Rochester Institute of Technology
RIT Scholar Works

Articles

2005

Converged vs. Dedicated IPSec Encryption Testing in Gigabit Ethernet Networks

Luther Troell
Rochester Institute of Technology

Jason Burns
Rochester Institute of Technology

Kurt Chapman
Rochester Institute of Technology

Dave Goddard
Rochester Institute of Technology

Matt Soderlund
Rochester Institute of Technology

See next page for additional authors

Follow this and additional works at: http://scholarworks.rit.edu/article

Recommended Citation
Troell, Luther; Burns, Jason; Chapman, Kurt; Goddard, Dave; Soderlund, Matt; and Ward, Chris, "Converged vs. Dedicated IPSec Encryption Testing in Gigabit Ethernet Networks" (2005). *Technical Report*,Accessed from
http://scholarworks.rit.edu/article/1743

This Technical Report is brought to you for free and open access by RIT Scholar Works. It has been accepted for inclusion in Articles by an authorized administrator of RIT Scholar Works. For more information, please contact ritscholarworks@rit.edu.

Authors
Luther Troell, Jason Burns, Kurt Chapman, Dave Goddard, Matt Soderlund, and Chris Ward

This technical report is available at RIT Scholar Works: http://scholarworks.rit.edu/article/1743

Converged vs. Dedicated IPSec Encryption Testing in Gigabit Ethernet Networks

Luther Troell
Jason Burns
Kurt Chapman
Dave Goddard
Matt Soderlund
Chris Ward

3/8/2014

Table of Contents

Executive Summary

The type of encryption technology to use depends largely on the intended application. A converged, all-in-one solution can be the right choice for some, while a dedicated solution may be a better option for others. In terms of performance, the dedicated SafeNet HA4000 seems well suited to the type of applications where the existing infrastructure does not support a converged solution, and where low latency is key to performance. The Converged Cisco VPN Accelerator is well suited to applications where the existing infrastructure supports adding another module to an existing device, and where latency is less important.

Introduction

Gigabit Ethernet has become an increasingly popular technology used for connecting metropolitan networks as well as carrier networks. While Gigabit Ethernet cannot offer the same degree of reliability as SONET, Gigabit Ethernet offers a considerable price advantage. As a result, it is becoming an increasingly popular solution to connect offices within city limits at high speed.

Unfortunately, tapping into Ethernet networks is relatively trivial. There are numerous open source and commercial software packages that can easily analyze and parse through data passing over Ethernet links. In the case of hospital systems or government offices, this is unacceptable. Highly sensitive data travels through those networks ever day. Many other businesses also have similar security needs.

This reality drives the need for wire speed data encryption. While Gigabit Ethernet links are cheaper than alternatives, they are still considerably expensive. It is in an organization's best interest to ensure that the Gigabit Ethernet link is being fully utilized for data transfer. However, encrypting packets at wire speed is not a trivial task. Encryption is extremely processor intensive. Depending on the combination of software and hardware used, it is expected that the performance of the encryption will vary. In this paper, we will discuss the results of our evaluation of the performance of the converged Cisco IPSec VPN Accelerator blade (WS-SVC-IPSEC-1) and the dedicated SafeNet HA4000.

Purpose

The purpose of this set of tests is to determine the difference in performance between converged and dedicated encryption technology. It can be argued that a standalone device completely dedicated to the task of encryption can perform better at this task than an integrated device that handles many other functions besides encryption. The aim of the test is to put two comparable encryption devices through the same set of tests and analyze the differences in throughput, frame loss, and latency.

Experimental Design

Testing Methodology

We ran a battery of tests according to the methods outlined in RFC 2544. The three areas of interest for our testing were throughput, frame loss, and latency. These tests allowed for a more complete picture of the performance differences across different encryption technologies than using just sheer throughput as a performance indicator. Many technologies today, like VoIP and streaming media, are becoming more sensitive to network latency and frame loss, making these tests valuable as well.

The throughput test is aimed at finding the maximum possible throughput, in frames per second, across a link with absolutely no frame loss. This test runs multiple iterations for each trial. Each trial starts by sending 100% of the link's maximum theoretical throughput. The maximum theoretical throughput is calculated in frames per second for each frame size by taking into account the Ethernet preamble and inter-frame gap to find the actual number of frames minus overhead that can be transmitted. If any frames are dropped at the tested frame rate, the test will run again at a lower throughput using a binary search algorithm. After several iterations the highest possible throughput without frame loss will be discovered. Our tests ran with iterations lasting one minute, with ten trials for each of the following frame sizes in bytes: 64, 128, 256, 512, 1024, 1280, and 1420. We chose the previous frame sizes to give a representative sampling from smallest to largest while ensuring that no fragmentation will occur with the addition of IPSec overhead.

The frame loss test determines what percentage of frames is dropped at a certain level of throughput. The frame loss test starts at 100% maximum theoretical throughput for each trial, and then drops by 10% for each iteration within that trial until no frames are dropped. We ran this test with 10,000,000 frames per iteration and 10 trials for each of the following frame sizes in bytes: 64, 128, 256, 512, 1024, 1280, and 1420. This test works well in conjunction with the throughput tests because it allows us to examine the level of frame loss that can be expected when the bandwidth limits for a link are exceeded. The level of acceptable frame loss will vary depending on the application in use.

The latency test measures the time in nanoseconds needed for a packet leaving one testing interface on the packet generator to enter the receiving testing interface. The packet generator measures this by tagging one frame every second with a time stamp. Because of the way frames are tagged, it is essential that the throughput test be ran first and each latency test is not run above the maximum throughput for that frame size. Frame loss during the latency test would interfere with the results. The latency test was run for one minute per trial, with ten trials for each of the following frame sizes in bytes: 64, 128, 256, 512, 1024, 1280, and 1420. The throughput selected for each test was the maximum throughput previously determined in testing for that combination of frame size and encryption method. In order to make the latency testing comparable between setups we calculated the throughput at which the encryption technology ran for a certain frame size,

and then ran a latency test at the same percentage and frame size on the baseline setup with no encryption. This allows for a comparison of baseline latency to encrypted latency determining the amount of time that is added solely due to encryption.

Topologies

For purposes of comparison, we conducted our tests using a baseline with no encryption, encryption with the Cisco VPN accelerators, and encryption with the SafeNet HA4000s. The baseline topology consisted of two Cisco Catalyst 6509s connected directly to each other with Gigabit Fiber connections (Figure 1). To test the link between the devices we attached an Ixia 400T traffic generator with Gigabit fiber cards to each side of the topology and sent data across the connecting link. Our baseline was ran with no encryption, and default settings throughout the topology. The baseline allowed us to determine the maximum layer 3 switching performance of the Catalyst 6509s. This provides a constant to compare both the SafeNet and Cisco encryption technologies to. Additionally, it verified the Cisco Catalyst could make routing decisions at line speed. The difference in performance data between the baseline test and the encryption tests can then be attributed wholly to the encryption technology in use.

After the baseline tests were completed, we added two SafeNet High Assurance 4000 Gateways in between the link connecting the two Catalyst 6509s (Figure 2). These devices were configured to encrypt traffic coming from the two Ixia subnets on the Catalyst 6509s with 3DES IPSec. We used 3DES with SHA1 for both Phase 1 and Phase 2 IPSec encryption negotiation and set security association lifetimes of one day. One day lifetimes ensured that re-keying would not happen in the middle of a test, adversely affecting the results. The HA4000s acted transparently in the topology, and there was no change necessary on either of the Catalyst 6509s to facilitate this setup.

The HA4000s were tested with two different types of memory. The first tests were run with 800MHz RAM. During the testing, SafeNet upgraded the HA4000 line to use faster 1066MHz RAM. Time constraints limited us to testing only throughput with the faster memory. The frame loss and latency results are derived from the slower 800MHz memory. The results of these tests with the faster RAM are expected to meet or exceed the 800MHz results. Further testing would be needed to confirm this.

