



IPSec Virtual Private Network (VPN) between an Avaya G350 Media Gateway and Nortel Contivity 1100 Secure IP Services Gateway – Issue 1.0

Abstract

These Application Notes provide a sample configuration with steps to configure a Peer-to-Peer IPSec Virtual Private Network (VPN) tunnel between an Avaya G350 Media Gateway and a Nortel Contivity 1100. The G350 Media Gateway is controlled by Avaya S8700 Media Servers with a G650 Media Gateway. The G350 Media Gateway is equipped with a Local Survivable Processor (LSP) in the event that communication with the Avaya S8700 Media Servers is lost. The sample configuration uses the newer Advanced Encryption Standard with 128-bit key (AES-128) encryption for optimized performance and Perfect Forward Secrecy (PFS) for added protection.

Table of Contents

1. INTRODUCTION.....	3
2. EQUIPMENT AND SOFTWARE VALIDATED.....	6
3. CONFIGURE THE AVAYA G350 MEDIA GATEWAY	6
3.1. G350 Media Gateway VoIP Administration	6
3.2. Basic Switch Administration	8
3.3. Layer 3 Routing Administration	9
3.4. Quality of Service (QoS) Administration Tasks	11
3.5. Virtual Private Network (VPN) Administration Tasks.....	13
4. CONTIVITY 1100 CONFIGURATION.....	19
4.1. Configure the Private LAN Interface from the Console Port.....	19
4.2. Configure the Public LAN Interface from the Web	20
4.3. Enable Branch Office-to-Branch Office VPN Tunnels	22
4.4. Globally Enable Required IPSec Services	22
4.5. Configure Static Routing	23
4.6. Define Protected Networks.....	25
4.7. Create and Configure Branch Office Group	26
4.8. Create and Configure Branch Office VPN Connection.....	29
5. VERIFICATION STEPS	32
5.1. Configuration and Connectivity	32
5.2. IPSec VPN Tunnel Establishment.....	35
5.3. Tunnel Recovery – Deleting Nortel Security Associations	37
5.4. Tunnel Recovery – Deleting G350 Security Associations	37
6. VPN TROUBLESHOOTING TIPS	38
6.1. How to Inspect G350 ISAKMP Security Associations.....	38
6.2. How to Inspect G350 IPSec Security Associations	39
6.3. How to Inspect Contivity Security Associations.....	40
7. CONCLUSION	41
8. ADDITIONAL REFERENCES	41

1. Introduction

These Application Notes describe a peer-to-peer IPSec Virtual Private Network (VPN) between an Avaya G350 Media Gateway and a Nortel Contivity 1100 Secure IP Services Gateway (**Figure 1**). IPSec is used to provide interoperable, cryptographically-based security for IPv4 voice and data traffic flows between designated subnets and/or hosts. It can be used to provide access control, origin authentication, confidentiality and protection from replay attacks for Avaya IP Telephony. A VPN replay attack, also known as “brute force attack” occurs when a hacker attempts to exploit the mathematical rules used to encrypt a message. The hacker tries to test all possible key values that may have been used to secure a message, and then decrypt it if the key is discovered. The sample configuration uses IPSec to secure communications across a Wide Area Network (WAN) between Avaya IP Telephones, IP Softphones, S8700 Media Servers, G650 Media Gateway, and a G350 Media Gateway.

The sample configuration uses the Internet Key Exchange (IKE) protocol to establish an Internet Security Association and Key Management Protocol (ISAKMP) encrypted control channel between peers. ISAKMP is used to add, modify and remove IPSec Security Associations and periodically update encryption keys in a secure manner. IKE establishes an ISAKMP Security Association (SA) by negotiating attributes in a proposal exchange known as Main Mode (Phase 1). An ISAKMP SA can only be established between peers if they both agree to a common set of security attributes in the phase 1 proposal exchange. The following ISAKMP security attributes were administered for use in the sample configuration:

ISAKMP (Phase 1) proposal:

- Encryption Algorithm: 3DES
- Hash Algorithm: SHA
- Diffie-Hellman Group: 2
- Lifetime (seconds): 86400

For detailed information on these attributes including how they are exchanged and used, please see the Additional References section of these Applications Notes where the applicable RFC standards available from the Internet Engineering Task Force (IETF) are listed.

Once an ISAKMP Security Association has been established, the peers can proceed to negotiate IPSec protection for specific traffic flows. IKE does this by establishing IPSec Security Associations (SAs) in a proposal exchange known as Quick Mode (Phase 2). The following IPSec security attributes were administered for use in the sample configuration:

IPSec (Phase 2) proposal:

- Encryption Algorithm: AES-ESP
- Hash Algorithm: HMAC-SHA-ESP
- Security Association Lifetime (seconds): 3600
- Perfect Forward Secrecy: Enabled
- Diffie-Hellman Group: 2

The IP Encapsulating Security Payload (ESP) protocol is used to secure voice and data traffic in the sample configuration, because of the added confidentiality protection provided (i.e. data payload is completely encrypted). The alternative protocol, IP Authentication Header (AH), only provides origin and replay protection. The data payload is not encrypted, making voice packets more vulnerable to potential interception and playback.

The sample configuration also makes use of the Advanced Encryption Standard with a 128-bit key (AES-128) to protect voice and data communications between the two locations. The AES encryption standard was selected because of its higher throughput performance and reduced latency when compared with older encryption standards (e.g. 3DES).

Perfect Forward Secrecy (PFS) was enabled on the VPN in order to strengthen the tunnel against brute force attacks. The PFS feature provides additional security protection by deriving secret keys from a Diffie-Hellman shared secret value. This is advantageous because if one key is compromised on a given tunnel, all previous and subsequent keys will remain secure because they are no longer derived from previous keys.

Dynamic Host Configuration Protocol (DHCP) or static IP addressing may be used to assign networking parameters to Avaya IP Telephones. Static IP addressing was chosen to keep the example simple.

In Communication Manager, each location was assigned to a different IP Network Region using the IP Network Map, interface, and media gateway forms. This allowed granular control of codec selection and Call Admission Control (CAC) over the Wide Area Network (WAN). WAN calls placed between region 1 and 2 were configured to use the G.729A codec. Local Area Network (LAN) calls placed within region 1 or within region 2 were configured to use the G.711MU codec. Static CAC was used to limit the number of calls placed between region 1 and region 2 to a total of two calls. These settings can be customized based on bandwidth constraints and calling requirements.

Always review bandwidth requirements carefully before deploying Virtual Private Networks, especially on asymmetrical connections like cable modems (e.g., uplink 2 Mbps, downlink 128 Kbps). IPSec encrypted voice calls consume more bandwidth than unencrypted calls because of the additional IPSec header length and payload padding required by the ESP protocol. As a result, IPSec may not be the optimal security solution for certain bandwidth limited applications. In these configurations Communication Manager media encryption can be deployed as an alternative to IPSec. The Avaya Media Encryption feature can secure RTP audio streams using AES-128 encryption without increasing the size of the original audio packet. See reference [3].

Detailed Avaya Communication Manager configuration steps such as codec selection between IP network regions, media gateway registration and Call Admission Control (CAC) are described in reference [4].

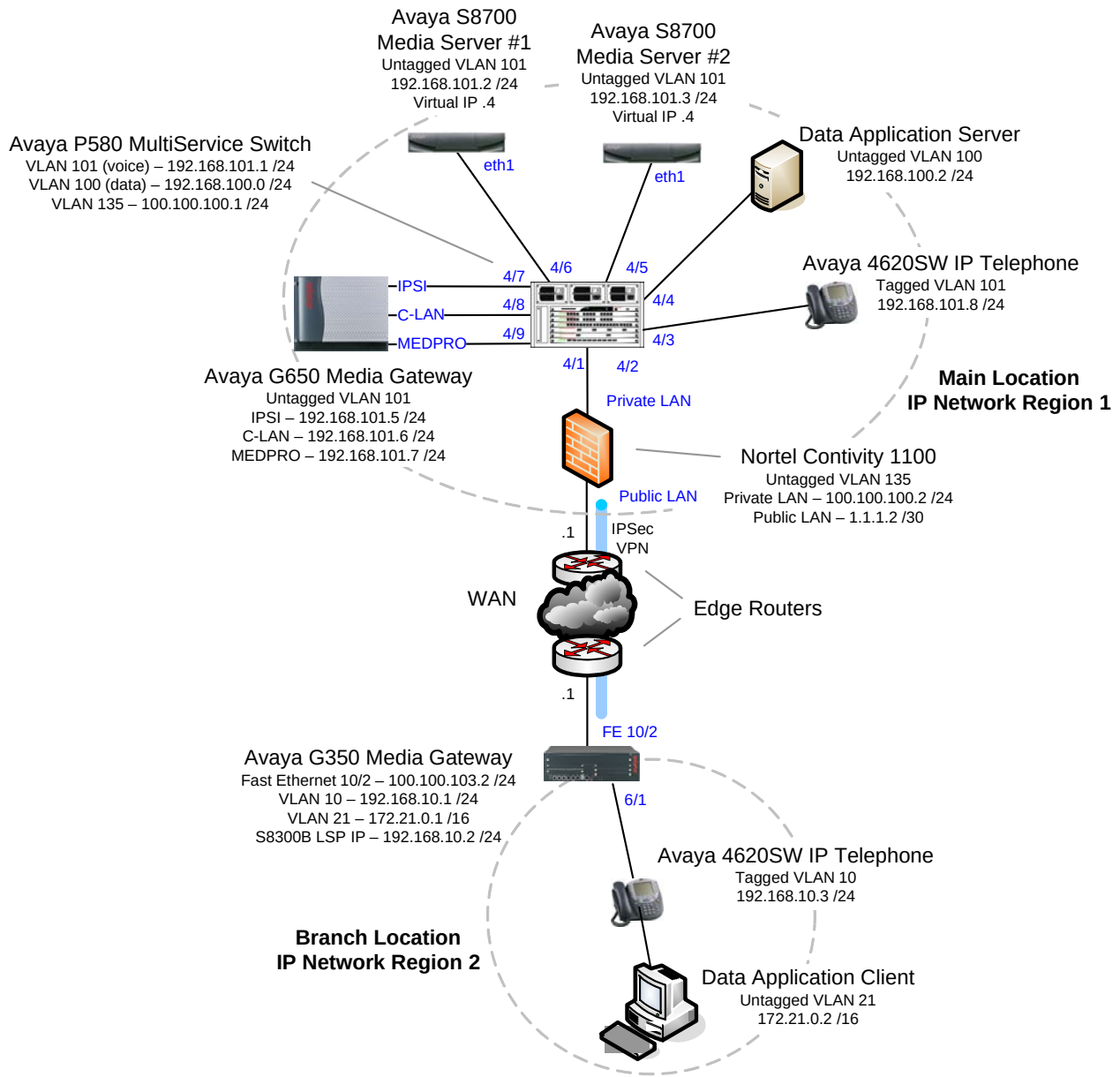


Figure 1: Peer-to-Peer VPN Configuration

2. Equipment and Software Validated

Please reference **Table 1** to review the equipment and software validated for the sample configuration provided:

Equipment	Software
Avaya S8300B Media Server	R012x.01.0.411.7 (R2.1)
Avaya S8700 Media Servers with G650 Media Gateway	R012x.01.0.411.7 (R2.1)
Avaya G350 Media Gateway	23.10.0
Avaya P580 MultiService Switch	v6.0
Avaya 4620SW IP Telephones	R2.0
Avaya IP Softphone	R5.1
Nortel Contivity 1100 Secure IP Services Gateway	V04_80.124

Table 1: Equipment and Software Validated

3. Configure the Avaya G350 Media Gateway

The following steps use the command line interface (CLI) of the Avaya G350 Media Gateway to configure it as shown in **Figure 1**. Several commands are described using their default values for reference purposes. These steps assume a factory default configuration prior to execution. This section illustrates the following configuration tasks:

- G350 Media Gateway Voice over IP (VoIP) Administration
- Basic Switch Administration
- Advanced Layer 3 Routing Administration
- Quality of Service (QoS) Administration
- Virtual Private Network (VPN) Administration

3.1. G350 Media Gateway VoIP Administration

1. Start a terminal session to the Avaya G350 Media Gateway console port.

- ☐ Bits per second **9600**
- ☐ Data bits **8**
- ☐ Parity **None**
- ☐ Stop bits **1**
- ☐ Flow control **None**

2. Log in using a valid login ID and password.
3. Configure separate Virtual LANs for voice and data.

```
G350-???(super)# set vlan 10 name voice10
G350-???(super)# set vlan 21 name data21
```

Note: The question marks will be replaced with a Media Gateway number once the Media Gateway is registered with a Media Gateway Controller (MGC).

4. Configure the Primary Management Interface (PMI) and ICC-VLAN.

The Avaya G350 Media Gateway uses a single IP address for H.248 signaling and voice processing known as the PMI. When the G350 Media Gateway is equipped with an S8300 Media Server, the two are connected through an internal switch. The `icc-vlan` command specifies the VLAN interface used for communication between the S8300 Media Server ICC/LSP and the G350 Media Gateway. The `icc-vlan` interface and S8300 Media Server must reside on the same subnet for proper operation.

```
G350-???(super)# interface vlan 10
G350-???(super-if:Vlan 10)# ip address 192.168.10.1 255.255.255.0
G350-???(super-if:Vlan 10)# pmi
G350-???(super-if:Vlan 10)# icc-vlan
G350-???(super-if:Vlan 10)# exit
```

5. Configure the Media Gateway Controller (MGC) list.

The Avaya G350 Media Gateway maintains a statically provisioned list of controllers. Two IP addresses are configured for the sample configuration. The first IP address 192.168.101.6 is the C-LAN on the Avaya G650 Media Gateway. The second IP address 192.168.10.2 is the Avaya S8300B Media Server LSP. If the G350 fails to register with the C-LAN it will register with its local processor.

```
G350-???(super)# set mgc list 192.168.101.6,192.168.10.2
```

6. Save the running configuration and reset.

```
G350-???(super)# copy run start
G350-???(super)# reset
This command will reset the device
*** Reset the device *** - do you want to continue (Y/N)? y
```

3.2. Basic Switch Administration

1. Configure a port for an Avaya IP Telephone with attached PC.

Important! There are two ways to configure an Avaya G350 Media Gateway switch port to support Avaya IP Telephones.

If security and traffic segmentation are desired, the port attached to the Avaya IP Telephone should be configured as an 802.1Q tagged trunk. Keep in mind that trunk ports cannot support directly attached PCs a majority of the time because most PC Network Interface Cards (NICs) cannot process VLAN tags. When G350 Media Gateways ports are provisioned in this manner egress frames from both the port VLAN and static VLAN will be tagged. An Avaya IP Telephone must reside between a trunk provisioned switch port and PC so it can add and remove VLAN tags on traffic associated with the PC.

```
G350-001(super)# set port vlan 21 6/1
G350-001(super)# set trunk 6/1 dot1q
G350-001(super)# set port vlan-binding-mode 6/1 static
G350-001(super)# set port static-vlan 6/1 10
```

If flexibility to support either a standalone PC or and Avaya IP Telephone with attached PC is more desirable for pre-staging purposes the port can optionally be configured as an untagged access link with a statically bound VLAN. Please be advised that this exposes the voice segment to PCs on the data segment, which may be a security threat.

```
G350-001(super)# set port vlan 21 6/1
G350-001(super)# set trunk 6/1 off
G350-001(super)# set port vlan-binding-mode 6/1 static
G350-001(super)# set port static-vlan 6/1 10
```

2. Configure the data network router interface.

```
G350-001(super)# interface vlan 21
G350-001(super-if:Vlan 21)# ip address 172.21.0.1 255.255.0.0
G350-001(super-if:Vlan 21)# exit
```

3.3. Layer 3 Routing Administration

1. (Optional) Configure an inbound access control list (ACL) to permit trusted traffic only.

Access control lists should be implemented on all public-facing interfaces in order to limit external access into protected subnetworks. The sample configuration will work with or without the inbound ACL in place.

Access list rule descriptions:

- Rule 1 -* Allow ICMP messages to reach the G350 Media Gateway local address for Path MTU Discovery (PMTUD) from any source.
- Rule 2 -* Permit IKE protocol (UDP port 500) message exchanges from any peer to the G350 Media Gateway local address. Administrators may choose to limit IKE from specific peers only.
- Rule 3 -* Permit ESP protocol (IANA protocol 50) traffic from any peer to the G350 Media Gateway local address. Administrators may choose to limit ESP traffic from specific peers only.
- Rule 4 -* Permit any traffic between trusted voice networks (post decryption)
- Rule 5 -* Permit any traffic between trusted data networks (post decryption)
- Rule 6 -* Permit any traffic between trusted voice and data networks for Avaya IP Softphone client connectivity (post decryption). Administrators may choose to limit traffic between the voice and data network segments further by only allowing required protocols and ports.
- Rule Default -* Deny any other traffic flows, which do not match ACL criteria

```
G350-001(super)# ip access-control-list 301
G350-001(super-ACL 301)# name "Permit VPN Traffic Only"
G350-001(super-ACL 301)# ip-rule 1
G350-001(super-ACL 301/ip rule 1)# ip-protocol icmp
G350-001(super-ACL 301/ip rule 1)# source-ip any
G350-001(super-ACL 301/ip rule 1)# destination-ip host 100.100.103.2
G350-001(super-ACL 301/ip rule 1)# exit

G350-001(super-ACL 301)# ip-rule 2
G350-001(super-ACL 301/ip rule 2)# ip-protocol udp
G350-001(super-ACL 301/ip rule 2)# udp destination-port eq ike
G350-001(super-ACL 301/ip rule 2)# source-ip any
G350-001(super-ACL 301/ip rule 2)# destination-ip host 100.100.103.2
G350-001(super-ACL 301/ip rule 2)# exit

G350-001(super-ACL 301)# ip-rule 3
G350-001(super-ACL 301/ip rule 3)# ip-protocol esp
G350-001(super-ACL 301/ip rule 3)# source-ip any
G350-001(super-ACL 301/ip rule 3)# destination-ip host 100.100.103.2
G350-001(super-ACL 301/ip rule 3)# exit
```

```

G350-001(super-ACL 301)# ip-rule 4
G350-001(super-ACL 301/ip rule 4)# source-ip 192.168.101.0 0.0.0.255
G350-001(super-ACL 301/ip rule 4)# destination-ip 192.168.10.0 0.0.0.255
G350-001(super-ACL 301/ip rule 4)# exit

G350-001(super-ACL 301)# ip-rule 5
G350-001(super-ACL 301/ip rule 5)# source-ip 192.168.100.0 0.0.0.255
G350-001(super-ACL 301/ip rule 5)# destination-ip 172.21.0.0 0.0.255.255
G350-001(super-ACL 301/ip rule 5)# exit

G350-001(super-ACL 301)# ip-rule 6
G350-001(super-ACL 301/ip rule 6)# source-ip 192.168.101.0 0.0.0.255
G350-001(super-ACL 301/ip rule 6)# destination-ip 172.21.0.0 0.0.255.255
G350-001(super-ACL 301/ip rule 6)# exit

G350-001(super-ACL 301)# ip-rule default
G350-001(super-ACL 301/ip default)# composite-operation deny
G350-001(super-ACL 301/ip default)# exit
G350-001(super-ACL 301)# exit

```

1. Assign IP Address and ACL to the Fast Ethernet interface.

Assigning an inbound Access Control List (ACL) on the public facing interface is optional.

```

G350-001(super)# interface FastEthernet 10/2
G350-001(super-if:FastEthernet 10/2)# description "Public Interface"
G350-001(super-if:FastEthernet 10/2)# ip address 100.100.103.2 255.255.255.0
G350-001(super-if:FastEthernet 10/2)# ip access-group 301 in
G350-001(super-if:FastEthernet 10/2)# exit

```

2. Configure a default static route destined for the router peer opposite the VPN.

The G350 Media Gateway will fail to establish a VPN with the Nortel Contivity without the necessary routing information. The Media Gateway requires either a default or static route such that its locally protected subnets can forward protected traffic to a peers protected subnets. In this example, the G350 Media Gateway is configured with a default route using the edge routers IP address as the next-hop.

```

G350-001(super)# ip route 0.0.0.0 0.0.0.0 100.100.103.1

```

3.4. Quality of Service (QoS) Administration Tasks

1. Use the default IP Qos-List 400 to classify voice and data traffic on all interfaces.

To review the default qos-list policies enforced by the G350 Media Gateway, use the **show ip qos-list** command. The G350 uses the Trust-DSCP-CoS operation to compare the 802.1P priority (Layer 2) of a frame with the encapsulated DSCP value (Layer 3). Forwarding priority is determined by the greater of the two. The default QoS list classifies DSCP 34 as VoIP Control and DSCP 46 as VoIP Bearer. These traffic classifications receive preferential queuing treatment by the G350 Media Gateway interfaces and they are intentionally consistent with Avaya Communication Manager IP Network Region defaults.

```
G350-001(super)# show ip qos-list 400
```

Index	Name	Owner
400	Default QoS List	other

Pre-classification : trust-cos-dscp

Index	Protocol DSCP	IP	Wildcard	Port	Operation
Deflt	Any Any	Src Any Dst Any		Any Any	Trust-DSCP-CoS

Index	Name	CoS	DSCP	Trust
0	CoS0	0	no-change	No
1	CoS1	1	no-change	No
2	CoS2	2	no-change	No
3	CoS3	3	no-change	No
4	CoS4	4	no-change	No
5	CoS5	5	no-change	No
6	CoS6	6	no-change	No
7	CoS7	7	no-change	No
9	No-Change	no-change	no-change	No
10	Trust-DSCP	-	-	DSCP
11	Trust-DSCP-CoS	-	-	DSCP-and-CoS

