Integrating – VPN and IDS – An approach to Networks Security

Yudhvir Singh, yudhvirsingh@rediffmail.com
Department of Computer Science and Engineering,
Guru Jambheshwar University of Science & Technology
Hisar –125001
Haryana, INDIA

Dr. Yogesh Chaba, yogeshchaba@yahoo.com
Department of Computer Science and Engineering,
Guru Jambheshwar University of Science & Technology
Hisar –125001
Haryana, INDIA

Prabha Rani, prabharani_ys@yahoo.co.in
Computer Science
Kurukshetra University, Kurukshetra
INDIA

Abstract

The Internet and recent global cyber terrorism have fundamentally changed the way organizations approach security. Recent worm and virus incidents such as Code Red, Nimda, and the Slammer worm have heightened security awareness. Also, numerous other threats have emerged recently that are particularly troublesome. Hence some solution must be provided to encounter the new generation of complex threats. Building up this solution requires the Integration of different security devices**.** Also system administrators, under the burden of rapidly increasing network activity, need the ability to rapidly understand what is happening on their networks. Hence Correlation of security events provide Security Engineers a better understanding of what is happening for enhanced security situational awareness. Visualization leverages human cognitive abilities and promotes quick mental connections between events that otherwise may be obscured in the volume of IDS alert messages. Keeping all these points in mind we have chosen to integrate VPN and IDS to provide an efficient solution for security engineers.

Keywords: Integrating security devices, IPSecVPN and Intrusion Detection Systems.

1. INTRODUCTION

To provide the end-to end security solution, we must keep in mind the security products chosen which can be integrated and provide a balance between the access and protection by performing the following functions:

- Access control, including identity services, authentication, authorization, accounting (AAA), access control
- Servers and certificate authorities
- Network and host-based intrusion detection and protection

- Centralized security (and policy) management
- Secure connectivity through encryption and VPNs.

Hence we have chosen the VPN and IDS to provide an in depth solution, because VPN and IDS guarantee the secure operations of the enterprise network access control to traffic, encryption / authentication to protect traffic from interception Modification/Fabrication and IDS must be placed at the edge of the enterprise network to discover attacks.

1.1 Virtual Private Networks

A virtual private network can establish secured virtual links among different organizations, such as branch offices. Tunneling by appending additional headers facilitates the virtual lease line while cryptographic technologies prevent private information passing through the public Internet from being intercepted, modified, or fabricated. However, when complex cryptographic algorithms are employed for encryption and decryption within VPN tunnels, it becomes the performance bottleneck. Hence, dedicated hardware has been proposed to maximize the throughput and minimize the latency. Modern VPN technologies include PPTP, L2TP, and IPSec PPTP and L2TP work at the data link layer and are suitable for secure remote access between mobile users and enterprises. In contrast, IPSec works at the network layer

1.2 IPSec VPN

IPSec provides secure tunnels among the subnets. The important features that IPSec provides are the encryption and authentication mechanisms for the IP protocol suite. IPSec can also be configured to provide data encryption, device authentication and credential, data integrity, address hiding, and security-association (SA) key aging.

1.4 IP Addressing [2]

Proper IP addressing is critical for a successful VPN as any large IP network. In order to maintain capability, performance, and manageability, it is highly recommended that remote sites use a subnet of the major network to allow for summarization. This way, the cryptographic ACLs will contain a single line for every local network, possibly a single entry if the local networks are themselves summarizable on all devices to classify traffic flows. IP addressing also affects many facets of VPNs including remote management connection of overlapping networks.

1.5 Network Address Translation

NAT can occur before and after IPSec. It is important to realize when NAT will occur since in some cases NAT may interfere with IPSec by blocking tunnel establishment or traffic flow through the tunnel.

1.6 NAT Before IPSec

When two sites are connected via IPSec if any of the network address ranges at each site overlap, the tunnel will not establish. This occurs because it is not possible for the VPN termination devices to determine the site to which to forward the packets. Utilizing NAT before IPSec overcomes this restriction by translating one set of the overlapping networks into a unique network address range that will not interfere with the IPSec tunnel establishment. This is the only scenario where the application of NAT is recommended.

1.7 NAT After IPSec

We may consider applying NAT after IPSec encryption for address hiding. However, this provides no benefit because the actual IP addresses of the devices utilizing the tunnel for transport are hidden via the encryption. Only the public IP addresses of the IPSec peers are visible, and address hiding of these addresses provides no real additional security. NAT application after IPSec encapsulation will occur in cases where IP address conservation is taking place.

1.8 Intrusion Detection Systems (IDS)

Many network intrusions cannot be identified until the traffic has been passively analyzed. For example, denial of service (DoS) attacks such as ICMP-flooding are difficult to recognize until

numerous ICMP packets have arrived within a small time interval; application-specific buffer-overflow attacks to obtain root privilege, such as subverting an FTP server by a long “MKDIR” command, may require buffering and reassembling several packets before seeing the whole FTP command. A network-based IDS can detect such attacks by matching a sub-string, for example, the “phf” in “ GET/cgi-bin/phf?,” to identify those network packets as vehicles of a web server attack. When such kinds of potential hostile activities are detected, IDS will alert system administrators and may block the activity. The above examples describe the basic functions of a network based IDS.

