IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 15, Issue 4 (Nov. - Dec. 2013), PP 93-99
www.iosrjournals.org

Protecting the movable Endeavor with Network-Based validation and Virtual Computing

K.A.Varunkumar[1], S.Sibi Chakkaravarthy[2], A.Laxmareddy[3], M.Ganesan3[#,] K.Kavitha[4,] M.Dhilsath fathima[4#].

[1, 2, 3] *M Tech Scholars, Dept. Of Computer Science and Engineering*
[3#] *M Tech Scholars, Dept. Of Dept.Of Information Technology*
[4#] *Assistant professor, Dept.Of Information Technology VelTech Dr.RR & Dr.SR Technical University, Chennai*
Senior Technical Officer – CDAC ACTS

***Abstract**: A new security architecture for the mobile enterprise which uses network-based security and cloud computing has been proposed in these paper. This newly proposed architecture is mainly for both simplifying and enhancing the security of enterprises, and reinstates the currently disappearing security perimeter.*
***Keywords**-cloud computing; cloud-based security; enterprise security architecture; mobile enterprise; network-based security; security.*

I. Introduction

Visualize an endeavor computing and communication surroundings that enhances security and satisfy right to use requirements for today's mobile workforce while sinking the organization's protection load. Cloud Computing incorporated with Network- Based protection has the impending to make this a actuality. The characteristic of endeavor computing surroundings has become an timid mash-up of architecture portion parts. Applications are dispersed between endeavor information centers and powerful PCs. The process of accessing possessions varies depending on such things as: whether the individual is "on site" at a company building or working remotely; whether the way in is from an employee, a partner, a contractor, or even from a machine; more in recent times, whether the appliance is a company-issued computer, a company mobile device, or a user-owned mobile device; and many other uniqueness. Unfortunately, the basic security structure defensive this surroundings has evolved very little from the distinctive DMZ shielding the "good inside" from the "bad outside" even though the distinction between indoors and outside is rapidly vanishing in today's mobile commerce world. To support all of this, the typical endeavor today has a intricate LAN with special "add-ons" for various types of remote access. This design in twist requires that an endeavor have a significant security organization to protect the LAN and applications. If an endeavor can move all of its data center applications into the cloud, the design can be mainly cut down so that all types of access use the same design, able it with different policies. All infrastructures go between the endpoints and the cloud – no traffic remains local on the LAN. By applying sharp protection in the network and in the Cloud, an endeavor can shift the endeavor security burden while maintaining or even enhancing safety.

II. Recent Computing Environment

The recent endeavor computing background (shown schematically in Figure 1) distributes applications between authoritative and sharp endpoints – PCs and laptops – and servers in endeavor-hosted information centers. The authoritative endpoints usually run the Ms Office suite of applications (MsWord, MsPowerPoint,Ms Excel,MsOutlook, and sometimes Visio). information center applications are typically proprietary web-based applications such as employee directory, Data portals, control, and time-entry applications, along with endeavor critical business-maintain and operations-support systems (BSS/OSS). Remote employees, counting those that work at home or are roaming, and endeavor associates access the enterprise applications through Virtual Private Networks (VPN). All of this access is enabled through the mixture of Local Area Networks (LAN) and Wide Area Networks (WAN). Access to Internet applications is through an endeavor proxy. Voice associations today are usually inheritance switched services or newer Voice over IP (VoIP) alternatives.

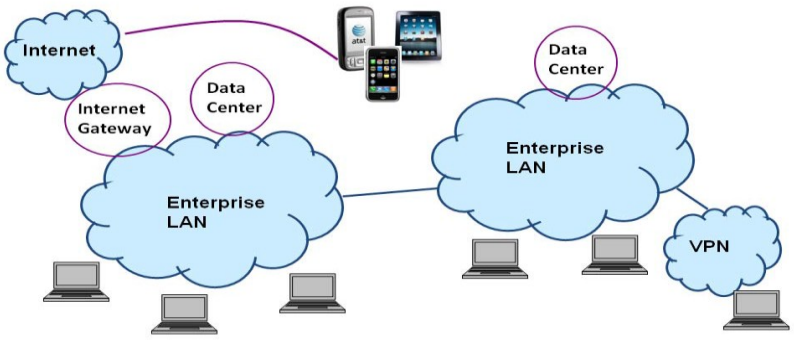

Fig1: Typical enterprise computing environment

III. Security In The Current Environment

Security in the current environment (with the problems highlighted in Figure 2) mirrors the distributed nature of computing. Endpoint security includes frequent patches for security vulnerabilities and endpoint-based security such as anti-virus, anti-spyware, host intrusion prevention, and host based firewall.

