Detailed Analysis of Antivirus based Firewall and Concept of Private Cloud Antivirus based Firewall

Parminder Singh Arneja
Server/SAN Administrator
NIC Parliament Informatics Division
New Delhi, India

Sidharth Sachdev
Mainframe System Programmer
IBM India Pvt. Ltd.
Bangalore, India

ABSTRACT

Network security is a concept which combines various business models and technologies together to deliver provisions and policies for comprehensive intrusion detection and unauthorized access. The only secured computer is the one with no power and no user. Any other computer can be compromised. Network Security is the most important issue for any organization. This paper includes the different security issues that occur in a private network which can be managed and minimized using software based firewalls like Antivirus based firewall. This paper also includes how we can improve the network security by implementing the same Antivirus based firewall on a Private Cloud using Software as a Service (SaaS) approach for better scalability and improved reliability. Antivirus software on a system does not provide full security as they fail to detect many modern threats and modern virus codes and the increasing complexity are being exploited by malware. This paper brings a new model of end hosts threat detection technique based on threat analysis by antivirus software services as a cloud network service[12]. This paper describes how the whole network infrastructure can be controlled flexibly at administrator and client level.

Keywords

Firewalls, private cloud, Antivirus (AVR), infrastructure, Software as a Service (SaaS), in- cloud network service.

1. INTRODUCTION

Network security is best described as policies and procedures implemented according to an organization as per required authorizations to access the network and to avoid the unauthorized exploitation and intrusions. The network administrator controls the security which involves the authorization of access to the network data.

Data security is a challenging issue for data transmissions over a communication channel, hence strong data encryption techniques should be implemented to maintain the security of the data.

Network security can be accomplished through hardware as well as through software, but there must not be a single layered security[5]. The security must always include multiple layers as if one fails, other stands and the secured data could not be compromised.

Security components often include:-

- Intrusion prevention systems (IPS), to identify fast-spreading threats.
- Virtual Private Networks (VPNs), to provide secure remote access.
- Firewalls to block unauthorized access to your network.
- Anti-virus and anti-spyware[5].

Here are some security issues every organization faces during implementation of a network:

i) Access Control - Imagine ticket less air travel, where a person can board the flight based on a positive identification or authorization verified biometrically at the time of boarding at the gateway [3]. Similarly, the access to the server's hardware and even software should be made with proper authorized access. Following things must not be overlooked – a) is the access to intranet sites restricted to internal network? b) Is the access to specific content accessible only to the specific employees based on their job function?

ii) Remote access - Remote access to client devices may be used in hostile environments but may not be configured for them. The communication may be carried over non trusted networks. Does the organization allow wireless access from any location to the internal network or the access provided is behind the firewall or not? Do the end users have the rights for remote login? Such scenarios must be considered to carefully handle remote access and precautions must be taken for wireless access, including the use of WEP security, but valuable services are denied at the same time by restricting them to the same network access in front of the firewall.

iii) Virus and Rogue code - Client workstations have disk drives and if the users can bring their personal diskette drives in the organization premises which could be infected with malicious viruses and rouge codes can ultimately compromise the entire network for intrusions. The issue- Are the users permitted to bring their personal drives? Must not be overlooked. Antivirus software does not only includes the virus protection, but also implements security procedures which includes settings for the mail client and the types of executable permissions implemented for various users, for eg- rouge code, i.e. Java or any other executable embedded in a webpage opened by an application can compromise the network. Hence, appropriate policies must be employed at the client level[6].

iv) Standard Software – Is the user permitted to bring and install third party software? If yes, then a close look at policies and their enforcement should be implied. In many organizations, any third party software from any source other than the administrator is not permitted on any network connected device. Government organizations specify a standard antivirus software and browser and configure security settings for those using permissions, policies and deny the installation for any unauthorized programs on the network. Many rouge codes, Trojans and sniffers can be traced to such unauthorized software.

All these issues can be handled with certain policies maintained at firewalls. There are basically two types of firewalls:

- Hardware Based Firewalls.
- Software Based Firewalls.

1.1 Hardware-based Firewalls

Hardware firewalls are typically found in broadband routers or can also be purchased as a separate hardware, and are an integral part of a network setup especially for those on broadband. These firewalls are external to the computer and no additional software or application is required for normal running operation. The hardware based firewall protects many hosts at once, as it intercepts all the traffic from the Internet before it enters the internal private network of an organization. Hence a hardware firewall should be the first thing on your private network which connects with the public network [4] as shown in figure 1.

Hardware firewalls use a packet filtering technique which examines the packet header to determine the packet's source and destination [16]. Then this information is compared to predefined policies of the organization which then concludes whether the packet is to be forwarded or dropped. Hardware-based firewalls also have some limitations. Like if you use a laptop at your office which is in the network, and it travels to other locations, then hardware based firewall at your organization can't help, that means the security policies at your organization does not implement while you're roaming. Hence, hardware based firewall can't protect your system if the internet is accessed at some other location.

