Secure Router
VPN Router
Engineering

SR-VPN Router VPN Interoperability Solutions and Technical Configuration Guide

Enterprise Solutions Engineering
Document Date: November 2010
Document Number: NN48500-597
Document Version: 1.1

Notices
While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer
Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer
Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty
Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support
Please note that if you acquired the product from an authorized reseller, the warranty is provided to you by said reseller and not by Avaya.

Licenses
THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Copyright
Except where expressly stated otherwise, no use should be made of the Documentation(s) and Product(s) provided by Avaya. All content in this documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components
Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

Trademarks
The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party. Avaya is a registered trademark of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.

Downloading documents
For the most current versions of documentation, see the Avaya Support. Web site: http://www.avaya.com/support.

Contact Avaya Support
Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support

Abstract

This document is a VPN interoperability solution and technical configuration guide intended to provide LAB example and proof of VPN interoperability between Avaya Secure Routers and Avaya VPN Routers. The purpose of the document is to aid the Avaya sales team in positioning the Secure Routers in Avaya multi-product network and VPN deployments. The configurations in this example were successfully tested and may be used by the Avaya sales team to demonstrate VPN inter-operability solution for their customers and channel partners.

Table of Contents

1. Overview 5

2. Network Topology & VPN Requirement 6

2.1 Key Components Overview 7
2.1.1 Secure Router 7
2.1.2 VPN Router 8

3. Configuration 9

3.1 Configuring Secure Router 9
3.1.1 Interface IP Address and Route Configuration 9
3.1.2 Trusted/Untrusted Interface Configuration 10
3.1.3 IKE Policy Configuration 11
3.1.4 IPsec Policy Configuration 12
3.1.5 Firewall Internet Configuration to Accept IKE Service 13
3.1.6 Firewall Corp Configuration to Allow Transit Traffic 14
3.1.7 Firewall Internet Configuration to Allow Remote Management of SR Passing Through BOT 14
3.1.8 Show Running-Configuration 15
3.2 Configuring VPN Router (aka Contivity) 16
3.2.1 Interface Configuration 16
3.2.2 Branch Office Group Configuration 16
3.2.3 Branch Office Connection Configuration 19
3.3 Verification/Testing the BOT Connection 20
3.3.1 Workstation Configuration 21
3.3.2 Send Traffic to Trigger BOT Connection 21
3.3.3 Event Log Message 22
3.3.4 Verify BOT Session 22

4. Extra Sample Configurations 23

4.1 Configuring Secure Router via HTTP GUI 23
4.1.1 Interface Configuration 23
4.1.2 IKE Policy Configuration 23
4.1.3 IPSec Policy Configuration 24
4.1.4 Firewall Internet Configuration 24
4.1.5 Firewall Corp Configuration 25
4.2 Configuring VPN Router via CLI 26
4.2.1 BO Group Configuration 26
4.2.2 BO Connection Configuration 26
4.3 Configuring Secure Router with Two or More Transform Proposals 27
4.3.1 Multiple IKE Proposals 27
4.3.2 Multiple IPsec Proposals 28
4.4 Configuring Secure Router with Multiple Local/Remote Accessible Networks 30
4.4.1 Add a Second IPSec Policy & Associate the Proper Match Address 30
4.4.2 Allow Inbound Transit Traffic for the Configured Match Address 31
4.4.3 Test & Verify BOT Session for the Two IPSec Policies 31

5. Customer service 32

5.1 Getting technical documentation 32
5.2 Getting product training 32
5.3 Getting help from a distributor or reseller 32
5.4 Getting technical support from the Avaya Web site 32

Appendix: Abbreviations/Glossary 33

1. Overview

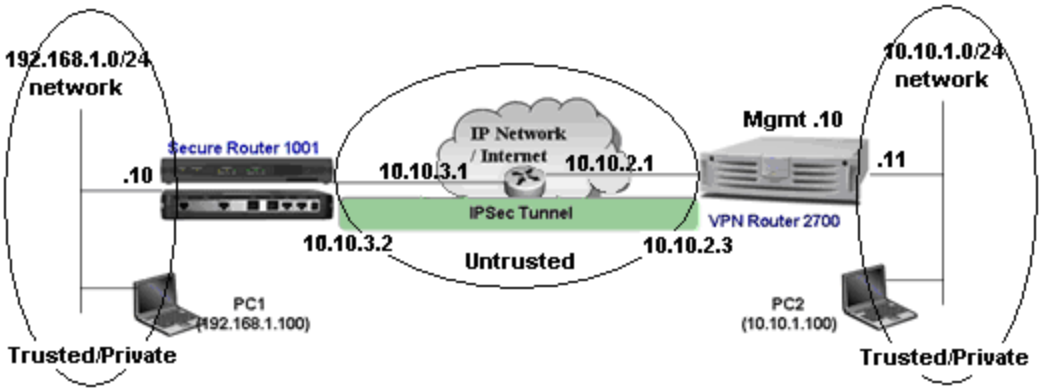
More and more enterprises use VPN to establish end-to-end private network connections over the Internet to reduce communication expenses while maintaining privacy, and allowing their branches and mobile workers to take advantage of high speed connectivity while keeping up productivity.

There are two basic flavors of VPNs, each with an associated set of business requirements: Site to Site VPN and Remote Access VPN. *Site-to-Site VPN* basically connects two remote offices or a branch office to headquarters wherein each site is connected to the internet through a security gateway. The objective of the site to site VPN is to create a secure tunnel between the two security gateways through the public network which is the Internet. All the network traffic from the site to internet traverses the local security gateway. The security gateway monitors the network traffic and chooses to secure the packets headed to the other site based on the policy defined. *Remote Access VPN* facilitates individual users such as telecommuters connect to a corporate network. The user's laptop usually has a VPN client and policy is defined such that the traffic destined to the corporate network needs protection. When the VPN client detects an access to the corporate network, a secure tunnel to the security gateway (a.k.a. VPN server) at the corporate headquarters is created. This document focuses on Site-to-Site VPN or commonly known as Branch Office Tunnel VPN connection.

Many Avaya customers have implemented Avaya VPN Router for their VPN & FW needs and Avaya Secure Router to accommodate their requirement of security & high performance edge router. For sure, many of those customers are requiring or will soon require the use of both Secure Router and VPN Router for their Site-to-Site VPN needs to reduce communication expenses by taking advantage of the Internet connection while maintaining security and privacy.

This document will discuss Site-to-Site VPN Inter-operability between Avaya Secure Router and Avaya VPN Router in order to aid Avaya sales force in positioning the Secure Routers in Avaya multi-product network and VPN deployments. As such, this document can be used as a reference or guide for demo purposes that will show the VPN inter-operability of Secure Routers and VPN Routers.

2. Network Topology & VPN Requirement



The network setup mainly consists of three routers: Secure Router, VPN Router, and any type of router in between which simulates the Internet. The router that simulates the Internet does not have any route to reach the private/local LAN side of the two routers. The only route it knows is to reach the public interfaces (facing the internet/untrusted network) of the Secure Router and VPN Router. Thus, the only way for the network devices on the private/local LAN of Secure Router to reach the network devices on the private/local LAN of the VPN Router (and vice-versa) is to form a Branch Office Tunnel. Take note that the inter-connection between the routers uses the Ethernet ports to simplify the setup and configuration (using any supported WAN interface and WAN protocols should work as well). The diagram shows the IP address of the network devices used in the network setup as well as the private/local LAN network on both the Secure Router and VPN Router so please refer to the diagram in every step of the configuration.

The specific hardware and software used in this network setup are Secure Router 1001 running v8.3.5 and VPN Router 2700 running v6.0.

Also, in this network setup, we will use the following as the requirement for the VPN (Virtual Private Network) configuration:

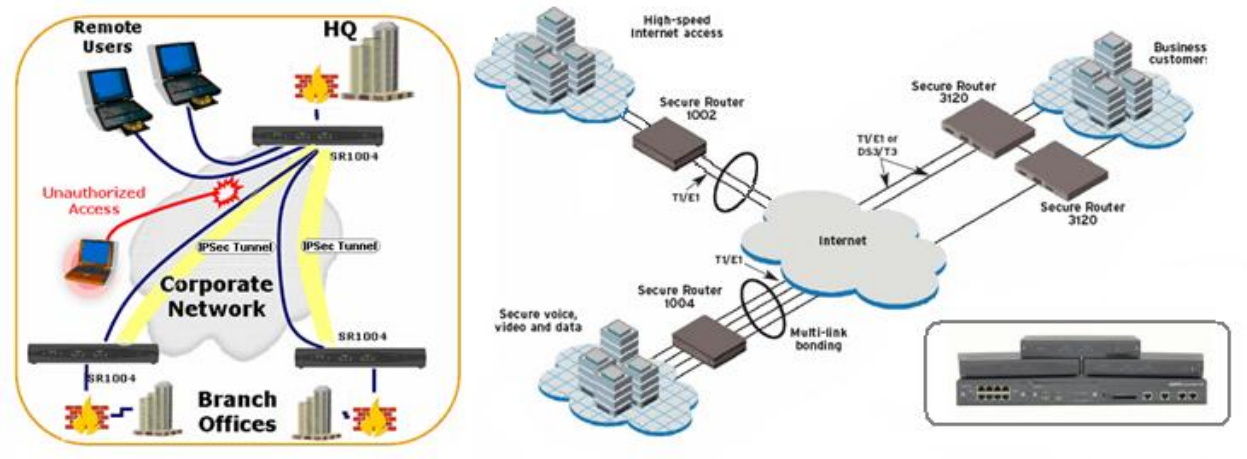
- IKE Encryption, Hash algorithm, and DH group: 3DES-SHA1 with DH group 2
- IKE exchange type: Peer-to-Peer or Both (can be initiator or responder)
- IKE mode: Main mode
- IPSec Encryption and Hash algorithm: 3DES-SHA1
- IPSec protocol: ESP
- IPSec encapsulation: Tunnel mode
- Authentication method: Pre-Shared Key

2.1 Key Components Overview

2.1.1 Secure Router

Avaya Secure Router Portfolio enables secure end-to-end converged solutions. The Secure Routers combine robust IP routing, flexible WAN connectivity and security in a single cost-effective device. Ideal for enterprise branch, remote or regional site environments, Avaya Secure Routers are optimized to deliver the low-latency, high packet throughput required by IP telephony and multimedia applications. Providing wire-speed performance even with advanced WAN services enabled, they are the right solution for enterprises requiring high-speed Internet or private WAN connectivity.

Avaya Secure Routers also include an extensive suite of advanced security features, including Virtual Private Networking (VPN), Stateful packet inspection Firewall, Encryption, etc. This built-in security protects against unauthorized access and network disruption, while ensuring the privacy and integrity of transmitted data.

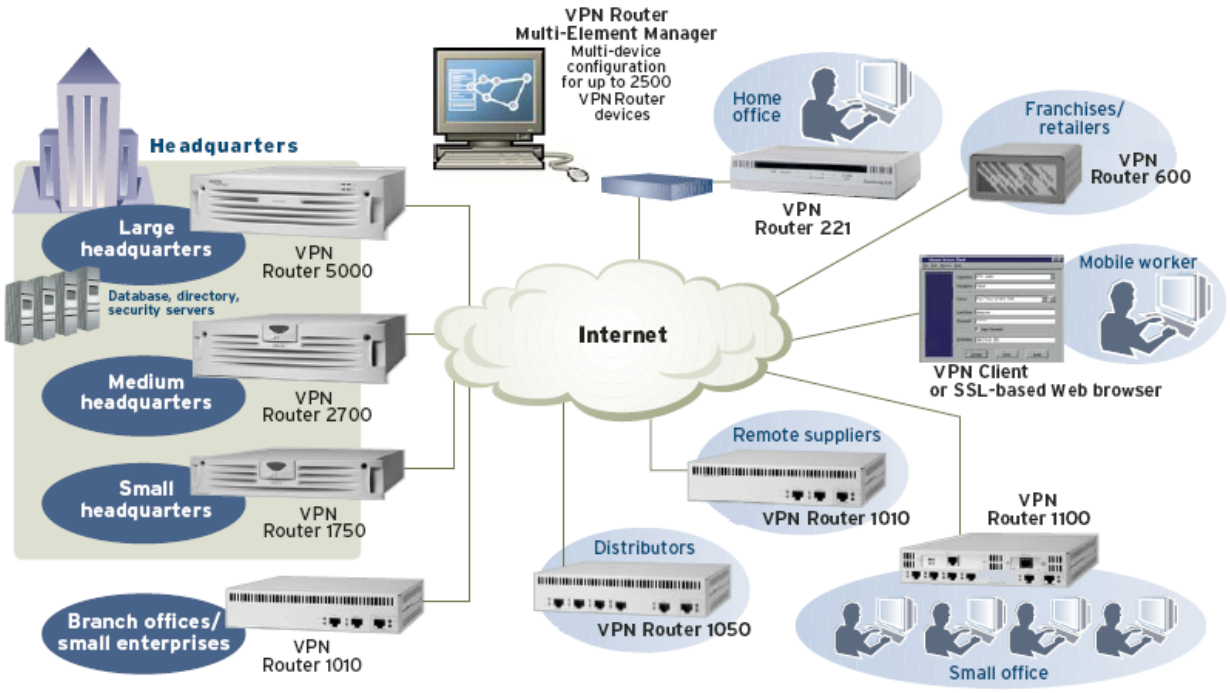


As of today, the Avaya Secure Router platform consists of SR 100x series and SR 3120. The SR 100x series are ideal for installation in small to medium enterprise remote sites and branch offices while the SR 3120 platform is ideal for medium to large branch and regional enterprise environments.

