Cisco ASA 5505 IPSEC L2L Tunnel Failover Architecture for Bank of Smithtown

Background and Installation Process/Testing Procedures

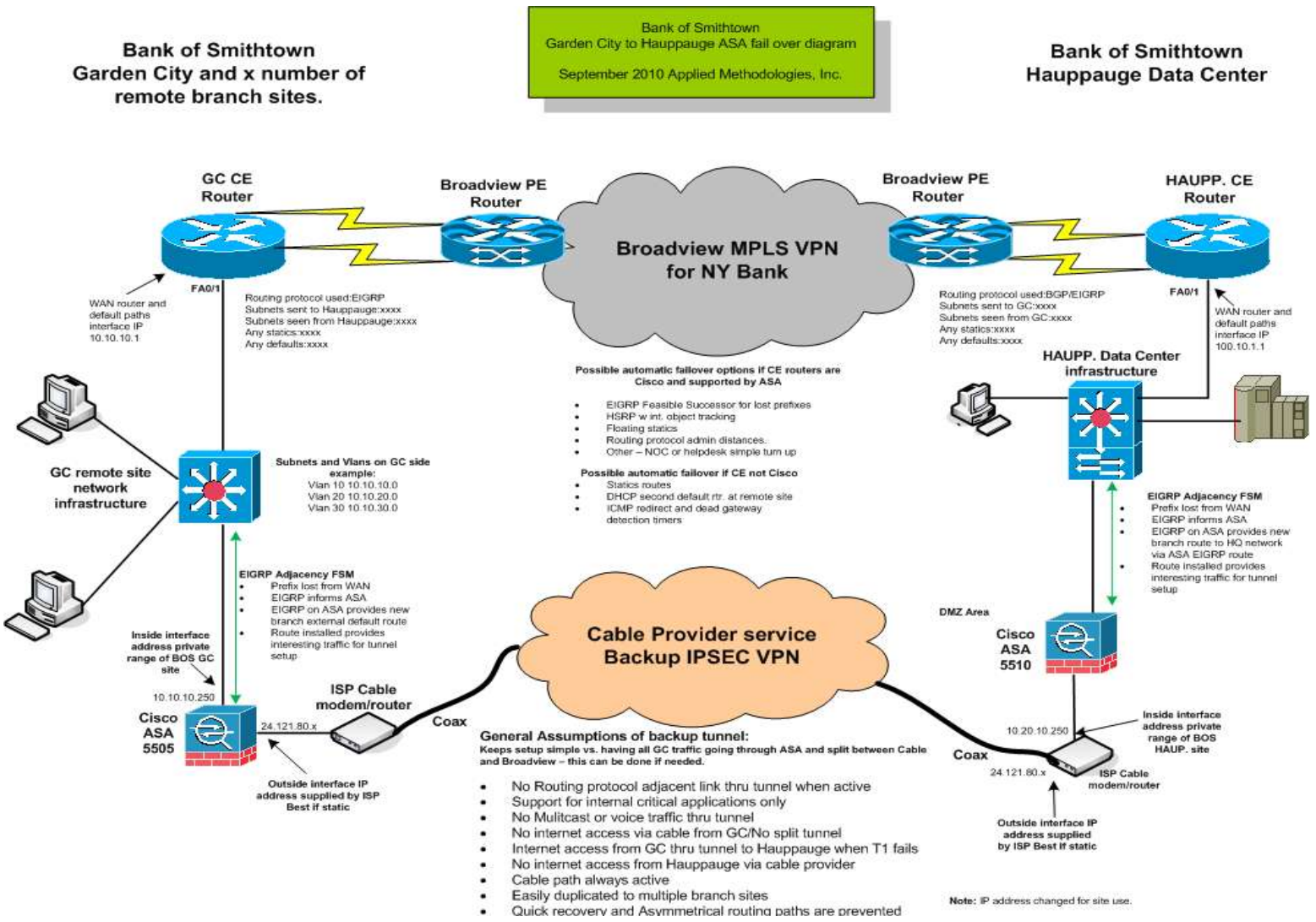
Applied Methodologies, Inc.

September, 2010

Contents

Introduction:

Bank of Smithtown(BOS) requires the use of Cisco ASA 5505 security appliances to provide a secure and encrypted failover LAN to LAN (L2L) tunnel between its Hauppauge headquarters office and many of its remote branches in NY. This tunnel is required for their WAN provider is experiencing quality issues at several locations starting with their Garden City branch. The L2L tunnel architecture will consists of an ASA 5505 at the company headquarters with an initial L2L tunnel established to the Garden City branch. This solution will utilize a local cable ISP for connectivity between sites. A simple solution was needed to ensure operational continuity before the bank merged with a competitor. A strategic DMVPN solution was not considered due to the merger activities and time required. The tactical solution was to utilize the ASA's on a per branch site basis. This solution can scale up to 25 remote branches before an upgrade in the headquarters site from ASA 5505 to 5510 is required. This approach provides both banks a low cost, very secure and easy to manage architecture to support the branch sites during the merger. The ASAs have been pre tested and staged in AMILABS' networking lab with a simulated environment that reflects BOS's MPLS/MBGP WAN. The following diagram below outlines the basic architecture.



This document outlines the basic installation, testing process and post installation behavior of the devices involved. Additional branches can achieve failover protection by duplicating this setup resulting in the Hauppauge ASA becoming a L2L hub to the branch ASA spoke based sites. The configuration files contain a template for additional sites to be added. Cisco ASDM can also be used to manage and install additional sites.

Some general points:

- **Enable passwords and AAA are not set on devices – should be set after testing from NOC**
- **The tunnel is only for prefix loss not device loss. Since the ASA's don't support HSRP/VRRP at time of this writing EIGRP Feasible Successor FSM was used for prefix loss detection. ICMP redirects and Dead Gateway detection methods were too slow for proper failover detection.**
- The tunnel will only be active when interesting traffic destined for Hauppauge or GC is present when the Broadview path is unavailable.
- The tunnel will deactivate after 1 minute of idle time when no traffic for either site is present to go through the tunnel. This prevents the tunnel from remaining active once the Broadview path is active again. Asymmetrical routing paths are prevented.
- Logging is enabled to be buffered in the device – NOC can setup syslogging according to its standards
- Use of ASDM is highly recommended to monitor, adjust configurations, debug, log and setup additional features of ASA.
- HTTPS server is set for INSIDE 123.45.X.X subnet on each device for management
- The HUB Hauppauge ASA has example commands for a second branch(not active) and with the routing statements removed.

For second site

```
crypto map BRANCHES 20 match address nextsite
crypto map BRANCHES 20 set pfs group1
crypto map BRANCHES 20 set peer 174.220.90.26 – fake address from lab
crypto map BRANCHES 20 set select based on policy
crypto map BRANCHES interface outside

tunnel-group 174.220.90.26 type ipsec-l2l – fake address from lab
tunnel-group 174.220.90.26 ipsec-attributes
 pre-shared-key *****
```

Installation

Installation process for Cisco ASA 5505 IPSEC L2L appliances to backup Broadview MPLS WAN path between Hauppauge and Garden City branch

Below are the steps to install the ASA once delivered to sites.

1). HAUPPAUGE INSTALL
Install the ASA in Hauppauge network switching infrastructure. *The ASA is preconfigured to join the BOS EIGRP routing process of 1038 and no further configuration is necessary on BOS routers at the Hauppauge site.*

Port 1 is for the inside vlan 1 network – This goes to the 123.45.4.0 network
The IP address of the ASA Vlan 1 interface is 123.45.4.25
All the other ports 2-7 are set for the inside network of vlan1 123.45.4.0.

Port 0 is for the Cat 5 cable from the Cable Modem to the ASA – This is the outside network of 222.111.90.26/29
The IP address of the outside Vlan2 interface is 222.111.90.98
Check for EIGRP neighbor on ASA – SH EIG NEG
Check for EIGRP neighbors on other Hauppauge routers - SH IP EIG NEIGHBOR
Make sure you can ping 123.45.4.1 and .243 routers respectively from the ASA

Check routing table to Garden City network – should still go through Broadview path
From ASA ping outside Garden City cable modem interface of 222.111.90.25 if allowed from ISP.

2). GARDEN CITY INSTALL
Install ASA in Garden City network
Port 1 is for the inside vlan 1 network – This goes to the 123.45.33.0 network
The IP address of the ASA Vlan 1 interface is 123.45.33.25
All the other ports 2-7 are set for the inside network of vlan1 123.45.33.0.

Port 0 is for the Cat 5 cable from the Cable Modem to the ASA – This is the outside network of 222.111.90.24/29
The IP address of the outside Vlan2 interface is 222.111.90.26
From ASA ping outside Hauppauge cable modem interface of 222.111.90.27 if allowed from ISP.
From ASA ping outside Hauppauge ASA interface of 222.111.90.98

3). Add changes to Garden City Broadview router:

Interface FA0/0
no ip redirects
remove secondary address

Global statements:
ip route 0.0.0.0 0.0.0.0 Serial0/0
ip route 0.0.0.0 0.0.0.0 123.45.33.25 200

router eigrp 21 – *separate process from BOS HQ and will not affect WAN routing used for cutover function*
network 10.0.0.0
no auto-summary
(no redistribution here for the ASA has EIGRP and is redistributing its route)

Check for EIGRP neighbor on ASA – SH EIG NEG
Check for EIGRP neighbors on other Hauppauge routers - SH IP EIG NEIGHBOR
Make sure you can ping 123.45.33.1 router respectively from the ASA
At this point both ASAs should be up in each site and we should be able to ping between their outside interfaces GC 222.111.90.26 -- Hauppauge 222.111.90.98
Check routing table to Hauppauge network – should still go through Broadview path.

Failover testing process:

1. Submission of Change Control if applicable
2. Notification of NOC if applicable
3. Shut down of Garden City Serial 0/0/0
4. Conduct check on Garden City router of routes to Hauppauge – path should now be through the ASA
5. From GC router ping Hauppauge devices
6. From GC ASA verify tunnel is up with show commands listed earlier in documentation
7. From Hauppauge routers verify path to 123.45.33.0
8. From Hauppauge ASA verify tunnel is up with show commands listed earlier in documentation
9. Run ping from Hauppauge to devices in GC.

10. In GC run applications and access internet via tunnel.
11. Note any issues and correct.

Conduct final configuration changes to devices:

1. Enable passwords, SSH and AAA
2. Setup and test SNMP, traps and NMS if applicable
3. Exchange tunnel pre-shared key with BOS personnel
4. Setup ASDM if applicable for BOS personnel
5. Demonstrate ASDM for BOS personnel if applicable

POST Installation

Normal state of ASA when Broadview path is up between Garden City and Hauppauge

Garden City

Output of Cisco ASA 5505 in Garden City

Normal ASA activity when Garden City's Broadview link is operating normally **UP– NO TUNNEL IS ACTIVE**

EIGRP neighbor is in place between ASA and Garden City Broadview router
BOSGCASA# sh eig nei
EIGRP-IPv4 neighbors for process **21 - separate process from HQs 1038**

```
H   Address            Interface      Hold Uptime   SRTT   RTO  Q  Seq
                           (sec)       (ms)       Cnt Num
0   123.45.33.1          Vl1           13  00:39:57 1    200   0   10
BOSGCASA#
```

BOSGCASA# **sh ipsec sa**

There are no ipsec sas
BOSGCASA# **sh isakmp sa**

There are no isakmp sas
BOSGCASA#

Vlan 1 is **the inside 123.45.33.0 network** and there should be little traffic noted on the interface.

```
BOSGCASA# sh int vlan1
Interface Vlan1 "inside", is up, line protocol is up
  Hardware is EtherSVI, BW 100 Mbps, DLY 100 usec
      Description: BOS GardenCity Branch Local LAN
      MAC address 68ef.bdcc.818e, MTU 1500
      IP address 123.45.33.25, subnet mask 255.255.255.0
  Traffic Statistics for "inside":
      191 packets input, 11449 bytes
      225 packets output, 13772 bytes
      0 packets dropped
    1 minute input rate 0 pkts/sec,  13 bytes/sec
    1 minute output rate 0 pkts/sec,  13 bytes/sec
    1 minute drop rate, 0 pkts/sec
    5 minute input rate 0 pkts/sec,  13 bytes/sec
    5 minute output rate 0 pkts/sec,  13 bytes/sec
    5 minute drop rate, 0 pkts/sec
```

Vlan2 is the **outside interface to the cable network provider** and should also have little traffic if any noted since the tunnel is not currently up.

```
BOSGCASA# sh int vlan 2
Interface Vlan2 "outside", is up, line protocol is up
  Hardware is EtherSVI, BW 100 Mbps, DLY 100 usec
      Description: BOS GardenCity Branch Cable ISP backup link
      MAC address 68ef.bdcc.818e, MTU 1500
      IP address 222.111.90.26, subnet mask 255.255.255.248
  Traffic Statistics for "outside":
      2 packets input, 650 bytes
      0 packets output, 0 bytes
```

```
     1 packets dropped
    1 minute input rate 0 pkts/sec,  0 bytes/sec
    1 minute output rate 0 pkts/sec,  0 bytes/sec
    1 minute drop rate, 0 pkts/sec
    5 minute input rate 0 pkts/sec,  0 bytes/sec
    5 minute output rate 0 pkts/sec,  0 bytes/sec
    5 minute drop rate, 0 pkts/sec
BOSGCASA#
```

From Garden City router:

```
GardenCity#sh ip rou

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

    10.0.0.0/8 is variably subnetted, 3 subnets, 3 masks
C       123.45.8.253/32 is directly connected, Serial0/0
C       123.45.8.254/31 is directly connected, Serial0/0
C       123.45.33.0/24 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 is directly connected, Serial0/0
GardenCity#
```

Output of Cisco ASA 5505 in Hauppauge

Normal ASA activity when Hauppauge's Broadview link is operating normally **UP– NO TUNNEL IS ACTIVE**

EIGRP neighbor is in place between ASA and Hauppauge Broadview router

```
Broadview#sh ip eig nei
IP-EIGRP neighbors for process 1038
H   Address            Interface      Hold Uptime   SRTT   RTO  Q  Seq
                                      (sec)         (ms)       Cnt Num
3   123.45.4.1         Fa0/0          14 00:41:01   60   360  0  24
2   123.45.4.244       Fa0/0          13 00:41:14    3   200  0  23
1   123.45.4.240       Fa0/0          14 00:42:30   21   200  0  36
0   123.45.4.25        Fa0/0          10 00:42:30   21   200  0  45   ASA as EIGRP neighbor
Broadview#
```

```
BOSHAUPPASA# sh ipsec sa

There are no ipsec sas
BOSHAUPPASA# sh isakmp sa

There are no isakmp sas
BOSHAUPPASA#
```

Vlan 1 is **the inside 123.45.4.0 network** and there should be little traffic noted on the interface.

```
BOSHAUPPASA# sh int vlan 1
Interface Vlan1 "inside", is up, line protocol is up
  Hardware is EtherSVI, BW 100 Mbps, DLY 100 usec
      Description: BOS Hauppaugh HQ
      MAC address 68ef.bdcc.97ba, MTU 1500
      IP address 123.45.4.25, subnet mask 255.255.254.0
  Traffic Statistics for "inside":
      1798 packets input, 113043 bytes
      569 packets output, 47600 bytes
      0 packets dropped
    1 minute input rate 0 pkts/sec,  52 bytes/sec
    1 minute output rate 0 pkts/sec,  14 bytes/sec
    1 minute drop rate, 0 pkts/sec
    5 minute input rate 0 pkts/sec,  52 bytes/sec
    5 minute output rate 0 pkts/sec,  14 bytes/sec
    5 minute drop rate, 0 pkts/sec
```

Vlan2 is the **outside interface to the cable network provider** and should also have little traffic if any noted since the tunnel is not currently up.

BOSHAUPPASA# sh int vlan 2
Interface Vlan2 "outside", is up, line protocol is up
  Hardware is EtherSVI, BW 100 Mbps, DLY 100 usec
     Description: BOS Hauppaugh Cable ISP backup link
     MAC address 68ef.bdcc.97ba, MTU 1500
     IP address 222.111.90.98, subnet mask 255.255.255.248
  Traffic Statistics for "outside":
     25 packets input, 4282 bytes
     22 packets output, 3420 bytes
     1 packets dropped
    1 minute input rate 0 pkts/sec, 0 bytes/sec
    1 minute output rate 0 pkts/sec, 0 bytes/sec
    1 minute drop rate, 0 pkts/sec
    5 minute input rate 0 pkts/sec, 0 bytes/sec
    5 minute output rate 0 pkts/sec, 0 bytes/sec
    5 minute drop rate, 0 pkts/sec
BOSHAUPPASA#

From Broadview router:
Broadview#**sh ip rou 123.45.33.0**
Routing entry for 123.45.0.0/16
  Known via "static", distance 1, metric 0 (connected)
  Redistributing via eigrp 1038
  Advertised by eigrp 1038
  Routing Descriptor Blocks:
  * **directly connected, via Serial0/0/0**
     Route metric is 0, traffic share count is 1

From Cisco 3745 Verizon Default Gateway router:
MotorParkway_DEFGW>
MotorParkway_DEFGW>**sh ip route 123.45.33.0**
Routing entry for 123.45.0.0/16
  Known via "eigrp 1038", distance 90, metric 2172416, type internal
  Redistributing via eigrp 1038
  Last update from 123.45.4.243 on FastEthernet0/0, 00:06:03 ago
  Routing Descriptor Blocks:
  * **123.45.4.243, from 123.45.4.243**, 00:06:03 ago, via FastEthernet0/0
     Route metric is 2172416, traffic share count is 1
     Total delay is 20100 microseconds, minimum bandwidth is 1544 Kbit
     Reliability 255/255, minimum MTU 1500 bytes
     Loading 1/255, Hops 1

From Perimeter router:
Premiter#**sh ip rou 123.45.33.0**
Routing entry for 123.45.0.0/16
  Known via "eigrp 1038", distance 90, metric 2172416, type internal
  Redistributing via eigrp 1038
  Last update from 123.45.4.243 on FastEthernet0/0, 00:09:55 ago
  Routing Descriptor Blocks:
  * **123.45.4.243, from 123.45.4.243, 00:09:55 ago, via FastEthernet0/0**
     Route metric is 2172416, traffic share count is 1
     Total delay is 20100 microseconds, minimum bandwidth is 1544 Kbit
     Reliability 255/255, minimum MTU 1500 bytes
     Loading 1/255, Hops 1

State of ASA when Broadview path is DOWN between Garden City and Hauppauge

Garden City

Output of Cisco ASA 5505 in Garden City

Normal ASA activity when Garden City's Broadview link is **DOWN– IPSEC TUNNEL IS ACTIVE**

GardenCity#**sh ip rou**

Gateway of last resort is **123.45.33.25** to network 0.0.0.0

```
    10.0.0.0/24 is subnetted, 1 subnets
C       123.45.33.0 is directly connected, FastEthernet0/0
D*EX 0.0.0.0/0 [170/30720] via 123.45.33.25, 00:00:06, FastEthernet0/0
```

Normal ASA activity when Garden City's Broadview link is DOWN – **IPSEC TUNNEL IS ACTIVE**

BOSGCASA# **sh isakmp sa**

```
  Active SA: 1
   Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 222.111.90.98
   Type    : L2L          Role    : initiator
   Rekey   : no           State   : MM_ACTIVE
```

BOSGCASA# **sh ipsec sa**

```
interface: outside
   Crypto map tag: TOHAUPP, seq num: 1, local addr: 222.111.90.26

     access-list tohaupp extended permit ip 123.45.33.0 255.255.255.0 any
     local ident (addr/mask/prot/port): (123.45.33.0/255.255.255.0/0/0)
     remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
     current_peer: 222.111.90.98

     #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10 – some traffic
     #pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 10, #pkts comp failed: 0, #pkts decomp failed: 0
     #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
     #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
     #send errors: 0, #recv errors: 0

     local crypto endpt.: 222.111.90.26/0, remote crypto endpt.: 222.111.90.98/
0
     path mtu 1500, ipsec overhead 74, media mtu 1500
     current outbound spi: 19D39d0B2DA
     current inbound spi : A21d97919B3

   inbound esp sas:
     spi: 0xA2198A19B3 (271958953971)
       transform: esp-aes-256 esp-sha-hmac no compression
       in use settings ={L2L, Tunnel, PFS Group 1, }
       slot: 0, conn_id: 4096, crypto-map: TOHAUPP
       sa timing: remaining key lifetime (kB/sec): (3914999/28784)
       IV size: 16 bytes
       replay detection support: Y
       Anti replay bitmap:
        0x00000000 0x000007FF
   outbound esp sas:
```

```
    spi: 0x19D0B542DA (43313107674)
      transform: esp-aes-256 esp-sha-hmac no compression
      in use settings ={L2L, Tunnel, PFS Group 1, }
      slot: 0, conn_id: 4096, crypto-map: TOHAUPP
      sa timing: remaining key lifetime (kB/sec): (3914999/28784)
      IV size: 16 bytes
      replay detection support: Y
      Anti replay bitmap:
       0x00000000 0x00000001
```

Vlan2 now has some traffic going through it.

```
BOSGCASA#
BOSGCASA#
BOSGCASA# sh int vlan2
Interface Vlan2 "outside", is up, line protocol is up
  Hardware is EtherSVI, BW 100 Mbps, DLY 100 usec
      Description: BOS GardenCity Branch Cable ISP backup link
      MAC address 68ef.bdcc.818e, MTU 1500
      IP address 222.111.90.26, subnet mask 255.255.255.248
  Traffic Statistics for "outside":
      57 packets input, 9592 bytes
      59 packets output, 9440 bytes
      1 packets dropped
    1 minute input rate 0 pkts/sec,  89 bytes/sec – some traffic
    1 minute output rate 0 pkts/sec,  92 bytes/sec
    1 minute drop rate, 0 pkts/sec
    5 minute input rate 0 pkts/sec,  0 bytes/sec
    5 minute output rate 0 pkts/sec,  0 bytes/sec
    5 minute drop rate, 0 pkts/sec
BOSGCASA#
```

Hauppauge

Output of Cisco ASA 5505 in Hauppauge

Normal ASA activity when Garden City's Broadview link is **DOWN– IPSEC TUNNEL IS ACTIVE**
EIGRP neighbor is in place between ASA and Hauppauge Broadview router

Broadview#sh ip eig nei

```
IP-EIGRP neighbors for process 1038
H   Address            Interface      Hold Uptime   SRTT   RTO  Q  Seq
                         (sec)        (ms)       Cnt Num
3   123.45.4.1          Fa0/0          13 00:49:39   60   360  0  24
2   123.45.4.244         Fa0/0           11 00:49:53    3   200  0  23
1   123.45.4.240         Fa0/0           13 00:51:08   21   200  0  36
0   123.45.4.25          Fa0/0           10 00:51:08   21   200  0  45
```

