Ascend

TECHNOLOGY OVERVIEW

ASCEND'S SECURE ACCESS FIREWALL

EXECUTIVE SUMMARY

Dynamic firewall technology is a key feature of Ascend Communications Secure Access Firewall. When the Secure Access Firewall is part of a network's Firewall security, It provides fluid, self-adapting control of network access. Dynamic firewall technology only allows access through the network firewall when you want and only for as long as you want. This makes Secure Access Firewall a powerful part of any protective firewall solution. Dynamic firewall technology examines every packet passing through the network interface. When a packet meets the requirements of Secure Access Firewall rules, it triggers dynamic firewall technology to write new, temporary rules on-the-fly. These rules open, lock and time all aspects of the each session. This ability to adapt to network traffic provides a distinct advantage over ordinary static packet filtering, a widely used technology which can leave networks vulnerable to attack by intruders or hackers.

INTRODUCTION

This paper explains the network security benefits of dynamic firewall technology by comparing its control process to that of static packet filtering. At the heart of each process are rules for screening Internet Protocol (IP) packets like those that pass between a remote site and a network server during a common File Transfer Protocol (FTP) session.

The paper includes background information on FTP as an enhancement to this comparison. A short guide to the step-by-step communications between a remote user and a network FTP server illustrates why network security is vulnerable in an FTP session .

INTERNET PACKETS

All data traversing the Internet is divided into bundles called packets. Each packet conforms to a specific structure which allows the network elements of the Internet to successfully route a packet from its source to its destination. All the information needed for routing and for delivery to the appropriate application at the receiving end is contained in IP headers. These IP headers are added to each packet of data at various stages as it enters the network.

Networking protocols on the Internet generally include four layers: Application, Transport, Network, and Data Link. Examples of what may reside in each layer :

- **Application** — *FTP* provides services which allow a user to copy files from one host to another
- **Transport** — *Transmission Control Protocol (TCP)* divides the application data into appropriately-sized chunks for the network and assigns packet numbers to ensure successful delivery
- **Network** — *Internet Protocol (IP)* moves the packets around the network. (Routers are part of the network layer.)
- **Data Link** — *Network Interface Card (NIC)* hardware that handles the details of the physical network cable interface

ASCEND

Data	Network	Transport	Application	
Ethernet	IP	TCP	Application	User Data
Header	Header	Header	Header	

Figure 1 Headers are added at each level of the protocols until the packet contains all the above components.

Packet Security

In simple terms, each packet's user data and headers indicate what the user wants and where the packet should go. Packets can travel across network boundaries, from an internal host to an external host or vice versa. The hosts are the packet's source and destination machines. Security policies must consider this back and forth movement between internal and external machines to provide adequate protection of proprietary information on internal networks. Fewer constraints are typically put on internal to external traffic so as not to impede Internet access of internal users.

Dynamic firewall

Dynamic firewall rules provide one of the best ways to control inbound and outbound packets. These rules operate outside the network protocols and are transparent to the user. Generally, the rules are stored in routers because routers pass packets from LAN to LAN or between a LAN and an external network.

The dynamic firewall rules implement the System Administrator's policies for network traffic. The policies develop from one of these extremes:

A. That which is not expressly prohibited is permitted.

B. That which is not expressly permitted is prohibited.

Obviously, premise B is less permissive than premise A. It is more secure to block packets than to pass them if they don't match a rule. Approach A requires constant attention. It requires advance planning to add rules when new services are added to the network if filtering is to successfully recognize every packet that should be blocked.

FTP

Many companies recognize the commercial and partnering opportunities inherent in maintaining an FTP server. Recently users have become increasingly concerned about the wisdom of allowing inbound FTP sessions on their networks.

Routers, through packet filtering rules, usually control external access of a network's FTP server. They do this by blocking many of the server's ports. A port is a numbered access point for data to enter and exit, not a physical connection like those for ethernet or telephone cables. Each side of an FTP connection must know the other's port number to successfully send and receive data or commands. Ports below number 1024 are generally reserved or, in the case of a network server, provide access to non-public applications and services. Each side of an FTP connection has over 65,000 TCP ports available.

During an FTP session, a router's packet filter can be a security risk because FTP requires two connections. Commands which control the FTP session are transmitted over Connection A and data is transferred over Connection B. By convention, the control, or command, session uses the server's Port Number 21. The router's filtering rules allow access to that established port number. Creating the data connection opens the security risk. At the TCP level, the machines negotiate the port numbers which will be used for the data session. At the end of these negotiations the ports are activated by the machines, but the router does not know the server's data session port number because it was not part of the negotiations.

Here is the security risk: The router does know which of the server's thousands of ports will be chosen for the data connection. Therefore, it cannot block port numbers above 1024. This provides ample choices for negotiations between the remote machine and the server for the second data connection. However, these ports remain open to probing attacks from unauthorized sources.