More information on the Avaya Secure Router portfolio can be located at: https://support.avaya.com/css/Products. Choose your version of Secure Router from the products list.

2.1.2 VPN Router

Avaya VPN Routers provide Routing, IPSec and SSL VPN, Firewall, Encryption, etc. for secure connectivity across managed IP networks and the Internet. Avaya VPN Routers connect remote users, branch offices, suppliers, and customers with the cost and performance advantages of public IP networks and the security and control found in private networks. Avaya VPN Router family of products has many features but mainly it provides comprehensive VPN services. Its primary purpose is to provide Secure Routing and VPN connection.



The Avaya VPN Routers also provide a secure connection infrastructure for converged networks – supporting voice, video, and data. As such, Avaya VPN Routers can be combined with Avaya voice solutions to extend multimedia capability to teleworkers, mobile users, and small/medium/large branch offices. Avaya VPN Routers can be deployed to meet a variety of different solution requirements.

More information on the Avaya VPN Router portfolio can be located at:

https://support.avaya.com/css/Products. Choose your version of VPN Router from the products list.

3. Configuration

3.1 Configuring Secure Router

There are two methods to configure Secure Router (SR) for VPN functionality: CLI and GUI. The most common method used by most engineers when configuring SR is through CLI configuration. As such, this document will show how to configure the SR system using CLI commands. The configuration through HTTP GUI will be discussed under Section 4.1.

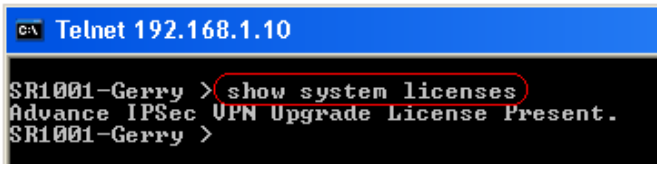
To configure VPN on the Secure Router through CLI, please follow the following steps/procedures:

3.1.1 Interface IP Address and Route Configuration

Assign IP address to the interfaces that will be used for connecting to the trusted/private/LAN side as well as on the untrusted/public/Internet side. Initially, you will need to access the Secure Router through console connection and assign an IP address. Then succeeding configuration can be performed either through console or Telnet session. In our setup, we will use Ethernet 0 as the private interface and Ethernet 1 as the public interface. Follow the CLI commands shown in the figure below. In addition to assigning IP address, we also need to add a route in order to reach the remote peer device. In our example, we will use a default route of 0.0.0.0/0 with a gateway address of 10.10.3.1 which is the IP address of the next-hop router.

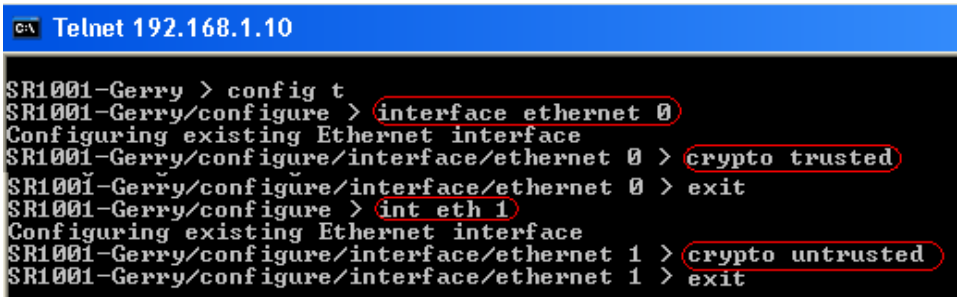
```
SR1001-Gerry > configure term
SR1001-Gerry/configure > interface ethernet 0
Configuring existing Ethernet interface
SR1001-Gerry/configure/interface/ethernet 0 > ip address 192.168.1.10 24
SR1001-Gerry/configure/interface/ethernet 0 > exit
SR1001-Gerry/configure > interface ethernet 1
Configuring existing Ethernet interface
SR1001-Gerry/configure/interface/ethernet 1 > ip address 10.10.3.2 24
SR1001-Gerry/configure/interface/ethernet 1 > exit
SR1001-Gerry/configure > ip route 0.0.0.0 0 10.10.3.1
```

NOTE: Before proceeding to the next steps, ensure that VPN license is installed in the Secure Router. To verify if VPN license is present, issue a CLI command ‘show system licenses’. If there’s no VPN license yet, purchase a VPN upgrade license and install it in the Secure Router system.

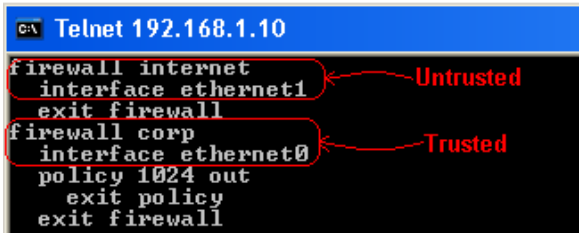


3.1.2 Trusted/Untrusted Interface Configuration

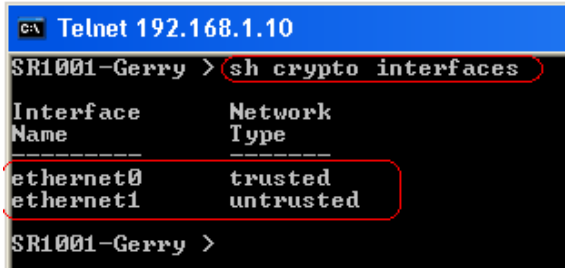
Assign Ethernet 0 as part of the trusted network (this will be the private/LAN side of SR). Then assign Ethernet 1 as part of the untrusted network (this will be the public/internet side of SR).



Take note that the VPN functionality of SR requires Firewall. After assigning an interface to a *Trusted* network, the particular interface will be automatically added/associated with Firewall *Corp* as shown in the figure below (note: the figure below is a screenshot capture after executing 'show running-config' from the CLI). Likewise, the interface associated to an *Untrusted* network will be automatically added/associated with Firewall *Internet*. Both Firewall Corp and Internet are default firewall policies in Secure Router. Firewall configuration will be further discussed later in this document.



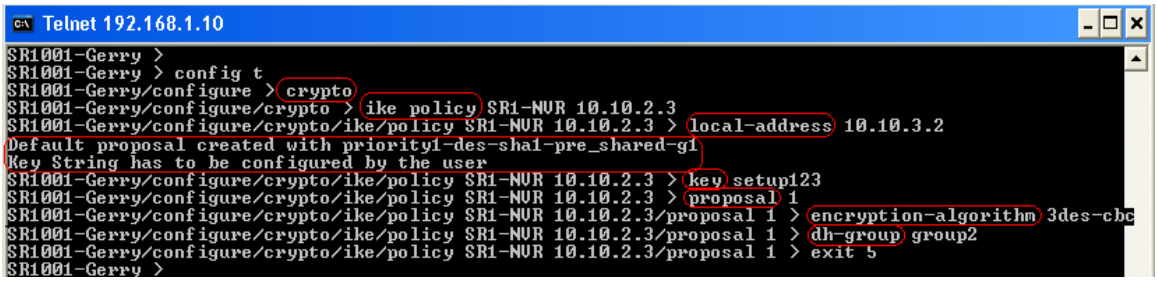
To see the list of trusted and untrusted interfaces, use the CLI command 'show crypto interfaces'.



3.1.3 IKE Policy Configuration

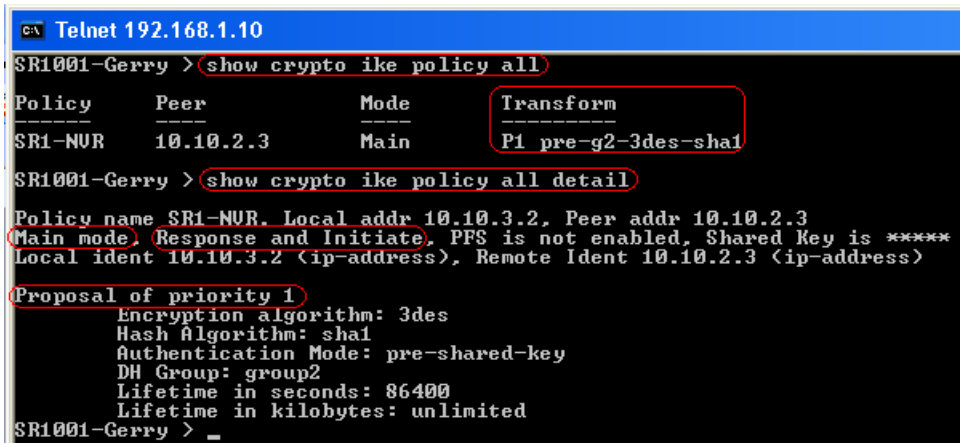
The next step is to configure an IKE Policy. To do this, type 'configure term' to enter configuration mode. Then type 'crypto' command to access crypto configuration commands. Create an IKE policy by entering 'ike policy <policy name> <peer address>' wherein the policy name can be any name and the peer address must be the IP address of the remote peer device. In our example, this will be the IP address (10.10.2.3) of the Avaya VPN Router public interface. Then define the local address of the SR (in our example, this will be the IP address of SR's untrusted interface facing the internet side). Configuring the correct local and peer address is important as both local and peer address will be used for IKE negotiation.

Take note that under IKE policy configuration, the IKE exchange-type and IKE mode should be configured as well. SR's default IKE exchange-type is 'both' (a.k.a. peer-to-peer) which means that it can be either initiator or responder. The requirement is peer-to-peer so it is not necessary to explicitly configure the IKE exchange-type. The default IKE mode is main mode and we want to use main mode so we don't have to explicitly configure it as well.



By default, SR will automatically create a transform proposal for the IKE policy that is being configured. As shown from the above figure, a default proposal of *priority1-des-sha1-preshared-g1* was created. Since the requirement is to use 3DES encryption and Diffie Hellman group 2, we need to manually define that the transform proposal must use 3DES encryption and DH group2. To do this, edit proposal 1 and type 'encryption-algorithm 3des-cbc' to change the encryption from DES to 3DES. To change DH group from group1 to group2, enter 'dh-group group2'. Another requirement is to use pre-shared key authentication method so we need to define the secret key. To define the secret key, type 'key <secret key>' as shown in the above screenshot. The secret key used in our example is 'setup123'. This secret key must match with the peer device's secret key.

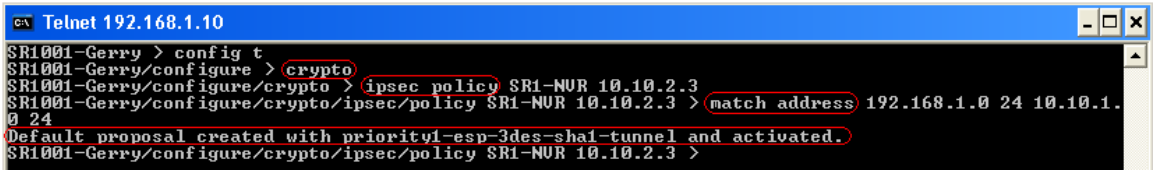
To see the configured IKE policy, enter 'show crypto ike policy all' (note: add detail at the end if you want to see more info). As shown from the figure below, the transform proposal is pre-g2-3des-sha1 which means Pre-shared key authentication, DH group2, 3DES encryption, and SHA1 hash algorithm. Displaying the IKE policy will also show the IKE mode which is main mode in this case. The 'Response and Initiate' shown in the figure below basically mean that the IKE exchange-type is both or peer-to-peer.