In the next set of tests Cisco encryption technology was added to the topology (Figure 1). We used one Cisco WS-SVC-IPSEC-1 VPN accelerator card inside of each Catalyst 6509 chassis to encrypt the traffic flowing from and to the Ixia. We set up crypto maps that encrypted the traffic coming from the two Ixia subnets with 3DES IPSec. We chose a crypto map with a transform set and other encryption variables that exactly matched the HA4000's encryption variables. See the attached Cisco configuration examples in appendix A for more information.

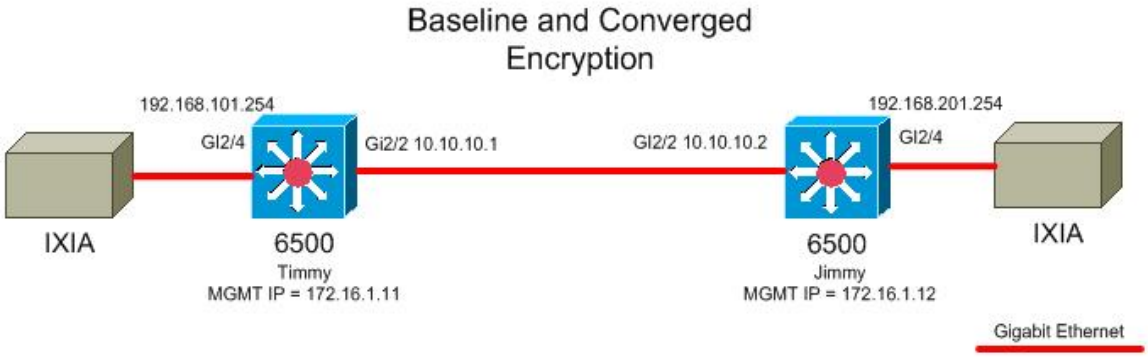

Figure 1

Figure 2

Results

Throughput

Baseline

Throughput in the baseline topology reached 100% of the maximum theoretical limit for all of the tested frame sizes (Figure 3).

HA4000

The HA4000 was able to outperform the Cisco VPN Accelerator at smaller frame sizes and kept pace with the IPSec maximum theoretical throughput at larger frame sizes. There was virtually no difference in throughput between the VPN Accelerator and the HA4000 at larger frame sizes (Figure 3).

WS-SVC-IPSEC-1

The Cisco VPN Accelerator reached a maximum of 96% throughput without dropping any frames. The performance at smaller frame sizes was slightly less than that of the HA4000, and at larger frame sizes the VPN accelerator performed as well as the HA4000 in terms of throughput (Figure 3).

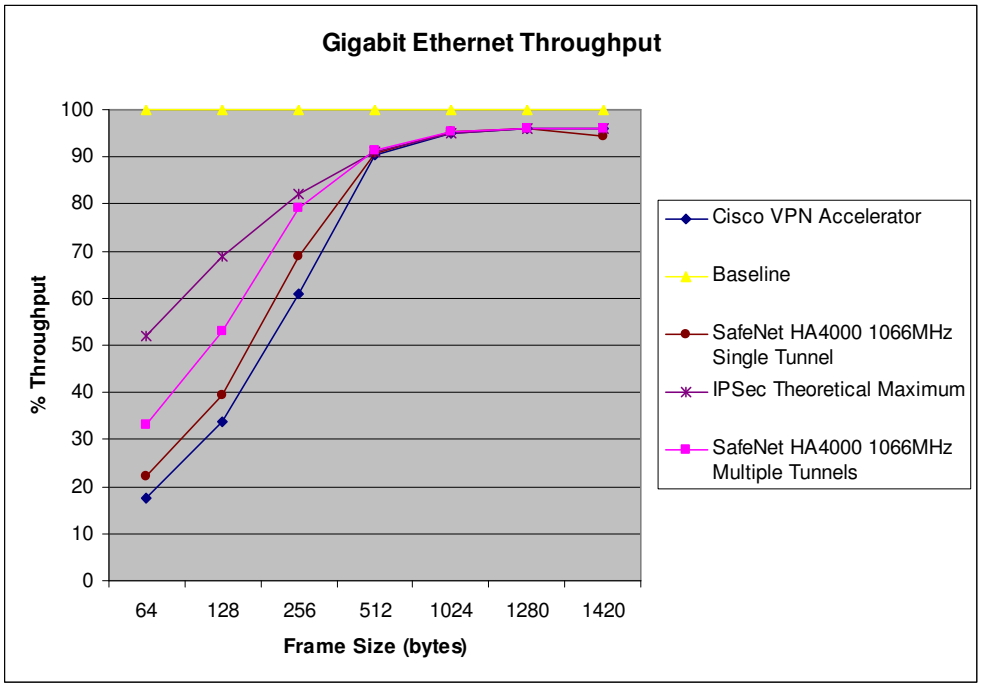

Figure 3

Frame Loss

Baseline

During the baseline testing there were no dropped frames at any of the tested throughputs or frame sizes.

HA4000

The SafeNet HA4000 followed the following frame loss pattern (Figure 4).

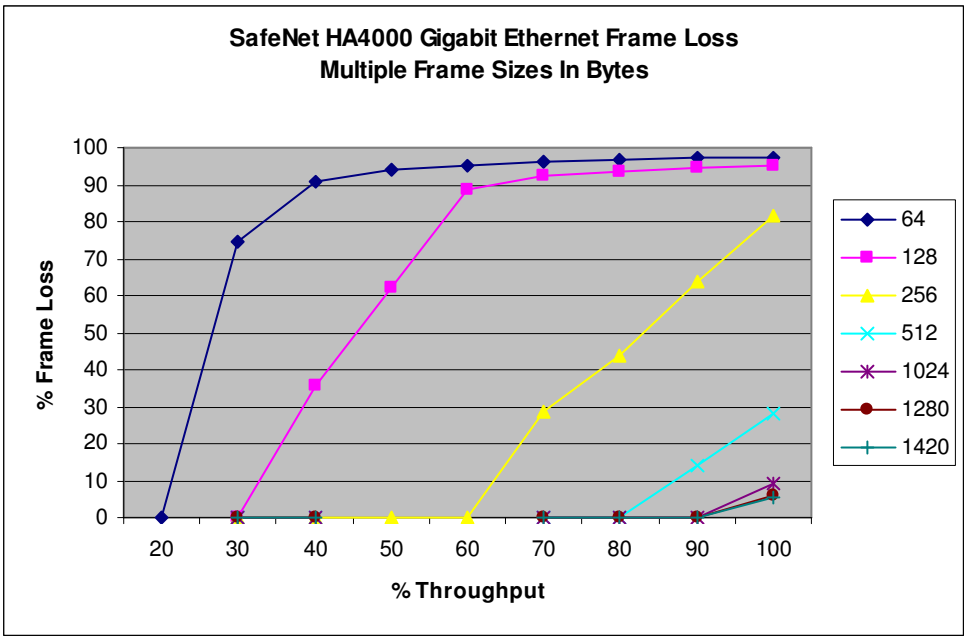

Figure 4

This test shows that when the HA4000 is oversubscribed with smaller frames it starts to drop them rapidly. It drops fewer frames when handling larger frames.

WS-SVC-IPSEC-1

The following graph shows the percentage of frame loss at different frame sizes and throughput levels for the Cisco VPN accelerator (Figure 5).

