Net Admin Weekly
52,000 Subscribers Worldwide
December 4, 2002
Issue #19

Feature

Q & A

Security Advisories

News Headlines & Resources

Download of the Week

Feature

The Story of "This a Stateful Firewall" Part 1: Transport and Network Layer Protocols

to top

We've all had the joy of calling up tech support to get information that the vendor of a troublesome program forgot to include in the help file. If you happen to be the firewall administrator for your organization, then you might have this problem more often than most. If you can fight back the tears of frustration, such calls are often good for a laugh.

A buddy of mine, Jerry, shared with me such an experience he had last week. Jerry was trying to configure his firewall to work with a well-computer-to-PSTN gateway application, and he needed to know the protocol details used by the application. The help desk told him "you need to open ports 123, 456, 789, 321, 654, 987" (I've changed the port number to protect the guilty). My buddy said, "What are you talking about? I'm configuring a firewall, not a packet filtering router". The tech support guy was apparently offended and told my buddy that "these *are* the ports you open on the firewall". Jerry told the tech support guy he was FOS and that the call needed to be passed upwards. They hung up on each other.

The company called Jerry back. This time the company's "firewall guru" called and said the problem was with my friend's firewall. He is using ISA Server 2000 and the "firewall guru" told him that "ISA Server 2000 is not a stateful firewall and therefore our software won't work with it". Unfortunately, my buddy didn't really understand what stateful meant, so he accepted this trash talk from this clueless "expert".

After Jerry told me about what happened, I realized the term "state" is bandied about like some sort of political fact. Everyone uses the word, but no one seems to know what they're talking about (or they're all talking about different things). If some company's "firewall guru" called you can said that your firewall won't work because it's not a "stateful firewall", would you just lay down and accept it? Or would you pin the guy to the mat and make him prove to you that he's a moron?

What is State?

What is state and how does a firewall determine the state of a communication between a source and destination host? State can be loosely defined as the "condition or status of a connection between two communicating hosts". States might be defined as beginning, middle, and end, or beginning and end, or sent and received, or none of the above (as seen with "stateless" protocols). The first rule about communication states is that they vary with the protocols used.

Regardless of the protocol and how it manages its state of communication, a firewall needs to keep track of the communication status between a source and destination host. This information is stored in what is called a "state table". Various types of information is stored in a state table and the information varies with the protocol used by the

communicating hosts. Examples of information kept in a state table include:

- Source and destination IP address
- Source and destination port
- Protocol, flags, sequence and acknowledge numbers
- ICMP Code and Type numbers
- Secondary connection information communicated in application layer headers
- Application layer specific command sequences (GET, PUT, OPTIONS, etc.)

For example, one of the main jobs a firewall performs is to block all unsolicited inbound connections while allowing responses from servers that internal network clients have made outbound connections to. The firewall can block the unsolicited inbound connections while allowing the servers to respond by keeping track of the outbound connections in its state table.

For example, when the internal network client makes an outbound connection, the firewall might enter the source and destination IP address and port number in the state table (it might also enter flag, sequence number, and ack number information too). When the firewall receives the server's response, it checks the state table to see if anyone made an outbound request to that server. If so, and if the flags, sequence, and acknowledge numbers are appropriate (for TCP communications), then the firewall passes the response to the internal network client that made the outbound request.

Transmission Control Protocol (TCP) States

A firewall assesses connection state differently depending on which protocol it's managing or tracking. The Transmission Control Protocol (TCP) is a connection-oriented, session-based protocol that is truly stateful. TCP has true start and finish states, as well as a number of intermediate states. A firewall can draw a fine bead on the status of a TCP connection because of the granularity of state information provided by TCP.

In fact, RFC 793 provides for 11 TCP states which can be loosely grouped into the "connection establishment states" and the "connection close states".

The connection establishment states are:

CLOSED
State of a non-existent connection; the state of a connection after it's been closed.

LISTEN
State of a host when waiting for a connection. For example, a Web

server listens on TCP 80 while waiting for a connection.

SYN_SENT
The state of a connection after a source host has sent a SYN to a destination host and is waiting for a SYN-ACK packet from the destination host.

SYN_RCVD
The state of a connection after a destination host receives a SYN packet from the source host and the destination host has sent back an ACK packet.