In fact, the IDS model can be host-based IDS (HIDS) or network-based IDS (NIDS). HIDS is installed at a host to periodically monitor specific system logs for patterns of intrusions. In contrast, an NIDS sniffs the traffic to analyze suspicious behaviors. A *signature-based* NIDS (SNIDS) examines the traffic for patterns of known intrusions. SNIDS can quickly and reliably diagnose the attacking techniques and security holes without generating an over-whelming number of false alarms because SNIDS relies on known signatures. However, *anomaly-based* NIDS (ANIDS) detects unusual behaviors based on statistical methods. ANIDS could detect symptoms of attacks without specific knowledge of details. However, if the training data of the normal traffic are inadequate, ANIDS may generate a large number of false alarms.

2. RELATED WORK

In this section we are presenting the wok that has been done up to now in the area of Integrity of various security tools and correlating the events from the integrated tools and at last how the visualization tools can help in providing the results that can be interpreted easily**.** YING-DAR LIN, HUAN-YUN WEI AND SHAO-TANG YU, [1] discusses how the integrated security gateway can be implemented using the open source packages. These open source packages ensure the interoperability between the packages. Glenn A. Fink, Paul Muessig, and Chris North [4] introduces Portall, visualization tool that gives system administrators a view of the communicating processes on the monitored machine correlated with the network activity in which the processes participate.

Ron Gula[5] presents the vulnerability correlation with the IDS alerts and specify two methods of correlating the vulnerability with the IDS alerts. These are Persistent VA/IDS Correlation and near time VA/IDS Correlation. netForensics[6] integrates three distinct yet complimentary forms of event correlation – the first is rules based correlation which separates false positive security alarms from potentially significant security incidents by invoking “time aware” security policy rules for each event received from IDS, OS, APPS, or AVS devices monitored by netForensics. The second is Statistical Correlation and third one is Vulnerability correlation. Robert Ball, Glenn A. Fink, Anand Rathi, Sumit Shah, and Chris North [7] explains a tool named VISUAL (Visual Information Security Utility for Administration Live) that provides insight for networks with up to 2,500 home hosts and 10,000 external hosts, shows the relative activity of hosts, displays them in a constant relative position, and reveals the ports and protocols used.

3. PROBLEM DEFINITION

Studying and going through all the references, we have found that the existing problems in today’s network security are most relevant to the – insertion and evasion techniques. Furthermore the limitation is that NIDS can’t deal with switched and encrypted data.

- To deal with the switched data we have implemented the NIDS in the switch itself. As far as the encrypted data is concerned, we configure the IPSecVPN Server within the proxy server or gateway then the encrypted data coming will be first decrypted at the VPN server and forwarded to the NIDS.

- To handle for the insertion and evasion techniques and for reducing the False alarms we must have some technique for correlating the IP traffic to host where the IP traffic is going to reside finally.

4. CONFIGURATIONS AND IMPLEMENTATION

We are having the following requirements for implementation:

- Cisco Catalyst 3750 24-Port Ethernet Switch [8]
- Cisco Intrusion Detection System 4215 Sensor [9]

4.1 Architectural Description

In this paper, we have integrated the VPN and IDS. The physical and logical architecture of the experimental set up is as shown in the Figure 1 and Figure 2 respectively.

The PIX firewall has been configured as VPN to which the remote client installed on the windows machine will connect over the Internet. Since we know that a traditional VPN sever has two network interface cards (NICs), one reachable through the Internet (eth0) and the other on the more trusted network (eth1). These two are connected to the ports 3 and 7 respectively. The victim server is connected to the port 20. There is distribution switch that is working in the DMZ zone between the firewall and the Internet to which the Internet router is connected. The IP addresses used are as shown in the table 1:

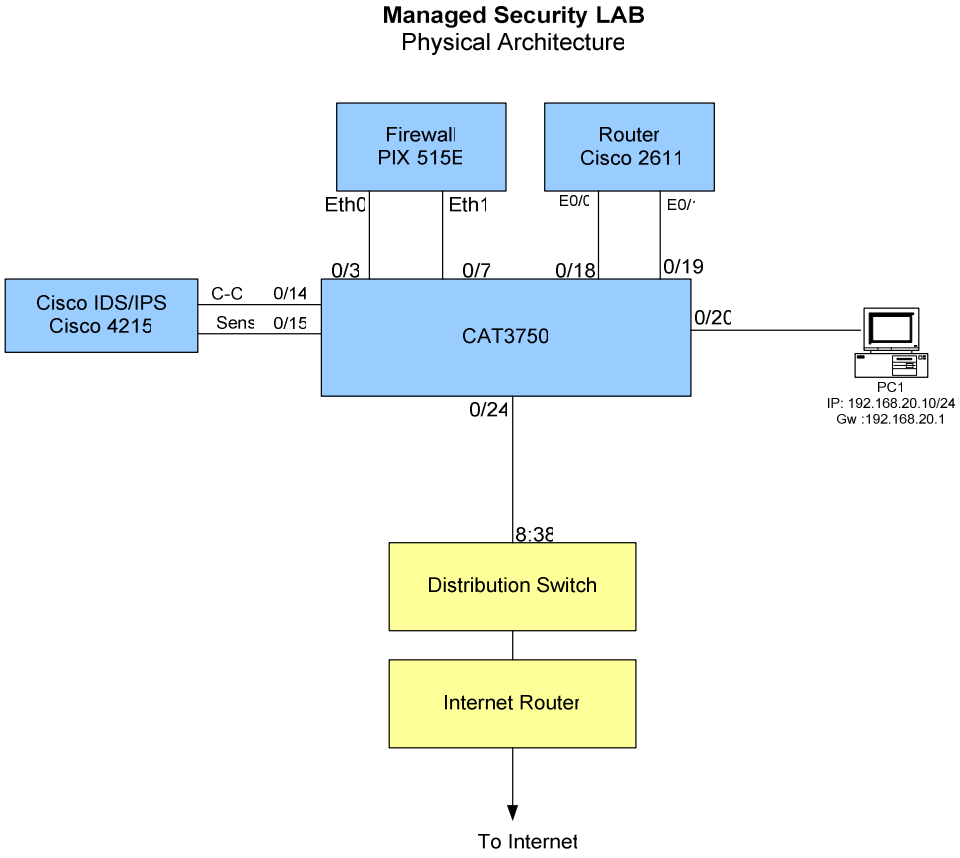


FIGURE 1: Physical Architecture of Managed Security Lab.

Parameter	IP Addresses
Eth0 Server	203.166.97.52/28
Eth1 Server	192.168.20.3/24
Router	203.166.97.50/28
Gateway	192.168.20.1
Clients on LAN	192.168.20.60/24
NAT IP	203.166.97.60

TABLE 1: Logical IP Addresses

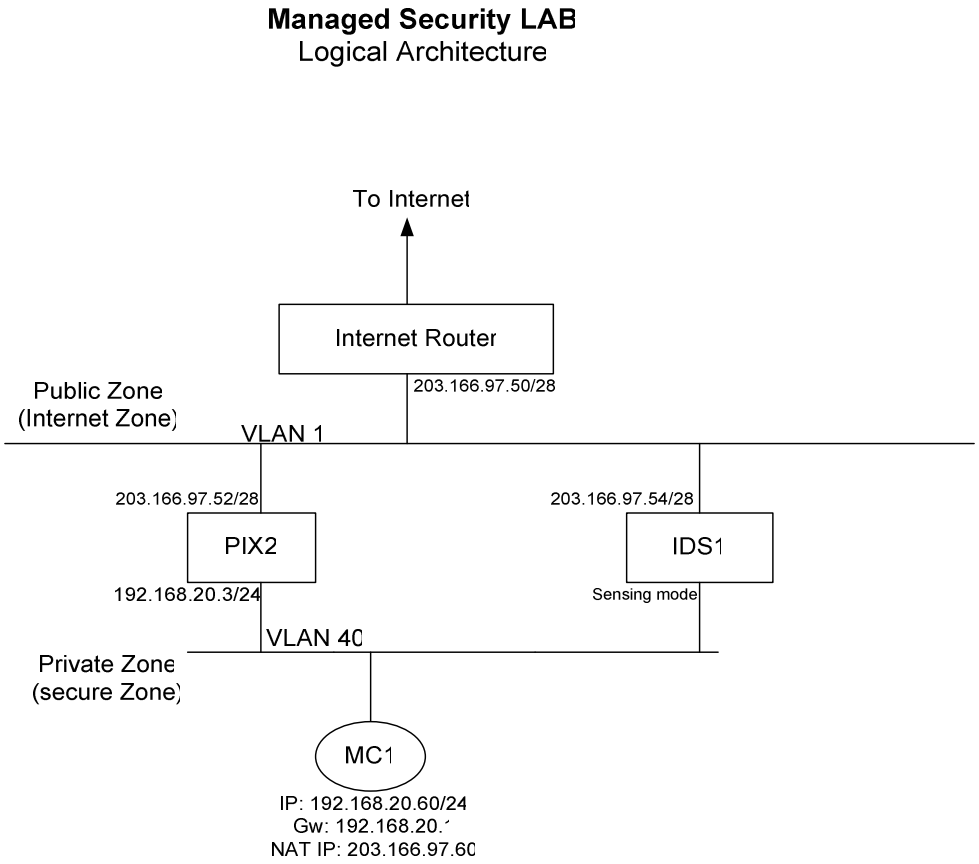


FIGURE 2: Logical Architecture of Security Lab

4.1 Integration network with IDS

The IDS box will sit in the LAN behind the proxy server or gateway in the Private (secure zone) and it will sense all the traffic passing through the proxy server or gateway. The IDS is defined with the relevant rules for the sensed traffic, so it will generate alarm or take action based on the defined rules. In our test setup we have defined the rules for ICMP traffic (Ping), it will detect the ICMP traffic from Internet to an inside server and it take action. In our case IDS box will automatically login into proxy server or gateway and apply the desired rules on the ICMP traffic.