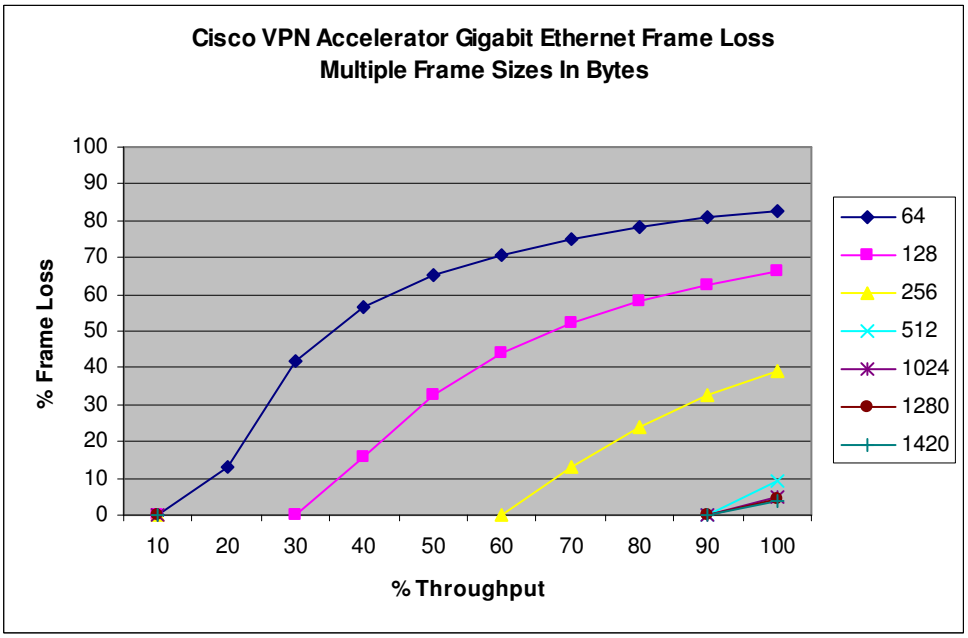

Figure 5

The Cisco VPN accelerator manages well when it is oversubscribed and passes more traffic than the HA4000 in the same overload conditions.

Latency

Baseline

The baseline latency at 100% of traffic throughput reached a maximum of 500,000 nanoseconds with larger frame sizes (Figure 6). Increasing the frame size increased the amount of latency. This level of latency was expected since the devices were forwarding packets at 100% of maximum theoretical throughput.

HA4000

The latency of the SafeNet HA4000 during the testing steadily increased along with frame size, yet remained much lower than the latency of the Cisco VPN accelerator. At smaller frame sizes the HA4000 does exceptionally well (Figure 6).

WS-SVC-IPSEC-1

The Cisco VPN Accelerator added more latency to the topology than the HA4000 encryption device. On average the VPN Accelerator added 100,000 more nanoseconds of latency to the topology than the SafeNet HA4000 (Figure 6).

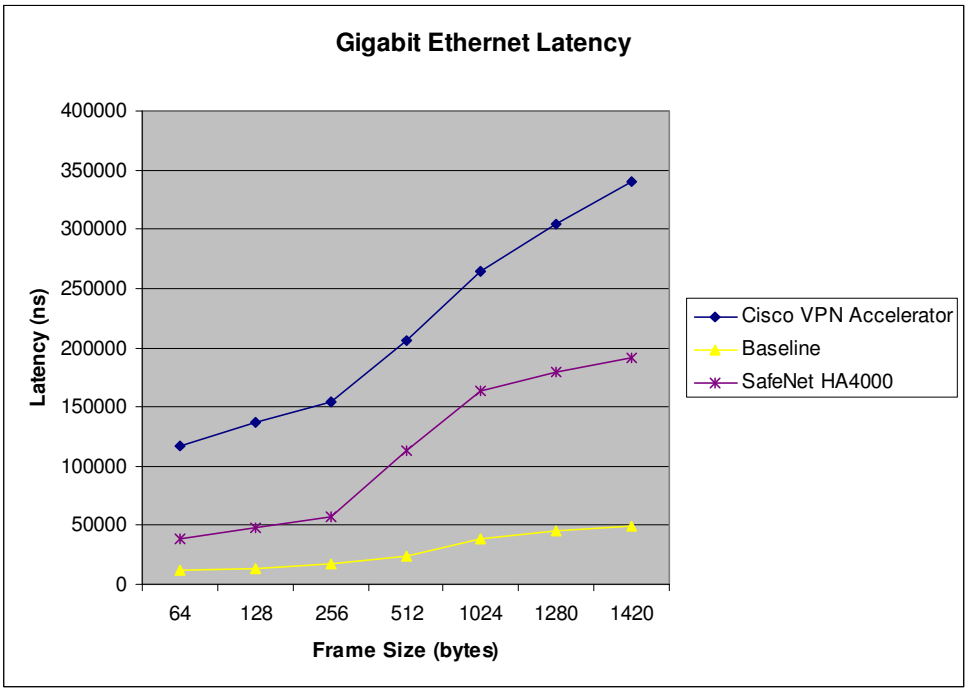

Figure 6

Discussion

Throughput

The maximum throughput of an IPSec link is limited by the amount of overhead IPSec adds. For each packet traversing the encrypted link there is an additional IP header to encapsulate the encrypted IP packet, as well as additional encryption overhead.

In terms of throughput, the Cisco VPN accelerator reached 1.9Gb/s throughput bi-directionally, which is approximately the maximum theoretical throughput with IPSec over a Gigabit link. The HA4000, with 1066 MHz RAM achieved performance at all frame sizes that met or exceeded the level of performance of the Cisco VPN Accelerator. The SafeNet HA4000s were able to perform at even higher throughput by increasing the number of encryption tunnels between the devices. The results with multiple encryption tunnels are displayed as well as the results for only a single tunnel. See appendix B for more information. Unfortunately, time constraints prevented us from testing the Cisco VPN accelerator with multiple encryption tunnels.

The SafeNet HA 4000 with 800MHz RAM followed very closely behind with 1.7Gb/s throughput bi-directionally. This difference in performance is small when average link utilization is considered. The typical link will never see full utilization except under unusual circumstances. In a typical network environment, a link being utilized at levels above 50% to 70% will probably be upgraded, or have some kind of QoS implemented to minimize the bandwidth utilization. Therefore, the maximum bandwidth of the HA4000 with 800MHz RAM is still acceptable in most circumstances.

Frame Loss

When a link becomes over utilized it is important to understand how the device handles the extra traffic delivered to it, but not entirely practical from a real world standpoint. A link reaching its full utilization will probably be upgraded, as mentioned previously.

The Cisco VPN accelerator handled the excess frames better than the HA4000 most likely because of buffer size. Unfortunately, increasing buffer size to minimize frame loss has its drawbacks. This trade-off will be discussed next in latency.

Latency

Latency is one of the most important performance parameters to consider as delay sensitive network applications, such as VoIP, become more prevalent. The SafeNet HA4000 does exceptionally well at minimizing network latency. The Cisco VPN accelerator does well at providing throughput with minimal frame loss, but does so at the cost of added latency. Because the Cisco Catalyst buffers more packets, it takes longer for a packet reaching an interface to be transmitted while under heavy load. In terms of real world applications, the HA4000 would perform well in situations where a high volume of smaller frames were being transmitted that required low consistent latency, like VoIP and streaming applications. The Cisco VPN accelerator would be better suited

to applications needing maximum throughput with larger frame sizes fully utilizing the link, such as secure file transfers and backups between data centers.

Recommendations for Further Research

Performance Under Load

While testing the Cisco VPN accelerator, it would have been helpful to see if performance decreased when the Catalyst 6509 was under normal and heavy loads with traffic unrelated to the encryption. This testing could have provided a helpful real world scenario to better understand the benefits of using a dedicated standalone encryption device versus a converged encryption device.

Multiple Encryption Tunnels

It is possible to run multiple encryption tunnels with each of the devices tested. Our results do not fully address the effects multiple tunnels would have on encryption performance with all devices tested. To further understand how this affects performance we recommend running the previous tests with numerous simultaneous tunnels on both sets of equipment and comparing performance.

