Regis University
ePublications at Regis University

All Regis University Theses

Spring 2010

Simultaneous Implementation Of Ssl And Ipsec Protocols For Remote Vpn Connection

Deyan Mihaylov
Regis University

Recommended Citation

Mihaylov, Deyan, "Simultaneous Implementation Of Ssl And Ipsec Protocols For Remote Vpn Connection" (2010). *All Regis University Theses*. 745.
https://epublications.regis.edu/theses/745

SIMULTANEOUS IMPLEMENTATION OF SSL AND IPSEC PROTOCOLS FOR REMOTE VPN CONNECTION

A THESIS

SUBMITTED ON 28 OF FEBRUARY, 2011

TO THE DEPARTMENT OF INFORMATION TECHNOLOGY

OF THE SCHOOL OF COMPUTER & INFORMATION SCIENCES

OF REGIS UNIVERSITY

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS OF MASTER OF SCIENCE IN SYSTEMS ENGINEERING

BY

Deyan Mihaylov

APPROVALS

Robert Sjodin

Robert Sjodin, Thesis Advisor

James A Lupo

James A Lupo

Stephen D. Barnes

Abstract

A Virtual Private Network is a wide spread technology for connecting remote users and locations to the main core network. It has number of benefits such as cost-efficiency and security. SSL and IPSec are the most popular VPN protocols employed by large number of organizations. Each protocol has its benefits and disadvantages. Simultaneous SSL and IPSec implementation delivers efficient and flexible solution for companies' with heterogeneous remote connection needs. On the other hand, employing two different VPN technologies opens questions about compatibility, performance, and drawbacks especially if they are utilized by one network device.

The study examines the behavior of the two VPN protocols implemented in one edge network device, ASA 5510 security appliance. It follows the configuration process as well as the effect of the VPN protocols on the ASA performance including routing functions, firewall access lists, and network address translation abilities. The paper also presents the cost effect and the maintenance requirements for utilizing SSL and IPSec in one edge network security device.

Acknowledgements

I would like to thank the management of the Roaring Fork Club for letting me use their computer network environment. Without their generous support the research project would not be able to collect data from real production network and support the thesis statement with actual real-time data.

I would also like to express my gratitude to two people without whom the study would not be possible:

Shannon Fink, IT manager of the Roaring Fork Club. He consistently guided me through the VPN configuration process and network performance analysis in accordance with the peculiarity of club's network.

Robert Sjodin, the Department of Information Technologies in Regis University. As a thesis advisor he systematically walked me through the whole process starting with the thesis proposal to the final approval of the research paper.

Table of Contents

List of Figures

List of Tables

Chapter 1 – Introduction

A Virtual Private Network (VPN) is a set of technologies that extend an organization's private network to include remote offices, business partners, telecommuters, and mobile workers. It is an IP-based model that uses encryption and tunneling over a public network (Internet) to connect securely remote users and branch offices to their corporate network. A VPN connection can be presented as a pipe carrying encapsulated private data through a public network.

Travelling agents, home workers, and several remote offices is a common scenario for large businesses. To communicate and perform in efficient way all these remote sites need a connection to the main network. Moreover, they need to communicate in secure and confidential manner. VPN has several advantages over the competitive options such as leased lines and Dial-ups. It is considerably more cost-effective than a leased line although it cannot offer the same low latency and line capacity. It depends on a business needs whether to use VPN or leased line. Compared to Dial-up, VPN is more cost-effective and a more secure way to connect remote users. As Diab et al. (2007) state in their paper, VPN is considered the strongest security solution for remote communications over the Internet. It includes cryptographic protocols to assure confidentiality of data, authentication and authorization procedures to identify users, and message control to provide integrity of data.

To make the decision to implement VPN as a remote communication technology is the first and the easiest step preceding numerous consideration and issues to be solved. There are several questions that need answers before starting a VPN deployment. What are the various types of VPN available? Which one best fits the corporate network remote access requirements? How does it affect application performance when they are accessed remotely? Is one VPN technology able to fulfill all the company's various requirements for remote connection? The answer of the last question is the motivation behind the research in this paper.

IPSec satisfies the permanent, always-on VPN access requirement. It provides access to all network resources including VoIP through a single log-in. Corporation offices need full-service and secure network access available on the IPSec tunnel. Moreover, all servers and clients are part of the business network and they can be managed, configured, and maintained by the corporate IT department. SSL, on the other hand, is suitable for mobile workers that need occasional, on-demand access to the main network resources usually through public terminals. SSL is logical solution for business partners and customers who are out of reach of the IT staff. Simple browser with SSL capabilities is enough for their network access needs.

Both IPSec and SSL have their advantages and limitations. They are effective, standardized, and secure choices for granting remote access. Simultaneous implementation can grant scalability of access levels and flexibility for IT administrators to effectively manage the different levels of remote connections.

IPSec and SSL VPNs can be implemented with software installed on a server acting as a gateway or as hardware modules included or separately added to edge routers. IPSec modules have been part of most commercial routers for years. To address the growing popularity of SSL VPN and the cost issues associated with both technologies deployed in one network, manufacturers release devices that include SSL in addition to IPSec VPN making simultaneous implementation easier and more affordable. Leaders in network technologies like Cisco and Netgear are the first to offer such products on the market. Utilizing both protocols in one device is a new approach that opens questions about SSL and IPSec VPNs working simultaneously in one edge router. The study intends to explore the behavior of an edge security appliance that includes VPN modules. IPSec and SSL VPN technologies can be enabled and configured in one edge router without causing network performance issues or creating conflicts in router configuration.

Chapter 2 – Review of Literature and Research Objectives

The literature available for IPSec and SSL VPN protocols is fairly large, but it is not in the subject of both technologies working simultaneously in one edge network device. There are numerous articles and research papers considering which protocol is suitable for certain situation and what are the security issues applicable for each VPN technology. There are number of papers that discuss the benefits of mix-and-match various protocols but they do not go in details of how they work together and what the possible issues are when these protocols are implemented in the same computer network.

Martin Heller (2006) follows the path of VPNs from their beginning as trusted networks (leased lines) to today's secure private lines over public packed-switched network, the Internet. He describes several VPN protocols such as L2TP, IPSec, IPSec over L2TP, SSL, TLS as well as the benefits and the security risks they expose. Heller defines two problems in combining two different VPN technologies. First, he states that combining the use of two VPN technologies simultaneously can expose the company's network to the outside world and make it vulnerable to intruders. Second, there is an issue that comes from the network address translation (NAT) technology. SSL/TLS can work and should work through NAT-based firewall while site-to-site IPSec should bypass the NAT translation. Since the study proposes the use of IPSec and SSL in one front edge device (edge router) both protocols will be filtered through the same firewall making the issue significant for the research.

Frankel et al. (2008) from the National Institute of Standards and Technology provides a detailed guide to SSL VPNs including explanation of every step from identifying the needs of

VPN to deployment and management of the virtual network. The authors suggest that a company should produce technical documentation in the deployment phase to address the following issues:

1. Encrypted traffic can affect firewalls, IDS (intrusion detection system), QoS (quality of service), and congestion control.
2. Access policies may block SSL traffic in firewalls and routers.
3. Unexpected performance issues may arise from the overhead of the SSL packets.

The paper includes a case study in which a company implements a SSL VPN appliance while at the same time leaves IPSec tunnels to some of its remote resources. The study does not consider any impact of SSL on the IPSec performance and configuration. On the other hand, the issues above suggest the opposite as the IPSec traffic is filtered by the same firewalls and access policies which have to distinguish between the two protocols. Frankel et al. (2008) as well as the National Webcast Initiative (2005) consider IPSec and SSL to be complimentary VPN technologies but do not provide any details of how they can be implemented simultaneously.

As most of the articles about SSL and IPSec, Michael Daye Jr. (2007) compares the two protocols based on several different parameters: encryption, accessibility, complexity, scalability, cost, and so on. He concludes that each VPN has its strengths and weaknesses and using SSL or IPSec depends on a certain scenario. He mentions that deploying both of them is possible but the cost factor puts only one of them in favor over the other. Arif Basha (2005) presents a cost comparison in his article that claims that the cost is equal for an organization with 100 users or more. The cost factor is very important and it presents the non-technical side of the two VPN technologies working simultaneously. Cost considerations explained in the articles are not an issue on the market today as most of the network equipment vendors include SSL and IPSec modules in their network gear. Another point that Basha mentions is the maintenance and use factors. He states that SSL VPN is significantly ahead of IPSec in that aspect as it requires less time for maintenance and support from the network administrator. The study includes the maintenance factor as one of the parameters to be explored.

The study on SSL and IPSec simultaneous implementation takes place in small country club that uses Cisco network equipment and specifically Cisco ASA5510 VPN edition edge router. Cisco is one of the leaders in providing network solutions. Heary (2009) presents a comparison between top vendors in several different areas. The statistics in his article are based on Infonetics Network IDS/IPS Market Share Q3 CY’09. Cisco takes third position in the SSL VPN market after Juniper and Checkpoint. On the other hand, the company is a leader in Intrusion Prevention Systems (IPS), Security Appliances, and Integrated Security (i.e. secure routers). The results provided by Infonetics confirm the presence of Cisco products in large number of business networks worldwide meaning the study can have positive and informative effect in the VPN community.

Cisco introduces ASA 5500 Series SSL/IPSec VPN edition in their Web page as a single platform that delivers customizable, simple, and flexible VPN solution that eliminate the cost of deploying multiple, parallel remote-access connections. It offers client and clientless VPN as well as the standard routing and firewall capabilities. Richard Deal (2005) compares the ASA 5500 capabilities to the other Cisco VPN options like Cisco VPN 3000 concentrators and IOS-based routers. ASA and respectively PIX series have been designed for network address translation (NAS) and they can handle complex translation polices such as bidirectional NAT on multi-interfaced router. Stateful firewall services are main strength of the ASA appliance. It includes application layer inspection in addition to the basic firewall filtering.

The following table presents features of Cisco ASA5510 and ASA5505 which are used in the study.

Table 2.1. *Specifications of Cisco ASA 5505 and ASA 5510 Security Appliance Models*

Platform	Cisco ASA 5505	Cisco ASA 5510
Maximum VPN throughput	100 Mbps	170 Mbps
Maximum concurrent SSL VPN sessions	25	250
Maximum concurrent IPsec VPN sessions	25	250
Interfaces	8-port 10/100 switch 2 Power over Ethernet ports 4 - SFP (with 4GE SSM)	5 Fast Ethernet 2 Gigabit Ethernet 3 Fast Ethernet
Stateful failover	No	Licensed feature
Profile	Desktop	1-RU
VPN load balancing	No	Licensed feature
Shared VPN License Option	No	Yes

From the perspective provided by the articles and the papers discussed above, the present study is made with some specific objectives. The objectives of the study are as follows:

1. Install and configure SSL and IPSec VPN connections on Cisco ASA 5500 Series.
2. Identify if there are any issues in router's configuration file such as ACL and firewall rules that are in conflict because of the two VPNs running together.
3. Capture and analyze network packets via Wireshark or dSniff to identify possible overhead and conflicting headers.
4. Analyze data flow going through the ASA VPN appliance and compare it with both VPN technologies running simultaneously and only IPSec enabled on the VPN router. Analyze router's performance under the different scenarios.
5. Identify if data coming from VPN tunnel and data coming from Internet is routed correctly to reach the final destination.
6. Identify if IPSec and SSL VPNs are running simultaneously without causing conflicts in the edge VPN router.

Chapter 3 – Methodology

Experimental Environment

The research will take place in a real network environment at a private golf club that includes a main facility, several close remote locations, and employees connecting to the club's network resources from home. A sister ski club located 15 miles away in the mountains is included in main club's network through VPN.

The club's lodge houses all servers and main network. The following figures show the network configuration at both locations before implementing SSL and IPSec VPNs.

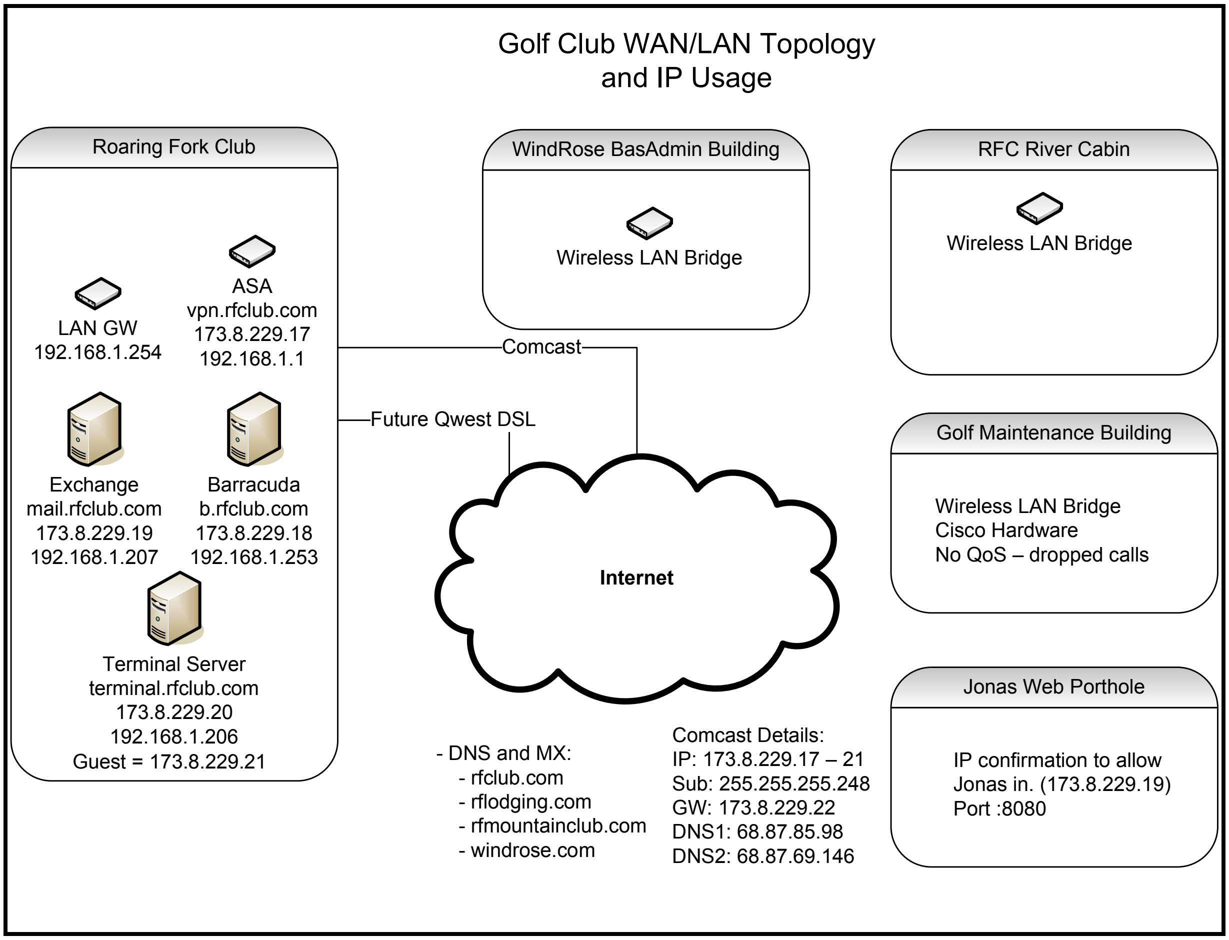


Figure 3.1.1. Network topology of Club's main facility

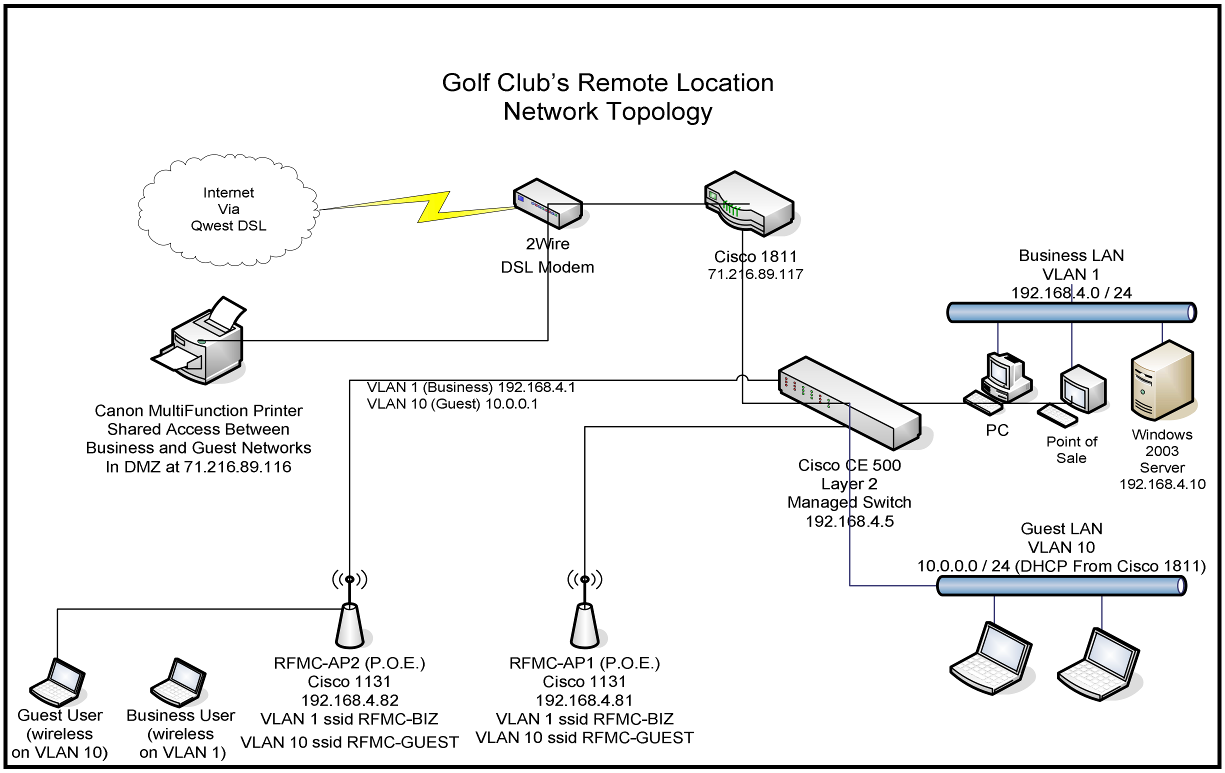


Figure 3.1.2. Network topology of Club's remote location

The network configuration does not include IPSec tunnel or SSL VPN. The main facility connects to the Internet through Comcast Cable Modem and to its close locations (administration and golf maintenance building and river cabin) through wireless LAN bridges. Routing and security are maintained by ASA 5510 firewall router. Club's remote location connects to Internet with Qwest DSL modem and uses Cisco 1811 for routing and security. In order to conduct the study an IPSec tunnel between the two clubs will be enabled and configured as well as clientless SSL VPN on the ASA security appliance at the lodge network. To avoid compatibility issues and for better network utilization ASA 5505 will be added to the edge of a remote location's network. The following figures present the topology of the two networks after the changes made to allow SSL and IPSec implementation. There are additional changes that do not concern the study although they improve the network performance and reliability.

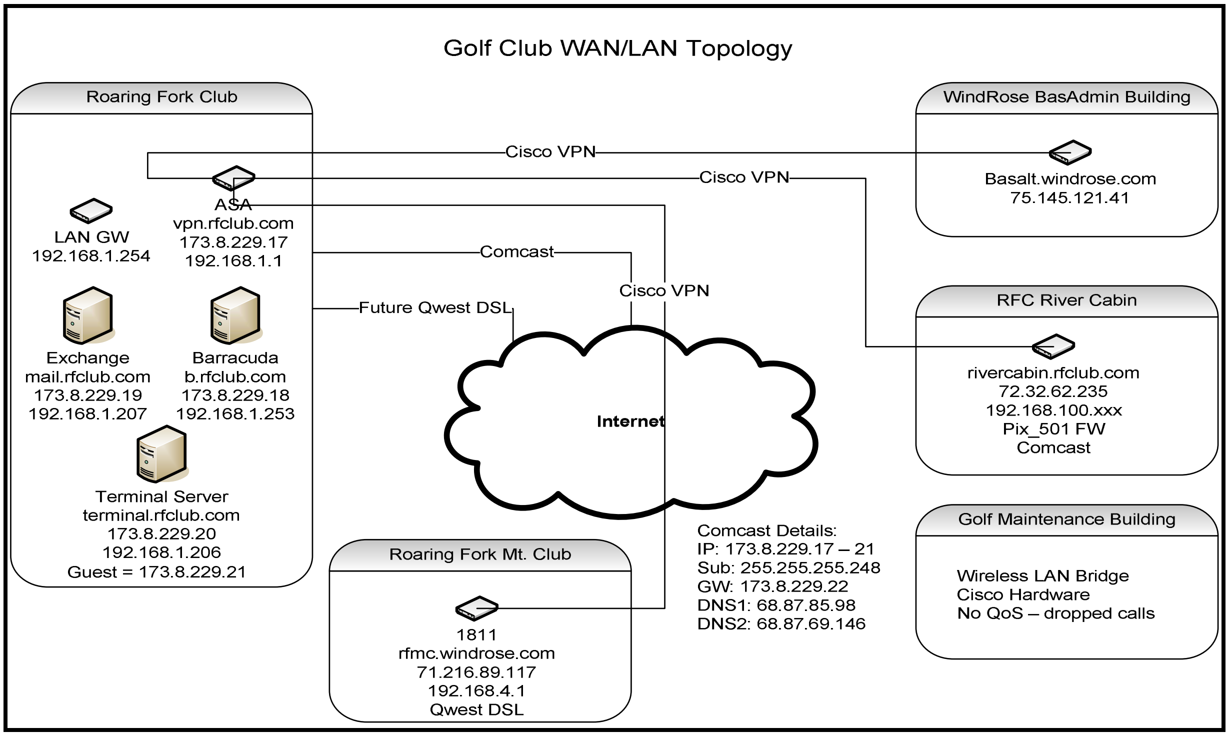


Figure 3.1.3. Club’s network topology after building the IPSec tunnels.

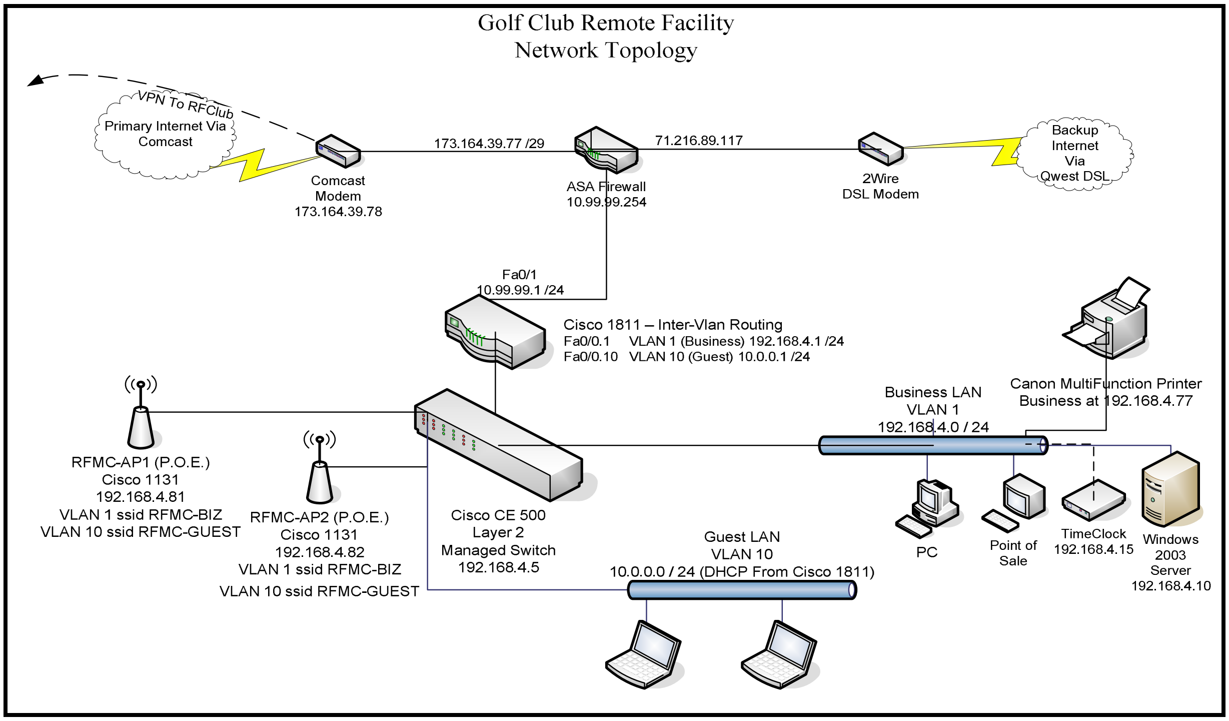
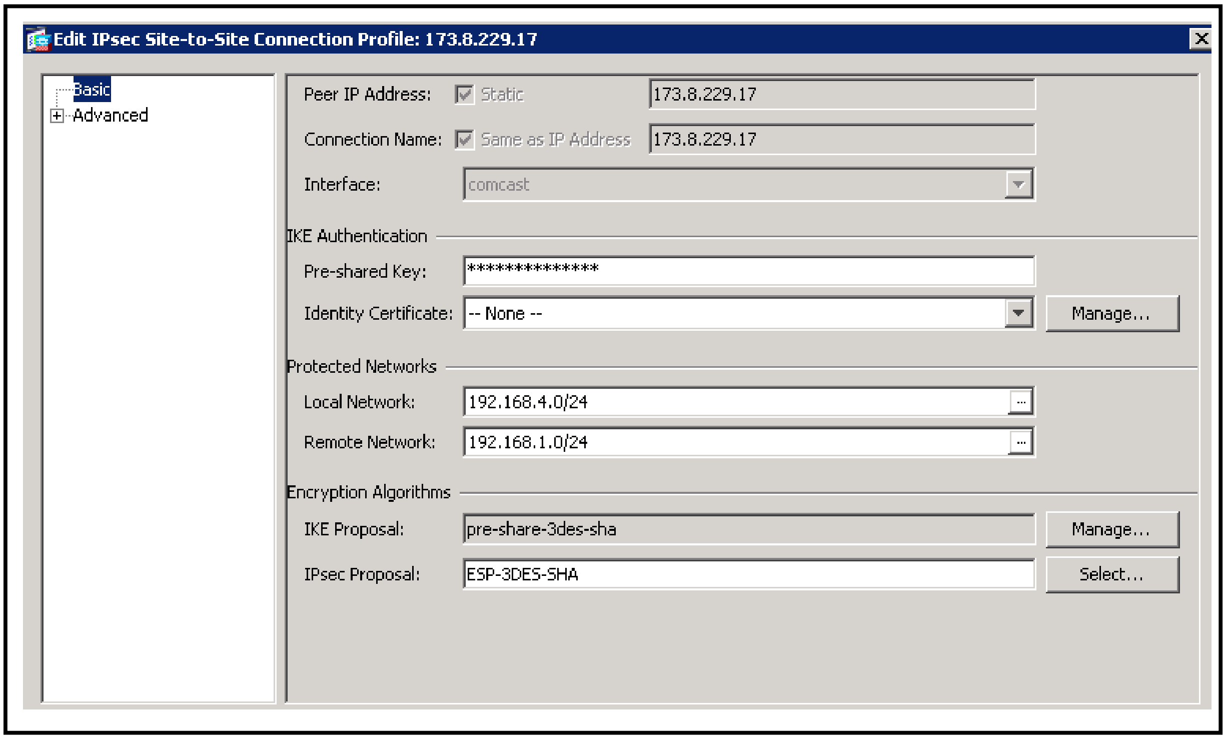


Figure 3.1.4. Remote location’s network topology with ASA firewall router.

Changes in the main club network include two IPSec VPN tunnels that replace the unreliable wireless bridge connections to the administration building and the river cabin. An additional IPSec tunnel connects the remote mountain location to the golf club. The tunnel is configured between golf club's ASA5510 and mountain club's newly installed ASA5505 firewall appliance. A Comcast subscription (set as primary Internet connection) assures redundancy set as failover procedure in the ASA5505. SSL Clientless VPN is configured on main club's ASA router to allow employees to connect to certain network resources from home.

IPSec VPN Configuration

Cisco ASDM-IDM module provides convenient user interface to configure the IPSec tunnel on Cisco ASA5510 and ASA5505. The following screenshots present the IPSec configuration on the mountain club's ASA appliance.



Edit IPsec Site-to-Site Connection Profile: 173.8.229.17

Peer IP Address: ☑ Static 173.8.229.17

Connection Name: ☑ Same as IP Address 173.8.229.17

Interface: comcast

IKE Authentication

Pre-shared Key: **************

Identity Certificate: -- None --

Protected Networks

Local Network: 192.168.4.0/24

Remote Network: 192.168.1.0/24

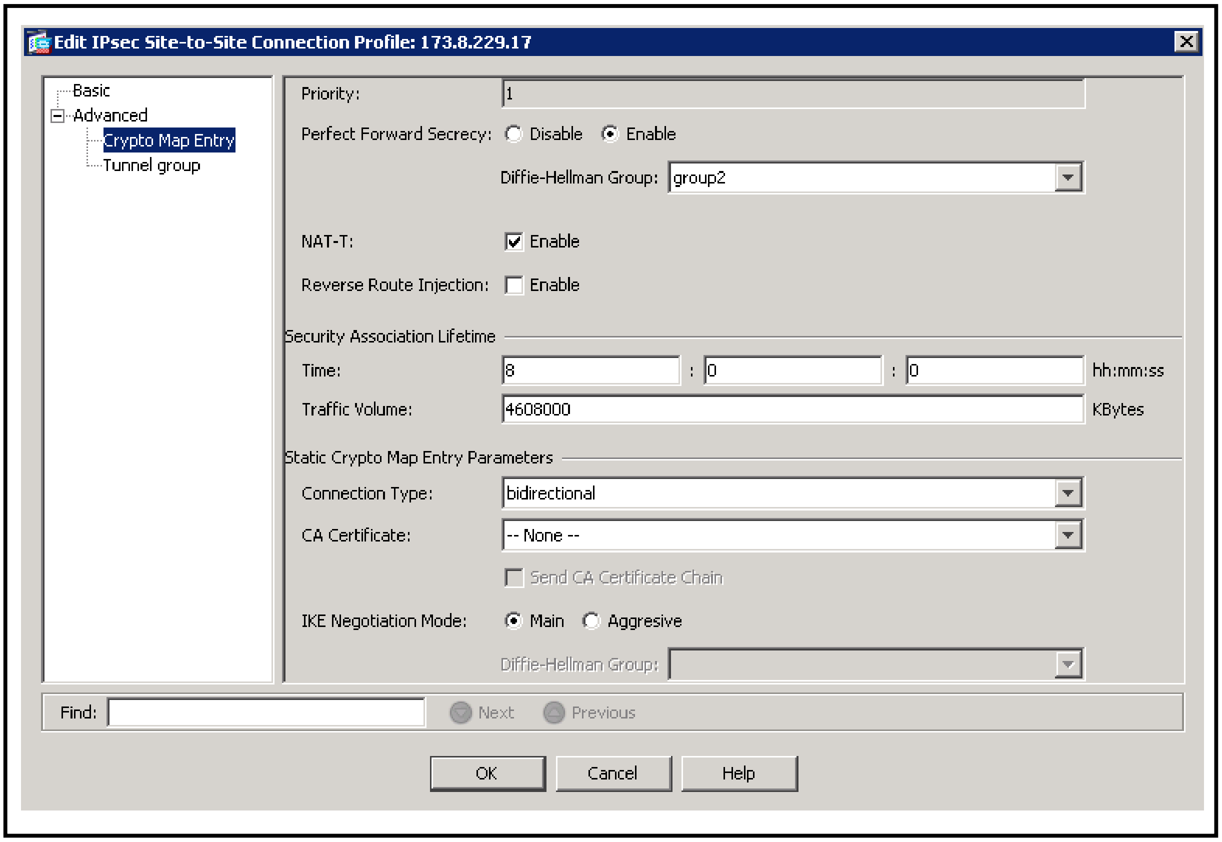
Encryption Algorithms

IKE Proposal: pre-share-3des-sha

IPsec Proposal: ESP-3DES-SHA

Figure 3.2.1. Basic IPSec configuration.

The figure shows that the IPSec tunnel connects networks 192.168.1.0 (golf club) and 192.168.4.0 (mountain club) using pre-shared key for authentication, 168-bit Triple DES (3des) encryption mechanism, and SHA hash policy to ensure integrity.



Edit IPsec Site-to-Site Connection Profile: 173.8.229.17

Priority: 1

Perfect Forward Secrecy: ○ Disable ● Enable

Diffie-Hellman Group: group2

NAT-T: ☑ Enable

Reverse Route Injection: □ Enable

Security Association Lifetime

Time: 8 : 0 : 0 hh:mm:ss

Traffic Volume: 4608000 KBytes

Static Crypto Map Entry Parameters

Connection Type: bidirectional

CA Certificate: -- None --

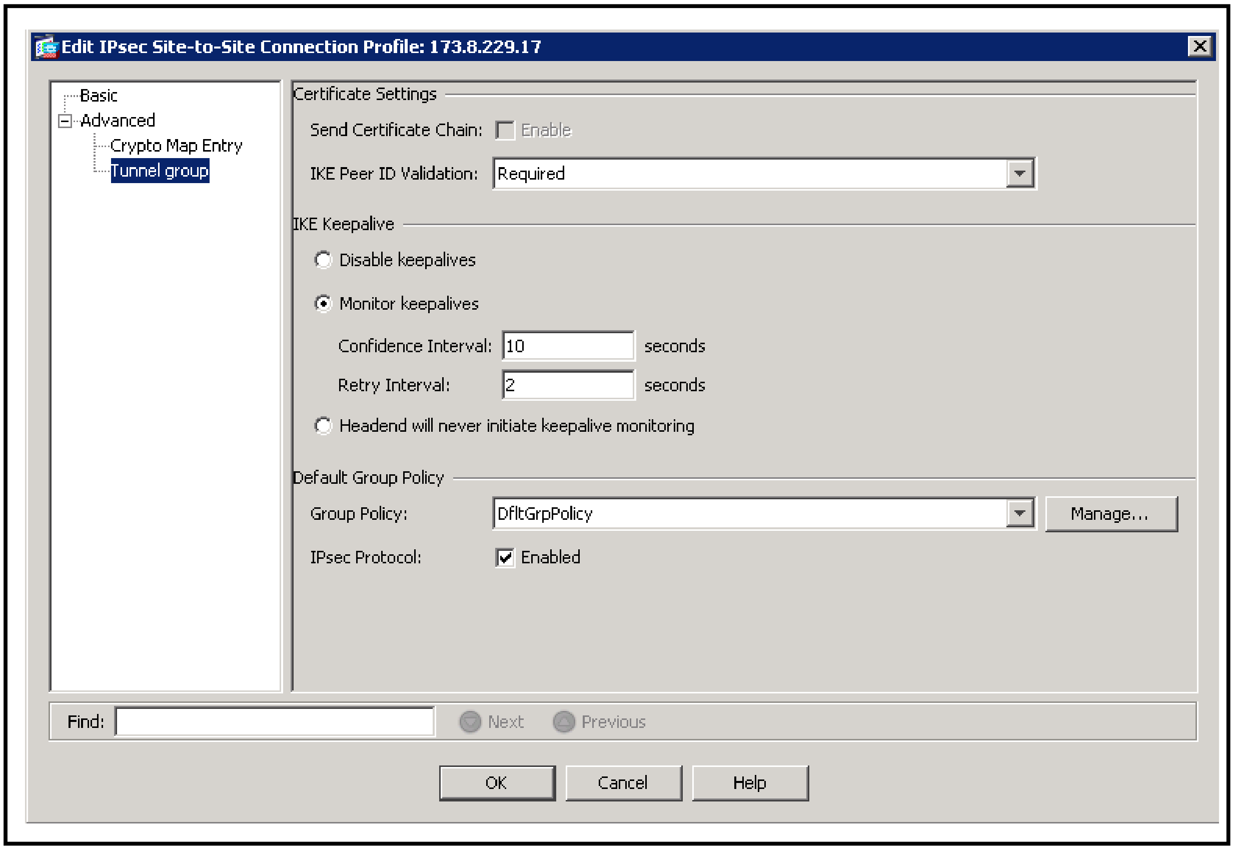
□ Send CA Certificate Chain

IKE Negotiation Mode: ● Main ○ Aggresive

Diffie-Hellman Group:

Figure 3.2.2. IPSec crypto maps.

The crypto map specifies Diffie-Hellman Group 2 which uses 1024-bit encryption to derive the shared secret. It also defines the connection type as bi-directional and the crypto map lifetime to 8 hours which is the default value in ASA to assure secure ISAKMP negotiations. Network address translation traversal (NAT-T) is enabled to allow the IPSec data through the NAT devices.



Edit IPsec Site-to-Site Connection Profile: 173.8.229.17

- Basic
- Advanced
  - Crypto Map Entry
  - Tunnel group

Certificate Settings

Send Certificate Chain: □ Enable

IKE Peer ID Validation: Required

IKE Keepalive

○ Disable keepalives

● Monitor keepalives

Confidence Interval: 10 seconds

Retry Interval: 2 seconds

○ Headend will never initiate keepalive monitoring

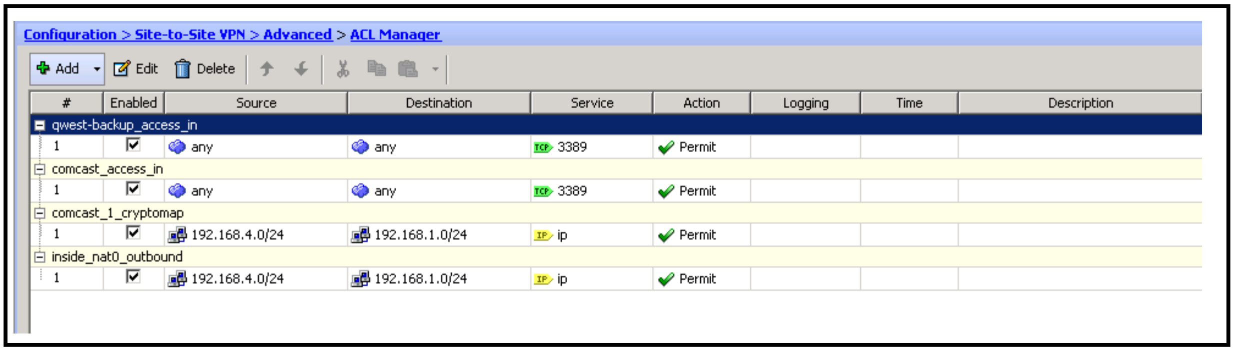
Default Group Policy

Group Policy: DfltGrpPolicy

IPsec Protocol: ☑ Enabled

Figure 3.2.3. IPSec IKE settings.

IKE keepalives is enabled to identify any connection failure between the two hosts.



Configuration > Site-to-Site VPN > Advanced > ACL Manager

#	Enabled	Source	Destination	Service	Action	Logging	Time	Description
qwest-backup_access_in								
1	☑	any	any	TCP 3389	✓ Permit			
comcast_access_in								
1	☑	any	any	TCP 3389	✓ Permit			
comcast_1_cryptomap								
1	☑	192.168.4.0/24	192.168.1.0/24	IP ip	✓ Permit			
inside_nat0_outbound								
1	☑	192.168.4.0/24	192.168.1.0/24	IP ip	✓ Permit			

Figure 3.2.4. Access Control Lists for IPSec tunnel.

Access control list (ACL) assigned to the IPSec crypto map identifies the traffic between the two subnets, 192.168.1.0 and 192.168.4.0. The access rule allows network traffic to pass through the IPSec tunnel without being blocked by the firewall.

Main lodge’s ASA5510 has the same IPSec configuration: pre-shared key for authentication, 168-bit 3DES encryption mechanism, and SHA hash policy for data integrity. In addition to the VPN between the golf and the ski club, ASA5510 utilizes two more IPSec tunnels to connect two close locations, the River Cabin and the administration building. The IPSec tunnel configured through the Cisco ASDM-IDM appears in router’s configuration file as shown on the figures below.

```
interface Ethernet0/1
 nameif COMCAST
 security-level 0
 ip address 173.8.229.17 255.255.255.248
!
tunnel-group 75.145.121.41 type ipsec-l2l
tunnel-group 75.145.121.41 ipsec-attributes
 pre-shared-key *
tunnel-group 173.164.39.77 type ipsec-l2l
tunnel-group 173.164.39.77 ipsec-attributes
 pre-shared-key *
tunnel-group RFCLUB-EZVPN type remote-access
tunnel-group RFCLUB-EZVPN general-attributes
 address-pool EZVPN-POOL
 default-group-policy RFCLUB-EZVPN
tunnel-group RFCLUB-EZVPN ipsec-attributes
 pre-shared-key *
tunnel-group 173.14.13.25 type ipsec-l2l
tunnel-group 173.14.13.25 ipsec-attributes
 pre-shared-key *
!
crypto isakmp identity address
crypto isakmp enable COMCAST
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
```

Figure 3.2.5. Part of the ASA5510 configuration file showing the IPSec tunnels and their configuration.

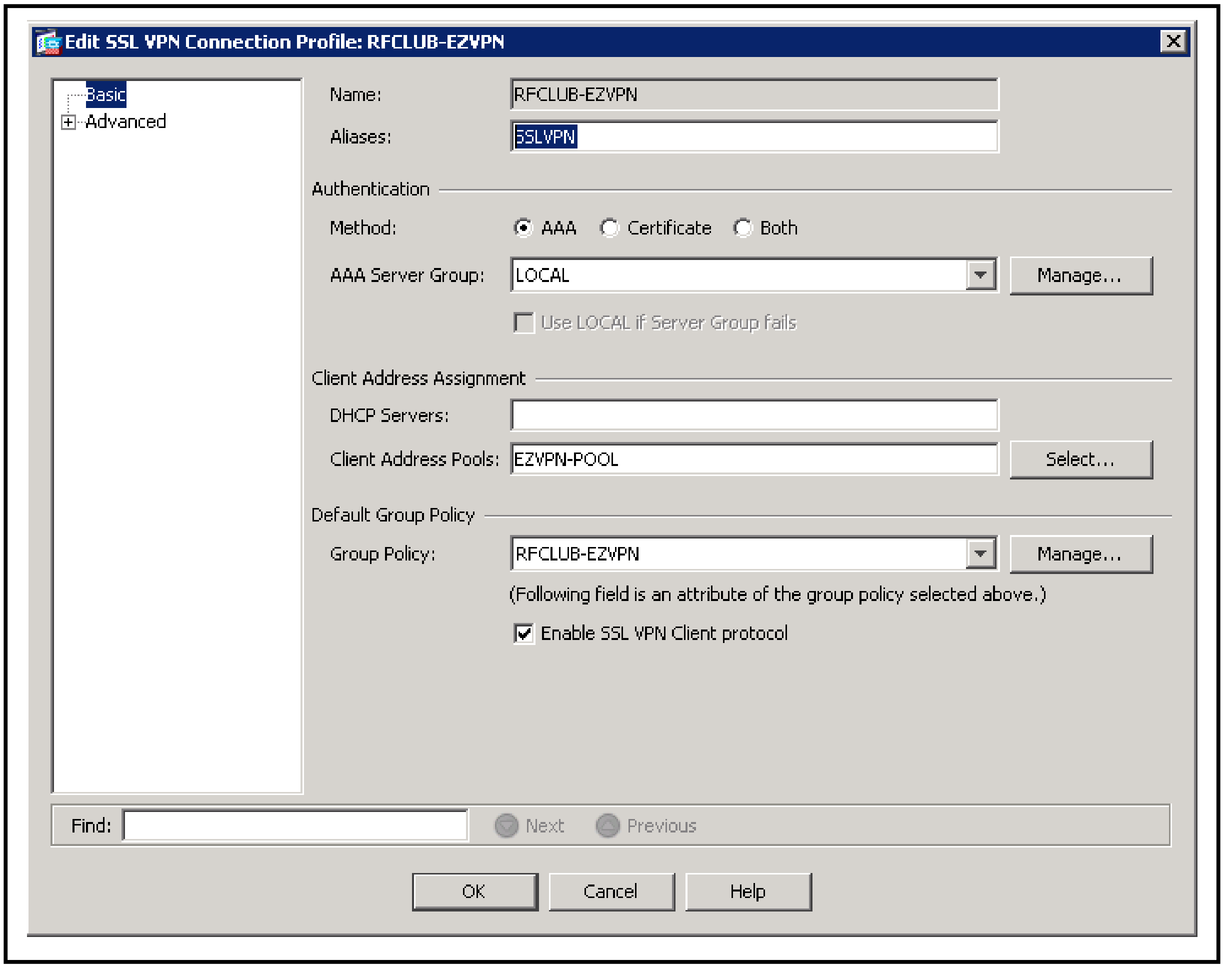
```
access-list COMCAST_cryptomap extended permit ip 192.168.1.0 255.255.255.0
10.100.10.0 255.255.254.0
access-list RFCLUB_nat0_outbound extended permit ip 192.168.1.0 255.255.255.0
10.100.10.0 255.255.254.0
access-list RFCLUB_nat0_outbound extended permit ip 192.168.1.0 255.255.255.0
10.255.255.0 255.255.255.0
access-list RFCLUB_nat0_outbound extended permit ip 192.168.1.0 255.255.255.0
192.168.100.0 255.255.255.0
access-list RFCLUB_nat0_outbound extended permit ip 192.168.1.0 255.255.255.0
192.168.4.0 255.255.255.0
access-list COMCAST_2_cryptomap extended permit ip 192.168.1.0 255.255.255.0
192.168.4.0 255.255.255.0
access-list OUTSIDE_cryptomap extended permit ip any 10.255.255.0 255.255.255.0
access-list Split_Tunnel_ACL standard permit 192.168.1.0 255.255.255.0
access-list COMCAST_access_in extended permit tcp any host 173.8.229.17 eq 200
access-list COMCAST_access_in extended permit tcp any host 173.8.229.17 eq 212
access-list COMCAST_3_cryptomap extended permit ip 192.168.1.0 255.255.255.0
192.168.100.0 255.255.255.0
```

Figure 3.2.6. Part of ASA5510 configuration file showing ACL rules.

Figure 9 and 10 show only that part of the configuration part that concerns the IPSec tunnels. The full running configuration file of ASA5510 is included in Appendix A. All three tunnels are configured on the Comcast Ethernet interface 0/1 which holds five different static IP addresses with subnet mask 255.255.255.248 assigned from the ISP. Access lists allow the home network, 192.168.1.0 to identify traffic from the remote ones 10.100.10.0, 10.255.255.0, 192.168.100.0, and ski club’s 192.168.4.0.

AnyConnect SSL VPN Configuration

Clientless SSL VPN is advertised as a remote connection that does not need a VPN client installed on user’s computer to build a secure tunnel. That connection requires only SSL-enabled browser to access data through https, ftp, or CIFS protocols. The clientless VPN provides very limited access which is insufficient for the club’s needs. ASA 5510 offers SSL AnyConnect VPN through a small client (SVC) that is installed on the remote work station and can be removed after the secure session is terminated. SVC allows users to access all resources on the network based on their credentials. Installing SVC does not require the network administrator to have access to user's computer. The following figures show the steps taken to configure SSL VPN on the ASA 5510 appliance.



Edit SSL VPN Connection Profile: RFCLUB-EZVPN

Name: RFCLUB-EZVPN

Aliases: SSLVPN

Authentication

Method: ● AAA ○ Certificate ○ Both

AAA Server Group: LOCAL

□ Use LOCAL if Server Group fails

Client Address Assignment

DHCP Servers:

Client Address Pools: EZVPN-POOL

Default Group Policy

Group Policy: RFCLUB-EZVPN

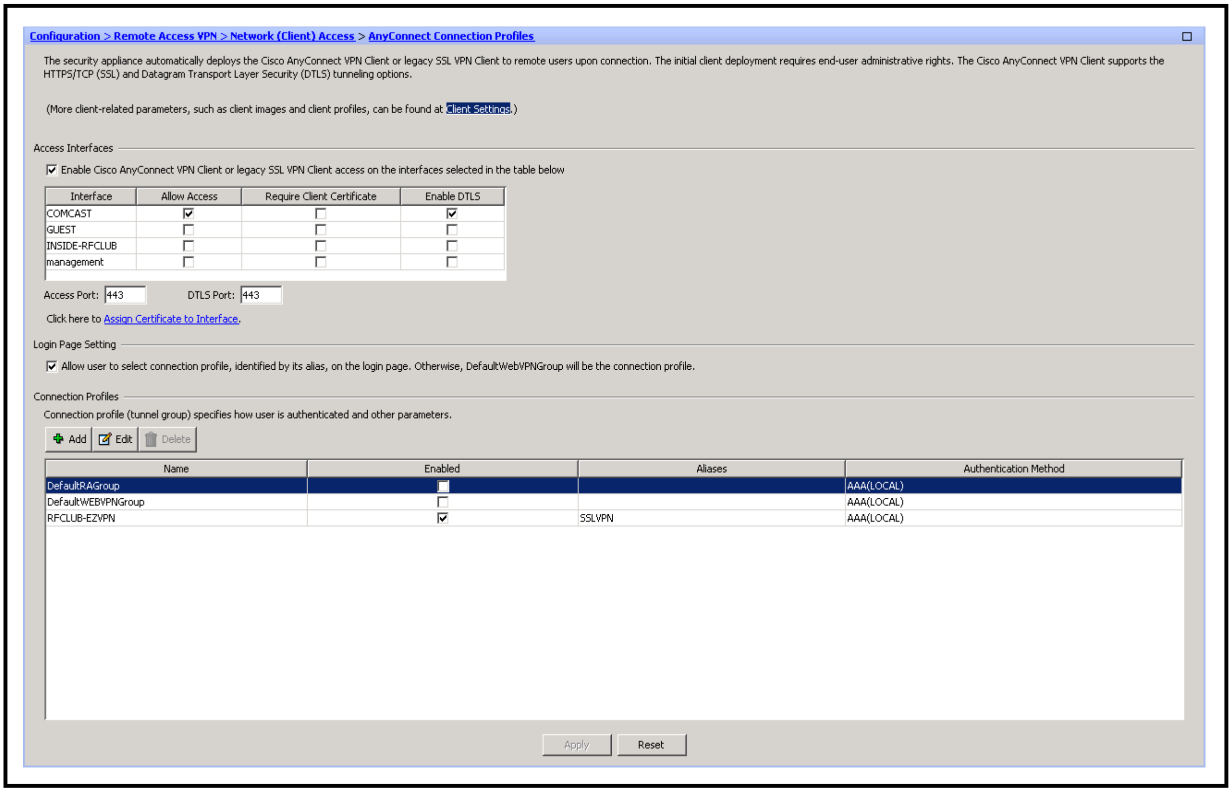
(Following field is an attribute of the group policy selected above.)

☑ Enable SSL VPN Client protocol

Figure 3.3.1. Enable SSL VPN as an alias to existing group policy.

Current ASA configuration allows using the preexisting connection profile RFCLUB-EZVPN to enable the SSL VPN. Authentication uses the local AAA server group, the address pool is inherited from EZVPN-POOL, and the SSL VPN client protocol is enabled for that profile. Detailed information about RFCLUB-EZVPN and EZVPN-POOL is provided in the full ASA running configuration file in Appendix A.

Figure 12 contains a screenshot from the ASDM interface presenting the SSL VPN enabled as RFCLUB-EZVPN alias with AAA local authentication attached to the COMCAST interface of the ASA router.



Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles

The security appliance automatically deploys the Cisco AnyConnect VPN Client or legacy SSL VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports the HTTPS/TCP (SSL) and Datagram Transport Layer Security (DTLS) tunneling options.

(More client-related parameters, such as client images and client profiles, can be found at Client Settings.)

Access Interfaces

☑ Enable Cisco AnyConnect VPN Client or legacy SSL VPN Client access on the interfaces selected in the table below

Interface	Allow Access	Require Client Certificate	Enable DTLS
COMCAST	☑	□	☑
GUEST	□	□	□
INSIDE-RFCLUB	□	□	□
management	□	□	□

Access Port: 443   DTLS Port: 443

Click here to Assign Certificate to Interface.

Login Page Setting

☑ Allow user to select connection profile, identified by its alias, on the login page. Otherwise, DefaultWebVPNGroup will be the connection profile.

Connection Profiles

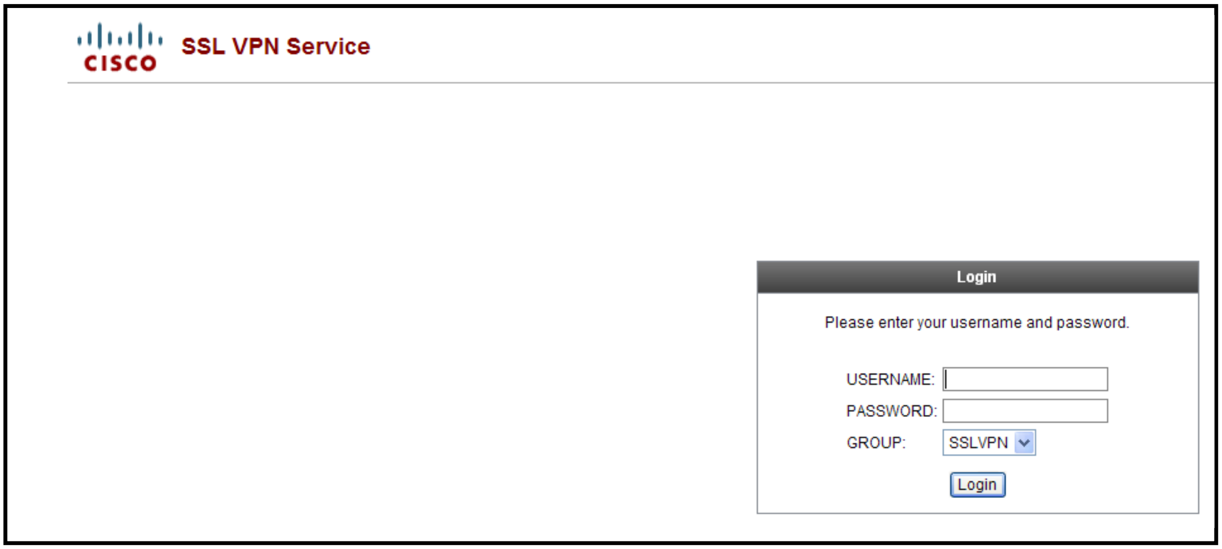
Connection profile (tunnel group) specifies how user is authenticated and other parameters.

Name	Enabled	Aliases	Authentication Method
DefaultRAGroup	□		AAA(LOCAL)
DefaultWEBVPNGroup	□		AAA(LOCAL)
RFCLUB-EZVPN	☑	SSLVPN	AAA(LOCAL)

Figure 3.3.2. SSL VPN configuration overview.

Procedures

VPN tunnels verification. The first step after configuring the IPSec and SSL on the ASA appliances is to verify that the router is able to build the remote connections. To test the SSL VPN we use a laptop connected to Internet through a Verizon wireless card. The public IP address assigned to the outside interface of ASA has a DNS record vpn.rfclub.com. The following figures present the SSL VPN interface showing in the user’s Web browser and the connection details after downloading and installing the SVC.



SSL VPN Service

Login

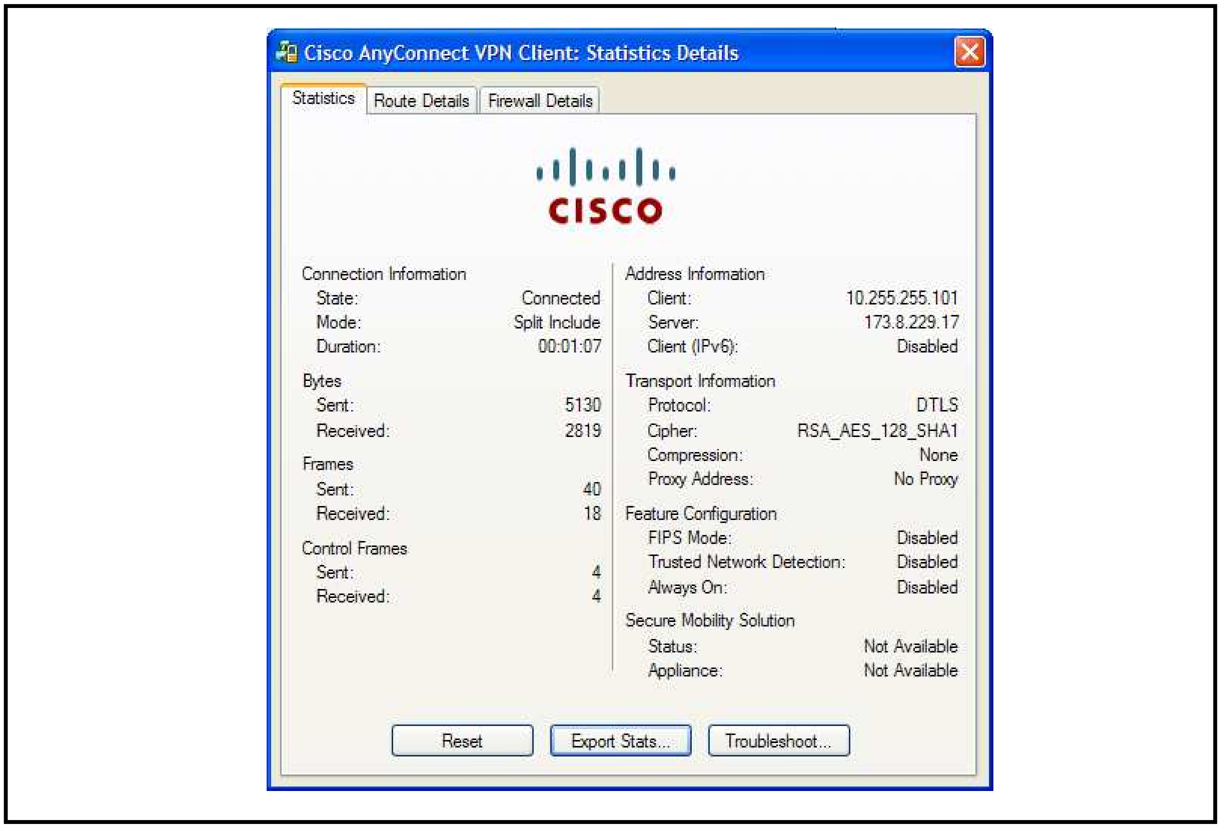
Please enter your username and password.

USERNAME:

PASSWORD:

GROUP: SSLVPN

Figure 3.4.1. SSL VPN login page.

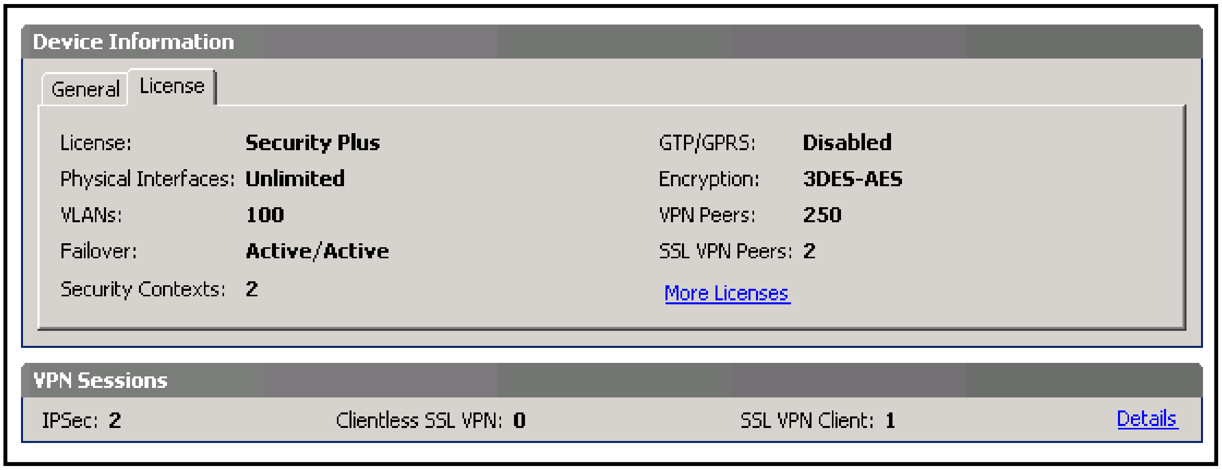


Cisco AnyConnect VPN Client: Statistics Details

```
Connection Information                    Address Information
  State:                   Connected        Client:                       10.255.255.101
  Mode:                Split Include        Server:                          173.8.229.17
  Duration:                 00:01:07        Client (IPv6):                       Disabled
Bytes                                     Transport Information
  Sent:                         5130        Protocol:                                DTLS
  Received:                     2819        Cipher:                      RSA_AES_128_SHA1
Frames                                      Compression:                             None
  Sent:                           40        Proxy Address:                       No Proxy
  Received:                       18      Feature Configuration
Control Frames                              FIPS Mode:                           Disabled
  Sent:                            4        Trusted Network Detection:           Disabled
  Received:                        4        Always On:                           Disabled
                                          Secure Mobility Solution
                                            Status:                         Not Available
                                            Appliance:                      Not Available
```

Figure 3.4.2. SSL VPN client information.

Statistics presented in figure 14 confirm that the SSL tunnel is running. The client has an internal IP assigned from the ASA’s DHCP server and uses RSA in combination with AES128 and SHA1 for data encryption/ decryption. Monitoring information from the ASDM also confirms the SSL connection as well as the IPSec tunnel between the mountain and the golf clubs and between the administration building and the golf club.



License: Security Plus
Physical Interfaces: Unlimited
VLANs: 100
Failover: Active/Active
Security Contexts: 2
GTP/GPRS: Disabled
Encryption: 3DES-AES
VPN Peers: 250
SSL VPN Peers: 2

IPSec: 2
Clientless SSL VPN: 0
SSL VPN Client: 1

Figure 3.4.3. Information from the ASDM software, confirming the IPSec and the SSL VPN sessions.

Monitoring Information. A quantitative approach will help in monitoring and gathering data about the IPSec and SSL tunnels while running simultaneous sessions through the ASA appliance. Cisco’s ASDM software provides extensive information about the ASA router that can be used to analyze its behavior while utilizing VPN sessions. Monitoring diagrams include RAM and CPU load, dropped packets, queued packets, IPSec session statistics, SSL session statistics, and error and warning messages during the sessions. The monitoring statistics will discover if the ASA appliance is able to support both VPN tunnel without disturbing any of its normal functions.

Running Configuration File Analysis. Configuration file analysis will compare the file before and after enabling the SSL protocol on the ASA device. It will identify if there are any conflicts in the access control list (ACL) configuration. We will also use the ASDM to find if there are any warnings or errors in the router configuration file.

WireShark Packet Monitoring. Packet monitoring will provide information of how the ASA appliance tag packets assigned to the SSL tunnel and to the IPSec tunnel. That information will discover if the router is able to tag VPN packet correctly for the different session and respectively if the router can handle the different protocols at the same time.

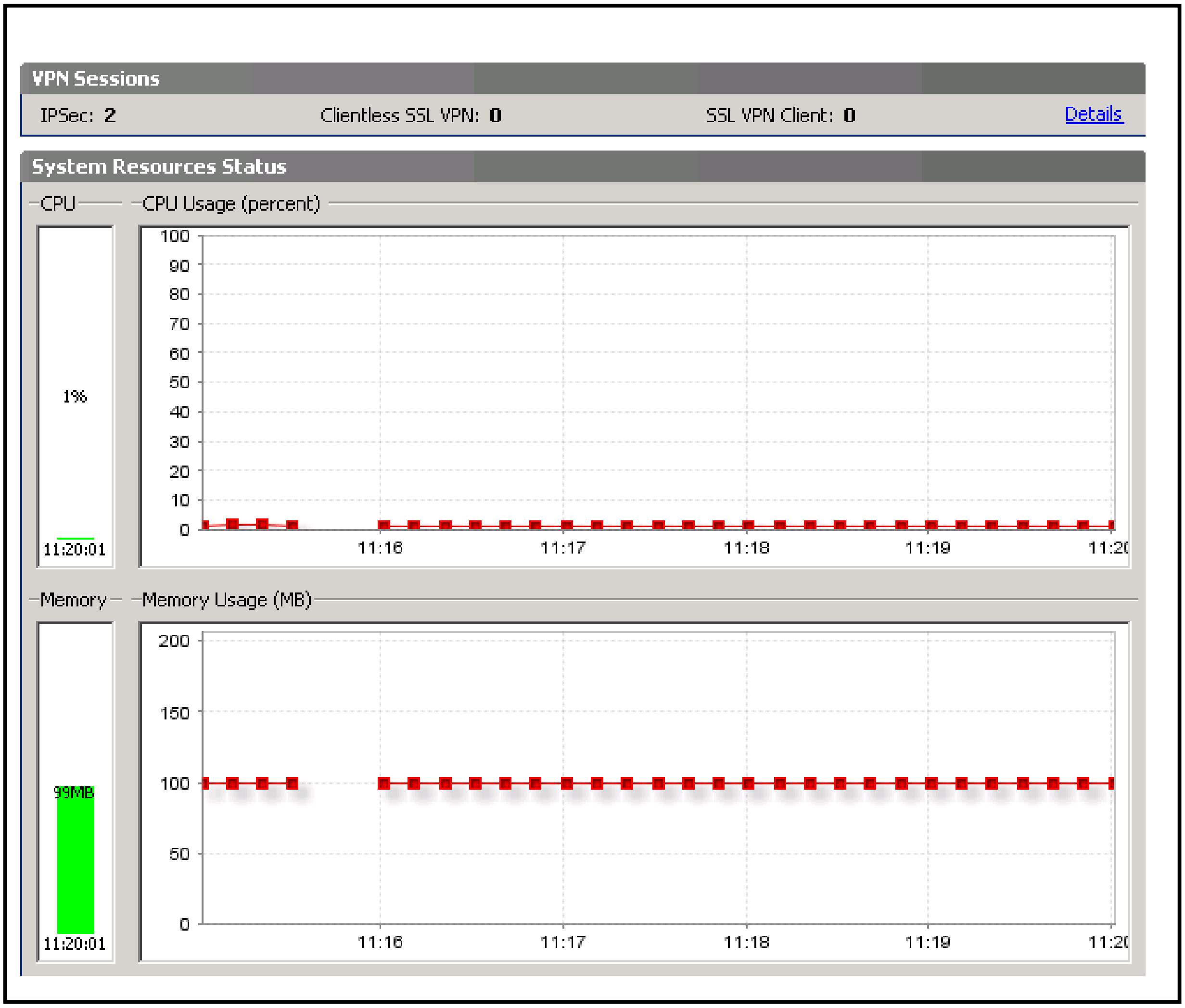
Cost Factors. SSL and IPSec sessions require licenses that affect the company's budget. It is a non-technical factor that also identifies if the two protocols can be implemented simultaneously. Data will be gathered about license cost and will be compared to other VPN solutions to provide objective information about the cost effect of running IPSec and SSL simultaneously.

Maintenance Requirements and Statistics. The time frame for configuring and maintaining the different VPN protocols will be measured to identify how they affect the network administrator's work load. It is additional information to show if administrators are able to support both protocols without affecting their normal work flow.

Chapter 4 – Project Results and Analysis

ASDM ASA Monitoring

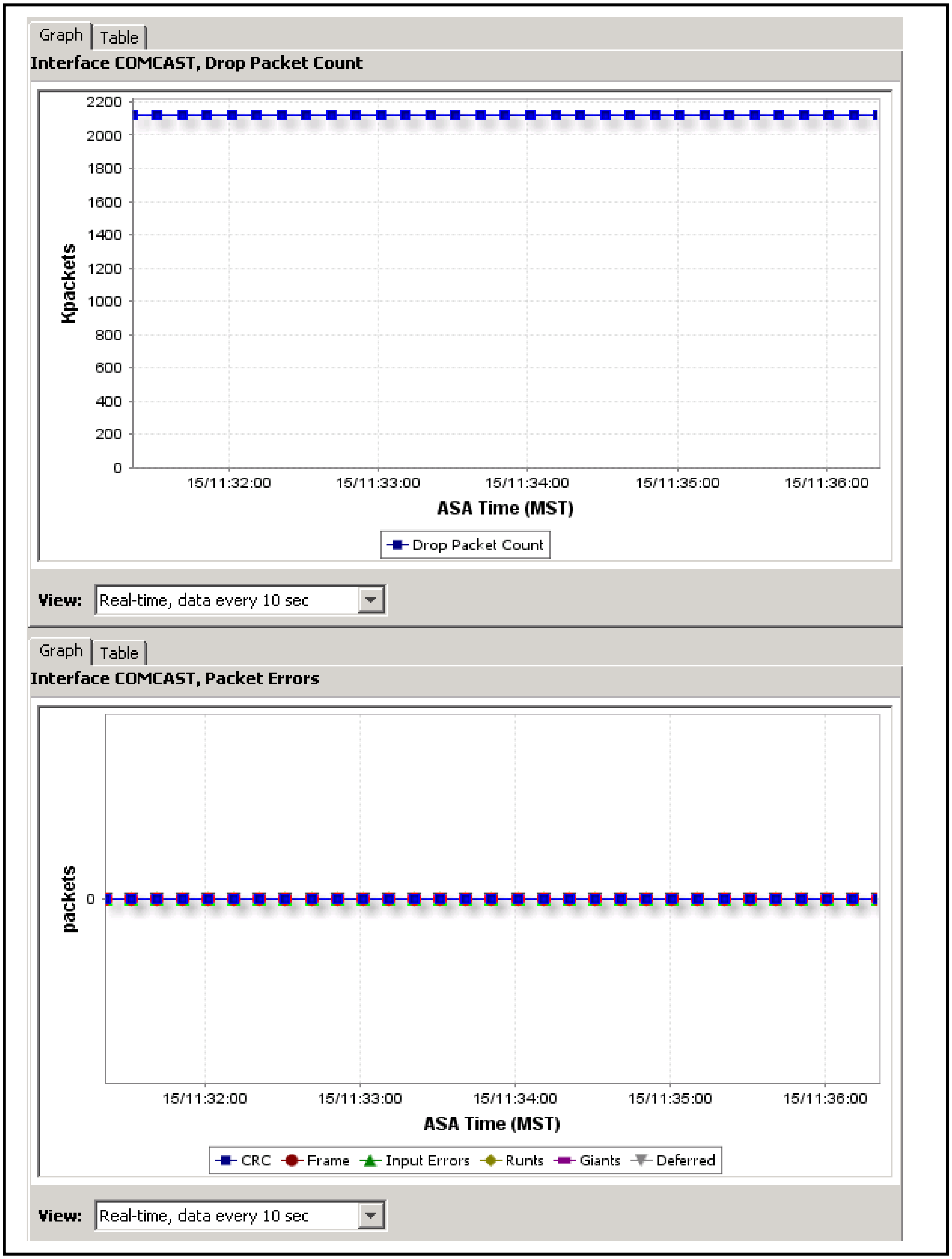
ASA Resource and Interface Graphs with Two IPSec Tunnels. Figures 4.1.1 through 4.1.12 present graphs acquired from the ASDM software. ASDM monitoring includes information about the ASA appliance while running two simultaneous IPSec tunnels. All sessions are loaded with bulk data transfer which is the primary use of the remote connections.



