Avaya Solution & Interoperability Test Lab

Configuring Policy Based Routed Encryption using the Extreme Networks Sentriant CE150 and BlackDiamond 12k to support Avaya Communication Manager H.323 Trunk – Issue 1.0

Abstract

These Application Notes describe the steps for configuring a Policy Based Routed Encryption solution using an Extreme Networks Sentriant CE150 and a BlackDiamond 12k switch. The BlackDiamond 12k is used to route H.323, RTP (voice media) and sample application data traffic traversing two locations to the Sentriant CE150 for encryption as well as to perform traffic shaping and bandwidth management. Information in these Application Notes has been obtained through Developer*Connection* compliance testing and additional technical discussions. Testing was conducted via the Developer*Connection* Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

The Extreme Networks Sentriant CE150 is a dedicated encryption appliance capable of supporting either copper or fiber Gigabit Ethernet interface. The CE150 supports AES, 3DES, and DES encryption and Sha and MD5 hashing algorithm. Designed as a high speed, low latency encryptor, the CE150 relies on the connected Ethernet switches to manage the Quality of Service (QoS) for all outgoing traffic. This includes both traffic prioritization and bandwidth management.

These Application Notes illustrate a solution to encrypt H.323, RTP (voice media) and sample application traffic that traverses two locations. The sample application traffic is used as an example of how the solution can provide QoS to any data application even though the application does not provide any QoS mechanism natively. This could be a call center application or a customer database application which requires reliable access to a backend server in conjunction with Avaya VoIP calls. As depicted in **Figure 1**, a sample network consisting of Location-A and Location-B are connected together via a Gigabit Ethernet connection. An Extreme Networks BlackDiamond (BD) 12k is used to route H.323, RTP (voice media) and sample application traffic to the CE150 for encryption before being sent to the other location, as well as to provide Quality of Service management for this traffic. All other traffic is forwarded by the BD12k to the intended destination, directly bypassing the CE150. For simplicity, there is only one IP subnet, or Virtual Local Area Network (VLAN) in each location[1]. An additional VLAN was configured for the connection linking the two locations together.

1.1. Traffic Flow

An access policy is configured on the BD12k at both Location-A and Location-B. This access policy is applied to the local VLAN identifying outgoing H.323, RTP (voice media) and sample application traffic and forwards the selected traffics to the "Local" interface on the CE150. In addition to identifying outgoing traffic for encryption, the access policy prioritizes traffic based on various attributes such as Source/Destination IP address, Source/Destination port, and protocol. Bandwidth management is achieved through a rate limiting feature for the different priority queues residing on the egress port of the BD12k that connects to the CE150 "Local" interface. The CE150s forward all the incoming traffic from the "Local" interface securely through the IPSec tunnel that has been established with the CE150 at the other location. Once the opposing CE150 receives the traffic from the IPSec tunnel, the traffic is decrypted and forwarded to the destination IP address.

As mentioned earlier, H.323, RTP (voice media) and sample application traffic is configured to be encrypted by the CE150. The sample configuration defines each type of traffic as follows:

- H.323 traffic is generally defined as any traffic between the Avaya Media Server located in each location.
- RTP (voice media) traffic is defined as UDP traffic between the two locations with a port range of 2048 to 3029 as defined in Section 5, Step 9.
- Sample application was defined as UDP traffic between the two locations with a port number of 4000.

[1] The recommended Best Practice for VLAN configuration is to have separate VLAN for Voice and Data traffic.

The BD12k access policy uses the above criteria to identify each type of traffic and assigns them to different QoS profile queues.

2. Configuration

Figure 1 illustrates the configuration used in these Application Notes. All Avaya IP Telephones with extension range of 3xxxx are registered with Avaya Communication Manager at Location-A and all Avaya IP Telephones with extension range of 4xxxx are registered with Avaya Communication Manager at Location-B. An H.323 trunk, configured between the two Avaya Communication Manager servers, routes calls between the two sites. All IP addresses are statically administered. The CE150 at each site is managed out-of-band via the management port IP address. The design and configuration of the out-of-band management network is beyond the scope of these Application Notes.

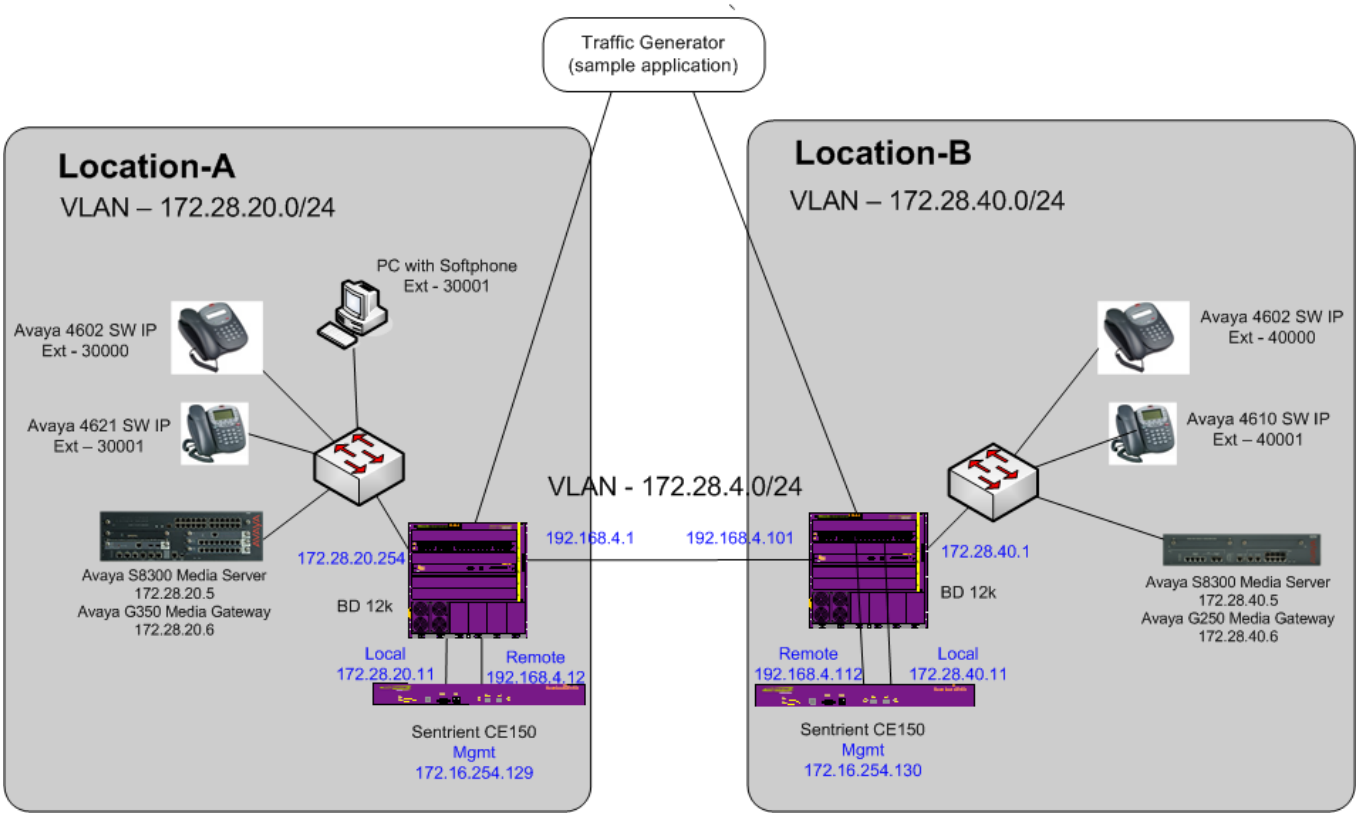


Figure 1: Sample Network Configuration

3. Equipment and Software Validated

The following equipment and software/firmware were used for the sample configuration:

DEVICE DESCRIPTION	VERSION TESTED
Avaya S8300 Media Server with G250 Media Gateway	Avaya Communication Manager R3.1.2 (R013x.01.2.632.1)
Avaya S8300 Media Server with G350 Media Gateway	Avaya Communication Manager R3.1.2 (R013x.01.2.632.1)
Avaya 4602SW IP Telephone	R2.3 – Application (a02d01b2_3.bin)
Avaya 4610SW IP Telephone	R2.3 – Application (a10d01b2_6.bin)
Avaya 4621SW IP Telephone	R.2.3 – Application (a20d01b2_6.bin)
Avaya IP Softphone	R5.24.8
Extreme Networks Sentriant CE150	IPS 3.2.1
Extreme Networks BlackDiamond 12k	XOS 11.4.3.4

4. Configure Extreme Networks equipment

This section describes the configuration for Extreme Network BlackDiamond 12k and Sentriant CE150 as shown in **Figure 1**. for Location-B. All steps in this section must be repeated for Extreme Networks devices in Location-A using the appropriate IP addresses.

4.1. Configure the Sentriant CE150

This section shows the necessary steps in configuring the Sentriant as shown in the **Figure 1**.

4.1.1. Configure initial Sentriant setup

This section shows the initial steps in configuring the Sentriant interfaces using the console interface.

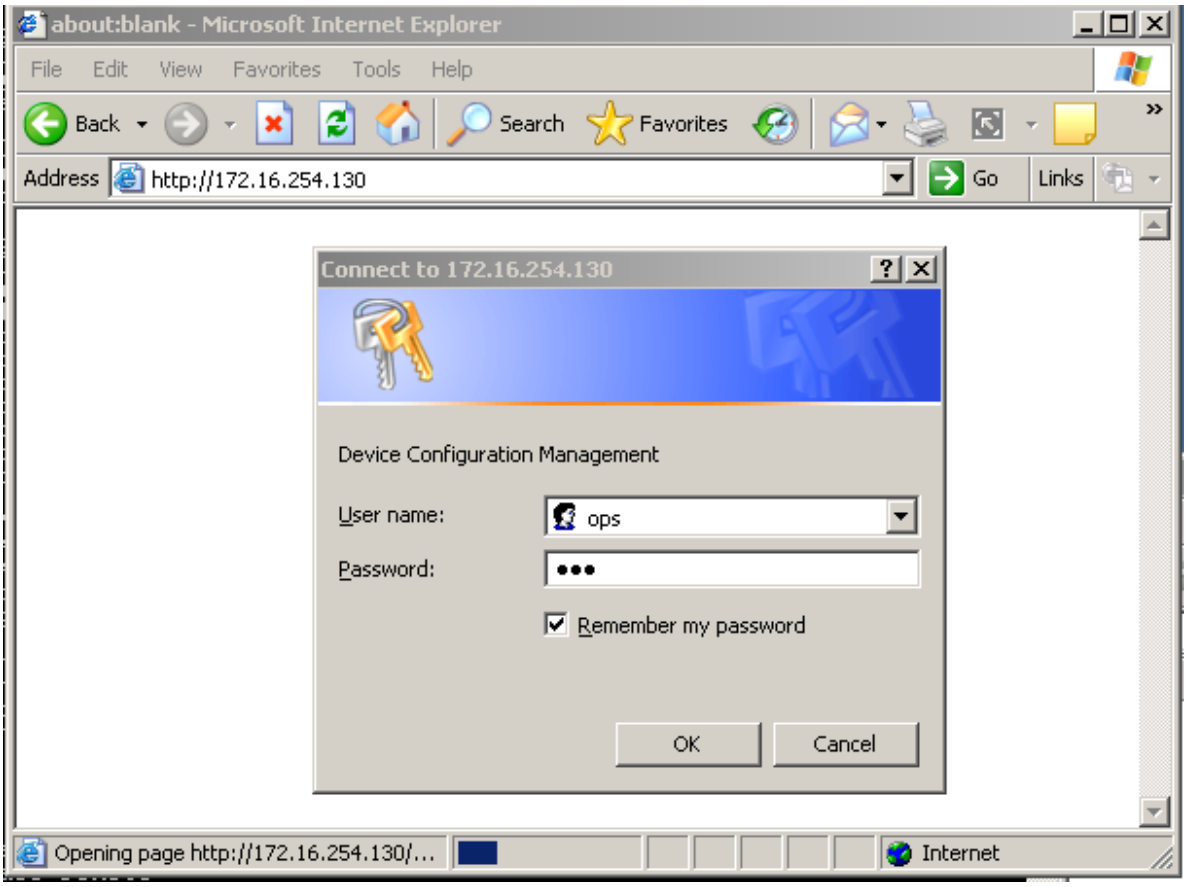
Step	Description
1.	Connect to the Sentriant via the console port using the following port setting. Bits per second: ***115200*** Data bits: ***8*** Parity: ***None*** Stop bits: ***1*** Flow control**:** ***None***

Step	Description
2.	Log in to the Sentriant using the appropriate user name and password User Access Verification Username: ***ops*** Password: ops>
3.	Configure the Sentriant Management, Local and Remote interfaces. ops> ***config t*** config> ***interface management*** config-ifMan> **ip *address 172.16.254.130 255.255.255.0*** config-ifMan> ***exit*** config> ***interface local*** config-ifLocal> ***ip Address 172.28.40.11 255.255.255.0*** config-ifLocal> ***macResolutionMechanism arp*** config-ifLocal> ***exit*** config-ifRemote> ***ip Address 192.168.4.112 255.255.255.0*** config-ifRemote> ***exit*** config> **exit** ←--------- save the configuration--------------→ ops> ***copy system:running nvram:config***

