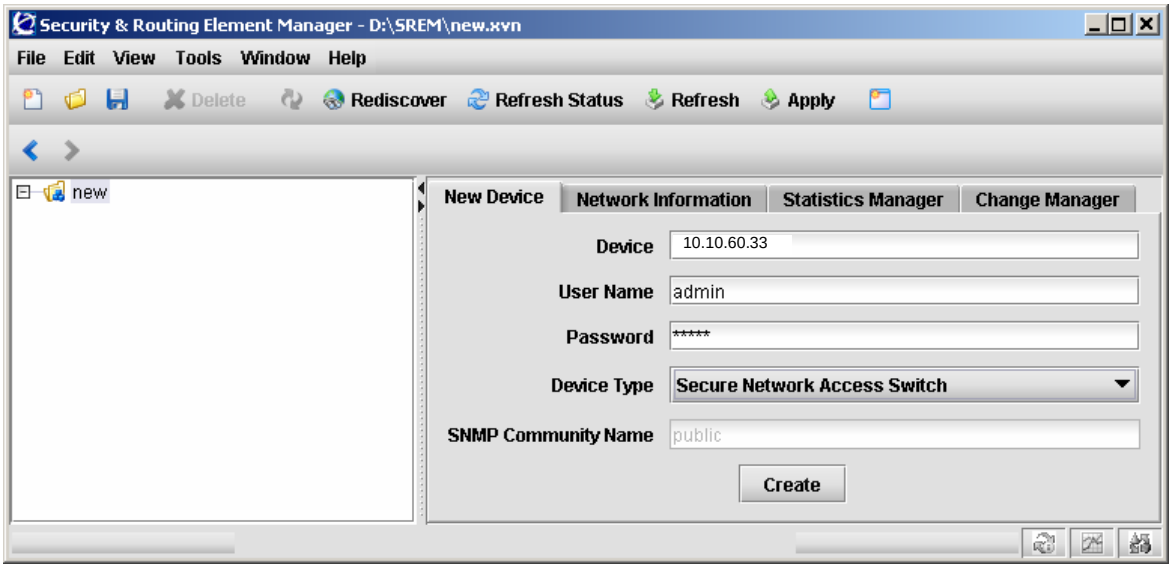
1. Launch SREM and create new device:

   Device = **IP address of SNAS**

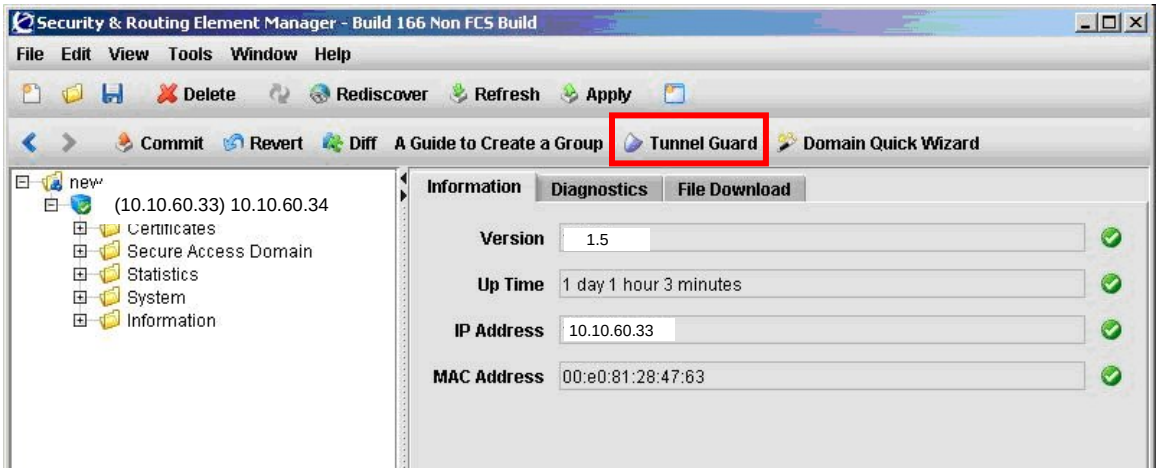
   Username = **admin**

   Password = **admin**

   Device Type = **Secure Network Access Switch**

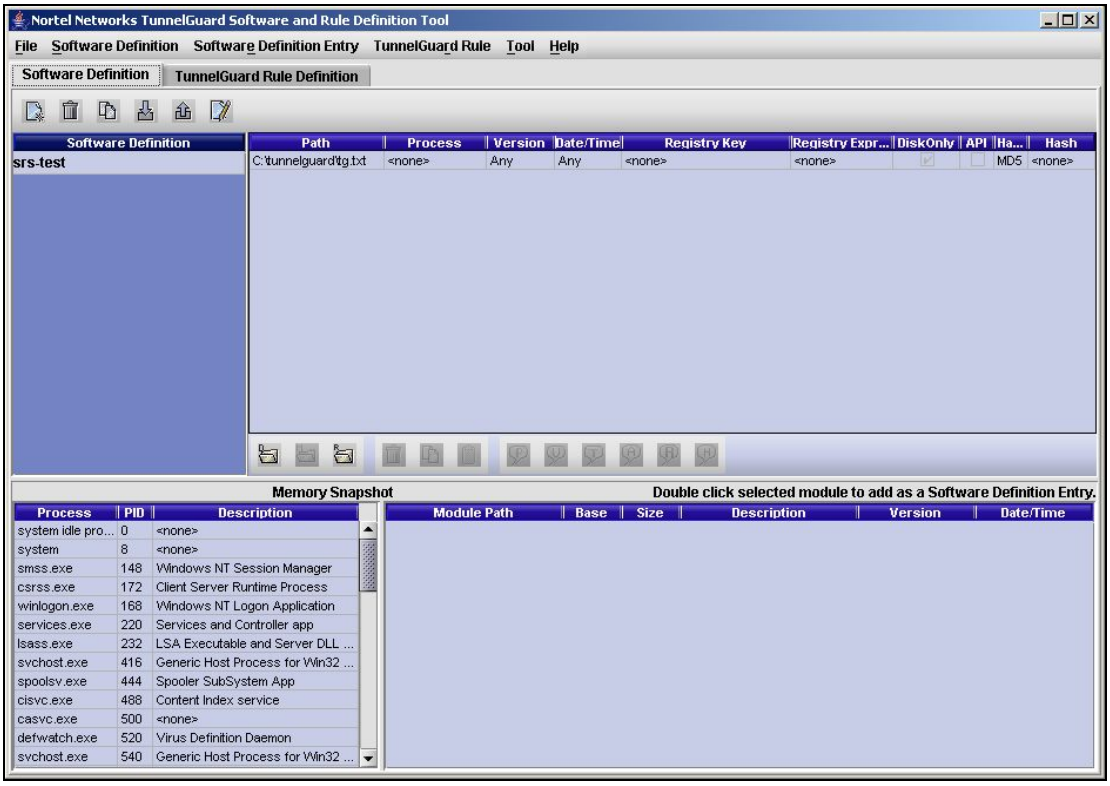


2. Go to SREM file menu and click on TunnelGuard



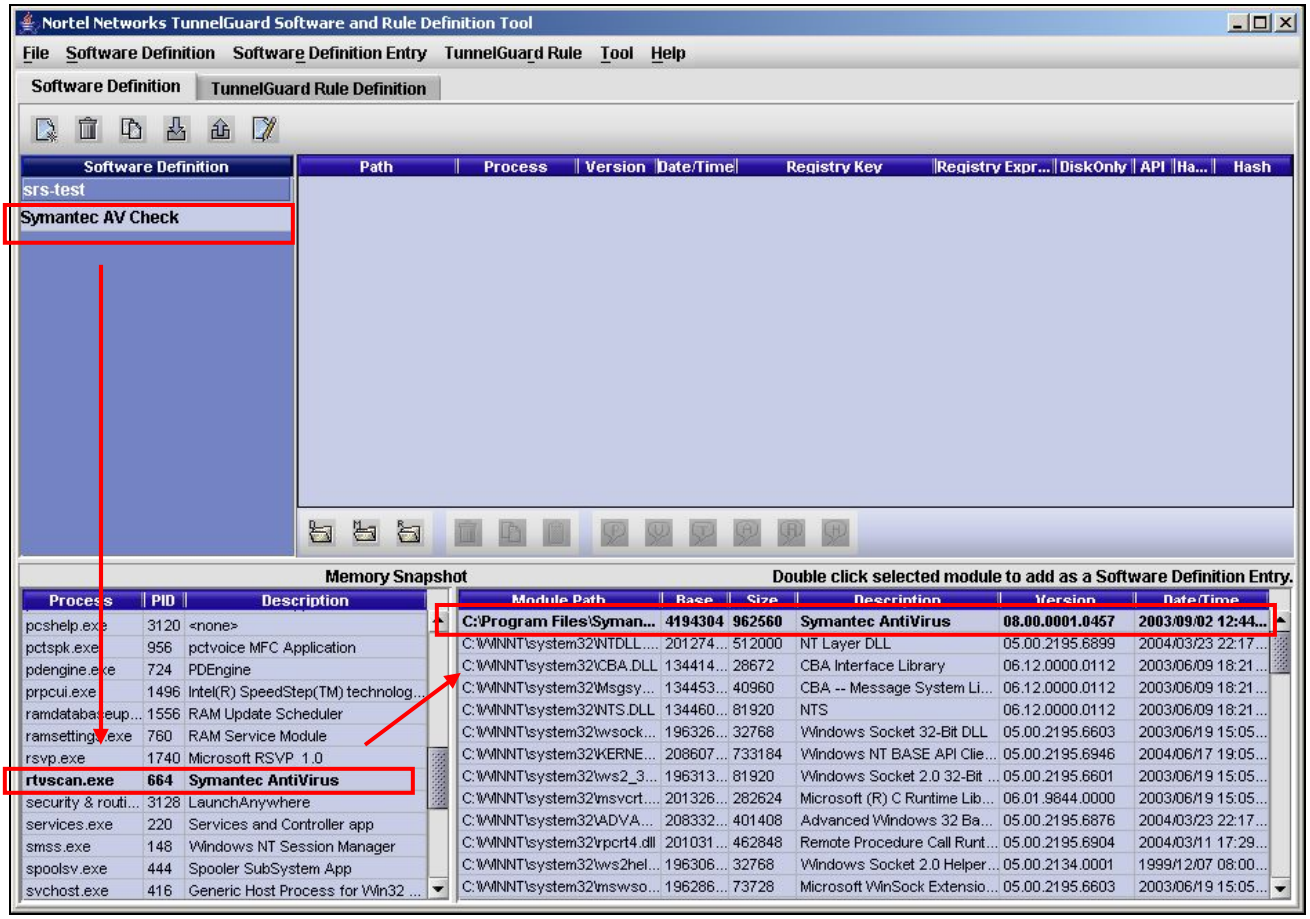
3. Select Domain 1 for the Domain ID then click “OK”.

4. An existing software definition called “srs-test” is displayed; this was created by the NSNAS setup wizard during the initial configuration.

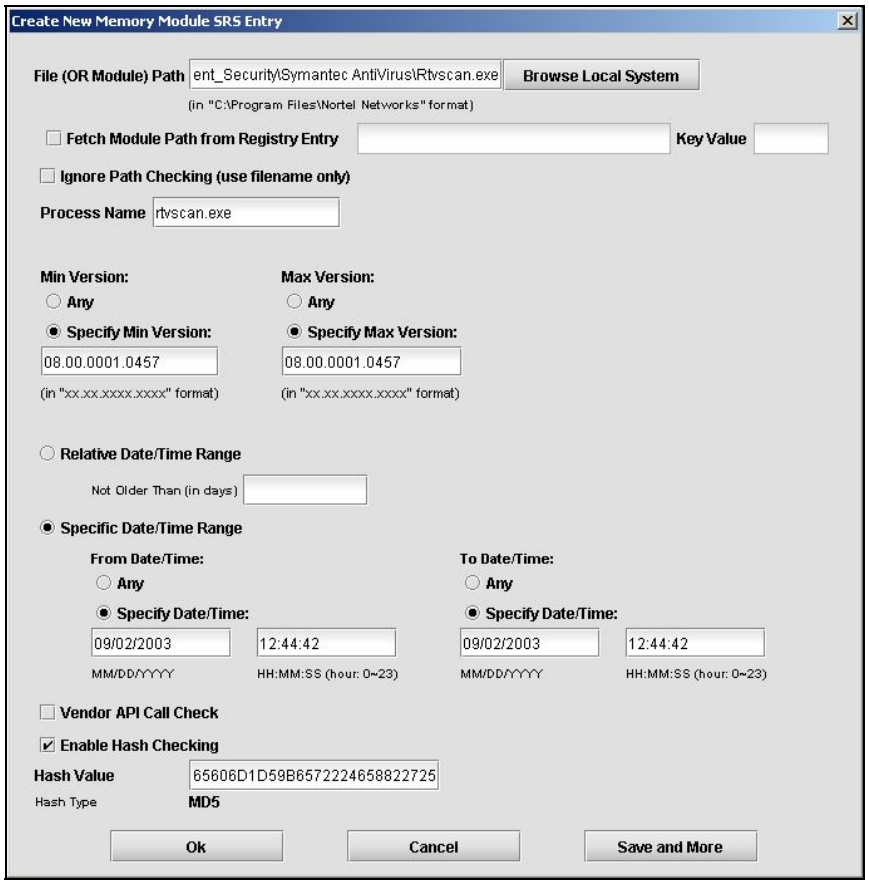


5. Create a new SRS Definition. From the file menu ***Software Definition->New Software Definition***. Call the definition Symantec AV Check.

6. Select the desired process from the management PC. The lower left section of the Editor contains all running software processes running on the local host using the SRS Policy Editor (it's a memory snap shot that occurs when the editor is started. Find and select the process for Symantec Antivirus, *rtvscan.exe* (assuming that the machine has it currently running). In the lower right section of the Policy Editor all of the software modules associated with the process "rtvscan.exe" should appear when the process is selected. Double click the module for the Symantec Client itself.

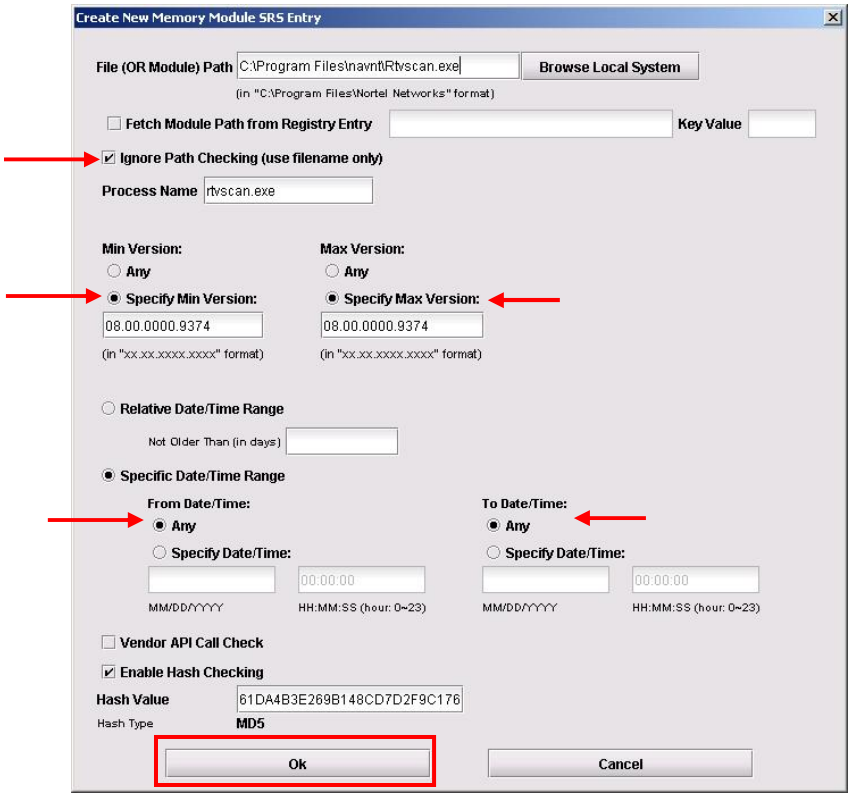

Nortel Networks TunnelGuard Software and Rule Definition Tool
File Software Definition Software Definition Entry TunnelGuard Rule Tool Help
Software Definition
TunnelGuard Rule Definition
Software Definition
srs-test
Symantec AV Check
Path
Process
Version
Date/Time
Registry Key
Registry Expr...
DiskOnly
API
Ha...
Hash
Memory Snapshot
Double click selected module to add as a Software Definition Entry.
Process
PID
Description
pcshelp.exe 3120 <none>
pctspk.exe 956 pctvoice MFC Application
pdengine.exe 724 PDEngine
prpcui.exe 1496 Intel(R) SpeedStep(TM) technolog...
ramdatabaseup... 1556 RAM Update Scheduler
ramsetting.exe 760 RAM Service Module
rsvp.exe 1740 Microsoft RSVP 1.0
rtvscan.exe 664 Symantec AntiVirus
security & routi... 3128 LaunchAnywhere
services.exe 220 Services and Controller app
smss.exe 148 Windows NT Session Manager
spoolsv.exe 444 Spooler SubSystem App
svchost.exe 416 Generic Host Process for Win32 ...
Module Path
Base
Size
Description
Version
Date/Time
C:\Program Files\Syman... 4194304 962560 Symantec AntiVirus 08.00.0001.0457 2003/09/02 12:44...
C:\WINNT\system32\NTDLL.... 201274... 512000 NT Layer DLL 05.00.2195.6899 2004/03/23 22:17...
C:\WINNT\system32\CBA.DLL 134414... 28672 CBA Interface Library 06.12.0000.0112 2003/06/09 18:21...
C:\WINNT\system32\Msgsy... 134453... 40960 CBA -- Message System Li... 06.12.0000.0112 2003/06/09 18:21...
C:\WINNT\system32\NTS.DLL 134460... 81920 NTS 06.12.0000.0112 2003/06/09 18:21...
C:\WINNT\system32\wsock... 196326... 32768 Windows Socket 32-Bit DLL 05.00.2195.6603 2003/06/19 15:05...
C:\WINNT\system32\KERNE... 208607... 733184 Windows NT BASE API Clie... 05.00.2195.6946 2004/06/17 19:05...
C:\WINNT\system32\ws2_3... 196313... 81920 Windows Socket 2.0 32-Bit ... 05.00.2195.6601 2003/06/19 15:05...
C:\WINNT\system32\msvcrt.... 201326... 282624 Microsoft (R) C Runtime Lib... 06.01.9844.0000 2003/06/19 15:05...
C:\WINNT\system32\ADVA... 208332... 401408 Advanced Windows 32 Ba... 05.00.2195.6876 2004/03/23 22:17...
C:\WINNT\system32\rpcrt4.dll 201031... 462848 Remote Procedure Call Runt... 05.00.2195.6904 2004/03/11 17:29...
C:\WINNT\system32\ws2hel... 196306... 32768 Windows Socket 2.0 Helper... 05.00.2134.0001 1999/12/07 08:00...
C:\WINNT\system32\mswso... 196286... 73728 Microsoft WinSock Extensio... 05.00.2195.6603 2003/06/19 15:05...