A. Security in the Current Environment

Security for enterprise proprietary applications is similar. Servers and applications are initially hardened to reduce the number of vulnerabilities that can be exploited. Servers are (or should be) scanned regularly and patched to maintain security at a high-level. Firewalls and Access Control Lists (ACL) provide some level of access control. Authentication and authorization are used to provide more fine-grained access and privilege control. Access to the Internet is provided through Internet Gateways in a Demilitarized Zone (DMZ) that proxy and filter traffic to provide security. Spam and antivirus for email are also typically provided as part of a DMZ. This DMZ largely defines the security perimeter of the enterprise. However, because of the large increase in the number of mobile devices (smart phones, tablets, sensors, smart meters, etc) and varied needs for interconnection (with partners, suppliers, etc.), the enterprise perimeter is rapidly disappearing. Overall, this security architecture has evolved little from the early days of firewalls and DMZs [1], and it is not flexible enough for today's security needs, in particular for securing access from mobile devices, dealing with exceptions, etc. The disadvantages of this architecture (shown in Figure 2) include a complex DMZ, an incompletely defined, disappearing perimeter, expensive equipment, operations, and support, as well as high complexity (and associated costs) on the LAN and WAN.

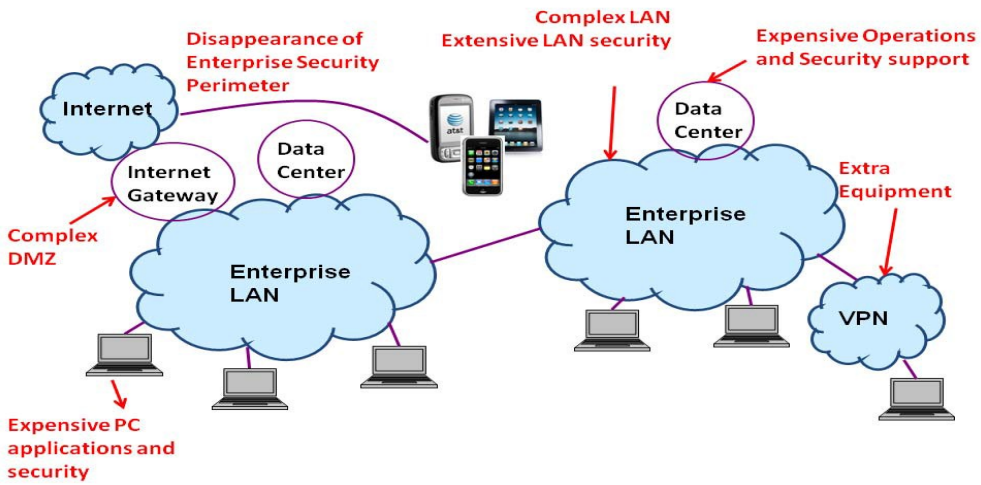

Fig 2: Security for current environment

A closer look at the LAN shows that communications within this environment can be abstracted as shown in Figure 3.

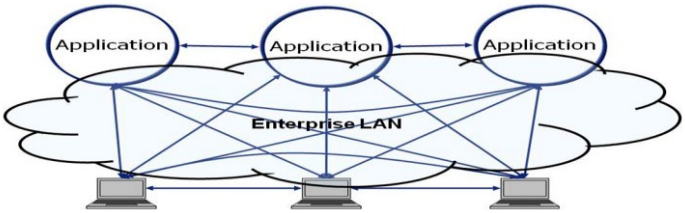

Fig 3: Many to Many communications in enterprise

This model allows virtually any node – and each endpoint is a node – to communicate with every other node. The network must be architected this way because it is difficult to know which nodes should be communicating. Any attempt to provide fine-grained access control is likely to result in a self inflicted denial of service (DoS). Therefore, typical access controls consist of fairly coarse firewall rules or ACLs. And these rules often become quite complex since any attempt to delete old rules may break needed access, and also lead to DoS. This behaviour can be seen frequently when companies merge. It is common for the merged companies to have difficulty exchanging information and accessing shared systems for some time after the merger has occurred. All of this security and networking is supported by often overworked groups that struggle to define policy, deploy and maintain security and networks, monitor for an ever-increasing number of sophisticated attacks, and attempt to provide incident response and forensic support when the inevitable exploit occurs.

IV. Network-Based Security, Cloud Computing, And A Transformed Enterprise

Imagine now an architecture whose very design intrinsically provides a high-level of simplicity and, Correspondingly, security. This architecture is shown abstractly in Figure 4.

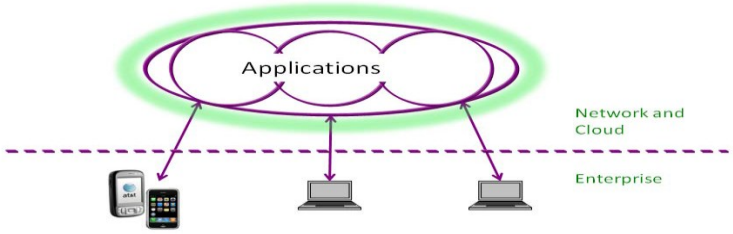

Fig 4: Many to One Communication in Enterprise

In this architecture, endpoints only communicate with logically-centralized applications greatly simplifying the LAN architecture.

A. The Cloud-Based Enterprise

The proposed instantiation is shown in Figure 5. The salient features of this architecture are as follows: All enterprise data centre applications are hosted in the Cloud 2. This includes voice applications if an enterprise is moving to Voice over IP (VoIP). The requirement for all applications to be in the cloud is critical: if any applications remain in the legacy architecture, the complex LAN must still be maintained. Further benefits can be attained by moving to the Cloud applications such as the Microsoft Office suite that were hosted on the intelligent endpoints (PCs, laptops, and increasingly on mobile devices – smart phones, tablets, etc). Internet

applications are still accessible in this architecture. Applications are accessed from either fixed or mobile endpoints using the most cost-effective means available at the
time – wired, Wi-Fi, or cellular. Endpoints are either fixed or mobile depending on how they are connected at the time. There is no functional difference. Small-form-factor endpoints (e.g. smart phones) can be "docked" to full-size accessories such as a keyboard, mouse, and monitor for long duration computing. IP network transport is provided to applications in the Cloud or on the Internet.

Fig 5: Transformed Enterprise Architecture

B. Simplified Security for the Transformed Enterprise

With the architecture described above, security is simplified for the enterprise. This is accomplished by moving security into the Cloud and into the network. Networking and operations can similarly be simplified for the enterprise. The overall security is shown schematically in Figure 6 and described below.

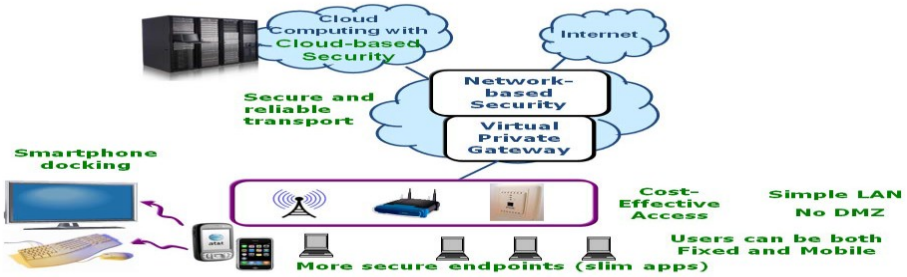

Fig 6: Security For Transformed Enterprise

Starting from the bottom of Figure 6, the first improvement in security is in the endpoints. Because the typical PC-based applications now reside in the Cloud, the applications on the endpoints can be reduced substantially – in most cases a web browser is all that is needed. In some cases, a virtual desktop may suffice for even higher levels of security. Slimmed-down applications and storage lead to enhanced security. With cloud storage as part of the architecture, one can foresee endpoints with very limited data storage, and storage that does not persist indefinitely. This provides enhanced protection should an endpoint be lost or stolen.