BOSHAUPPASA# **sh isakmp sa**

```
  Active SA: 1
   Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 222.111.90.26
   Type    : L2L          Role    : responder
   Rekey   : no           State   : MM_ACTIVE
BOSHAUPPASA#
```

```
BOSHAUPPASA# sh ipsec sa
interface: outside
   Crypto map tag: BRANCHES, seq num: 10, local addr: 222.111.90.98

     access-list togardencity extended permit ip any 123.45.33.0 255.255.255.0
     local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
     remote ident (addr/mask/prot/port): (123.45.33.0/255.255.255.0/0/0)
     current_peer: 222.111.90.26

     #pkts encaps: 64, #pkts encrypt: 64, #pkts digest: 64 – some traffic going through
     #pkts decaps: 64, #pkts decrypt: 64, #pkts verify: 64
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 64, #pkts comp failed: 0, #pkts decomp failed: 0
     #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
     #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
     #send errors: 0, #recv errors: 0

     local crypto endpt.: 222.111.90.98/0, remote crypto endpt.: 222.111.90.26/
0
     path mtu 1500, ipsec overhead 74, media mtu 1500
     current outbound spi: 7488602F44
     current inbound spi : 998A60B08B

   inbound esp sas:
     spi: 0x9A603B08B (25900927915)
        transform: esp-aes-256 esp-sha-hmac no compression
        in use settings ={L2L, Tunnel, PFS Group 1, }
        slot: 0, conn_id: 16384, crypto-map: BRANCHES
        sa timing: remaining key lifetime (kB/sec): (4373993/28680)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0xFFFFFFFF 0xFFFFFFFF
   outbound esp sas:
     spi: 0x748027F44 (19545257764)
        transform: esp-aes-256 esp-sha-hmac no compression
        in use settings ={L2L, Tunnel, PFS Group 1, }
        slot: 0, conn_id: 16384, crypto-map: BRANCHES
        sa timing: remaining key lifetime (kB/sec): (4373993/28680)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x00000001

BOSHAUPPASA#

BOSHAUPPASA# sh int vlan 2
Interface Vlan2 "outside", is up, line protocol is up
  Hardware is EtherSVI, BW 100 Mbps, DLY 100 usec
       Description: BOS Hauppaugh Cable ISP backup link
       MAC address 68ef.bdcc.97ba, MTU 1500
       IP address 222.111.90.98, subnet mask 255.255.255.248
  Traffic Statistics for "outside":
       365 packets input, 60018 bytes
       353 packets output, 58060 bytes
       1 packets dropped
     1 minute input rate 0 pkts/sec,  0 bytes/sec
     1 minute output rate 0 pkts/sec,  0 bytes/sec
     1 minute drop rate, 0 pkts/sec
     5 minute input rate 0 pkts/sec,  67 bytes/sec – some traffic going out to GC
     5 minute output rate 0 pkts/sec,  66 bytes/sec
     5 minute drop rate, 0 pkts/sec
BOSHAUPPASA#
```

Routing in Hauppauge to GC

From Broadview router:

```
Broadview#sh ip route 123.45.33.0
Routing entry for 123.45.0.0/16
  Known via "eigrp 1038", distance 170, metric 30720, type external
  Redistributing via eigrp 1038
  Last update from 123.45.4.25 on FastEthernet0/0, 00:13:30 ago
  Routing Descriptor Blocks:
  * 123.45.4.25, from 123.45.4.25, 00:13:30 ago, via FastEthernet0/0  - USE ASA
      Route metric is 30720, traffic share count is 1
      Total delay is 200 microseconds, minimum bandwidth is 100000 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
```

From Cisco 3745 Verizon Default Gateway router:

```
MotorParkway_DEFGW#sh ip rou 123.45.33.0
Routing entry for 123.45.0.0/16
  Known via "eigrp 1038", distance 170, metric 30720, type external
  Redistributing via eigrp 1038
  Last update from 123.45.4.25 on FastEthernet0/0, 00:03:54 ago
  Routing Descriptor Blocks:
  * 123.45.4.25, from 123.45.4.25, 00:03:54 ago, via FastEthernet0/0 - USE ASA
      Route metric is 30720, traffic share count is 1
      Total delay is 200 microseconds, minimum bandwidth is 100000 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
MotorParkway_DEFGW#
```

From Perimeter router:

```
Premiter#sh ip rou 123.45.33.0
Routing entry for 123.45.0.0/16
  Known via "eigrp 1038", distance 170, metric 30720, type external
  Redistributing via eigrp 1038
  Last update from 123.45.4.25 on FastEthernet0/0, 00:04:31 ago
  Routing Descriptor Blocks:
  * 123.45.4.25, from 123.45.4.25, 00:04:31 ago, via FastEthernet0/0 - USE ASA
      Route metric is 30720, traffic share count is 1
      Total delay is 200 microseconds, minimum bandwidth is 100000 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
Premiter#
```

When Broadview path is returned the output of the commands will reflect the same results as outlined in the earlier sections.