ESTABLISHED
State that exists after the appropriate ACK packet is received by the source host and SYN_ACK is received by the destination host.

The connection close states are:

FIN_WAIT_1
State of a connection on the source host sending a FIN packet requesting a graceful close.

CLOSE_WAIT
State of a connection on the destination host receiving the FIN packet and after the destination host sends an ACK to the FIN.

FIN_WAIT_2
State of a connection on the source host receiving the ACK from the destination host that received the FIN; the source host remains in this state until it receives a FIN from the destination host.

LAST_ACK
State of the connection on the destination host after sending its FIN packet. At this point both source and destination hosts have sent FIN packets requesting a graceful close of the connection.

TIME_WAIT
State of the connection on the source host after it sends its ACK to the final FIN sent by the destination host. The TIME_WAIT state continues until a predefined timeout, after which the connection is CLOSED on the source host and LISTENING on the destination host.

CLOSING
State of both hosts in the event that both hosts send a simultaneous FIN and ACK.

This information, combined with TCP sequence and acknowledgement numbers, provides a very precise picture of the state of a TCP session, and the firewall can place all of this information into its state table to determine which communications are legitimate and illegitimate.

State tables remove entries regarding each connection after a predefined timeout interval, although to reduce resource expenditure, entries can

stay for a long time (several minutes to several hours). For example, although the TCP connections can be terminated gracefully using a FIN packets, communications are often abruptly disconnected. Firewalls can keep information in the state table so that clients and server can potentially reused resources already allocated.

UDP "States"

While TCP does a great job of providing information about the state of a current connection, other protocols such as UDP and ICMP are connectionless, sessionless, and for all intents and purposes, are "stateless". UDP and ICMP connections do not negotiate session parameters between and source and destination host, and there are no flags, sequence, or acknowledgement numbers for the firewall to keep track of.

Firewalls have to use some method to track these "stateless" communications and give some semblance of connection state so that they can enter useful information into state tables for connection management. A firewall can enter the source and destination IP address and port numbers of the source and destination hosts. But that's about all the useful information the firewall can get from the UDP header. The firewall can add timers to the entries in the state table and time out entries as needed.

For example, DNS queries use the UDP protocol. When an internal network client sends a DNS query to a DNS server on the external network, the firewall puts the source and destination IP addresses and port numbers into its state table. UDP doesn't include information about whether the connection was successful, or whether it's opening or closing. The only thing that will happen is the DNS server will or will not respond to the query. Since the firewall doesn't know if the DNS client and server will ever communicate again, the firewall keeps the information about this connection in its state table of a short time and then removes it.

If the firewall removes the entry from the state table too soon, the same client may send another request to the same DNS server very soon after the entry is removed; in this case the firewall will have to use system resources to create a new state table entry for virtually the same connection. However, if the firewall leaves the UDP connection entry in the state table too long, system resources are wasted on keeping information that's not required, and also can potentially provide a portal of attack if someone were to obtain that information.

Another problem you can run into with stateless protocols like UDP is that some firewalls have built-in intrusion detection systems (IDSs) that will fire off an alert if the entry is removed from the state table before the destination server has time to respond. These "false alerts" often play havoc with a firewall administrator's sense of well-being.

ICMP "States"

The Internet Control Message Protocol (ICMP) shares UDP's "stateless" nature. You don't have sequence numbers, acknowledgement numbers and flags indicating connection state. But at least UDP has source and destination port numbers! That's right, ICMP is a network layer protocol, does not use source and destination port numbers, and doesn't create "sockets" like the transport protocols.

ICMP is different in many ways from the transport protocols. First, it's not a transport protocol at all – it's a network layer protocol. ICMP is also a "one-way" protocol that's used primarily to share status and error information between hosts. For example, UDP doesn't have any built-in method for a destination host to inform a downstream router that it's being flooded with queries. ICMP can be used to send an "ICMP source quench" message to the downstream router to stop the flood of packets. In this way, ICMP supports connection control for brain-dead transport protocols like UDP.

ICMP is often used as a "request-response" protocol. Yes, TCP and UDP have aspects of this "request-response" nature, but ICMP is different because the request and response messages are determined by ICMP message types and codes. The most common example is the ICMP Echo Request and the ICMP Echo Replay messages. Both messages are ICMP Code 0 (zero) by the Echo Request message is type 8, while the Echo Replay message is type 0 (zero).