One of the key security enhancements in this architecture comes from the fact that there is no LAN in the typical sense. In this architecture, the LAN functions strictly as an ISP to transport traffic between the endpoints and the centralized applications (refer to the abstract depicted in Figure 4). Because all traffic goes between the endpoints and the Cloud via the access network – there is no local traffic – the access
network "sees" all traffic and can function as a choke "point" for enterprise traffic. Therefore all LAN security can be moved into the network and Cloud. Network-based security includes functionality such as email and web anti-virus, URL filtering and blocking, firewall, DDoS protection, IDS/IPS, etc.3 The network-based security is implemented in the access network, by a specialized network security provider, and supported by security professionals who in many cases have a higher concentration of skills than the enterprise security team. At the same time, all the security policies are completely under the control of the enterprise. Enterprise security policy and audit teams remain as key requirements under the transformed enterprise architecture.

C. Enhanced Network-Based Security for the Transformed Enterprise

Using enhanced network-based security functionality can provide even more security for the enterprise. The proposed enhanced architecture protects traffic between endpoints and the cloud (or the Internet), while providing mechanisms for applying enterprise security policies in a uniform manner.

One of the key components in the proposed enhanced architecture is the Virtual Private Gateway (VPG – shown schematically in Figure 7) for end devices. With the VPG, end devices always have a VPN between any of their endpoints (mobile phones, laptops, or PCs) and the VPG4 . Furthermore, there is a VPN (either IPSec or MPLS) between the VPG and the Cloud. Therefore, all communications between the endpoints and the Cloud are uniformly protected, and fine grained policies can be easily applied to both inbound and outbound traffic. Policies are provisioned into and evaluated by the Policy Engine in the VPG. Once a policy is matched to a given packet, it is either dropped or assigned to a routing engine. The Routing Engine is responsible for getting the packet to the proper destination network. The NAT function is designed such that the all related packets will return back to this VPG instance. The VPG also routes Internet-bound traffic from endpoints directly to the Internet, if allowed by enterprise policies, without this traffic having to go all the way to the enterprise before being sent back to the Internet. The VPG will drop traffic that is not allowed per enterprise policies as early as the traffic reaches the VPG instead of this traffic having to go all the way to the enterprise before being discarded. This can serve for a variety of purposes, including DoS/DDoS protection.

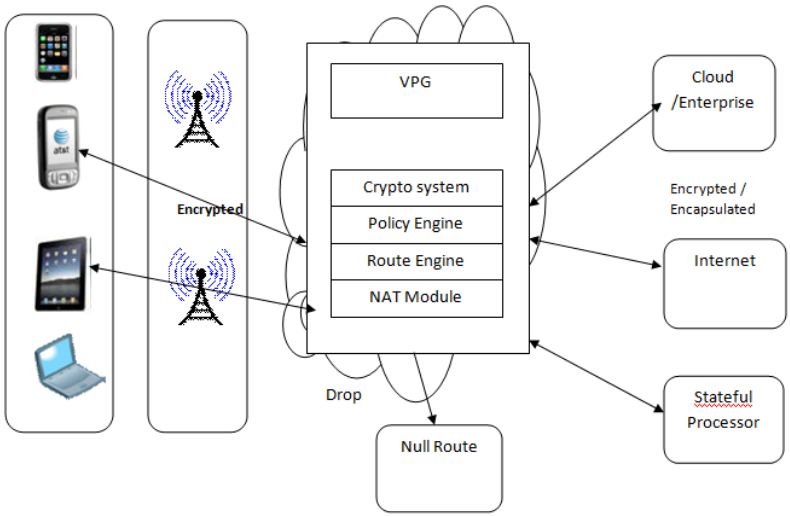

Fig 7. Enhanced Network-Based Security.