ASA self documented configurations

- Internal site route configurations not provided for security purposes
- ASA configurations changed for security purposes.

```
ASA Version 8.3(2)
!*********************************!
!Bank of Smithtown Hauppauge ASA  !
!5505 - 2010 AMILABS              !
!*********************************!
!
!Second branch config left in for example
!
hostname BOSHAUPPASA
domain-name default.domain.invalid
enable password encrypted
passwd encrypted
names
!
!*****Interface for local LAN environment****
interface Vlan1
 description BOS Hauppaugh HQ
 nameif inside
 security-level 100
 ip address 11.103.4.25 255.255.254.0
!
!*****Interface for cable ISP Cat 5 ********
interface Vlan2
 description BOS Hauppaugh Cable ISP backup link
 nameif outside
 security-level 0
 ip address 169.198.90.98 255.255.255.248
!
!
!*** This is where the cable isp cat 5 cable connects to***
interface Ethernet0/0
 switchport access vlan 2
!
!
!****This is where you connect the ASA into your local infrastructure
interface Ethernet0/1
!
!
!***The rest of these interfaces can remain down but if used put into
vlan1
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
```

```
interface Ethernet0/6
!
interface Ethernet0/7
!
banner login
banner login BOSHAUPPASA
banner login BOS Hauppaugd ASA
banner motd BOS Hauppauge ASA
banner asdm BOS Hauppauge ASA
boot system disk0:/asa832-k8.bin
ftp mode passive
dns server-group DefaultDNS
 domain-name default.domain.invalid
object-group network obj_any
object-group network NETWORK_OBJ_11.103.33.0_24
object-group network NETWORK_OBJ_11.103.4.0_23
!
!***Access lists to identify traffic that will bring the tunnel up*****
!***The tostjames list was just for a test of another branch and can be
removed***
!
access-list togardencity extended permit ip any 11.103.33.0 255.255.255.0
access-list tostjames extended permit ip any 11.103.53.0 255.255.255.0
!
pager lines 24
logging enable
logging buffered warnings
logging asdm informational
mtu inside 1500
mtu outside 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-633.bin
no asdm history enable
arp timeout 14400
!
!
!
!****Joining BOS routing environment so backup path can be
distributed*******
router eigrp 1038
 no auto-summary
 network 11.0.0.0 255.0.0.0
 redistribute static
!
!
!***Static routes for tunnel path creation***
!***this route gets you out to the cable path***
route outside 11.103.0.0 255.255.0.0 169.198.90.97 180
!
!***this route was a test from the second branch for scaling
route outside 11.103.53.0 255.255.255.0 169.199.90.97 180
!
```

```
!***This route gets you to the other Garden City ASA Peer outside
interface***
route outside 169.198.90.24 255.255.255.248 169.198.90.97 1
!****The static routes had to be specific recursive for we cannot use a
default route like the branches would*****
!
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat
0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect
0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
!
!***HTTP enabled for ASDM usage***
https server enable
https 11.103.4.0 255.255.254.0 inside
!***Set snmp as same as broadview and GC routers
snmp-server host inside 121.111.60.66 community *****
no snmp-server location
no snmp-server contact
snmp-server community *****
snmp-server enable traps snmp authentication linkup linkdown coldstart
!
!
!*** IPSEC and ISAKMP SA information to peer with GC ASA***
crypto ipsec transform-set scrubbed
crypto ipsec security-association lifetime seconds scrubbed
crypto ipsec security-association lifetime kilobytes scrubbed
crypto map BRANCHES 10 match address togardencity
crypto map BRANCHES 10 set pfs group1
crypto map BRANCHES 10 set peer 169.198.90.26
crypto map BRANCHES 10 set scrubbed
!*******next set was used to test second branch for scaling****
crypto map BRANCHES 20 match address tostjames
crypto map BRANCHES 20 set pfs group1
crypto map BRANCHES 20 set peer 170.200.90.26
crypto map BRANCHES 20 set scrubbed
crypto map BRANCHES interface outside
crypto isakmp enable outside
crypto isakmp policy 10
 authentication pre-share
 encryption - scrubbed
 hash sha
 group 2
 lifetime scrubbed
!
!***very important to keep on prevents NAT from messing up tunnel****
no crypto isakmp nat-traversal
telnet timeout 5
ssh timeout 5
console timeout 0
```

```
management-access inside
!
threat-detection basic-threat
threat-detection statistics host
threat-detection statistics port
threat-detection statistics protocol
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ntp server 11.103.4.1
webvpn
!
!****Tunnel policies*****
group-policy DfltGrpPolicy attributes
!*** time out tunnel after 1 minute of no activity
 vpn-idle-timeout 1
!**** This was a test tunnel to another branch not in use***
tunnel-group 170.200.90.26 type ipsec-l2l
tunnel-group 170.200.90.26 ipsec-attributes
 pre-shared-key *****
!
!*****This is your tunnel to Garden City*******
tunnel-group 169.198.90.26 type ipsec-l2l
tunnel-group 169.198.90.26 ipsec-attributes
 pre-shared-key *****