Static Packet Filtering

Whether the basic premise of one's security policy is to permit or prohibit access, packet filtering rules are invariably static rather than dynamic. That is, they are established before, rather than during, their execution.

The following example illustrates static packet filtering in an FTP session. The example shows that static packet filtering may create gaps in security even if the policy is based on prohibition.

FTP under Static Filtering

The static packet filtering rules shown below control the FTP command and data sessions on a server at IP address 137.175.2.7. The command session is the connection through which an external client machine and the server communicate. In this example the client is at IP Address 192.9.200.1. The data session between these two machines is established as a separate connection. The number of the server's port for this data session falls within the 1024 to 65535 range.

A. recv/syn/dstport=ftp/dstaddr=137.175.2.7

Rule A allows the router to pass the first packet of an inbound FTP request to the FTP server at 137.175.2.7. The ìsynî flag appears in the header of the inbound packet to indicate it is the first packet in the request.

B. !recv/syn/dstport=ftp

The exclamation point, or ìbangî, at the beginning of this rule tells the router to discard any packet meeting the requirements of this rule. The rest of the rule is similar to rule A. This rule prevents FTP requests from reaching the established FTP port of any other server on the network.

C. syn/dstport=1024-65535

This rule allows an FTP data session to be established on any port between 1024 and 65535 on the FTP server. Hopefully, the only inbound packet which will enter at these ports is the first one from a data session which is related to the inbound FTP request allowed by rule A.

D. tcp/estab

Rule D allows passage of packets for established TCP sessions. These could include FTP commands and data sessions meeting the requirements of rules A and C.

Consider the consequences of these static packet filtering rules. Rule C opens at least two loopholes which could be exploited to circumvent network security policy. First, anyone probing these ports could send a packet for an FTP data session to these ports since the router has no means of determining if the IP address in the packet's header matches the IP address in the header of an approved FTP command session. Second, the router has no means of identifying which port in that wide range has been chosen by the server's TCP to be its data session port. Theoretically, the router cannot block the thousands of ports between 1024 to 65535, which could allow any port to accept a packet with the syn flag header.

Rule D is even more dangerous, though it is necessary within the scope of these static packet filtering rules. **It will allow any machine, anywhere, to send non-syn TCP packets to any port on any internal machine.**

Logical Operations of Static Filtering Rules

The rules shown above can have one of four results:

1. If the packet *matches* the requirement of the current filter rule, go to the next step.
2. If the packet *does not match* the requirements of the current filter rule, skip to a later point in the filter rules.
3. Allow the packet to pass and stop processing it.
4. Discard the packet

Dynamic Firewall Technology

Dynamic firewall technology is superior to any other type of packet filtering because it adapts rules based on information in the packets that pass through the router. It monitors packets and their headers, looks for triggers, then edits prepared templates that temporarily allow network accessibility. Static packet filtering affects a packet in one of four ways. Dynamic firewall technology provides a fifth alternative for packet processing.

The Fifth Rule:

Recognize information in the packet data as a special trigger. Use the trigger to generate a new set of filtering rules to be inserted into the filtering process for some period of time.

FTP under Dynamic Firewall Technology

The ability of dynamic firewall technology to recognize and interpret a trigger, and to use the discovered information to generate new code with specific controls, profoundly affects the handling of an FTP server's ports.

A request for an inbound FTP session is a trigger for the dynamic firewall. As the router monitors the packet header information and the datagram, it recognizes the trigger and a rule template is edited to add new filtering rules. These rules incorporate the source and destination addresses and FTP ports. In the following example the client machine sends its request for an FTP session from port 1300 . When the request has been accepted, the client's TCP chooses port 1400 for the client's data connection. For the server's side of the data connection, its TCP chooses port 2000.

The first rule of the template is the same as Rule A in the illustration of static packet filtering rules shown above.

1. **recv/syn/dstport=ftp/dstaddr=137.175.2.7**

When the server receives an FTP syn packet from port 1300 on 192.9.200.1, new rules shown below are generated by the dynamic firewall technology process.

2. **recv/tcp/estab/srcport/srcaddr/dstport/dstaddr/ftpport**

Rule 2 detects FTP PORT commands sent to the FTP server. FTP PORT commands tell the server what the client's data port number will be.

3. **send/tcp/estab/srcport/srcaddr/dstport/dstaddr/ftp227**

Rule 3 is needed to detect FTP227[1] commands sent by the FTP server. Recognizing FTP227 responses allows the router to see the number of the port the server will use for a data connection and to copy the number of this negotiated port into a dynamic firewall rule.

4a. **recv/tcp/estab/srcport=1300/srcaddr=192.9.200.1/dstport=ftp/dstaddr=137.175.2.7**

4b. **send/ tcp/estab/srcport=1300/srcaddr=192.9.200.1/srcport=ftp/srcaddr=137.175.2.7**

Rules 4a and 4b cause the router to pass all "non-syn" packets for an FTP command session. FTP session packets are tracked by the client's and server's ports and IP addresses. These have been incorporated into the rules.