Preliminary testing was performed with multiple encryption tunnels on the SafeNet HA4000. See appendix B for additional information.

Encryption Algorithms

The SafeNet HA4000 was capable of performing encryption in AES. Unfortunately the Cisco VPN accelerator was not capable of performing AES encryption. It would have been interesting to test the effects of the encryption algorithm on throughput, frame loss, and latency.

Conclusion

In our testing the dedicated SafeNet HA4000 outperformed the throughput of the converged Cisco VPN Accelerator at smaller frame sizes. Both the converged and dedicated solutions were able to achieve nearly maximum theoretical throughput with IPSec at larger frame sizes. For applications sending smaller frame sizes it can be argued that the HA4000 would be the appropriate choice. The SafeNet HA4000 with 1066 MHz RAM is a better performer in throughput throughout the entire range of frame sizes. The HA4000 is the better performer in terms of throughput and latency: two vital measures of network performance.

The dedicated SafeNet HA4000 was able to significantly beat the converged solution in latency. This makes the HA4000 a good choice for real-time applications that

need low and consistent latency. The Cisco VPN Accelerator added much more latency to the encryption process and data transfer.

The Cisco VPN Accelerator was able to perform well under a heavy load without losing a large number of frames. The HA4000 lost considerably more frames under heavy load. These numbers may only have importance in certain situations, but where a link is going to be saturated, and frame loss is unacceptable, the converged solution could be a better option.

Based on our findings neither the dedicated nor converged solution outperforms in all categories. The type of application can have a significant effect on determining which product will perform best in a certain role.

Acknowledgement

We would like to thank Ixia Corporation for the generous loan of the test generation and measurement equipment used in this study. This consisted of the Ixia 400 chassis, Encryption Load Module, OC-48 PoS Load Module, Ethernet Load Module, and corresponding software (IxCharriot, IxExplorer and IxVPN). The use of these Ixia products provided significant benefit in our test execution and data gathering efforts. It would not have been possible to perform this study in the three-month timeframe without use of this equipment and on-site assistance provided by Ixia. We are deeply appreciative of their support.

Appendix A – Configuration Examples

The following are the Cisco Catalyst 6509 configurations for the different tests. Extraneous material has been omitted from the configurations.

Gigabit Ethernet Baseline and HA4000 Test Configuration

Timmy

```
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
service password-encryption
service counters max age 10
!
hostname timmy
!
boot system flash s72033-pk9sv-mz.122-18.SXD3.bin
enable secret 5 $1$3kha$v7M6Xr2wK9XkbnoqOAMqc/
!
no aaa new-model
clock timezone EST -5
ip subnet-zero
!
!
ip domain-name sonetbonnet.com
ip host jimmy 172.16.1.12
ip host smcmgmt.sonetbonnet.com 172.16.1.23
!
mls ip multicast flow-stat-timer 9
no mls flow ip
no mls flow ipv6
mls cef error action freeze
!
!
power redundancy-mode combined
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
!
redundancy
 mode sso
 main-cpu
  auto-sync running-config
!
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
!
!
interface GigabitEthernet2/1
 no ip address
 shutdown
!
interface GigabitEthernet2/2
 ip address 10.10.20.11 255.255.255.0
```

```
!
interface GigabitEthernet2/3
 no ip address
 shutdown
!
interface GigabitEthernet2/4
 no ip address
 switchport
 switchport access vlan 101
 switchport mode access
!
!
interface FastEthernet3/1
 ip address 172.16.1.11 255.255.255.0
!
!
interface GigabitEthernet5/1
 no ip address
 shutdown
!
interface GigabitEthernet5/2
 no ip address
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan101
 ip address 192.168.101.254 255.255.255.0
!
ip classless
ip route 192.168.201.0 255.255.255.0 10.10.20.12
no ip http server
!
!
!
!
!
control-plane
!
!
!
line con 0
line vty 0 4
 password 7 111A160B120609030A242E30
 login
!
!
ntp clock-period 17181621
ntp server 172.16.1.23
end
```

Jimmy

```
!
version 12.2
service timestamps debug uptime
```

```
service timestamps log uptime
service password-encryption
service counters max age 10
!
hostname timmy
!
boot system flash s72033-pk9sv-mz.122-18.SXD3.bin
enable secret 5 $1$3kha$v7M6Xr2wK9XkbnoqOAMqc/
!
no aaa new-model
clock timezone EST -5
ip subnet-zero
!
!
ip domain-name sonetbonnet.com
ip host jimmy 172.16.1.12
ip host smcmgmt.sonetbonnet.com 172.16.1.23
!
mls ip multicast flow-stat-timer 9
no mls flow ip
no mls flow ipv6
mls cef error action freeze
!
!
power redundancy-mode combined
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
!
redundancy
 mode sso
 main-cpu
  auto-sync running-config
!
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
!
!
interface GigabitEthernet2/1
 no ip address
 shutdown
!
interface GigabitEthernet2/2
 ip address 10.10.20.11 255.255.255.0
!
interface GigabitEthernet2/3
 no ip address
 shutdown
!
interface GigabitEthernet2/4
 no ip address
 switchport
 switchport access vlan 101
 switchport mode access
!
!
interface FastEthernet3/1
 ip address 172.16.1.11 255.255.255.0
!
!
interface GigabitEthernet5/1
```

```
 no ip address
 shutdown
!
interface GigabitEthernet5/2
 no ip address
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan101
 ip address 192.168.101.254 255.255.255.0
!
ip classless
ip route 192.168.201.0 255.255.255.0 10.10.20.12
no ip http server
!
!
!
!
!
control-plane
!
!
!
line con 0
line vty 0 4
 password 7 111A160B120609030A242E30
 login
!
!
ntp clock-period 17181621
ntp server 172.16.1.23
end
```