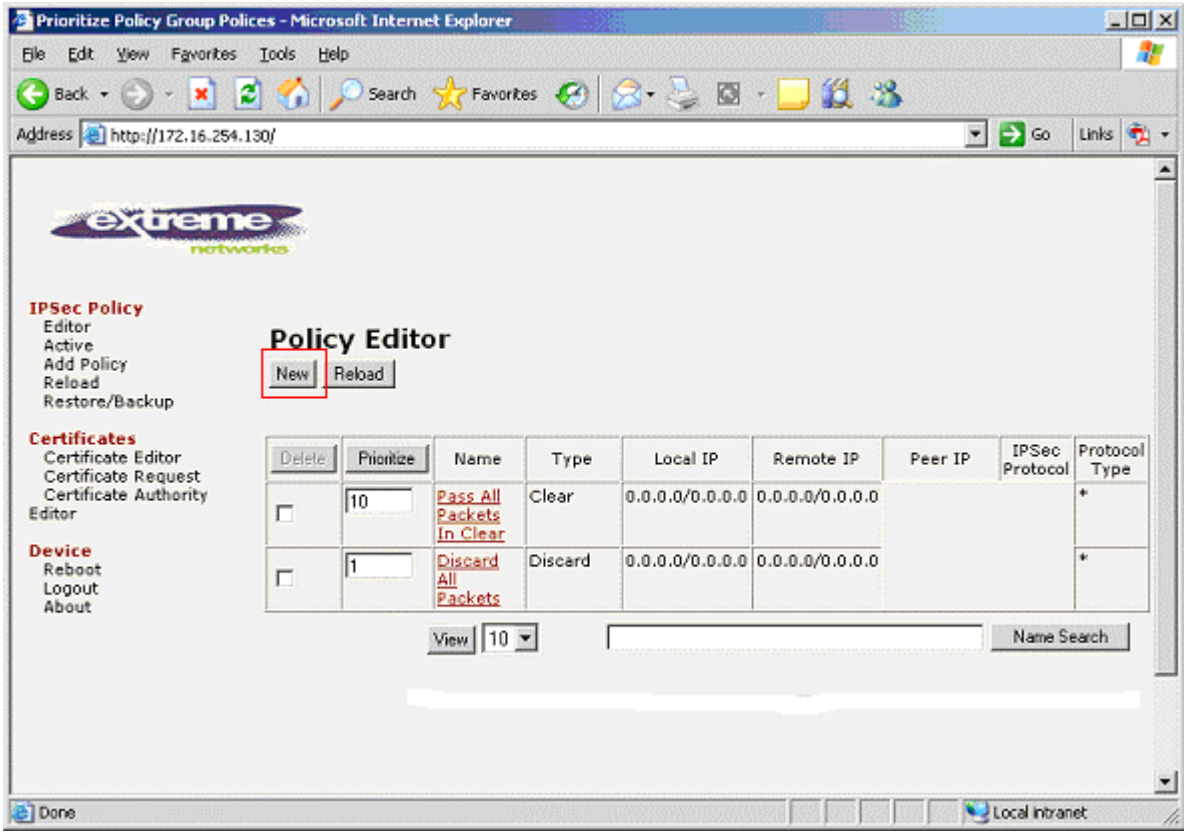
4.1.2. Configure Sentriant encryption policy

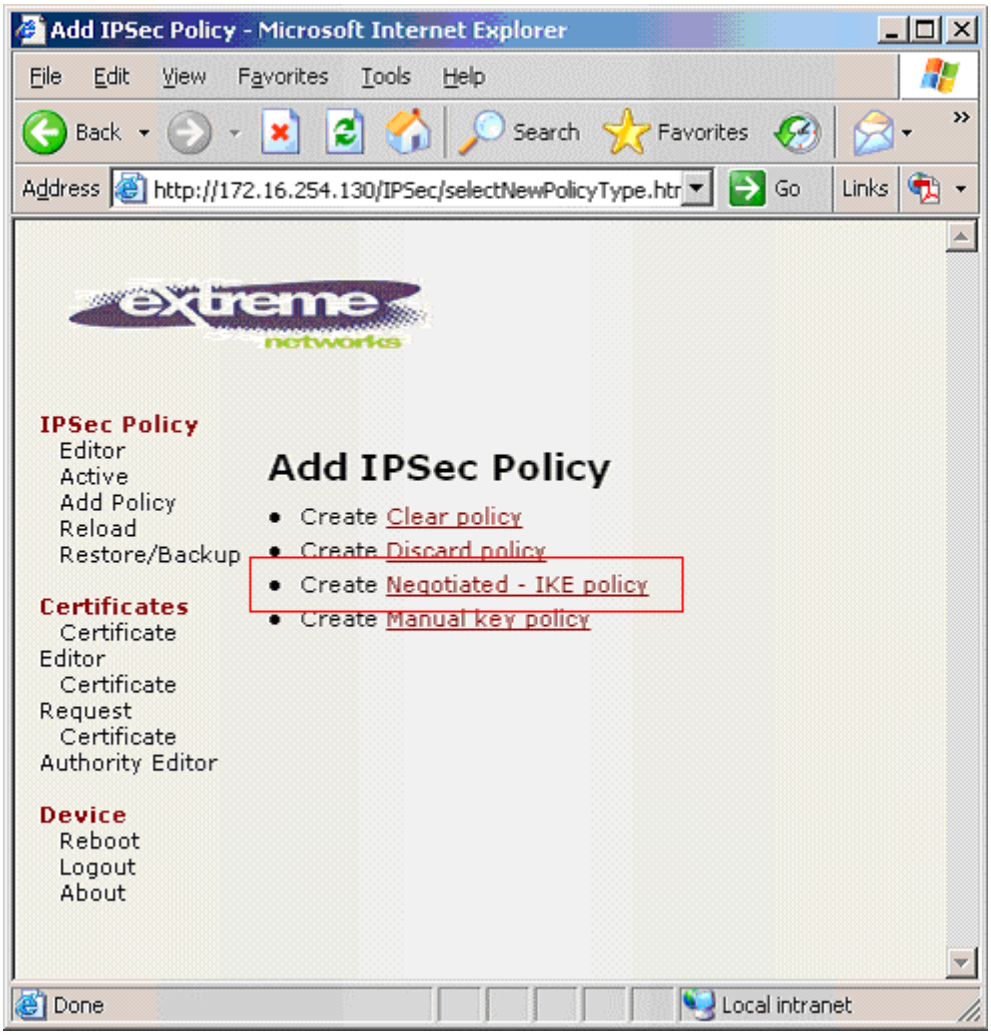
This section shows the steps in configuring an encryption policy on the Sentriant.

1.	Connect to the CE150 via a web browser. Enter the IP address of the CE150's management interface as the Address. Log in using the appropriate **User name** and **Password**.