3.1.4 IPsec Policy Configuration

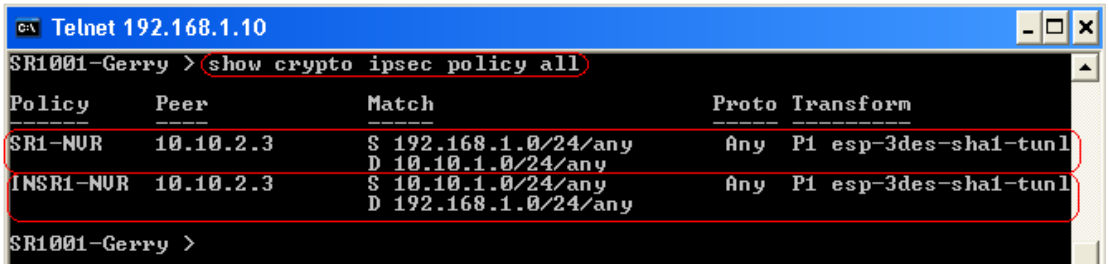
After configuring IKE policy, the next step is to define an IPSec policy. To do this, enter configuration mode and execute the CLI command 'crypto' to access the crypto configuration commands. Enter 'ipsec policy <policy name> <peer address>' wherein the policy name can be any name (note: the same policy name used in IKE policy was also used in our IPSec policy for consistency) and the peer address is the public IP address of VPN Router.

Then next is to define the match source and destination network address in which IPSec will be applied to (note: this is similar to the VPN Router's local and remote accessible networks). To do this, enter 'match address <source/local address/network> <subnet mask/prefix> <destination/remote address/network> <subnet mask/prefix>'. In our example, the source/local network and subnet prefix is 192.168.1.0/24 while the destination/remote network and subnet prefix is 10.10.1.0/24. Take note that aside from matching the source/local and destination/remote network, a protocol (udp/tcp/icmp/any) and/or port can also be added to the match address rule. In our example, we want to allow *any* protocol and *any* port as long as the source/local and destination/remote addresses are match. The default is any protocol and any port so it is not necessary to explicitly define the protocol and ports when configuring match address for the IPSec policy.



As shown in the above figure, SR automatically created a default IPSec proposal with *priority1-esp-3des-sha1-tunnel* transform. Since the requirement is to use ESP protocol, 3DES encryption, SHA1 hash algorithm, and Tunnel mode IPSec encapsulation, it is not necessary to explicitly configure the IPSec proposal.

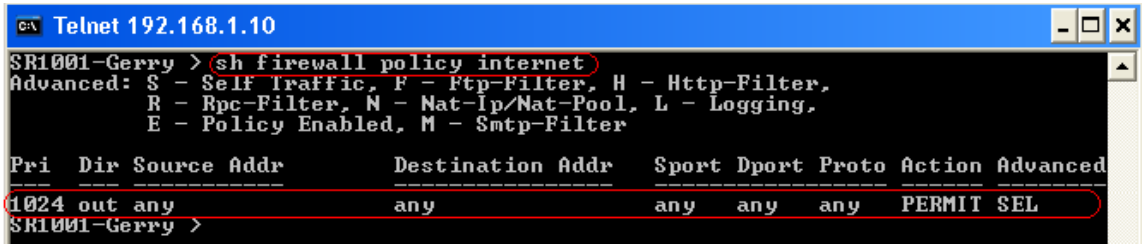
To see the configured IPSec policy, execute the command 'show crypto ipsec policy all'. It will display all IPSec policies configured in the SR system. As you can see from the figure below, there are two IPSec policies even though we only configured one. The IPSec policy that we just configured is for outbound direction. SR automatically created the IPSec policy for inbound direction wherein it simply prepends the word 'IN' to the original policy name and reverse the source/local and destination/remote networks. The rest of the settings are just copied from the original IPSec policy.



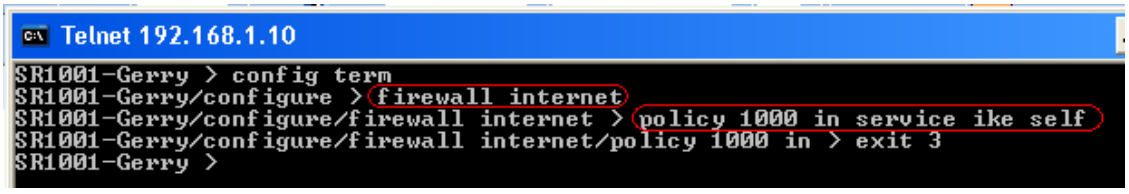
Note: At this stage, Branch Office Tunnel can be established as long as traffic is initiated from the SR side (assuming VPN Router has been configured already). If you want traffic to be initiated from the VPN Router side, then the SR must be manually configured to accept IKE negotiations which will be discussed on the next step.

3.1.5 Firewall Internet Configuration to Accept IKE Service

As discussed in Section 3.1.2, the untrusted interface (facing the internet) is bind to Firewall policy Internet. By default, the only rule in Firewall policy Internet, as shown below, is to allow any outbound traffic coming from the SR system itself.

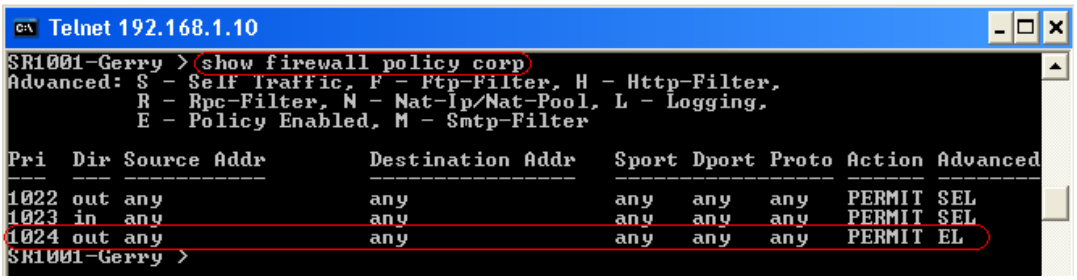


As such, in order to allow IKE negotiations, it is required to manually allow inbound IKE port/service. To do this, edit Firewall *Internet* and enter 'policy <priority/rule number> in service ike self' where "in" means incoming direction, "service ike" is obviously the IKE service and "self" is traffic directed to the SR system itself. Permit is the default action so it is not necessary to explicitly add it in the command. Alternatively, you can enter 'policy <priority/rule number> in *permit* service ike self'.

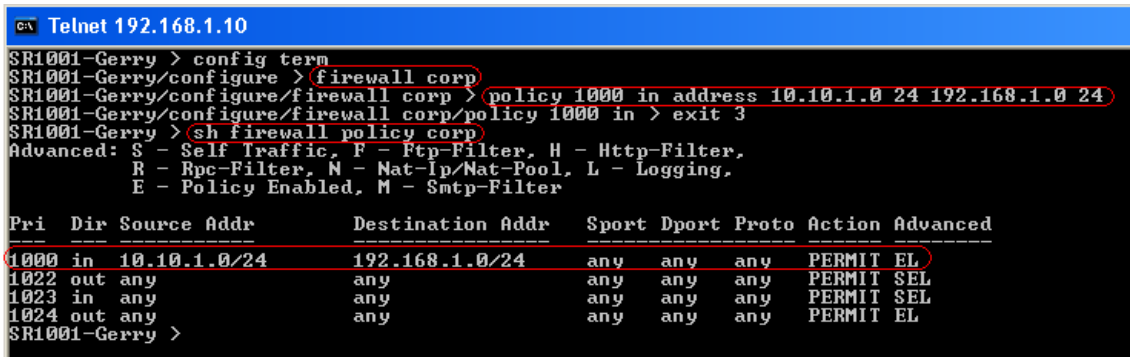


3.1.6 Firewall Corp Configuration to Allow Transit Traffic

Assuming that VPN Router has been properly configured already and the BOT has been established after traffic is initiated either from the SR or VPN Router side, the network devices from the trusted/private side of SR will be able to reach the devices on the private side of VPN Router. However, the network devices from the private side of VPN Router will not be able to reach the devices on the trusted/private side of SR. The reason is that SR has a default policy under Firewall policy *Corp*, as shown below, that allows any *outbound transit* traffic but no inbound *transit* traffic.

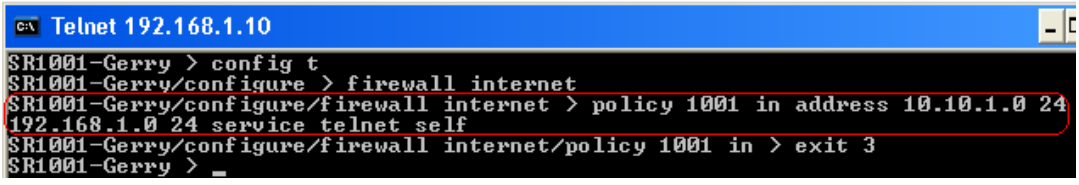


As such, the SR must be manually configured to allow *inbound* transit traffic from a particular source network (this will be 10.10.1.0/24 in our example) to a particular destination network (this will be 192.168.1.0/24 in our example). To do this, edit Firewall policy *Corp* and then type 'policy <priority/rule number> in address 10.10.1.0 24 192.168.1.0 24'. To see the added policy for Firewall policy Corp, use the CLI command 'show firewall policy corp'.



3.1.7 Firewall Internet Configuration to Allow Remote Management of SR Passing Through BOT

If there's a requirement to remotely manage SR passing through the BOT, this last step is necessary. If such requirement is not needed then proceed to the next step. To allow remote management of SR (using telnet, for example) passing through the BOT, edit Firewall policy Internet and type 'policy <priority/rule number> in address 10.10.1.0 24 192.168.1.0 24 service telnet self' which basically means you are just allowing inbound *self* traffic that is destined to SR from a remote network address 10.10.1.0/24 and only when the service is telnet.



3.1.8 Show Running-Configuration

SR's BOT and FW configuration is now complete! Enter 'show running-config' to see the active configuration.

```
module  t1 1
   exit t1
interface  ethernet 0
   ip  address 192.168.1.10 255.255.255.0
   crypto trusted
   exit ethernet
interface  ethernet 1
   ip  address 10.10.3.2 255.255.255.0
   crypto untrusted
   exit ethernet
hostname SR1001-Gerry
log utc
ftp_server
ssh_server
  exit ssh_server
system  logging
   console debugging
   syslog
     host_ipaddr 192.168.1.101
     enable
     vpn debug
     exit syslog
   exit logging
ip
  load_balance per_flow
  route 0.0.0.0 0.0.0.0 10.10.3.1 1
  dhcps
    exit dhcps
  exit ip
crypto
  ike  policy SR1-NVR 10.10.2.3
     local-address 10.10.3.2
     key setup123
     proposal 1
       dh-group group2
       encryption-algorithm 3des-cbc
       exit proposal
     exit policy
  ipsec  policy SR1-NVR 10.10.2.3
     match  address 192.168.1.0 255.255.255.0 10.10.1.0
255.255.255.0
     proposal 1 esp
       exit proposal
     exit policy
  exit crypto
firewall global
  exit firewall
firewall internet
  interface ethernet1
  policy 1000 in service ike self
    exit policy
  policy 1001 in address 10.10.1.0 24 192.168.1.0 24
          service telnet self
    exit policy
  exit firewall
firewall corp
  interface ethernet0
  policy 1000 in address 10.10.1.0 24 192.168.1.0 24
    exit policy
  policy 1024 out
    exit policy
  exit firewall
snmp-server
  chassis-id SR1001-Gerry
  exit snmp-server
```

3.2 Configuring VPN Router (aka Contivity)

There are two methods to configure Avaya VPN Router for VPN functionality: CLI and GUI. The most common method used by most engineers when configuring VPN Router is through HTTP GUI. As such, this document will show how to configure the VPN Router system using HTTP GUI. The configuration through CLI commands will be discussed under Section 4.2.

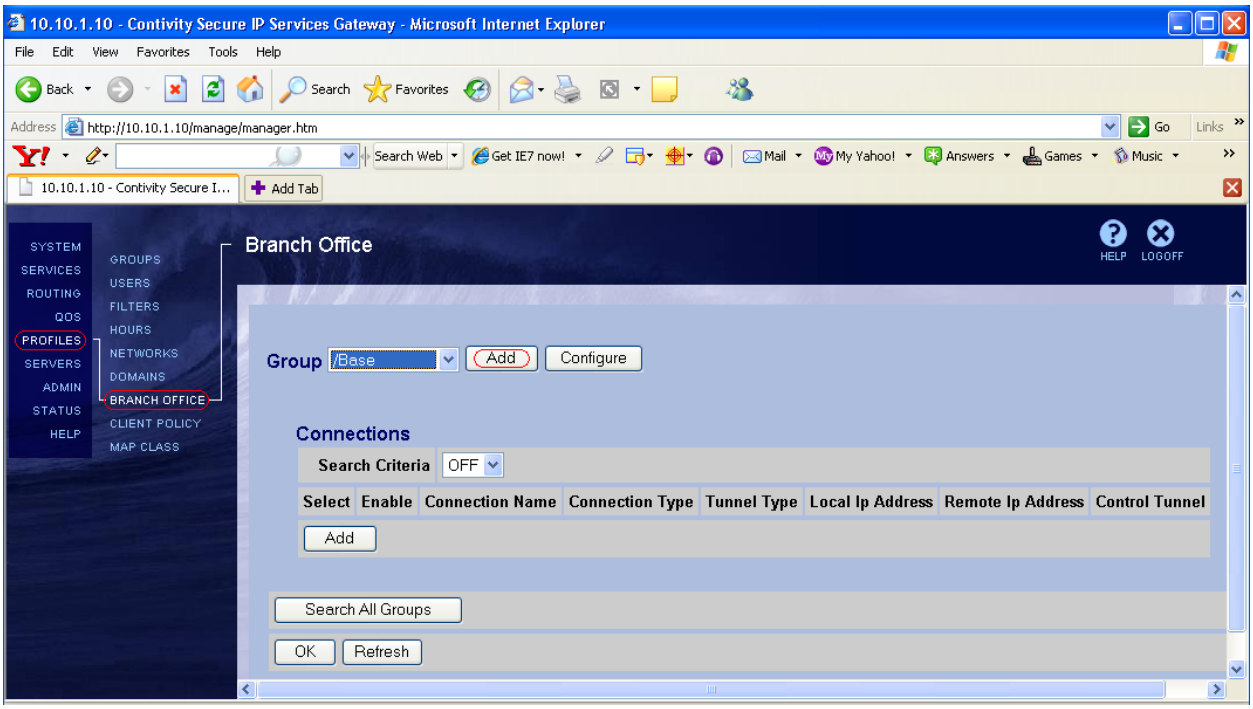
To configure VPN on the VPN Router through HTTP GUI, please follow the following steps/procedures:

3.2.1 Interface Configuration

Assign an IP address to the private and public interfaces through console connection. A management IP address must be assigned as well. Once proper IP address has been assigned to the VPN Router system, open an internet browser and enter the management address of VPN Router. In our example, the management address of VPN Router is 10.10.1.10 so we enter 'http://10.10.1.10' from the Internet browser.

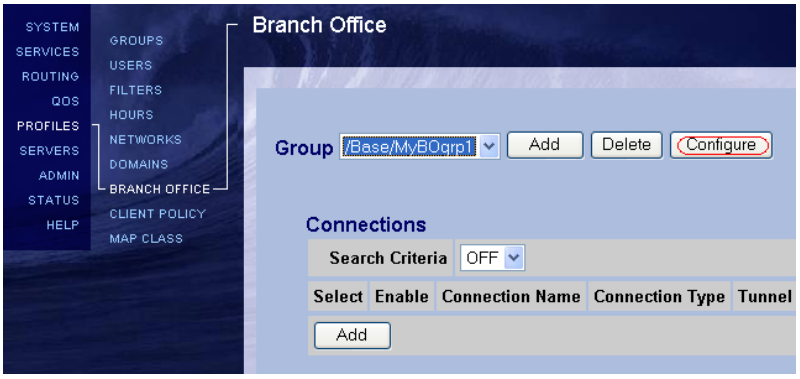
3.2.2 Branch Office Group Configuration

Go to Profiles > Branch Office, then click Add button to add a branch office group under /Base group.

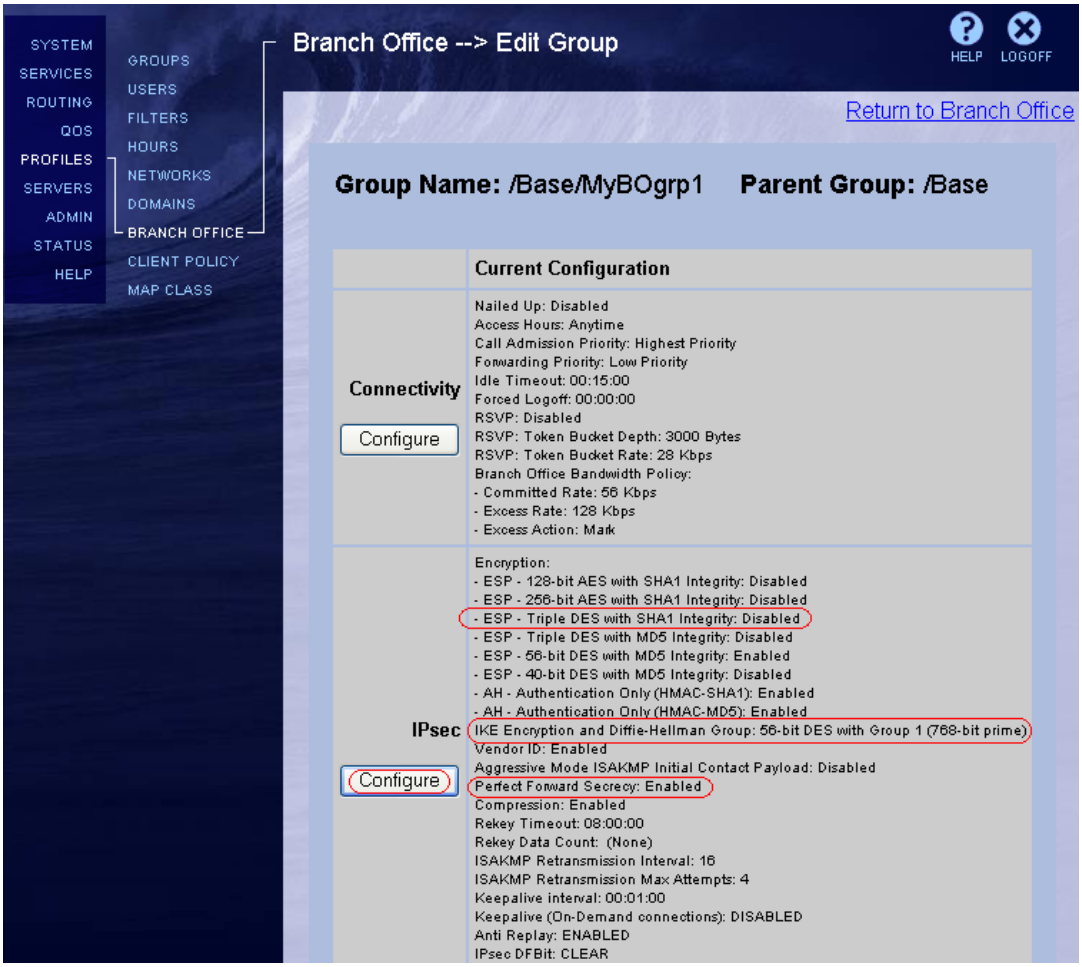


Under Add Group page, enter your preferred group name (i.e. MyBOgrp1) and hit OK.

After adding the BO group, click on Configure button to double check or modify the BO group's settings.



The selected BO group's current configuration page will appear. As shown in the figure below, the VPN Router's IKE and IPSec settings do not completely match with the Secure Router so we have to modify the VPN Router's configuration to match the SR. To do this, click on the IPSec Configure button.

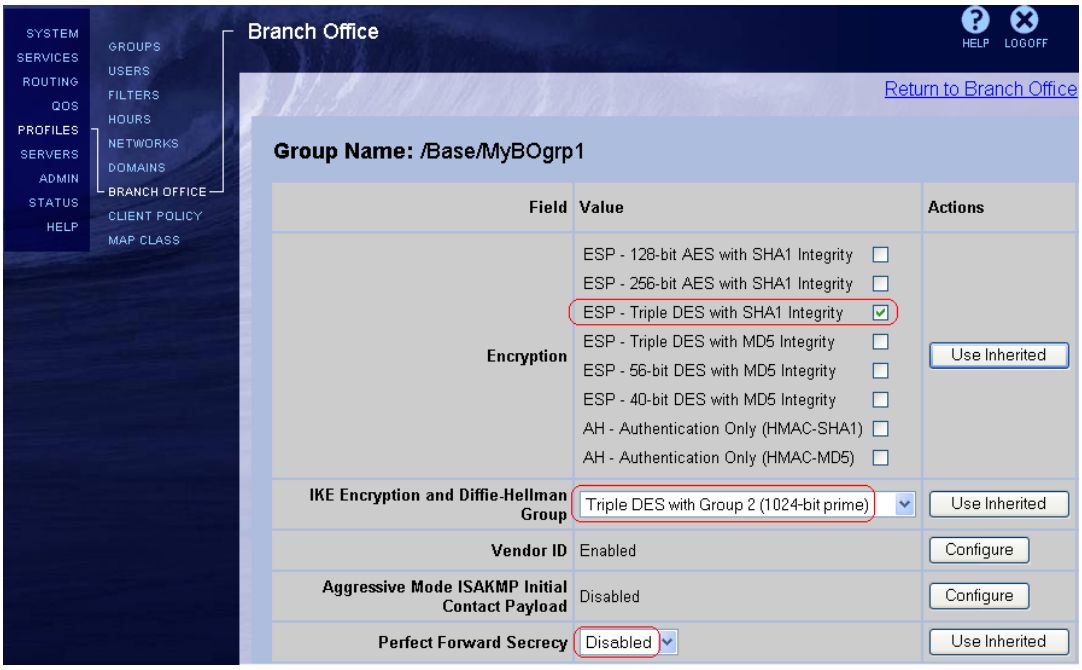


The Secure Router is configured for one IPSec transform proposal which is ESP – 3DES – SHA1 so we must configure the same proposal on the VPN Router to have a match in order to successfully establish the VPN connection. Under encryption field, enable ESP – Triple DES with SHA1 Integrity.

The Secure Router is also configured for one IKE transform proposal which is PSK auth – DH Group2 – 3DES – SHA1 so we also have to change the default IKE encryption and Diffie-Hellman group setting on the VPN Router to Triple DES with Group2 (1024-bit) to match with the Secure Router. Take note that the PSK (pre-shared key) authentication method will be configured on another page which will be discussed on Section 3.2.3.

PFS or Perfect Forward Secrecy is disabled on the Secure Router so PFS must be disabled on the VPN Router as well.

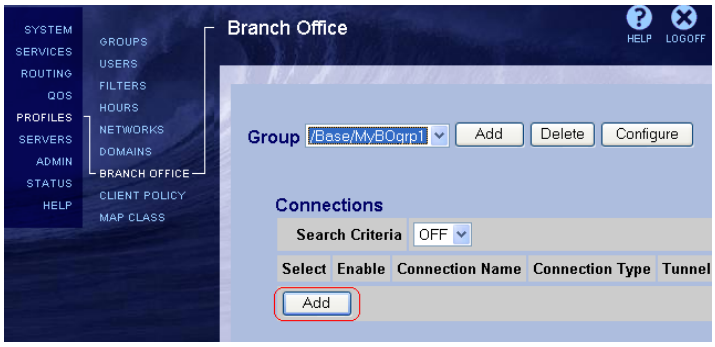
Click on the OK button.



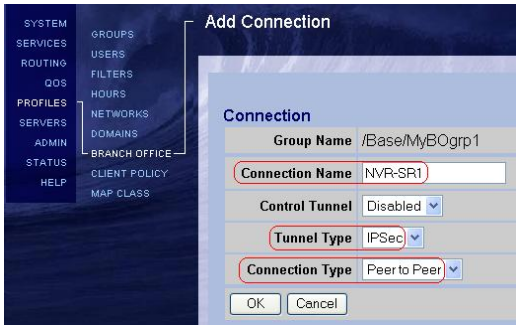
Note: If the desired IPSec transform proposal (shown on the right side of the encryption field) and/or the IKE encryption & DH group is/are not listed in the available options, go to Services > IPSec page and enable/check the desired IPSec transform (shown under encryption portion) as well as the desired IKE encryption and DH group.

3.2.3 Branch Office Connection Configuration

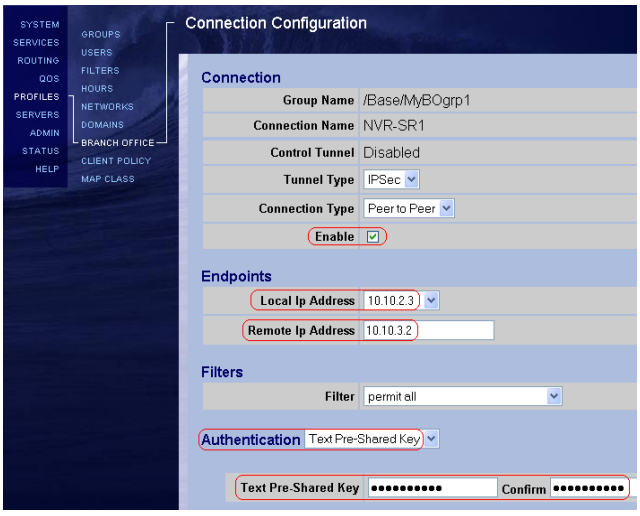
Go back to Profiles > Branch Office page and select the group that you just created. Under Connections, click on Add button to add a BO connection.



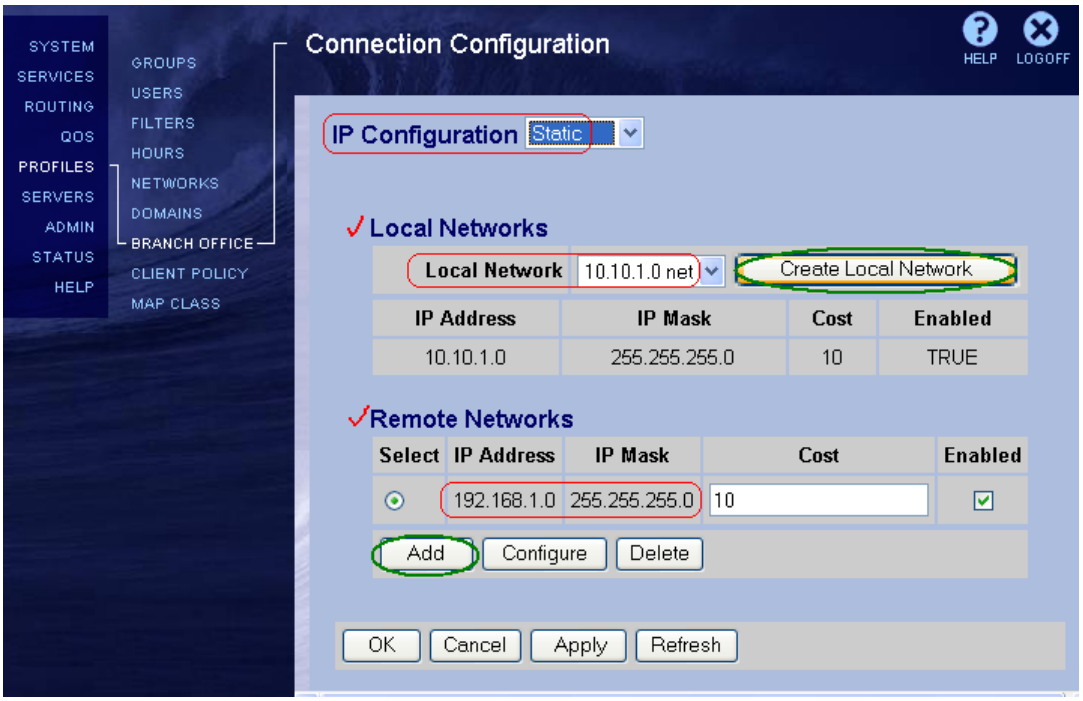
Under Add Connection page, enter your preferred BO connection name. Ensure that tunnel type is IPSec and connection type is Peer-to-Peer. Click on the OK button.



Under BO connection configuration page, check/select Enable to enable the connection. Then select the Local IP address (this would be 10.10.2.3 in our example) as the local endpoint and enter the Remote IP address (this will be the IP address of the Secure Router which is 10.10.3.2 in our example) as the remote end point or the peer address. Under authentication, select Text Pre-Shared Key and enter the secret key. The secret key must match with the secret key configured on the Secure Router.



Under IP Configuration, select Static. Then manually enter the local and remote networks. Click on the Create Local Network button to create a local network(s) and click on the Add button to create a remote network(s). In our example, the network on the private side of VPN Router is 10.10.1.0/24 and this is the network that we want to be accessible from the remote (SR) side of the BO connection so 10.10.1.0/24 should be entered under the Local Networks portion. Likewise, 192.168.1.0/24 is the network on the trusted/private side of SR and we want it to be accessible from the VPN Router side of the BO connection so 192.168.1.0/24 should be entered under Remote Networks.



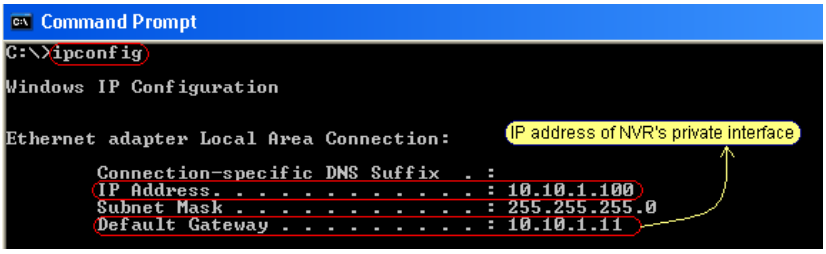
Leave the other settings on its default configuration and click on the OK button. VPN Router's BOT configuration is now complete!

3.3 Verification/Testing the BOT Connection

Since the VPN configuration uses peer-to-peer connection/exchange type, testing of BOT connection is simply done by sending traffic from the SR side or VPN Router side. A simple ICMP request (ping) will trigger the establishment of the BOT connection. This section will show a simple step by step procedure on how to test and verify if the BOT connection has been successfully established between the Secure Router and VPN Router.

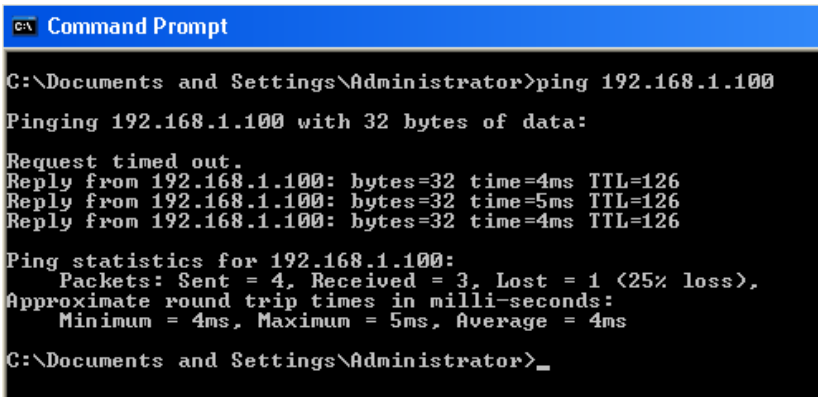
3.3.1 Workstation Configuration

Ensure that the workstations are properly configured. If using a MS-Windows operating system, launch a command prompt and type 'ipconfig'. Its IP address must be part of the subnet where it is connected to and its default route must be pointing to its gateway. This will be the SR in the case of PC1 and VPN Router in the case of PC2, as shown in the figure below.



3.3.2 Send Traffic to Trigger BOT Connection

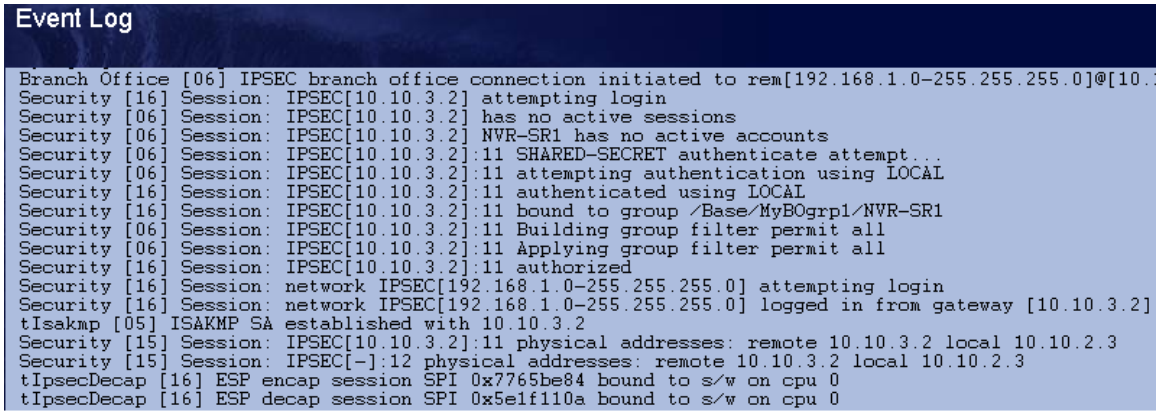
Send a ping request from a workstation (PC2) on the VPN Router side to another workstation (PC1) on the SR side. Take note that since the connection type or IKE exchange type is peer-to-peer, you can also initiate sending traffic from the SR side going to VPN Router side. Sending traffic from the local side to the remote side of the BO connection will trigger the BO tunnel establishment. As soon as the tunnel is established, PC1 should receive the ping request and sends it reply back to PC2. The ping reply will pass through the BOT and will be received by PC2. This means that BOT has been successfully established and bidirectional traffic can flow from/to either side of the BO connection.



Note: Another option to bring the tunnel up is to send an ICMP ping packet from either the VPN Router or SR itself. If sending ping packet from the SR itself, ensure that the ping command includes a source IP address that is part of the match address on the SR such as the SR's eth0 IP address (192.168.1.10). Otherwise, the tunnel will not be brought up since the source address will be the SR's eth1 IP address (10.10.3.2) which is not part of the match address configured in the IPSec policy discussed in Section 3.1.4.

3.3.3 Event Log Message

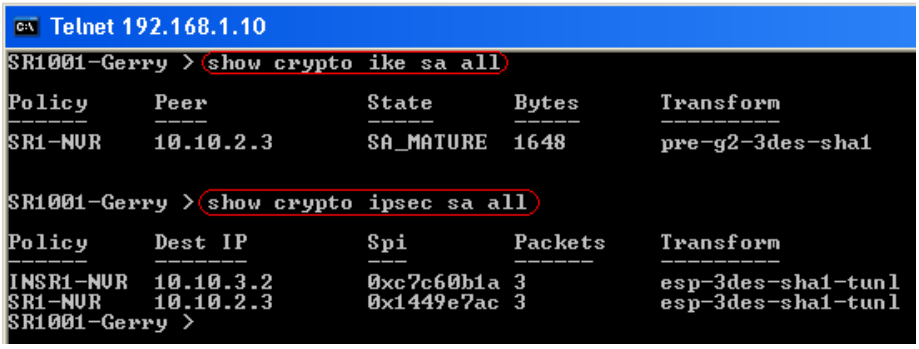
From the VPN Router side, you should see the following event log messages.



3.3.4 Verify BOT Session

To see the active BOT session(s) on VPN Router, go to Status > Sessions page.

To see the active tunnel session(s) on SR, use the CLI commands 'show crypto *ike* sa all' to see the IKE SAs and 'show crypto *ipsec* sa all' to see the IPSec SAs.