Gigabit Ethernet IPSec with VPN Acceleration

Timmy

```
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service counters max age 10
!
hostname Timmy
!
boot system flash bootflash:s72033-pk9sv-mz.122-18.SXD3.bin
boot system flash bootflash:
enable secret 5 $1$PFW1$8BBnI3NrSPGbyDOVDiLc9.
!
no aaa new-model
ip subnet-zero
!
!
```

```
ip domain-name sonetbonnet.com
ip host smcmgmt.sonetbonnet.com 172.16.1.23
ip host jimmy 172.16.1.12
!
mls ip multicast flow-stat-timer 9
no mls flow ip
no mls flow ipv6
mls cef error action freeze
!
crypto ca trustpoint smcmgmt.sonetbonnet.com
 enrollment profile timmyCAprofile
 serial-number
 fqdn Timmy.sonetbonnet.com
 ip-address 10.10.10.1
 subject-name C=US, ST=New York, L=Rochester, O=RIT, OU=IT, CN=Timmy
 revocation-check none
 rsakeypair timmykey
!
crypto ca profile enrollment timmyCAprofile
 enrollment url  http://smcmgmt.sonetbonnet.com:80/cgi-bin/pkiclient.exe
!
!
crypto ca certificate chain smcmgmt.sonetbonnet.com
 certificate 1E
  3082028C 308201F5 02011E30 0D06092A 864886F7 0D010105 05003071 310B3009
  06035504 06130255 53311130 0F060355 04081308 4E657720 596F726B 31123010
  06035504 07130952 6F636865 73746572 310C300A 06035504 0A130352 4954310B
  30090603 55040B13 02495431 20301E06 03550403 13174365 72746966 69636174
  696F6E20 41757468 6F726974 79301E17 0D303530 34323231 38343933 305A170D
  33303034 32323138 34393330 5A3081AB 310E300C 06035504 03130554 696D6D79
  310B3009 06035504 0B130249 54310C30 0A060355 040A1303 52495431 12301006
  03550407 1309526F 63686573 74657231 11300F06 03550408 13084E65 7720596F
  726B310B 30090603 55040613 02555331 4A300B06 03550405 13044136 44313017
  06092A86 4886F70D 01090813 0A31302E 31302E31 302E3130 2206092A 864886F7
  0D010902 16155469 6D6D792E 736F6E65 74626F6E 6E65742E 636F6D30 819F300D
  06092A86 4886F70D 01010105 0003818D 00308189 02818100 C6B3651F 3A07E55F
  A1C75663 58D6A809 C1FD58A2 7FD7182C A4EAD83F CF0405ED 0B86BC81 1988085C
  FB6B5AD3 D7A4F040 488E4ED2 221F9FFA 9B6B773B 55BA1717 DCBC8739 CDB6A8D2
  813D63ED EFC2FB81 A2CE33ED 7D16D69C 2C2FB788 9BB0E96B 86B1EC83 6C9EE86F
  C78ADF5A C5E3606B D35650F4 82BF35A6 8054462F 767DAEB5 02030100 01300D06
  092A8648 86F70D01 01050500 03818100 28CB926B 322E719D 334A3CF2 605D0A20
  0FE97667 66810442 33717CA2 3BEE4F2E 7F5317FA 202A7D62 D46E3FBA B39D8D8B
  81746667 F830D63A E5E4FF14 8C412099 316653B4 353E6431 590A7E65 C9C6CED2
  9DA064B0 5BC08682 2D0695D7 890DBAE7 947EBEAA 02C1E15A 7C30E21E 936B7159
  C14C88D1 24012AF0 6D5F3ED3 3BC62598
  quit
 certificate ca 02
  30820251 308201BA 02010230 0D06092A 864886F7 0D010105 05003071 310B3009
  06035504 06130255 53311130 0F060355 04081308 4E657720 596F726B 31123010
  06035504 07130952 6F636865 73746572 310C300A 06035504 0A130352 4954310B
  30090603 55040B13 02495431 20301E06 03550403 13174365 72746966 69636174
  696F6E20 41757468 6F726974 79301E17 0D303530 33313531 37343130 365A170D
  33303033 31353137 34313036 5A307131 0B300906 03550406 13025553 3111300F
  06035504 0813084E 65772059 6F726B31 12301006 03550407 1309526F 63686573
  74657231 0C300A06 0355040A 13035249 54310B30 09060355 040B1302 49543120
  301E0603 55040313 17436572 74696669 63617469 6F6E2041 7574686F 72697479
  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00AB9F12
  59352433 6356CD84 DF59F059 9EAD3A41 DED50FEA 13D08BB9 220A6103 9F27F071
  5E958954 6145EFE1 B5102A55 A9EBF988 C950E4AC 650BA38C 48DF9373 DB420AE8
  E1C381A1 1DDBCBFF 2F85920E 3FCC1EC4 E531C4B1 05100E52 702D0E4D 29681DEE
  9B84D7F1 AF0A973A F1276A94 9E17BF98 1B0C8EF4 38BFB332 C31014FF 71020301
  0001300D 06092A86 4886F70D 01010505 00038181 001F744F DCB6BB42 675BB031
  CFB282AD 3F730210 10431901 4B47F4D7 0612D5B6 62924153 53840C10 664BC757
```

```
  81BF4288 3B4E34C5 A648D8AA 7B3F693C 9B58AA07 A26011AA 0AD93218 4DB59993
  864AB9AE 58402490 F3B433A0 33EE6ED9 74965563 1132752D DBFDA24F C90601CE
  0B1E1691 0AAA83D3 8758F0D7 987FE2DF F9A2C7AD 7D
  quit
!
!
crypto isakmp policy 100
 encr 3des
 group 2
crypto isakmp profile timmyprofile
   ca trust-point smcmgmt.sonetbonnet.com
   match identity address 10.10.10.2 255.255.255.255
!
crypto ipsec security-association lifetime kilobytes 536870912
!
crypto ipsec transform-set set1 esp-3des esp-sha-hmac
!
crypto map toJimmy 10 ipsec-isakmp
 set peer 10.10.10.2
 set transform-set set1
 match address 101
!
!
power redundancy-mode combined
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
!
redundancy
 mode sso
 main-cpu
  auto-sync running-config
!
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
!
interface GigabitEthernet1/1
 no ip address
 flowcontrol receive on
 flowcontrol send off
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,102,1002-1005
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/2
 no ip address
 flowcontrol receive on
 flowcontrol send off
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,1002-1005
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet2/1
 no ip address
 shutdown
!
interface GigabitEthernet2/2
```

```
 no ip address
 crypto connect vlan 102
!
interface GigabitEthernet2/3
 no ip address
 shutdown
!
interface GigabitEthernet2/4
 no ip address
 switchport
 switchport access vlan 101
 switchport mode access
!
!
interface FastEthernet3/1
 no ip address
 switchport
 switchport access vlan 172
 switchport mode access
!
!
interface GigabitEthernet5/1
 no ip address
 shutdown
!
interface GigabitEthernet5/2
 no ip address
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan101
 ip address 192.168.101.254 255.255.255.0
!
interface Vlan102
 ip address 10.10.10.1 255.255.255.0
 crypto map toJimmy
 crypto engine slot 1
!
interface Vlan172
 ip address 172.16.1.11 255.255.255.0
!
ip classless
ip route 192.168.200.0 255.255.255.0 10.10.10.2
ip route 192.168.201.0 255.255.255.0 10.10.10.2
no ip http server
!
!
!
access-list 101 permit ip 192.168.101.0 0.0.0.255 192.168.201.0 0.0.0.255
!
!
!
control-plane
!
!
!
line con 0
line vty 0 4
 password 7 111A160B120609030A242E30
 login
```

```
!
!
end
```