2.	Create a new policy by clicking on **New**.

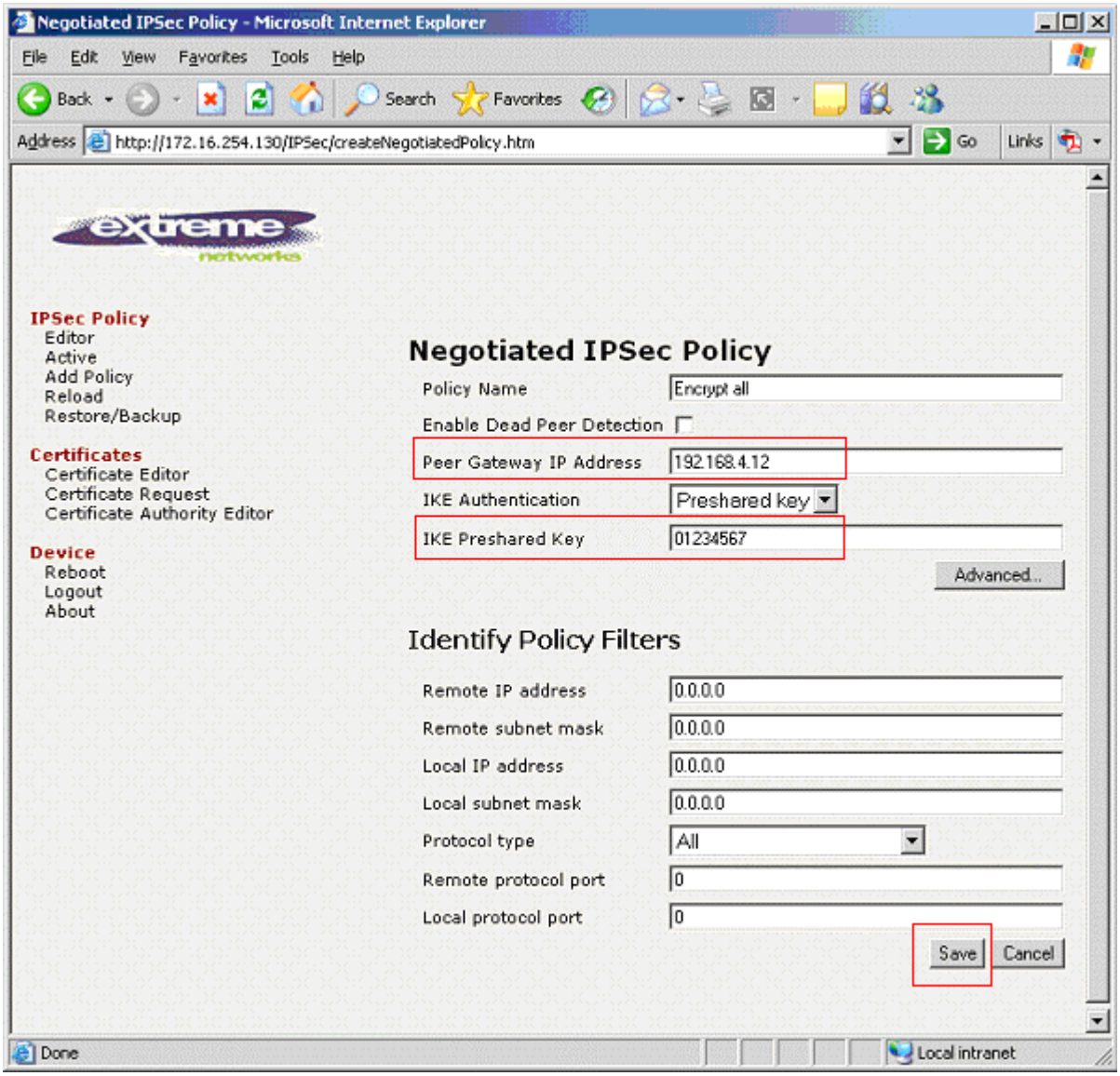


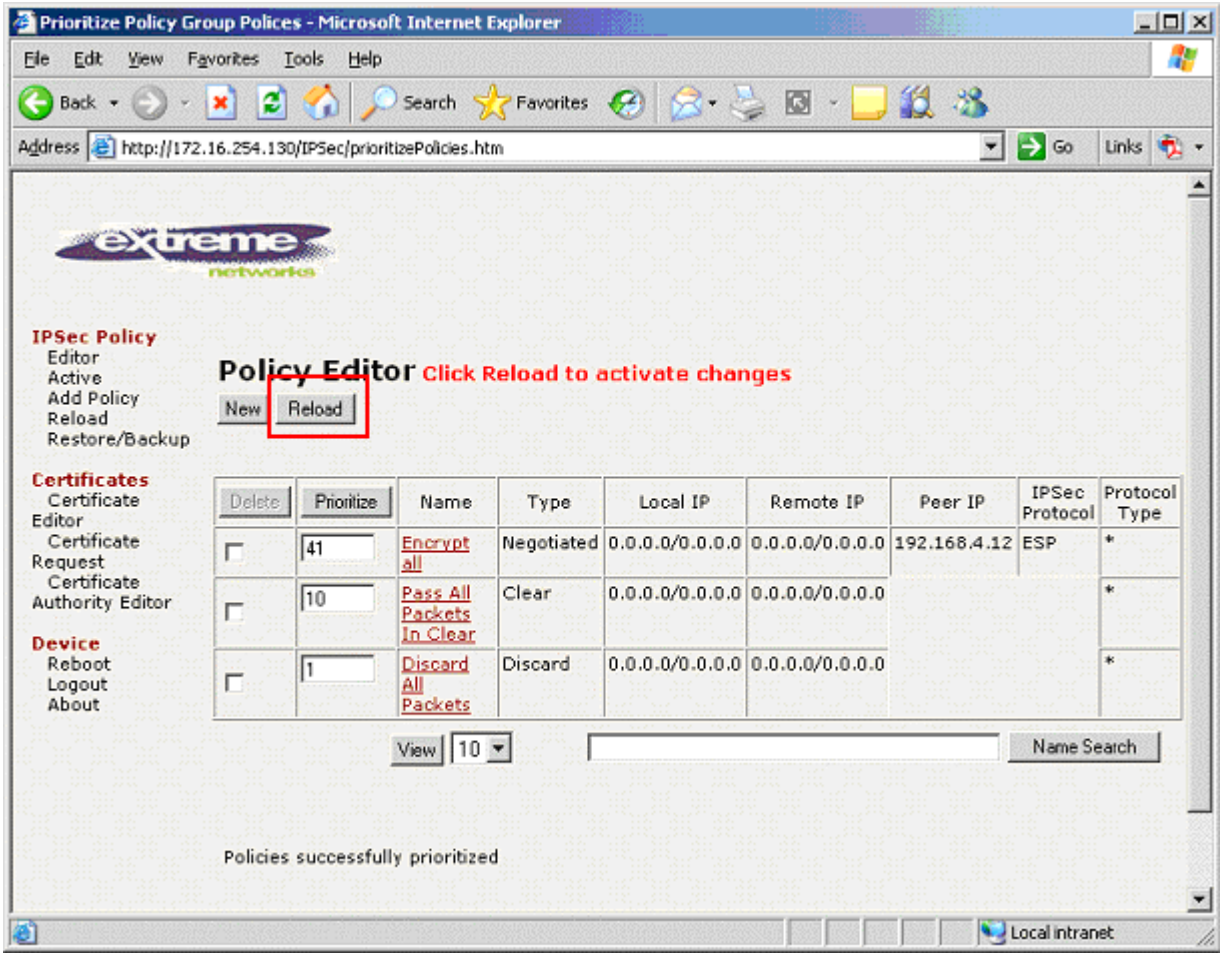
3.	Click on **Negotiated – IKE policy** to create an encryption policy. 