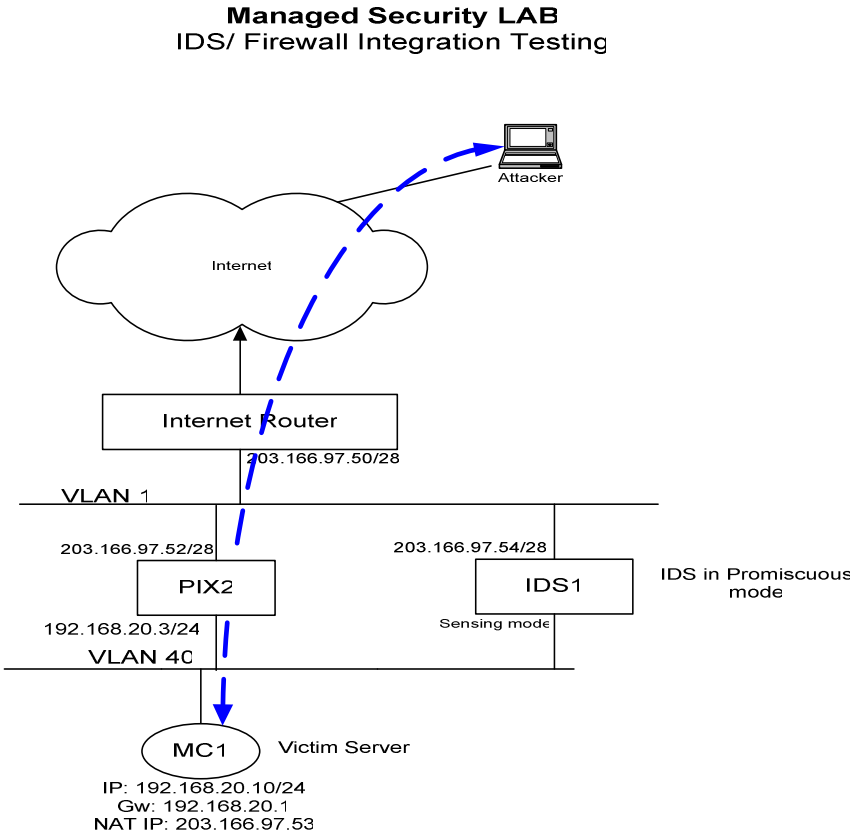


FIGURE 3: Network with IDS Integrated

4.2 Integration of Network and VPN

PIX firewall / proxy server / gateway has been configured as a VPN concentrator (VPN server Box), to which a remote client installed on a Windows machine will connect over Internet. This client will initiate IPSEC tunnel parameters for data encryption while forwarding it to PIX firewall /proxy server / gateway. Once the session is established between client and firewall, the traffic between them will flow encrypted**.**

4.3 Configuration Rules

To implement the above structural diagrams, we defined some configuration rules; based on these configuration rules only few snapshots of the final results have been shown here. The different configuration rules defined are as:

4.3.1 Configuration Rules for Network and IDS Integration

- Defining the interface configuration
- Defining the interface security value for inside highest secure zone
- Defining the rules for ICMP traffic on allowed to pass through
- Defining the interface IP addresses
- Defining the access rule applied for ICMP traffic
- Defining the rules for proxy server/gateway /firewall login/ management configuration
- Defining the rules for IDS box to apply dynamic Access control list on firewall proxy server or gateway

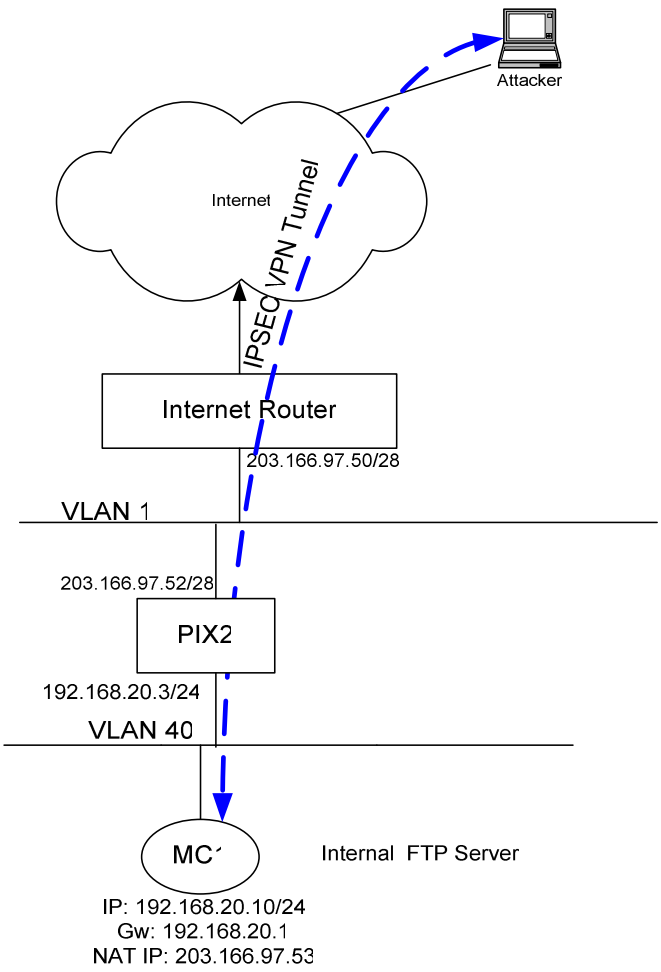


FIGURE 4: Network and VPN Integration

4.3.2 Configuration Rules for Network and VPN Integration

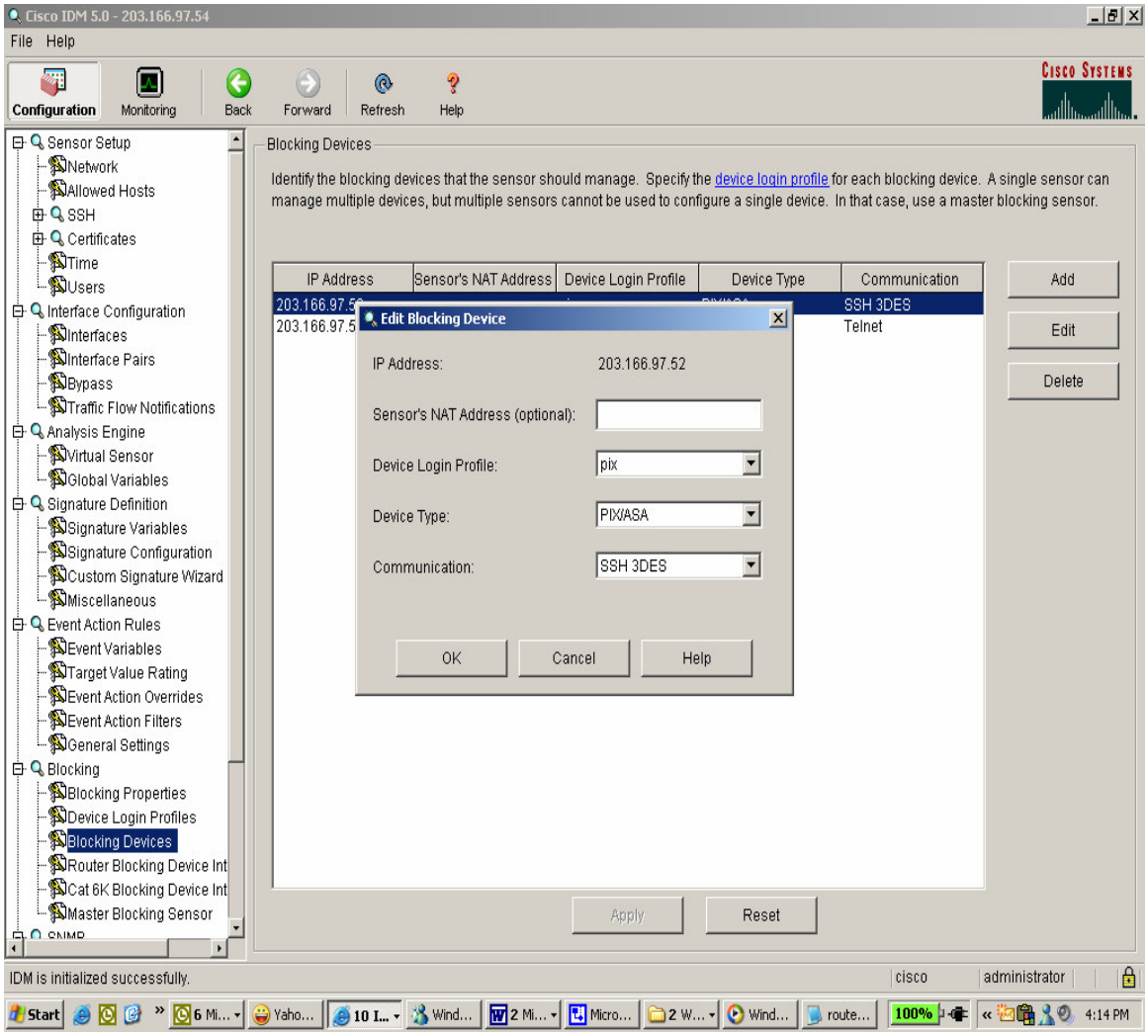
- Defining the rules for physical interface configuration.
- Defining the rules for interface security configuration.
- Defining the access rule for allowing FTP/ICMP services.
- Defining the interface IP address configuration
- Defining the local IP pool for VPN connected customers.
- Defining the rules fro IPSEC VPN configuration and VPN group configuration
- Defining the rules for Firewall Management

4.3.3 PIX logs before the IPSEC session is established

- Defining the IP pool details
- Defining ISAKMP session before tunnel establishment

4.3.4 PIX logs during IPSEC tunnel establishment

- ISAKMP negotiation logs
- IP Pool details after session is established



IGURE 5: Snapshot for blocking device Configuration (PIX 515E)

4.3.5 FTP/ICMP session between client and the FTP server over IPSEC VPN as shown in Figure 8.

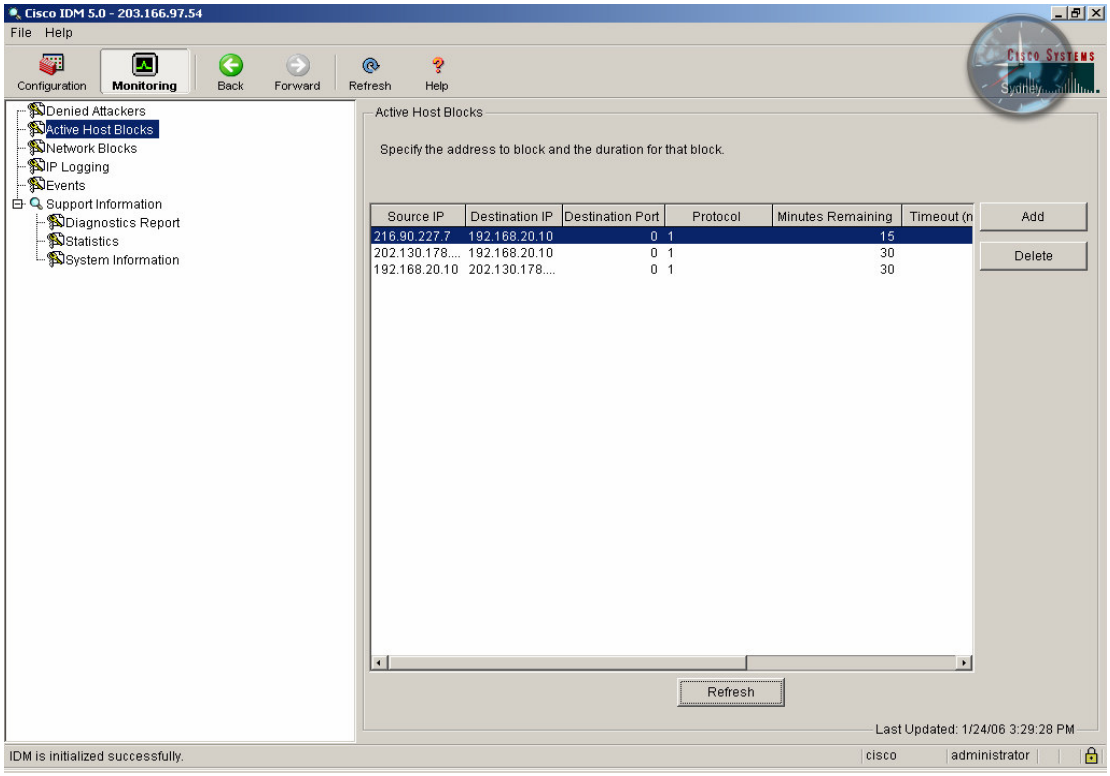


FIGURE 6. Snapshot showing Active Blocking Of Intruders

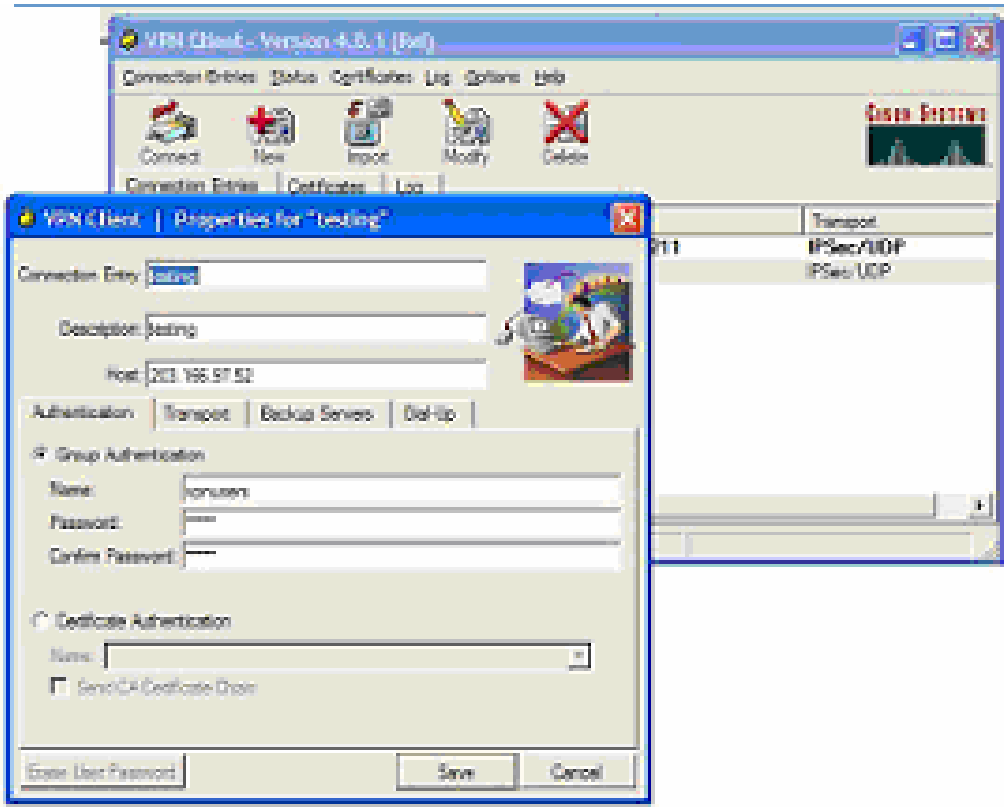


FIGURE 7. VPN Client Configuration

5. RESULTS

5.1 Networks and IDS Integration

In this paper the TCP/UDP and ICMP protocols have been used. After integration of network and IDS the IDS/IPS login to the network as per the configuration rules.

To get the access control list applied by the IDS after logging into the network, we have used the command ***sh log*** as shown below.

fw1-lab1.syd4# sh log

Now the PIX 515E log details appeared highlighting the blocking profile applied by the IDS box. This blocking profile applied by the IDS/IPS in the terms of access rules. The corresponding snapshots showing the details of the active hosts blocked are given in the figure 6.

5.2 Networks and VPN Integration

In this paper, we have used the FTP and ICMP protocols to test the performance of our proposed solution. The different snapshots obtained before the session and after the session are shown as in Figure 8. After the VPN client is configured and connected to the server it is assigned the dynamic IP address. As we specify the configuration rules, the following output will be shown before the IPSec tunnel establishment. To get the IP pool details before the session is established type “show IP local after the # and we will get the following output:

IP pool details

Fw1.lab1.syd4.# show ip local pool

Pool Begin End Mask Free In use vpnpool configured
172.16.20.10 172.16.20.250 Not 241 0

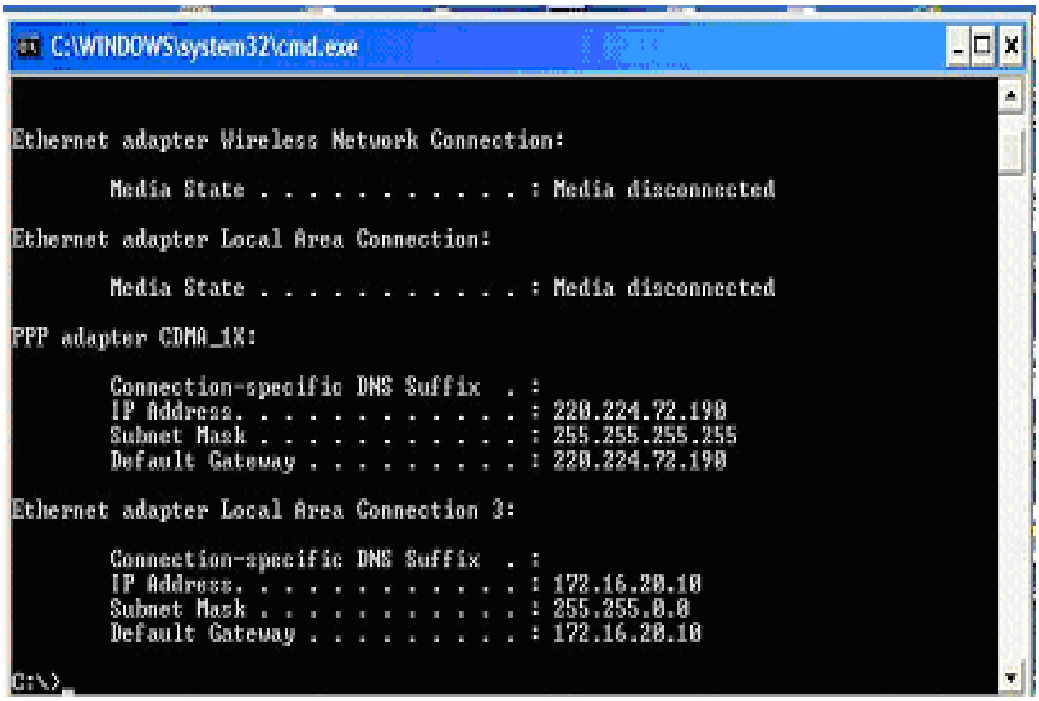


FIGURE 8: PIX Logs before the session is established

And when typed '***sh run'*** after the #, output obtained is as:

```
fw1.lab1.syd4# sh run
Total     : 0
Embryonic : 0
       dst             src       state     pending     created
fw1.lab1.syd4#
```

This above output shows that there are no security associations established in the before the IPSec tunnel establishment. During the IPSec tunnel establishment- The ISAKMP negotiations rules are defined whose corresponding output. Now when the IPSec Tunnel is established between the client and server, the IPSec/ISAKMP associations are created which can be verified by typing the command "***show isakmp sa***" after #
Hence the final output after the creation of tunnel is as:

```
Fw1.lab1.syd4# show isakmp sa
Total     : 1
Embryonic : 0
       dst             src       state     pending     created
  203.166.97.52   220.224.72.190    QM_IDLE        0          1
fw1.lab1.syd4#
```

The above output shows that one session is established between the client and the server.