Jimmy

```
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
service password-encryption
service counters max age 10
!
hostname Jimmy
!
boot system bootflash:s72033-pk9sv-mz.122-18.SXD3.bin
boot system bootflash:
enable secret 5 $1$ASW1$CbDspCvW1uQqW6oqmxIYj1
!
no aaa new-model
ip subnet-zero
!
!
ip domain-name sonetbonnet.com
ip host smcmgmt.sonetbonnet.com 172.16.1.23
ip host smcmgmt 172.16.1.23
ip host timmy 172.16.1.11
!
mls ip multicast flow-stat-timer 9
no mls flow ip
no mls flow ipv6
mls cef error action freeze
!
crypto ca trustpoint smcmgmt.sonetbonnet.com
 enrollment profile jimmyCAprofile
 serial-number
 fqdn Jimmy.sonetbonnet.com
 ip-address 10.10.10.2
 subject-name C=US, ST=New York, L=Rochester, O=RIT, OU=IT, CN=Jimmy
 revocation-check none
 rsakeypair jimmykey
!
crypto ca profile enrollment jimmyCAprofile
 enrollment url  http://smcmgmt.sonetbonnet.com:80/cgi-bin/pkiclient.exe
!
!
crypto ca certificate chain smcmgmt.sonetbonnet.com
 certificate 1F
  3082028C 308201F5 02011F30 0D06092A 864886F7 0D010105 05003071 310B3009
  06035504 06130255 53311130 0F060355 04081308 4E657720 596F726B 31123010
  06035504 07130952 6F636865 73746572 310C300A 06035504 0A130352 4954310B
  30090603 55040B13 02495431 20301E06 03550403 13174365 72746966 69636174
  696F6E20 41757468 6F726974 79301E17 0D303530 34323231 38343935 395A170D
  33303034 32323138 34393539 5A3081AB 310E300C 06035504 0313054A 696D6D79
  310B3009 06035504 0B130249 54310C30 0A060355 040A1303 52495431 12301006
  03550407 1309526F 63686573 74657231 11300F06 03550408 13084E65 7720596F
  726B310B 30090603 55040613 02555331 4A300B06 03550405 13043743 39433017
  06092A86 4886F70D 01090813 0A31302E 31302E31 302E3230 2206092A 864886F7
  0D010902 16154A69 6D6D792E 736F6E65 74626F6E 6E65742E 636F6D30 819F300D
  06092A86 4886F70D 01010105 0003818D 00308189 02818100 9ABB9654 74E1E370
  03EEDBB0 F0A72BFF 698A521E 9F3F441D 10DAC4EC 4DE926E4 671AB422 B8C169F3
```

```
  FD76F3A6 D1D852A7 15D39DAF BEF03287 EAF51320 8A477AB2 DE9E32A6 B71F128A
  B0A3943A 4BD44606 5ED3D1AC 85A99920 C6F41B50 C76FB905 DEBE8ABF BDDB267B
  A46EEA2E 93E8FF34 A5F2C331 E9E67688 BAB4B276 5E0DC615 02030100 01300D06
  092A8648 86F70D01 01050500 03818100 1D0047E7 894D3596 4DDDB1DC 5A549EB2
  3785FE1D 11E368DA 4A12228F 49BC8658 20030C5E DA4CBFCB C7C30D1B F351B31F
  6C0AE20F 9CBD4D53 119E243F C72A6A00 CA3E5EEA 5CC70446 EF6E71AA 63E092ED
  4BEAD927 C3A10A05 B8C6ABA6 6201BFA0 046AEB61 F429BAEE 5F536E5B 9E278B9B
  CA922967 D10E8342 E6863B20 6B9BD3C5
  quit
 certificate ca 02
  30820251 308201BA 02010230 0D06092A 864886F7 0D010105 05003071 310B3009
  06035504 06130255 53311130 0F060355 04081308 4E657720 596F726B 31123010
  06035504 07130952 6F636865 73746572 310C300A 06035504 0A130352 4954310B
  30090603 55040B13 02495431 20301E06 03550403 13174365 72746966 69636174
  696F6E20 41757468 6F726974 79301E17 0D303530 33313531 37343130 365A170D
  33303033 31353137 34313036 5A307131 0B300906 03550406 13025553 3111300F
  06035504 0813084E 65772059 6F726B31 12301006 03550407 1309526F 63686573
  74657231 0C300A06 0355040A 13035249 54310B30 09060355 040B1302 49543120
  301E0603 55040313 17436572 74696669 63617469 6F6E2041 7574686F 72697479
  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00AB9F12
  59352433 6356CD84 DF59F059 9EAD3A41 DED50FEA 13D08BB9 220A6103 9F27F071
  5E958954 6145EFE1 B5102A55 A9EBF988 C950E4AC 650BA38C 48DF9373 DB420AE8
  E1C381A1 1DDBCBFF 2F85920E 3FCC1EC4 E531C4B1 05100E52 702D0E4D 29681DEE
  9B84D7F1 AF0A973A F1276A94 9E17BF98 1B0C8EF4 38BFB332 C31014FF 71020301
  0001300D 06092A86 4886F70D 01010505 00038181 001F744F DCB6BB42 675BB031
  CFB282AD 3F730210 10431901 4B47F4D7 0612D5B6 62924153 53840C10 664BC757
  81BF4288 3B4E34C5 A648D8AA 7B3F693C 9B58AA07 A26011AA 0AD93218 4DB59993
  864AB9AE 58402490 F3B433A0 33EE6ED9 74965563 1132752D DBFDA24F C90601CE
  0B1E1691 0AAA83D3 8758F0D7 987FE2DF F9A2C7AD 7D
  quit
!
!
crypto isakmp policy 100
 encr 3des
 group 2
crypto isakmp profile jimmyprofile
   ca trust-point smcmgmt.sonetbonnet.com
   match identity address 10.10.10.1 255.255.255.255
!
crypto ipsec security-association lifetime kilobytes 536870912
!
crypto ipsec transform-set set1 esp-3des esp-sha-hmac
!
crypto map toTimmy 10 ipsec-isakmp
 set peer 10.10.10.1
 set transform-set set1
 match address 101
!
!
power redundancy-mode combined
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
!
redundancy
 mode sso
 main-cpu
  auto-sync running-config
!
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
```

```
!
interface GigabitEthernet1/1
 no ip address
 flowcontrol receive on
 flowcontrol send off
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,102,1002-1005
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/2
 no ip address
 flowcontrol receive on
 flowcontrol send off
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,1002-1005
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet2/1
 no ip address
 shutdown
!
interface GigabitEthernet2/2
 no ip address
 crypto connect vlan 102
!
interface GigabitEthernet2/3
 no ip address
 shutdown
!
interface GigabitEthernet2/4
 no ip address
 switchport
 switchport access vlan 201
 switchport mode access
!
interface FastEthernet3/1
 no ip address
 switchport
 switchport access vlan 172
 switchport mode access
!
!
interface GigabitEthernet5/1
 no ip address
 shutdown
!
interface GigabitEthernet5/2
 no ip address
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan102
 ip address 10.10.10.2 255.255.255.0
 crypto map toTimmy
 crypto engine slot 1
!
```

```
interface Vlan172
 ip address 172.16.1.12 255.255.255.0
!
interface Vlan201
 ip address 192.168.201.254 255.255.255.0
!
ip classless
ip route 192.168.101.0 255.255.255.0 10.10.10.1
no ip http server
!
!
!
access-list 101 permit ip 192.168.201.0 0.0.0.255 192.168.101.0 0.0.0.255
!
!
!
control-plane
!
!
!
line con 0
line vty 0 4
 password 7 1316181C0E180625252A2D27
 login
!
!
end
```