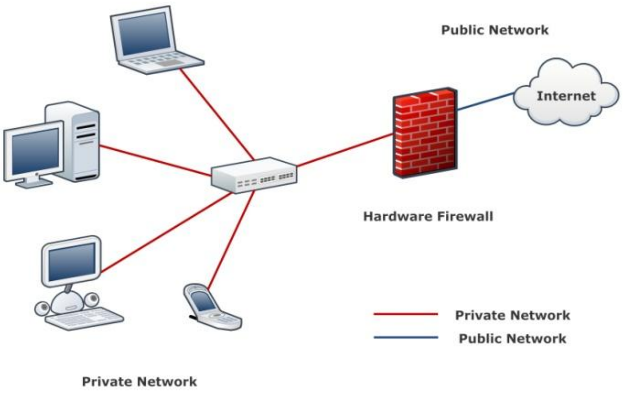


Figure 1: shows the architecture of basic hardware firewall [1]

1.2 Software based Firewalls

In contrast to hardware based firewalls, software based firewalls are more reliable and ideal for individuals even using a broadband connection wirelessly as these firewalls are part of the user's computer and are installed as a software rather than having an expensive hardware. Since a software based firewall is physically part of a computer, this protection follows everywhere which is more effective if a laptop is used at home or at the office.

Software based firewalls identifies the applications that are creating security risks on the computer. If a threat infects your system and attempts to open up the secured network, a software based firewall will identify this new application and will prompt you to confirm the new application or to prevent its use and puts up a warning that a malicious program is attempting to enter the network.

Although these firewalls prompts for malicious inactivity but they can't prevent viruses from entering the system through legitimate sources such as a web browser or email, Hence a frequently updated antivirus program must always be included in an overall security strategy[4].

Software based firewalls are worthless if these are not installed on every system on the network as they can't protect an entire network. For an organization to ensure optimal security, these antivirus(AVR) based firewalls must be installed and managed properly in each and every system on the network.

Hence to make them more reliable, we plot a concept of moving the software based firewalls like antivirus base firewalls on a Private Cloud of the organization for more efficient security and functionality.

1.3 Concept of Private Cloud Based Antivirus based Firewall

This paper advocates a new model for AVR based firewall functionality for efficient and more productive measures and also for the detection functionality currently performed by the AVR software. Firstly, the firewall services provided by the host based AVR based firewalls can be effectively provided as a private cloud network service based on **software as a service (SaaS)** approach. Secondly, the identification of unwanted and malicious software should be determined by new heterogeneous detection techniques.

As the name suggests, there is a whole lot of difference between AVR software and AVR based firewall like in their functionality and usability. The AVR based firewall works as an AVR software for virus detection and also as a LAN firewall for internal network security.

1.4 What is Private Cloud

A Private Cloud is a type of a cloud computing model that involves a secure and distinct cloud based environment for the particular organization and is solely managed by the IT department of that organization behind the organization's own firewall with greater privacy. As with other cloud models, this model provides the service within a virtualized environment that eliminate the issues related to control of data and security. This model offers the capability where new policies can be added quickly as per the requirements. This cloud model is similar to the traditional model of individual local access networks (LANs) used by the organization but with the advantage of virtualization [2][13].

Some Advantages of Private Cloud

i) Security - As the private cloud services are dedicated to a particular organization, the hardware, data storage, and network can be designed using techniques such as distinct pools of resources with access restricted to connections, leased lines to assure high levels of security that cannot be accessed by other clients in the same data center[11].

ii) Greater control and customizable - Since the hardware is on-site, organizations have more control over the Hardware performance, storage performance and network performance. These can be specified and customized in the private cloud as they have complete oversight of their data with less worries over security.

iii) Higher performance and reliability - Since the private cloud is deployed inside the organization's firewall in the intranet, the transfer rates are dramatically increased. Even where the resources are internal, the virtualized environment makes the network more resilient to individual failures as the resources of the remaining unaffected servers can be fetched ensuring the physical security too[2].

