Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Protecting the Next Generation Network -Distributed Firewalls

Corporate networks are constantly changing to meet the needs of businesses and continue to expand in ways that we couldn't have imagined only a few years ago. Gone are the days of a closed network with one external point of access. With the expansion of high speed Internet access via DSL and cable modems, users can now work from home using VPNs. Many companies are expanding their networks even farther with wireless technology allowing access for devices that aren't even physically connected to the network. Suddenly the...

Copyright SANS Institute
Author Retains Full Rights

AD

Protecting the Next Generation Network – Distributed Firewalls

Robert Gwaltney

October 7, 2001

Introduction

Corporate networks are constantly changing to meet the needs of businesses and continue to expand in ways that we couldn't have imagined only a few years ago. Gone are the days of a closed network with one external point of access. With the expansion of high speed Internet access via DSL and cable modems, users can now work from home using VPNs. Many companies are expanding their networks even farther with wireless technology allowing access for devices that aren't even physically connected to the network. Suddenly the networks with one or two points of access now have multiple points of access that can change from day to day.

Many people think their network is protected because they only use VPN for remote access. But, how secure are the devices on the end of the VPN connection? If the hacker compromises the end user's machine, they can then use the machine to connect to your corporate network. This is what happened to Microsoft in October of 2000 using an employee's home computer. Securing these new networks requires a different approach, which distributed firewalls provide.

Traditional Firewalls

Traditional firewalls are devices often placed on the edge of the network that act as a bouncer allowing only certain types of traffic in and out of the network. Often called perimeter firewalls, they divide the network into two parts—trusted on one side and untrusted on the other. For this reason they depend heavily on the topology of the network. The firewall is used to enforce a central policy of what traffic is allowed in and out of the network. When traffic flows through the firewall it is evaluated by a set of rules based on ip address, port, etc. and either allowed or denied. All traffic entering or leaving the network must pass through this point. This requirement itself is often one of the downfalls of the firewall. For example, users might go around the firewall by using a modem or some other connection to the Internet. Another problem is encrypted tunnels, which provide a hole through the firewall where the traffic isn't evaluated and flows freely.

Distributed Firewalls

Steven M. Bellovin of AT&T Research is credited with the idea of distributed firewalls. Unlike traditional firewalls, distributed firewalls are not placed in one location. As the name implies, the distributed firewall is installed throughout the network to all endpoints. Distributed firewalls are based on three main points.

Policy Language

The policy language is used to create polices for each of the firewalls. These policies are the collection of rules, which direct the firewall in how to evaluate the network traffic.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

System Management Tools

The system management tools are used to distribute the policy to the firewalls and to collect logging and reporting information.

IPSEC

IPSEC provides network-level encryption used to secure network traffic and the transmission of policies. It also provides a more important function of providing a way to cryptographically verify the sender of information. Senders can then be uniquely verified by their certificate.

How it Works

Most distributed firewalls run in kernel mode and sit at the bottom of the OSI stack. The firewall evaluates all network traffic whether it is from the Internet or the internal network. This protects the system much in the same way as a traditional firewall protects the network. After the firewall is installed on all network endpoints, a central policy is developed. This policy is written using the policy language and then compiled in a format to be transferred to each firewall. The system management tools are then used to transfer the policy to each firewall. Because the firewalls are in different locations throughout the network and may be on a machine that changes locations, they cannot depend on the network topology to determine the sender of the network traffic. For this they use the certificates provide by IPSEC. These certificates uniquely identify the sender and don't depend on the network topology. The firewall then evaluates the traffic based on the central policy and decides to allow or deny it. The firewall can also then transfer logging information to a central location where it can be used for reporting.

Implementation

In its purest form of implementation, every network endpoint would contain a firewall and all network traffic would be secured using IPSEC. However, many legacy systems do not offer support for IPSEC, and many companies already have an investment in traditional firewalls. Therefore most implementations take on some hybrid form.

Remote Access

In a remote access implementation the systems are outside of the traditional firewall and therefore unprotected. These systems establish a VPN connection through an IPSEC gateway setup on the corporate network. The IPSEC tunnels provide protection for the network traffic as it is transferred in and out of the network. A distributed firewall is also installed on the system that receives the central policy from the corporate network. The distributed firewall then enforces the policy and offers it the same protection as machines on the trusted network.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Layered Protection

Distributed firewalls can also be installed on machines that are behind a traditional firewall and already on the trusted network. This offers a second layer of protection in the event that there is an error in the configuration or failure of the traditional firewall. This implementation can also be used to specialize the security on critical servers that may need more protection than the traditional firewall provides. They also protect the systems from internal attacks, which would not pass through an external firewall.