Gigabit Ethernet IPSec without VPN Accelerator

Timmy

```
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service counters max age 10
!
hostname Timmy
!
boot system flash bootflash:s72033-pk9sv-mz.122-18.SXD3.bin
boot system flash bootflash:
enable secret 5 $1$PFW1$8BBnI3NrSPGbyDOVDiLc9.
!
no aaa new-model
ip subnet-zero
!
!
ip domain-name sonetbonnet.com
ip host smcmgmt.sonetbonnet.com 172.16.1.23
ip host jimmy 172.16.1.12
!
mls ip multicast flow-stat-timer 9
no mls flow ip
no mls flow ipv6
mls cef error action freeze
!
crypto ca trustpoint smcmgmt.sonetbonnet.com
 enrollment profile timmyCAprofile
```

```
 serial-number
 fqdn Timmy.sonetbonnet.com
 ip-address 10.10.10.1
 subject-name C=US, ST=New York, L=Rochester, O=RIT, OU=IT, CN=Timmy
 revocation-check none
 rsakeypair timmykey
!
crypto ca profile enrollment timmyCAprofile
 enrollment url  http://smcmgmt.sonetbonnet.com:80/cgi-bin/pkiclient.exe
!
!
crypto ca certificate chain smcmgmt.sonetbonnet.com
 certificate 1E
  3082028C 308201F5 02011E30 0D06092A 864886F7 0D010105 05003071 310B3009
  06035504 06130255 53311130 0F060355 04081308 4E657720 596F726B 31123010
  06035504 07130952 6F636865 73746572 310C300A 06035504 0A130352 4954310B
  30090603 55040B13 02495431 20301E06 03550403 13174365 72746966 69636174
  696F6E20 41757468 6F726974 79301E17 0D303530 34323231 38343933 305A170D
  33303034 32323138 34393330 5A3081AB 310E300C 06035504 03130554 696D6D79
  310B3009 06035504 0B130249 54310C30 0A060355 040A1303 52495431 12301006
  03550407 1309526F 63686573 74657231 11300F06 03550408 13084E65 7720596F
  726B310B 30090603 55040613 02555331 4A300B06 03550405 13044136 44313017
  06092A86 4886F70D 01090813 0A31302E 31302E31 302E3130 2206092A 864886F7
  0D010902 16155469 6D6D792E 736F6E65 74626F6E 6E65742E 636F6D30 819F300D
  06092A86 4886F70D 01010105 0003818D 00308189 02818100 C6B3651F 3A07E55F
  A1C75663 58D6A809 C1FD58A2 7FD7182C A4EAD83F CF0405ED 0B86BC81 1988085C
  FB6B5AD3 D7A4F040 488E4ED2 221F9FFA 9B6B773B 55BA1717 DCBC8739 CDB6A8D2
  813D63ED EFC2FB81 A2CE33ED 7D16D69C 2C2FB788 9BB0E96B 86B1EC83 6C9EE86F
  C78ADF5A C5E3606B D35650F4 82BF35A6 8054462F 767DAEB5 02030100 01300D06
  092A8648 86F70D01 01050500 03818100 28CB926B 322E719D 334A3CF2 605D0A20
  0FE97667 66810442 33717CA2 3BEE4F2E 7F5317FA 202A7D62 D46E3FBA B39D8D8B
  81746667 F830D63A E5E4FF14 8C412099 316653B4 353E6431 590A7E65 C9C6CED2
  9DA064B0 5BC08682 2D0695D7 890DBAE7 947EBEAA 02C1E15A 7C30E21E 936B7159
  C14C88D1 24012AF0 6D5F3ED3 3BC62598
  quit
 certificate ca 02
  30820251 308201BA 02010230 0D06092A 864886F7 0D010105 05003071 310B3009
  06035504 06130255 53311130 0F060355 04081308 4E657720 596F726B 31123010
  06035504 07130952 6F636865 73746572 310C300A 06035504 0A130352 4954310B
  30090603 55040B13 02495431 20301E06 03550403 13174365 72746966 69636174
  696F6E20 41757468 6F726974 79301E17 0D303530 33313531 37343130 365A170D
  33303033 31353137 34313036 5A307131 0B300906 03550406 13025553 3111300F
  06035504 0813084E 65772059 6F726B31 12301006 03550407 1309526F 63686573
  74657231 0C300A06 0355040A 13035249 54310B30 09060355 040B1302 49543120
  301E0603 55040313 17436572 74696669 63617469 6F6E2041 7574686F 72697479
  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00AB9F12
  59352433 6356CD84 DF59F059 9EAD3A41 DED50FEA 13D08BB9 220A6103 9F27F071
  5E958954 6145EFE1 B5102A55 A9EBF988 C950E4AC 650BA38C 48DF9373 DB420AE8
  E1C381A1 1DDBCBFF 2F85920E 3FCC1EC4 E531C4B1 05100E52 702D0E4D 29681DEE
  9B84D7F1 AF0A973A F1276A94 9E17BF98 1B0C8EF4 38BFB332 C31014FF 71020301
  0001300D 06092A86 4886F70D 01010505 00038181 001F744F DCB6BB42 675BB031
  CFB282AD 3F730210 10431901 4B47F4D7 0612D5B6 62924153 53840C10 664BC757
  81BF4288 3B4E34C5 A648D8AA 7B3F693C 9B58AA07 A26011AA 0AD93218 4DB59993
  864AB9AE 58402490 F3B433A0 33EE6ED9 74965563 1132752D DBFDA24F C90601CE
  0B1E1691 0AAA83D3 8758F0D7 987FE2DF F9A2C7AD 7D
  quit
!
!
crypto isakmp policy 100
 encr 3des
 group 2
crypto isakmp profile timmyprofile
   ca trust-point smcmgmt.sonetbonnet.com
```

```
   match identity address 10.10.10.2 255.255.255.255
!
crypto ipsec security-association lifetime kilobytes 536870912
!
crypto ipsec transform-set set1 esp-3des esp-sha-hmac
!
crypto map toJimmy 10 ipsec-isakmp
 set peer 10.10.10.2
 set transform-set set1
 match address 101
!
!
power redundancy-mode combined
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
!
redundancy
 mode sso
 main-cpu
  auto-sync running-config
!
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
!
interface GigabitEthernet2/1
 no ip address
 shutdown
!
interface GigabitEthernet2/2
 no ip address
 switchport
 switchport access vlan 102
 switchport mode access
!
interface GigabitEthernet2/3
 no ip address
 shutdown
!
interface GigabitEthernet2/4
 no ip address
 switchport
 switchport access vlan 101
 switchport mode access
!
interface FastEthernet3/1
 no ip address
 switchport
 switchport access vlan 172
 switchport mode access
!
!
interface GigabitEthernet5/1
 no ip address
 shutdown
!
interface GigabitEthernet5/2
 no ip address
 shutdown
!
interface Vlan1
```

```
 no ip address
 shutdown
!
interface Vlan101
 ip address 192.168.101.254 255.255.255.0
!
interface Vlan102
 ip address 10.10.10.1 255.255.255.0
 crypto map toJimmy
!
interface Vlan172
 ip address 172.16.1.11 255.255.255.0
!
ip classless
ip route 192.168.201.0 255.255.255.0 10.10.10.2
no ip http server
!
!
!
access-list 101 permit ip 192.168.101.0 0.0.0.255 192.168.201.0 0.0.0.255
!
!
!
control-plane
!
!
!
line con 0
line vty 0 4
 password 7 111A160B120609030A242E30
 login
!
end
```