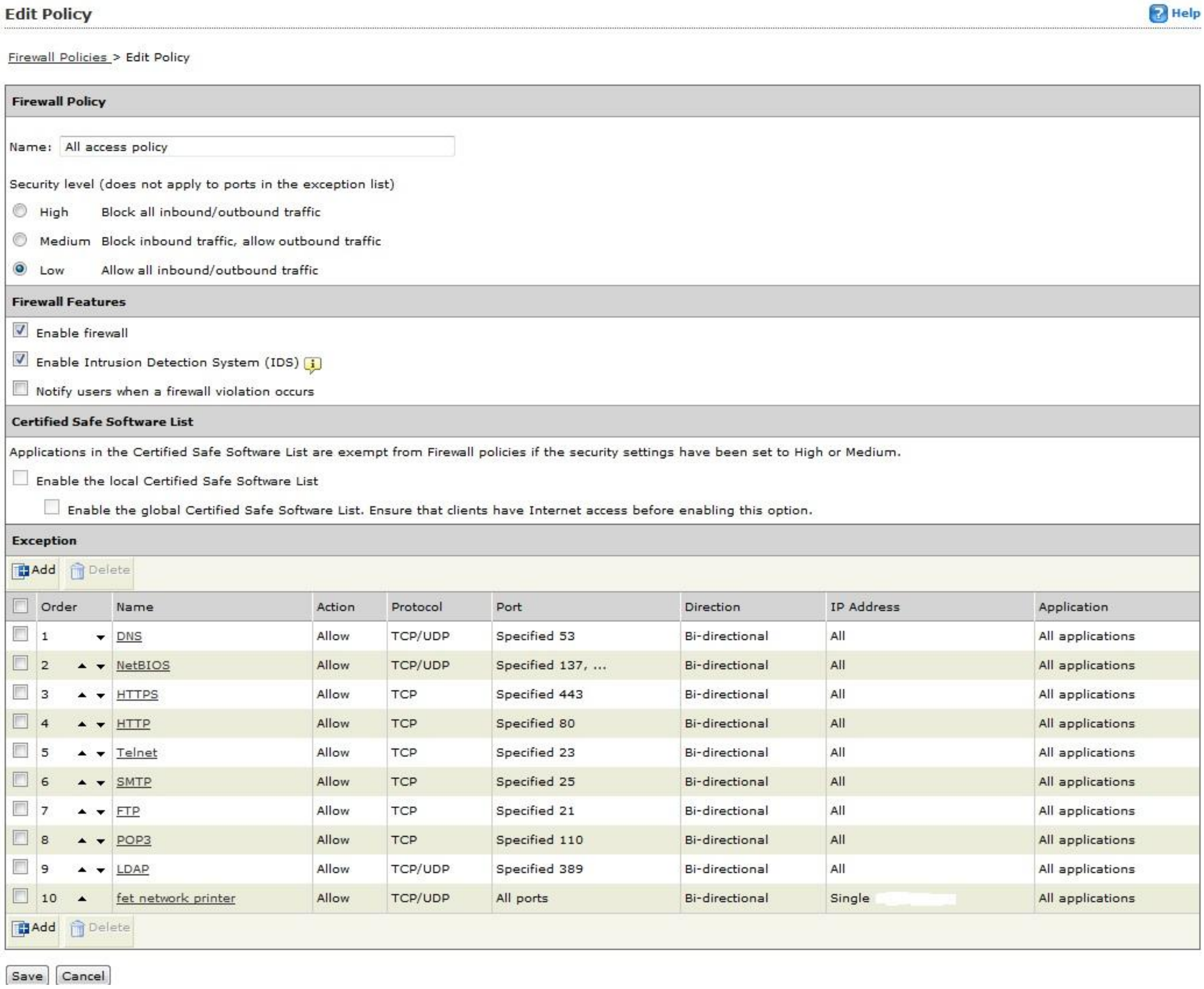
iv) Cost and energy efficiency - Implementing a private cloud in an organization improves the resource allocation in the entire network by ensuring the availability of resources to every department which can directly respond to their demands[11]. This is more effective than the traditional LANs as they make more effective use of computer resources which reduces the investment into unused capacity.

2. Antivirus based Firewalls – Detailed Analysis

As already explained, AVR based firewall is not just for virus detection and the main advantage of using these firewalls at vast organizations or offices is that it can be used as a firewall also. In organizations having several nodes or several sites, their firewall policies can be maintained by the IT security department from a single administrative level.

According to needs, policy, traffic, and data sharing for each and every node or the IP can be handled separately. For eg: - you have different departments in your organization, and you want a different policy of sharing for each of them. This can easily be done by enabling or disabling file sharing for particular VLAN, or even for a particular IP or node.

We worked on Trend Micro Office Scan Server. Let us show how these policies are actually managed from the admin level.



Edit Policy

Help

Firewall Policies > Edit Policy

Firewall Policy

Name: All access policy

Security level (does not apply to ports in the exception list)

○ High Block all inbound/outbound traffic

○ Medium Block inbound traffic, allow outbound traffic

● Low Allow all inbound/outbound traffic

Firewall Features

☑ Enable firewall

☑ Enable Intrusion Detection System (IDS)

□ Notify users when a firewall violation occurs

Certified Safe Software List

Applications in the Certified Safe Software List are exempt from Firewall policies if the security settings have been set to High or Medium.

□ Enable the local Certified Safe Software List

□ Enable the global Certified Safe Software List. Ensure that clients have Internet access before enabling this option.

Exception

Add Delete

□	Order	Name	Action	Protocol	Port	Direction	IP Address	Application
□	1 ▼	DNS	Allow	TCP/UDP	Specified 53	Bi-directional	All	All applications
□	2 ▲ ▼	NetBIOS	Allow	TCP/UDP	Specified 137, ...	Bi-directional	All	All applications
□	3 ▲ ▼	HTTPS	Allow	TCP	Specified 443	Bi-directional	All	All applications
□	4 ▲ ▼	HTTP	Allow	TCP	Specified 80	Bi-directional	All	All applications
□	5 ▲ ▼	Telnet	Allow	TCP	Specified 23	Bi-directional	All	All applications
□	6 ▲ ▼	SMTP	Allow	TCP	Specified 25	Bi-directional	All	All applications
□	7 ▲ ▼	FTP	Allow	TCP	Specified 21	Bi-directional	All	All applications
□	8 ▲ ▼	POP3	Allow	TCP	Specified 110	Bi-directional	All	All applications
□	9 ▲ ▼	LDAP	Allow	TCP/UDP	Specified 389	Bi-directional	All	All applications
□	10 ▲	fet network printer	Allow	TCP/UDP	All ports	Bi-directional	Single	All applications

Add Delete

Save Cancel

Figure 2: Different firewall policies under AVR based firewall server

Figure 2 shows different firewall policies made in the Trend Micro AVR firewall Server. You can modify the policy for various services like HTTPS, Telnet, FTP, DNS for each and every VLAN for inbound and outbound traffic or any port can be blocked or unblocked for that particular service.

