A Review Paper on Unified Threats Management

Prof. Ms. Pranita P. Deshmukh[1] Ms. Kshama V.Gade[2] Ms. Arti P. Falke[3] Mr. Shubham Shendre[4] Mr. Vaibhav Bode[5]

[1]Assistant Professor

[1,2,3,4,5]Department of Computer Science & Engineering

[1,2,3,4,5]Prof Ram Meghe Institute of Technology & Research, Badnera, Amravati, India

Abstract— Unified Threat Management (UTM) is an emerging development in the firewall security market. It is then evolution of the traditional firewall that not only guards against intrusion but performs content filtering, spam filtering, intrusion detection and anti-virus duties traditionally handled by multiple systems. UTM firewall is the only firewall that inserts user identity in firewall rule matching criteria, enabling creativities to configure policies and identify users directly by the username rather than through IP addresses. It is a powerful hardware firewall that provides stately and deep packet inspection thereby protecting enterprises from IP spoofing attacks, access control, user authentication, and network and application-level protection. This paper will discover the advent of UTM working criteria, functions and prove how it is better in comparison with the ordinary firewall and VPN.

Key words: Unified Threat Management, Network Address Translation, Intrusion Detection (or Prevention) System

I. INTRODUCTION

Unified threat management (UTM) refers to a inclusive security product which integrates a range of security features into a single appliance. Unified threat management (UTM) or Unified security management (USM), is the evolution of traditional firewall into an all-inclusive Security product able to perform multiple security functions within one system as network firewalling network intrusions detection/prevention (IDS/IPS), gateway antivirus, VPN, content filtering load balancing, data loss prevention and on-appliance reporting.

UTM designed to protect users from blended threats while reducing complexity. The goal of UTM is to simplify the overall security solution despite the growing scope and rising complexity of the security problem. The further most specious feature of this simplification is the physical consolidation of point products into a single technology; hence the term unified threat management. As the hardware powering today‘s enterprise firewalls became more robust it became viable to add functions that were traditionally off the technology right into the firewall.

The IDC Press Issue "The development of UTM usages will be driven by request in the midmarket for new software features, virtual applications, cloud services, and vulnerabilities associated with internet of things,” says Jiaqi Sun, a research analyst at IDC South Africa. "The ultimate objective of security technology development is to protect data or information assets – in other words, minimizing data loss within corporate networks if all layers of an enterprise security system fail." IDC believes that, over the next five years, the revenue generated by the sale of UTM technologies will exceed that of standard firewall/VPNs, effectively replacing these products. DC forecasts that the threat management security technology market will grow at a combined annual growth rate of 17 percent from 2003 to 2008. The technologies are becoming more popular by being a simple means of delivering security software. The Problem with traditional security solutions are that they are focused on protection against external threats only so insider threat protection not given due importance. They are ineffective against blended threats. UTMs for enterprise customers may also include more advanced features such as identity-based access control, load balancing, quality of service (QoS), intrusion prevention, SSL and SSH inspection and application awareness. The major benefit of a UTM product is its ability to reduce intricacy. The principal disadvantage is that a UTM appliance can become a single point of failure (SPOF).

Companies are increasingly finding the idea of unified threat management (UTM) devices attractive, and vendors are responding with a range of products. Although minor companies were the logical adopters of UTM technology, now even huge enterprises see the benefits UTM has to offer. If UTM is in your organization's future, there are several factors to consider before purchasing, including how the product incorporates various security elements, the scale of its deployment and whether it should be hardware or a virtual product. This important guide on UTM appliances outlines critical questions to ask potential UTM vendors and provides insight on the UTM features that will best meet your enterprise requirements.

Network security by definition is limited to finding those attacks that involve the transmission of network traffic. However, there are still many security events today that occur without network traffic being involved. A classic example is a person inserting an infected USB drive into a laptop, thereby infecting that laptop. There's simply no way for network-based controls to recognize this, unless possibly after the fact, when the malware uses network traffic to propagate or to transfer sensitive data from the infected laptop to an external host. And by then the damage may be done. Host-based antivirus software is needed on the laptop to stop this malware from infecting Another common example of the need for host security is the loss or theft of a mobile device, such as a laptop, smartphone or tablet. Simply put, network security controls are useless at protecting a mobile device from an attacker with physical access to it. Someone who acquires a mobile device that is protected only through network-based means will easily be able to recover any sensitive data stored on the device in a matter of minutes by using forensic regaining tools or perhaps even more basic services. It is necessary to use host-based security controls on mobile devices, specifically full-disk encryption technologies, to ensure that their contents are strongly encrypted so that, if they're lost or stolen, unauthorized parties cannot recover their sensitive information.

II. LITERATURE REVIEW

In the late 1990s and early 2000s, firewall technology was critical for monitoring and controlling incoming and outgoing network traffic. By the mid-2000s, cyber security experts were realizing that companies had needs that far stripped the capabilities of most firewall software. Unified threat management was a natural outgrowth of firewall software. Rather than forcing companies to rely on patchwork solutions that may not completely cover the needs of a business, unified threat management is designed to be a comprehensive cyber security solution that protects businesses with just one software program, or a small well-integrated suite of them. The list of threats a unified threat management system protects against varies from product to product, but most unified threat management solutions include:

- A network firewall
- Gateway anti-spam and antivirus capabilities
- Network intrusion protection
- A secure VPN

Because unified threat management tools are typically just one package, they're easy to implement at most companies. And it's usually very simple to effectively use this software, even for people with comparatively little cyber security experience.

III. PROTECTING YOUR BUSINESS

Too many small and mid-size businesses succumb to cyber-attacks, and hacking attempts are common for small businesses, due to the (all-too-accurate) assumption that many of them have poor network security.

Your business may not be able to afford dedicated IT staff, but unified threat management solutions, provided by a managed IT service provider, solve most common cyber security vulnerabilities, leaving hackers out in the cold. Not only are they well within the price range of even most small businesses, but your company can't afford not to have one. If you're a small or mid-sized business owner, you may not know why your business would ever be targeted by hackers. After all, your business probably doesn't handle nearly as much money or personal information as larger companies do. While that's true, most large companies are aware that they're major hacking targets. They have the money to invest in cutting-edge cyber security, and they do so. Hacking a single small or mid-size business won't produce a lot of money or personal information for a hacker. However, it's much easier. Small businesses are low-hanging fruit, compared to larger organizations, and hacking a few small businesses successfully is far more profitable than trying to hack a major company .And while a large business can usually bounce back from even a catastrophic hack, small businesses suffer far more. Experts estimate that 60% of small businesses go under within six months of a successful cyber-attack. The huge financial damage, combined with the lost trust of their customers, is enough to force small businesses to shutter their doors. Unfortunately, even if a small company knows it's a potential target for hackers, it may assume it needs large amounts of money to protect its systems. After all, the argument goes, a good cyber security solution must be expensive and difficult to implement

IV. TECHNICAL SPEC

A unified threat management (UTM) usage uses several detection and prevention capabilities to stop malicious activity. However, the exact combination of these capabilities varies somewhat among different products. The network security capabilities that UTM appliances most often support include the following.

- Anti-spam
- Antivirus for Web and email
- Application control
- Firewall
- Intrusion prevention
- Virtual private network (VPN)
- Web content filtering

Some UTM products provide supplementary network security capabilities besides these core features, such as load balancing, data loss prevention (DLP) and bandwidth management.

V. SECURITY CAPABILITIES

Let's examine each of the core network security capabilities of UTM systems more closely. As already cited, the extent to which a UTM product supports each security capability may differ significantly among products. For example, this may include a product that supports only the most basic Web content filtering, such as checking URLs for malicious content, while another product does much more demanding Web content filtering, such as using reputation services and advanced analytics to determine the likely nature -- benign or malicious -- of each website.

A. Anti-spam:

Just about everyone is already familiar with anti-spam technologies. What you may not realize is how effective anti-spam software can be at stopping incoming email-based attacks. Various spam messages are malevolent in nature; for instance, they might try to trick users into revealing sensitive personal information (e.g., passwords, PINs, not stop. The perfect technique intrusion prevention technologies use various particularly between products, but generally, the most effective products use a combination of methods, such as signature-, anomaly- and reputation-based detection. This allows intrusion prevention software to stop both previously known and unknown attacks, with the latter filling an important gap in UTM exposure capabilities.

B. VPN:

Most of the UTM network security capabilities, which are geared toward attack helpful and wildcat strike, the virtual private network is a technology specifically designed to protect an organization's network activity from eavesdropping or unauthorized manipulation. A VPN Social Security numbers) through social engineering techniques. As the community engineering becomes one of the wonderful common procedures for achieving system compromises and identity theft, it is critical that as many malicious emails as possible be blocked from reaching users, or marked as spam and stored in a separate spam folder for subsequent evaluation by users.