Jimmy

```
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
service password-encryption
service counters max age 10
!
hostname Jimmy
!
boot system bootflash:s72033-pk9sv-mz.122-18.SXD3.bin
boot system bootflash:
enable secret 5 $1$ASW1$CbDspCvW1uQqW6oqmxIYj1
!
no aaa new-model
ip subnet-zero
!
!
ip domain-name sonetbonnet.com
ip host smcmgmt.sonetbonnet.com 172.16.1.23
ip host timmy 172.16.1.11
!
mls ip multicast flow-stat-timer 9
no mls flow ip
no mls flow ipv6
mls cef error action freeze
!
```

```
crypto ca trustpoint smcmgmt.sonetbonnet.com
 enrollment profile jimmyCAprofile
 serial-number
 fqdn Jimmy.sonetbonnet.com
 ip-address 10.10.10.2
 subject-name C=US, ST=New York, L=Rochester, O=RIT, OU=IT, CN=Jimmy
 revocation-check none
 rsakeypair jimmykey
!
crypto ca profile enrollment jimmyCAprofile
 enrollment url  http://smcmgmt.sonetbonnet.com:80/cgi-bin/pkiclient.exe
!
!
crypto ca certificate chain smcmgmt.sonetbonnet.com
 certificate 1F
  3082028C 308201F5 02011F30 0D06092A 864886F7 0D010105 05003071 310B3009
  06035504 06130255 53311130 0F060355 04081308 4E657720 596F726B 31123010
  06035504 07130952 6F636865 73746572 310C300A 06035504 0A130352 4954310B
  30090603 55040B13 02495431 20301E06 03550403 13174365 72746966 69636174
  696F6E20 41757468 6F726974 79301E17 0D303530 34323231 38343935 395A170D
  33303034 32323138 34393539 5A3081AB 310E300C 06035504 0313054A 696D6D79
  310B3009 06035504 0B130249 54310C30 0A060355 040A1303 52495431 12301006
  03550407 1309526F 63686573 74657231 11300F06 03550408 13084E65 7720596F
  726B310B 30090603 55040613 02555331 4A300B06 03550405 13043743 39433017
  06092A86 4886F70D 01090813 0A31302E 31302E31 302E3230 2206092A 864886F7
  0D010902 16154A69 6D6D792E 736F6E65 74626F6E 6E65742E 636F6D30 819F300D
  06092A86 4886F70D 01010105 0003818D 00308189 02818100 9ABB9654 74E1E370
  03EEDBB0 F0A72BFF 698A521E 9F3F441D 10DAC4EC 4DE926E4 671AB422 B8C169F3
  FD76F3A6 D1D852A7 15D39DAF BEF03287 EAF51320 8A477AB2 DE9E32A6 B71F128A
  B0A3943A 4BD44606 5ED3D1AC 85A99920 C6F41B50 C76FB905 DEBE8ABF BDDB267B
  A46EEA2E 93E8FF34 A5F2C331 E9E67688 BAB4B276 5E0DC615 02030100 01300D06
  092A8648 86F70D01 01050500 03818100 1D0047E7 894D3596 4DDDB1DC 5A549EB2
  3785FE1D 11E368DA 4A12228F 49BC8658 20030C5E DA4CBFCB C7C30D1B F351B31F
  6C0AE20F 9CBD4D53 119E243F C72A6A00 CA3E5EEA 5CC70446 EF6E71AA 63E092ED
  4BEAD927 C3A10A05 B8C6ABA6 6201BFA0 046AEB61 F429BAEE 5F536E5B 9E278B9B
  CA922967 D10E8342 E6863B20 6B9BD3C5
  quit
 certificate ca 02
  30820251 308201BA 02010230 0D06092A 864886F7 0D010105 05003071 310B3009
  06035504 06130255 53311130 0F060355 04081308 4E657720 596F726B 31123010
  06035504 07130952 6F636865 73746572 310C300A 06035504 0A130352 4954310B
  30090603 55040B13 02495431 20301E06 03550403 13174365 72746966 69636174
  696F6E20 41757468 6F726974 79301E17 0D303530 33313531 37343130 365A170D
  33303033 31353137 34313036 5A307131 0B300906 03550406 13025553 3111300F
  06035504 0813084E 65772059 6F726B31 12301006 03550407 1309526F 63686573
  74657231 0C300A06 0355040A 13035249 54310B30 09060355 040B1302 49543120
  301E0603 55040313 17436572 74696669 63617469 6F6E2041 7574686F 72697479
  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00AB9F12
  59352433 6356CD84 DF59F059 9EAD3A41 DED50FEA 13D08BB9 220A6103 9F27F071
  5E958954 6145EFE1 B5102A55 A9EBF988 C950E4AC 650BA38C 48DF9373 DB420AE8
  E1C381A1 1DDBCBFF 2F85920E 3FCC1EC4 E531C4B1 05100E52 702D0E4D 29681DEE
  9B84D7F1 AF0A973A F1276A94 9E17BF98 1B0C8EF4 38BFB332 C31014FF 71020301
  0001300D 06092A86 4886F70D 01010505 00038181 001F744F DCB6BB42 675BB031
  CFB282AD 3F730210 10431901 4B47F4D7 0612D5B6 62924153 53840C10 664BC757
  81BF4288 3B4E34C5 A648D8AA 7B3F693C 9B58AA07 A26011AA 0AD93218 4DB59993
  864AB9AE 58402490 F3B433A0 33EE6ED9 74965563 1132752D DBFDA24F C90601CE
  0B1E1691 0AAA83D3 8758F0D7 987FE2DF F9A2C7AD 7D
  quit
!
!
crypto isakmp policy 100
 encr 3des
 group 2
```

```
crypto isakmp profile jimmyprofile
   ca trust-point smcmgmt.sonetbonnet.com
   match identity address 10.10.10.1 255.255.255.255
!
crypto ipsec security-association lifetime kilobytes 536870912
!
crypto ipsec transform-set set1 esp-3des esp-sha-hmac
!
crypto map toTimmy 10 ipsec-isakmp
 set peer 10.10.10.1
 set transform-set set1
 match address 101
!
!
power redundancy-mode combined
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
!
redundancy
 mode sso
 main-cpu
  auto-sync running-config
!
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
!
interface GigabitEthernet2/1
 no ip address
 shutdown
!
interface GigabitEthernet2/2
 no ip address
 switchport
 switchport access vlan 102
 switchport mode access
!
interface GigabitEthernet2/3
 no ip address
 shutdown
!
interface GigabitEthernet2/4
 no ip address
 switchport
 switchport access vlan 201
 switchport mode access
!
interface FastEthernet3/1
 no ip address
 switchport
 switchport access vlan 172
 switchport mode access
!
!
interface GigabitEthernet5/1
 no ip address
 shutdown
!
interface GigabitEthernet5/2
 no ip address
 shutdown
```

```
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan102
 ip address 10.10.10.2 255.255.255.0
 crypto map toTimmy
!
interface Vlan172
 ip address 172.16.1.12 255.255.255.0
!
interface Vlan201
 ip address 192.168.201.254 255.255.255.0
!
ip classless
ip route 192.168.101.0 255.255.255.0 10.10.10.1
no ip http server
!
!
!
access-list 101 permit ip 192.168.201.0 0.0.0.255 192.168.101.0 0.0.0.255
!
!
!
control-plane
!
!
!
line con 0
line vty 0 4
 password 7 1316181C0E180625252A2D27
 login
!
end
```

Appendix B – Multiple Encryption Tunnels

Adding multiple encryption tunnels to the HA4000 did have a positive impact on performance (Figure 7). This test was run with four Security Associations on each HA4000. We created an additional subnet on each of the Ixia testing devices and sent traffic from each subnet over the HA4000 in its own IPSec tunnel. A total of four tunnels were created: one for each subnet in each direction.

Running these same tests with the addition of 1066MHz RAM to the HA4000s showed a dramatic increase in performance at smaller frame sizes. Additional testing would be needed to test the effect of multiple tunnels on the Cisco VPN Accelerator.

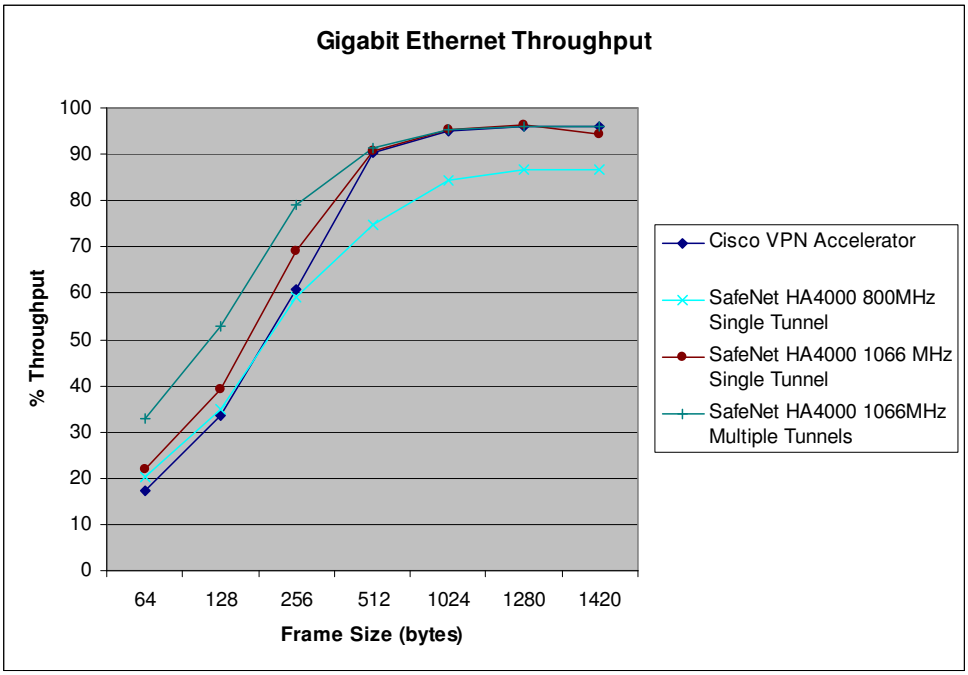

Figure 7