Let us see how these policies actually work:

i) The most important security violation occurs when the user installs third party software's in the organization's nodes which might prove to be a major problem. The solution to this is provided by the firewall which opposes any new software installations in the system. And in any case, if the required software needs to be installed like the drivers of the printer attached, then also the firewall can simply give the user the access to unload the firewall for the time being until the next restart.

This is done by simply clicking the 'unload officeScan' in the client machine as shown in the figure 3, but which off course requires a password. Even if the user is to be given full access to be able to disable the firewall completely for all the policies, that can also be done from the admin level. In that case user is given the right to enable or disable the firewall completely with an added option in the trend micro window as shown in figure 3.

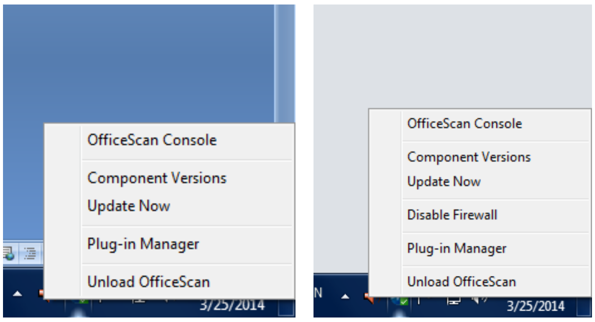
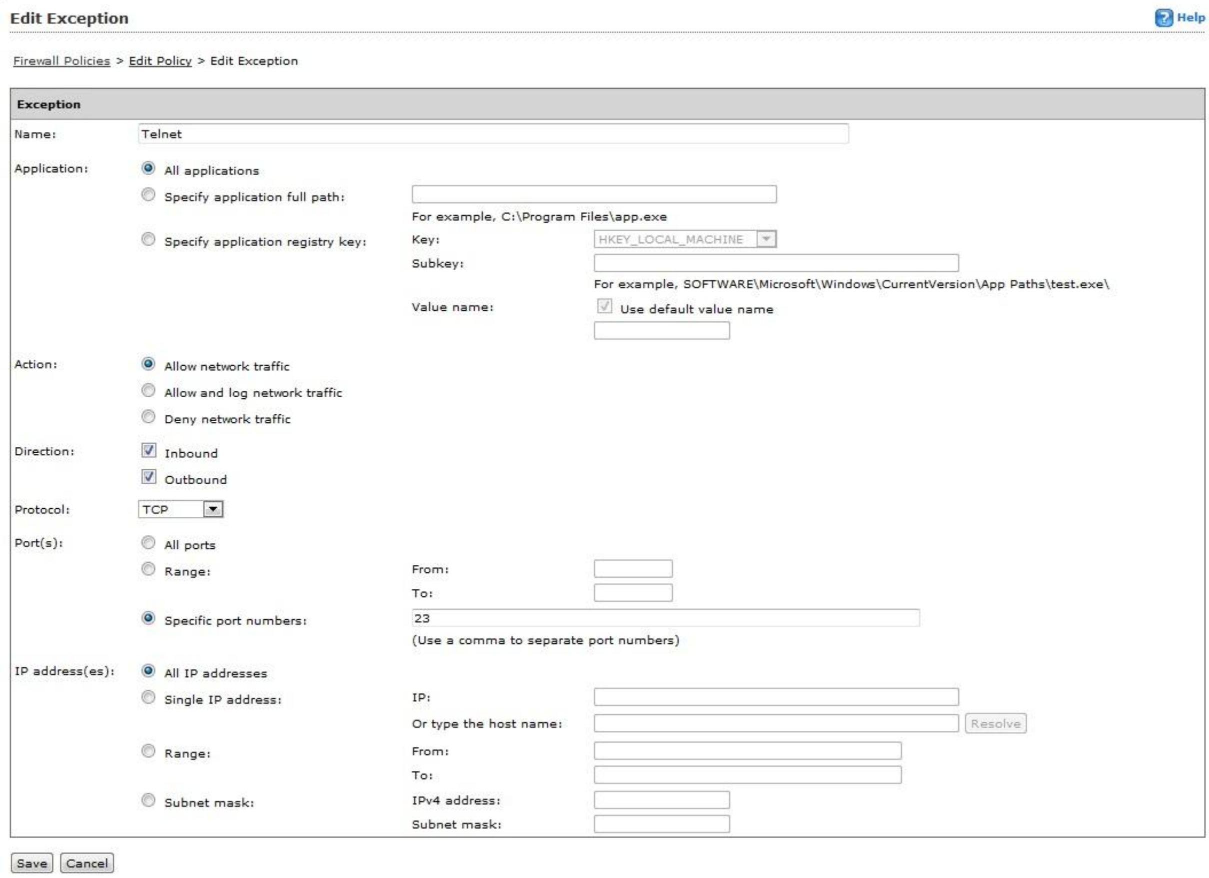


Figure 3: Before and after giving user the permission to disable firewall

ii) Another issue we considered is the ‘Telnet’ service. A network connected in a simple manner by default provide the access to switches and routers to the clients, which could prove to be harmful in some cases as any user would be able to take the access through telnet to any manageable switch. Either way it could be risky, so in such cases you need to block the Telnet services for every node which could be easily done through the AVR firewall by disabling or enabling Telnet services for any such client or even for a particular VLAN.

Everything can be managed from this console for the Telnet service as shown in figure 4. User can maintain the traffic for Telnet, can allow or deny inbound and outbound traffic, and importantly allow or disallow the user or an entire VLAN to the Telnet access by assigning the IP range or entire segments at the bottom.



Edit Exception

Firewall Policies > Edit Policy > Edit Exception

Exception

Name: Telnet

Application:
● All applications
○ Specify application full path:
For example, C:\Program Files\app.exe
○ Specify application registry key: Key: HKEY_LOCAL_MACHINE
Subkey:
For example, SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\test.exe\
Value name: ☑ Use default value name

Action:
● Allow network traffic
○ Allow and log network traffic
○ Deny network traffic

Direction:
☑ Inbound
☑ Outbound

Protocol: TCP

Port(s):
○ All ports
○ Range: From: To:
● Specific port numbers: 23
(Use a comma to separate port numbers)

IP address(es):
● All IP addresses
○ Single IP address: IP:
Or type the host name:
○ Range: From: To:
○ Subnet mask: IPv4 address: Subnet mask:

Figure 4: Policy for Telnet Service

Similarly like this, various policies according to the requirements of the organizations, can be made to minimize and oppose the security issues discussed earlier in **section I.**

Many remote location clients or whole VLAN’s can be monitored for scans and for the virus definition updates, pushing the AVR services to the clients or can be monitored even for the threat tracking by the AVR firewall.

We have shown how the AVR based firewall is useful for an organization’s internal network for security. But for more security and privacy, there is a better way to implement the AVR firewall server in an organization which is by the concept of CLOUD COMPUTING.

3. ANTIVIRUS BASED FIREWALL AS SOFTWARE AS A SERVICE (SAAS)

Software as a Service (SaaS): In this type of distribution model, the cloud service provider will provide the platform and services hosted by the IT department and are made available for all the clients to use their applications remotely over the entire network, like mail services, e-commerce applications etc. The clients using these services will have the common interface which provides the added advantage of not to pay for extra licenses [12].

SaaS is a model of software deployment where the AVR based firewall can be hosted as a service which can be provided to the clients across the intranet of the organization. This can be managed by the IT department of the organization itself. Figure 5 shows the architecture of how the services deployed on the private cloud can be accessed securely by the clients within the security perimeter.

The essence of the model is that the client does not have to buy the software or install it on the system but still the services it provides can be used infinitely by the end user clients [12]. As a result, with SaaS, clients get access to the necessary application on a cloud server which allows saving money and quickly introducing the software. It is needless to say that as a result everyone wins as it is reliable, efficient, secured and above all, it quickly provides the clients with the necessary service over the entire network and saves time too.