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
!
service-policy global_policy global
prompt hostname context
call-home
```

```
 profile CiscoTAC-1
  no active
  destination address http
https://tools.cisco.com/its/service/oddce/services/DD
CEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly
  subscribe-to-alert-group configuration periodic monthly
  subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:scrubbed
: end


!**********POST Deployment NOC and Security Group will add additional
!security**************




ASA Version 8.3(2)
!
!*********************************!
!Bank of Smithtown Garden City ASA!
!5505 - 2010 AMILABS              !
!*********************************!
!
hostname BOSGCASA
domain-name default.domain.invalid
enable password  encrypted
passwd encrypted
names
!
!*****Interface for local LAN environment****
interface Vlan1
 description BOS GardenCity Branch Local LAN
 nameif inside
 security-level 100
 ip address 169.198.33.25 255.255.255.0
!
!*****Interface for cable ISP Cat 5 ********
interface Vlan2
 description BOS GardenCity Branch Cable ISP backup link
 nameif outside
 security-level 0
 ip address 169.198.90.26 255.255.255.248

!!*** This is where the cable isp cat 5 cable connects to***
interface Ethernet0/0
 switchport access vlan 2
```

```
!
!****This is where you connect the ASA into your local infrastructure
interface Ethernet0/1
!
!
!***The rest of these interfaces can remain down but if used put into
vlan1
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
banner login BOSGCASA
banner login BOS GardenCity ASA
banner motd BOS Gardencity ASA
banner asdm BOS GardenCity ASA
banner asdm BOS GardenCity ASA
boot system disk0:/asa832-k8.bin
ftp mode passive
dns server-group DefaultDNS
 domain-name default.domain.invalid
object-group network obj_any
object-group network NETWORK_OBJ_169.198.33.0_24
object-group network NETWORK_OBJ_169.198.4.0_23
!
!***Access lists to identify traffic that will bring the tunnel up*****
access-list tohaupp extended permit ip 169.198.33.0 255.255.255.0 any
!
snmp-map bos
!
pager lines 24
logging enable
logging buffered informational
logging asdm informational
mtu inside 1500
mtu outside 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-633.bin
no asdm history enable
arp timeout 14400
!
!
!****EIGRP used to tie GC router and ASA together for dynamic path
allocation***
router eigrp 21
 no auto-summary
```

```
 network 10.0.0.0 255.0.0.0
 redistribute static
!
!
!***this route gets you out to the cable path***
route outside 0.0.0.0 0.0.0.0 169.198.90.25 200
!
!
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat
0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect
0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy

!***HTTP enabled for ASDM usage***
https server enable
!
!***Set snmp as same as broadview and GC routers
http 169.198.33.0 255.255.255.0 inside
snmp-server host inside 121.111.60.66 community *****
no snmp-server location
no snmp-server contact
snmp-server community *****
snmp-server enable traps snmp authentication linkup linkdown coldstart

!*** IPSEC and ISAKMP SA information to peer with GC ASA***
crypto ipsec transform-set scrubbed
crypto ipsec transform-set scrubbed
crypto ipsec security-association lifetime seconds
crypto ipsec security-association lifetime kilobytes
crypto map TOHAUPP 1 match address tohaupp
crypto map TOHAUPP 1 set pfs group1
crypto map TOHAUPP 1 set peer 169.198.90.98
crypto map TOHAUPP 1 set transform-set scrubbed
crypto map TOHAUPP interface outside
crypto isakmp enable outside
crypto isakmp policy 10
 authentication pre-share
 encryption scrubbed
 hash sha
 group 2
 lifetime scrubbed
!***very important to keep on prevents NAT from messing up tunnel****
no crypto isakmp nat-traversal
!
telnet timeout 5
ssh timeout 5
console timeout 0
management-access inside
```

```
threat-detection basic-threat
threat-detection statistics host
threat-detection statistics port
threat-detection statistics protocol
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ntp server 169.198.4.1
webvpn
!!****Tunnel policies*****
group-policy DfltGrpPolicy attributes
!**** This was a test tunnel to another branch for scaling***
 vpn-idle-timeout 1
!!*****This is your tunnel to Hauppauge*******
tunnel-group 169.198.90.98 type ipsec-l2l
tunnel-group 169.198.90.98 ipsec-attributes
 pre-shared-key *****
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
!
service-policy global_policy global
prompt hostname context
call-home
 profile CiscoTAC-1
  no active
  destination address http
https://tools.cisco.com/its/service/oddce/services/DD
CEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
```

```
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly
  subscribe-to-alert-group configuration periodic monthly
  subscribe-to-alert-group telemetry periodic daily
Cryptochecksum: scrubbed
: end
BOSGCASA#

!**********POST Deployment NOC and Security Group will add additional
!security**************
```