DSCP	Action	Name
0	No-Change	DSCP#0
1	No-Change	DSCP#1
2	No-Change	DSCP#2
3	No-Change	DSCP#3
4	No-Change	DSCP#4
5	No-Change	DSCP#5
6	No-Change	DSCP#6
7	No-Change	DSCP#7
8	No-Change	DSCP#8
9	No-Change	DSCP#9
10	No-Change	DSCP#10
11	No-Change	DSCP#11
12	No-Change	DSCP#12
13	No-Change	DSCP#13

14	No-Change	DSCP#14
15	No-Change	DSCP#15
16	No-Change	DSCP#16
17	No-Change	DSCP#17
18	No-Change	DSCP#18
19	No-Change	DSCP#19
20	No-Change	DSCP#20
21	No-Change	DSCP#21
22	No-Change	DSCP#22
23	No-Change	DSCP#23
24	No-Change	DSCP#24
25	No-Change	DSCP#25
26	No-Change	DSCP#26
27	No-Change	DSCP#27
28	No-Change	DSCP#28
29	No-Change	DSCP#29
30	No-Change	DSCP#30
31	No-Change	DSCP#31
32	No-Change	DSCP#32
33	No-Change	DSCP#33
34	CoS7	VoIP Control
35	No-Change	DSCP#35
36	No-Change	DSCP#36
37	No-Change	DSCP#37
38	No-Change	DSCP#38
39	No-Change	DSCP#39
40	No-Change	DSCP#40
41	CoS7	VoIP Control
42	No-Change	DSCP#42
43	CoS6	VoIP Bearer RESV
44	CoS6	VoIP Bearer RESV
45	No-Change	DSCP#45
46	CoS6	VoIP Bearer
47	No-Change	DSCP#47
48	No-Change	DSCP#48
49	No-Change	DSCP#49
50	No-Change	DSCP#50
51	No-Change	DSCP#51
52	No-Change	DSCP#52
53	No-Change	DSCP#53
54	No-Change	DSCP#54
55	No-Change	DSCP#55
56	No-Change	DSCP#56
57	No-Change	DSCP#57
58	No-Change	DSCP#58
59	No-Change	DSCP#59
60	No-Change	DSCP#60
61	No-Change	DSCP#61
62	No-Change	DSCP#62
63	No-Change	DSCP#63

3.5. Virtual Private Network (VPN) Administration Tasks

1. Configure ISAKMP policy (i.e. IKE phase 1 proposal).

```
G350-001(super)# crypto isakmp policy 1
G350-001(super-isakmp:1)# description "P1 Proposal"
G350-001(super-isakmp:1)# encryption 3des
G350-001(super-isakmp:1)# hash sha
G350-001(super-isakmp:1)# group 2
G350-001(super-isakmp:1)# authentication pre-share
G350-001(super-isakmp:1)# lifetime 86400
G350-001(super-isakmp:1)# exit
```

Note: The ISAKMP policy attributes must be configured identically on both peers. The ISAKMP policy sub-commands have been listed below with syntax as a reference.

Description commands:

Syntax: description <desc>
<desc> - string (1-80)

Encryption commands:

Syntax: encryption {3des|des|aes}
Default: des

Hash commands:

Syntax: hash {sha|md5}
Default: md5

Group commands:

Syntax: group {1|2}
Default: 1

Lifetime commands:

Syntax: lifetime <seconds>
<seconds> - lifetime in seconds (60 - 86400)
Default: 86400 (1 Day)

2. Configure the Nortel ISAKMP peer.

```
G350-001(super)# crypto isakmp peer address 1.1.1.2  
G350-001(super-peer:1.1.1.2)# description "Nortel Contivity Peer"  
G350-001(super-peer:1.1.1.2)# isakmp-policy 1  
G350-001(super-peer:1.1.1.2)# pre-shared-key avaya123  
G350-001(super-peer:1.1.1.2)# exit
```

Note: The **isakmp peer address** is the IP address of the remote peer, which the G350 Media Gateway will negotiate with to establish a secure ISAKMP channel. The **crypto isakmp peer address** sub-command syntax has been listed below as a reference.

Description commands:
Syntax: **description <desc>**
<desc> - string (1-80)

Isakmp-policy commands:
Syntax: **isakmp-policy <id>**
<id> - isakmp policy id (1-20)

Pre-shared-key commands:
Syntax: **pre-shared-key <psk-str>**
<psk-str> - pre-shared secret string (1-127)

3. Configure the **transform-set** (i.e. IKE phase 2 proposal).

Transform-sets define security attributes, such as the protocol to employ, the algorithm to be used, etc.

```
G350-001(super)# crypto ipsec transform-set contivity esp-aes esp-sha-hmac
G350-001(super-transform:contivity)# set security-association lifetime seconds 3600
G350-001(super-transform:contivity)# set pfs group2
G350-001(super-transform:contivity)# exit
```

Note: The following command and sub-command syntax applies to IPSec transform-sets.

Crypto ipsec transform-set commands:

Syntax: crypto ipsec transform-set <name> {{esp-des|esp-3des|esp-aes}
[{{esp-md5-hmac|esp-sha-hmac}}]|esp-null {{esp-md5-hmac|esp-sha-hmac}}}
<name> - transform-set name without spaces (1-32)

Set security-association lifetime seconds commands:

Syntax: set security-association lifetime seconds <seconds>
<seconds> - lifetime in seconds (120 - 86400)
Default: 3600 (1 Hour)

Set security-association lifetime kilobytes commands:

Syntax: set security-association lifetime kilobytes <kilobytes>
<kilobytes> - lifetime in kilobytes (2560 - 536870912)
Default: 4608000

Set pfs commands:

Syntax: set pfs [group1 | group2]
Default: no pfs

4. Configure the **crypto map**.

Crypto maps define the peers to negotiate IPsec (IKE phase 2) protection with and the transform-sets to secure the traffic flows.

```
G350-001(super)# crypto map 1
G350-001(super-crypto:1)# description "P2 with Nortel"
G350-001(super-crypto:1)# set transform-set contivity
G350-001(super-crypto:1)# set peer 1.1.1.2
G350-001(super-crypto:1)# exit
```

Note: The following command and sub-command syntax applies to crypto maps.

Crypto map commands:

Syntax: crypto map <id>
<id> - integer(1-50)

Description commands:

Syntax: description <desc>
<desc> - string (1-80)

Set transform-set commands:

Syntax : set transform-set <name>

Set peer commands:

Syntax : set peer <peer address>
<peer address> - remote peer address

5. Configure a **crypto-list**.

Crypto-lists contain **ip-rules**, which select traffic flows requiring IPSec protection according to source and destination IP addressing.

```
G350-001(super)# ip crypto-list 901
G350-001(super-Crypto 901)# name "Protect This Traffic"
G350-001(super-Crypto 901)# local-address 100.100.103.2
G350-001(super-Crypto 901)# ip-rule 1
G350-001(super-Crypto 901/ip rule 1)# protect crypto map 1
G350-001(super-Crypto 901/ip rule 1)# source-ip 192.168.10.0 0.0.0.255
G350-001(super-Crypto 901/ip rule 1)# destination-ip 192.168.101.0 0.0.0.255
G350-001(super-Crypto 901/ip rule 1)# exit
G350-001(super-Crypto 901)# ip-rule 2
G350-001(super-Crypto 901/ip rule 2)# protect crypto map 1
G350-001(super-Crypto 901/ip rule 2)# source-ip 172.21.0.0 0.0.255.255
G350-001(super-Crypto 901/ip rule 2)# destination-ip 192.168.100.0 0.0.0.255
G350-001(super-Crypto 901/ip rule 2)# exit
G350-001(super-Crypto 901)# ip-rule 3
G350-001(super-Crypto 901/ip rule 3)# protect crypto map 1
G350-001(super-Crypto 901/ip rule 3)# source-ip 172.21.0.0 0.0.255.255
G350-001(super-Crypto 901/ip rule 3)# destination-ip 192.168.101.0 0.0.0.255
G350-001(super-Crypto 901/ip rule 3)# exit
G350-001(super-Crypto 901)# exit
```

Note: The following command and sub-command syntax applies to crypto-lists.

Ip crypto-list commands:

Syntax : ip crypto-list <index>
<index> - integer (901..999)

Name commands:

Syntax : name <name>
<name> - list name

Local address commands:

Syntax : local-address <ip-address>
<ip-address> - an IP address that belongs to a local IP interface

Ip-rule commands:

Syntax : ip-rule {<index> | default}
<index> - integer (1..9999)

Protect crypto commands:

protect crypto map Protect traffic that matches this rule, by applying the IPSec processing configured by the specified crypto map.

Source-ip commands:

Syntax :source-ip {host <ip-address> | any | <ip-address> <wildcard>}
<ip-address> - ip network
<wildcard> - ip network wildcard

Destination-ip commands:

Syntax :destination-ip {host <ip-address> | any | <ip-address> <wildcard>}
<ip-address> - ip network
<wildcard> - ip network wildcard

6. Assign **crypto-group** to Fast Ethernet interface and save running configuration.

Crypto-groups enable IPsec processing on a router interface by binding a **crypto-list** to it. Administrators may only bind one **crypto-list** to an interface at a time. Once IPsec is enabled, the Security Policy Database (SPD) is consulted by the interface during the processing of all inbound and outbound traffic, including non-IPsec traffic.

The G350 Media Gateway Security Policy Database (SPD) includes the **crypto-lists**, **ip-rules**, **crypto maps** and **transform-sets**. The **crypto-list** contains **ip-rules**, which select traffic flows requiring IPsec protection based on source and destination IP addressing. Each **ip-rule** is protected by a **crypto map**. The **crypto map** defines the peer to negotiate IPsec (phase 2) protection with and the **transform-set** to secure the traffic flow. The **transform-set** defines security attributes, such as the protocol to employ (e.g. AH or ESP), and the algorithm to be used (e.g. DES, 3DES, AES).

```
G350-001(super)# interface FastEthernet 10/2
G350-001(super-if:FastEthernet 10/2)# ip crypto-group 901
G350-001(super-if:FastEthernet 10/2)# exit
G350-001(super)# copy run start
```

Note: The following sub-command syntax applies to interfaces.

Ip crypto-group commands:

Syntax : ip crypto-group <crypto-list-id>
<crypto-list-id> - integer (900..999, 900 - default crypto list)

4. Contivity 1100 Configuration

The following section describes the steps necessary to configure the Nortel Contivity 1100 for Virtual Private Networking (VPN) as shown in **Figure 1**. These steps assume a factory-default system configuration.

4.1. Configure the Private LAN Interface from the Console Port

1. Log into the console port using a valid username and password.
2. Configure the Contivity private LAN interface addressing from the console.

Main Menu: System is currently in NORMAL mode.