Antivirus for Web and email: Antivirus technologies are amongst the oldest network security

technologies. UTM tackle typically offer malware-scanning capabilities for email and Web application traffic, and in some cases, for other network-application traffic frequently used to spread malware (e.g. instant messaging services). Antivirus software is not as useful as it used to be because malware has become more targeted and customized, while antivirus software is primarily signature-based and better at detecting previously known instances of malware. Still, antivirus software is a essential because of the number of attacks that it can stop.

C. Application control:

As the name implies, application control is the process of administration which applications users can run. It may occupy application white listing functionality and decisive which applications may and may not be used, and it may also include limitations on application use. An example of such a drawback is setting which hours of the day, or days of the week, a particular application may be used. Another example is limiting the bandwidth that an application can use. Robust application control capabilities can detect and enforce application policies apart from of how the application is being used in order to evade detection (i.e., running on different ports, using alternate protocols and so on). Application control is all the time more essential for network security because many applications are either malicious in nature or contain exploitable vulnerabilities that can lead to compromises. Application control also helps an organization boundary the installation and use of applications, thus reducing overall attack surface.

D. Firewall:

The firewall is the most primary aspect of network security control, which restricts the establishment of network connections between hosts. Be fond of antivirus software, firewalls are not nearly as effective as they used to be because the nature of attacks has changed. At one time, a extensive percentage of all attacks involved establishing unauthorized network connections. While the likelihood of this happening has dropped considerably, it is still a concern, particularly for hosts containing sensitive information, such as database servers. Even organizations without much of a security limit still generally need firewalling to protect their most valuable cyber assets.

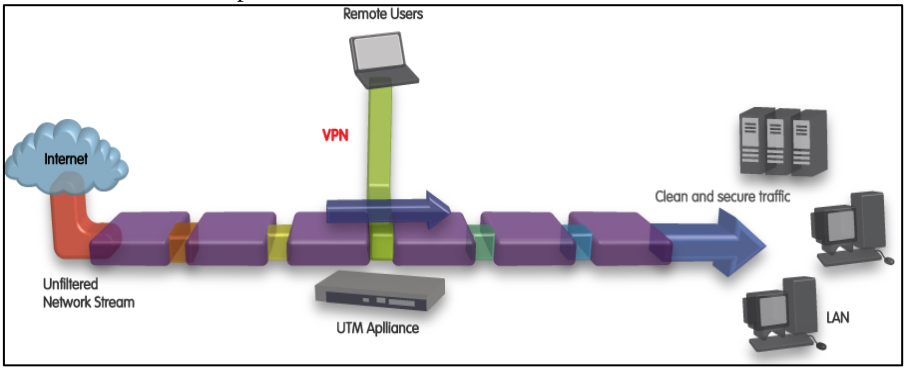
Intrusion prevention: Intrusion prevention technologies (also known as intrusion detection technologies or intrusion detection and prevention technologies) are used to identify and prevent forms of attack that other UTM network security capabilities provides a protected tunnel through which other network activity can pass. VPNs have been increasingly utilized for network protection of an organization's mobile hosts, like laptops, smartphones and tablets. These devices frequently use unsecured or weakly secured external networks, so VPNs provide protection for the use of these networks. VPNs can also be configured to subway all the transfer from mobile hosts to the UTM appliance, which allows all UTM network security checks to be applied to the mobile traffic, thus dropping security incidents involving these devices.

Web content filtering: Web contented filtering was initially a simple technology that prevented access to websites known to be unauthorized for workplace use. Since then, Web content filtering capabilities have greatly extended and diversified to cover a range of techniques for determining if a web request should be permitted or not. An example is using reputation services to rate the likely benevolent or malicious nature of each website. There are also analytical techniques that can scan websites for security violations that designate that a site may have serious security problems, such as a compromise or malicious content. The extent to which your organization needs to use Web contented filter services may depend leading your organization's particular Web security policies, especially when it comes to flagging sites that are simply "unsuitable" and not essentially malicious in nature.

E. Technical architecture:

As you would be anticipate as of a system protection technology, UTM appliances feature a primary technical architecture of one or more network appliances or servers. Typically, these devices are positioned at key points within the network perimeter, such as within proximity of where external communications links attach to the organization's networks. Particularly in larger enterprises, UTM appliances or servers may also be deployed at restrictions between portions of the enterprise, including different division of a company. Basically, UTMs may be most effectively deployed at any network margin, where networks with different levels of trust or security policies intersect.