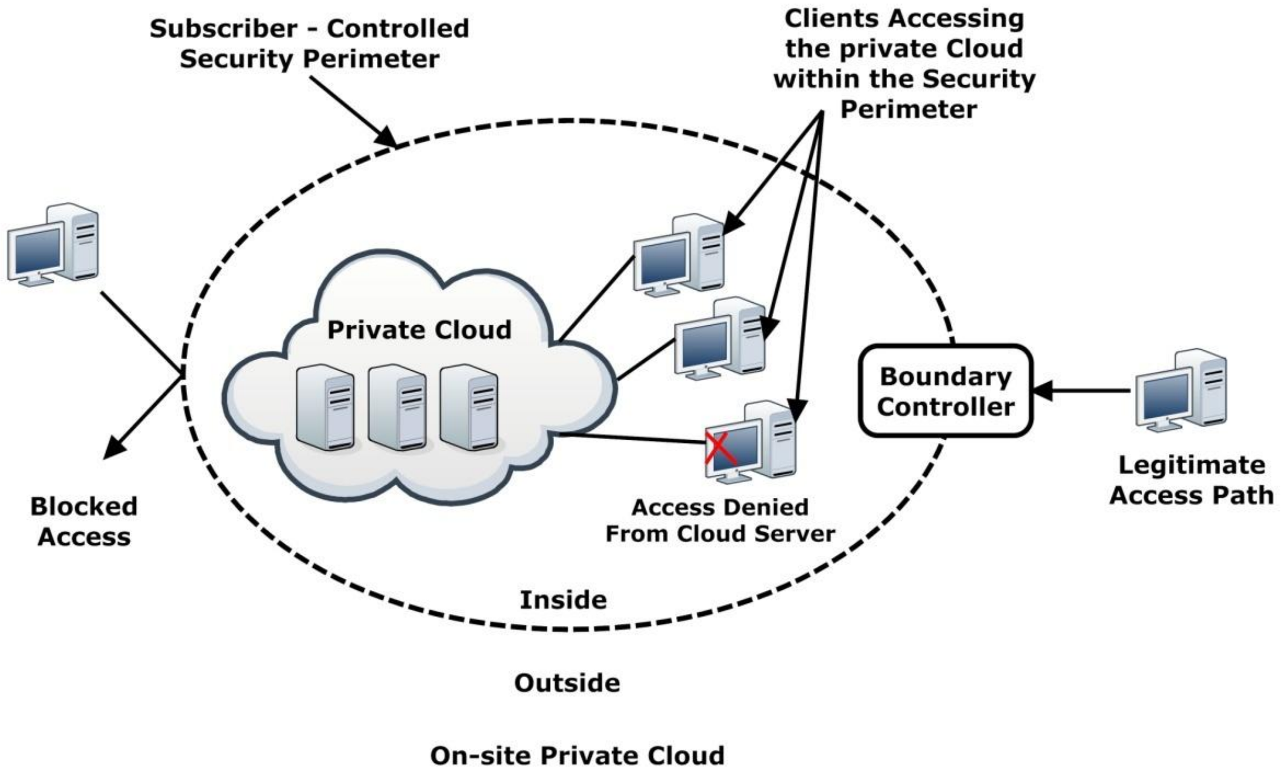

Subscriber - Controlled Security Perimeter
Clients Accessing the private Cloud within the Security Perimeter
Private Cloud
Boundary Controller
Legitimate Access Path
Blocked Access
Access Denied From Cloud Server
Inside
Outside
On-site Private Cloud

Figure 5: **Architecture of software as a service (SaaS) on a private cloud.** [15]

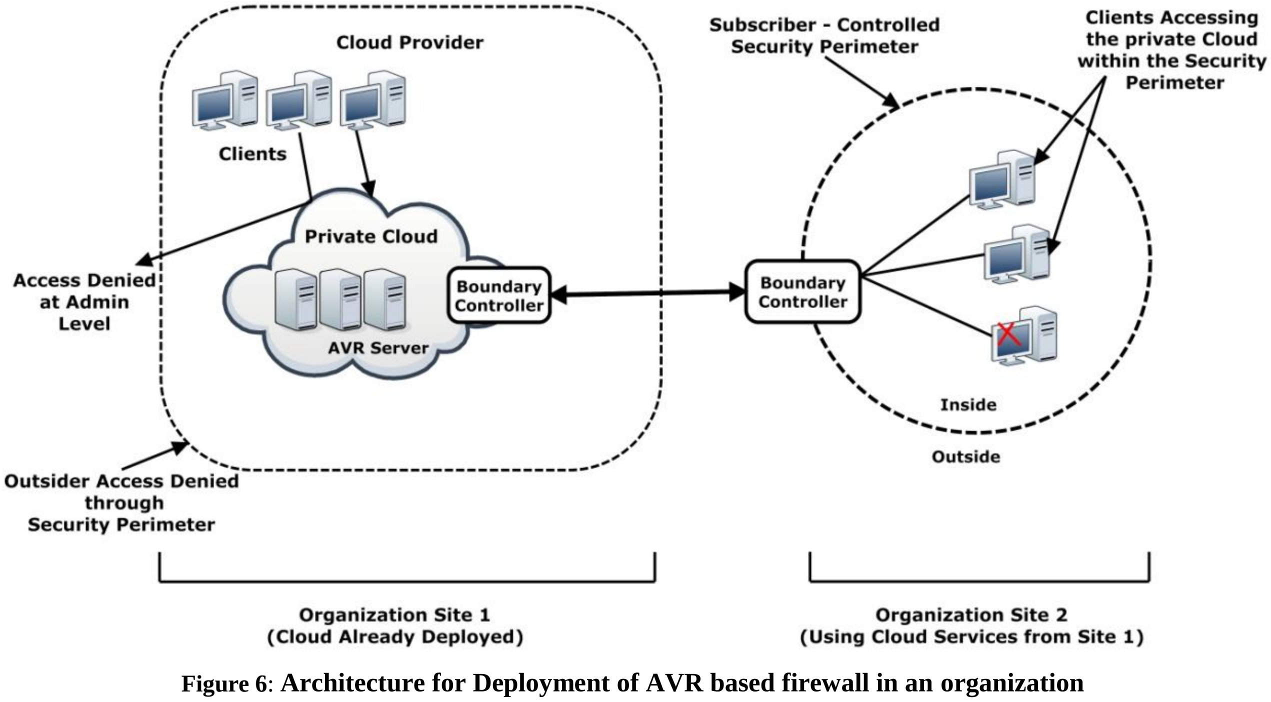

Cloud Provider
Clients
Private Cloud
Boundary Controller
AVR Server
Access Denied at Admin Level
Outsider Access Denied through Security Perimeter
Subscriber - Controlled Security Perimeter
Clients Accessing the private Cloud within the Security Perimeter
Boundary Controller
Inside
Outside
Organization Site 1 (Cloud Already Deployed)
Organization Site 2 (Using Cloud Services from Site 1)

Figure 6: **Architecture for Deployment of AVR based firewall in an organization**

Figure 6 shows the cloud is deployed at the organization site 1 with the purpose of providing the AVR based firewall services to the entire internal network of the organization regardless of the geographical region. A security perimeter must be employed to deny the access to an outsider or any type of intruder through the firewall policy employed by the firewall team itself. Hence the access to the network will always be restricted to the legitimate users only. As shown in the figure 6, the specific users can also be provided or denied access to various network based services as discussed in the section- II, through the centralized management of the AVR based firewall on the cloud. The users across the entire network, even at the organization site 2, can also be provided with the firewall services that too within the security perimeter assuring the network security all through the network of the organization regardless of the geographical area.