E-commerce

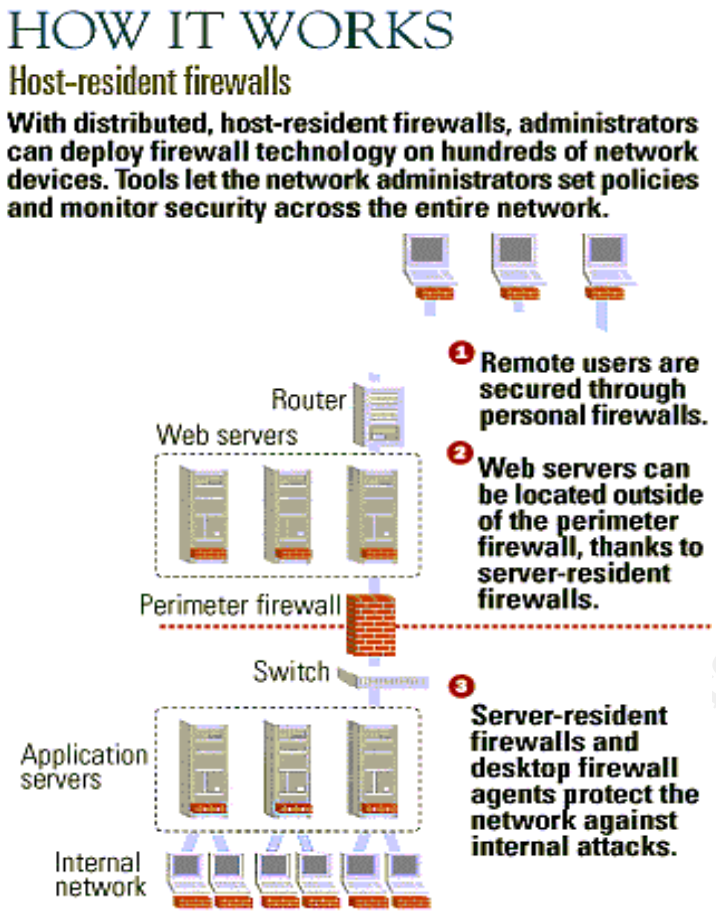
In an e-commerce implementation the performance and availability of the server is usually a high priority. Because distributed firewalls are installed on the host system, they allow servers to be placed outside the traditional firewall on the untrusted network. This reduces any performance loss that might be caused by all the traffic flowing through the traditional firewall. This also removes the traditional firewall as a single point of failure.

These different implementations can also be combined to fit the varying needs of your network. Steve Hunt of Giga Information Group sums it up well.

"It's a migration, or adapting your current infrastructure to meet the new demands. The solution involves using all routers, firewalls, and VPNs. To do that, you will need administration processes, but once you have co-ordinated [these], you can have distributed authorization"(Gerald, p.2).

The distributed firewall enables this system of distributed authorization. No longer is network traffic evaluated only at one point on the network, but it is now evaluated or authorized at every network endpoint. (Figure 1)

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.



(Figure 1)

Features

Distributed firewalls may not be the solution for everyone. They enhance the features provided by a traditional firewall in many ways but do have disadvantages. Traditional firewalls perform some tasks better than distributed firewalls. Below is a list of features and issues along with a brief summary of how each type of firewall deals with the situation. Hopefully this will help in determining the correct type of firewall for your network.

Network Topology

As discussed earlier traditional firewalls depend heavily on network topology because they divide the network into trusted and untrusted. Because of their static location they also can be circumvented by users going around the firewall. There also can be a performance bottleneck because they are the single choke point on the network, and therefore, a single point of failure. Distributed firewalls don't suffer from these disadvantages because they are installed on each system, which removes the single choke point on the network. They also operate independent of the network topology because they evaluate all traffic that is sent to the machine.

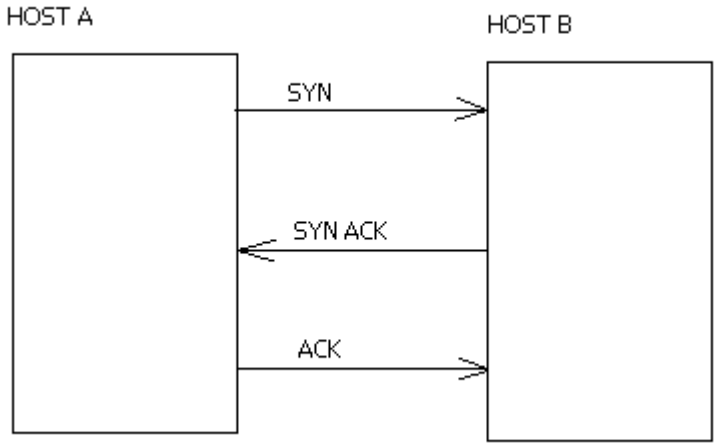
© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Policy Enforcement

Traditional firewalls use rules based on ip address, port, packet flags, etc. Many of these items can be spoofed allowing traffic to penetrate the firewall. Distributed firewalls' use of IPSEC and certificates prevent this. Certificates are not easily spoofed and make this a more secure method of uniquely identifying the sender of the traffic.