There are other security advantages to using the VPG for mediating access to Cloud Computing. All enterprise employees – remote and within the enterprise buildings, using any of their devices, including mobile – and partners now access applications using the same security. The enterprise security policies enforced at the VPG can be as fine grained as necessary to handle various types of end-users, devices,
Connectivity or other context for the traffic. Also, since traffic is routed at the IP layer to the VPG, all traffic from the devices are sent to the VPG regardless of the access network (e.g., cellular, WiFi, roaming). Therefore, the previously vanishing security perimeter is now restored. User access is shown schematically in Figure 8.

Fig 8:Any Where, Any Time, Any Device access

Naturally, since all communications now go to the Cloud through the access network, reliability, QoS, and availability are critical. With respect to security, the network itself must be able to protect itself against extreme levels of traffic as might be experienced during DDoS attacks. The network must also be monitored 24x7 for signs of security events that could potentially disrupt traffic.

D. Cloud-Based Security for the Transformed Enterprise

The other key security enhancement is security that can be provided in the Cloud. Ideally, the Cloud should use a layered security model to provide multi-level protection of all information, data and physical assets including data center environments. In this model, security does not depend on a single countermeasure. Rather, layers of security provide a reinforced system of countermeasures so a single point of failure does not compromise the entire system. Such a layered security protects the cloud from both physical and logical security threats and includes:

• Physical Security
• Network Security
• Intrusion Detection
• Firewall Management
• Environment Hardening
• Virtual Guest Security
• Anti-virus and Patch Management
• Access Controls
• Data Security – Encryption of Data

Security is continually monitored and adjusted to maintain protection at the highest level. Beyond this, there is more security that an enterprise can use to their advantage. Security that was previously performed by an enterprise in their data centers can now be provided in the Cloud. This includes tasks such as application scanning, token or biometric access control, threat management, and forensic analysis. Similar to network-based security, cloud-based security done by a specialized cloud security provider is supported by professionals, who more often have higher security skills than the enterprise security team. As discussed in [2], this can balance many of the initial security concerns related to migrating the enterprise applications and data to the cloud.

E. Enterprise Security Comparison

The overall transformation of enterprise security is shown in Table 1.

Current Computing	**Transformed Computing**
Complex LAN routing to connect assets	Simple LAN – route traffic to Cloud
Extensive LAN and DMZ security to protect assets	• DMZ provided in the network. • No costly and complex LAN Security Information Management (SIM) • Expert security and operations
Extensive Data Center security to protec applications and assets	• Security, Reliability, and Disaster Recovery are provided completely in the Network and Cloud • Security services can provide enhanced security
• Enterprise VPN protects only wired endpoints • Enterprise employees, remote employees, and partners use different access methods	• Same solution and protection for all employees and partners regardless of endpoints • Anytime, anywhere, any-device access

V. Conclusions

Network-based security and Cloud Computing promise to bring a large positive step change in the way that enterprises perform security functions. By moving applications completely into the Cloud, enterprises can take advantage of network- and cloud-based security that is provided by trained security specialists. By moving to a streamlined security architecture, enterprises can simultaneously simplify and enhance their security while potentially achieving cost savings as well.

The proposed new security architecture offers added flexibility for today's needs. The security perimeter that has been vanishing with the many mobile devices, the need to connect to partners, etc is being logically restored, and the new choke "point" in the architecture has significant security capabilities. This architecture can also help in detecting and handling Advanced Persistent Threats (APT) and attacks, which constitute the subject of further research work.

References

[1] William R. Cheswick and Steven M. Bellovin. Firewalls and Internet Security: Repelling the Wily Hacker. Addison-Wesley, Reading, MA, 1st edition, 1994.
[2] Steven M. Bellovin, Clouds from Both Sides, IEEE Security & Privacy, vol. 9, no. 3, May--June, 2011.