Because each UTM device (appliance or server) plays such a essential role in network security, it is imperative that all deployments have redundancy built in to mitigate the effect of a UTM failure. Remember that because a UTM is providing firewalling and other core security functions, a UTM failure will effectively prevent any network traffic from crossing the network location where the UTM is located. For many years, expert have suggested that organizations place redundant firewalls at key locations, and having redundant UTM devices at these spots is even more important. Also, don't forget about UTM during disaster recovery planning.



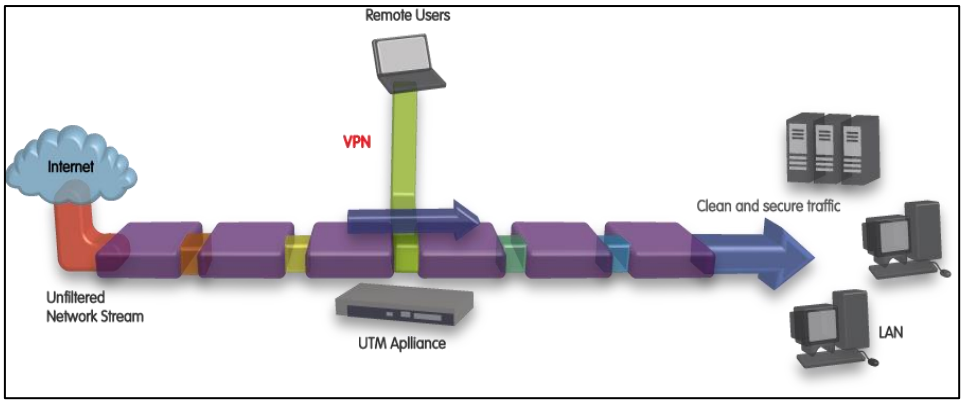


Fig. 1: Architecture of UTM

VI. ARCHITECTURE

This test showed that UTM firewalls come in all speeds, shapes and sizes. One of the appliances we received was simply an off-the-shelf server (IBM's System x3650). Other devices ranged from very lightly customized (Secure Computing put an IPS accelerator board and a customized BIOS in a Dell box to yield its Sidewinder 2150D) to the heavily engineered chassis found in the Juniper ISG-1000 and the FortinetFortiGate 3600A. In general, though, firewall vendors have taken advantage of the enormous boon that Intel has provided in low-cost, high-performance CPUs that are aimed at general-purpose computing.

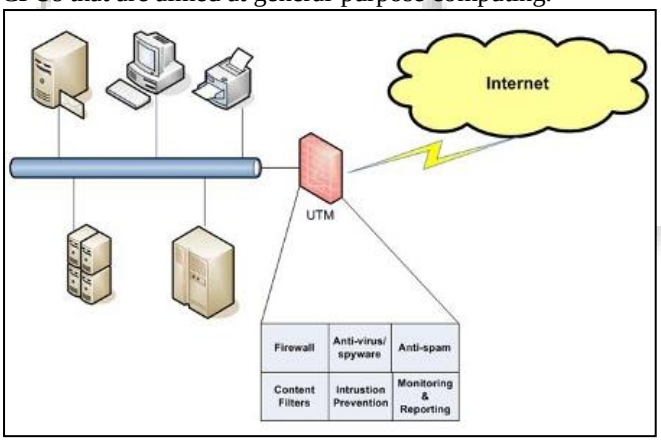


Fig. 2: UTM Network

VII. PROPOSED WORK

A. *Main Objective:*

Most companies in the world are vulnerable to cyber-attacks and selecting the right network security systems is the first step toward protecting your environment. The complexity of managing multiple appliances is time consuming, cost prohibitive and requires a lot of training with the potential for miss-configuration, putting your business at risk.

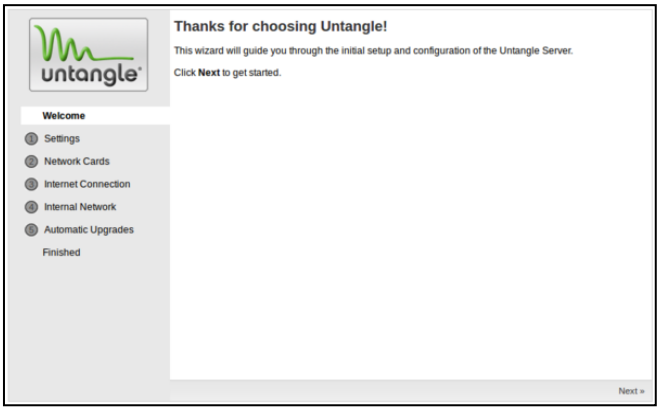
BLOCKBIT UTM (Unified Threat Management) is a leading-edge all-in-one cyber security product that includes the major network security capabilities, such as Next Generation Firewall, Intrusion Prevention System (IPS), IPsec VPN, SSL VPN, Secure Web Gateway, Advanced Threat Protection (ATP), and more.

In a single appliance BLOCKBIT UTM provides all the protection you need while operating on every layer of the Open Systems Interconnection (OSI) model. It hosts the most advanced security features all managed within a user-friendly graphical web interface incorporating numerous dashboards and reports. A 24X7X365 Intelligence lab constantly enhances threat detection through meticulous research and analysis of global threats providing up to date protection.

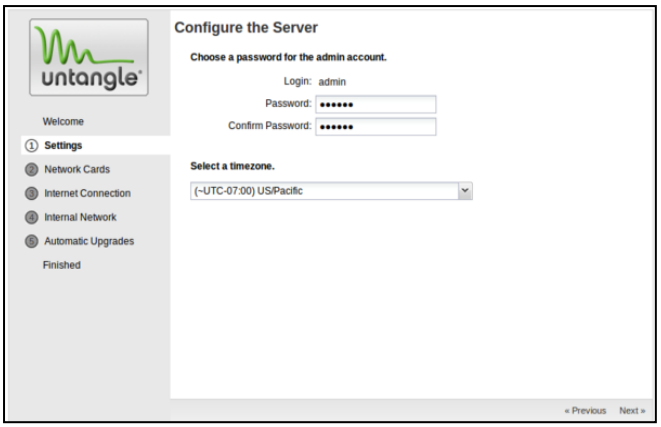
We replace the traditional firewall and integrate seamlessly with other modules inside platform, resulting in a greater ability to blocking attacks. Our Next Generation Firewall has the ability to combine simplicity with safety during the rules creation process allowing users to create policies for applications, users, groups, schedules and other features not available within conventional firewalls. IP Addressing, TCP/UDP ports, MAC addresses and group policies are also managed via the interface. Advanced Threat Protection (ATP) is a feature that incorporates multiple sophisticated security technologies and the latest intelligence feeds providing detection and protection against unknown and targeted attacks. These include advanced malware (trojan, virus, worm, etc) Advanced Persistent Threats and malicious callbacks. Out Advanced Threat Protection also utilizes intelligence to block persistent attacker IP addresses based on geographic location. The ATP also contains a database of applications and traffic that recognize violations of company policy, while blocking new vulnerabilities.

VIII. SCREENSHOTS

A. *Installation of Untangle*



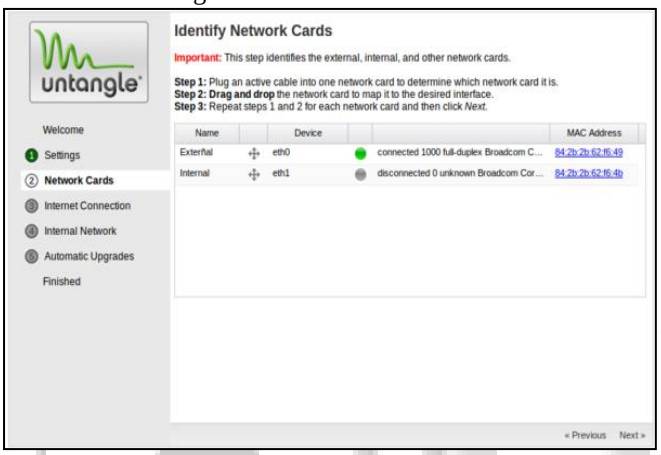
Screenshot 1: Welcome Page



Screenshot 2: Configure the Server

1) Step 1 - Configure the Server

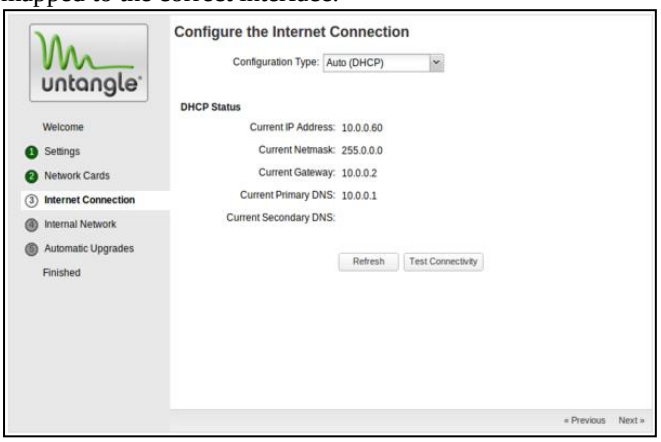
The first step has you set a password used for administrator account for Untangle and select a time zone.



Screenshot 3: Identify Networks Cards

2) Step2:

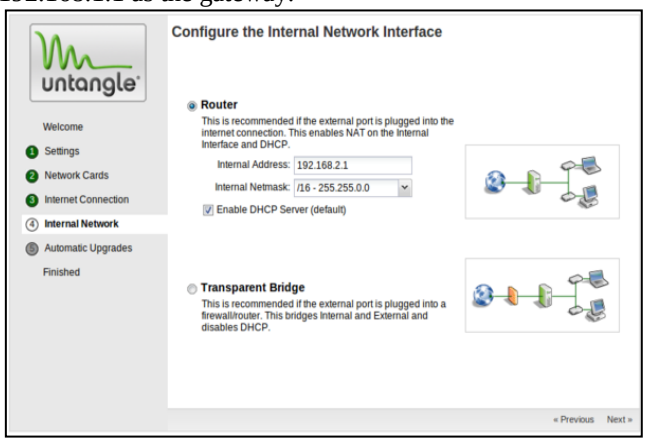
To determine that the physical network cards are mapped to the correct interface plug in one at a time and verify that it is in the correct position. For example, unplug all system cables from Untangle. Plug in the cable into the desired "External" physical network card. If the green light on "External" light up then that physical network card is mapped to the correct interface.



Screenshot 4: Configure Internet Connection

3) Step 3 - Configure the Internet Connection

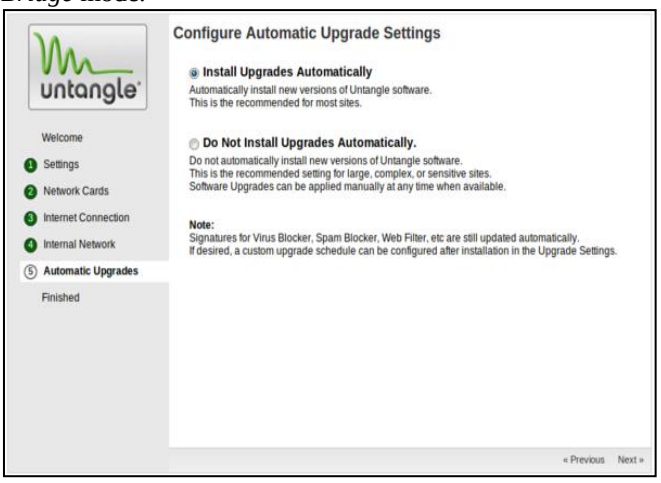
The third step configures your External (WAN) interface. The default is *Auto (DHCP)* and the existing automatically assigned address will be displayed if an address was successfully acquired. *Auto (DHCP)* is typical in home and small networks where ISPs provide no static addresses and DHCP is used to hand out addresses. Also, if Untangle is installed behind another device portion DHCP, this option can be used. However, If Untangle is being installed after a different firewall doing NAT the ISPs public address should not be used. It is common to use the gateway's IP plus one. For example if 192.168.1.1 is the gateway for Untangle you can use 192.168.1.2 for the address for Untangle and 192.168.1.1 as the gateway.



Screenshot 5: Internal Network Interface

4) Step 4 - Internal Network Interface

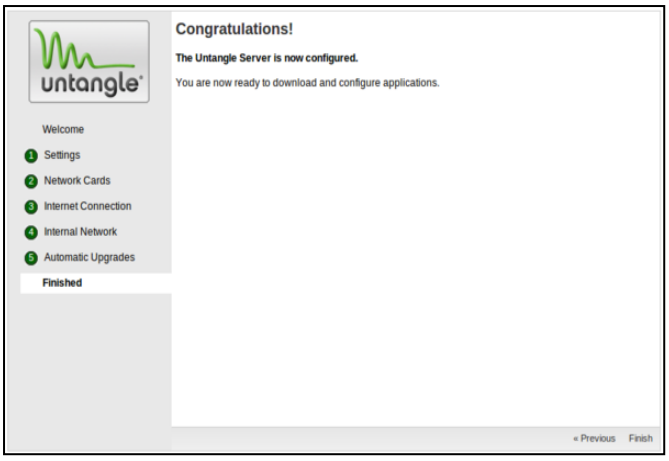
The fourth step resolve configure your "Internal" interface (and DHCP server and NAT configuration.) There are two choices. You can configure the internal interface with private static IP address (ie 192.168.2.1) and facilitate DHCP serving and NAT (Network Address Translation) so all internal machines will have private addresses and share one public IP. This is commonly referred to as *Router* mode. You can also configure the internal interface to be bridged to the external. In this mode the internal interface does not have its own address and is simply share the External's address. This is commonly referred to as *Transparent Bridge* mode.



Screenshot 6: Configure Automatic Upgrade Settings

5) Step 5 - Configure Automatic Upgrade Settings

In the fifth step *Automatic Upgrades* are configured. If regular Upgrades is enable resolve automatically check for new versions and upgrade automatically between 1am and 2am every morning.



Screenshot 7: Finished

6) Step 7– Finished

The next step is installing the desired applications and possibly further tuning the arrangement of your Untangle server, then actually dropping Untangle into the network if it is not already in place.

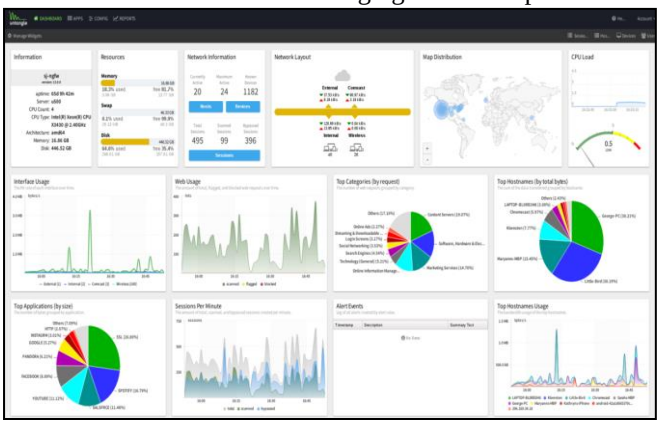
Screenshot 8: Administrator Login

This table supplies the administration accounts that can administer Untangle. administrator include full administrator/root access to the Untangle server.

By default, there is only one *admin* account with the password set during configuration. Other accounts can be created. This can be useful in a few scenarios:

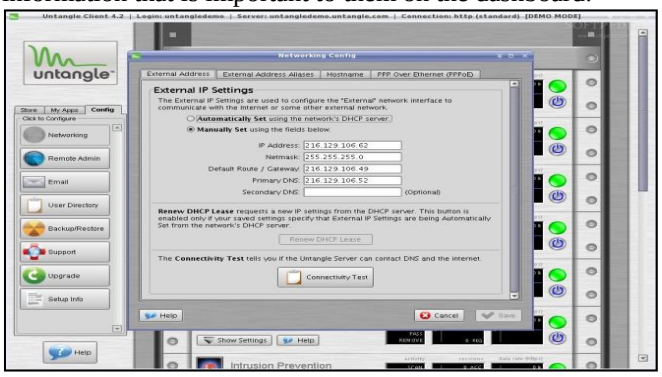
If you have multiple administrators and you wish to be able to distinguish who logged in at what time.

You want to be able to easily disable/enable access for an administrator without changing the *admin* password.



Screenshot 9: Dashboard

By default the dashboard will several *widgets* which show varying information. However, the dashboard is completely customizable. Widgets can be removed and added so the administrator sees exactly the information that is important to them on the dashboard.



Screenshot 10: External Network Interface

Untangle will be the edge device on your *network* and serve as a router and *firewall*. In this case you'll need to set up your *External* and Internal *interfaces* correctly for traffic to flow, which should have been done while *installing*

IX. FUTURE SCOPE OF WORK:

Though the design, development, deployment and testing of proactive network

Surveillance framework for solving network security problem has been successfully demonstrated by use of different result vectors and threat vectors, but there have been some limitations in the research work carried out in this thesis. One of the limitations, in the propose framework, is automatic integration of new intruder signature to the Intruder Database. This portion of the framework requires human intervention arid lacks intelligence to incorporate new

Signatures automatically. Also, at Fifth layer, proposed work used a low interaction Deflect, which could be replaced with medium or high interaction counterpart to achieve better know-how about the unknown threats.

In future this research effort can be put on to a dedicated hardware platform with embedded Linux functionality. As a dedicated out of the box product this effort would fit into

Unified Threat management group of devices. Another point which is left to the future development is integration of the database dumps into graph generation engine. In the research effort, we produced graphs manually, which takes a lot of effort and as observed many of the steps are of repeated nature. Thus, this portion of the work can also be automated. Hence, there is a lot of future scope of the research work to be carried out in this vital area of great significance to mankind.