7. The following window should appear. This shows the possible options when creating the SRS entry. Notice the options for checking versions, checking dates, checking registry values, etc.

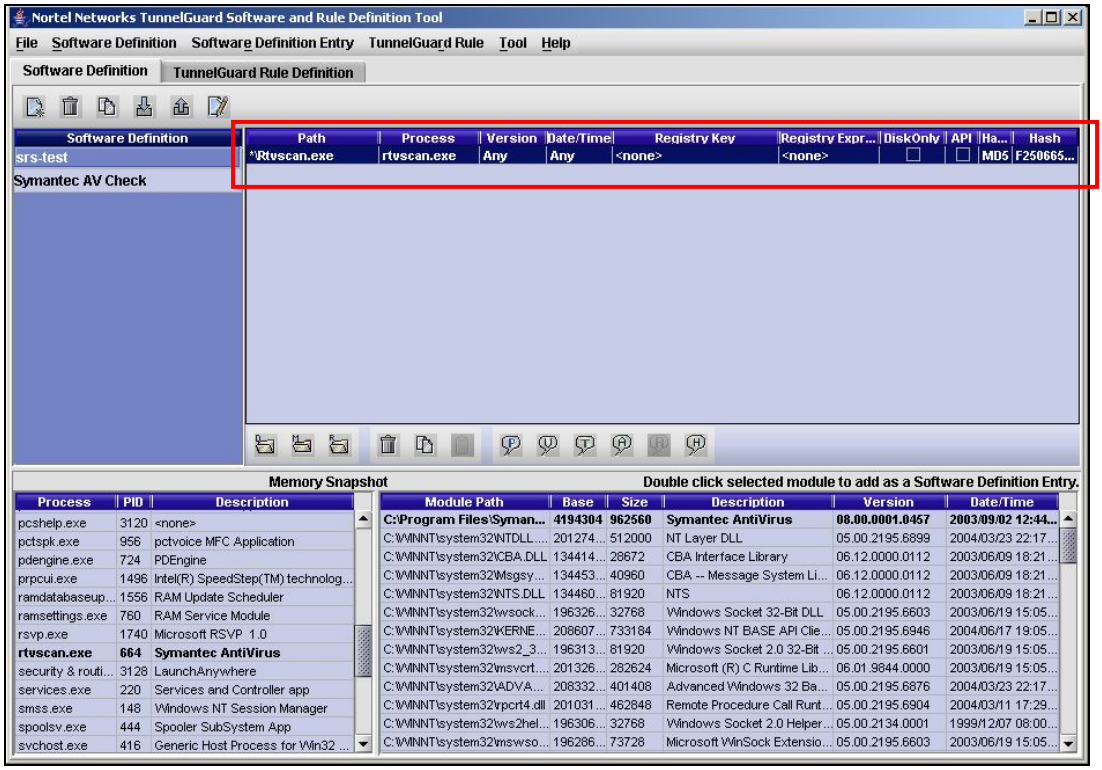


8. For the first SRS entry, modify the following settings for the SRS definition. For the purposes of this example, use the following parameters:

   Ignore Path Checking = "***check***"
   Min Version = **Specify minimum version required**
   Max Version = **Specify maximum version required**
   From Date/Time = **Any or specify date/time**
   To Date/Time = **Any or specify date/time**



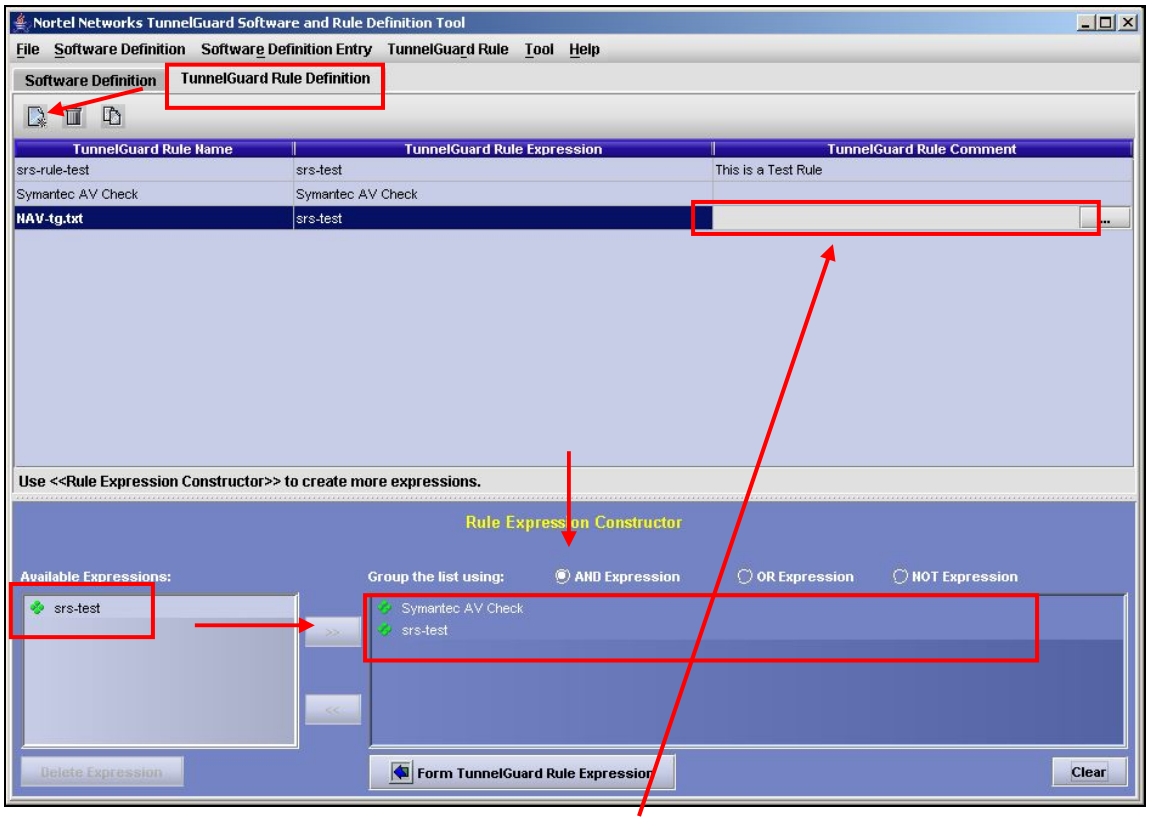
9. The SRS Entry should now be added to the list.

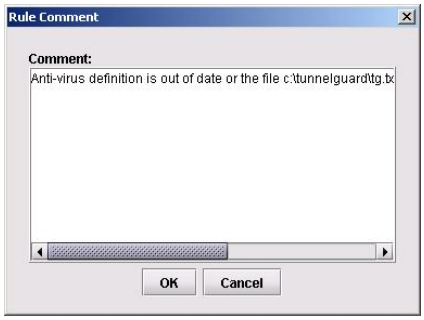


10. Create the rule definition. With TunnelGuard, there is an option to check for multiple expressions in each rule using Boolean expressions. This example will configure the Rule Definition to check for the existence of c:/tunnelguard/tg.txt and that the user is running Symantec AV.

    Go to the Rule Constructor Menu by clicking the "TunnelGuard Definition" tab. Create a new rule from the file menu (TunnelGuard Rule->New TunnelGuard Rule or the "New" icon) and name it "NAV-tg.txt."