VPN Sessions

IPSec: 2 Clientless SSL VPN: 0 SSL VPN Client: 0

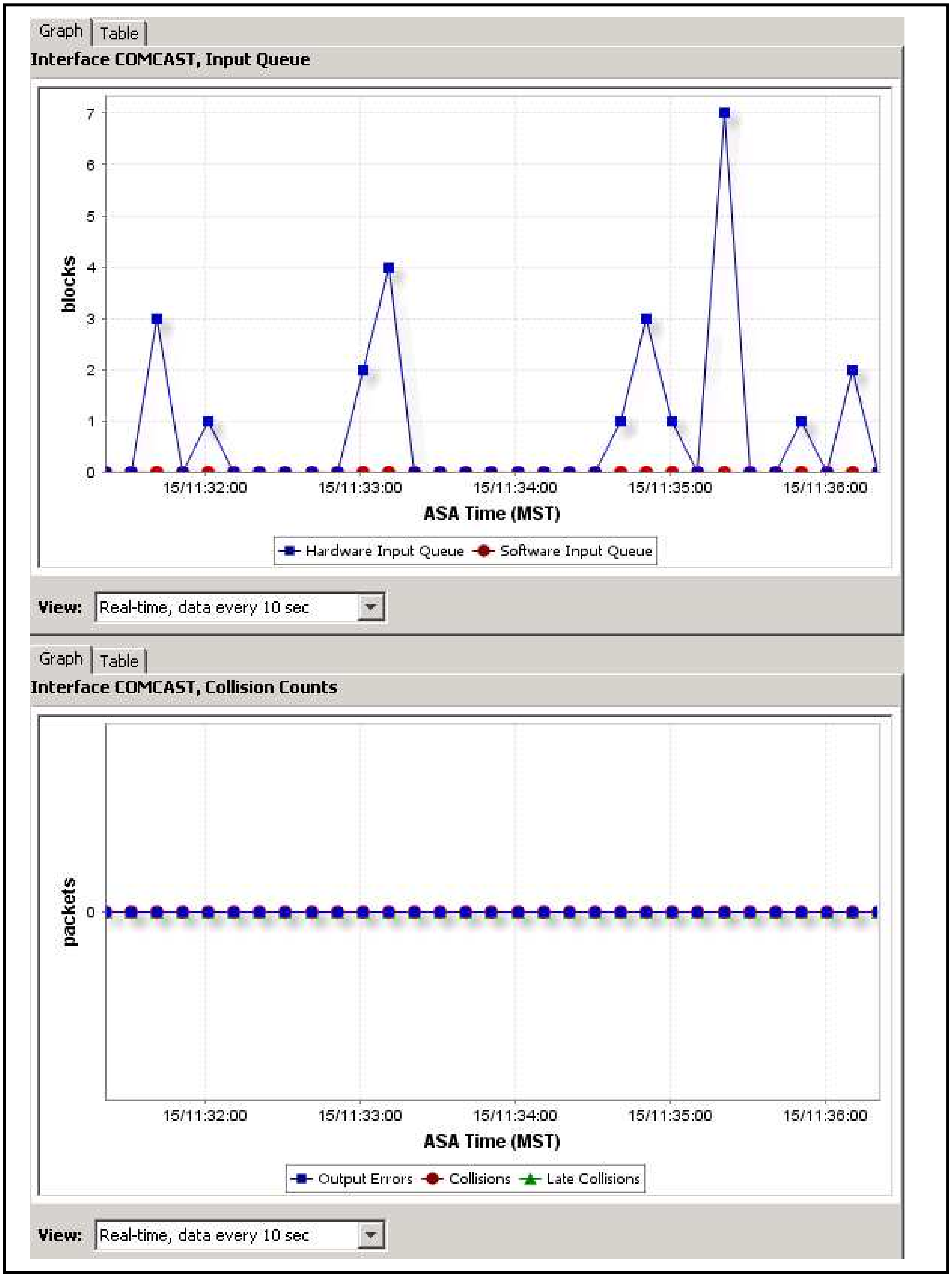
Figure 4.1.1. CPU and RAM usage with two IPSec tunnels.



View: Real-time, data every 10 sec

View: Real-time, data every 10 sec

Figure 4.1.2. Dropped packets and packet errors graphs with two IPSec tunnels.

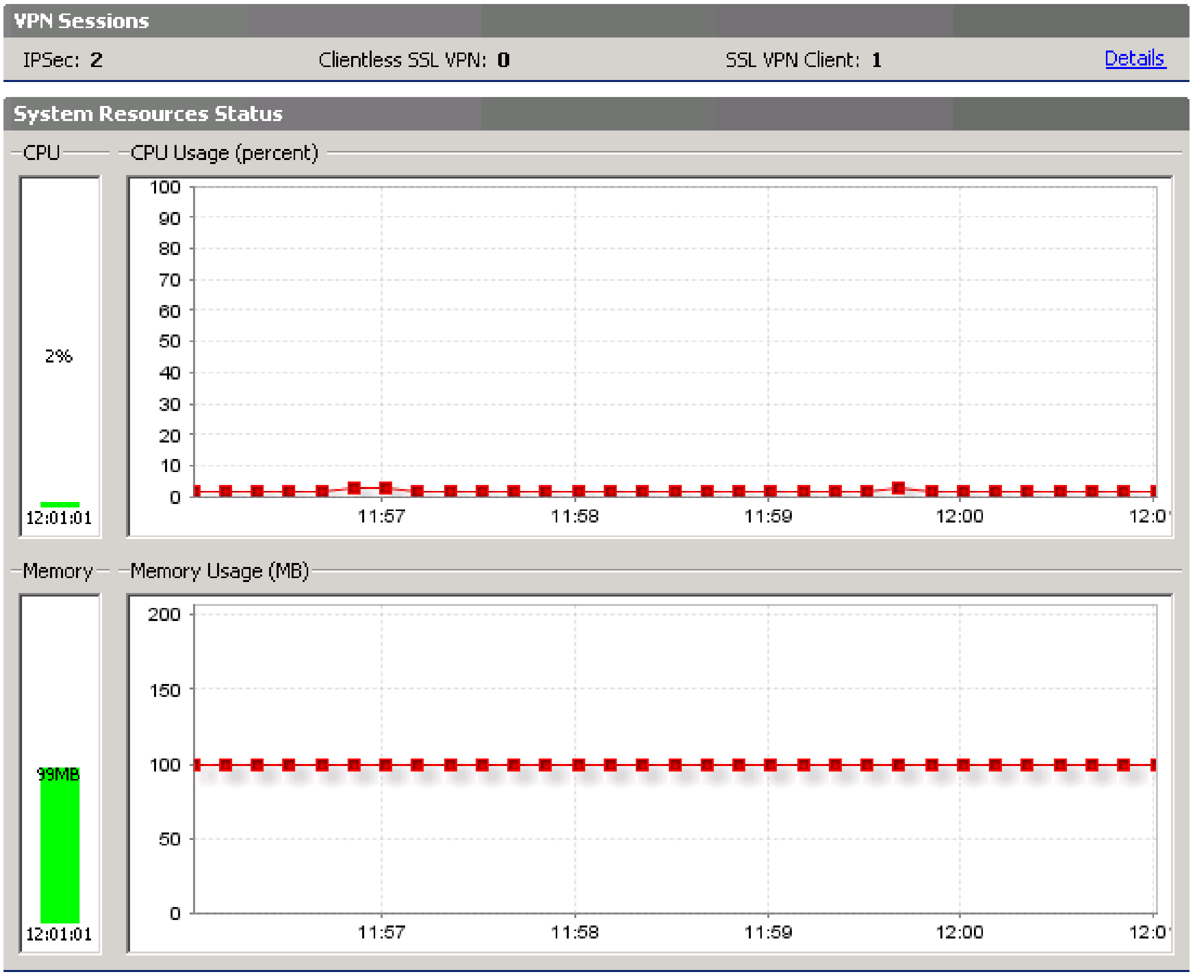


View: Real-time, data every 10 sec

View: Real-time, data every 10 sec

Figure 4.1.3. Input queue and collision counts graph with two IPSec tunnels.

ASA Resource and Interface Graphs with One SSL and Two IPSec Sessions. This section shows the same ASA statistics while utilizing a SSL session on top of the two IPSec tunnels. All VPN tunnels are loaded with bulk data transfer which is the primary use for the remote connections.



VPN Sessions

IPSec: **2** Clientless SSL VPN: **0** SSL VPN Client: **1**

Figure 4.1.4. CPU and RAM usage with two IPSec and one SSL session.

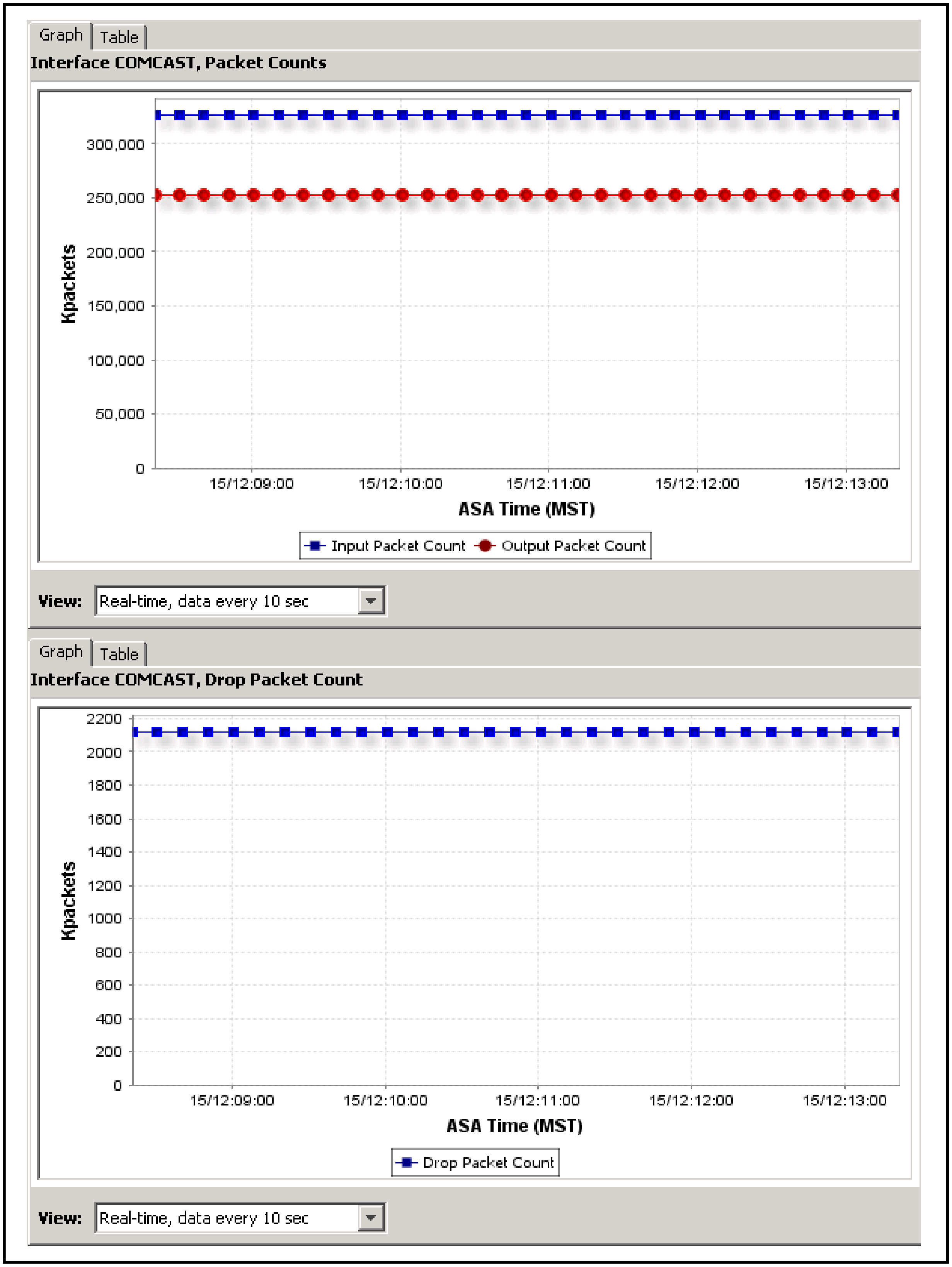
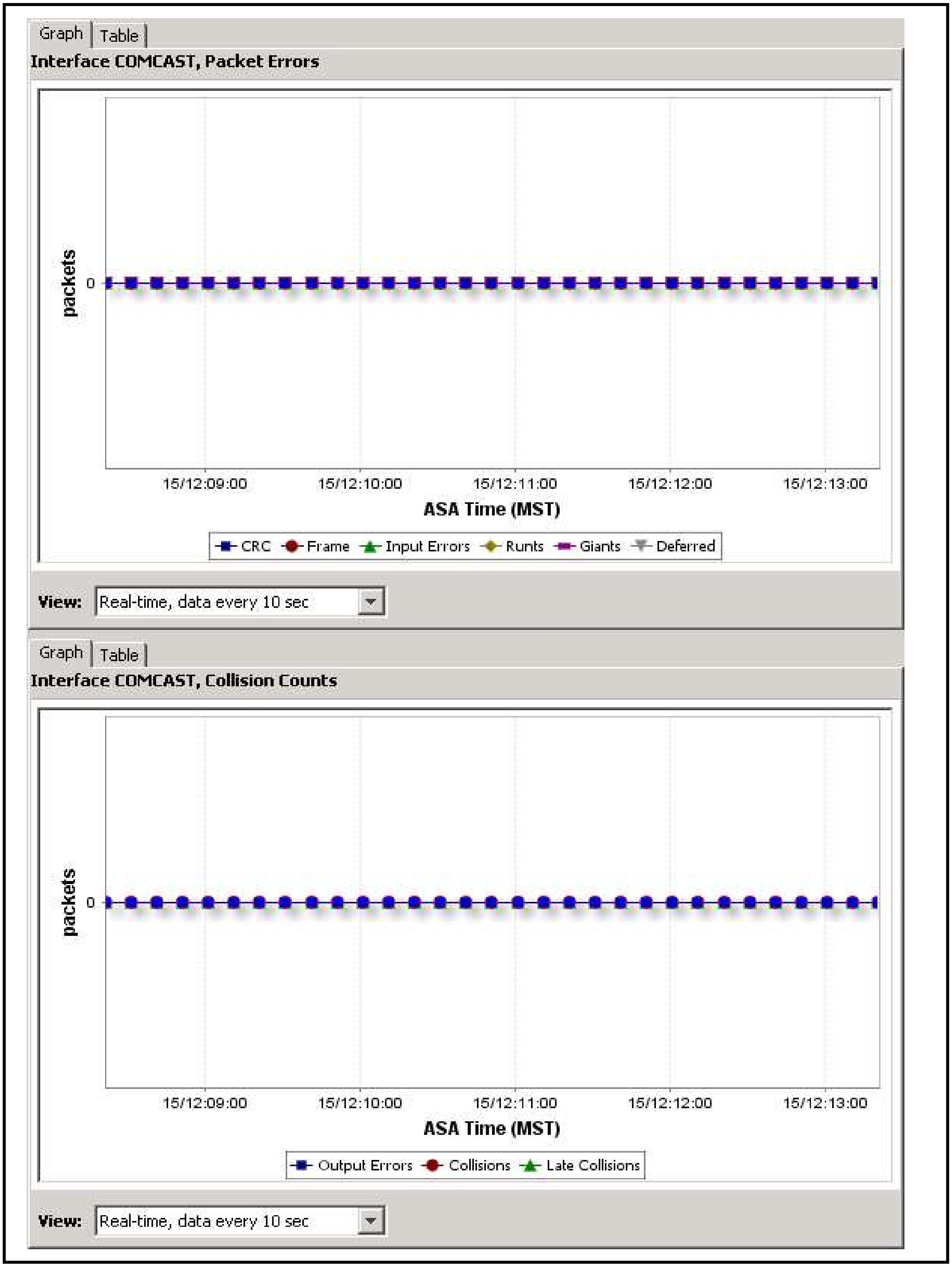


Figure 4.1.5. Packet counts vs. drop packet with two IPSec and one SSL session.



View: Real-time, data every 10 sec

View: Real-time, data every 10 sec

Figure 4.1.6. Packer errors and collision counts with two IPSec and one SSL session.

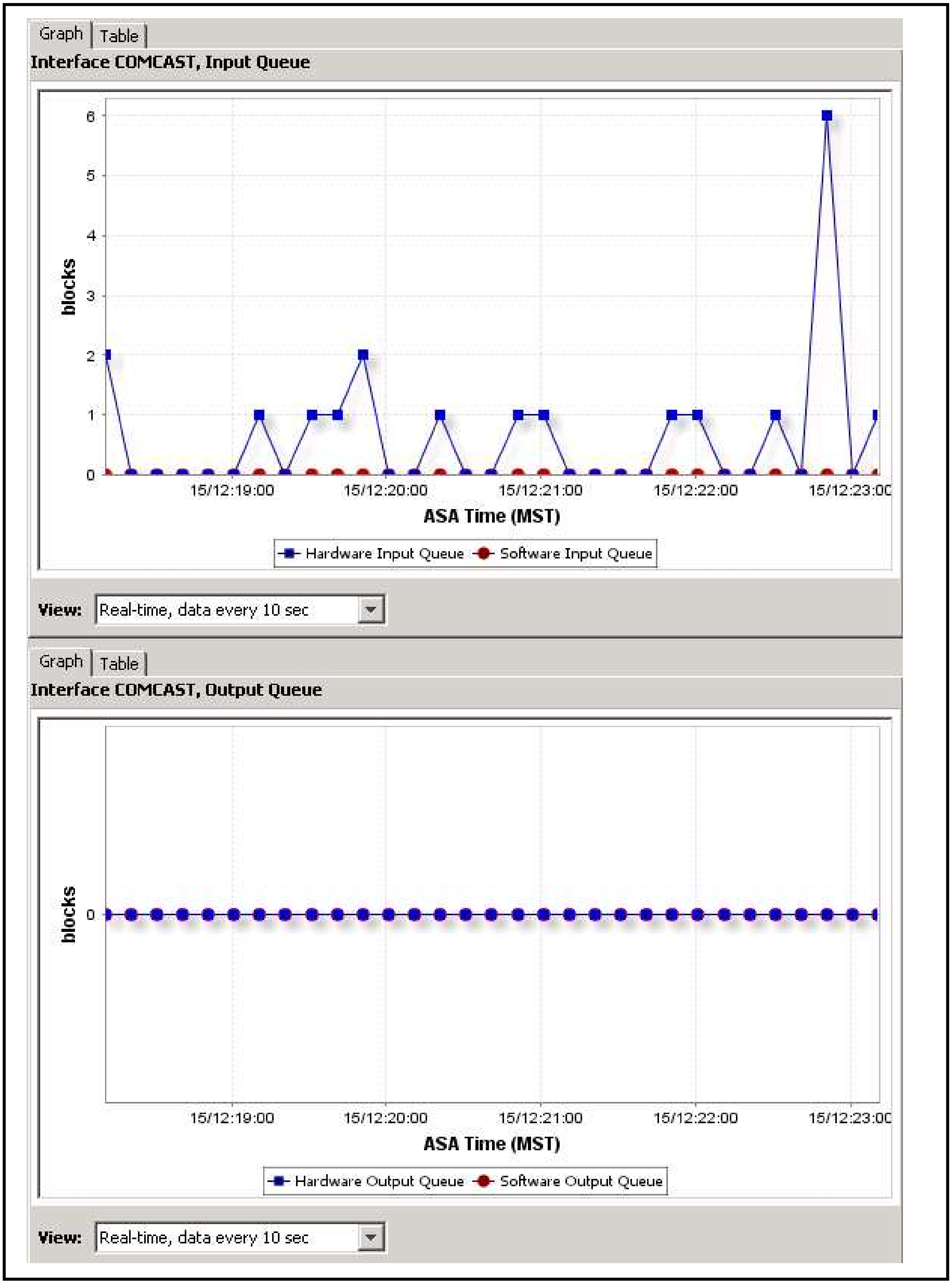
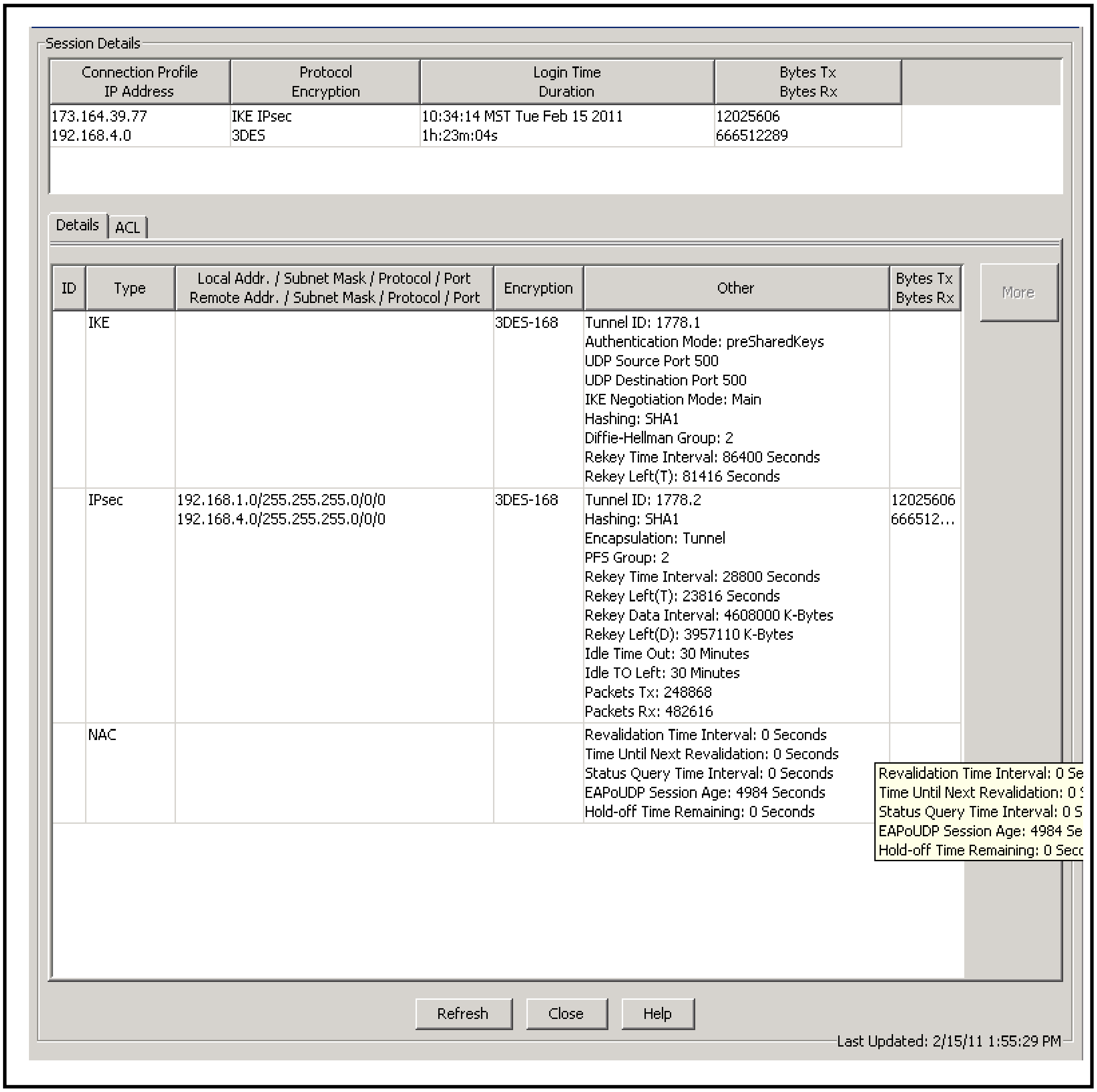


Figure 4.1.7. Packet input queue vs. output queue with two IPSec and one SSL session.

VPN Session Statistics. This part includes IPSec and SSL session statistics as well as global encryption statistics for the two VPN technologies for the time they have been working simultaneously.



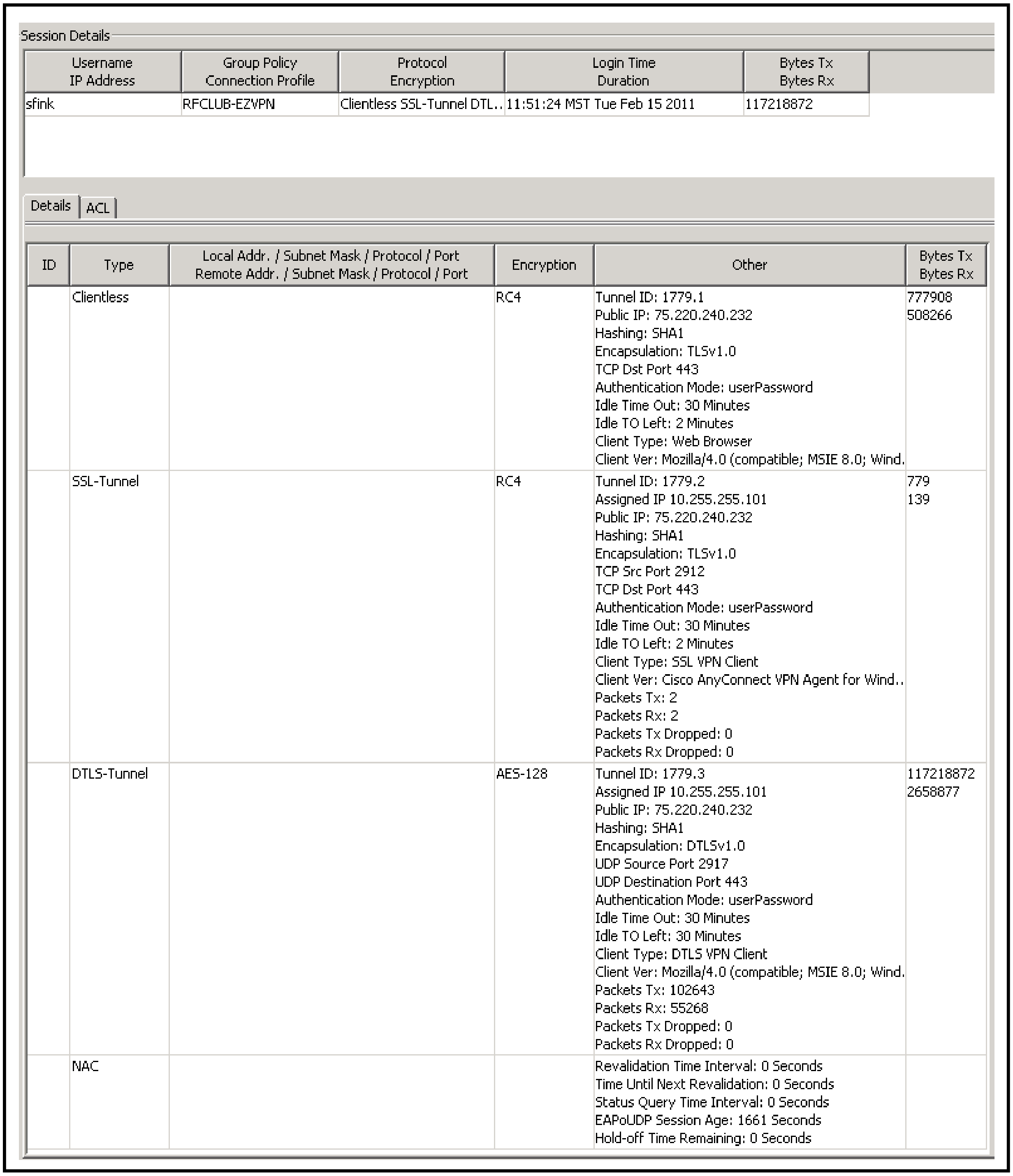
Connection Profile IP Address	Protocol Encryption	Login Time Duration	Bytes Tx Bytes Rx
173.164.39.77 192.168.4.0	IKE IPsec 3DES	10:34:14 MST Tue Feb 15 2011 1h:23m:04s	12025606 666512289

ID	Type	Local Addr. / Subnet Mask / Protocol / Port Remote Addr. / Subnet Mask / Protocol / Port	Encryption	Other	Bytes Tx Bytes Rx
	IKE		3DES-168	Tunnel ID: 1778.1 Authentication Mode: preSharedKeys UDP Source Port 500 UDP Destination Port 500 IKE Negotiation Mode: Main Hashing: SHA1 Diffie-Hellman Group: 2 Rekey Time Interval: 86400 Seconds Rekey Left(T): 81416 Seconds	
	IPsec	192.168.1.0/255.255.255.0/0/0 192.168.4.0/255.255.255.0/0/0	3DES-168	Tunnel ID: 1778.2 Hashing: SHA1 Encapsulation: Tunnel PFS Group: 2 Rekey Time Interval: 28800 Seconds Rekey Left(T): 23816 Seconds Rekey Data Interval: 4608000 K-Bytes Rekey Left(D): 3957110 K-Bytes Idle Time Out: 30 Minutes Idle TO Left: 30 Minutes Packets Tx: 248868 Packets Rx: 482616	12025606 666512...
	NAC			Revalidation Time Interval: 0 Seconds Time Until Next Revalidation: 0 Seconds Status Query Time Interval: 0 Seconds EAPoUDP Session Age: 4984 Seconds Hold-off Time Remaining: 0 Seconds	

Revalidation Time Interval: 0 Se
Time Until Next Revalidation: 0 S
Status Query Time Interval: 0 S
EAPoUDP Session Age: 4984 Se
Hold-off Time Remaining: 0 Secc

Last Updated: 2/15/11 1:55:29 PM

Figure 4.1.8. Details for the IPSec session between the mountain club and the golf club.

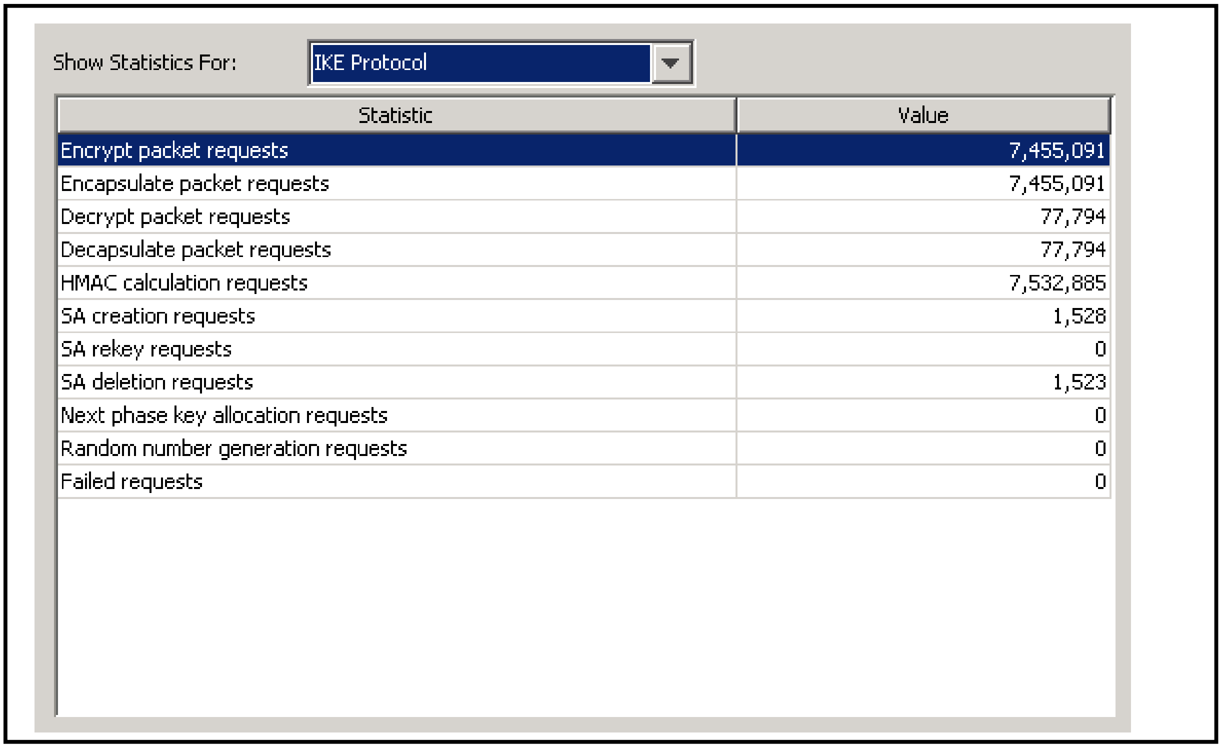


Session Details

Username IP Address	Group Policy Connection Profile	Protocol Encryption	Login Time Duration	Bytes Tx Bytes Rx
sfink	RFCLUB-EZVPN	Clientless SSL-Tunnel DTL..	11:51:24 MST Tue Feb 15 2011	117218872

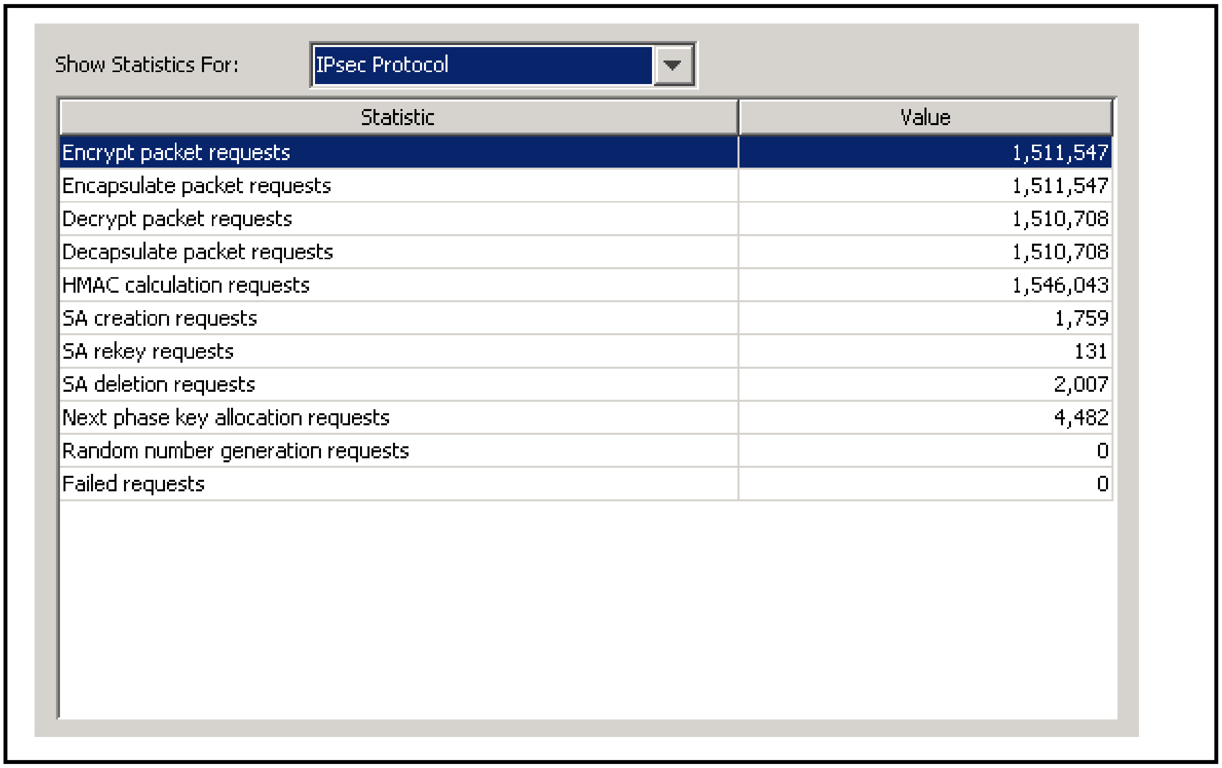
ID	Type	Local Addr. / Subnet Mask / Protocol / Port Remote Addr. / Subnet Mask / Protocol / Port	Encryption	Other	Bytes Tx Bytes Rx
	Clientless		RC4	Tunnel ID: 1779.1 Public IP: 75.220.240.232 Hashing: SHA1 Encapsulation: TLSv1.0 TCP Dst Port 443 Authentication Mode: userPassword Idle Time Out: 30 Minutes Idle TO Left: 2 Minutes Client Type: Web Browser Client Ver: Mozilla/4.0 (compatible; MSIE 8.0; Wind.	777908 508266
	SSL-Tunnel		RC4	Tunnel ID: 1779.2 Assigned IP 10.255.255.101 Public IP: 75.220.240.232 Hashing: SHA1 Encapsulation: TLSv1.0 TCP Src Port 2912 TCP Dst Port 443 Authentication Mode: userPassword Idle Time Out: 30 Minutes Idle TO Left: 2 Minutes Client Type: SSL VPN Client Client Ver: Cisco AnyConnect VPN Agent for Wind.. Packets Tx: 2 Packets Rx: 2 Packets Tx Dropped: 0 Packets Rx Dropped: 0	779 139
	DTLS-Tunnel		AES-128	Tunnel ID: 1779.3 Assigned IP 10.255.255.101 Public IP: 75.220.240.232 Hashing: SHA1 Encapsulation: DTLSv1.0 UDP Source Port 2917 UDP Destination Port 443 Authentication Mode: userPassword Idle Time Out: 30 Minutes Idle TO Left: 30 Minutes Client Type: DTLS VPN Client Client Ver: Mozilla/4.0 (compatible; MSIE 8.0; Wind. Packets Tx: 102643 Packets Rx: 55268 Packets Tx Dropped: 0 Packets Rx Dropped: 0	117218872 2658877
	NAC			Revalidation Time Interval: 0 Seconds Time Until Next Revalidation: 0 Seconds Status Query Time Interval: 0 Seconds EAPoUDP Session Age: 1661 Seconds Hold-off Time Remaining: 0 Seconds	

Figure 4.1.9. Details for the SSL session between employee laptop and the golf club.



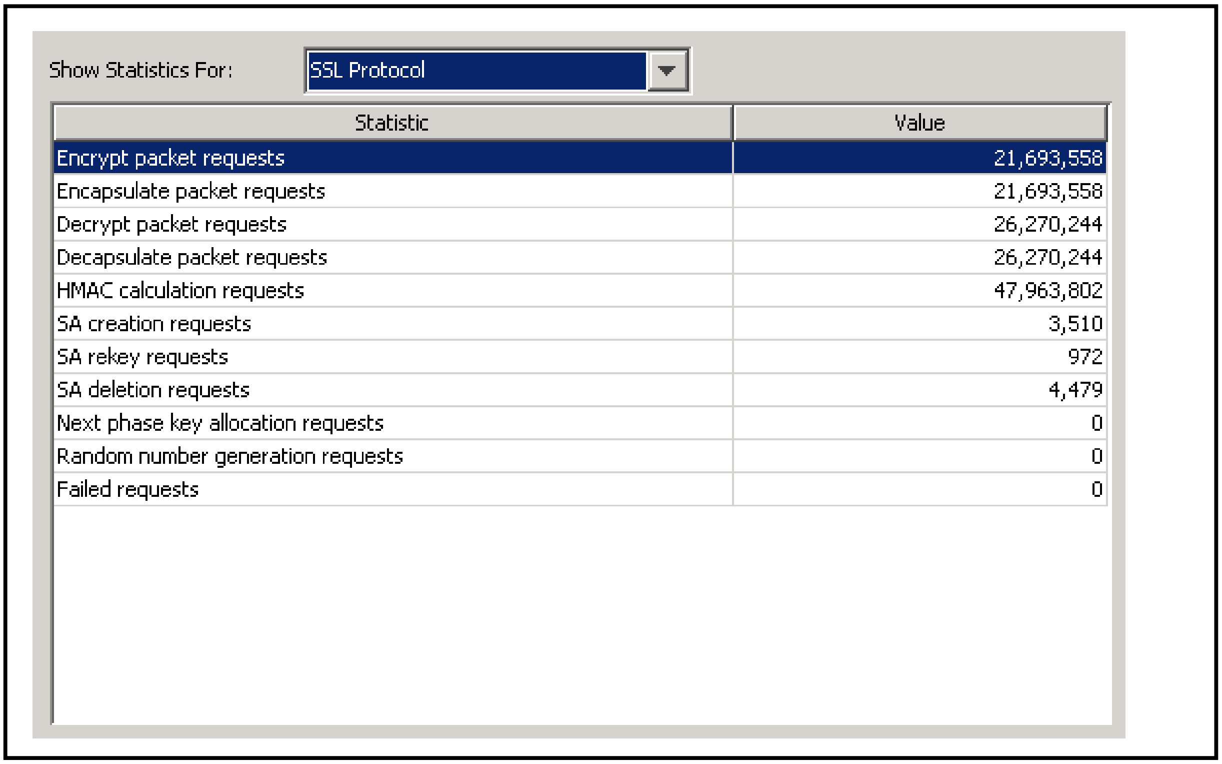
Statistic	Value
Encrypt packet requests	7,455,091
Encapsulate packet requests	7,455,091
Decrypt packet requests	77,794
Decapsulate packet requests	77,794
HMAC calculation requests	7,532,885
SA creation requests	1,528
SA rekey requests	0
SA deletion requests	1,523
Next phase key allocation requests	0
Random number generation requests	0
Failed requests	0

Figure 4.1.10. IKE protocol crypto statistics.



Statistic	Value
Encrypt packet requests	1,511,547
Encapsulate packet requests	1,511,547
Decrypt packet requests	1,510,708
Decapsulate packet requests	1,510,708
HMAC calculation requests	1,546,043
SA creation requests	1,759
SA rekey requests	131
SA deletion requests	2,007
Next phase key allocation requests	4,482
Random number generation requests	0
Failed requests	0

Figure 4.1.11. IPSec protocol crypto statistics.



Statistic	Value
Encrypt packet requests	21,693,558
Encapsulate packet requests	21,693,558
Decrypt packet requests	26,270,244
Decapsulate packet requests	26,270,244
HMAC calculation requests	47,963,802
SA creation requests	3,510
SA rekey requests	972
SA deletion requests	4,479
Next phase key allocation requests	0
Random number generation requests	0
Failed requests	0

Figure 4.1.12. SSL protocol crypto statistics.

Analysis. Figures 4.1.1 and 4.1.4 compare the ASA router resource usage while running two IPSec tunnels and a SSL session in addition to the tunnels. A slight change can be seen only in the CPU diagram and it is negligible as the CPU usage increase with only 1%. We also take in account that ASA 5510 is rated to support 250 IPSec and 250 SSL sessions. Running large number of concurrent VPN session is a matter of hardware upgrade and not the two technologies implemented together. SSL and IPSec running simultaneously do not affect the ASA hardware resources.

Figures 4.1.2, 4.1.3, 4.1.5, 4.1.6, and 4.1.7 identify the effect of the VPN sessions on the overall ASA performance. In normal work conditions, with two IPSec tunnels in idle mode and no SSL session, the outside interface (Comcast) drops around 2100 from the approximately 320000 incoming packets. In addition, for the time interval of two hours (intervals of 5 minutes are shown in the graphs due to ASDM configuration) there are no collisions or packet errors. The statistics does not change when SSL session is running and IPSec tunnels are loaded with data transfer. During the increased packet processing through the Comcast interface, the number of dropped or error packets stays unchanged. SSL and IPSec have a zero effect on the input and output queue as well as on the overall performance of the ASA security appliance.

Figures 4.1.8 and 4.1.9 provide statistics for the IPSec session between the two clubs and the SSL session between the employee laptop and the club. Sessions are built according to the associated crypto maps with the correct encryption protocols and valid IPs assigned by the DHCP server. The statistics does not identify any dropped packets or incorrect parameters for the both sessions. In addition, figures 4.1.10, 4.1.11, and 4.1.12 show zero failures from the millions of encrypt packet requests. IPSec and SSL sessions are built and utilized simultaneously without packet or request failures. The following figure includes real time log information from the ASDM that confirms the IPSec and SSL flawless simultaneous existence.

```
6|Feb 15 2011|13:01:58|302020|10.255.255.101|1280|RFCSERVER|0|Built inbound ICMP
connection for faddr 10.255.255.101/1280 gaddr RFCSERVER/0 laddr RFCSERVER/0
(sfink)
6|Feb 15 2011|13:01:58|605005|RFCSERVER|31913|192.168.1.1|https|Login permitted from
RFCSERVER/31913 to INSIDE-RFCLUB:192.168.1.1/https for user "admin"
6|Feb 15 2011|13:01:58|611101|||||User authentication succeeded: Uname: admin
6|Feb 15 2011|13:01:58|113008|||||AAA transaction status ACCEPT : user = admin
6|Feb 15 2011|13:01:58|113012|||||AAA user authentication Successful : local database : user
= admin
6|Feb 15 2011|13:01:58|725002|RFCSERVER|31913|||Device completed SSL handshake
with client INSIDE-RFCLUB:RFCSERVER/31913
6|Feb 15 2011|13:01:58|725003|RFCSERVER|31913|||SSL client INSIDE-
RFCLUB:RFCSERVER/31913 request to resume previous session.
6|Feb 15 2011|13:01:58|725001|RFCSERVER|31913|||Starting SSL handshake with client
INSIDE-RFCLUB:RFCSERVER/31913 for TLSv1 session.
```

Figure 4.1.13. Real-time log: SSL handshake process.

```
6|Feb 15 2011|13:02:22|302020|10.255.255.101|1280|RFCSERVER|0|Built inbound ICMP
connection for faddr 10.255.255.101/1280 gaddr RFCSERVER/0 laddr RFCSERVER/0
(sfink)

6|Feb 15 2011|13:02:22|302014|192.168.4.15|1619|192.168.1.210|8889|Teardown TCP
connection 18492859 for COMCAST:192.168.4.15/1619 to INSIDE-
RFCLUB:192.168.1.210/8889 duration 0:00:00 bytes 683 TCP FINs

6|Feb 15 2011|13:02:21|302021|10.255.255.101|1280|RFCSERVER|0|Teardown ICMP
connection for faddr 10.255.255.101/1280 gaddr RFCSERVER/0 laddr RFCSERVER/0
(sfink)

6|Feb 15 2011|13:02:21|302014|192.168.4.15|80|192.168.1.210|4264|Teardown TCP
connection 18492858 for COMCAST:192.168.4.15/80 to INSIDE-
RFCLUB:192.168.1.210/4264 duration 0:00:00 bytes 1059 TCP FINs

6|Feb 15 2011|13:02:21|302020|10.255.255.101|1280|RFCSERVER|0|Built inbound ICMP
connection for faddr 10.255.255.101/1280 gaddr RFCSERVER/0 laddr RFCSERVER/0
(sfink)

6|Feb 15 2011|13:02:21|302013|192.168.4.15|1619|192.168.1.210|8889|Built inbound TCP
connection 18492859 for COMCAST:192.168.4.15/1619 (192.168.4.15/1619) to INSIDE-
RFCLUB:192.168.1.210/8889 (192.168.1.210/8889)

6|Feb 15 2011|13:02:21|302014|192.168.4.15|80|192.168.1.210|4263|Teardown TCP
connection 18492856 for COMCAST:192.168.4.15/80 to INSIDE-
RFCLUB:192.168.1.210/4263 duration 0:00:01 bytes 1032 TCP FINs

6|Feb 15 2011|13:02:20|302021|10.255.255.101|1280|RFCSERVER|0|Teardown ICMP
connection for faddr 10.255.255.101/1280 gaddr RFCSERVER/0 laddr RFCSERVER/0
(sfink)

6|Feb 15 2011|13:02:20|302013|192.168.1.210|4264|192.168.4.15|80|Built outbound TCP
connection 18492858 for COMCAST:192.168.4.15/80 (192.168.4.15/80) to INSIDE-
RFCLUB:192.168.1.210/4264 (192.168.1.210/4264)
```

Figure 4.1.14. Real-time log: IPSec and SSL requests.

An IPSec tunnel exists between the mountain club network, 192.168.4.0 and the golf club network 192.168.1.0. An SSL session is on the 10.255.255.0 network. Both connections accept and send messages to the correct destination generating no errors or warnings.

ASA Configuration

Enabling the SSL VPN changes the ASA configuration files by adding few lines that define the SSL protocol (Figure 4.2). The VPN is enabled on the Comcast interface and the path to the SSL client is “disk0:/anyconnect-dart-win-2.5.2017-k9.pkg 1“.SSL is set as alias to RFCLUB-EZVPN tunnel group. RFCLUB-EZVPN is a legacy group policy used for IPSec in the past. The change appears in the policy-group attributes under “vpn-tunnel-protocol” where the SSL VPN Client (svc) is added to the IPSec.

```
webvpn
 enable COMCAST
 svc image disk0:/anyconnect-dart-win-2.5.2017-k9.pkg 1
 svc enable
 tunnel-group-list enable
group-policy DfltGrpPolicy attributes
 webvpn
  url-list value RFC
```

```
group-policy RFCLUB-EZVPN attributes
 wins-server value 192.168.1.207
 dns-server value 192.168.1.207
 vpn-tunnel-protocol IPSec svc
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value Split_Tunnel_ACL
 default-domain value rfclub
 nem enable

tunnel-group RFCLUB-EZVPN webvpn-attributes
 group-alias SSLVPN enable
```

Figure 4.2. Changes in ASA configuration file after adding SSL.

Changes due to the SSL protocol in the configuration file do not reflect on the group policy and the crypto-maps as it is able to use preexisting ones. VPNs are set to overpass the ACL rules and adding SSL does not affect them either. In this configuration SSL and IPSec have not interfering points in router’s configuration files. They avoid conflicting access control rules and the ASA is able to process and route their packets correctly.

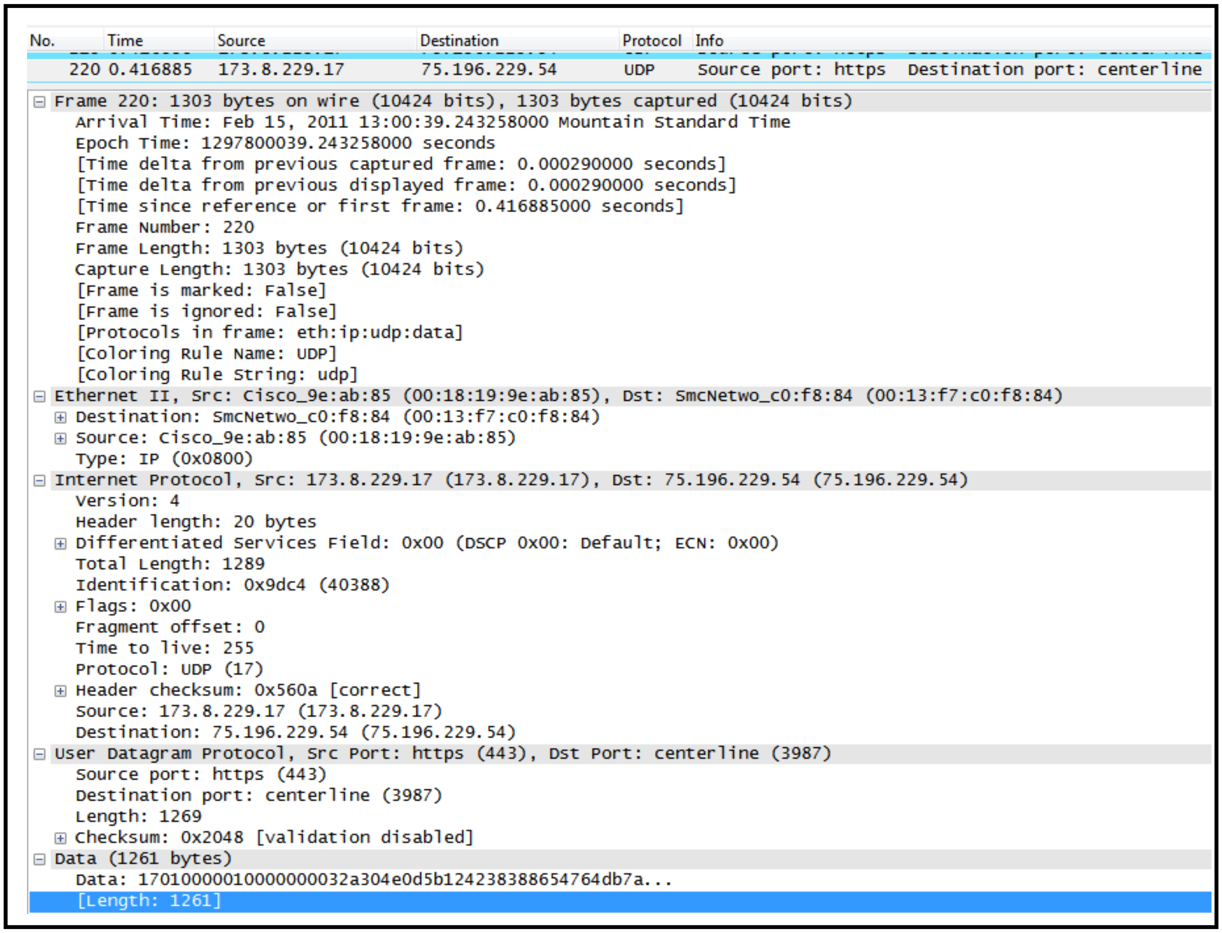
Wireshark Packet Capture and Analysis

The purpose of packet analysis is to find how the ASA appliance process VPN traffic. Different packets have to be properly encapsulated and decapsulated on both inside and outside router interfaces with correct headers depending on the VPN protocol. The following figure presents ingress traffic captured on the Comcast interface of the ASA appliance. The traffic is from both SSL and IPSec sessions consequently captured by Wireshark. For better analysis additional figures include detailed information about one packet of each VPN protocol.

```
220: 13:00:39.243258 173.8.229.17.443 > 75.196.229.54.3987:  udp
1261
 221: 13:00:39.243532 173.8.229.17.443 > 75.196.229.54.3987:  udp
1261
 222: 13:00:39.243761 173.8.229.17.443 > 75.196.229.54.3987:  udp
973
 223: 13:00:39.246401 75.196.229.54.3987 > 173.8.229.17.443:  udp 93
 224: 13:00:39.246477 75.196.229.54.3987 > 173.8.229.17.443:  udp 93
 225: 13:00:39.250505 173.164.39.77 > 173.8.229.17:  ip-proto-50,
length 1452
 226: 13:00:39.250872 173.164.39.77 > 173.8.229.17:  ip-proto-50,
length 1452
 227: 13:00:39.251314 173.164.39.77 > 173.8.229.17:  ip-proto-50,
length 1452
 228: 13:00:39.251802 173.8.229.17 > 173.164.39.77:  ip-proto-50,
length 84
 229: 13:00:39.252275 173.8.229.17 > 173.164.39.77:  ip-proto-50,
length 84
```

Figure 4.3.1. Packets captured on Comcast ingress interface.

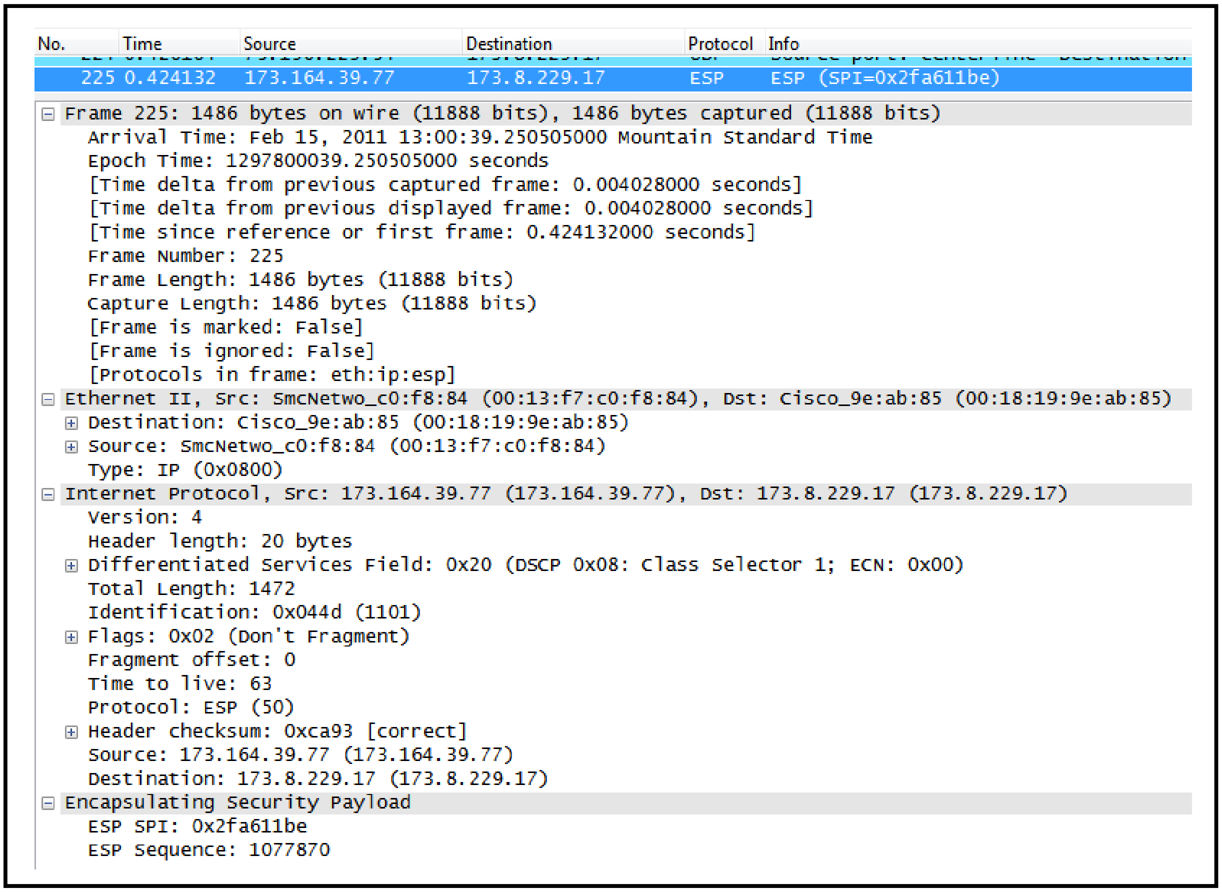
SSL session transfers data through the HTTPS protocol which is enabled in every Web browser. The IP assigned to the outside interface on the club’s router is 173.8.229.17. Employee laptop receives IP 75.196.229.54 from the Verizon wireless card. 443 is the HTTPS port that sends data from the ASA appliance to the employee’s laptop on a random high port (3987 in our case) encapsulated in UPD container. The IPSec tunnel between mountain club’s ASA 5505 and golf club's ASA 5510 respectively with IPs 173.164.39.77 and 173.8.229.17 encapsulate data with IP protocol 50. Protocol 50 identifies encapsulating security payload (ESP) which is a member of the IPSec protocol suite.



```
No.  Time       Source         Destination     Protocol  Info
 220 0.416885   173.8.229.17   75.196.229.54   UDP       Source port: https   Destination port: centerline

⊟ Frame 220: 1303 bytes on wire (10424 bits), 1303 bytes captured (10424 bits)
    Arrival Time: Feb 15, 2011 13:00:39.243258000 Mountain Standard Time
    Epoch Time: 1297800039.243258000 seconds
    [Time delta from previous captured frame: 0.000290000 seconds]
    [Time delta from previous displayed frame: 0.000290000 seconds]
    [Time since reference or first frame: 0.416885000 seconds]
    Frame Number: 220
    Frame Length: 1303 bytes (10424 bits)
    Capture Length: 1303 bytes (10424 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ip:udp:data]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
⊟ Ethernet II, Src: Cisco_9e:ab:85 (00:18:19:9e:ab:85), Dst: SmcNetwo_c0:f8:84 (00:13:f7:c0:f8:84)
  ⊞ Destination: SmcNetwo_c0:f8:84 (00:13:f7:c0:f8:84)
  ⊞ Source: Cisco_9e:ab:85 (00:18:19:9e:ab:85)
    Type: IP (0x0800)
⊟ Internet Protocol, Src: 173.8.229.17 (173.8.229.17), Dst: 75.196.229.54 (75.196.229.54)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 1289
    Identification: 0x9dc4 (40388)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 255
    Protocol: UDP (17)
  ⊞ Header checksum: 0x560a [correct]
    Source: 173.8.229.17 (173.8.229.17)
    Destination: 75.196.229.54 (75.196.229.54)
⊟ User Datagram Protocol, Src Port: https (443), Dst Port: centerline (3987)
    Source port: https (443)
    Destination port: centerline (3987)
    Length: 1269
  ⊞ Checksum: 0x2048 [validation disabled]
⊟ Data (1261 bytes)
    Data: 1701000001000000000032a304e0d5b124238388654764db7a...
    [Length: 1261]
```

Figure 4.3.2. Detailed information for SSL session: encapsulated frame No. 220.

The additional SSL frame information reveals that it a common Ethernet frame that includes a UDP packet sent between two peers using the HTTPS protocol. It includes source and destination MAC address, source and destination IP address, source and destination ports, control data, and frame consequent number. The SSL session frame does not differ from a common HTTPS frame and it is confirmed by the figures above.



```
No.   Time      Source          Destination     Protocol Info
  225 0.424132  173.164.39.77   173.8.229.17    ESP      ESP (SPI=0x2fa611be)

⊟ Frame 225: 1486 bytes on wire (11888 bits), 1486 bytes captured (11888 bits)
    Arrival Time: Feb 15, 2011 13:00:39.250505000 Mountain Standard Time
    Epoch Time: 1297800039.250505000 seconds
    [Time delta from previous captured frame: 0.004028000 seconds]
    [Time delta from previous displayed frame: 0.004028000 seconds]
    [Time since reference or first frame: 0.424132000 seconds]
    Frame Number: 225
    Frame Length: 1486 bytes (11888 bits)
    Capture Length: 1486 bytes (11888 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ip:esp]
⊟ Ethernet II, Src: SmcNetwo_c0:f8:84 (00:13:f7:c0:f8:84), Dst: Cisco_9e:ab:85 (00:18:19:9e:ab:85)
  ⊞ Destination: Cisco_9e:ab:85 (00:18:19:9e:ab:85)
  ⊞ Source: SmcNetwo_c0:f8:84 (00:13:f7:c0:f8:84)
    Type: IP (0x0800)
⊟ Internet Protocol, Src: 173.164.39.77 (173.164.39.77), Dst: 173.8.229.17 (173.8.229.17)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x20 (DSCP 0x08: Class Selector 1; ECN: 0x00)
    Total Length: 1472
    Identification: 0x044d (1101)
  ⊞ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 63
    Protocol: ESP (50)
  ⊞ Header checksum: 0xca93 [correct]
    Source: 173.164.39.77 (173.164.39.77)
    Destination: 173.8.229.17 (173.8.229.17)
⊟ Encapsulating Security Payload
    ESP SPI: 0x2fa611be
    ESP Sequence: 1077870
```

Figure 4.3.3. Detailed information for IPSec session: encapsulated frame No. 225.

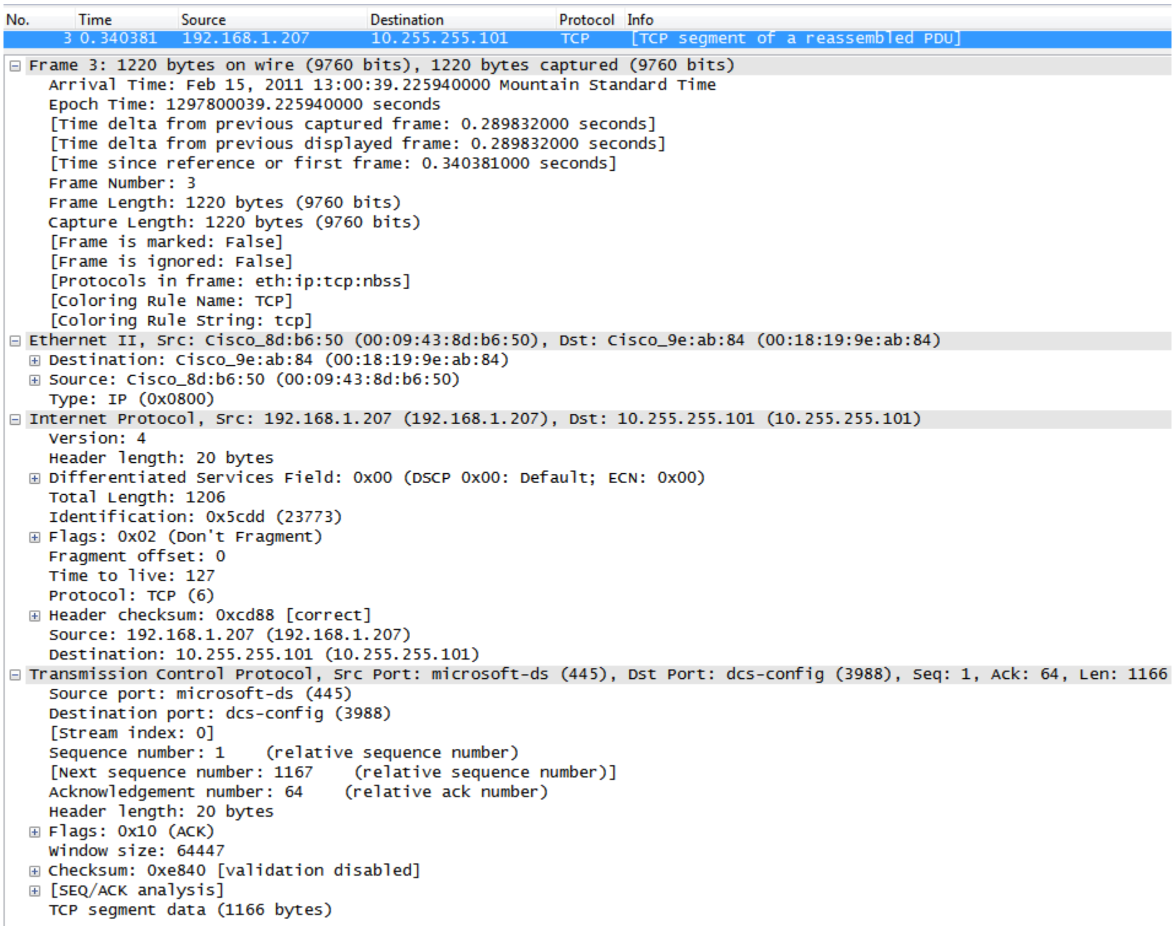
IPSec tunnels transfer packets encapsulated in ESP container. The frame consists of Ethernet, IP, and ESP protocols. ESP encapsulates the TCP and UDP protocols and they stay transparent to the Ethernet frame. The frame contains information similar to the one in the SSL frame differing only by the sequence number which is common for the TCP protocol.

The ASA routers produce and receive valid SSL and IPSec session frames with correct encapsulation and valid headers. Packet sequence is strictly followed and it is not disturbed by the two VPN protocols running simultaneous sessions.

The next figures depict the router’s decapsulation abilities i.e. the egress data from the inside interface of the ASA appliance.

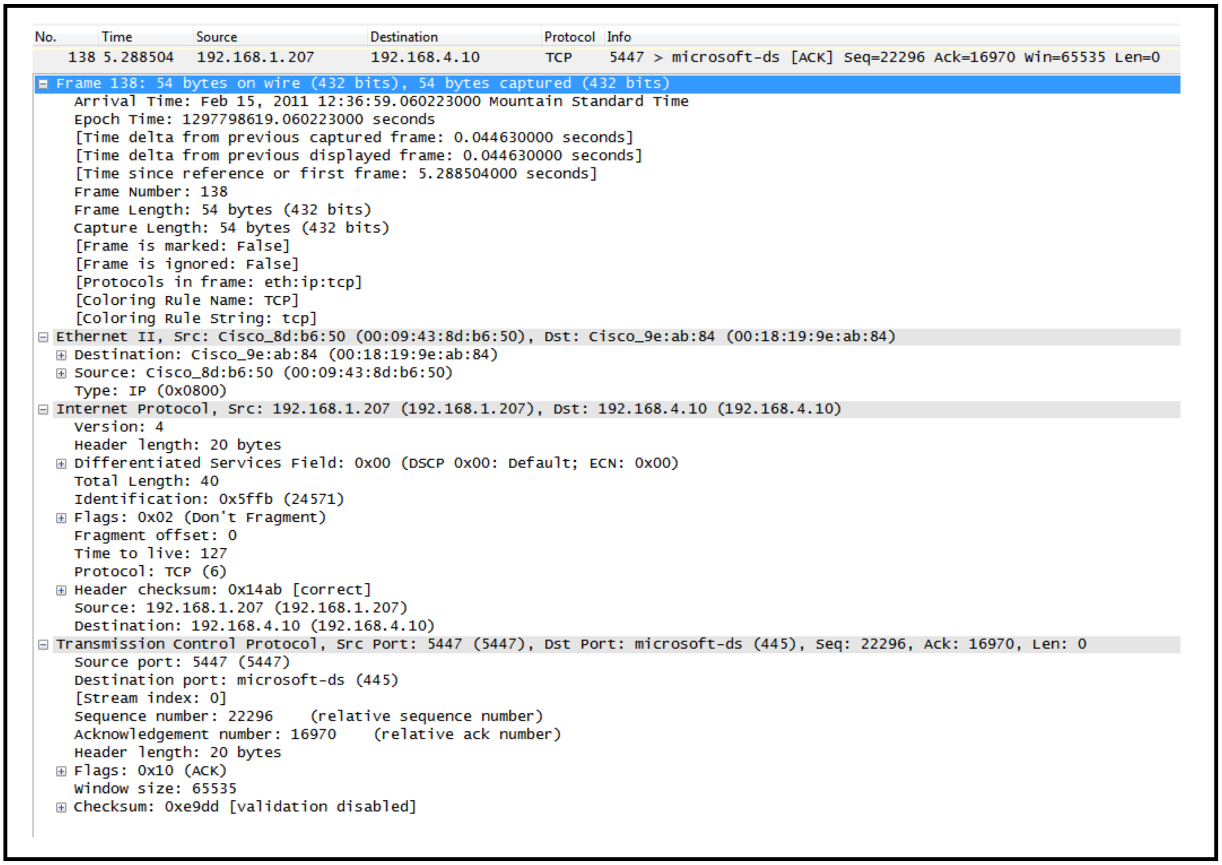
```
3: 13:00:39.225940 192.168.1.207.445 > 10.255.255.101.3988: .
3369242874:3369244040(1166) ack 1489450167 win 64447
4: 13:00:39.226505 192.168.1.207.445 > 10.255.255.101.3988: .
3369244040:3369245206(1166) ack 1489450167 win 64447
5: 13:00:39.227023 192.168.1.207.445 > 10.255.255.101.3988: .
3369245206:3369246372(1166) ack 1489450167 win 64447

5668: 12:37:42.641705 192.168.1.207.5447 > 192.168.4.10.445: . ack
179053373 win 65535
5669: 12:37:42.642697 192.168.1.207.5447 > 192.168.4.10.445: . ack
179057513 win 65535
5670: 12:37:42.648510 192.168.1.207.5447 > 192.168.4.10.445: . ack
179060273 win 65535
```

Figure 4.3.4. Packets captured on ASA inside network interface.



```
No.    Time       Source          Destination      Protocol  Info
     3 0.340381   192.168.1.207   10.255.255.101   TCP       [TCP segment of a reassembled PDU]
⊟ Frame 3: 1220 bytes on wire (9760 bits), 1220 bytes captured (9760 bits)
    Arrival Time: Feb 15, 2011 13:00:39.225940000 Mountain Standard Time
    Epoch Time: 1297800039.225940000 seconds
    [Time delta from previous captured frame: 0.289832000 seconds]
    [Time delta from previous displayed frame: 0.289832000 seconds]
    [Time since reference or first frame: 0.340381000 seconds]
    Frame Number: 3
    Frame Length: 1220 bytes (9760 bits)
    Capture Length: 1220 bytes (9760 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ip:tcp:nbss]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
⊟ Ethernet II, Src: Cisco_8d:b6:50 (00:09:43:8d:b6:50), Dst: Cisco_9e:ab:84 (00:18:19:9e:ab:84)
  ⊞ Destination: Cisco_9e:ab:84 (00:18:19:9e:ab:84)
  ⊞ Source: Cisco_8d:b6:50 (00:09:43:8d:b6:50)
    Type: IP (0x0800)
⊟ Internet Protocol, Src: 192.168.1.207 (192.168.1.207), Dst: 10.255.255.101 (10.255.255.101)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 1206
    Identification: 0x5cdd (23773)
  ⊞ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 127
    Protocol: TCP (6)
  ⊞ Header checksum: 0xcd88 [correct]
    Source: 192.168.1.207 (192.168.1.207)
    Destination: 10.255.255.101 (10.255.255.101)
⊟ Transmission Control Protocol, Src Port: microsoft-ds (445), Dst Port: dcs-config (3988), Seq: 1, Ack: 64, Len: 1166
    Source port: microsoft-ds (445)
    Destination port: dcs-config (3988)
    [Stream index: 0]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 1167    (relative sequence number)]
    Acknowledgement number: 64    (relative ack number)
    Header length: 20 bytes
  ⊞ Flags: 0x10 (ACK)
    Window size: 64447
  ⊞ Checksum: 0xe840 [validation disabled]
  ⊞ [SEQ/ACK analysis]
    TCP segment data (1166 bytes)
```

Figure 4.3.5. Detailed information for SSL session: decapsulated frame No. 3.



```
No.   Time      Source          Destination     Protocol Info
  138 5.288504  192.168.1.207   192.168.4.10    TCP      5447 > microsoft-ds [ACK] Seq=22296 Ack=16970 Win=65535 Len=0

⊟ Frame 138: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
    Arrival Time: Feb 15, 2011 12:36:59.060223000 Mountain Standard Time
    Epoch Time: 1297798619.060223000 seconds
    [Time delta from previous captured frame: 0.044630000 seconds]
    [Time delta from previous displayed frame: 0.044630000 seconds]
    [Time since reference or first frame: 5.288504000 seconds]
    Frame Number: 138
    Frame Length: 54 bytes (432 bits)
    Capture Length: 54 bytes (432 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ip:tcp]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
⊟ Ethernet II, Src: Cisco_8d:b6:50 (00:09:43:8d:b6:50), Dst: Cisco_9e:ab:84 (00:18:19:9e:ab:84)
  ⊞ Destination: Cisco_9e:ab:84 (00:18:19:9e:ab:84)
  ⊞ Source: Cisco_8d:b6:50 (00:09:43:8d:b6:50)
    Type: IP (0x0800)
⊟ Internet Protocol, Src: 192.168.1.207 (192.168.1.207), Dst: 192.168.4.10 (192.168.4.10)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 40
    Identification: 0x5ffb (24571)
  ⊞ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 127
    Protocol: TCP (6)
  ⊞ Header checksum: 0x14ab [correct]
    Source: 192.168.1.207 (192.168.1.207)
    Destination: 192.168.4.10 (192.168.4.10)
⊟ Transmission Control Protocol, Src Port: 5447 (5447), Dst Port: microsoft-ds (445), Seq: 22296, Ack: 16970, Len: 0
    Source port: 5447 (5447)
    Destination port: microsoft-ds (445)
    [Stream index: 0]
    Sequence number: 22296    (relative sequence number)
    Acknowledgement number: 16970    (relative ack number)
    Header length: 20 bytes
  ⊞ Flags: 0x10 (ACK)
    Window size: 65535
  ⊞ Checksum: 0xe9dd [validation disabled]
```

Figure 4.3.6. Detailed information for IPSec session: decapsulated frame No. 225.

Frames captured from the inside ASA interface have smaller size as the decapsulation process removes IPSec and SSL headers and trailers used to transfer frames through the public network. The IP protocol contains destination and source addresses of machines on the local network and packets are ready to be routed to the designated destination. The captured SSL packet carries data from reassembled Protocol Data Unit (PDU). The important information in the frame is the IP destination and source address. 10.255.255.101 is the employee laptop IP address assigned to the SSL client from the DHCP server. 192.168.1.207 is the club’s server address. All information in the packet is correct meaning the decapsulation of the SSL packet is successful and the packet can be processed further on the local network. Source and destination IPs in the IPSec packet also confirm successful decapsulation as 192.168.1.207 and 192.168.4.10 are golf club and respectively mountain club server IP addresses.

Decapsulation is applied simultaneously on IPSec and SSL session packets and the result is valid data packets with correct LAN source and destination address as well as valid control information. ASA appliance is able to correctly decapsulate simultaneously sent IPSec and SSL packets.

VPN Maintenance Requirements

Setup and maintenance are important factors for both technologies to be utilized properly. The table below identifies what is the time required to set up an IPSec site-to-site, IPSec remote access, and SSL client VPNs. It also includes the times to add an IPSec tunnel, and to add a SSL remote connection. ASDM software is the primary tool for ASA VPN configuration.

Table 4.1. *Times to setup IPSec and SSL virtual networks*

VPN \ Time	*Time to Set Up*	*Time to Resolve Issues*
IPSec Site-to-Site	40 min (with matching devices)	60 min
IPSec Remote Access	40 min	60 min
SSL AnyConnect	20 min	30 min
Add IPSec Remote Access	40 min	N/A
Add SSL AnyConnect	10 min	N/A

Times presented in the table are taken from an interview with the club’s network administrator and from observation during the study that included VPN configuration and maintenance. The approximate time to set up the IPSec tunnel between the ASA 5510 and ASA 5505 is 40 minutes. A previous attempt to establish an IPSec tunnel between ASA 5510 and Cisco 1811 (before adding the ASA 5505) escalated to 2 hours and the tunnel was unstable and unreliable. Matching devices is a plus that needs to be taken in account when configuring VPN connections. IPSec remote access takes the same amount of time as the VPN client has to be installed and configured on a laptop. Having a desktop for remote connection requires the administrator to visit the location which increases the overall time for configuration. Time for additional IPSec connections do not differ from the time for basic setup as the same process needs to be repeated again.

SSL AnyConnect requires configuration only on the main ASA appliance and the setup time is less than the one for the IPSec. Resoling issues on the IPSec VPN connections is also time-consuming considering the two locations that need to be examined. Additional SSL connections are time consuming only if the user requires different credentials than the existing ones. Creating new user with specific access restrictions takes 10 minutes out of the network administrator’s time. SSL AnyConnect has the ability to completely replace the IPSec client for traveling agents or working from home employees. With that in mind, maintaining SSL AnyConnect and site-to-site VPNs reduce time to employ remote connections and respectively increases administrator’s productivity. Simultaneous SSL and IPSec implementation optimizes network administrator work and releases extra time for regular network maintenance jobs.

Cost Effect on Adding SSL VPN

The study is mainly focused on Cisco ASA 5510 security appliance and its ability to support IPSec and SSL sessions simultaneously. The device is the second most inexpensive model from the ASA family after the ASA 5505. It covers the connectivity needs of a small to medium size organization such as the golf club where the study is conducted. According to Cisco specifications the appliance is capable of 250 IPSec and 250 SSL concurrent sessions. By contrasts with IPSec, SSL AnyConnect peers are subject of license purchase. The basic license that comes with the ASA router allows 2 AnyConnect peers. Further levels include acquisition of

10, 25, 50, 100, or 250 SSL peers. The following table contains SSL and IPSec cost for the different number of connections. Prices are taken from CDW which is one of the biggest providers for business IT solutions.

Table 4.2. *SSL and IPSec cost per number of connections*

Cost per number Of VPN connections	SSL AnyConnect	IPSec
2	Included	Included
10	$772.99	Included
25	$2099.99	Included
50	$2469.99	Included
100	$4939.99	Included
250	$12349.99	Included

SSL license cost is affordable for a medium business but it is still not free as the IPSec VPN. It should be pointed out that only basic IPSec setup is free. Use of 3DES and AES strong encryption requires a license that worth $939.99 or almost the price for 10 SSL peers.

The computer network in the presented study is supported by one network administrator. The current number of employees using remote connection is 12 which is comparatively low and IPSec tunnels are manageable by one systems administrator. With the continuous development of the ski club and the planned expansion of the golf club, the number of employees that will require full, occasional remote connection tends to reach 30-35. That number of IPSec VPNs will be overloading for one person and the 50 users SSL is the better solution for the case. Combining IPSec and SSL requires more investments but the benefits overcome the price.

Chapter 6 – Conclusions

IPSec and SSL are two Virtual Private Network technologies that provide a cost-effective and secure way to include remote locations to a main corporate network. They replace the expensive leased lines with the common public network, the Internet. IPSec is the better solution for site-to-site VPN. It provides more flexibility, more security, and more controllable network environment for stationary remote locations. SSL is suitable for travelling agents or employees working from home that need occasional, limited access to the organization's network. Most businesses regardless of their size include both of these elements, remote offices and remote workers. Implementing IPSec and SSL simultaneously is the logical solution to meet organizations' heterogeneous remote connection needs.

Leading network equipment manufacturers like Cisco and Netgear respond to the market needs with edge gear that allows simultaneous IPSec and SSL implementation. In terms of affordability, edge router with VPN capabilities including remote peer licenses reach cost of $4000. The price allows small and mid-size organization to include both VPN technologies in their networks which was highly expensive in the past.

In terms of technical compatibility, SSL and IPSec are complementary technologies that can be enabled in one network device. Evaluation of the experimental results from Cisco's ASA 5510, show no issues with the two technologies working together. Device's hardware is able to utilize all sessions with minimal hardware load, without dropping packets, and without errors. VPN sessions do not affect router's performance.

The ASA security appliance is able to encapsulate, decapsulate, and route VPN packets correctly maintaining stable SSL and IPSec connections. For a two-hour session of data transfer, there are zero failed requests, no packet errors, and no interference between the two protocols. The DHCP server assigns correct IP addressed to the remote location through the VPN protocols allowing correct routing functions before and after capsulation processes. Two hours is the approximate time needed for a remote worker to use the SSL session to finish the daily tasks. It is the actual period of time when the two VPN protocols run simultaneously.

VPN interacts tightly with other network functions such as QoS, NAT, and Firewalls. SSL and IPSec functionality with these technologies is of a big concern in the study. The bottom line is: there are no technical issues with the ASA router's performance utilizing co-existing SSL and IPSec through NAT-T and ACL rules. Correct implementation is subject of thorough configuration of the security appliance and respectively administrator's knowledge of these technologies. Although, combination of SSL and IPSec reduces the workload on network administrators, their simultaneous implementation requires substantial knowledge and deep understanding of the VPN technologies.

References

Basha, A. (2005). Analysis of Enterprise VPNs. ECE 646 – Cryptography and Computer Network Security. Retrieved November, 2010 from http://ece.gmu.edu/coursewebpages/ECE/ECE646/F09/project/reports_2005/VPN_report.pdf

Cisco (2010). Cisco Secure Remote Access Cisco ASA 5500 Series SSL/IPSec VPN Edition. Retrieved January, 2011 from http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/prod_brochure0900aecd80402e39.html

Daye, M. (2007). Virtual Private Networks: IPSec vs. SSL. ICTN 4040-001, April 16th 2007. Retrieved January, 2011 from http://www.infosecwriters.com/text_resources/pdf/VPN_MDaye.pdf

Deal, R. (2005). The Complete Cisco VPN Configuration Guide. Cisco Press, ISBN-10: 1-58705-204-0 (pp. 622-698)

Diab, W., Tohme, S., & Bassil, C. (2007). Critical VPN Security Analysis and New Approach for Securing VoIP Communications over VPN Networks. *ACM Digital Library*. Retrieved July 15, 2010 from http://delivery.acm.org.dml.regis.edu/10.1145/1300000/1298238/p92-boudiab.pdf?key1=1298238&key2=4450531721&coll=Portal&dl=ACM&CFID=86296516&CFTOKEN=66339951

Frankel, Sh., Hoffman, P., Orebaugh, A., Park, R. (2008). Guide to SSL VPNs. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-113. Retrieved November, 2010 from http://csrc.nist.gov/publications/nistpubs/800-113/SP800-113.pdf

Heary, J. (2009). Cisco Regains Top Spot in IPS Market. Network World Blogs & Columns. Retrieved January, 2011 from http://www.networkworld.com/community/node/49176

Heller, M. (2006). What You Need to Know about VPN Technologies, How They Work, What They Can Do for You, Problems to Watch For. Computer World UK, Published: 00:00 GMT, 01 September 06. Retrieved December, 2010 from http://features.techworld.com/networking/2763/what-you-need-to-know-about-vpn-technologies/

National Webcast Initiative (2005). IPSec and SSL: Complimentary VPN Technologies for Universal Remote Access. Retrieved November, 2010 from http://www.msisac.org/webcast/2005-07/info/ip_sec_ssl.pdf

Appendix

ASA 5510 Full Running Configuration File

```
Cryptochecksum: f525f2f2 95465b8e 274a9cd6 c3415371
: Saved
: Written by ***** at 15:34:37.292 MST Wed Feb 9 2011
!
ASA Version 8.0(4)
!
hostname edge
domain-name rfclub.com
enable password ***** encrypted
passwd ***** encrypted
names
name 192.168.1.207 RFCSERVER
name 192.168.1.206 TERMINALSERVER
name 192.168.1.54 Bellstaff
name 192.168.1.253 BARRACUDA
dns-guard
!
interface Ethernet0/0
 description Inside Interface to the RFClub LAN
 nameif INSIDE-RFCLUB
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
```

```
interface Ethernet0/1
 nameif COMCAST
 security-level 0
 ip address 173.8.229.17 255.255.255.248
!
interface Ethernet0/2
 description Interface to Guest networks
 nameif GUEST
 security-level 50
 ip address 10.0.0.1 255.255.255.0
!
interface Ethernet0/3
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface Management0/0
 shutdown
 nameif management
 security-level 100
 ip address 172.16.29.254 255.255.255.0
 management-only
!
boot system disk0:/asa822-k8.bin
boot system disk0:/asa804-k8.bin
```

```
ftp mode passive

clock timezone MST -7

clock summer-time MDT recurring

dns domain-lookup INSIDE-RFCLUB

dns server-group DefaultDNS

 name-server RFCSERVER

 name-server 216.237.77.2

 domain-name rfclub.com

same-security-traffic permit inter-interface

same-security-traffic permit intra-interface

object-group network Jonas

 network-object host 209.225.60.144

 network-object host 209.225.60.145

 network-object host 209.225.60.146

 network-object host 209.225.60.147

 network-object host 209.225.60.148

 network-object host 209.225.60.149

 network-object host 146.145.52.238

 network-object host 206.186.126.226

object-group service BARRACUDA

 service-object tcp eq *****

 service-object tcp eq smtp

object-group service RFCSERVER

 service-object tcp eq *****

 service-object tcp eq www

 service-object tcp eq https
 service-object tcp eq *****
object-group service TERMINALSERVER
 service-object tcp eq *****
access-list COMCAST_cryptomap extended permit ip 192.168.1.0
255.255.255.0 10.100.10.0 255.255.254.0
access-list RFCLUB_nat0_outbound extended permit ip 192.168.1.0
255.255.255.0 10.100.10.0 255.255.254.0
access-list RFCLUB_nat0_outbound extended permit ip 192.168.1.0
255.255.255.0 10.255.255.0 255.255.255.0
access-list RFCLUB_nat0_outbound extended permit ip 192.168.1.0
255.255.255.0 192.168.100.0 255.255.255.0
access-list RFCLUB_nat0_outbound extended permit ip 192.168.1.0
255.255.255.0 192.168.4.0 255.255.255.0
access-list COMCAST_2_cryptomap extended permit ip 192.168.1.0
255.255.255.0 192.168.4.0 255.255.255.0
access-list GUEST_access_in extended permit ip any any
access-list OUTSIDE_cryptomap extended permit ip any 10.255.255.0
255.255.255.0
access-list Split_Tunnel_ACL standard permit 192.168.1.0 255.255.255.0
access-list COMCAST_access_in extended permit object-group BARRACUDA
any host 173.8.229.18
access-list COMCAST_access_in extended permit object-group RFCSERVER
any host 173.8.229.19
access-list COMCAST_access_in extended permit object-group
TERMINALSERVER any host 173.8.229.20
```

```
access-list COMCAST_access_in extended permit tcp any host
173.8.229.17 eq 200
access-list COMCAST_access_in extended permit tcp any host
173.8.229.17 eq 212
access-list COMCAST_3_cryptomap extended permit ip 192.168.1.0
255.255.255.0 192.168.100.0 255.255.255.0
pager lines 24
logging enable
logging asdm informational
mtu INSIDE-RFCLUB 1500
mtu COMCAST 1500
mtu GUEST 1500
mtu management 1500
ip local pool EZVPN-POOL 10.255.255.101-10.255.255.200 mask
255.255.255.0
no failover
icmp unreachable rate-limit 1 burst-size 1
icmp permit any INSIDE-RFCLUB
icmp permit any echo COMCAST
icmp permit any echo-reply COMCAST
asdm image disk0:/asdm-631.bin
no asdm history enable
arp timeout 14400
global (COMCAST) 1 interface
global (COMCAST) 2 173.8.229.21 netmask 255.255.0.0
nat (INSIDE-RFCLUB) 0 access-list RFCLUB_nat0_outbound
nat (INSIDE-RFCLUB) 1 0.0.0.0 0.0.0.0
nat (GUEST) 2 0.0.0.0 0.0.0.0
static (INSIDE-RFCLUB,COMCAST) tcp interface 200 192.168.1.200 www
netmask 255.255.255.255
static (INSIDE-RFCLUB,COMCAST) 173.8.229.18 BARRACUDA netmask
255.255.255.255
static (INSIDE-RFCLUB,COMCAST) 173.8.229.19 RFCSERVER netmask
255.255.255.255
static (INSIDE-RFCLUB,COMCAST) 173.8.229.20 TERMINALSERVER netmask
255.255.255.255
access-group COMCAST_access_in in interface COMCAST
access-group GUEST_access_in in interface GUEST
route COMCAST 0.0.0.0 0.0.0.0 173.8.229.22 1
route INSIDE-RFCLUB 192.168.2.0 255.255.255.0 192.168.1.254 1
route INSIDE-RFCLUB 192.168.3.0 255.255.255.0 192.168.1.254 1
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
dynamic-access-policy-record DfltAccessPolicy
aaa authentication http console LOCAL
aaa authentication serial console LOCAL
aaa authentication ssh console LOCAL
aaa authentication telnet console LOCAL
aaa authentication enable console LOCAL
http server enable
http 75.151.95.141 255.255.255.255 COMCAST
http 0.0.0.0 0.0.0.0 INSIDE-RFCLUB
http 172.16.29.0 255.255.255.0 management
http 173.14.13.25 255.255.255.255 COMCAST
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
crypto ipsec transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
crypto ipsec transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac
crypto ipsec transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac
crypto ipsec transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac
crypto ipsec transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
crypto dynamic-map OUTSIDE_dyn_map 20 set transform-set ESP-AES-128-SHA
crypto dynamic-map OUTSIDE_dyn_map 20 set security-association lifetime seconds 28800
crypto dynamic-map OUTSIDE_dyn_map 20 set security-association
lifetime kilobytes 4608000
crypto dynamic-map COMCAST_dyn_map 1 set pfs
crypto dynamic-map COMCAST_dyn_map 1 set transform-set ESP-AES-128-SHA
ESP-3DES-SHA ESP-3DES-MD5
crypto dynamic-map COMCAST_dyn_map 1 set security-association lifetime
seconds 28800
crypto dynamic-map COMCAST_dyn_map 1 set security-association lifetime
kilobytes 4608000
crypto map OUTSIDE_map 100 ipsec-isakmp dynamic OUTSIDE_dyn_map
crypto map COMCAST_map0 1 match address COMCAST_cryptomap
crypto map COMCAST_map0 1 set pfs
crypto map COMCAST_map0 1 set peer 75.145.121.41
crypto map COMCAST_map0 1 set transform-set ESP-3DES-SHA
crypto map COMCAST_map0 1 set security-association lifetime seconds
28800
crypto map COMCAST_map0 1 set security-association lifetime kilobytes
4608000
crypto map COMCAST_map0 2 match address COMCAST_2_cryptomap
crypto map COMCAST_map0 2 set pfs
crypto map COMCAST_map0 2 set peer 173.164.39.77
crypto map COMCAST_map0 2 set transform-set ESP-3DES-SHA
crypto map COMCAST_map0 2 set security-association lifetime seconds
28800
crypto map COMCAST_map0 2 set security-association lifetime kilobytes
4608000
```

```
crypto map COMCAST_map0 3 match address COMCAST_3_cryptomap
crypto map COMCAST_map0 3 set peer 173.14.13.25
crypto map COMCAST_map0 3 set transform-set ESP-DES-MD5
crypto map COMCAST_map0 3 set security-association lifetime seconds
28800
crypto map COMCAST_map0 3 set security-association lifetime kilobytes
4608000
crypto map COMCAST_map0 65535 ipsec-isakmp dynamic COMCAST_dyn_map
crypto map COMCAST_map0 interface COMCAST
crypto isakmp identity address
crypto isakmp enable COMCAST
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto isakmp policy 30
 authentication pre-share
 encryption aes
 hash sha
 group 2
 lifetime 86400
crypto isakmp policy 50
 authentication pre-share
 encryption des
 hash md5
 group 1
 lifetime 86400
crypto isakmp ipsec-over-tcp port 10000
telnet 192.168.0.0 255.255.252.0 INSIDE-RFCLUB
telnet 172.16.29.0 255.255.255.0 management
telnet timeout 5
ssh 0.0.0.0 0.0.0.0 INSIDE-RFCLUB
ssh 0.0.0.0 0.0.0.0 COMCAST
ssh 172.16.29.0 255.255.255.0 management
ssh timeout 5
console timeout 0
management-access INSIDE-RFCLUB
dhcpd address 10.0.0.101-10.0.0.200 GUEST
dhcpd dns 216.237.77.2 205.171.3.65 interface GUEST
dhcpd lease 28800 interface GUEST
dhcpd domain rflcub.com interface GUEST
dhcpd enable GUEST
!
dhcpd address 172.16.29.1-172.16.29.5 management
dhcpd enable management
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ntp server 192.43.244.18 source INSIDE-RFCLUB prefer
```

```
webvpn
 enable COMCAST
 svc image disk0:/anyconnect-dart-win-2.5.2017-k9.pkg 1
 svc enable
 tunnel-group-list enable
group-policy DfltGrpPolicy attributes
 webvpn
  url-list value RFC
group-policy RFCLUB-EZVPN internal
group-policy RFCLUB-EZVPN attributes
 wins-server value 192.168.1.207
 dns-server value 192.168.1.207
 vpn-tunnel-protocol IPSec svc
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value Split_Tunnel_ACL
 default-domain value rfclub
 nem enable
username ***** password ***** encrypted privilege 15
username ***** password ***** encrypted
username ***** password ***** encrypted privilege 15
username ***** password ***** encrypted
username ***** password ***** encrypted
username ***** password ***** encrypted
username ***** password ***** encrypted privilege 0
username ***** attributes
 vpn-group-policy RFCLUB-EZVPN
```

```
username ***** password ***** encrypted
username ***** password ***** encrypted
tunnel-group 75.145.121.41 type ipsec-l2l
tunnel-group 75.145.121.41 ipsec-attributes
 pre-shared-key rfclub-letmein
tunnel-group 173.164.39.77 type ipsec-l2l
tunnel-group 173.164.39.77 ipsec-attributes
 pre-shared-key rfclub-letmein
tunnel-group RFCLUB-EZVPN type remote-access
tunnel-group RFCLUB-EZVPN general-attributes
 address-pool EZVPN-POOL
 default-group-policy RFCLUB-EZVPN
tunnel-group RFCLUB-EZVPN webvpn-attributes
 group-alias SSLVPN enable
tunnel-group RFCLUB-EZVPN ipsec-attributes
 pre-shared-key rfclub-letmein
tunnel-group 173.14.13.25 type ipsec-l2l
tunnel-group 173.14.13.25 ipsec-attributes
 pre-shared-key rfclub-letmein
!
class-map global-class
 match default-inspection-traffic
class-map GUEST-class
 match any
!
!
```

```
policy-map global-policy
 class global-class
  inspect ctiqbe
  inspect dcerpc
  inspect dns
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect http
  inspect icmp
  inspect icmp error
  inspect ils
  inspect ipsec-pass-thru
  inspect mgcp
  inspect netbios
  inspect pptp
  inspect rsh
  inspect rtsp
  inspect sip
  inspect skinny
  inspect snmp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect xdmcp
policy-map GUEST-policy
```

```
 class GUEST-class
  police input 2000000 1500
  police output 2000000 1500
!
service-policy global-policy global
service-policy GUEST-policy interface GUEST
prompt hostname context
Cryptochecksum:f525f2f295465b8e274a9cd6c3415371
: end
```

Annotated Bibliography

Bandel, D. (1998). CIDR: A Prescription for Shortness of Address Space. *Linux Journal, Volume 1998, Issue 56.* Retrieved from http://delivery.acm.org.dml.regis.edu/10.1145/330000/327570/a2-bandel.html?key1=327570&key2=0133591721&coll=ACM&dl=ACM&CFID=85482937&CFTOKEN=99241540

The article describes the concept of IP address spacing and the limitation of current Internet Protocol version, IPv4. It presents Classless Inter-Domain Routing (CIDR) as a solution for this shortage until the next generation IPv6 arrives. The article provides a simple description of public and private address space concept as well as of the relationship between them.

Basu, A. & Riecke (2001). Stability issues in OSPF routing. *SIGCOMM Computer Communication Review, Volume 31, Issue 4.* Retrieved from http://delivery.acm.org.dml.regis.edu/10.1145/390000/383077/p225-basu.pdf?key1=383077&key2=5937591721&coll=ACM&dl=ACM&CFID=85482937&CFTOKEN=99241540

The paper studies the stability of OSPF routing protocol under three conditions: OSPF deployed with TE extensions, OSPF deployed in networks with subsecond HELLO, and OSPF deployed in networks with alternative strategies for obtaining link-state information. The study finds that TE extensions do not change the OSPF stability while HELLO timers improve the convergence times. The authors provide valuable information for OSPF protocol and its parameters.

Bellovin, S. & Cheswick, W. (1994). Network Firewalls. *IEEE Communication Magazine, Volume 32, Issue 9*. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.127.5591&rep=rep1&type=pdf

The paper examines network firewalls, their components, and types. It describes the challenges they provide to network administrators and gives examples of possible solutions. The authors conclude that each firewall configuration should be unique to serve the unique requirements of each network.

Blake, E. (2007). Network Security: VoIP Security on Data Network – A Guide. *InfoSecCD '07: Proceedings of the 4th annual conference on Information Security curriculum development*. Retrieved from http://delivery.acm.org.dml.regis.edu/10.1145/1410000/1409938/a27-blake.pdf?key1=1409938&key2=5903691721&coll=ACM&dl=ACM&CFID=85482937&CFTOKEN=99241540

The paper provides an extensive analysis of VoIP technology and the security issues associated with it. It focuses on both technical and legal aspect of the problem while examining the past and the current solutions implemented in data networks. The paper is valuable with presenting the legal side of VoIP security which is usually ignored by security engineers.

Bradley, T. (2008). Introduction to Intrusion Detection Systems (IDS). *Aboutcom: Network Security*. Retrieved from http://netsecurity.about.com/cs/hackertools/a/aa030504.htm

The article introduces IDS and its features to monitor network traffic for suspicious activities. It presents the two different IDS: network (NIDS) and host (HIDS) as well as passive and reactive IDS. The author concludes that in spite it tends to produce false alarms the technology is a great tool for network protection.

Client/Server Benefits, Problems, Best Practices (May, 1998). *Communications of the ACM/Vol. 41, No. 5*. Retrieved from http://delivery.acm.org.dml.regis.edu/10.1145/280000/274961/p87-duchessi.pdf?key1=274961&key2=3687650121&coll=ACM&dl=ACM&CFID=27461557&CFTOKEN=68536016

The article introduces the client-server systems as one of the best network technologies to increase productivity, reduce cost, and improve customer service. It points some of the difficulties connected with the client/server implementation such as inadequate internal skills, counterproductive corporate politics, etc. However, client/server implementation can be eased by recognizing its significant benefits.

Cohen, R. (2000). On the Cost of Virtual Private Networks. *IEEE/AMC Transactions on Networking, Volume 8, No. 6*. Retrieved from http://delivery.acm.org.dml.regis.edu/10.1145/360000/358919/00893873.pdf?key1=358919&key2=9186691721&coll=ACM&dl=ACM&CFID=85482937&CFTOKEN=99241540

The paper analyzes Virtual Private Networks implemented using the CPE-based approach and the network-based approach. It compares the two approaches by two factors: the cost of the VPN links and the cost of the core routers. The author presents the complexity in both scenarios and proposes heuristics to solve their problems. The paper is valuable for the cost evaluation of VPNs.

Creeger, M. (2007). Embracing Wired Networks. *ACM Digital Library*. Retrieved from http://delivery.acm.org.dml.regis.edu/10.1145/1260000/1255428/p12-creeger.pdf?key1=1255428&key2=9708770121&coll=ACM&dl=ACM&CFID=27902022&CFTOKEN=14432562

The paper includes step by step instruction how to set up a small wired network. It compares the wired and wireless networks to determine some security and privacy issues occurring in WiFi networks. The paper also provides some properties of the network equipment as well as its cost.

Diab, W., Tohme, S., & Bassil, C. (2007). Critical VPN Security Analysis and New Approach for Securing VoIP Communications over VPN Networks. *ACM Digital Library*. Retrieved from http://delivery.acm.org.dml.regis.edu/10.1145/1300000/1298238/p92-boudiab.pdf?key1=1298238&key2=4450531721&coll=Portal&dl=ACM&CFID=86296516&CFTOKEN=66339951

The paper compares different VPN protocols and the security issues associated with them. It presents IPSec as the strongest VPN solution on behalf of security but not suitable for VoIP because of its complexity, compatibility, and performance issues. The authors propose their own solution to assure VoIP traffic without reducing the effective bandwidth. The paper is significant to the research with its analysis of the VPN effect on the VoIP applications.

Emerging Wireless Technologies, CDMA 1X Technology – High Speed Data and Voice (2004). *Homeland Security, Library*. Retrieved from http://www.safecomprogram.gov/NR/rdonlyres/607B804B-C5E5-4170-9279-AC1AFA2B39ED/0/cdma1x_final.pdf

The paper focuses on the third generation CDMA-based technologies. It examines the three 3G wireless technologies 1xRTT, 1xEV-DO, and 1xEV-DV while providing information about their data rates and the enhancements they include to allow high-speed data transmission over CDMA networks.

Francis, P. & Gummadi, R. (2001). IPNL: A NAT-Extended Internet Architecture. *ACM Digital Library*. Retrieved from http://delivery.acm.org.dml.regis.edu/10.1145/390000/383065/p69-francis.pdf?key1=383065&key2=3677891121&coll=ACM&dl=ACM&CFID=70280060&CFTOKEN=89327893

The article proposes an extension to IPv4 based networks called IPNX (IP Next Layer). The authors explain the pros and cons of NAT as an extension to IPv4 and compare their solution to it.

Francois, P., & Bonaventure, O. (2007). Avoiding Transient Loops during the Convergence of Link-State Routing Protocols. *IEEE/ACM Transactions on Networking, Volume 15, Issue 6*. Retrieved from http://delivery.acm.org.dml.regis.edu/10.1145/1380000/1373482/p1280-francois.pdf?key1=1373482&key2=2018591721&coll=ACM&dl=ACM&CFID=85482937&CFTOKEN=99241540

The paper discusses the forwarding loop issue that can occur when using link-state protocol like OSPF. It presents a mechanism based on ordering forwarding tables updates that optimize network convergence and minimize the possibility of transient loops. The paper is valuable with its proposal for avoiding one the biggest issues in link-state protocols.

Gast, M. (2002). Seven Security Problems of 802.11 Wireless. *O'Reily Media Wireless Devcenter*. Retrieved from http://www.oreillynet.com/pub/a/wireless/2002/05/24/wlan.html

The article discusses seven of the most critical problems in wireless networks. Wireless security is challenging but it can be addressed by reasonable solutions. Network design is constantly changing by user demands and new technologies and security technologies needs to be flexible and adjustable to new requirements.

Glisson, W., McDonald, A., Welland, R. (2006). Web Engineering Security: A Practitioner's Perspective. *ACM DigitalLibrary*. Retrieved from http://delivery.acm.org.dml.regis.edu/10.1145/1150000/1145633/p257-glisson.pdf?key1=1145633&key2=9258474121&coll=ACM&dl=ACM&CFID=34687824&CFTOKEN=96892541

The article discusses the critical factors that drive the security in Web Engineering. The factors include economic issues, people issues, and legislative issues. The criteria are based on empirical evidence and survey made within Fortune 500 financial service organizations. The factors presented in the paper can be used to improve the security in existing Web processes and for future Web Engineering.

Goldman, J., Rawles, Ph. (2004) Applied Data Communications, Business-Oriented Approach, Fourth Edition (pp. 269-282).

The book provides comprehensive analysis of communication technologies including design, integration, deploying, and securing communication systems. The business-oriented approach presented in the book provides the needed knowledge for information systems professionals to understand today's business needs.

Guideline for The Analysis Local Area Network Security (1994). *Federal Information Processing Standards Publication 191*. Retrieved from http://csrc.nist.gov/publications/fips/fips191/fips191.pdf

The paper presents LAN technology and its main security issues. It describes the common threats that can be found in networks and the possible services and mechanisms to control them. The paper also provides information for current approaches and elements of risk management as well as examples of security policies and contingency planning.

Heller, M. (2006). What You Need to Know about VPN Technologies, How They Work, What They Can Do for You, Problems to Watch For. *Computer World UK, Published: 00:00 GMT, 01 September 06*. Retrieved from http://features.techworld.com/networking/2763/what-you-need-to-know-about-vpn-technologies/

The article follows the path of VPNs from their beginning as trusted networks (leased lines) to today's secure private lines over public packed-switched network, the Internet. The author describes several VPN protocols such as L2TP, IPSec, IPSec over L2TP, SSL, TLS as well as the benefits and the security risks they expose.

Huang, H., Chen, G., Lau, F., & Xie, L. (1999). A Distance-Vector Routing Protocol for Networks with Unidirectional Links. *HKU CSIS Tech Report TR-00-03*. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.59.6046&rep=rep1&type=pdf

The paper proposes a distance-vector routing protocol based on Routing Information Protocol (RIP). It describes in details the limitations of distance-vector protocols inherited by the proposed algorithm. The authors also comment on the space and bandwidth issues associated with these protocols which make the article valuable to researches in this area.

IPsec and SSL: Complimentary VPN Technologies for Universal Remote Access. (2005). *National Webcast Initiative*. Retrieved from http://www.msisac.org/webcast/07_05/info/ip_sec_ssl.pdf

The paper presents IPSec and SSL technologies as complimentary VPN solutions to satisfy the wide range of remote user demands that change from moment to moment. It points the risk of standardizing on one specific protocol and thus, constraining their different locations' access requirements. The paper helps the research with its detailed information about IPSec and SSL protocols.

IPSec vs. SSL VPN: Transition Criteria and Methodology. (2007). *SonicWALL, Inc. Documents*. Retrieved from http://www.sonicwall.com/downloads/WP_SSLVPN_vs_IPSec_102907.pdf

The paper compares IPSec and SSL VPN technologies in terms of management, security, and interoperability. It presents criteria for retaining and replacing IPSec VPN as well as best practices for transition to SSL VPN. The paper is significant to the research with its detailed comparison between SSL and IPSec and in which situations each one fits best.

Kim, Ch., Gerber, A., Lund, C., Pei, D., & Sen, S. (2008). *Scalable VPN Routing via Relaying. ACM Digital Library, Sigmetrics '08*. Retrieved from http://delivery.acm.org.dml.regis.edu/10.1145/1380000/1375465/p61-kim.pdf?key1=1375465&key2=3289611721&coll=ACM&dl=ACM&CFID=85951617&CFTOKEN=61954336

The paper discusses providers' routing issues when clients use Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN). MPLS VPNs increase the number of routes per customer and routers run out of memory quickly creating scalability issues in providers' network. The authors propose a scalable VPN routing architecture (Relaying) that can be implemented by routing protocols modification only. Their research shows that Relaying can save 60% to 80% of routers' memory.

Kohler, E., Morris, R., & Poletto, M. (2002). Modular Components for Network Address Translation. *Parallel & Distributed Operating Systems Group, Papers*. Retrieved from http://pdos.csail.mit.edu/~rtm/papers/rewriter-openarch02.pdf

The paper presents Click, a component-based network system that include general-purpose toolkit for network address translation. The authors present their NAT components as more flexible alternative to the traditional monolithic ones and defend that statement with several examples. The paper provides understandable NAT functionality description and an attractive alternative to the traditional NAT implementation.

Kumar, B. (1993). Integration of Security in Network Routing Protocols. *ACM Digital Library, SIGSAC Review, Volume 11, Issue 2*. Retrieved from http://delivery.acm.org.dml.regis.edu/10.1145/160000/153953/p18-kumar.pdf?key1=153953&key2=9260219621&coll=ACM&dl=ACM&CFID=82501630&CFTOKEN=17928155

The paper introduces threats in routing protocols. It analyzes issues such as subverted routers and intruders and provides information about possible measures to secure the routing protocols. The author concludes that securing distance vector routing protocol is simpler than the link state routing protocol.

Mao, Z., Johnson, D., Spatscheck, O., van deMerwe, J., & Wang, J. (2003). Efficient and Robust Streaming Provisioning in VPNs. *WWW '03: Proceedings of the 12th international conference on World Wide Web.* Retrieved from http://delivery.acm.org.dml.regis.edu/10.1145/780000/775170/p118-mao.pdf?key1=775170&key2=4044691721&coll=ACM&dl=ACM&CFID=85482937&CFTOKEN=99241540

The paper presents the VPN technology and its popularity for live content distribution. Streaming caches or splitters are required to avoid network overload when distributing this type of data over VPN. The authors prove that the general problem is NP-hard and evaluate different solution to it using extensive simulations. The paper provides helpful information for streaming data over VPN tunnels.

Mullins, M. (2005). Implementing Switch Security on Your Network. *Tech Republic White Papers.* Retrieved from http://articles.techrepublic.com.com/5100-10878_11-5754342.html

The paper discusses switch security as an important part of the local area network security planning. It outlines that switches are often overlooked as managers focus mostly on the borders of LAN and forget about port locking and VLAN setting.

Myers, B. (2008) Connect to the Internet using your cell phone and laptop computer. *Bill Myers Online*. Retrieved from http://www.bmyers.com/public/938.cfm?sd=30

The article provides a number of considerations to be made when using a cell phone and laptop to connect to Internet. It includes tips when choosing a cell phone, a service plan, Internet provider, and physical devices. The article provides an example with Verizon service plan.

Ou, G. (2007). Essential Lockdowns for Layer 2 Switch Security. *Tech Republic White Papers.* Retrieved from http://articles.techrepublic.com.com/5100-10878_11-6154589.html

The article provides information regarding layer 2 switch security. It present number of security procedures that are essential in protecting layer 2 of the OSI model. Procedures include SSH or Telnet remote connection, SNMP, VTP, and basic ports lockdowns, as well as VLAN trunking management.

Ou, G. (2006, June 28). IP Subnetting Made Easy. *Tech Republic*. Retrieved from http://articles.techrepublic.com.com/5100-10878_11-6089187.html

The article provides information about IP subnetting as a fundamental subject that is critical for network engineers. The author uses a simple graphical approach to explain the basics of IP subnets such as public IP, private IP, and subnet mask.

Pal, F. (2003). Configuration of Tunnel Mode IPSec VPN Using Cisco Routers. *SANS GSEC Practical Version 1.4b Option 1*. Retrieved form http://www.giac.org/certified_professionals/practicals/gsec/3402.php

The paper presents IPSec VPNs as secure method for organizations to share data over the Internet. It provides step-by-step guide how to configure IPSec on Cisco routers using manual key management and automated key management (IKE). The paper is significant to the research with defining exact command lines for IPSec configuration on Cisco routers.

Pei, D., & van der Merwe, J. (2006). BGP Convergence in Virtual Private Networks. ***IMC '06:*** *Proceedings of the 6th ACM SIGCOMM Conference on Internet Measurement*. Retrieved from http://delivery.acm.org.dml.regis.edu/10.1145/1180000/1177117/p283-pei.pdf?key1=1177117&key2=1106691721&coll=ACM&dl=ACM&CFID=85482937&CFTOKEN=99241540

The paper presents a systematic study of BGP convergence in MPLS Virtual Private Networks. The authors state that invisibility problem in iBGP is the main factor for convergence delays in VPN. They propose several configuration changes that can solve this issue and improve the routing convergence time. The paper uses data from a large Tier-1 ISP to provide accurate analysis and results.

Point-to-Point GRE over IPSec Design and Implementation (n.d.). *Cisco Point-to-Point GRE over IPsec Design Guide*. Retrieved from http://www.ccda.biz/en/US/docs/solutions/Enterprise/WAN_and_MAN/P2P_GRE_IPSec/2_p2pGRE_Phase2.html

The paper provides comprehensive guide for designing and implementing VPN using GRE over IPSec tunnel technology. It describes multiple considerations that need to be taken in account during the design phase. The guide is significant to the research with its information about how QoS, NAT, and firewall affect the VPN implementation.

Ramsey, M. (2000). PoPToP, a Secure and Free VPN Solution. *ACM Digital Library*, ***Linux Journal***, *Volume 2000 Issue 74es*. Retrieved from http://delivery.acm.org.dml.regis.edu/10.1145/350000/349335/a7-ramsay.html?key1=349335&key2=5378611721&coll=ACM&dl=ACM&CFID=85951617&CFTOKEN=61954336

The article presents the Virtual Private Network (VPN) and its two main implementation technologies PPTP and IPsec. It also describes the free PoPToP VPN server for Linux which is widely accepted in business and home network environment. Instructions on how to set PoPToP on Linux machine are included in the paper.

Site-to-Site and Extranet VPN Business Scenarios (n.d.). *Cisco IOS Enterprise VPN Configuration Guide, Chapter 3*. Retrieved from http://www.cisco.com/en/US/docs/security/vpn_modules/misc/Archive_-6342/6342cmbo.html#wp1064626

The document is a comprehensive step-by-step configuration guide for implementing site-to-site virtual private networks. It includes VPN tunnel, NAT, IPSec, QoS, and firewall configuration as well as the exact command lines to do the configuration on Cisco VPN gateways. The document is significant to the research with its detailed information on how to set a VPN tunnel in site-to-site scenario.

Sustar, B. (n.d.). Designing Site-To-Site IPSec VPNs – Part 2. *NIL IP Corner*. Retrieved from http://www.nil.com/ipcorner/IPsecVPN2/

The article covers GRE over IPSec tunnel configuration using crypto maps. It describes how different routing protocols including RIP, OSPF, and EIGRP adjust to the VPN. The paper also analyses the QoS possibilities in the GRE over IPSec tunnel which makes it significant to the research.

The ABCs of Spanning Tree Protocol. (2006). *Contemporary Conntrols, Info Sheet*. Retrieved from http://www.ctrlink.com/pdf/abc7.pdf

The paper presents the Spanning Tree Protocol (STP) and its essentials including possible issues and advantages. It discusses the stability problem in STP when a topology change occurs. Protocol timers and aging timers vary and it is impossible to predict the recovery time window. The paper is valuable with its comprehensive description of STP.

Venkatachalam, G. (2006). Developing P2P Protocols across NAT. *Linux Journal, Volume 2006, Issue 148.* Retrieved from http://delivery.acm.org.dml.regis.edu/10.1145/1150000/1149834/9004.html?key1=1149834&key2=0570591721&coll=ACM&dl=ACM&CFID=85482937&CFTOKEN=99241540

The article introduces the basic issues with network address translation technology. NAT is a problem for public Web hosting and FTP servers as well as P2P applications. The author presents the UPD hole punching technique as a solution for NAT issues and provides some details for its implementation. The article is helpful with its detailed review of UDP hole punching.

Verlag, B. (2000). Economic Benefits of Standardization. *DIN German Institute for Standardization e.V.* Retrieved from www.din.de/sixcms_upload/media/2896/**Economic**%20**benefits**%20of%20**standardization**.pdf

The article presents a research made by B. Verlag about the benefits of standardization for business and the economic as a whole. It finds that company standards have the greatest positive effect on business as they improve the business processes. On the other hands the industry-wide standards have the greatest effect when it comes to relationship with suppliers and customers. The article also provides practical examples of standards defined by international companies.

Welch-Abernathy. (2001, Dec 28). Network Address Translation. *Inform IT Network*. Retrieved from http://www.informit.com/articles/article.aspx?p=24661&seqNum=6

The chapter introduces the Network Address Translation technology. It explains what it is, why it was created, and how it can be implemented in FireWall-1. It discusses the possible problems in using the NAT with applications such as FTP, RealAudio, and Microsoft Networking.