The security perimeter shown above is controlled by the following three domains:

- Physical Domain
- Social Domain
- Digital Domain

Physical Domain: For every organization, physical security is a must. This security domain not only includes the physical devices or equipments a user or an employee are permitted to bring into the organization premises but also includes the deployment of cameras, scanners etc.

Social Domain: This security domain depends on the employee's role or functions in the organization. Keeping that in mind, the access to various resources or services to that employee or that particular department is provided ensuring the security. For e.g.: An organization has their network based services outsourced to third party companies, let us say, Wipro InfoTech. Even though the Wipro team sits in their office premises, the organization does not want them to have the full access to their network. Hence they have certain firewall policies made for that team accordingly and maybe even with certain ports blocked. Hence even with restricted access, when a risk occurs, the same can be easily rectified without compromising the entire network. This is configured accordingly from the AVR based firewall as discussed in the **section-II**.

Digital Domain: This security domain consists of validating the employee. This includes the authorization of the legitimate users even when they are outside the organization premises.

"Are you who you say you are?" The question needs to be verified [14].

Even after the authorization, what services? , what features? , how much access needs to be granted? , to the users who are accessing the network from outside the premises must be considered. Any type of information or data can be bagged by a third person. Hence only limited access should be granted. So, whenever the physical perimeter is exited, the restrictions should be imposed which can also be managed by the firewall team according to the organization's policy [14].

Consider a case- If a company wants to give access to their internal network to the employees regardless of their location, a particular global login for the employees are made which requires a login, plus the authentication through SecureID devices like RSA SecureID, which generates a token ID like an OTP to give time based authentications. After the authentication is passed, the firewall services should come into place ensuring the security that only certain resources could be accessible to the employees who are accessing the intranet through remote locations to provide security for eavesdropping and data bagging. For e.g. when an employee login through remote location, different sets of firewall policies come into place, like- Closed FTP access – Port 21 is closed, to disallow the file transfer. Hence, a restricted access should only be provided.

This is how 'Boundary Controller' (in figure 6) works to provide access to legitimate users through legitimate paths. It is very important that also these three domains are properly aligned, otherwise the network could be compromised in any way.

3.1 Advantages of using AVR based Firewall as SaaS on a Private Cloud

i) No software installation - SaaS works as an alternative to the standard model of software installed on the clients (standard delivery model). There is no need to install the AVR software to each and every client machine. All they need to do is to connect their thin client to the network.

ii) Firewall services - Each and every system which is connected to the network will be automatically behind the firewall. Even when a new system comes in the network, necessary firewall services are automatically pushed from the cloud management application which maintains the security and the makes the network more reliable.

iii) No updates required - No need to update the AVR software as the cloud maintains the updated AVR dictionary.

iv) Compatibility **-** Each and every system in the network will be using the same version of the antivirus firewall software and hence there will be no compatibility issues.

v) Antivirus as a network service -The detection capabilities currently provided by the client based antivirus software could be made more efficient and effective by using antivirus as a *cloud network service*. The client will be running a lightweight process to detect files instead of whole system scanning and complex software analysis. This report will be fetched by the network service for analysis which will automatically quarantine the detected malicious codes and by pushing the required patches not only to the specified client but to the entire network for improved network security [10].

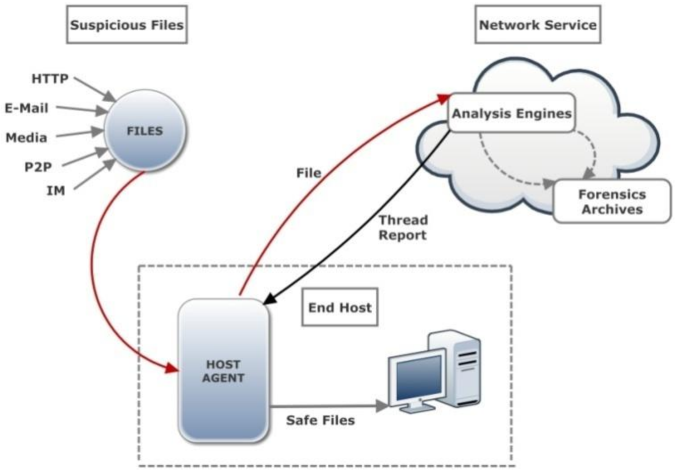


Figure 7: **Architectural approach for cloud file analysis service.** [12]

Figure 7 shows a malicious virus on the host PC is detected and is pushed to the AVR network service on the cloud for file analysis. When the AVR server detects any malicious inactivity or any new virus code in any of the systems in the entire network of the organization, it will automatically update the virus dictionary for new virus definitions and the network and antivirus team can then work on the threat report for forensics analysis and make suitable patches and then these patches will be pushed to the entire network.