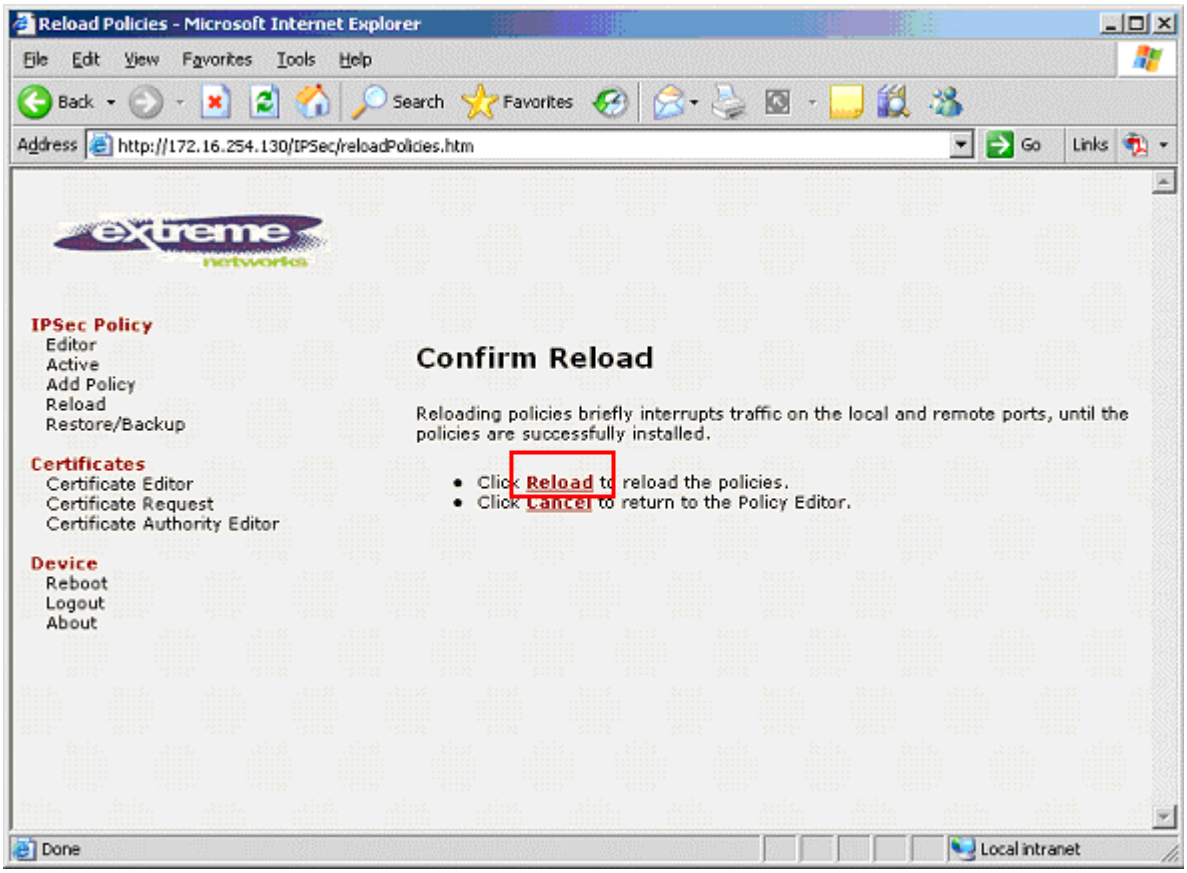
4. Enter the appropriate information in all the highlighted fields. All other fields are left at their default value. Click **Save** to complete.

The **Peer Gateway IP address** is the IP address of the peering CE150's Remote port.
The same **IKE Preshared Key** string will need to be entered at the peering CE150 policy.

By default, the CE150 uses AES for both Phase 1 and Phase 2 encryption algorithm and Sha for hash algorithm. In addition to AES, the CE150 support 3DES and DES for encryption and MD5 hash algorithm. Click the Advanced button to change the encryption and hash algorithm.



5.	Click **Reload** to activate changes. 

6.	Click **Reload** again to confirm. 
7.	Repeat all steps in this section for the CE150 in Location-A using appropriate IP addresses.

4.2. Configure the BlackDiamond 12k

This section shows the steps for configuring the Black Diamond 12k to interoperate with the CE150 to provide for policy based routing and Quality of Service.

1.	Connect to the BD 12k and log in using the appropriate credential.
	
	`login: user`
	`password:`
	`BD-12804.1 #`

2.	Create the necessary VLANs. VLAN v40 is the local IP network for Location-B, and VLAN v4 is the IP network that interconnections the two locations.
	
	`BD-12804.1 # create vlan v40`
	`BD-12804.1 # config vlan v40 tag 40`
	`BD-12804.1 # config vlan v40 ipaddress 172.28.40.1/24`
	`BD-12804.1 # enable ipforwarding v40`
	`BD-12804.1 # create vlan wan`
	`BD-12804.1 # config vlan wan tag 4`
	`BD-12804.1 # config vlan wan ipaddress 192.168.4.101/24`
	`BD-12804.1 # enable ipforwarding wan`

3.	Assign the VLAN to the appropriate port.
	
	`BD-12804.1 # configure vlan v40 add ports 2:10,2:13,2:18 untagged`
	`BD-12804.1 # configure vlan wan add ports 2:7,2:11 untagged`

4. Create a policy to redirect H.323, RTP (voice media) and sample application traffic for encryption and QoS profile assignment. Any name can be used for this policy. The sample configuration uses a policy called **sentriant.pol**. The ***edit policy sentriant.pol*** command will initiate a "vi" style text editor to create the script. The port range used for VoIP-RTP portion of the policy must be the same as the **UDP Port Min** and **UDP Port Max** value shown in Section 5, Step 9. For information regarding the use of this editor, please refer to reference document [5] and [6].

```
BD-12804.1 # edit policy sentriant.pol
```

Below shows the sentriant.pol policy.

```
#   Entry for Avaya VoIP Signaling traffic
#
entry VoIP-Signal {
if match all {
    source-address 172.28.40.5/32;
    destination-address 172.28.20.5/32;
}
then {
    qosprofile qp7;
    redirect 172.28.40.11;
}
}
#  Entry for Avaya VoIP Media traffic
#
entry VoIP-RTP {
if match all {
    source-address 172.28.40.0/24;
    destination-address 172.28.20.0/24;
    protocol udp;
    destination-port 2048-3029;
}
then {
    qosprofile qp7;
    redirect 172.28.40.11;
}
}
#   Entry for sample application
#
entry sample-app {
if match all {
    source-address 172.28.40.0/24;
    destination-address 172.28.20.0/24;
    protocol udp;
    source-port 4000;
    destination-port 4000;
}
then {
    qosprofile qp2;
    redirect 172.28.40.11;
}
}
```

5.	Assign the sentriant policy to the appropriate VLAN. `BD-12804.1 #` ***configure access-list sentriant vlan v40 ingress***
6.	Configure the QoS profile for the port connecting to the Local CE150 port. In this case port 2:10 on the BD12k. The following configuration specifies that traffic in QP2 will use no more than 90% of total bandwidth and traffic in QP7 will be allocated with a minimum of 10% bandwidth. The bandwidth allocation in the sample configuration is for testing purposes only, specific bandwidth allocation should be determined based on the expected volume of VoIP calls over the link and the codec used. `BD-12804.1 #` ***configure qosprofile QP2 minbw 0 maxbw 90 ports 2:10*** `BD-12804.1 #` ***configure qosprofile QP7 minbw 10 maxbw 100 ports 2:10***
7.	Repeat all steps in this section for the BD12k switch at Location-A using appropriate IP addresses.

5. Configure Avaya Communication Manager

This section shows the necessary steps in configuring Avaya Communication Manager. For detailed information on the installation, maintenance, and configuration of Avaya Communication Manager, please consult reference [1], [2], [3] and [4]. The following steps describe the configuration of Avaya Communication Manager at Location-B. Repeat these steps at the Avaya Communication Manager at Location-A unless otherwise noted.

Step	Description
1.	Add a new station for the Avaya IP Telephones to the Avaya Communication Manager using the **add station** command. Configure the following fields. • **Extension:** ***40001*** (Extension number for the Avaya Telephone) • **Type:** ***4610*** (Avaya Telephone type used for this extension) • **Port:** ***IP*** (Type of connection for the Avaya Telephone) • **Security Code:** ***123456*** (Security code used by the Avaya Telephone to register with Avaya Communication Manager) • **Direct IP-IP Audio Connections:** ***y*** (Enable Shuffling) The first two pages of the **add station 40001** configuration are shown below. Repeat this step for each station.

Step	Description

```
add station 40001                                          Page   1 of   4
                                    STATION

Extension: 40001                          Lock Messages? n          BCC: 0
     Type: 4610                           Security Code: 123456      TN: 1
     Port: IP                          Coverage Path 1:             COR: 1
     Name: Room 18                     Coverage Path 2:             COS: 1
                                       Hunt-to Station:

STATION OPTIONS
             Loss Group: 19            Personalized Ringing Pattern: 1
                                                 Message Lamp Ext: 40001
           Speakerphone: 2-way                Mute Button Enabled? y
       Display Language: english
 Survivable GK Node Name:
         Survivable COR: internal                Media Complex Ext:
   Survivable Trunk Dest? y                           IP SoftPhone? n




                                                  Customizable Labels? y
```

```
add station 40001                                          Page   2 of   4
                                    STATION
FEATURE OPTIONS
          LWC Reception: spe              Auto Select Any Idle Appearance? n
         LWC Activation? y                          Coverage Msg Retrieval? y
  LWC Log External Calls? n                               Auto Answer: none
            CDR Privacy? n                           Data Restriction? n
   Redirect Notification? y                    Idle Appearance Preference? n
 Per Button Ring Control? n                  Bridged Idle Line Preference? n
   Bridged Call Alerting? y                        Restrict Last Appearance? y
  Active Station Ringing: single           Conf/Trans on Primary Appearance? n
                                                      EMU Login Allowed? n
       H.320 Conversion? n          Per Station CPN - Send Calling Number?
      Service Link Mode: as-needed
        Multimedia Mode: enhanced
    MWI Served User Type:                       Display Client Redirection? n
            AUDIX Name:                        Select Last Used Appearance? n
                                                 Coverage After Forwarding? s

                                               Direct IP-IP Audio Connections? y
 Emergency Location Ext: 40001     Always Use? n      IP Audio Hairpinning? y
```

2. Add the S8300 Media Server IP address located at Location-A into Avaya Communication Manager using the **change node-names ip** command. The screen below shows the entry for Avaya Communication Manager in **Location-A** with IP address of **172.28.20.5**.

```
change node-names ip                                       Page   1 of   1
                                 IP NODE NAMES
    Name                  IP Address          Name             IP Address
Location-A              172.28 .20 .5                           .   .   .
procr                   172.28 .40 .5                           .   .   .
                           .   .   .                            .   .   .
                           .   .   .                            .   .   .
```

Step	Description
3.	Configure a signaling group for the H.323 trunk between Avaya Communication Manager in Location-A and Location-B using the **add signaling-group** command. Make sure the following fields are configured. • **Group Type:** ***h.323*** (Signaling type used) • **Near-end Node Name:** ***procr*** (This is the **procr** name as shown in Step 2) • **Near-end Listen Port:** ***1720*** (Default port number for H.323 signaling) • **Far-end Node Name:** ***Location-A*** (Node name for Location-A system defined in Step 2) • **Far-end Listen Port:** ***1720*** (Default port number for H.323 signaling) • **Far-end Network Region:** ***2***

```
add signaling-group 1                                        Page   1 of   5
                                SIGNALING GROUP

 Group Number: 1              Group Type: h.323
                            Remote Office? n          Max number of NCA TSC: 0
                                      SBS? n           Max number of CA TSC: 0
                                 IP Video? n        Trunk Group for NCA TSC:
       Trunk Group for Channel Selection:
          Supplementary Service Protocol: a          Network Call Transfer? n
                          T303 Timer(sec): 10

   Near-end Node Name: procr                Far-end Node Name: Location-A
 Near-end Listen Port: 1720                 Far-end Listen Port: 1720
                                         Far-end Network Region: 2
         LRQ Required? n                  Calls Share IP Signaling Connection? n
         RRQ Required? n
     Media Encryption? n                      Bypass If IP Threshold Exceeded? n
                                                      H.235 Annex H Required? n
         DTMF over IP: out-of-band             Direct IP-IP Audio Connections? y
                                                        IP Audio Hairpinning? y
                                                 Interworking Message: PROGress
                                          DCP/Analog Bearer Capability: 3.1kHz
```

Step	Description
4.	Configure an H.323 trunk group. Use the **add trunk-group** command to create a new trunk group. • **Group Type:** ***isdn*** • **TAC:** ***101*** (User assigned) • **Carrier Medium:** ***H.323*** (Type of trunk) • **Member Assignment Method:** ***auto*** • **Signaling Group:** ***1*** (Signaling group number created in Step 3) • **Number of Members:** ***5*** (Number of members for this trunk group) **add trunk-group 1** **Page 1 of 21** TRUNK GROUP Group Number: 1 **Group Type: isdn** CDR Reports: y Group Name: To Branch COR: 1 TN: 1 **TAC: 101** Direction: two-way Outgoing Display? n **Carrier Medium: H.323** Dial Access? n Busy Threshold: 255 Night Service: Queue Length: 0 **Service Type: tie** Auth Code? n **Member Assignment Method: auto** **Signaling Group: 1** **Number of Members: 5**
5.	Configure the trunk group selection for the signaling group created in Step 3. Use the **change signaling-group** command to configure the signaling group. **change signaling-group 1** **Page 1 of 5** SIGNALING GROUP Group Number: 1 Group Type: h.323 Remote Office? n Max number of NCA TSC: 0 SBS? n Max number of CA TSC: 0 IP Video? n Trunk Group for NCA TSC: **Trunk Group for Channel Selection: 1** Supplementary Service Protocol: a Network Call Transfer? n T303 Timer(sec): 10 Near-end Node Name: procr Far-end Node Name: Location-A Near-end Listen Port: 1720 Far-end Listen Port: 1720 Far-end Network Region: 2 LRQ Required? n Calls Share IP Signaling Connection? n RRQ Required? n Media Encryption? n Bypass If IP Threshold Exceeded? n H.235 Annex H Required? n DTMF over IP: out-of-band Direct IP-IP Audio Connections? y IP Audio Hairpinning? y Interworking Message: PROGress DCP/Analog Bearer Capability: 3.1kHz

Step	Description
6.	Configure the dial plan to route calls to Location-A. Use the **change dialplan analysis** command to configure calls to extension range 4xxxx. The following configures any 5 digit number starting with a 3 as an "aar" Call Type. ARS/AAR Dialing without FAC was enabled in the sample configuration. The "display system-parameters customer-options" command can be used to verify if this option is enabled. **change dialplan analysis** **Page 1 of 12** DIAL PLAN ANALYSIS TABLE Percent Full: 1 Dialed String / Total Length / Call Type 1 / 3 / dac 2 / 5 / ext 221 / 5 / aar **3 / 5 / aar** 4 / 5 / aar 5 / 5 / ext 9 / 3 / fac **display system-parameters customer-options** **Page 3 of 10** OPTIONAL FEATURES Abbreviated Dialing Enhanced List? n — Audible Message Waiting? n Access Security Gateway (ASG)? n — Authorization Codes? n Analog Trunk Incoming Call ID? n — Backup Cluster Automatic Takeover? n A/D Grp/Sys List Dialing Start at 01? n — CAS Branch? n Answer Supervision by Call Classifier? n — CAS Main? n ARS? y — Change COR by FAC? n ARS/AAR Partitioning? y — Computer Telephony Adjunct Links? n **ARS/AAR Dialing without FAC? y** — Cvg Of Calls Redirected Off-net? n ASAI Link Core Capabilities? n — DCS (Basic)? n ASAI Link Plus Capabilities? n — DCS Call Coverage? n Async. Transfer Mode (ATM) PNC? n — DCS with Rerouting? n Async. Transfer Mode (ATM) Trunking? n ATM WAN Spare Processor? n — Digital Loss Plan Modification? n ATMS? n — DS1 MSP? n Attendant Vectoring? n — DS1 Echo Cancellation? n
7.	Configure AAR to use the appropriate route pattern using the **change aar analysis** command. The following shows that when a 5 digit number starting with 3 is dialed, Route Pattern **1** is used. **change aar analysis 3** **Page 1 of 2** AAR DIGIT ANALYSIS TABLE Percent Full: 1 Dialed String / Total Min / Total Max / Route Pattern / Call Type / Node Num / ANI Reqd **3 / 5 / 5 / 1 / aar / n** 5 / 7 / 7 / 999 / aar / n

Step	Description
8.	Configure the route pattern using the **change route-pattern** command. The following screen shows calls using **route-pattern 1** are routed to trunk group **1** configured in Step 4. **change route-pattern 1** **Page 1 of 3** Pattern Number: 1 Pattern Name: SCCAN? n Secure SIP? n Grp FRL NPA Pfx Hop Toll No. Inserted DCS/ IXC No Mrk Lmt List Del Digits QSIG Dgts Intw **1: 1 0** n user 2: n user 3: n user
9.	Configure the IP network region using the **change ip-network-region** command. Note the values for **UDP Port Min**, and **UDP Port Max**. These values are needed to configure the access policy on the BD12k in Section 4.2, Step 4. The IP NETWORK REGION form also specifies which Codec Set that will be used. Intra-Region calls are set to use ip-network region of 1. Inter-Region calls are set to use ip-network-region of 2 codec-set 2. **change ip-network-region 2** **Page 1 of 19** IP NETWORK REGION Region: 2 Location: Authoritative Domain: Name: MEDIA PARAMETERS Intra-region IP-IP Direct Audio: yes **Codec Set: 2** Inter-region IP-IP Direct Audio: yes **UDP Port Min: 2048** IP Audio Hairpinning? y **UDP Port Max: 3029** DIFFSERV/TOS PARAMETERS RTCP Reporting Enabled? y Call Control PHB Value: 34 RTCP MONITOR SERVER PARAMETERS Audio PHB Value: 46 Use Default Server Parameters? y Video PHB Value: 26 802.1P/Q PARAMETERS Call Control 802.1p Priority: 6 Audio 802.1p Priority: 6 Video 802.1p Priority: 5 AUDIO RESOURCE RESERVATION PARAMETERS H.323 IP ENDPOINTS RSVP Enabled? n H.323 Link Bounce Recovery? y Idle Traffic Interval (sec): 20 Keep-Alive Interval (sec): 5 Keep-Alive Count: 5 **change ip-network-region 2** **Page 3 of 19** Inter Network Region Connection Management src dst codec direct Dynamic CAC rgn rgn set WAN WAN-BW-limits Intervening-regions Gateway IGAR 2 1 2 y :NoLimit n 2 2 1 2 3 2 4

Step	Description
10.	Configure the appropriate Audio Codec using the **change ip-codec** command. The following shows ip-codec-set 2 using G.729B. G.711 codec was also verified during compliance testing. **change ip-codec-set 2** **Page 1 of 2** IP Codec Set Codec Set: 2 Audio Codec / Silence Suppression / Frames Per Pkt / Packet Size(ms) **1: G.729B n 2 20** 2: 3: 4: 5: 6: 7: Media Encryption 1: none 2: 3:
11.	Save the configuration using the **save translation** command. **save translation** SAVE TRANSLATION Command Completion Status — Error Code Success — 0
12.	Repeat Steps 1-10 in this section for Avaya Communication Manager in Location-A to complete the configuration. Make sure the appropriate IP address information is entered when configuring Location-A. At Location-A, the "near end" is the Avaya S8300 Media Server and the "far end" is the Media Server at Location-B.

