

End to End v/s Firewall Security

A guide to strengthen Perimeter Security

A New Approach to secure the perimeter and beyond

Overview

Firewalls have been a key component of any organizations Network Security Infrastructure. The basic task of the Firewall is to regulate/deter un-authorized access at the perimeter. However Firewalls have done little to thwart un-authorized access inside private networks. There are several inherent deficiencies that exist with Firewalls and this paper examines/explores the ways and means of solving this.

Firewalls do not protect data outside their perimeter. Any data coming in through the firewall properly has to be considered a risk. Firewalls are also the most visible portion of a network installation to the outside world and thus make attractive targets for attack. Any use of firewalls should be supplemented by a defense-in-depth strategy utilizing several layers of protection such as access control, anti-virus software, and intrusion detection.

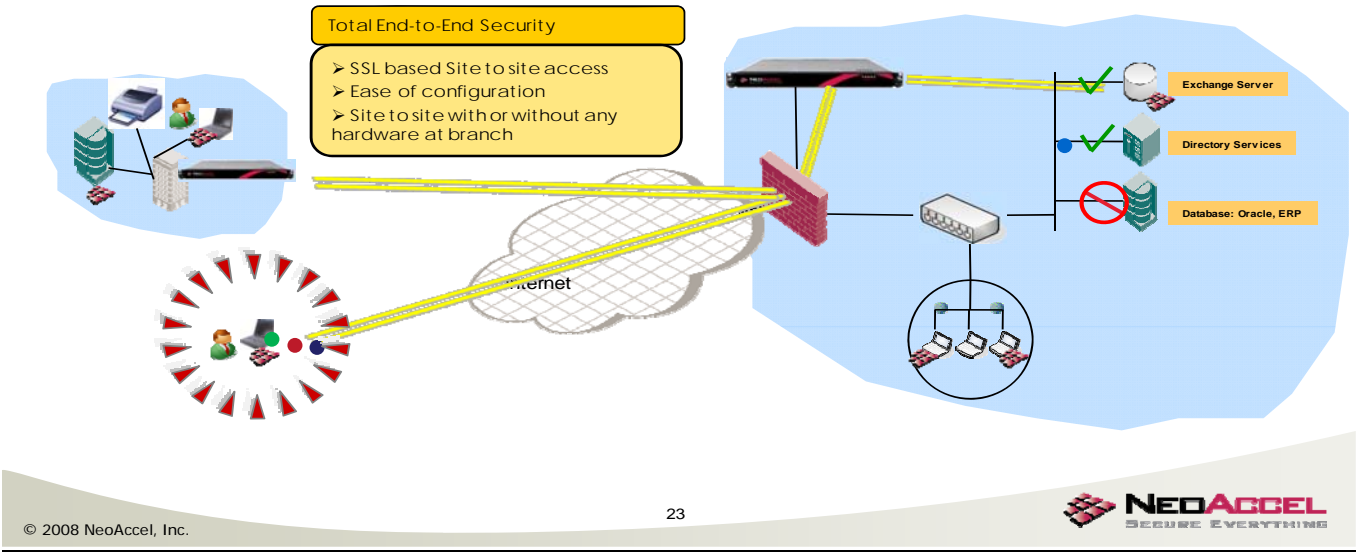
It is important to know that firewalls are vulnerable to attack. They can be penetrated and lend themselves to aiding further in an attack once they themselves are defeated. Proper configuration is a must to maintain the efficacy of any firewall system. It should be updated periodically to ensure it is current with the internal and external environment of the network. Activity logs should also be checked on a regular basis to find attempted and successful intrusions. A major limitation is that firewalls have only minor control over the data that passes through them. Malicious or inaccurate code has to be controlled from inside the perimeter.