3.2 Virus Detection Technique

This new model provides several important security benefits:-

i) Better virus detection capability - With a combination of many antivirus engines working simultaneously, the overall inspection and identification of virus codes, malicious threats and unwanted software can comparatively improve and hence the detection capability.

ii) Improved forensics capabilities - The forensics and intrusion analysis can subsequently improve due to the enhanced information rich databases about the hosts which include timely relationships between access events of the files and different hosts [8].

iii) Retrospective detection - Previous records and historical information can be analyzed for different hosts regarding identical threats. Take an example, whenever a new virus or even intrusion is detected, the analysis of execution history of different hosts on the network can help identify which other different hosts might also be affected by the same intrusion [12].

iv) Easy management - Moving the detection techniques from the hosts and into the network significantly improves the software deployment management on a wide range and simultaneously enables the network and antivirus administrators to centrally control the management and enforce access policies.

4. CONCLUSION

To address the ever growing security issues and threats of modern malicious software for an organization, we have proposed a new model for the deployment of the antivirus based firewall by providing antivirus firewall as a network service on private cloud using Software as a Service (SaaS) approach. This model provides significant advantages over the traditional host based antivirus firewall services which include better security through virus detections, improved forensics capability, ease of management and retrospective detection of the entire network.

In the coming future, we plan to investigate and evaluate the effectiveness of this proposed model to demonstrate how it provides significant improvement for the entire network security with greater protection for the clients against modern threats with centralized management.

5. ACKNOWLEDGEMENT

We would like to thank Mr. N.S. Arneja (Sr. Technical Director & HOD, NIC Parliament Informatics Division) for providing us the opportunity to work on the network infrastructure and providing the required hardware and network access.

6. REFERENCES

[1] vicomsoft.com [Online], Article: Firewalls, Available: http://www.vicomsoft.com/learning-center/firewalls/

[2] Aerohive Networks: Public or Private Cloud: The Choice is Yours, White Paper, 2013

[3] Micki Krause, Harold F. Tipton, "Handbook of Information Security Management",Auerbach Publications, CRC Press LLC

[4] networkuptime.com [Online], Article: Software-based Firewalls and Hardware-based Firewalls, Available: http://www.networkuptime.com/winfw/page01-02.html

[5] Cisco.com [Online], Article: "What is Network Security?", Available: http://www.cisco.com/cisco/web/solutions/small_business/resource_center/articles/secure_my_business/what_is_network_security/index.html

[6] Carl E. Landwehr & David M. Goldschlag, "Security issues in networks with Internet access", Proceedings of the IEEE 85(12): 1034-2051, December 1997.

[7] Fred Cohen, "Computer Viruses Theory and Experiments", Computers and Security 6:22-35, 1987

[8] Fortinet, "Improving Network Protection and Performance with Network-Based Antivirus Technology", Fortinet White Paper, October 2002

[9] CDW-G, Private Cloud And Software As A Service, CDW-G White Paper, 2012

[10] Addison Snell, "Solving Big Data Problems with Private Cloud Storage", Intersect360 Research, October 2011

[11] Intel, "Architecting Software as a Service for the Enterprise", IT@Intel White Paper, October 2009

[12] Jon Oberheide, Evan Cooke & Farnam Jahanian, "CloudAV: N-Version Antivirus in the Network Cloud", Available:http://www.eecs.umich.edu/fjgroup/pubs/usenix08-cloudav.pdf

[13] Ilango Sriram & Ali Khajeh-Hosseini, "Research Agenda in Cloud Technologies", LSCITS Technical Report, 2010

[14] Prof. Dr. Pieter H. Hartel, "VISPER: The Virtual Security Perimeter for digital, physical and organisational security", March 2010, Available: http://www.utwente.nl/ewi/is/documents/visper_proposal.pdf

[15] techno-pulse.com [Online], Article: Cloud Deployment Models – Private, Community, Public, Hybrid with Examples, Available: http://www.techno-pulse.com/2011/10/cloud-deployment-private-public-example.html resources.infosecinstitute.com [Online],Network Design: Firewall, IDS/IPS, Available: http://resources.infosecinstitute.com/network-design-firewall-idsips/

7. AUTHOR'S PROFILE

Parminder Singh Arneja pursued his Bachelor of Technology in Electronics and Communication Engineering from Punjab Technical University, Punjab, India. Right now he is working in SAN administration at NIC Parliament Informatics Division, Rajya Sabha Secretariat through CyberQ Consulting Pvt. Ltd., New Delhi, India. Before that he worked as a Network and Security Engineer for Wipro Infotech Pvt. Ltd and his fields of interests are Storage Area Network, Network Security and cloud Virtualization.

Sidharth Sachdev pursued his Bachelor of Technology in Computer Science and Engineering from Punjab Technical University, Punjab, India. Right now he is a Mainframe System Programmer at IBM India Pvt. Ltd., Bangalore, India. Before that he worked as trainee in University of Jammu, Jammu and Trainee in Rooman Technologies, Bangalore and his Fields of interests are Mainframe Administration, Virtualisation, Linux Administration, Information Security and Open Source Cloud Computing.