6. Interoperability Compliance Testing

The interoperability compliance testing focused on assessing the ability of the Sentriant CE150 and BlackDiamond 12k configured in a Policy Based Routed Encryption solution to support an Avaya IP Telephony infrastructure consisting of Avaya Communication Manager and Avaya IP Telephones. A data traffic generator was used to simulated traffic for a hypothetical application which would require encryption and compete with Voice over IP (VoIP) traffic for bandwidth.

6.1. General Test Approach

Quality of Service was verified by injecting simulated application traffic into the network using a traffic generator while calls were being established and maintained using Avaya IP Telephones. The BD12k was configured to perform the necessary prioritization to maintain Quality of Service for VoIP traffic. DTMF detection was tested using the Meet-me conference configured in the S8300 Media Server.

The objectives were to verify the Policy Based Routed Encryption solution consisting of the Extreme Networks Sentriant CE150 and BlackDiamond 12k supports the following:

- CE150 encryption interoperates with Avaya VoIP Telephony
- CE150 encryption interoperates with Advanced Encryption Standard (AES) encrypted traffic (configuration not shown in this Application Notes).
- QoS (Quality of Service) for VoIP traffic.
- Basic calling (e.g. call, transfer, conference, DTMF pass-through)

6.2. Test Results

The Policy Based Routed Encryption solution consisting of the Extreme Networks Sentriant CE150 and BlackDiamond 12k successfully achieved objectives. Quality of Service for VoIP traffic was maintained throughout the testing in the presence of competing simulated traffic. VoIP traffic was successfully established and maintained through the CE150 encrypted link.

7. Verification Steps

The following steps may be used to verify the configuration:

- The Local and Remote interfaces do not respond to ICMP request. Therefore, ping command to these two interfaces should not be used as a method to verify network connectivity for the Sentriant CE150.
- Place inter-site calls between the Avaya IP Telephones.
- Use the "show policy" command on the BD12k to verify the content of the access policy is correctly entered.

```
* BD-12804.3 # show policy sentriant
Policies at Policy Server:
Policy: sentriant
entry VoIP-RTP {
if match all {
    source-address 172.28.40.0/24 ;
    destination-address 172.28.20.0/24 ;
    protocol udp ;
    destination-port 2048-3029 ;
}
then {
    qosprofile qp7 ;
    redirect 172.28.40.11 ;
}
}
entry sample-app {
if match all {
    source-address 172.28.40.0/24 ;
    destination-address 172.28.20.0/24 ;
}
```

```
then {
    qosprofile qp2 ;
    redirect 172.28.40.11 ;
}
}
Number of clients bound to policy: 1
Client: acl bound once
```

- Use the “show access-list” command on the BD12k to verify that the access policy is correctly applied.

```
* BD-12804.7 # show access-list
Vlan Name    Port   Policy Name          Dir      Rules  Dyn Rules
=========================================================================
v40          *      sentriant            ingress  2      0
```

- Use the “show port” command on the BD12k to verify that the bandwidth allocation is correctly assigned for the port connected to the CE150 “Local” interface.

```
* BD-12804.4 # show port 2:10 info detail
Port:   2:10
        Virtual-router: VR-Default
        Type:           UTP
        Random Early drop:      Unsupported
        Admin state:    Enabled with  auto-speed sensing  auto-duplex
        Link State:     Active, 1Gbps, full-duplex
        Link Counter: Up        0 time(s)
        VLAN cfg:
                 Name: v40, Internal Tag = 40, MAC-limit = No-limit,
Virtual rou
ter: VR-Default

        STP cfg:

        Protocol:
                 Name: v40          Protocol: ANY      Match all
protocols.
        Trunking:       Load sharing is not enabled.
        EDP:            Enabled
        ELSM:           Disabled
        Learning:       Enabled
        Unicast Flooding:       Enabled
        Multicast Flooding:     Enabled
        Broadcast Flooding:     Enabled
        Jumbo:          Disabled
        QoS Profile:    None configured
        Aggregate Queue:
                QP0  MinBw =          0% MaxBw =        100%  Pri = 8
        Queue:
                QP1  MinBw =          0% MaxBw =        100%  Pri = 1
                QP2  MinBw =          0% MaxBw =         90%  Pri = 2
                QP3  MinBw =          0% MaxBw =        100%  Pri = 3
                QP4  MinBw =          0% MaxBw =        100%  Pri = 4
                QP5  MinBw =          0% MaxBw =        100%  Pri = 5
                QP6  MinBw =          0% MaxBw =        100%  Pri = 6
```

```
                QP7  MinBw =          10% MaxBw =         100%  Pri = 7
                QP8  MinBw =           0% MaxBw =         100%  Pri = 8
        Ingress Rate Shaping :           Unsupported
        Ingress IPTOS Examination:       Disabled
        Egress IPTOS Replacement:        Disabled
        Egress 802.1p Replacement:       Disabled
        NetLogin:                        Disabled
        NetLogin port mode:              Port based VLANs
        Smart redundancy:                Enabled
        Software redundant port:         Disabled
        Preferred medium:                Fiber
```

8. Support

For technical support on the Extreme Networks product, contact Extreme Networks at (800) 998-2408, or refer to http://www.extremenetworks.com

9. Conclusion

These Application Notes have described the administration steps required to configure Policy Based Routed Encryption solution utilizing Extreme Networks Sentriant CE150 and BlackDiamond 12k to support and Avaya H.323 trunk, Avaya VoIP media and a sample application.

10. Additional References

Product documentation for Avaya products may be found at http://support.avaya.com

[1] *Administrator Guide for Avaya Communication Manager*, Doc # 03-300509, Issue 2.1, May 2006
[2] *Avaya Communication Manager Advanced Administration Quick Reference*, Doc # 03-300364, Issue 2, June 2005
[3] *Administration for Network Connectivity for Avaya Communication Manager*, Doc # 555-233-504, Issue 11, February 2006
[4] *Avaya IP Telephony Implementation Guide*, May 1, 2006

Product documentation for Extreme Networks products may be found at http://www.extremenetworks.com

[5] *ExtremeWare XOS Concepts Guid, Software Version 11.4*, Part number 100218-00 Rev. 01, March 2006
[6] *ExtremeWare XOS Command Reference Guide, Software Version 11.4*, Part number 100219-00 Rev. 01, March 2006
[7] *Sentriant CE150*, Part number 100225-00 Rev. 01, June 2006

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Developer*Connection* Program at devconnect@avaya.com.