The firewall can use type and code information, along with source and destination IP address and enter this information into its state table. In this way the firewall can allow incoming ICMP Code 0 Type 0 messages from an external host in response to an internal client sending an outbound ICMP Code 0 Type 8 message.

Summary

In this article we covered what communication state is, how it works differently with different protocols, and how firewalls can use state information to control inbound and outbound access. You saw that TCP is a truly stateful protocol that provides a lot of information about current connection status. UDP and ICMP are essentially "stateless" protocols. Firewalls can still use information provided by these stateless protocols and place it in a state table to help control access through firewall.

Next week we'll wrap up our conversation on stateful firewalls with a discussion on how firewalls leverage application layer state and the challenges made on firewalls because of the vagaries imposed by some application layer protocols. Until then, don't let those "firewall gurus" tell you that your firewall isn't "stateful" until they can prove it!

This week's feature article by

Thomas W Shinder M.D., etc.
Net Admin Weekly Author

Q & A

Question: Remote Control Options

to top

Question:

Hi Dr. Tom,
Can an administrator or anyone bring up the desktop of a Windows 2000 Professional Machine from another Windows 2000 Professional Machine? I believe I saw this before, but I am not sure. If you have any information, I would appreciate it greatly. –Remote Admin

Answer:

Hey admin, you have a lot of options when it comes to remote management of Windows 2000 Pro machines. While Windows 2000 Pro doesn't have a built-in Terminal Server like Windows XP's Remote Desktop, you can use other applications to make it possible. VNC is a free remote control application that is compatible with Windows 2000 Pro. The nice thing about VNC is that you can remote control the Windows 2000 machine from non-Windows machines. Of course, pcAnywhere is the grand-daddy of remote control applications and it's also compatible with Windows 2000 Pro. One remote control application that doesn't get enough respect is NetMeeting. One of the nice things about NetMeeting is that is comes with Windows 2000 Pro and you can control many of its properties via Windows 2000 Group Policy. The primary disadvantage I see with NetMeeting is that it can be a bit heavy handed in terms of resource use.

Windows 2000 Active Directory NetBIOS Domain Names

to top

Question:

Dear Dr. Tom,
This isn't a quiz! I was just wondering: How would a 9x client log into a domain called child.somedomain.com? If the domain name was somedomain.com then the client would be OK and could log on to the NETBIOS-named SOMEDOMAIN domain. There's also the issue of a 15 character limitation for NETBIOS names. Any pointers appreciated! Bye for now, - Tharg

Answer:

Yo Tharg! Think about what happens when you create a new domain using the DCPROMO tool. You have to create a NetBIOS name for the domain. This is the name that downlevel clients can use to log into the Windows 2000 domain. Keep in mind that 9x clients are NetBIOS dependent. That means you need a supporting NetBIOS name resolution infrastructure to help those downlevel clients out. The best thing you can do is roll out a WINS server. The Windows 2000 domain controller will register its NetBIOS domain name with the WINS server and the 9x clients can query the WINS server for the name and IP address of the

DC.

Security Advisories

Buffer Overrun in Microsoft Data Access Components Could Lead to Code Execution

to top

A security vulnerability resulting from an unchecked buffer in the MDAC Data Stub affects versions of MDAC prior to version 2.7 (the version that shipped with Windows XP). By sending a specially malformed HTTP request to the Data Stub, an attacker could cause data of his or her choice to overrun onto the heap. Microsoft has confirmed that it would possible to exploit the vulnerability to run code of the attacker's choice on the user's system. Web clients and servers are both affected by the problem. Microsoft considers this a critical vulnerability and it should be patched ASAP.

Read more...

Hardening Linux Systems

to top

I read a lot about how to harden Windows systems, but what about Linux? It's often thought that Linux is an impenetrable barrier right out of the box. While that sounds nice, it not true. This article covers key concepts and procedures that will allow you to lock down that Linux system air tight.

Read more...

Hacking the Xserve

to top

If you follow the IIS and Apache security alerts, you have to wonder if there's much of a difference. OK, Apache has fewer problems right now, but when IIS 6.0 hits the streets, will the playing field be leveled? Do you have the time to find out? Maybe you should check on OS X's Xserve. How often do you hear about Xserve being hacked? Check out this article for details if you're looking for something different.

Read more...

News Headlines and Resources

Private VLANS

to top

You've probably worked with VLANs. These "virtual" LANS allow you to segment Ethernet broadcast traffic. But what if you want to further segment that Ethernet traffic, perhaps even to the host-to-host level? Then you might want to implement a Private VLAN (PVLAN). In this article, Lloyd Lancaster does a great job of introducing you to the concept.

Read more...

Windows 2000 CHKDSK Management

to top

We've used the chkdsk command since Windows NT 3.1. This venerable

command keeps our disks clean and, if run regularly, can avert potential disasters. But there is lot more going on with chkdsk than meets the eye. Check out this white paper on chkdsk, and become the local chkdsk guru.

Read more...

File Services Community Center

to top

Need information about the Windows 2000 File system? The Windows NT 4.0 File system? Server Consolidation? File and Print services? Then the place to check out first is the Microsoft File Services Community Center. You'll find plenty of white papers and FAQs about Windows 2000 and other Windows-based servers file services.

Read more...

Security Operations Guide for Windows 2000 Server

to top

Are you looking for best practices for securing Windows 2000 Servers? Need to know the best way to lock down a Windows 2000 server and minimize vulnerabilities? Then check out the Windows 2000 Security Operations guide. It's a great place to start when putting together a secure Windows 2000 infrastructure. Symantec also has put out a companion guide that builds on the information in the Microsoft guide. These are "must reads" for all Windows admins.

Win2K Security Operations Guide

Symantec Companion Guide

Windows .NET 2003 Server Feature Highlights Sorter

to top

The first thing we need to know before even considering a Win2003 upgrade is what features does Win2003 have that Windows 2000 doesn't? If you're going to have to deal with egregious Win2003 licensing issues, then you better get a big bang for your buck! Head on over to this site and check out the array of new features.

Read more...

Profile of Internet Stalkers

to top

They *are* out to get you. But who are "they"? Law enforcement officers regularly use profiles to determine who most likely is going to gun you down given half a chance. You can take advantage of this same method to learn who wants to lay waste to your network! This short article briefly covers the concepts of network criminal profiling. For a full-blown discussion on network and Internet criminal profiles, check out Deb Shinder's "Scene of the Cybercrime".

Profile of Internet Stalkers:

Scene of the Cybercrime:

TechNet Webcast: Protecting Exchange and IIS Deployments with Internet Security and Acceleration (ISA) Server 2000, featuring

to top

Symantec AntiVirus for ISA Server

ISA Server is quickly becoming the standard firewall and Web Proxy solution for Microsoft shops. This TechNet Webcast will cover new feature enhancements for ISA Server to further integrate ISA Server seamlessly with Exchange and IIS. They'll also cover Symantec's new Antivirus for ISA Server. This promises to be a great talk and one you won't want to miss.

Read more...

Download of the Week

to top

Ability Server

Are you tired of IIS-related hacks and security alerts? Tired of installing hotfixes that close one security hole and end up breaking something else? Need a Web, FTP, POP3, and SMTP server that doesn't look like candy to every click kiddie on the Internet? Then you should consider Ability Server from code-crafters. This is one cool piece of software. You get all these features and the entire code is only a 64K download! You can use the freeware version that has some limitations, or you can get the full version and pay what you think it's worth! If you heed a Web and mail server, then check this out.

Read more...

Free Cramsession IT Newsletters - Choose Your Topics!

H = HTML Format **T** = Text Format

H	T		H	T		H	T	
☐	☐	A+ Weekly	•	☐	Exam Tips 'N Tricks	☐	•	.NET Insider
☐	•	ByteBack!	☐	•	IT Career Tips	•	☐	Script Shots
☐	☐	Cisco Insider	•	☐	Linux News	☐	☐	Security Insider
☐	☐	Developers Digest	☐	•	Must Know News	•	☐	Trainers News

Enter your Email

Subscribe Now!

CramSession
Prepare for Success!

Your subscribed e-mail address is:steven.thode@toadworld.net
To unsubscribe, simply **click here** and hit "send" in your e-mail reader.