Now the router's filtering rules allow an FTP command session to take place. The ports and addresses included in the modified template rules are now flags for the router. They give the router the means to identify all the subsequent packets sent between the client and server in FTP command and data sessions.

Dynamic firewall technology adds another temporary rule when the router sees an outgoing FTP packet that matches Rule 3 and contains an FTP227 response. At this point the dynamic firewall does some very important editing. Rule 5 now includes information that the server is waiting for an incoming connection on the destination port 2000.

5. recv/tcp/syn/srcaddr=192.9.200.1/dstport=2000/dstaddr=137.175.2.7

This rule allows an incoming FTP data connection requested by the FTP227 response that was detected by Rule 3. It includes the specific data port number of the server and limits access to that port.

The following temporary rules are added if the router's dynamic firewall technology detects an incoming TCP SYN packet from client port 1400 that matches Rule 5. This incoming packet from the client's machine includes a request for one of its ports to be activated for a data session.

6a recv/tcp/estab/srcport=1400/srcaddr=192.9.200.1/dstport=2000/dstaddr=137.175.2.7

6b send/tcp/estab/dstport=1400/dstaddr=192.9.200.1/srcport=2000/srcaddr=137.175.2.7

Rule 6 passes all packets for an established FTP data session except the first SYN packet. This allows all other identified FTP data packets from the session to pass. The first SYN packet was passed by Rule 5.

Rules 5 and 6 cause the router to open the single server port for an FTP data session. This is the advantage that dynamic firewall technology has over static packet filtering, which needs to keep thousands of ports available for the same session to take place.

Summary

Dynamic firewall technology:

- transforms the router's network security role
- refines the inflexible, coarse security net provided by static filtering
- enhances timing's role in security policy

When it is incorporated within the router the dynamic firewall transforms that component of the IP connection. A router with dynamic firewall technology doesn't simply dispatch packets. It manages traffic following precise guidelines defined by packet header information.

Dynamic firewall technology's adaptable intelligence provides tighter control of inbound and outbound connections because it uses particular IP addresses and port numbers to create new security instructions as needed.

The new rules also include a mechanism for timing connections. When connection traffic ends the dynamic firewall closes network access.

A Graphic Illustration

Figures 2 and 3 use graphic images to compare the filtering security offered by dynamic firewall versus static filtering.

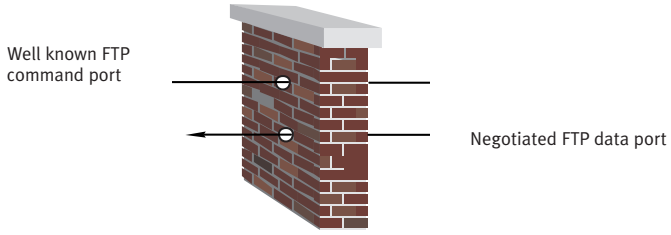

Figure 2 **In dynamic firewall technology, FTP's well -known port 21 is opened and a data session has been requested to download files through a particular port on the client. This triggers a rule change in the packet filtering to allow packets that are recognizably part of the data transfer to pass until an end of the session flag is detected by the filter.**

Figure 3 illustrates the security risk described in the example of static packet filtering rules.

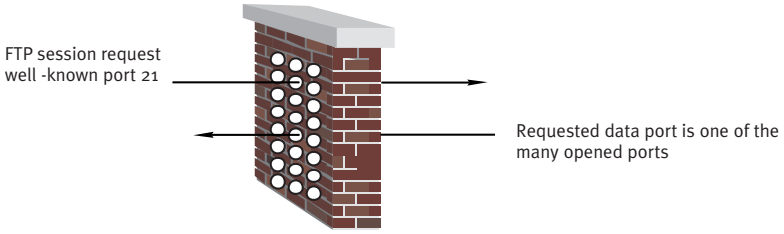

Figure 3 **In static filtering, FTP well-known port 21 is open to transmit FTP commands and many other ports are open in anticipation of a session that will transfer chosen files from the server host to the client host. The server opens various ports to accommodate the request, because no specific port has been negotiated.**

[1] *FTP227 is sent by the server in response to FTP PASV commands sent by the FTP client machine. The client's FTP PASV command tells the server to activate a port the client's TCP has chosen for the client's command or data connection. The port number will accompany the FTP PASV command.*

ASCEND

Ascend Communications, Inc.
1275 Harbor Bay Parkway
Alameda, CA 94502, USA
TEL: 510.769.6001
FAX: 510.814.2300

E-mail: info@ascend.com
Toll Free: 800.621.9578
FAX Server: 415.688.4343
Internet Home Page:
http://www.ascend.com