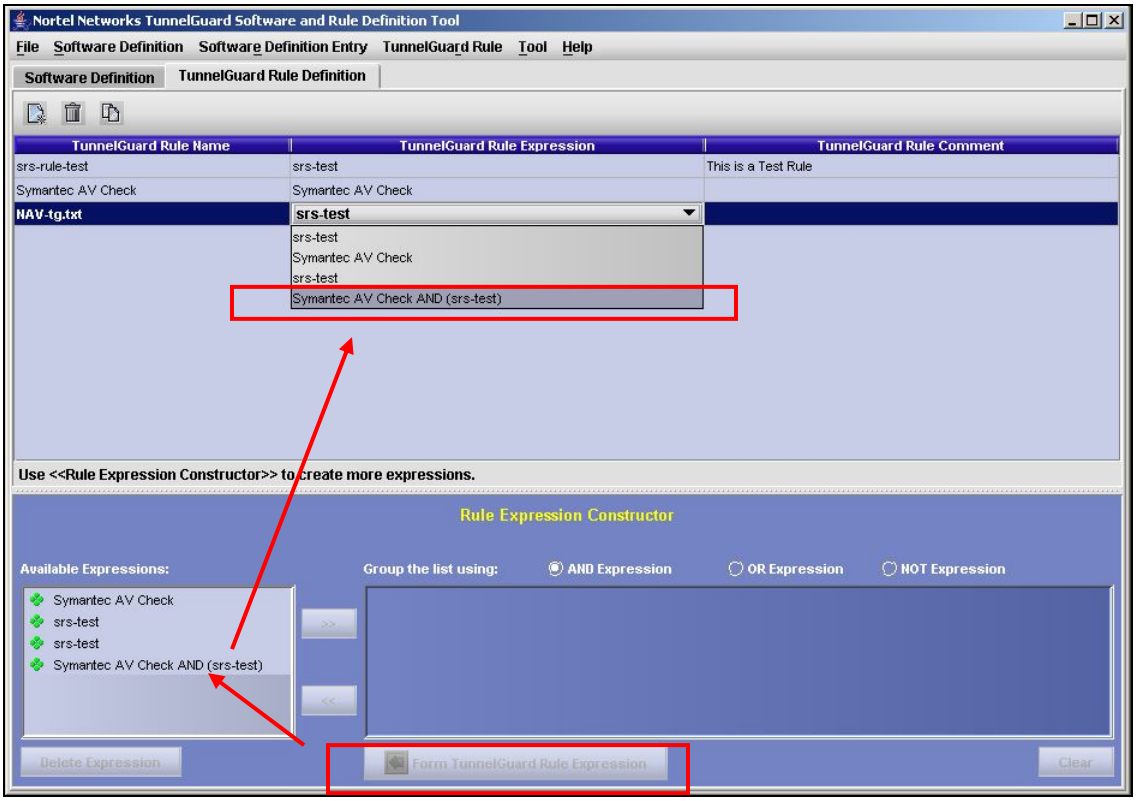
    Next construct a rule expression for the new rule to look for the definitions "Symantec AV Check" AND "srs-test." Do this by selecting "Symantec AV Check" under Available Expressions, click the ">>" button, select the "AND Expression" radio button, then select the "srs-test" Expression, followed again by the ">>" button.





Add any comment here for when tunnel guard fails. This message will be sent to the end user when tunnel guard fails this rule.

11. Finish off the expression. Click the “Form TunnelGuard Rule Expression” button at the bottom of the screen to construct this expression. For the “NAV-tg.txt” rule select the “Symantec AV Check AND srs-test” expression.



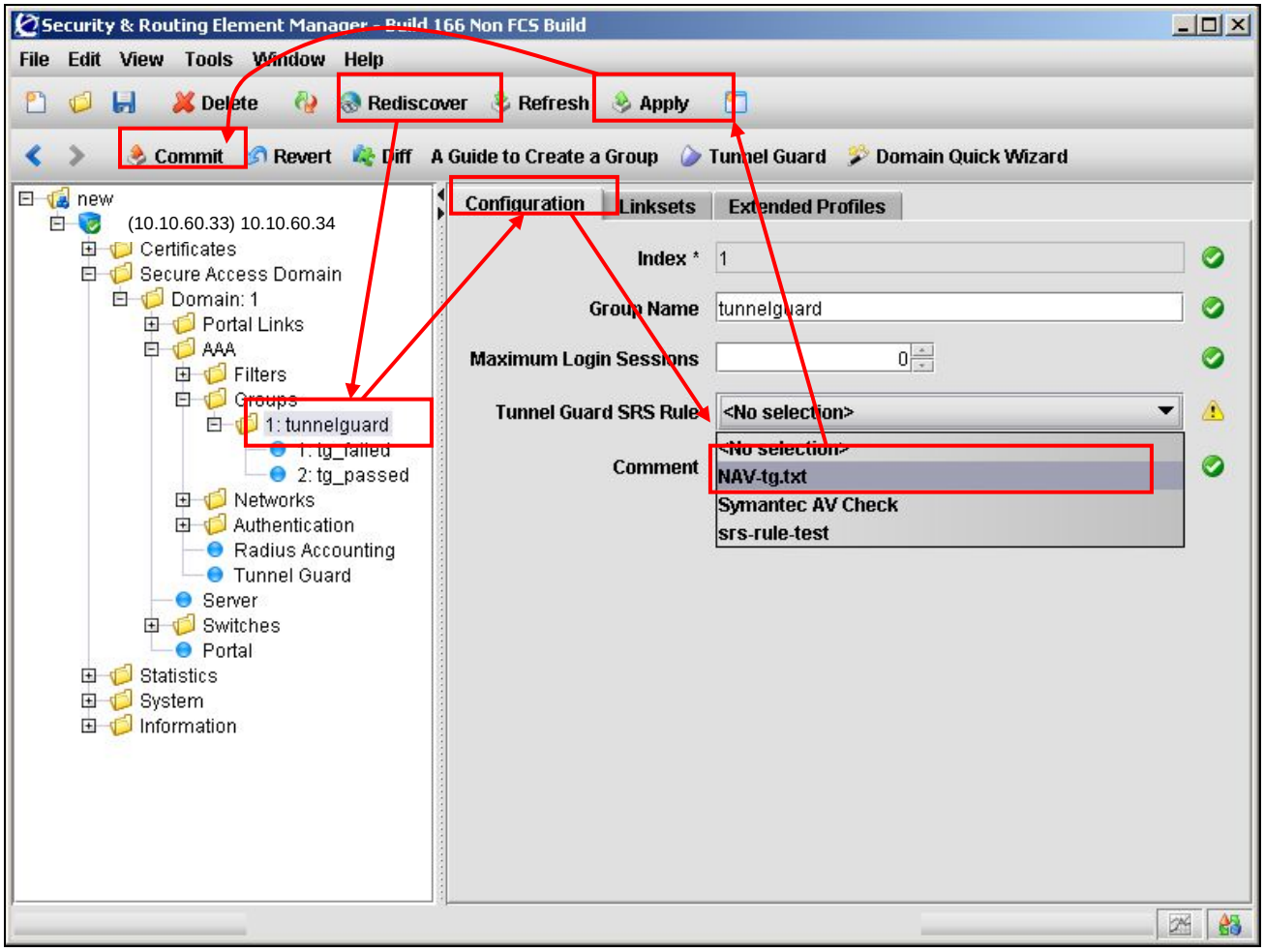
12. Save the SRS Policy (File->Save) and exit the SRS Policy Editor (File->Exit).

13. Apply and commit the changes. Go to SREM and click the “Rediscover” button in the SREM file menu bar. Now expand the tree on the left of SREM and go to

    Secure Access Domain ->Domain 1->AAA->Groups->1: tunnelguard

    On the Configuration tab, select the TunnelGuard SRS rule “Symantec and tg.txt” then