4. Extra Sample Configurations

4.1 Configuring Secure Router via HTTP GUI

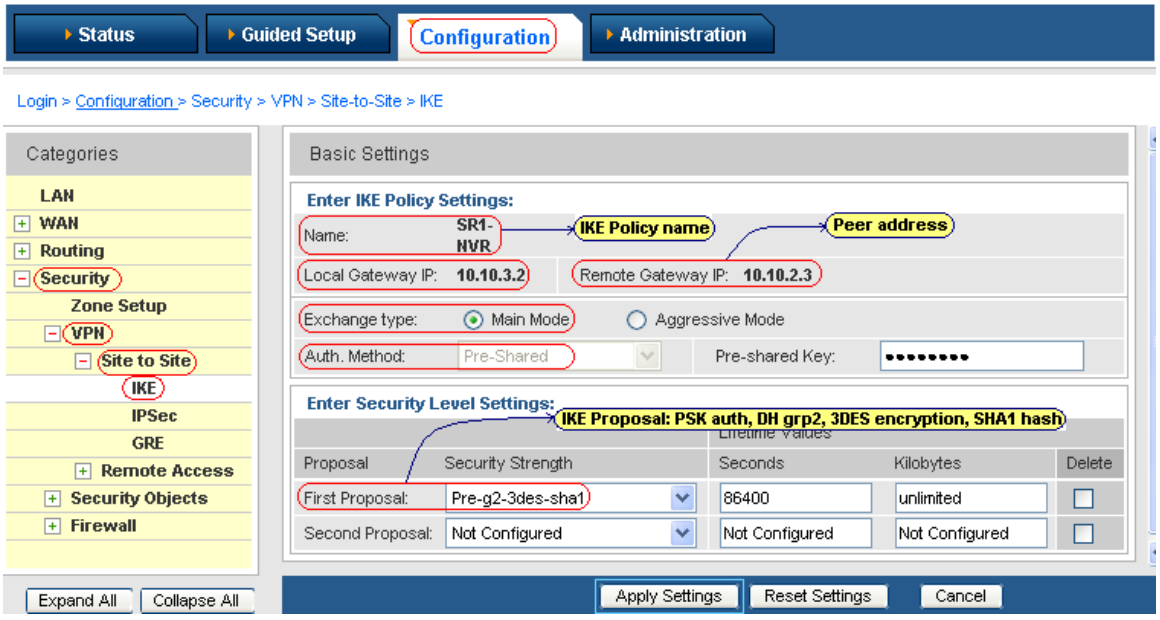
HTTP GUI (Graphical User Interface) is another method of configuring the Secure Router. One main intention of the HTTP GUI is to aid in configuring complex features such as VPN and FW. Using a GUI reduces the time and effort in configuring the SR system as the user doesn't need to remember the numerous CLI (Command Line Interface) commands and the tree structure of the CLI. Take note, however, that not all CLI commands are also available in HTTP GUI as of today.

4.1.1 Interface Configuration

First, you need to assign IP address on the interface and this can be done through console. Once an IP address is assigned to the interface, open up an internet browser and enter 'http://<SR ip address>'. Input the user name and password to enter the SR's HTTP GUI main menu. In addition to assigning an IP address, the interface facing the internet must be assigned as untrusted interface while the interface facing the local LAN must be assigned as trusted interface. Assigning interfaces as trusted or untrusted can be performed via CLI command.

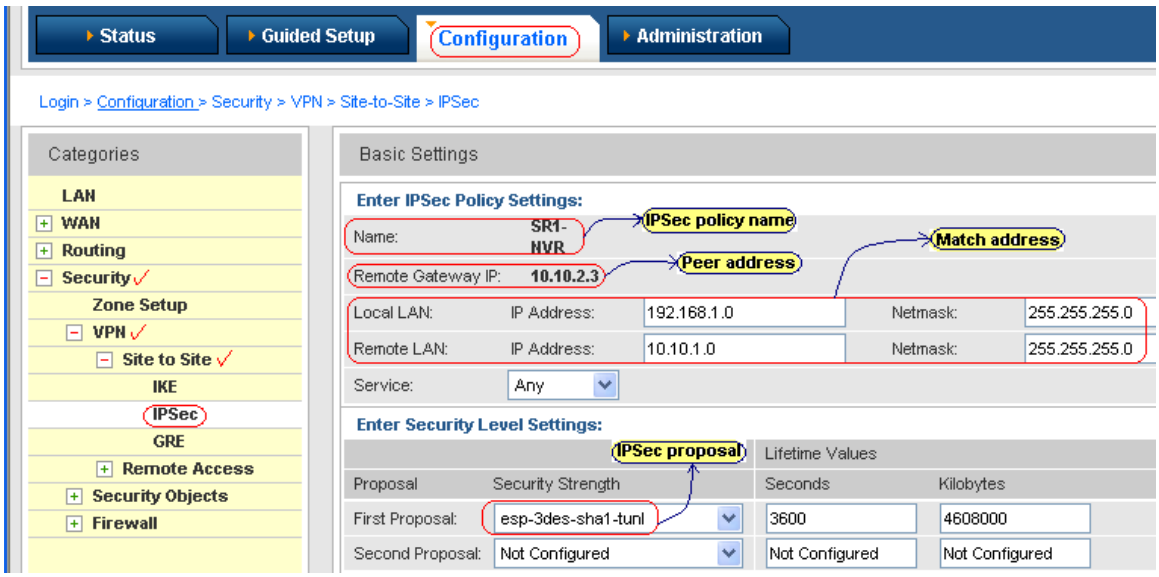
4.1.2 IKE Policy Configuration

The next step is to configure IKE policy. To add or modify IKE policy, click on the Configuration tab and then browse through the categories on the left side of the screen towards Security > VPN > Site to Site > IKE. Click on New to add a new policy or click on the existing policy to modify it. The figure below shows an example of how IKE policy is configured using HTTP GUI. As you can see, the logic is similar with CLI configuration wherein you have to enter the policy name, peer address, local address, IKE mode, Authentication method, IKE proposal, and IKE lifetime values. The advantage, as previously stated, is that you don't have to enter the commands. All you need to do is enter the values for the IKE settings.



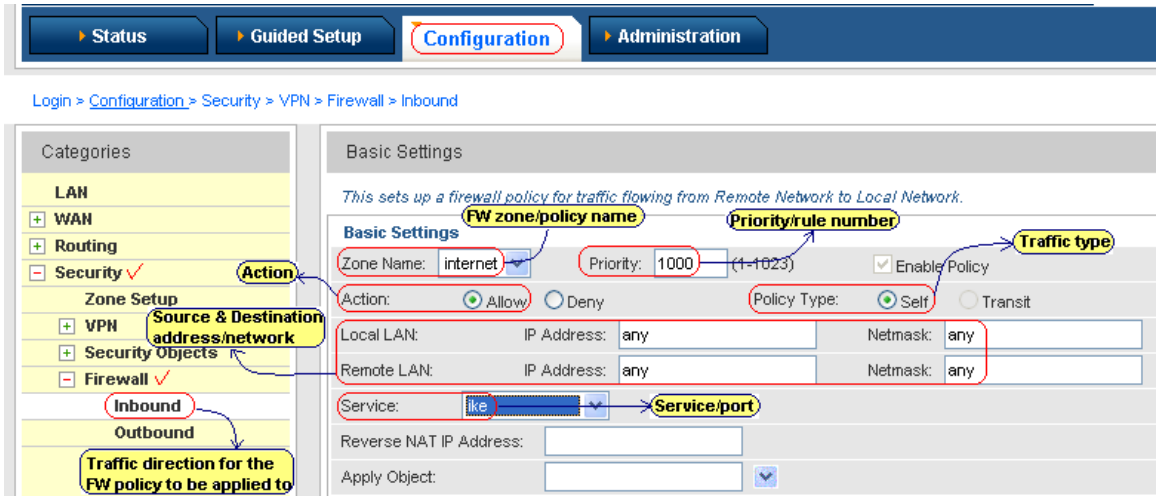
4.1.3 IPSec Policy Configuration

To add or modify an IPSec policy, click on Configuration tab and go to Security > VPN > Site to Site > IPSec. Then click on New button to add new IPSec policy or click on the existing IPSec policy to modify it. If adding a new IPSec policy, enter the IPSec policy name, peer address (remote gateway IP), and match address which is basically the source/local network and destination/remote network. And then select the desired IPSec proposal.



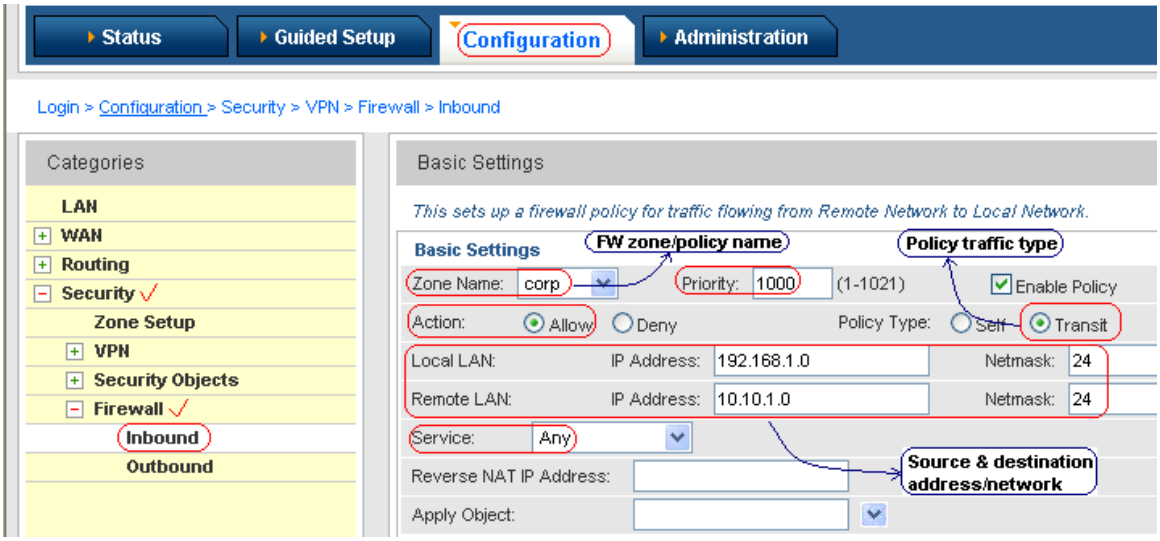
4.1.4 Firewall Internet Configuration

After configuring IKE and IPSec policies, the FW internet must be configured to allow IKE service in order for the Secure Router to accept inbound IKE negotiation and connection request. To do this via HTTP GUI, simply click on Configuration tab and go to Security > Firewall > Inbound. Then click on the New button to add a new FW policy. Select *internet* under Zone Name, enter *priority/rule number* under Priority, select *allow/permit* under Action, choose *self* for the Policy Traffic Type, and select *ike* under Service. For the source/local LAN & destination/remote LAN, just leave the default value of any.



4.1.5 Firewall Corp Configuration

In order to allow *transit* traffic from the network on the other side of the BOT (10.10.1.0/24 in our example) destined to the local LAN (192.168.1.0/24 in our example) on the private/trusted side of SR, a new policy under Firewall *Corp* must be added. As shown below, the new policy should allow any inbound transit traffic from 10.10.1.0/24 destined to 192.168.1.0/24 network. Take note that it is important that the policy traffic type must be set to 'transit' instead of 'self'. Otherwise, the traffic will not traverse beyond the Secure Router.

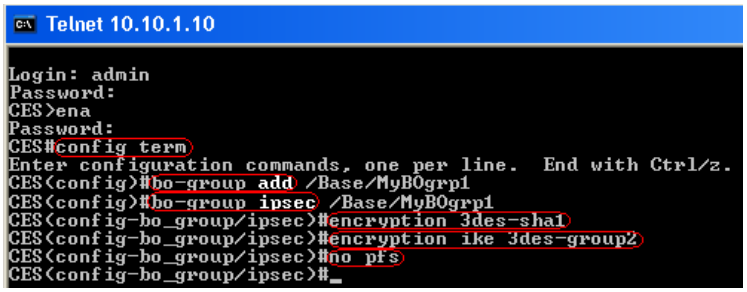


4.2 Configuring VPN Router via CLI

Another method of configuring the Avaya VPN Router is via CLI (Command Line Interface) which can be accessed either through console connection or telnet session. This section will show how to perform BO VPN configuration using CLI commands. It is assumed that physical and management interfaces have been properly configured and IP address has been assigned.

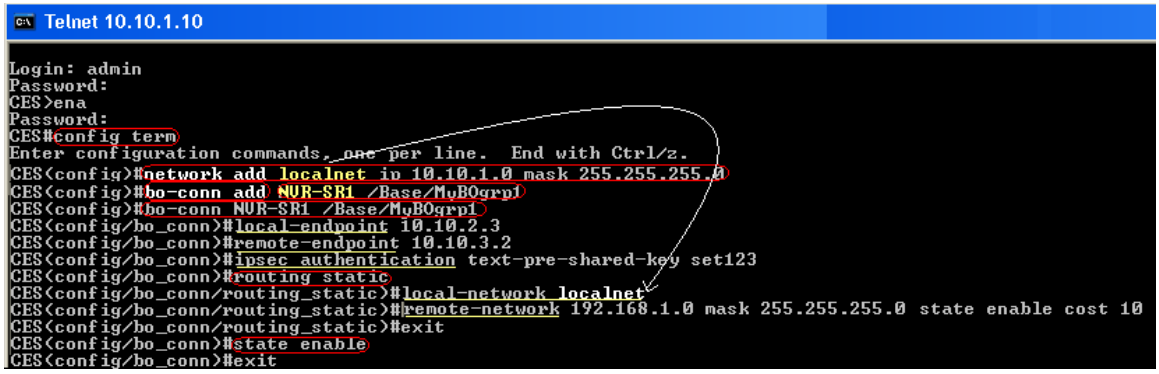
4.2.1 BO Group Configuration

The first step is to enter into configuration mode and then create a BO group. Take note that /Base must be included in front of the new BO group name and they are case sensitive. Once the new BO group has been added, modify the IPSec settings of the newly configured BO group and ensure that they match with the peer device (Secure Router). The default IPSec encryption is DES-MD5 so it must be changed to 3DES-SHA1. Also, the default IKE encryption and DH group is DES with DH group1 so it must be changed to 3DES with DH group2. The peer device has PFS disabled so it must be disabled in the VPN Router as well. The rest of the BO group settings should be left in its default value.



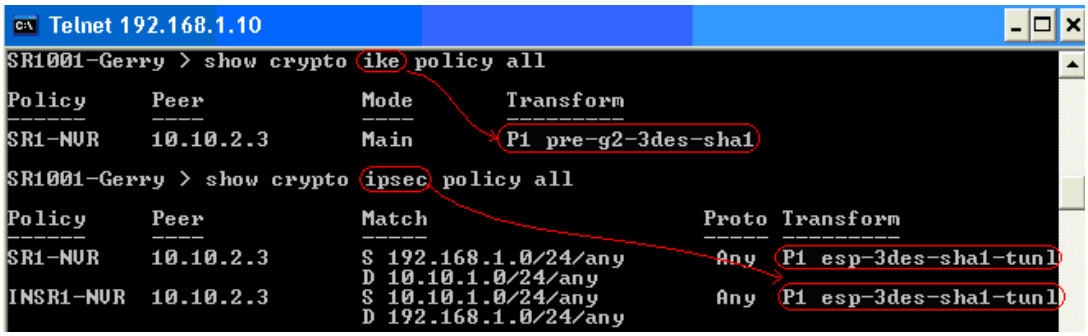
4.2.2 BO Connection Configuration

The next step is to add a BO connection under the configured BO group. But before configuring the BO connection, create a network by issuing the CLI command 'network add <network name> ip <local network> mask <subnet mask>'. The created network will be used as the local network when configuring the BO connection. As shown from the figure below, the BO connection is configured by entering the local & remote endpoints, authentication method with its secret key, and the local & remote accessible networks. Lastly, the BO connection must be enabled by issuing 'state enable' CLI command. By default, the tunnel type and connection type is IPSec and Peer to Peer, respectively so there's no need to explicitly configure the tunnel and connection type. The rest of the settings should remain the same.



4.3 Configuring Secure Router with Two or More Transform Proposals

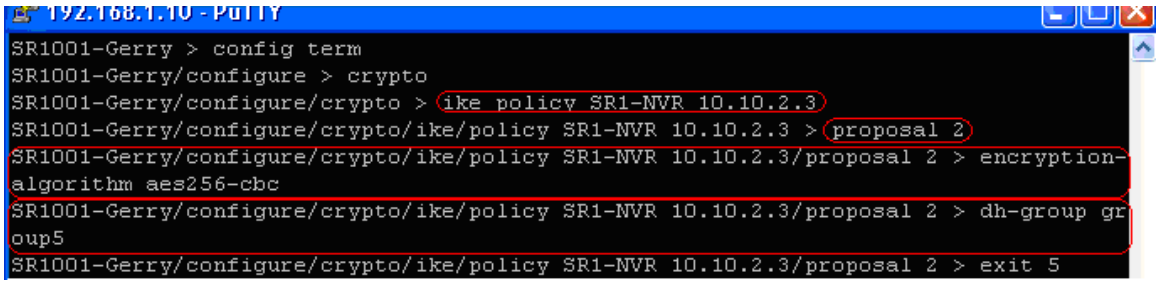
There maybe certain situation(s) that will require you to create two or more proposals. This section will show you how to configure Secure Router for two or more IKE or IPSec proposals. In our previous example, both IKE and IPSec policies have one proposal (P1) which can be seen from the figure below.



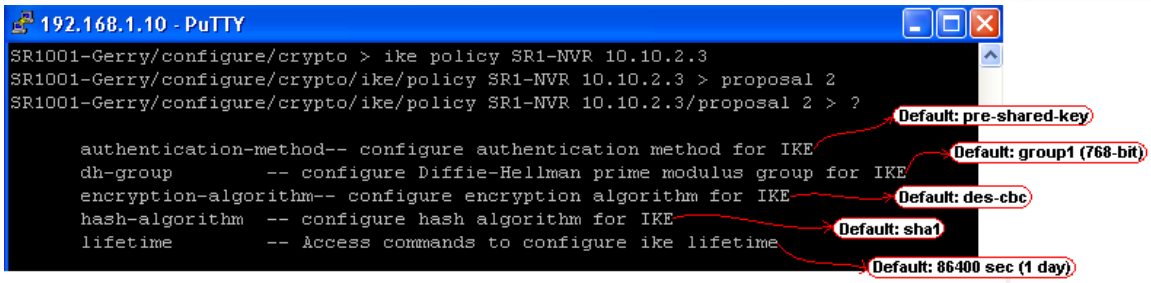
4.3.1 Multiple IKE Proposals

IKE establishes a secure communication channel for itself in phase 1 before negotiating the IPsec proposals in phase 2. During phase 1, IKE may propose multiple protection suites. Each IKE proposal specifies a particular choice for all of Authentication method, Encryption algorithm, Hash algorithm, DH group, and IKE lifetime. Some proposal in the list must be agreeable to both peers for the negotiation to proceed. Only one proposal on the list will ultimately be negotiated and used by the peers.

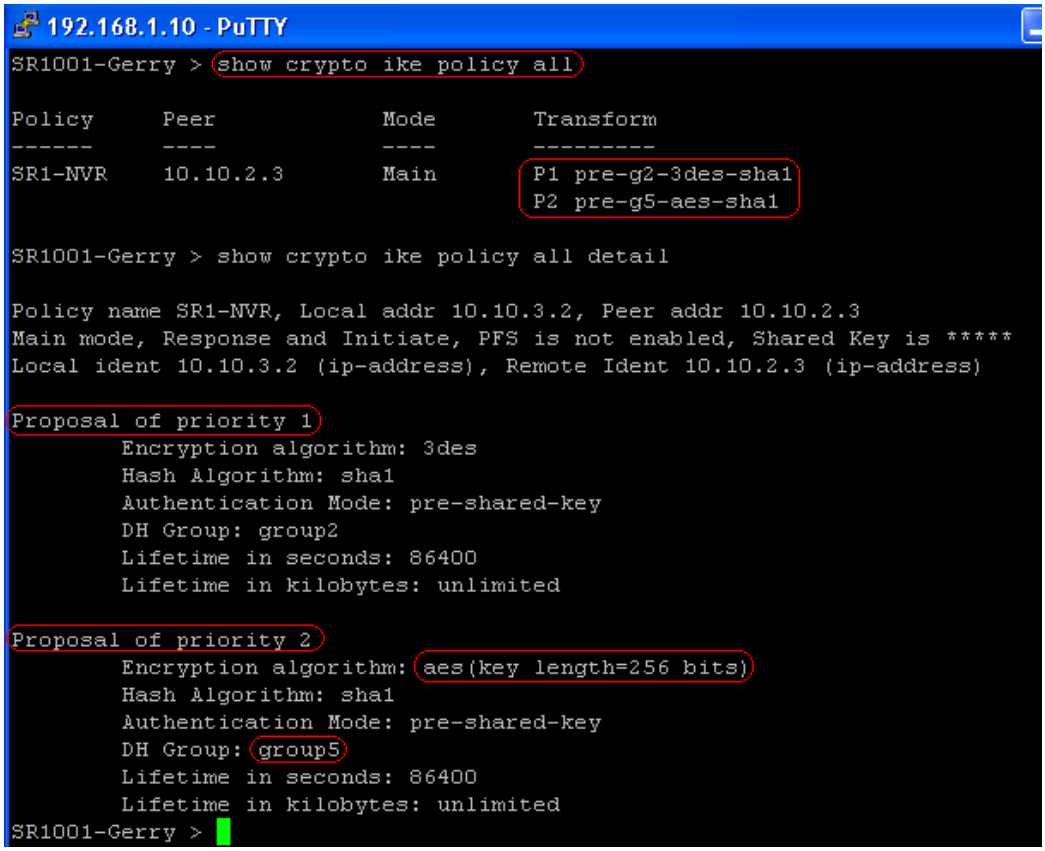
Let's assume that a second IKE proposal is necessary and the requirement is PSK authentication method, AES256 encryption, DH group5, and SHA1 hash algorithm. To add a proposal (note: SR accepts up to 5 proposals only) under IKE policy, simply edit the configured IKE policy as shown in the figure below.



Then enter 'proposal <priority number>' and modify the default IKE transform proposal. As shown from the figure below, the default authentication method is pre-shared-key so there's no need to modify the authentication method. The default DH-group is group1 so it should be modified to group5. Also, the default encryption algorithm is DES so it should be changed to AES256. The default hash algorithm is SHA1 so it is not necessary to modify the hash algorithm. In our example, there's no specific requirement for IKE lifetime so we will just leave it in its default value.



To see the proposals for IKE policy, use the CLI command 'show crypto ike policy all' or use 'show crypto ike policy all detail' for detailed information.

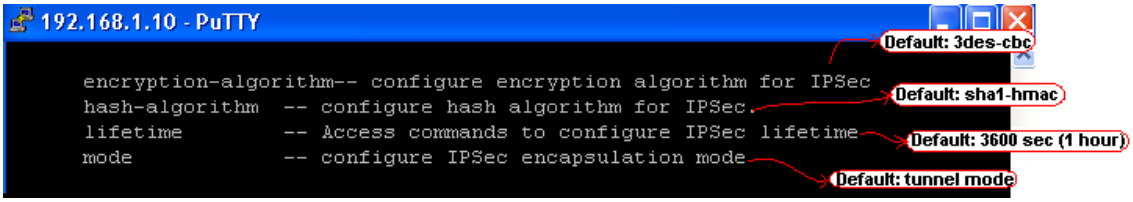


4.3.2 Multiple IPsec Proposals

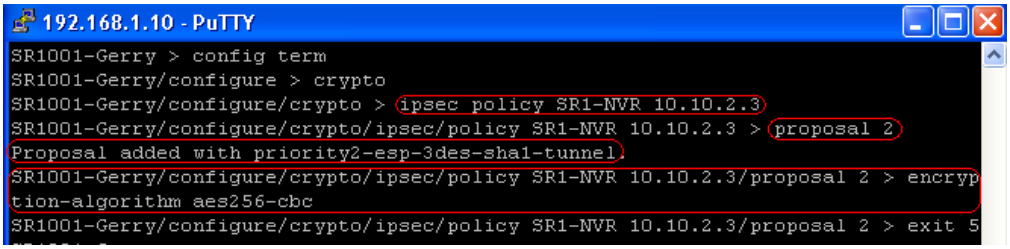
After IKE establishes a secure communication channel for itself in phase 1, it proceeds to negotiate the IPSec proposals in phase 2. During phase 2, IKE may propose multiple protection suites for IPSec protocols such as ESP and AH. Each phase 2 proposal specifies a choice for all of Encryption algorithm, Hash algorithm, IPSec lifetime, and Encapsulation mode. At least one proposal in the list must be agreeable to both peers for the negotiation to proceed.

Assuming that a second IPSec proposal is also necessary and the specified requirement is AES256 encryption algorithm and SHA1 hash algorithm. Similar to configuring IKE proposal, the same logic is applied when configuring IPSec proposal wherein the default IPSec proposal is modified in order to match the requirement.

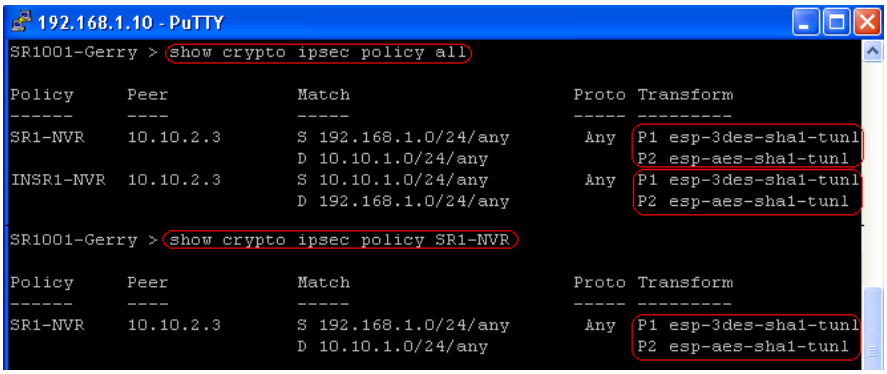
As shown from the figure below, the default encryption algorithm for IPSec proposal is 3DES so it should be changed to AES256. The default hash algorithm is SHA1 so it is not necessary to modify the IPSec proposal's default hash algorithm. In our example, there's no specific IPSec lifetime requirement so we will just use the default value. The IPSec encapsulation mode for BO connection should be tunnel mode so there's no need to modify it.



To add a second IPSec proposal, simply edit the configured IPSec policy as shown in the figure below and then add proposal 2. As shown below, SR automatically added the default IPSec proposal. However, the IPSec encryption does not match with the requirement so it was modified from 3DES to AES256.



To see the proposals for all the configured IPSec policies, use the CLI command show crypto ipsec policy all'. To see the proposals for a particular IPSec policy only, use the CLI command 'show crypto ipsec policy <policy name>'.

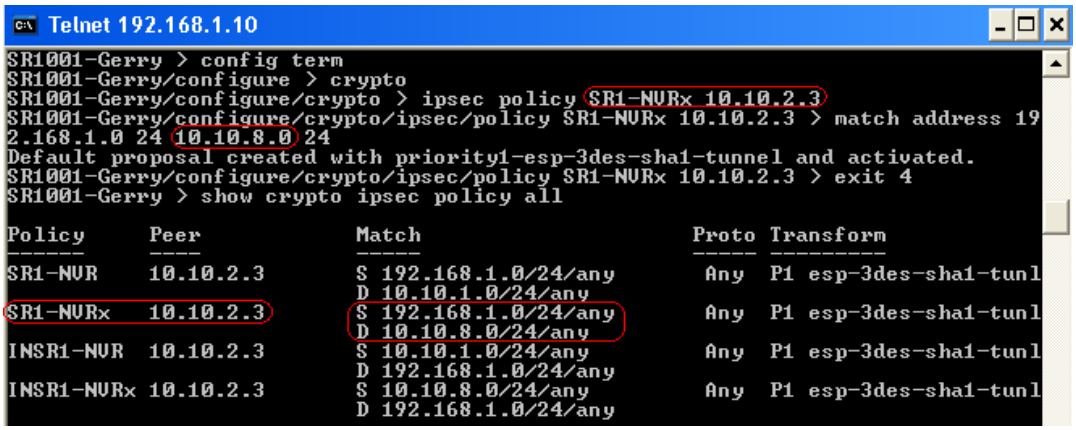


4.4 Configuring Secure Router with Multiple Local/Remote Accessible Networks

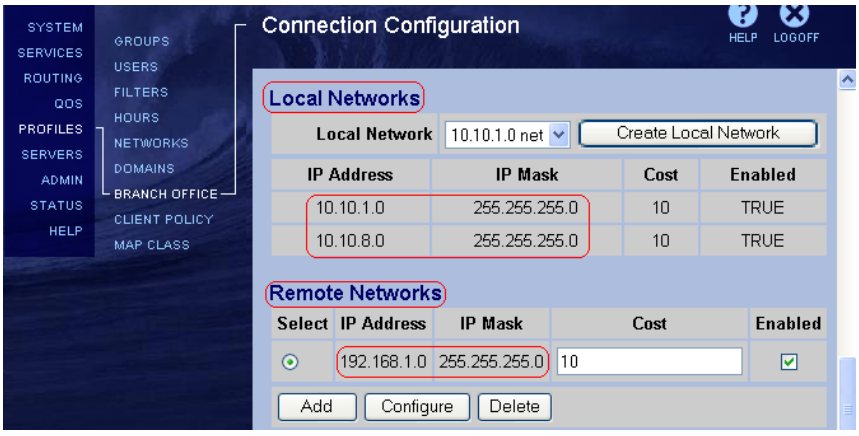
In our previous example, the Secure Router has one source/local network (192.168.1.0/24) and one destination/remote network (10.10.1.0/24). But how do we configure SR if there are multiple source/local or destination/remote networks? This section will show you how. As of to date, the Secure Router does not support multiple source/local or destination/remote networks for a particular IPSec policy. The solution is to create a single IPSec policy for each source/local network and destination/remote network match.

4.4.1 Add a Second IPSec Policy & Associate the Proper Match Address

Let's assume that SR has one source/local network (192.168.1.0/24) but has two destination/remote networks (10.10.1.0/24 and 10.10.8.0/24). SR should be configured, as shown in the figure below, by *adding a second IPSec policy* with a match address of 192.168.1.0/24 as the source/local network and 10.10.8.0/24 as the destination/remote network. Take note that if the multiple networks can be summarized then you only have to create one IPSec policy which will contain the summarized networks in the match address.

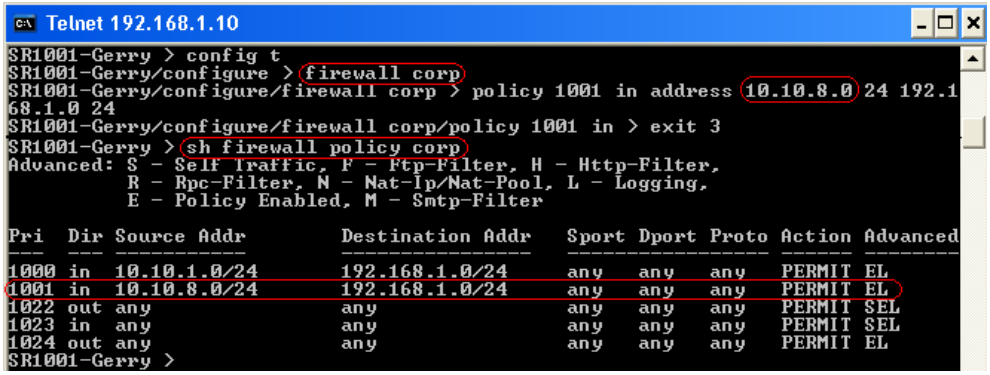


In VPN Router, all you need to do is edit the BO connection and simply add the network (which is 10.10.8.0/24 in our example) under the local networks portion of the BO connection configuration page.



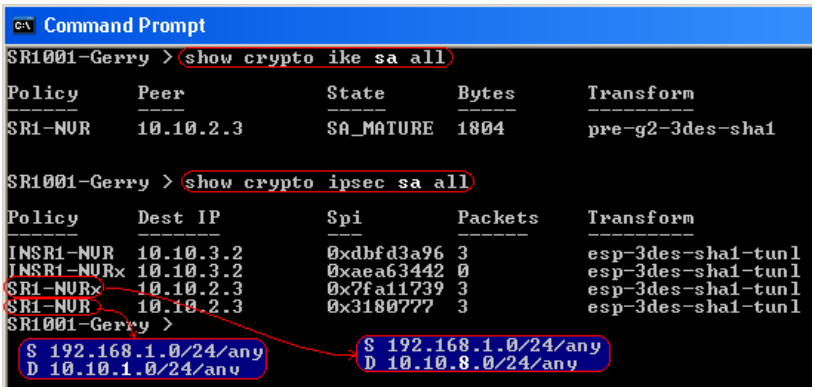
4.4.2 Allow Inbound Transit Traffic for the Configured Match Address

As discussed in Section 3.1.6, the SR must be manually configured to allow *inbound* transit traffic from a particular source network (this will be 10.10.1.0/24 and 10.10.8.0/24 in our example) to a particular destination network (this will be 192.168.1.0/24 in our example). Since there's already an existing firewall policy that allows inbound transit traffic from 10.10.1.0/24 network, we only need to create another policy that will allow inbound transit traffic from 10.10.8.0/24 network. To do this, edit Firewall policy *Corp* and then type 'policy <priority/rule number> in address 10.10.8.0 24 192.168.1.0 24'. To see the added policy for Firewall Corp, use the CLI command 'show firewall policy corp'.

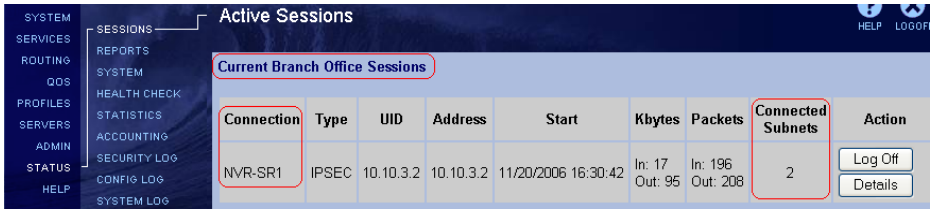


4.4.3 Test & Verify BOT Session for the Two IPSec Policies

To establish BOT connection for the configured IPSec policies, send traffic towards the 10.10.1.0/24 and 10.10.8.0/24 networks. Once the BOT has been successfully established between SR-VPN Router networks, you should be able to see one IKE SA and two pairs of IPSec SAs (one pair for each of the configured IPSec policies: SR1-NVR and SR1-NVRx in our example) in the Secure Router as shown in the figure below.



In VPN Router, as shown in the figure below, you should be able to see one BO session with two connected subnets. Click on the 'Details' button and you should see 10.10.*1*.0 – 192.168.1.0 and 10.10.*8*.0 – 192.168.1.0 connected subnets.



5. Customer service

Visit the Avaya Web site to access the complete range of services and support that Avaya provides. Go to www.avaya.com or go to one of the pages listed in the following sections.

5.1 Getting technical documentation

To download and print selected technical publications and release notes directly from the Internet,go to www.avaya.com/support.

5.2 Getting product training

Ongoing product training is available. For more information or to register, you can access the Web site at www.avaya.com/support. From this Web site, you can locate the Training contacts link on the left-hand navigation pane.

5.3 Getting help from a distributor or reseller

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

5.4 Getting technical support from the Avaya Web site

The easiest and most effective way to get technical support for Avaya products is from the Avaya Technical Support Web site at www.avaya.com/support.

Appendix: Abbreviations/Glossary

Acronym	Term
AH	Authentication Header
BO	Branch Office
BOT	Branch Office Tunnel
CLI	Command Line Interface
DH	Diffie-Hellman
ESP	Encapsulating Security payload
FW	Firewall
GUI	Graphical User Interface
ICMP	Internet Control Message Protocol
IKE	Internet Key Exchange
IPsec	Internet Protocol Security
ISAKMP	Internet Security and Key Management Protocol
LAN	Local Area Network
PSK	Pre-Shared Key
SA	Security Association
SPI	Security Parameter Index
SR	Secure Router
VPN	Virtual Private Network
WAN	Wide Area Network