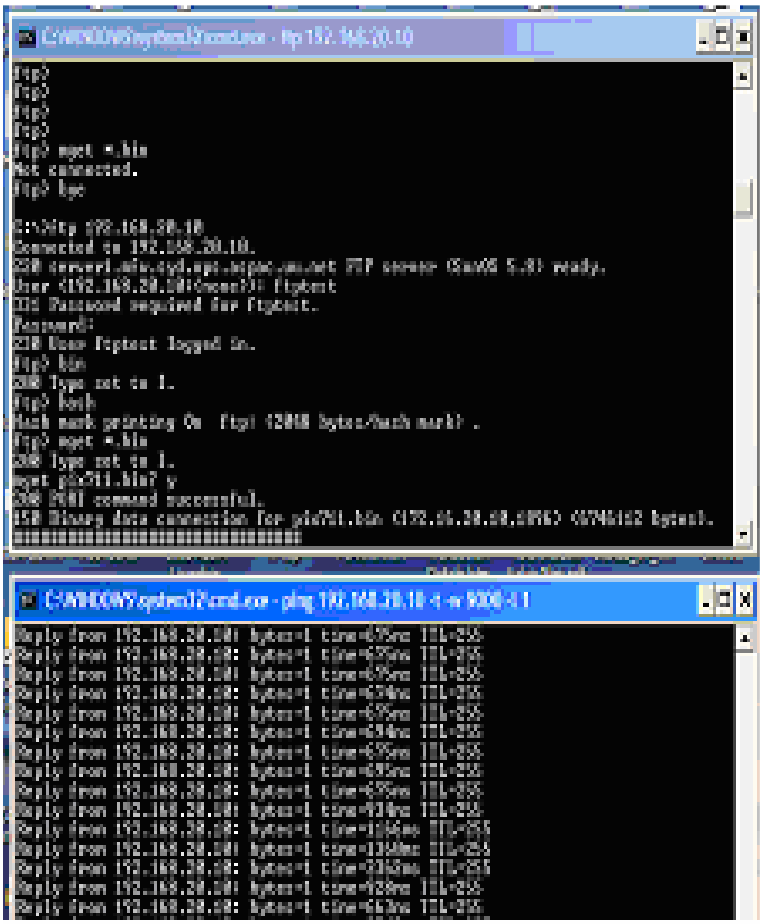


FIGURE 9: Active FTP and ICMP session from the connected client to the FTP Server over IPSEC tunnel

The snapshot in figure 9, demonstrates the creation of Active FTP and ICMP session from the connected client to the ftp server over IPSEC tunnel after the creation of IPSec Tunnel.

The integration of IDS and VPN definitely change the way the security is implemented with in an infrastructure. Also a number of security parameters are affected whenever a change is made. The same is there within this paper is implemented by us.

The different parameters affected by the implementation of this work are**:**

- System Status and Traffic status before and after the creation of a IPSec tunnel
- Time
- Security
- Cost

6. CONCLUSION & FUTURE WORK

Summing up all the things the concluding remarks that account for the implementation are as:

- The integration of various security devices helps in changing the security strategy and making it implement in a better way to defend the attacker.
- The results produced after the integration is satisfactory.
- The correlation of HIDS and NIDS placed at the edge helps in reducing the number of alerts.

Hence the overall point of conclusion is that integration of different devices in the networks security is workable only if deployed in the proper way at proper place.

The areas that can be worked upon to improve the overall security strategy are:

- Inter-IDS correlation
- Data Mining
- Visualization

9. References

[1] Ying-Dar Lin, Huan-Yunwei, and ShaoTangYu, Building an Integrated Security Gateway: Mechanisms performance Evaluations, Implementations and Research Issues, EEE communications Survey, the electronic Magazine of original peer reviewed survey articles. http://www.comsoc.org/pubs/surveys.

[2] Jason Halpern, Safe VPN IPSec Virtual Private Networks in Depth, White Paper, Page 5-8. [April 2001].

[3] Char Sample, Mike Nickle and Ian Poynter, Firewall and IDs shortcomings, first presented at SANS Network Security, Monterey, California. [October 2000].

[4] Glenn A. Fink, Paul Muessig, and Chris North, Visual Correlation of Host Processes and Network Traffic. http://infovis.cs.vt.edu.

[5] Ron Gula, Correlating IDS Alerts with Vulnerability Information, Tenable Network Security http://www.tenablesecurity.com , (December 2002).

[6] netForensics,Comprehensive Correlation: A Three Tiered Approach, http://www.netforensics.com,(2004).

[7] Robert Ball, Glenn A. Fink, Anand Rathi, Sumit Shah, and Chris North, Home-Centric Visualization of Network Traffic for Security Administration, http://infovis.cs.vt.edu/.

[8] Cisco Catalyst 3750 24-Port Ethernet Switch: Product Reviews.

[9] Cisco Intrusion Detection System 4215 Sensor (IDS-4215-K9) Network Monitoring Device: Product Features.

[10] CISCO PIX 515E SecurityAppliance, Datasheet Cisco Systems, (2005).

[11] Thomas H. Ptacek , "*Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection*", whitepaper from windows security, http://www.windowssecurity.com/.

[12] Corbin Del Carlo, "*Intrusion detection evasion: How Attackers get past the burglar alarm*", SANS Great Lakes, Chicago Illinois, May 18-23, 2003.

[13] Joshua Heling, CISSP CTO and Co-founder, Secure Pipe Inc." *Balancing Detection and Prevention in the Deployment of Network Intrusion Technology*", White Paper from Secure Pipe Managed Network Security.

[14] Haluk Aydin, "*NAT Traversal: Peace Agreement between NAT and IPSEC*", SANS Institute, August 12, 2001.

[15] Christopher Smith, "*IPsec's role in Network Security: Past, Present, Future*" SANS Institute, September 2001.

[16] S. Kent and R. Atkinson, "*IP Authentication Header*", IETF Network Working Group RFC 2402, November 1998.

[17] S. Kent and R. Atkinson, "*IP Encapsulating Security Payload*", IETF Network Working Group RFC 2406, November 1998.

[18] Joshua Haines, Dorene Kewley, Ryder ,Laura Tinnel, Stephen Taylor, "*Intrusion Alert Correlation- Validation of Sensor Alert Correlators*", Published by the IEEE Computer Soceity,2003.