    Apply -> Commit

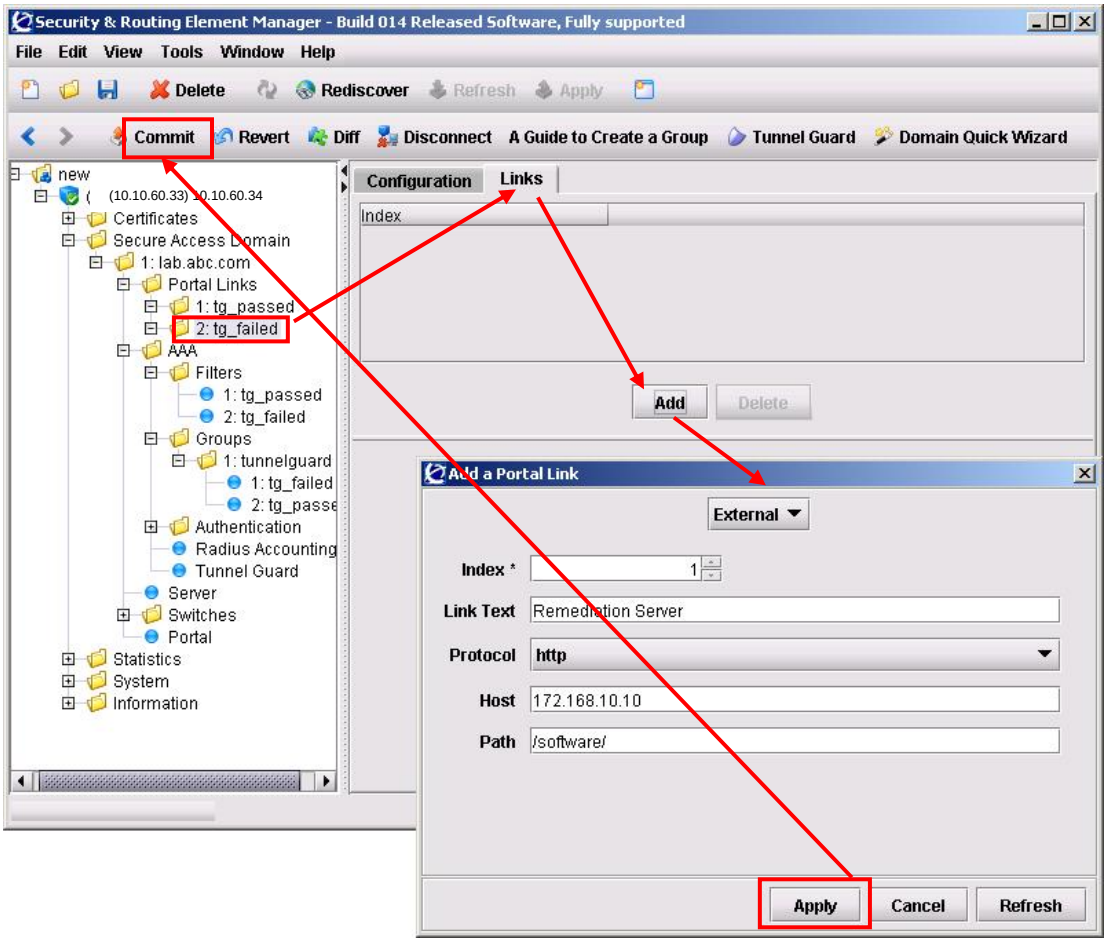


14. When TunnelGuard fails, SREM can be setup to send a link to the end user as to where to get remediation software. For example, assuming we wish to send to the client the HTTP address of the remediation server when TunnelGuard fails, go to

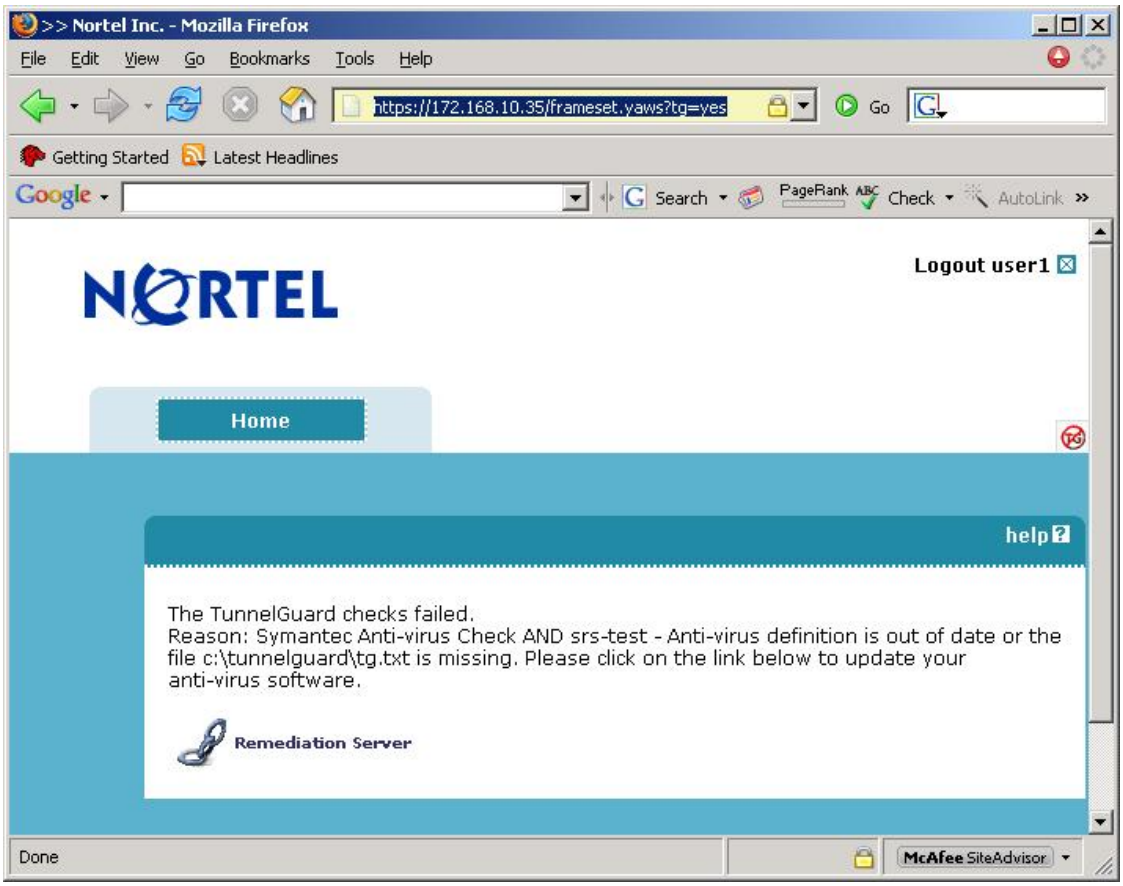
    Secure Access Domain ->domain name->Portal Links -> 2:tg_failed

    On the Links tab, click on *Add*

    Select *External;* enter the text you wish to send to the end user via the *Link Text* box, the HTTP address and the path where the software is located.



15. If TunnelGuard fails, the user should be prompted with a page such as the one shown below.



5. Appendix B

5.1 Create a Basic TunnelGuard SRS Rule

Configure a default TunnelGuard SRS rule that will check for the presence of the c:\tunnelguard\tg.txt file. Although this is a very basic check, TunnelGuard can be configured to check for many other criteria including the presence of security products such as firewalls, security patches, etc. A TunnelGuard user does not need to be created since it was created in the previous step.

```
>> Main# /cfg/domain 1/aaa/group 1/tgsrs srs-rule-test

>> Group 1# /cfg/domain 1/aaa/tg/quick

In the event that the TunnelGuard checks fails on a client,
the session can be teardown, or left in restricted mode
with limited access.
Which action do you want to use for TunnelGuard
failure? (teardown/restricted) [restricted]: restricted
Do you want to create a tunnelguard test user? (yes/no) [yes]: no
Using existing tg_passed filter
Using existing tg_failed filter
Using existing tg_passed linkset
Using existing tg_failed linkset
Adding test SRS rule srs-rule-test
  This rule check for the presence of the file
  C:\tunnelguard\tg.txt
Using existing tg_passed filter

Use 'diff' to view pending changes, and 'apply' to commit

>> TG# diff
Configuration/
  Domain 1/
    AAA/
      Group 1/
        TunnelGuard SRS Rule: "" -> srs-rule-test

>> TG# apply
Changes applied successfully.
```

6. Appendix C – Configuration Files

6.1 From Example 2.1: ERS5500 using SNAS

```
! *** IP ***
!
ip bootp server needed
ip default-gateway 10.24.24.1
ip address netmask 255.255.255.0
ip address stack 0.0.0.0
ip address switch 10.24.24.62
!
!
! *** VLAN ***
!
vlan configcontrol autopvid
auto-pvid
vlan name 1 "VLAN #1"
vlan create 10 name "vlan10_subnet_1" type port
vlan ports 1-6 tagging unTagAll filter-untagged-frame disable filter-unregistered-frames
enable priority 0
vlan ports 7 tagging tagAll filter-untagged-frame disable filter-unregistered-frames
enable priority 0
vlan ports 8-24 tagging unTagAll  filter-untagged-frame disable filter-unregistered-
frames enable priority 0
vlan members 1 NONE
vlan members 10 3-7
vlan ports 1-2 pvid 1
vlan ports 3-6 pvid 10
vlan ports 7 pvid 1
vlan ports 8-24 pvid 1
!
! *** QOS ***
!
qos agent reset-default
qos if-group name "vlan_10" class untrusted
qos if-assign port 3-6 name vlan_10
interface FastEthernet ALL
exit
qos ip-element 1 src-ip 10.24.24.16/28 dst-ip 10.10.60.35/32 protocol 17 dst-port-min 53
dst-port-max 53
qos ip-element 2 protocol 17 dst-port-min 67 dst-port-max 67
qos ip-element 3 protocol 1
qos ip-element 4 dst-ip 10.10.60.0/24 protocol 6 dst-port-min 80 dst-port-max 8
0
qos ip-element 5 dst-ip 10.10.60.0/24 protocol 6 dst-port-min 443 dst-port-max 443
qos ip-element 6 src-ip 10.24.24.48/28
qos ip-element 7
qos classifier 1 set-id 1 name "red_dns" element-type ip element-id 1
qos classifier 2 set-id 2 name dhcp element-type ip element-id 2
qos classifier 3 set-id 3 name icmp element-type ip element-id 3
qos classifier 4 set-id 4 name http element-type ip element-id 4
qos classifier 5 set-id 5 name https element-type ip element-id 5
qos classifier 6 set-id 6 name green element-type ip element-id 6
qos classifier 7 set-id 7 name "drop_all" element-type ip element-id 7
qos agent nvram-delay 10
qos agent buffer large
qos agent queue-set 2
qos agent ubp disable
qos policy 1 name "red_dns" if-group "vlan_10" clfr-type classifier clfr-id 1 in-profile-
action 2 precedence 13 track-statistics individual
qos policy 2 name dhcp if-group "vlan_10" clfr-type classifier clfr-id 2 in-profile-
action 2 precedence 12 track-statistics individual
qos policy 3 name icmp if-group "vlan_10" clfr-type classifier clfr-id 3 in-profile-
action 2 precedence 11 track-statistics individual
```

```
qos policy 4 name http if-group "vlan_10" clfr-type classifier clfr-id 4 in-profile-
action 2 precedence 10 track-statistics individual
qos policy 5 name https if-group "vlan_10" clfr-type classifier clfr-id 5 in-profile-
action 2 precedence 9 track-statistics individual
qos policy 6 name green if-group "vlan_10" clfr-type classifier clfr-id 6 in-profile-
action 2 precedence 8 track-statistics individual
qos policy 7 name "drop_all" if-group "vlan_10" clfr-type classifier clfr-id 7 in-
profile-action 1 precedence 7 track-statistics individual
!
! *** DHCP SNOOPING ***
!
ip dhcp-snooping
no ip dhcp-snooping vlan
ip dhcp-snooping vlan 10
interface FastEthernet ALL
default ip dhcp-snooping
ip dhcp-snooping port 7 trusted
exit
!
! *** ARP INPSECTION ***
!
no ip arp-inspection vlan
ip arp-inspection vlan 10
interface FastEthernet ALL
default ip arp-inspection
ip arp-inspection port 7 trusted
exit
!
```

6.2 From Example 2.3: ES470 using SNAS

ES470

```
!
! *** IP ***
!
ip bootp server needed
ip default-gateway 10.24.24.1
ip address netmask 255.255.255.0
ip address stack 0.0.0.0
ip address switch 10.24.24.62
!
! *** VLAN ***
!
auto-pvid
vlan name 1 "VLAN #1"
vlan create 10 name "VLAN-10_nsas" type port learning ivl
vlan ports 1-36 tagging unTagAll filter-tagged-frame disable filter-untagged-frame
disable  priority 0
vlan ports 37 tagging tagAll filter-tagged-frame disable filter-untagged-frame disable
priority 0
vlan ports 38-48 tagging unTagAll filter-tagged-frame disable filter-untagged-f
rame disable  priority 0
vlan members 1 NONE
vlan members 10 33-37
vlan ports 1-32 pvid 1
vlan ports 32-37 pvid 10
vlan ports 38-48 pvid 1
vlan mgmt 10
!
!
! *** QOS ***
!
qosagent reset-default
qos if-group name "vlan_10" create class untrusted
qos if-group name "test" create class untrusted
qos if-assign-list del portlist 33
qos if-assign-list add portlist 33 name vlan_10
```

```
qos if-assign-list del portlist 34
qos if-assign-list add portlist 34 name vlan_10
qos if-assign-list del portlist 35
qos if-assign-list add portlist 35 name vlan_10
qos if-assign-list del portlist 36
qos if-assign-list add portlist 36 name vlan_10
qosagent server-control disable retry-timer 5
qosagent packet-reordering enable
qosagent class-restrictions all-classes
qos ip-filter 1 create src-ip 10.24.24.16 255.255.255.240 dst-ip 10.10.60.35
255.255.255.255 protocol udp dst-port 53
qos ip-filter 2 create src-ip 10.24.24.32 255.255.255.240 dst-ip 10.10.60.35
255.255.255.255 protocol udp dst-port 53
qos ip-filter 3 create src-ip 10.24.24.32 255.255.255.240 dst-ip 172.30.30.20
255.255.255.255
qos ip-filter 4 create src-ip 0.0.0.0 0.0.0.0 dst-ip 0.0.0.0 0.0.0.0 protocol udp dst-
port 67
qos ip-filter 5 create src-ip 0.0.0.0 0.0.0.0 dst-ip 0.0.0.0 0.0.0.0 protocol icmp
qos ip-filter 6 create src-ip 0.0.0.0 0.0.0.0 dst-ip 10.10.60.0 255.255.255.0 protocol
tcp dst-port 80
qos ip-filter 7 create src-ip 0.0.0.0 0.0.0.0 dst-ip 10.10.60.0 255.255.255.0 protocol
tcp dst-port 443
qos ip-filter 8 create src-ip 10.24.24.48 255.255.255.240 dst-ip 0.0.0.0 0.0.0.0
qos ip-filter 9 create src-ip 0.0.0.0 0.0.0.0 dst-ip 0.0.0.0 0.0.0.0
qos ip-filter-set 1 create set 1 name allow filter 1 filter-prec 1
qos ip-filter-set 2 create set 1 name allow filter 2 filter-prec 2
qos ip-filter-set 3 create set 1 name allow filter 3 filter-prec 3
qos ip-filter-set 4 create set 1 name allow filter 4 filter-prec 4
qos ip-filter-set 5 create set 1 name allow filter 5 filter-prec 5
qos ip-filter-set 6 create set 1 name allow filter 6 filter-prec 6
qos ip-filter-set 7 create set 1 name allow filter 7 filter-prec 7
qos ip-filter-set 8 create set 1 name allow filter 8 filter-prec 8
qos ip-filter-set 9 create set 2 name deny_all filter 9 filter-prec 1
qos policy 1 create name \"non_snas_fwd\" if-group vlan_10 filter-set-type ip filter-set
1 in-profile-action 65527   order 1
qos policy 2 create name \"non_snas_drop\" if-group vlan_10 filter-set-type ip filter-set
2 in-profile-action 65526   order 2
!
```

6.3 From Example 2.4: WLAN Security Switch 2300 Using SNAS

```
# Configuration nvgen'd at 2007-1-22 20:04:03
# Image 5.0.7.1.0
# Model 2360
# Last change occurred at 2007-1-22 20:03:35
set ip route default 10.24.24.1 1
set system name WSS2360-1
set system ip-address 10.24.24.10
set system countrycode US
set service-profile NSNA-1X ssid-name NSNA-1X
set service-profile NSNA-1X dhcp-restrict enable
set service-profile NSNA-1X keep-initial-vlan enable
set service-profile NSNA-1X wpa-ie enable
set service-profile NSNA-1X attr vlan-name VLAN10
set service-profile NSNA-1X attr filter-id NSNA.in
set service-profile NSNA-PSK ssid-name NSNA-PSK
set service-profile NSNA-PSK dhcp-restrict enable
set service-profile NSNA-PSK auth-fallthru last-resort
set service-profile NSNA-PSK keep-initial-vlan enable
set service-profile NSNA-PSK wpa-ie enable
set service-profile NSNA-PSK auth-psk enable
set service-profile NSNA-PSK psk-phrase nortel
set service-profile NSNA-PSK attr vlan-name VLAN10
set service-profile NSNA-PSK attr filter-id NSNA.in
set radius server W3KServer address 172.30.30.20 key nortel
set server group IAS members W3KServer
```

set enablepass password nortel
set authentication dot1x ssid NSNA-1X ** pass-through IAS
set user admin password encrypted nortel
set radio-profile default service-profile NSNA-1X
set radio-profile default service-profile NSNA-PSK
set dap 1 serial-id stp1w20kc3 model 2330
set dap 1 name 233X-1
set dap 1 radio 1 channel 1 tx-power 10 mode enable
set dap 1 radio 2 channel 60 tx-power 10 mode enable
set ip https server enable
set vlan 1 name VLAN10
set vlan 1 port 1
set vlan 1 port 2
set vlan 1 port 3
set vlan 1 port 4
set vlan 1 port 5
set vlan 1 port 6
set vlan 1 port 7
set vlan 1 port 8
set interface 1 ip 10.24.24.10 255.255.255.0
set security acl ip NSNA permit ip 10.24.24.0 0.0.0.255 10.24.24.1 0.0.0.0
set security acl ip NSNA permit udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 range 67 68
set security acl ip NSNA permit udp 10.24.24.16 0.0.0.15 10.10.60.35 0.0.0.0 eq 53
set security acl ip NSNA permit tcp 10.24.24.16 0.0.0.15 10.10.60.35 0.0.0.0 eq 80
set security acl ip NSNA permit tcp 10.24.24.16 0.0.0.15 10.10.60.35 0.0.0.0 eq 443
set security acl ip NSNA permit udp 10.24.24.32 0.0.0.15 10.10.60.35 0.0.0.0 eq 53
set security acl ip NSNA permit tcp 10.24.24.32 0.0.0.15 10.10.60.35 0.0.0.0 eq 443
set security acl ip NSNA permit tcp 10.24.24.32 0.0.0.15 172.30.30.20 0.0.0.0 eq 80
set security acl ip NSNA permit 10.24.24.48 0.0.0.15
commit security acl NSNA

6.4 From Example 3.1: ERS8600 and NSAS Configurations

ERS8600:

```
#
# VLAN CONFIGURATION
#

vlan 1 ports remove 2/1-2/3,3/1-3/48 member portmember
vlan 5 create byport 1 name "VLAN-5_non_snas" color 2
vlan 5 ports remove 2/1-2/3,3/1-3/12,3/14-3/48,4/1-4/30 member portmember
vlan 5 ports add 3/13 member portmember
vlan 5 ip create 10.24.26.1/255.255.255.0 mac_offset 9
vlan 5 ip dhcp-relay enable
vlan 5 ip dhcp-relay mode dhcp
vlan 5 ip ospf interface-type passive
vlan 5 ip ospf enable

#
# DHCP CONFIGURATION
#

ip dhcp-relay create-fwd-path agent 10.24.26.1 server 10.10.60.34 mode dhcp state enable

#
# OSPF CONFIGURATION
#

ip ospf admin-state enable
ip ospf router-id 129.42.133.0
ip ospf enable

#
# R-MODULE FILTER CONFIGURATION
#
```

```
filter act 1 create name "ACT-1_non_snas"
filter act 1 ethernet vlan
filter act 1 ip srcIp,dstIp,ipProtoType
filter act 1 protocol tcpDstPort,udpDstPort,icmpMsgType
filter act 1 arp operation
filter act 1 apply
filter acl 1 create inPort act 1
filter acl 1 set global-action count
filter acl 1 port add 3/13
filter acl 1 ace 1 create name "icmp"
filter acl 1 ace 1 action permit
filter acl 1 ace 1 ethernet vlan-id eq 5
filter acl 1 ace 1 ip ip-protocol-type eq icmp
filter acl 1 ace 1 enable
filter acl 1 ace 2 create name "dhcp"
filter acl 1 ace 2 action permit
filter acl 1 ace 2 ethernet vlan-id eq 5
filter acl 1 ace 2 protocol udp-dst-port eq 67
filter acl 1 ace 2 enable
filter acl 1 ace 3 create name "red_yellow_dns"
filter acl 1 ace 3 action permit
filter acl 1 ace 3 ethernet vlan-id eq 5
filter acl 1 ace 3 ip src-ip eq 10.24.26.17-10.24.26.46
filter acl 1 ace 3 ip dst-ip eq 10.10.60.35
filter acl 1 ace 3 protocol udp-dst-port eq dns
filter acl 1 ace 3 enable
filter acl 1 ace 4 create name "yellow_redem"
filter acl 1 ace 4 action permit
filter acl 1 ace 4 ethernet vlan-id eq 5
filter acl 1 ace 4 ip src-ip eq 10.24.26.33-10.24.26.46
filter acl 1 ace 4 ip dst-ip eq 172.30.30.20
filter acl 1 ace 4 enable
filter acl 1 ace 5 create name "http"
filter acl 1 ace 5 action permit
filter acl 1 ace 5 ethernet vlan-id eq 5
filter acl 1 ace 5 ip dst-ip eq 10.10.60.1-10.10.60.255
filter acl 1 ace 5 protocol tcp-dst-port eq 80
filter acl 1 ace 5 enable
filter acl 1 ace 6 create name "https"
filter acl 1 ace 6 action permit
filter acl 1 ace 6 ethernet vlan-id eq 5
filter acl 1 ace 6 ip dst-ip eq 10.10.60.1-10.10.60.255
filter acl 1 ace 6 protocol tcp-dst-port eq 443
filter acl 1 ace 6 enable
filter acl 1 ace 7 create name "green"
filter acl 1 ace 7 action permit
filter acl 1 ace 7 ethernet vlan-id eq 5
filter acl 1 ace 7 ip src-ip eq 10.24.26.49-10.24.26.62
filter acl 1 ace 7 enable
filter acl 1 ace 8 create name "arp_req"
filter acl 1 ace 8 action permit
filter acl 1 ace 8 ethernet vlan-id eq 5
filter acl 1 ace 8 arp operation eq arprequest
filter acl 1 ace 8 enable
filter acl 1 ace 9 create name "arp_rpse"
filter acl 1 ace 9 action permit
filter acl 1 ace 9 ethernet vlan-id eq 5
filter acl 1 ace 9 arp operation eq arpresponse
filter acl 1 ace 9 enable
filter acl 1 ace 10 create name "deny_all"
filter acl 1 ace 10 action deny
filter acl 1 ace 10 ethernet vlan-id eq 5
filter acl 1 ace 10 enable
```

SNAS:

```
/*
/*
/* Configuration dump taken Tue Jun 27 09:55:04 EDT 2006
```

```
/* Version 1.4.1
/*
/*
/*
/cfg/.
/cfg/cert 1/.
        name test_cert
        cert
-----BEGIN CERTIFICATE-----
MIIEajCCA9OgAwIBAgIBADANBgkqhkiG9w0BAQQFADCBvzELMAkGA1UEBhMCVVMx
EzARBgNVBAgTCkNhbGlmb3JuaWExEDAOBgNVBAcTB1Rlc3RpbmcxKDAmBgNVBAoT
H1Rlc3QgSW5jLiAxIDEwOjMxOjM5IDIwMDYtMDYtMjIxEjAQBgNVBAsTCXRlc3Qg
ZGVwdDEgMB4GA1UEAxMXd3d3LmR1bW15c3NsdGVzdGluZy5jb20xKTAnBgkqhkiG
9w0BCQEWGnRlc3RlckBkdW1teXNzbHRlc3RpbmcuY29tMB4XDTA2MDYyMjE0MzEz
OVoXDTA3MDYyMjE0MzEzOVowgb8xCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxp
Zm9ybmlhMRAwDgYDVQQHEwdUZXN0aW5nMSgwJgYDVQQKEx9UZXN0IEluYy4gMSAx
MDozMTozOSAyMDA2LTA2LTIyMRIwEAYDVQQLEwl0ZXN0IGRlcHQxIDAeBgNVBAMT
F3d3dy5kdW1teXNzbHRlc3RpbmcuY29tMSkwJwYJKoZIhvcNAQkBFhp0ZXN0ZXJA
ZHVtbXlzc2x0ZXN0aW5nLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
zWyfgzYN39IBO/gabPqqCDKx3BPxfRqsxvgE4BXEyqtNIyKBl2MqnhhryUWSZ+iD
+KO+t9cf8ExdqWqqEwnn+sHGcnwnFBttqh041uIX5IMLuNBiOHkrTSjy6yNJk9On
JRHP9WZWmBLXwX4osgibP5Sux1yKSdgnZUwqYD0PFVECAwEAAaOCAXIwggFuMAwG
A1UdEwQFMAMBAf8wEQYJYIZIAYb4QgEBBAQDAgJEMDIGCWCGSAGG+EIBDQQlFiNB
bHRlb24vTm9ydGVsIEdlbmVyYXRlZCBDZXJ0aWZpY2F0ZTAdBgNVHQ4EFgQUcsEl
19CmJl+Sic+36AMDreAbLYYwgewGA1UdIwSB5DCB4YAUcsEl19CmJl+Sic+36AMD
reAbLYahgcWkgcIwgb8xCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlh
MRAwDgYDVQQHEwdUZXN0aW5nMSgwJgYDVQQKEx9UZXN0IEluYy4gMSAxMDozMToz
OSAyMDA2LTA2LTIyMRIwEAYDVQQLEwl0ZXN0IGRlcHQxIDAeBgNVBAMTF3d3dy5k
dW1teXNzbHRlc3RpbmcuY29tMSkwJwYJKoZIhvcNAQkBFhp0ZXN0ZXJAZHVtbXlz
c2x0ZXN0aW5nLmNvbYIBADAJBgNVHRIEAjAAMA0GCSqGSIb3DQEBBAUAA4GBAL6/
oV7SW1/UEVnW2YhvawE7Zbc6Njvw/cLUauhV2UchQoZW/VW3yTkbUn2Bo7G3WvcO
m7q+sHXEfMo9vO3tPK0LxrYIeNQUZZiq+TTbZ3aPq4rr+z+E4N74m2z+Wgfm73by
LqrNtndaFFO/ieK/Cow1LetLBkn1ODHTFL092XKD
-----END CERTIFICATE-----

...
/cfg/cert 1/revoke/.
/cfg/cert 1/revoke/automatic/.
        interval 1d
        ena disabled
/cfg/domain 1/.
        name abc.lab.com
        pvips 10.10.60.35
/cfg/domain 1/aaa/.
        authorder 1
/cfg/domain 1/aaa/tg/.
        recheck 15m
        heartbeat 1m
        hbretrycnt 3
        status-quo off
        action restricted
        details off
        loglevel info
/cfg/domain 1/aaa/auth 1/.
        type local
        name local
/cfg/domain 1/aaa/auth 1/local/.
/cfg/domain 1/aaa/auth 1/adv/.
/cfg/domain 1/aaa/auth 1/macdb/.
/cfg/domain 1/aaa/filter 1/.
        name tg_passed
        tg true
/cfg/domain 1/aaa/filter 2/.
        name tg_failed
        tg false
/cfg/domain 1/aaa/group 1/.
        name tunnelguard
        restrict 0
```

```
        tgsrs srs-rule-test
        mactrust none
        tgmode continous
        macreg false
        enftype vlan_filter
/cfg/domain 1/aaa/group 1/linkset/.
/cfg/domain 1/aaa/group 1/extend 1/.
        filter tg_failed
        vlan yellow
/cfg/domain 1/aaa/group 1/extend 1/linkset/.
        add tg_failed
/cfg/domain 1/aaa/group 1/extend 2/.
        filter tg_passed
        vlan green
/cfg/domain 1/aaa/group 1/extend 2/linkset/.
        add tg_passed
/cfg/domain 1/aaa/group 1/admrights/.
        user administrator
        action no_access
/cfg/domain 1/aaa/radacct/.
        ena false
/cfg/domain 1/aaa/radacct/servers/.
/cfg/domain 1/aaa/radacct/vpnattribute/.
        vendorid "1872 (alteon)"
        vendortype 3
/cfg/domain 1/server/.
        port "443 (https)"
        interface 0
/cfg/domain 1/server/trace/.
/cfg/domain 1/server/ssl/.
        cert 1
        cachesize 4000
        cachettl 5m
        protocol ssl3
        verify none
        ciphers ALL@STRENGTH
        ena enabled
/cfg/domain 1/server/adv/.
/cfg/domain 1/server/adv/traflog/.
        sysloghost 0.0.0.0
        udpport 514
        priority info
        facility local4
        ena disabled
/cfg/domain 1/portal/.
        logintext
This is a configurable text.
...
        iconmode fancy
        linktext
        linkurl off
        linkcols 2
        linkwidth 100%
        companyname "Nortel Inc."
        applet on
        ieclear on
/cfg/domain 1/portal/colors/.
        color1 #58b2c9
        color2 #d0e4e9
        color3 #2088a2
        color4 #accdd5
/cfg/domain 1/portal/content/.
        ena disabled
/cfg/domain 1/portal/lang/.
        setlang en
/cfg/domain 1/portal/lang/beconv/.
/cfg/domain 1/linkset 1/.
        name tg_passed
```

```
        text "The TunnelGuard checks succeeded!"
        autorun false
/cfg/domain 1/linkset 2/.
        name tg_failed
        text "The TunnelGuard checks failed.<br>Reason: <var:tgFa
ilureReason><br>"
        autorun false
/cfg/domain 1/vlan/.
        add yellow 120
        add green 110
/cfg/domain 1/dhcp/.
/cfg/domain 1/dhcp/subnet 1/.
        type hub
        name non_snas
        address 10.24.24.0
        netmask 255.255.255.0
        phone Nortel-i2004
        relaygreen 0.0.0.0
        ena enabled
/cfg/domain 1/dhcp/subnet 1/red/.
/cfg/domain 1/dhcp/subnet 1/red/ranges/.
        add 10.24.24.17 10.24.24.30
/cfg/domain 1/dhcp/subnet 1/red/stdopts 191/.
        value VLAN-A:99.
/cfg/domain 1/dhcp/subnet 1/yellow/.
/cfg/domain 1/dhcp/subnet 1/yellow/ranges/.
        add 10.24.24.33 10.24.24.46
/cfg/domain 1/dhcp/subnet 1/green/.
/cfg/domain 1/dhcp/subnet 1/green/ranges/.
        add 10.24.24.49 10.24.24.61
/cfg/domain 1/dhcp/subnet 1/green/stdopts 6/.
        value 10.10.30.5
/cfg/domain 1/dhcp/subnet 2/.
        type hub
        name non_snas_8600b
        address 10.24.26.0
        netmask 255.255.255.0
        phone Nortel-i2004-A
        relaygreen 0.0.0.0
        ena enabled
/cfg/domain 1/dhcp/subnet 2/red/.
/cfg/domain 1/dhcp/subnet 2/red/ranges/.
        add 10.24.26.17 10.24.26.30
/cfg/domain 1/dhcp/subnet 2/red/stdopts 3/.
        value 10.24.26.1
/cfg/domain 1/dhcp/subnet 2/yellow/.
/cfg/domain 1/dhcp/subnet 2/yellow/ranges/.
        add 10.24.26.33 10.24.26.46
/cfg/domain 1/dhcp/subnet 2/yellow/stdopts 3/.
        value 10.24.26.1
/cfg/domain 1/dhcp/subnet 2/green/.
/cfg/domain 1/dhcp/subnet 2/green/ranges/.
        add 10.24.26.49 10.24.26.61
/cfg/domain 1/dhcp/subnet 2/green/stdopts 3/.
        value 10.24.26.1
/cfg/domain 1/dhcp/subnet 2/green/stdopts 6/.
        value 10.10.30.5
/cfg/domain 1/dhcp/stdopts 3/.
        value 10.24.24.1
/cfg/domain 1/dhcp/stdopts 6/.
        value 10.10.60.35
/cfg/domain 1/dhcp/stdopts 15/.
        value abc.lab.com
/cfg/domain 1/dhcp/stdopts 51/.
        value 86400
/cfg/domain 1/sshkey/.
/cfg/domain 1/dnscapt/.
        ena true
```

```
/cfg/domain 1/dnscapt/exclude/.
      add windowsupdate
/cfg/domain 1/httpredir/.
      port 80
      redir on
/cfg/domain 1/adv/.
      interface 0
      log login
/cfg/sys/.
      mip 10.10.60.34
/cfg/sys/host 1/.
      ip 10.10.60.33
      gateway 10.10.60.1
/cfg/sys/host 1/routes/.
/cfg/sys/host 1/interface 1/.
      ip 10.10.60.33
      netmask 255.255.255.0
      gateway 0.0.0.0
      vlanid 0
      mode failover
      primary 0
/cfg/sys/host 1/interface 1/routes/.
/cfg/sys/host 1/interface 1/ports/.
      add 1
/cfg/sys/host 1/port 1/.
      autoneg on
      speed 0
      mode full
/cfg/sys/host 1/port 2/.
      autoneg on
      speed 0
      mode full
/cfg/sys/host 1/port 3/.
      autoneg on
      speed 0
      mode full
/cfg/sys/host 1/port 4/.
      autoneg on
      speed 0
      mode full
/cfg/sys/host 1/port 5/.
      autoneg on
      speed 0
      mode full
/cfg/sys/host 1/port 6/.
      autoneg on
      speed 0
      mode full
/cfg/sys/routes/.
/cfg/sys/time/.
      tzone "America/Toronto"
/cfg/sys/time/ntp/.
/cfg/sys/dns/.
      cachesize 1000
      retransmit 2s
      count 3
      ttl 3h
      health 10s
      hdown 2
      hup 2
      fallthrough off
/cfg/sys/dns/servers/.
      add 10.10.60.35
/cfg/sys/syslog/.
/cfg/sys/accesslist/.
/cfg/sys/adm/.
      sonmp off
      clitimeout 10m
```

```
        telnet on
        ssh off
/cfg/sys/adm/snmp/.
        ena true
        versions v1,v2c,v3
/cfg/sys/adm/snmp/snmpv2-mib/.
        snmpEnableAuthenTraps disabled
/cfg/sys/adm/snmp/community/.
        read public
        trap trap
/cfg/sys/adm/snmp/event/.
/cfg/sys/adm/audit/.
        vendorid "1872 (alteon)"
        vendortype 2
        ena false
/cfg/sys/adm/audit/servers/.
/cfg/sys/adm/auth/.
        timeout 10s
        fallback on
        ena false
/cfg/sys/adm/auth/servers/.
/cfg/sys/adm/srsadmin/.
        port 4443
        ena true
/cfg/sys/adm/sshkeys/.
/cfg/sys/adm/sshkeys/knownhosts/.
/cfg/sys/user/.
        expire 0
/cfg/lang/.
```

Software Baseline:

This document is in reference to software release 1.5 for NSNA, BOSS 3.6 for the ES470, BOSS 5.0 for the ERS5500, 4.1 for the ERS8600 and 5.0.9.4 for the WLAN 2300.

Contact us

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Nortel Networks service program, contact Nortel Technical Support. To obtain contact information online, go to www.nortel.com/contactus.

From the Technical Support page, you can open a Customer Service Request online or find the telephone number for the nearest Technical Solutions Center. If you are not connected to the Internet, call 1-800-4NORTEL (1-800-466-7835) to learn the telephone number for the nearest Technical Solutions Center.

An Express Routing Code (ERC) is available for many Nortel products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to www.nortel.com/erc.