REFERENCES

[1] Yaxuan Qi, Baohua Yang, Bo Xu and Jun Li, — "*Towards System-level Optimization for High Performance Unified Threat Management*", Proc. of Third International Conference on Networking and Services (ICNS'07), IEEE, 2007.

[2] J. P. Gupta and N. McKewon, — "*Algorithms for Packet Classification*", IEEE Network, March/April, 2001.

[3] Miguel Vargas Martin, Patrick C.K. Hung, ― "*Towards a Security policy for voip applications*", IEEE conference, May 2005.
[4] S Viveros, ― "*The economic impact of malicious code in Wireless mobile networks"*, IEE conference, 2003.
[5] George Lawton, ― "*Web 2.0 Creates Security Challenges*" Technology News, published by IEE Computer Society, October 2007.
[6] Michael B. Greenwald, Sandeep K. Singhal, Jonathan R. Stone, David R. Cheriton, ― "*Designing an Academic Firewall: Policy, Practice, and Experience with SURF",* Published in 1996 Internet Society Symposium on Network and Distributed System Security (SNDSS).
[7] Seny Kamara, Sonia Fahmy, Eugene Schultz, Florian Kerschbaum, and Michael Frantzen, ― "Analysis of Vulnerabilities in Internet Firewalls", Center for Education and Research in Information Assurance and Security (CERIAS), Purdue University.
[8] Michael R. Lyu and Lorrien K. Y. Lau, "Firewall Security Policies, Testing and Performance Evaluation", Department of Computer Science and Engineering.
[9] Biztech. 2008. SMBs Driving the Indian UTM Market. Biztech India.
[10] Jacob, John, 2009. *The Rise of Integrated Security Appliances*. Channel Business.
[11] S. R. Room, "Securing Network Infrastructure and Switched Networks," SANS Institute InfoSec Reading Room, 2001; http://www.sans.org, Date Visited: July 2010.
[12] I. Poynter; and B. Doctor, "BoyondThe Firewall: The next level of network security, " White Papers Series, January 2003; http://www. stillsecure.com/docs/StillSecure-BeyondtheFire wall.pdf, Date Visited: June 2010.
[13] I. Kenneth and F. Stephanie, "Network Firewalls, " a chatper in Enhancing Computer Security with Smart Technology, P. V. R. Vemuri, ed., CRC Press, University of California, 2004
[14] D. X. Song, D. Wagner, and X. Tian, "Timing analysis of keystrokes and timing attacks on SSH, " Proc. SSYM'01 Proceedings of the 10th conference on USENIX Security Symposium, 2001, pp. 1-25.
[15] I. Security, "The Complete Guide to Securing Your Small Business," 2007; www.itsecurity.com, Date Visited: July 2010.
[16] R. Eubanks, "Application Firewalls: Don't Forget About Layer 7, " SANS Institute InfoSec Reading Room, 2005; http://www.sans.org/reading-room/whitepapers/application/a pplication-firewalls-forget-about-layer-7-1632, Date Visited: July 2010.
[17] SonicWALL, "Unified Threat Management," Network Security, 2010; http://www.sonicwall.com/us/products/2270.html, Date Visited: July 2010.
[18] CISCO, "Virtual LAN Security Best Practices," White Papers Series, 2002; http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/ prod lit/vlnwp-wp.pdf, Date Visited: June 2010.
[19] Ji-Yeu Park1, Rosslin John Robles1, Chang-Hwa Hong1, Sang-Soo Yeo2, Tai-hoon Kim1, "IT Security Strategies for SME's", International Journal of Software Engineering and Its Applications Vol. 2, No. 3, July, 2008.
[20] Craig Allan, Justin Annear, Eric Beck, John Van Beveren, "A FRAMEWORK FOR THE ADOPTION OF ICT AND SECURITY TECHNOLOGIES BY SME'S", A paper for the Small Enterprise Association of Australia and New Zealand 16th annual Conference, Ballarat, 28 Sept-1 Oct, 2003.
[21] Jim Herbeck, "Writing Information Security Policy for SMEs", SANS Information Security Webcast 21 Feb 2012 Geneva, Switzerland https://www.sans.org/webcasts/writing-information-security-policy-smes-94939 Date Visited: June 2012.
[22] Michael KimWele, WaweruMwangi, Stephen Kimani, "Information Technology (IT) Security Framework for Kenyan Small and Medium Enterprises (SMEs)", Journal of Theoretical and Applied Information Technology 2005-2010 JATIT & LLS.