Some of the well known limitations of Firewalls are as follows:

1. A firewall protection is limited once you have an allowable connection open. This is where another program should be in place to catch Trojan horse viruses trying to enter your computer as unassuming normal traffic.
2. Firewalls currently available lack some degree of intelligence when it comes to observing, recognizing and identifying attack signatures that may be present in the traffic they monitor and the log files they collect.
3. Monitoring - firewalls can't notify you if someone has hacked into your network. Many organizations need additional security monitoring tools.
4. Encryption - firewalls don't provide formalized solutions to encrypt confidential documents and e-mail messages sent within your organization or to outside business contacts.

Total End-to-End Security

- | | |
|---------------------------|----------------------------------|
| SSL BASED TUNNELING | FASTER APP ACCESS - WAN Optimize |
| ENDPOINT COMPLIANCE | DATA LEAKAGE PREVENTION |
| STRONG AUTHENTICATION | LOG AND AUDIT REPORTING |
| USER BASED ACCESS CONTROL | ACCELERATED SITE-TO-SITE ACCESS |



The Paradigm Shift in implementing End to End Security the right way

NeoAccel's 3rd generation End to End Security Solution is a paradigm shift in Network Security Architecture and ensures that each and every connection is Encrypted and periodically validated. Every end user who wants to get access to the corporate resource is only allowed on a secure port 443. And the compliance to corporate policy (potential harm it can inflict to the corporate network resources) of the end point is determined in advance before allowing access. This approach of allowing entry into the corporate network is proven to be extremely safe and not prone to the vulnerabilities and promiscuous access methods of traditional Firewalls, since every end point coming from out of the perimeter is checked for compliance against the most up-to-date corporate policies in real-time.

The End Point Security policy database can be automatically updated to reflect and cater to the changes in the real world

By using NeoAccel's Solution, all internal communication between peers can be secured as-well. This gives the added advantage of securing all network communication from within the perimeter. The Administrator can also monitor in real time who have logged in

from within the corporate office, branches and who is coming from outside the organization. This single interface gives the administrator an enhanced overall picture of the network level activity in terms of usage, abuse and attacks. The enhanced monitoring and reporting component of the solution gives a very accurate chart of people using different resources and how long they have been using it and it can also pull up records of un-authorized access.

One of the prime sources of network security breaches and infection by malicious code inside the corporate network can be traced to an extraneous end point which was allowed access without conducting the necessary compliance checks.

NeoAccel's solution does not allow lapses in this process and conducts mandatory checks to thwart security breaches and attacks before allowing anyone access inside the corporate network.

- 1. End-Point Security Compliance (EPS)**
 - a. .Virus Scan, Key loggers, Application execution control..144 configurable checks**
 - b. Enforce Deep Packet Inspection to check and match signatures**

- 2. End-Point/User Authentication**
 - a. Machine Certificates, Radius,LDAP,AD,ACE**
 - b. Strong Multi Factor Authentication to determine the authenticity of the person seeking access.**

- 3. SSL Based Secure Tunneling**
 - a. Remote Access from behind a firewall**

- 4. User based granular Access Control**
 - a. User and Group access control and Not just IP address**

- 5. WAN Optimizations**
 - a. Fastest remote access solution, No TCP-Over-TCP meltdown, DynCompression**

- 6. Data Leakage Prevention (DLP) and Data Cleanup**
 - a. Secure Desktop and secure Laptop**

- 7. Intelligent Logging and Audit**
 - a. Track all use activities**

- 8. Accelerated site-to-site access**
 - a. High end server to server communication**

Summary

Application layer firewalls conduct deep packet inspection of all traffic coming into the network at the perimeter. This approach undermines performance and leads to a bottleneck due to the induced latency. Whereas NeoAccel's intelligent EPS engine can enforce deep packet inspection on every endpoint machine even before the packet leaves the source, thereby putting a end to viruses/malwares/Trojans/adware at the origin and bringing secure high performance access to the resources in the corporate network.

This approach of securing the end points is a one stop solution which can provide true security both inside and outside the company's perimeter

You don't need a glorified Firewall if you do the security the Right Way.