- 1) Interfaces
- 2) Administrator
- 3) Default Private Route Menu
- 4) Default Public Route Menu
- 5) Create A User Control Tunnel(IPsec) Profile
- 6) Restricted Management Mode FALSE
- 7) Allow HTTP Management TRUE
- 8) Firewall Options
- 9) Shutdown
- B) System Boot Options
- P) Configure Serial Port
- C) Controlled Crash
- L) Command Line Interface
- R) Reset System to Factory Defaults
- E) Exit, Save and Invoke Changes

Please select a menu choice: **1**

(Select 1 to enter the Interface Menu from the Main Menu)

Please select a menu choice: **0**

(Select 0 to modify Private LAN interface addressing)

New Management IP Address* = **100.100.100.254**

(Enter the Private LAN interface management IP address)

New Interface IP Address* = **100.100.100.2**

(Enter the Private LAN interface IP address)

New Subnet Mask = **255.255.255.0**

(Enter the Private LAN interface subnet mask)

3. Return to the Main Menu and save the changes.

Please select a menu choice: **R**

(Select R to return to the Main Menu)

Please select a menu choice (1 - 9,B,P,C,L,R,E): **E**

(Select E to save the changes)

4.2. Configure the Pubic LAN Interface from the Web

1. Web browse to the private LAN interface management IP address from a PC located on the Private LAN (e.g. <http://100.100.100.254>).
2. Click **MANAGE SWITCH** and authenticate the session using a valid username and password.

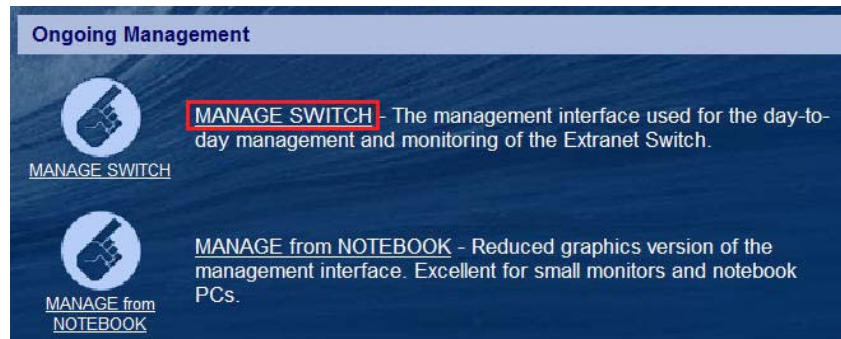


Figure 2: Welcome to Contivity Switch page

3. Navigate to **SYSTEM → LAN** and click **Cancel acquisition**.

Note: The Contivity 1100 Extranet Switch attempts to retrieve its Public LAN interface IP address via Dynamic Host Configuration Protocol (DHCP) by default. In order to configure a site-to-site VPN tunnel the interface must be statically administered.

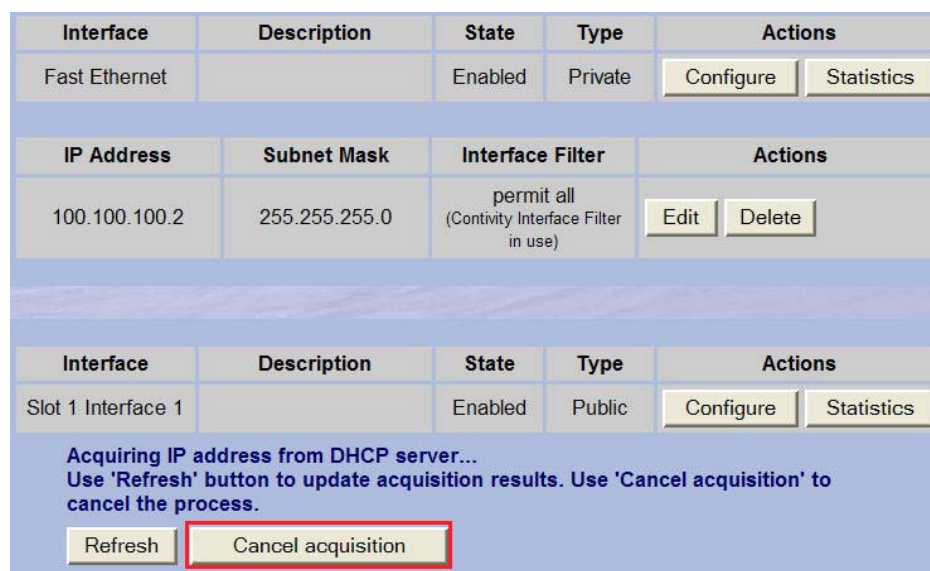


Figure 3: LAN Interface page

4. Click **Apply** next to the **Select Protocol** drop-down menu after the page refreshes.

Interface	Description	State	Type	Actions	
Slot 1 Interface 1		Enabled	Public	Configure	Statistics

Select Protocol	IP	Apply
-----------------	----	-------

Figure 4: LAN Interface page

5. Enter a unique static IP address (e.g. **1.1.1.2**) and subnet mask (e.g. **255.255.255.0**) required for the Public LAN interface, and then click **OK**.

Obtaining IP Address	☒ Static
	IP Address 1.1.1.2
	Subnet Mask 255.255.255.0
	☐ DHCP
	Cost 10
	Host Name (optional)
Interface Filter	deny all (Default Filter) (Contivity Interface Filter in use) New Interface Filter
OK Cancel	

Figure 5: LAN Interface → Add IP Address page

4.3. Enable Branch Office-to-Branch Office VPN Tunnels

1. Navigate to **SYSTEM → FORWARDING**, check **Allow Branch Office to Branch Office** under the **Tunnel to Tunnel Traffic** category, and then click **OK**.



Tunnel to Tunnel Traffic

☐ Allow End User to End User

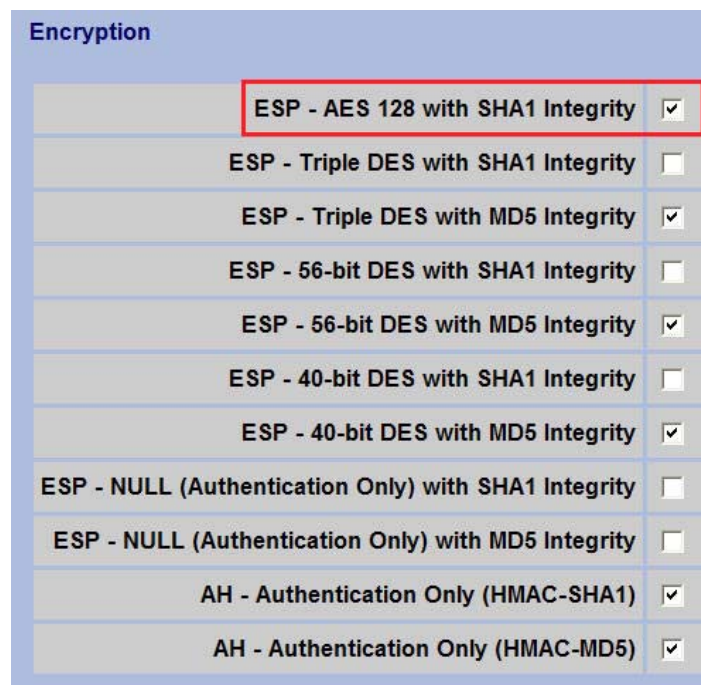
☐ Allow End User to Branch Office

☒ Allow Branch Office to Branch Office

Figure 6: Forwarding page

4.4. Globally Enable Required IPSec Services

1. Navigate to **SERVICES → IPSEC**, check **ESP - AES 128 with SHA1 Integrity** under the **Encryption** category.

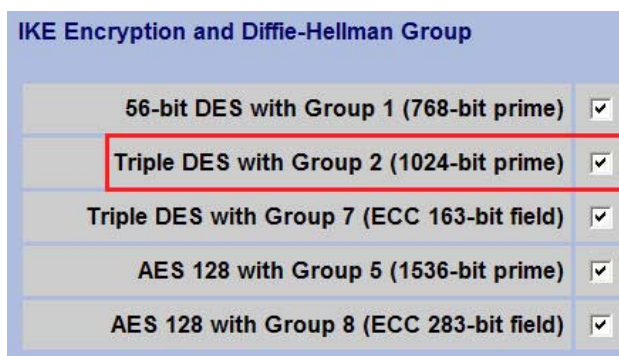


Encryption

ESP - AES 128 with SHA1 Integrity	☒
ESP - Triple DES with SHA1 Integrity	☐
ESP - Triple DES with MD5 Integrity	☒
ESP - 56-bit DES with SHA1 Integrity	☐
ESP - 56-bit DES with MD5 Integrity	☒
ESP - 40-bit DES with SHA1 Integrity	☐
ESP - 40-bit DES with MD5 Integrity	☒
ESP - NULL (Authentication Only) with SHA1 Integrity	☐
ESP - NULL (Authentication Only) with MD5 Integrity	☐
AH - Authentication Only (HMAC-SHA1)	☒
AH - Authentication Only (HMAC-MD5)	☒

Figure 7: IPsec Settings page

2. Scroll down to the **IKE Encryption and Diffie-Hellman Group** category and check **Triple DES with Group 2 (1024-bit prime)** then go to the bottom of the page and click **OK**.

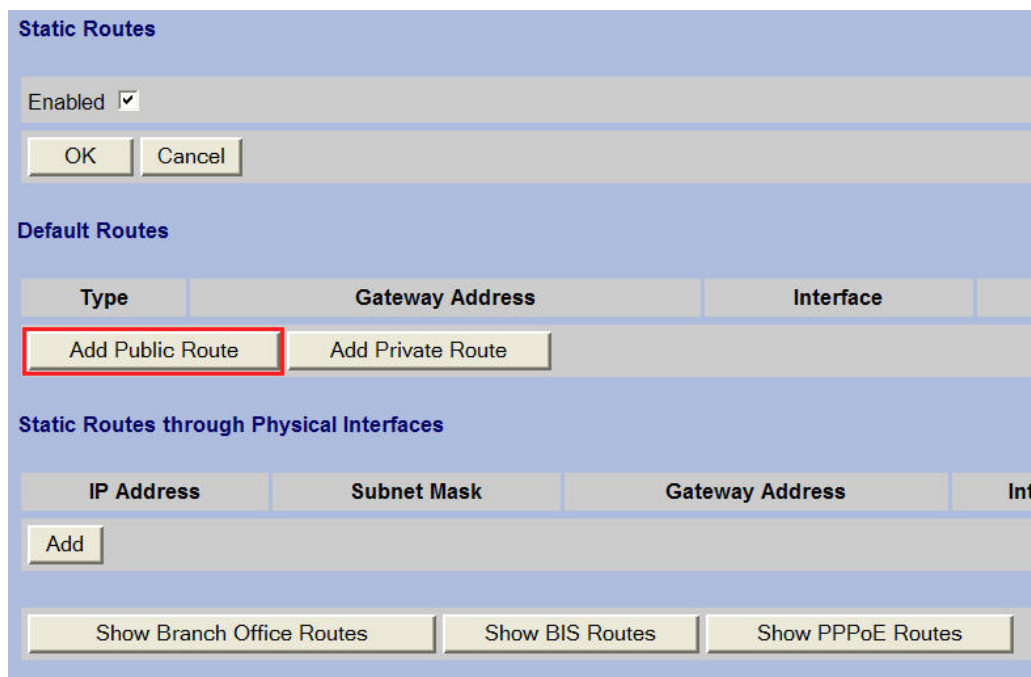


IKE Encryption and Diffie-Hellman Group	
56-bit DES with Group 1 (768-bit prime)	☒
Triple DES with Group 2 (1024-bit prime)	☒
Triple DES with Group 7 (ECC 163-bit field)	☒
AES 128 with Group 5 (1536-bit prime)	☒
AES 128 with Group 8 (ECC 283-bit field)	☒

Figure 8: IPsec Settings page

4.5. Configure Static Routing

1. Create a default route on the public LAN interface. Navigate to **ROUTING → STATIC ROUTES** and click **Add Public Route** under the **Default Routes** category.



Static Routes

Enabled ☒

OK Cancel

Default Routes

Type	Gateway Address	Interface
Add Public Route	Add Private Route	

Static Routes through Physical Interfaces

IP Address	Subnet Mask	Gateway Address	Int
Add			

Show Branch Office Routes Show BIS Routes Show PPPoE Routes

Figure 9: Static Routes page

2. Enter the necessary cost (e.g. **1**) and next hop gateway address (e.g. **1.1.1.1**) information then click **OK**.

Public Default Route

Admin State	Enable
Cost	1
Gateway Address	1.1.1.1

OK Cancel

Figure 10: Static Routes → Add Public Default Route page

3. Create static routes to all protected networks located on the private side of the Contivity. Click **Add** beneath the **Static Routes through Physical Interfaces** category.

Static Routes through Physical Interfaces

IP Address	Subnet Mask
Add	

Figure 11: Static Routes page

4. Enter the necessary cost (e.g. **1**), network (e.g. **192.168.101.0**), subnet mask (e.g. **255.255.255.0**) and gateway address (e.g. **100.100.100.1**) and then click **OK**. Repeat steps 3 and 4 until static routes for all protected networks have been defined.

Static Route

Admin State	Enable
Cost	1
Network Address	192.168.101.0
Subnet Mask	255.255.255.0
Gateway Address	100.100.100.1

OK Cancel

Figure 12: Static Route → Add Static Route page

4.6. Define Protected Networks

1. Create a network profile, which defines all networks that will be protected by the Contivity VPN. Navigate to **PROFILES → NETWORKS** and enter a unique network profile name (e.g. **PrivateNetworks**) then click **Create**.

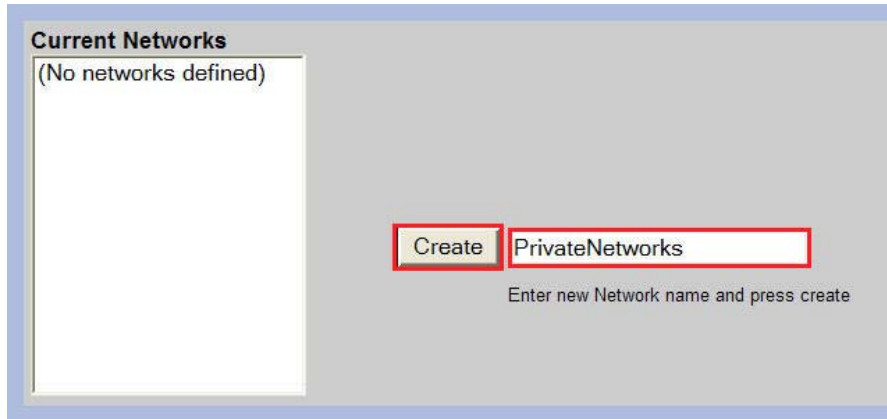


Figure 13: Networks page

2. Enter the IP address and mask for a protected subnet (e.g. **192.168.100.0**, **255.255.255.0**) and then click **Add**. Repeat this step until all protected networks have been added to the network profile and then click **Close** at the bottom of the page.

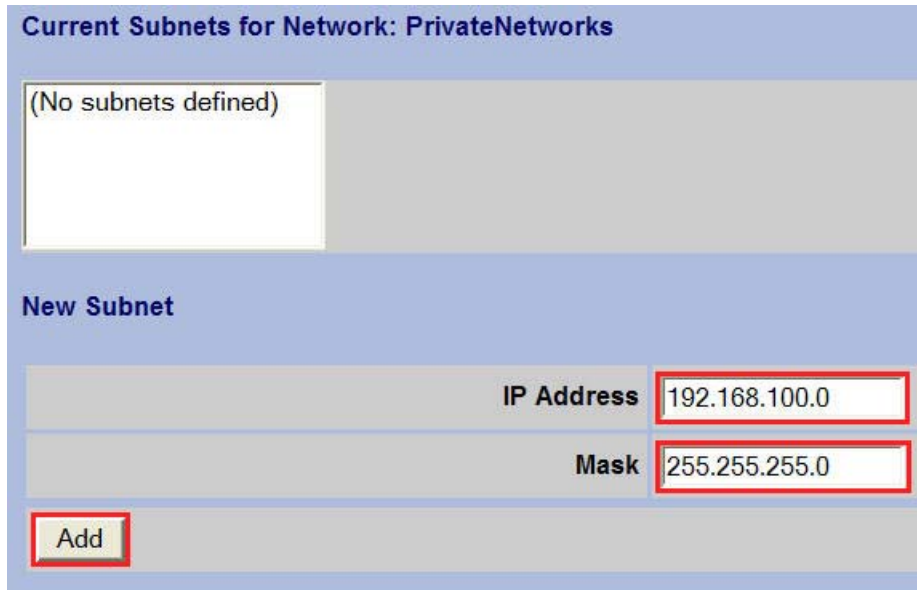
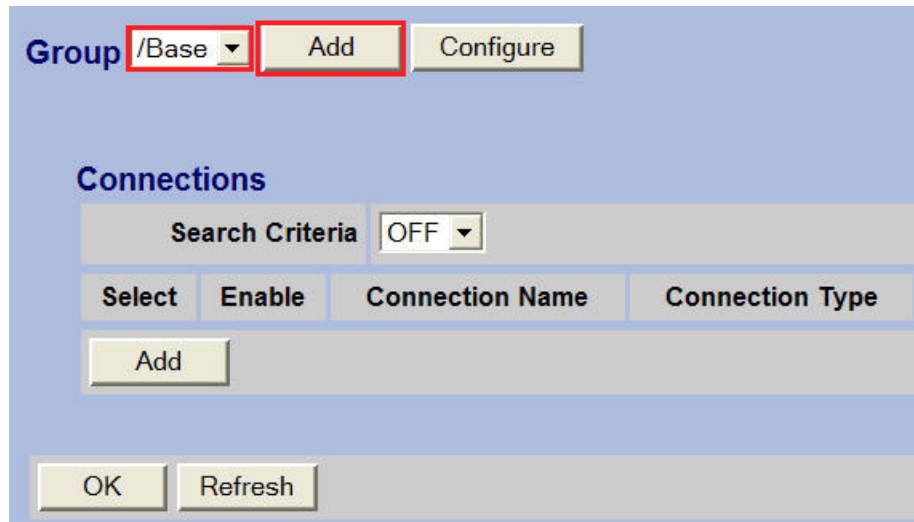


Figure 14: Current Subnets for Network: PrivateNetworks page

4.7. Create and Configure Branch Office Group

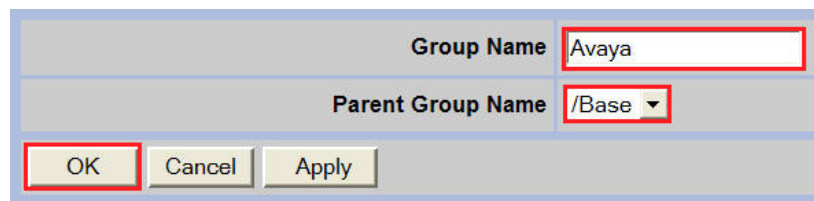
1. Add a new Branch Office group to customize security parameters for multiple connections. Navigate to **PROFILES → BRANCH OFFICE**, select **/Base** in the Group drop-down menu and click **Add** in the “Group” category.



The screenshot shows a web interface for managing Branch Office groups. At the top, there is a 'Group' section with a dropdown menu set to '/Base', an 'Add' button, and a 'Configure' button. Below this is a 'Connections' section with a 'Search Criteria' dropdown set to 'OFF'. Underneath, there is a table with columns 'Select', 'Enable', 'Connection Name', and 'Connection Type'. An 'Add' button is located below the table. At the bottom of the interface, there are 'OK' and 'Refresh' buttons.

Figure 15: Branch Office page

2. Define a new Branch Office group to control all connections to Avaya VPN devices. Enter a unique group name (e.g. **Avaya**) using the parent group **/Base** and then click **OK**.



The screenshot shows a dialog box for adding a new group. It has two input fields: 'Group Name' with the text 'Avaya' and 'Parent Group Name' with a dropdown menu set to '/Base'. At the bottom, there are three buttons: 'OK', 'Cancel', and 'Apply'.

Figure 16: Add Group page

- Configure security parameters for connections to Avaya VPN devices. Select **/Base/Avaya** and click **Configure** in the **Group** category.

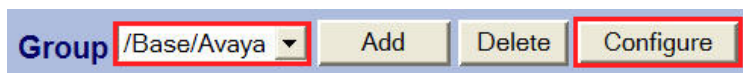


Figure 17: Branch Office page

- Configure IPSec parameters. Scroll down to the **IPSec** category and click **Configure**.

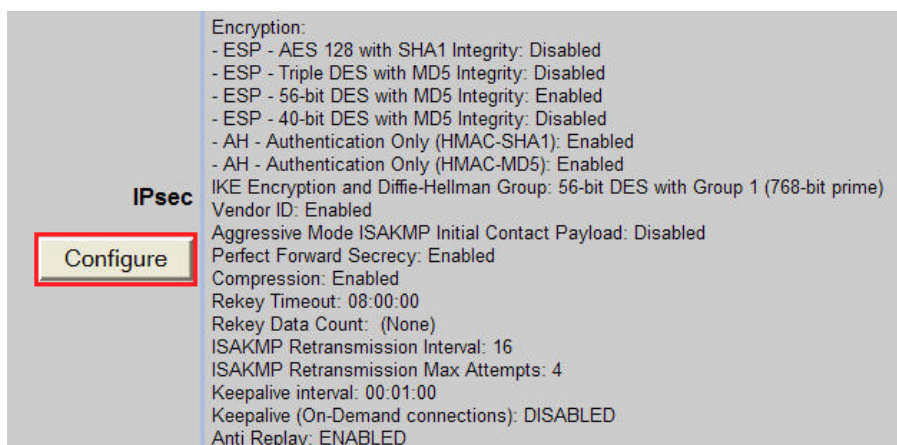


Figure 18: Branch Office → Edit Group page

- Choose to configure select parameters. Click **Configure** next to **Encryption**, **IKE Encryption** and **Diffie-Hellman Group**, **Compression**, and **Rekey Timeout**. All other parameter defaults should remain unchanged.

Field	Value	Actions
Encryption	ESP - AES 128 with SHA1 Integrity Disabled	Configure
	ESP - Triple DES with MD5 Integrity Disabled	
	ESP - 56-bit DES with MD5 Integrity Enabled	
	ESP - 40-bit DES with MD5 Integrity Disabled	
	AH - Authentication Only (HMAC-SHA1) Enabled	
	AH - Authentication Only (HMAC-MD5) Enabled	
IKE Encryption and Diffie-Hellman Group	56-bit DES with Group 1 (768-bit prime)	Configure
Vendor ID	Enabled	Configure
Aggressive Mode ISAKMP Initial Contact Payload	Disabled	Configure
Perfect Forward Secrecy	Enabled	Configure
Compression	Enabled	Configure
Rekey Timeout	08:00:00	Configure

Figure 19: Branch Office → Edit /Base/Avaya Group page

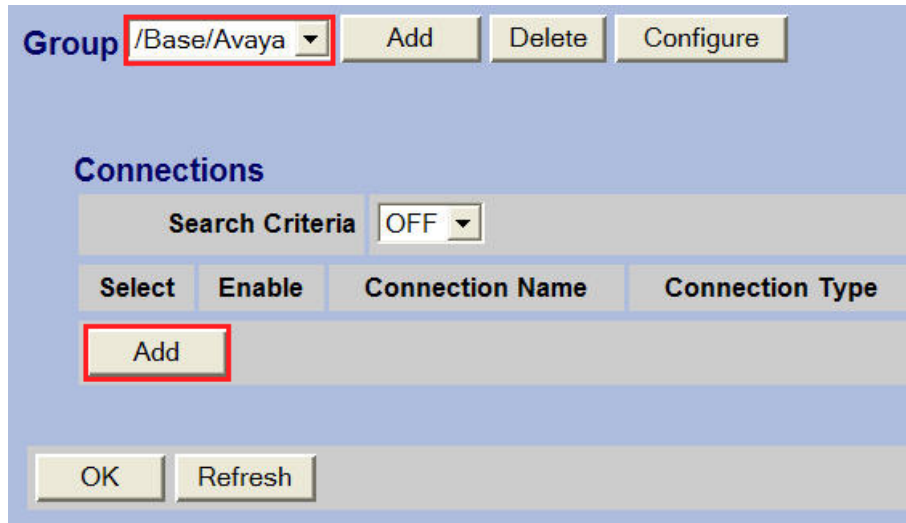
- Configure selected parameters. Enable **ESP – AES 128 with SHA1 Integrity** in the **Encryption** category, select **Triple DES with Group 2 (1024-bit prime)** from the **IKE Encryption and Diffie-Hellman Group** category drop-down menu, select **Disabled** from the **Compression** category drop-down menu, enter **01:00:00** in the **Rekey Timeout** category field, and then scroll down to the bottom of the page and click **OK**.

Group Name: /Base/Avaya	
Field	Value
Encryption	ESP - AES 128 with SHA1 Integrity ☒
	ESP - Triple DES with MD5 Integrity ☐
	ESP - 56-bit DES with MD5 Integrity ☒
	ESP - 40-bit DES with MD5 Integrity ☐
	AH - Authentication Only (HMAC-SHA1) ☒
	AH - Authentication Only (HMAC-MD5) ☒
IKE Encryption and Diffie-Hellman Group	Triple DES with Group 2 (1024-bit prime) ▼
Vendor ID	Enabled
Aggressive Mode ISAKMP Initial Contact Payload	Disabled
Perfect Forward Secrecy	Enabled
Compression	Disabled ▼
Rekey Timeout	01:00:00

Figure 20: Branch Office → Edit /Base/Avaya Group page

4.8. Create and Configure Branch Office VPN Connection

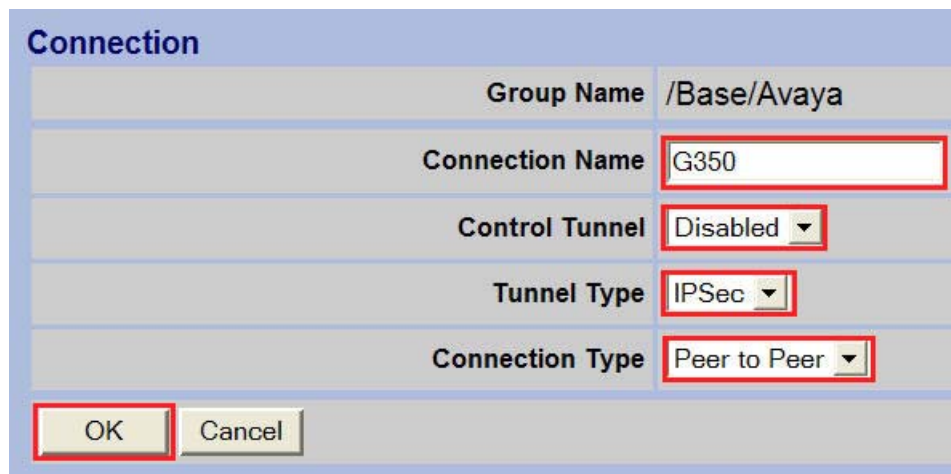
1. Create a new VPN connection to the G350 Media Gateway. Navigate to **PROFILES** → **BRANCH OFFICE**, select **/Base/Avaya** in the **Group** category drop-down menu and then click **Add** under the **Connections** category.



The screenshot shows a web interface for managing VPN connections. At the top, there is a 'Group' dropdown menu with '/Base/Avaya' selected, and buttons for 'Add', 'Delete', and 'Configure'. Below this is a 'Connections' section with a 'Search Criteria' dropdown set to 'OFF'. A table with columns 'Select', 'Enable', 'Connection Name', and 'Connection Type' is visible. An 'Add' button is highlighted with a red box. At the bottom are 'OK' and 'Refresh' buttons.

Figure 21: Branch Office page

2. Configure a new connection to the G350 Media Gateway. Enter a unique name (e.g. **G350**) in the **Connection Name** field, select **Disabled** in the **Control Tunnel** drop-down, select **IPSec** in the **Tunnel Type** drop-down, select **Peer to Peer** in the **Connection Type** drop-down and then click **OK**.



The screenshot shows the 'Add Connection' dialog box. It contains the following fields and values: 'Group Name' is '/Base/Avaya'; 'Connection Name' is 'G350'; 'Control Tunnel' is 'Disabled'; 'Tunnel Type' is 'IPSec'; and 'Connection Type' is 'Peer to Peer'. The 'OK' button is highlighted with a red box. At the bottom are 'OK' and 'Cancel' buttons.

Figure 22: Add Connection page

3. The **Connection Configuration** page appears. Scroll down to the **Connection** category and **Enable** the new connection.

Connection	
Group Name	/Base/Avaya
Connection Name	G350
Control Tunnel	Disabled
Tunnel Type	IPSec
Connection Type	Peer to Peer
Enable	☒

Figure 23: Connection Configuration page

4. Scroll down to the **Endpoints** context. Select the Public LAN interface address (e.g. **1.1.1.2**) from the **Local IP Address** drop-down. Enter the G350 Media Gateway public address (e.g. **100.100.103.2**) in the **Remote IP Address** field.

Endpoints	
Local Ip Address	1.1.1.2
Remote Ip Address	100.100.103.2

Figure 24: Connection Configuration page

5. Scroll down to the **Authentication** category. Select **Text Pre-Shared Key** from the drop-down menu. Enter the same unique secret configured on the G350 Media Gateway (e.g. **avaya123**) in the **Text Pre-Shared Key** and **Confirm** fields.

Authentication	
Text Pre-Shared Key	
Text Pre-Shared Key	Confirm

Figure 25: Connection Configuration page

6. Scroll down to the **Local Networks** context. Select the previously defined network profile (e.g. **PrivateNetworks**) from the drop-down menu.



The screenshot shows a section titled "Local Networks". Below the title is a label "Local Network" followed by a dropdown menu. The dropdown menu is open, and "PrivateNetworks" is selected and highlighted. The entire dropdown menu area is enclosed in a red rectangular box.

Figure 26: Connection Configuration page

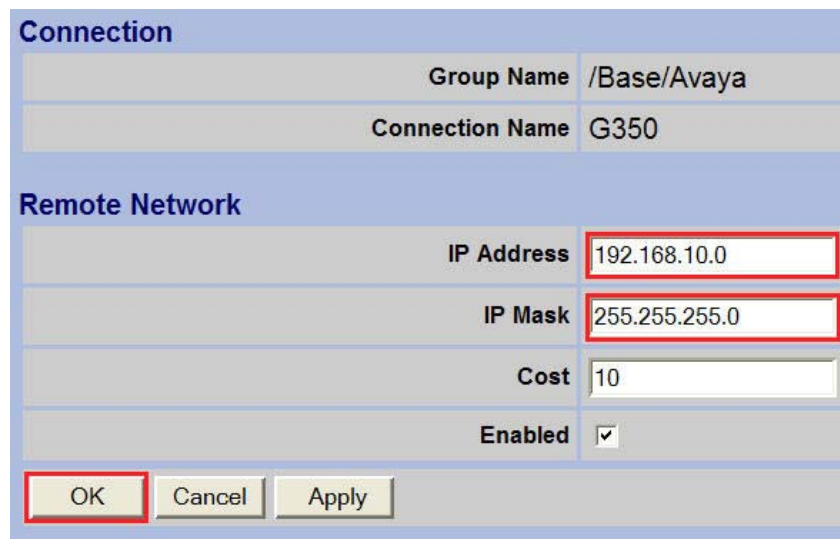
7. Scroll down to the **Remote Networks** context and click **Add**.



The screenshot shows a section titled "Remote Networks". Below the title is a table with two columns: "Select" and "IP Address". In the "Select" column, there is a button labeled "Add". This button is enclosed in a red rectangular box.

Figure 27: Connection Configuration page

8. The **Add Remote Network** page appears. Enter an IP address, mask for a subnetwork protected by the G350 Media Gateway (e.g. **192.168.10.0**, **255.255.255.0**) and click **OK**. Repeat steps 7 and 8 for all G350 protected networks. When all networks have been defined, scroll to the bottom of the **Connection Configuration** page and click **OK**.



The screenshot shows a dialog box titled "Connection". It contains two sections: "Connection" and "Remote Network".
In the "Connection" section, there are two fields: "Group Name" with the value "/Base/Avaya" and "Connection Name" with the value "G350".
In the "Remote Network" section, there are four fields: "IP Address" with the value "192.168.10.0", "IP Mask" with the value "255.255.255.0", "Cost" with the value "10", and "Enabled" with a checked checkbox. The "IP Address" and "IP Mask" fields are enclosed in red rectangular boxes.
At the bottom of the dialog box, there are three buttons: "OK", "Cancel", and "Apply". The "OK" button is enclosed in a red rectangular box.

Figure 28: Connection Configuration page

9. The **Connection Configuration** page should match **Figure 29** if everything was configured properly.

The screenshot shows a web interface for configuring a Branch Office. At the top, there is a 'Group' dropdown set to '/Base/Avaya' and three buttons: 'Add', 'Delete', and 'Configure'. Below this is a section titled 'Connections'. It features a 'Search Criteria' dropdown set to 'OFF'. A table lists the connections:

Select	Enable	Connection Name	Connection Type	Tunnel Type	Local Ip Address	Remote Ip Address	Control Tunnel
☐	☒	G350	Peer to Peer	IPSec	1.1.1.2	100.100.103.2	Disabled

Below the table are buttons for 'Add', 'Delete', 'Configure', 'Change Group', and 'Test'. At the bottom of the interface are 'OK' and 'Refresh' buttons.

Figure 29: Branch Office page

5. Verification Steps

Verify the configuration using a two-step approach. First, check configuration and connectivity and then establish a VPN between the peers and verify SA establishment. Verify tunnel initiation in both directions. Manually clear ISAKMP and IPSec security associations with active sessions and verify VPN recovery.

5.1. Configuration and Connectivity

Make sure that security attributes are correctly administered on the G350 Media Gateway and use ping to test connectivity.

5.1.1. Verify ISAKMP Policy (Phase 1 Proposal)

```
G350-001(super)# show crypto isakmp policy
```

Showing 1 rows

Id	Description	Encr	Hash	Authentication	DH group	life sec
1	P1 Proposal	3des	sha	Preshared key	2	86400

5.1.2. Verify ISKAMP Peer

```
G350-001(super)# show crypto isakmp peer
```

Showing 1 rows

Description	Peer identity	Auth	Plc
Nortel Contivity Peer	1.1.1.2	psk	1

5.1.3. Verify IPSec Transform-Set

```
G350-001(super)# show crypto ipsec transform-set contivity
```

Showing 1 rows

Name	ESP enc	ESP hash	PFS	Life Sec	Life KB	Mode
contivity	aes	sha-hmac	#2	3600	4608000	Tunnel

5.1.4. Verify Crypto Map

```
G350-001(super)# show crypto map 1
```

Showing 1 rows

Id	Description	Remote peer	Transform-set	DSCP
1	P2 with Nortel	1.1.1.2	contivity	copy

5.1.5. Verify Crypto List

Use the **show ip crypto-list 901 detail** command to verify the traffic flows, which are to be encrypted using the crypto map binding and associated transform-set.

```
G350-001(super)# show ip crypto-list 901 detail
```

Index	Description	Status	Owner
901	Encrypt This Traffic	valid	other

Local address: 100.100.103.2

Rules:

Index	Protocol	IP	Wildcard	Action	Crypto map
1	Any	Src 192.168.10.0 Dst 192.168.101.0	0.0.0.255 0.0.0.255	protect 1	} Defines traffic to be encrypted
2	Any	Src 172.21.0.0 Dst 192.168.100.0	0.0.255.255 0.0.0.255	protect 1	
3	Any	Src 172.21.0.0 Dst 192.168.100.0	0.0.255.255 0.0.0.255	protect 1	
Deflt	Any	Src Any Dst Any		bypass -	

Applicable crypto maps:

Id	Description	Remote peer	Transform-set	DSCP
1	P2 with Nortel	1.1.1.2	contivity	copy

Defines IPSec
encryption strength

5.1.6. Verify Private Static Routes to Contivity Protected Networks

Ping the private network router interfaces from the Contivity command line.

Main Menu: System is currently in NORMAL mode.

- 1) Interfaces
- 2) Administrator
- 3) Default Private Route Menu
- 4) Default Public Route Menu
- 5) Create A User Control Tunnel(IPsec) Profile
- 6) Restricted Management Mode FALSE
- 7) Allow HTTP Management TRUE
- 8) Firewall Options
- 9) Shutdown
- B) System Boot Options
- P) Configure Serial Port
- C) Controlled Crash
- L) Command Line Interface
- R) Reset System to Factory Defaults
- E) Exit, Save and Invoke Changes

Please select a menu choice (1 - 9,B,P,C,L,R,E): L

CES>ping 192.168.100.1

```
PING 192.168.100.1: 36 data bytes
64 bytes from 192.168.100.1: icmp_seq=0. time=<16 ms
64 bytes from 192.168.100.1: icmp_seq=1. time=<16 ms
64 bytes from 192.168.100.1: icmp_seq=2. time=<16 ms
64 bytes from 192.168.100.1: icmp_seq=3. time=<16 ms
----192.168.100.1 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms)  min/avg/max = <16/<16/<16
```

CES>ping 192.168.101.1

```
PING 192.168.100.2: 36 data bytes
64 bytes from 192.168.101.1: icmp_seq=0. time=<16 ms
64 bytes from 192.168.101.1: icmp_seq=1. time=<16 ms
64 bytes from 192.168.101.1: icmp_seq=2. time=<16 ms
64 bytes from 192.168.101.1: icmp_seq=3. time=<16 ms
----192.168.101.1 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms)  min/avg/max = <16/<16/<16
```

5.1.7. Verify Peer Connectivity from the G350

Ping the Nortel remote peer from the G350 command line:

G350-001(super)# ping 1.1.1.2

```
Reply from 1.1.1.2: bytes=32 time=1ms TTL=63
Reply from 1.1.1.2: bytes=32 time=1ms TTL=63
Reply from 1.1.1.2: bytes=32 time=1ms TTL=63
Ping statistics for 1.1.1.2:
    Packets: sent = 3, Received = 3, Lost = 0 (0% loss)
Approximate round trip times in milli-seconds:
    Minimum = 1, Maximum = 1, Average = 1
```

5.1.8. Verify Peer VPN Connectivity from the G350

Ping the Nortel remote peer from the G350 command line:

```
G350-001(super)# ping 192.168.101.1
Reply from 192.168.101.1: bytes=32 time=1ms TTL=63
Reply from 192.168.101.1: bytes=32 time=1ms TTL=63
Reply from 192.168.101.1: bytes=32 time=1ms TTL=63
Ping statistics for 192.168.101.1:
    Packets: sent = 3, Received = 3, Lost = 0 (0% loss)
Approximate round trip times in milli-seconds:
    Minimum = 1, Maximum = 1, Average = 1
```

5.2. IPSec VPN Tunnel Establishment

Verify that a VPN exists between the peers and check security associations. The following traces and show commands represent a successful IPSec VPN tunnel established between a G350 Media Gateway (Initiator) and a Contivity 1100 Secure IP Services Gateway (Responder). Either side may be elected the initiator depending which device receives a packet requiring IPSec protection first and launches the VPN tunnel negotiations.

5.2.1. How to Enable G350 VPN Syslog Console Port Debugging

Enable Syslog debug tracing from the console port and then enable ISAKMP and IPSec syslog debugging using the command line.

```
G350-001(super)# set logging session enable
G350-001(super)# set logging session condition isakmp debug
G350-001(super)# set logging session condition ipsec debug
```

5.2.2. G350 Syslog Debug Messages

The Initiating IKE phase1 negotiation message indicates the G350 is the initiator of the session. An ISAKMP SA is created when phase 1 completes. Then the IPSec inbound and outbound Security Associations are created when phase 2 completes. The SPIs should be identical with opposite directions on the Nortel Contivity.

```
11/29/2004,16:33:57:IPSEC-Informational: Call IKE negotiation for outgoing SPD entry
901_1:
```

```
Peers 100.100.103.2<->1.1.1.2
```

```
11/29/2004,16:33:57:ISAKMP-Informational: Initiating IKE phase 1 negotiation:
Peers 100.100.103.2<->1.1.1.2
```

```
11/29/2004,16:33:58:ISAKMP-Informational: Received IKE notify message:
Peers 1.1.1.2<->100.100.103.2, Type INITIAL_CONTACT (24578)
Icookie - baf5350558e51059, Rcookie - 1ef3aa5bbb12bb87
```

```
11/29/2004,16:33:58:ISAKMP-Informational: Finished IKE phase 1 negotiation, creating
ISAKMP SA:
```

```
Peers 100.100.103.2<->1.1.1.2
Icookie - baf5350558e51059, Rcookie - 1ef3aa5bbb12bb87
esp-3des, esp-sha-hmac, DH group 2, Lifetime 86400 seconds
```

11/29/2004,16:33:58:ISAKMP-Informational: Initiating IKE phase 2 negotiation:
Peers 100.100.103.2<->1.1.1.2

11/29/2004,16:33:58:ISAKMP-Informational: Finished IKE phase 2, creating outbound IPSEC SA:

SPI 0x192153, Peers 100.100.103.2<->1.1.1.2
Identities: 192.168.10.0/255.255.255.0->192.168.101.0/255.255.255.0
esp-aes, esp-sha-hmac, 3600 seconds, 4608000 KB, PFS #2

11/29/2004,16:33:58:ISAKMP-Informational: Finished IKE phase 2, creating inbound IPSEC SA:

SPI 0x26d8, Peers 1.1.1.2<->100.100.103.2
Identities: 192.168.101.0/255.255.255.0->192.168.10.0/255.255.255.0
esp-aes, esp-sha-hmac, 3600 seconds, 4608000 KB, PFS #2

5.2.3. Contivity 1100 Event Log

Using the Nortel web management interface, navigate to **STATUS → EVENT LOG** and verify successful ISAKMP and IPsec SA establishment.

11/29/2004 16:39:25 0 Security [11] Session: IPSEC[100.100.103.2] attempting login
11/29/2004 16:39:25 0 Security [01] Session: IPSEC[100.100.103.2] has no active sessions
11/29/2004 16:39:25 0 Security [01] Session: IPSEC[100.100.103.2] G350 has no active accounts
11/29/2004 16:39:25 0 ISAKMP [02] Oakley Main Mode proposal accepted from 100.100.103.2
11/29/2004 16:39:26 0 Security [01] Session: IPSEC[100.100.103.2]:4 SHARED-SECRET authenticate attempt...
11/29/2004 16:39:26 0 Security [01] Session: IPSEC[100.100.103.2]:4 attempting authentication using LOCAL
11/29/2004 16:39:26 0 Security [11] Session: IPSEC[100.100.103.2]:4 authenticated using LOCAL
11/29/2004 16:39:26 0 Security [11] Session: IPSEC[100.100.103.2]:4 bound to group /Base/Avaya/G350
11/29/2004 16:39:26 0 Security [01] Session: IPSEC[100.100.103.2]:4 Building group filter permit all
11/29/2004 16:39:26 0 Security [01] Session: IPSEC[100.100.103.2]:4 Applying group filter permit all
11/29/2004 16:39:26 0 Security [11] Session: IPSEC[100.100.103.2]:4 authorized
11/29/2004 16:39:26 0 ISAKMP [02] ISAKMP SA established with 100.100.103.2
11/29/2004 16:39:26 0 Security [11] Session: network IPSEC[192.168.10.0-255.255.255.0] attempting login
11/29/2004 16:39:26 0 Security [11] Session: network IPSEC[192.168.10.0-255.255.255.0] logged in from gateway [100.100.103.2]
11/29/2004 16:39:26 0 Security [12] Session: IPSEC[100.100.103.2]:4 physical addresses: remote 100.100.103.2 local 1.1.1.2
11/29/2004 16:39:26 0 Security [12] Session: IPSEC[-]:5 physical addresses: remote 100.100.103.2 local 1.1.1.2
11/29/2004 16:39:27 0 Outbound ESP from 1.1.1.2 to 100.100.103.2 SPI 0x000026d8 [03] ESP encap session SPI 0xd8260000 bound to cpu 0
11/29/2004 16:39:27 0 Inbound ESP from 100.100.103.2 to 1.1.1.2 SPI 0x00192153 [03] ESP decap session SPI 0x53211900 bound to cpu 0
11/29/2004 16:39:27 0 Branch Office [00] 734eb20 BranchOfficeCtxtCls::RegisterTunnel: rem[192.168.10.0-255.255.255.0]@[100.100.103.2] loc[192.168.101.0-255.255.255.0] overwriting tunnel context [0] with [6ea8258]
11/29/2004 16:39:27 0 ISAKMP [03] Established IPsec SAs with 100.100.103.2:
11/29/2004 16:39:27 0 ISAKMP [03] ESP AES-CBC-HMAC-SHA outbound SPI 0x26d8
11/29/2004 16:39:27 0 ISAKMP [03] ESP AES-CBC-HMAC-SHA inbound SPI 0x192153

5.3. Tunnel Recovery – Deleting Nortel Security Associations

Verify that the VPN tunnel recovers when Security Associations are manually removed from the Nortel Contivity through software. There must be active traffic flows in progress in order to restart the tunnel.

1. Navigate to **STATUS → SESSIONS** and click **Log Off** next to the active branch office session that you wish to remove. This will begin the delete process for both ISAKMP and IPsec SAs.

Current Branch Office Sessions								
Connection	Type	UID	Address	Start	Kbytes	Packets	Connected Subnets	Action
G350	IPSEC	100.100.103.2	100.100.103.2	11/30/2004 12:47:20	In: 31 Out: 30	In: 523 Out: 523	1	Log Off Details

Figure 30: Sessions page

2. Click **OK** to finalize removal of the ISAKMP and IPsec Security Associations.

Log Off this connection?

Connection: G350

OK

Cancel

Figure 31: Confirm Log Off? Page

5.4. Tunnel Recovery – Deleting G350 Security Associations

Verify that IPsec VPN tunnel connectivity recovers after Security Associations are manually removed from the G350 Media Gateway through software. There must be active traffic flows in progress in order to restart the tunnel.

1. Remove IPsec Security Associations using the command line.

```
G350-001(super)# clear crypto sa all
```

2. Remove ISAKMP Security Associations using the command line.

```
G350-001(super)# clear crypto isakmp
```

6. VPN Troubleshooting Tips

Recommended steps for troubleshooting Virtual Private Networks (VPNs).

1. Physical Connectivity
2. Network Connectivity
3. Confirm Phase 1 ISAKMP SA establishment
4. Confirm Phase 2 inbound and outbound IPsec SA establishment
5. Confirm bi-directional VPN forwarding

If the VPN has not been established and Layer 3 connectivity appears to be working correctly, always check SA establishment. If an ISAKMP SA and IPsec SAs are created between the peers, the problem is usually related to routing. Check the encryption and decryption statistics for the IPsec SAs from the G350 command line. If there is a routing problem on either side of the tunnel, encryption and decryption will typically only occur in one direction. This usually indicates that the remote network cannot route back through the tunnel.

VPNs typically break because of administration errors. The most commonly encountered problems with VPNs are either mismatched ISAKMP or IPsec security attributes or routing problems. Another source for potential problems may be network/host masking. The G350 Media Gateway uses wildcard subnet/host masking, while the Nortel Contivity 1100 uses variable length subnet/host masking. These masks must be configured to have the same meaning on both peers. Pay very close attention to these configuration items when administering a new VPN.

6.1. How to Inspect G350 ISAKMP Security Associations

Verify ISAKMP SAs by using the **show** command.

```
G350-001(super)# show crypto isakmp sa
```

C-id	Local	Remote	State	Cipher	Hash	Auth	DH	Sec	left
4	100.100.103.2	1.1.1.2	Ready	3des	sha	psk	2		86393

6.2. How to Inspect G350 IPSec Security Associations

Inspect active IPSec Security Associations by using **show** commands. Use **show crypto ipsec sa** to display all policies. The alternate form of the **show** command, depicted below, can be used to isolate specific security associations according to crypto list and even individual rules within a crypto list.

```
G350-001(super)# show crypto ipsec sa list 901 rule 1 detail
```

Inbound pkts errors (global):

```
Invalid spi          0
Invalid interface    0
```

Interface: FastEthernet 10/2

Crypto list id: 901, Local address: 100.100.103.2

Rule: 1, Crypto map: 1, "P2 with Nortel"

Local address: 100.100.103.2, Remote address: 1.1.1.2

Local identity: 192.168.10.0/255.255.255.0

Remote identity: 192.168.101.0/255.255.255.0

path mtu 1500, media mtu 1500

Current outbound spi: 0x192153

Inbound packets		Outbound packets	
-----		-----	
Total	1	Total	22
Total OK	1	Total OK	1
Decrypt	1	Encrypt	1
Verify	1	Digest	1
Decaps	1	Encaps	1
Total discards	0	Total discards	21
Invalid len	0	No sa	21
Replay failed	0	Seq rollover	0
Sa expired	0	Sa expired	0
Auth failed	0		
Bad padding	0		
Invalid identity	0		
Unprotected	0		
Other discards	0	Other discards	0

SA Type	SPI	Transform	PFS	Secs left	KB left	Mode
-----	-----	-----	-----	-----	-----	-----
Inbound ESP	0x26d8	esp-aes esp-sha-hmac	#2	3586	4607999	Tunnel
Outbound ESP	0x192153	esp-aes esp-sha-hmac	#2	3586	4607999	Tunnel

6.3. How to Inspect Contivity Security Associations

1. Navigate to **STATUS → SESSIONS** and click **Details** next to the active session that needs inspection.
2. Information such as encrypted and decrypted packet counters appears.

```
Date: 11/30/2004 Time: 12:58:19

Name: G350
Account Type: IPSEC
Number of Sessions: 1
  Session Subnet: 192.168.10.0 - 255.255.255.0
  Session Start Date: 11/30/2004
  Session Start Time: 12:47:20
  Session Total KBytes In: 36
  Session Total KBytes Out: 35
  Session Total Packets In: 606
  Session Total Packets Out: 606
  Session Filter Drops In: 0
  Session Filter Drops Out: 0
  Session Total QoSRandom Drops In: 0
  Session QoSRandom Drops Out: 0
  Session QoSForced Drops In: 0
  Session Total QoSForced Drops Out: 0
  Session IpHdr Drops In: 0
  Session IpHdr Drops Out: 0
  Session IpFrag In: 0
  Session IpFrag Out: 0
  Session IpFrag Drops In: 0
  Session IpFrag Drops Out: 0
  Session BWM Configured Committed Rate Kbps: 56
  Session BWM Runtime Committed Rate Kbps: 56
  Session BWM In-Profile KBytes: 0
  Session BWM Out-Of-Profile KBytes: 0
```

Figure 32: Active Sessions → Details page (Top)

```
ISAKMP security association established with 100.100.103.2
Local address: 1.1.1.2
Local Udp Port:500 Remote port:500
Initiator cookie: 618FD283C08A76D4
Responder cookie: EC74BD86CE1B1DB6
IKE encryption: Triple DES with Diffie-Hellman group 2 (MODP 1024-bit prime)
IKE Keepalive: Disabled.

IPSec tunnel mode security associations established:
Local subnet 192.168.101.0 mask 255.255.255.0
Remote subnet 192.168.10.0 mask 255.255.255.0
  ESP AES-CBC-HMAC-SHA outbound SPI 0x5BCA software session
    606 packets sent
  ESP AES-CBC-HMAC-SHA inbound SPI 0x14F77E software session
    606 packets successfully received
    0 packets truncated
    0 packets failed replay check
    0 packets failed authentication
    0 packets with invalid pad length (decryption failure)
Expires on TUE NOV 30 13:47:21 2004
```

Figure 33: Active Sessions → Details page (Bottom)

7. Conclusion

Peer-to-Peer IPSec VPN tunnel connectivity between the Avaya G350 Media Gateway and the Nortel Contivity 1100 Secure IP Services Gateway can be achieved using the guidelines demonstrated in these Application Notes. Use of the AES-128 encryption algorithm with Perfect Forward Secrecy (PFS) is recommended for optimized voice performance and added protection. The steps described in these Application Notes may be generalized for most configurations.

8. Additional References

The following references were obtained online. References without a specific website can be located from various mirror sites using a search engine such as <http://www.google.com>

- [1] Administration of the Avaya G350 Media Gateway, January 2005, Issue 3, Document Number: 555-245-501, <http://support.avaya.com>
- [2] Avaya G350 Media Gateway Command Line Interface (CLI) Guide, January 2005, Issue 3, Document Number: 555-245-202, <http://support.avaya.com>
- [3] Configuring Avaya Communication Manager for Media Encryption, April 2004, Issue 1.0, Avaya Solution & Interoperability Test Lab Application Notes, <http://www.avaya.com>
- [4] IPSec Virtual Private Network (VPN) between an Avaya G350 Media Gateway and a Cisco PIX 525 Firewall, December 2004, Issue 1.0, Avaya Solution & Interoperability Test Lab Application Notes, <http://www.avaya.com>
- [5] RFC 2401, Security Architecture for the Internet Protocol, November 1998
- [6] RFC 2402, IP Authentication Header, November 1998
- [7] RFC 2404, The Use of HMAC-SHA-1-96 within ESP and AH
- [8] RFC 2406, IP Encapsulating Security Payload (ESP), November 1998
- [9] RFC 2407, The Internet IP Security Domain of Interpretation for ISAKMP, November 1998
- [10] RFC 2408, The Internet Security Association and Key Management Protocol (ISAKMP), November 1998
- [11] RFC 2409, The Internet Key Exchange (IKE), November 1998
- [12] FIPS 197, Advanced Encryption Standard (AES), November 2001
- [13] Nortel Networks Tech Tip – Contivity – Cisco PIX IPSec peer-to-peer branch office tunnel using pre-shared key authentication, June 2004, <http://www.nortelnetworks.com>

©2005 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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 Solution & Interoperability Test Lab at interoplabnotes@list.avaya.com