Knowledge of Network Traffic

To understand this point, here is a brief primer on the three-way handshake used by TCP to establish a connection. Host A wants to make a connection to Host B so it sends a packet with the SYN flag (synchronize) set. When Host B receives the packet from Host A, it replies with a packet that has both the SYN and ACK (acknowledge) flags set. Host A then replies with a packet with the ACK flag and the connection is established. (Figure 2) Traditional firewalls evaluate traffic based on externally visible features. For example if a traditional firewall sees a packet with the ACK flag set it may allow it through because it assumes its part of a previously ongoing conversation. ACK packets can be used by some "stealth" port scanners. A distributed firewall, however, since it is on the host system, will know whether it is expecting an ACK packet in response to a connection it was establishing. It then can make a much more informed decision on whether to allow or deny the packet.



(Figure 2)

Application-level Proxies

Traditional firewalls do a very good job of providing application-level proxies. Many distributed firewalls do not include application-level proxies, but this is changing as the technology matures.

Intrusion Detection

Many traditional firewalls include some form of intrusion detection. However, only traffic passing through the firewall will be examined, so this excludes much of the

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

internal traffic. Distributed firewalls will see more of the internal traffic, but have the problem that they must all send log information to one central location. This can cause problems for remote users who may connect over slower networks.

Denial of Service

In the event of a denial of service attack, a traditional firewall may be able to block some attacks and contain them to the untrusted side of your network. While you wouldn't have external connectivity, the internal network would function as normal. If only distributed firewalls were used, the entire network would be affected because there would be no single choke point to stop the attack.

Inside Attacks

Distributed firewalls provide the only protection from an inside attack. Because it is host based, the distributed firewall will evaluate all traffic regardless of sender. Traditional firewalls will never see the traffic because it is on the internal network and never passes through the firewall.

Central Management and Reporting

Both traditional and distributed firewalls use methods of central management and reporting. Distributed firewalls do have one advantage. Again, because they are located on the host system, you can specialize the firewall policies and place systems in groups for easier management. A traditional firewall has one policy for the entire network

Current Solutions

Since distributed firewalls are a fairly new technology the list of vendors is quite small. Many vendors provide additional features. CyberwallPLUS by Network-1 is certified by the ICSA, a certification usually only held by traditional firewalls. CyberArmor by InfoExpress not only has rules for network traffic but also for applications. When installed, it takes cryptographic hash of the executable files. Rules can then be set up for which applications the user can execute. Secure Enterprise by Sygate has a feature they call the VPN Enforcer. The VPN Enforcer is installed on your VPN server and will only allow VPN connections from clients that are running the distributed firewall and have the current policy. These are just a sample of some of the features that are being added to distributed firewalls.

Conclusion

As networks continue to change and expand new tools are needed to keep them secure. Distributed firewalls take a new approach by securing every host on the network. They also have no trouble handling the changing topology of today's networks. This makes them a perfect match for telecommuters that work from remote locations and often use a VPN to connect to the corporate network. As they continue to develop, new features will be added that will only

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

increase their security and ease of use. Distributed firewalls just may be the tool to secure next generation networks.

References

Andress, Mandy. "Closing the gap in end-user security" 29 August 2000.
URL: http://www.infoworld.com/articles/es/xml/00/09/01/000901estca.xml

Anonymous. Maximum Security Second Edition. Indianapolis: SAMS, August 1998. 59-60.

Bellovin, Steven M. "Distributed Firewalls"
URL: http://www.research.att.com/~smb/papers/distfw.html

Fogei, Avi. "Distributed firewalls provide options for security topology" July 2000.
URL: http://www.serverworldmagazine.com/compaqent/2000/07/firewall.shtml

Geralds, John. "Distributed firewalls – protecting from the inside" 25 July 2000.
URL: http://www.vnunet.com/Analysis/1107338

Mark, Stuart. "Distributing firewall tasks" 23 April 2001.
URL: http://www.zdnet.co.uk/itweek/brief/2001/16/network/

Radcliff, Deborah. "Firewalls reach out" 26 March 2000.
URL: http://www.computerworld.com/cwi/stories/0,1199,NAV47-81_STO58975,00.html

URL: http://www.distributedfirewalls.com

URL: http://www.infoexpress.com/products/pf/index.html

URL: http://www.network-1.com/products/index.html

URL: http://www.sygate.com/products/sms_ov.htm

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: September 2nd, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced