Net Admin Weekly
52,000 Subscribers Worldwide
December 11, 2002
Issue #20

Feature

The Story of "This is a Stateful Firewall" Part 2: Application Layer State — Read it

Q & A

Saving Sent Items to an IMAP Server — Read it
Allow Inbound NetBIOS Access? — Read it

Security Advisories

E-mail Header Processing Flaw — Read it
Cumulative Patch for Internet Explorer — Read it
Honeypots - Definitions and Value of Honeypots — Read it

News Headlines & Resources

'Tis the Season for High Tech Toys — Read it
Product Documentation for Windows .NET Server 2003 — Read it
Microsoft Sees Threat from Linux Desktop — Read it
The Complete IP Addressing and Subnetting Web Site — Read it
Windows .NET Server RC1 Administration Tools Pack — Read it
Sign Up for Windows .NET Server 2003 Release Candidate 2 — Read it
Support WebCast - Windows .NET Server 2003 DNS — Read it

Download of the Week

Holiday Lights — Read it

Feature

The Story of "This a Stateful Firewall" Part 2: Application Layer State

to top

Last week we began our discussion on stateful firewalls by going over network and transport layer protocols and how the concept of communication "state" relates to them. In that article, you saw that TCP communications are truly stateful since each aspect of a TCP link has a specific connection state associated with it. On the other hand, you saw that UDP protocols do not have the flags, sequence numbers, and acknowledgement numbers that a firewall might use to track connection states; the same is true for network layer protocols like ICMP.

Firewalls can impose a "pseudo" statefulness to UDP protocols by tracking source and destination IP addresses and port numbers and enforcing time-out values to UDP connection information entries in the firewall's state table. ICMP connection state can be tracked by taking advantage of the fact that ICMP is most often used as a "request/response" protocol. The firewall can use ICMP type and code information in the state table, as well as source and destination IP address, to track ICMP state.

Tracking network layer (OSI layer 4) communications is easy compared to the task of tracking application layer state. Advanced firewalls can track the state of application layer communications between a source and destination host. However, application layer protocols force much greater demands on the stateful firewall because the firewall must be made "protocol aware".

This protocol awareness can take several forms. A lower level of protocol awareness pertains to the firewall's ability to open and close ports dynamically based on the how the particular application layer protocol works. For example, application layer protocols such as FTP and the H.323 suite require multiple connections for a single application layer session. These connections may be multiple outbound connections, or outbound and new inbound connections. The stateful firewall can "listen in" on the commands sent by the application layer protocol and allow these "secondary" connections to pass through the firewall.

A firewall can have an even higher level of protocol awareness when it understands the complete command structure of the particular protocol and makes decisions about packet handling based on its understanding of the application layer command structure. The application layer-aware stateful firewall can track application layer state and reject and allow the communication based on what it knows about the protocol's legitimate command structure.

Let's take a look at a couple of application layer protocols and see how advanced stateful firewalls handle application layer state.

Simple Mail Transfer Protocol

We all use the Simple Mail Transfer Protocol (SMTP). You get this

newsletter courtesy of SMTP. SMTP is a "simple" protocol because it requires a single outbound port number to successfully establish a connection with a destination host. Your stateful firewall only needs to allow outbound access to TCP port 25 and keep track of the network and transport layer state (to allow the destination host to respond).

The SMTP-aware stateful firewall can do a lot more than just examine and track the network and transport layer information for the SMTP communication. All application layer protocols have command sets that allow the protocol to carry out the operations specific to that protocol. SMTP has a number of commands specific to it. For example, some of the commands used by SMTP include:

HELLO (HELO)
Identifies the sender to the receiver; this allows the SMTP server to allow or reject messages from the SMTP client based on the name included in the HELO.

MAIL
Initiates the mail transfer from the SMTP client to SMTP server; it essentially lets the SMTP server know that the SMTP client has mail to deliver.

RECIPIENT (RCPT)
Identifies the recipient of a mail message.

DATA
The server treats lines after this command as mail data; this includes the text of the messages as well as attachments.

SEND
Used to initiate a mail transfer where the mail is delivered to one or more terminals (servers).

RESET (RSET)
Specifies that the SMTP transfer should be aborted; similar to a TCP reset message. Can be used for quality control if the integrity of the transfer is detected as corrupted.

VERIFY (VRFY)
Typically used to confirm a user exists or is legitimate for an SMTP server; the command is often disabled for security reasons.

EXPAND (EXPN)
Command is used to confirm that the receiver is a mailing list.

NOOP
Indicates to the server that an OK response is requested; can be used for SMTP server probes.

TURN/ETRN
Used to set status of server; an SMTP server can act as an SMTP client under certain circumstances depending on the results of the TURN and ETRN command; this allows "sometimes connected" SMTP clients (like an

Exchange Server) to request mail delivery from an SMTP server.

The SMTP application protocol-aware Firewall can watch for all of these commands. The firewall can reject SMTP messages if a particular command is detected. It can reject messages if a particular command is "larger" than what is expected; this situation can indicate a buffer overflow attack is being perpetrated against the SMTP server.

In addition to application layer protocol command set awareness, advanced stateful firewalls can analyze the application layer data. An application layer aware firewall with advanced SMTP knowledge can look at the subject and body of an SMTP message, the source and destination email address, and even email attachments to make allow or deny decisions.

For example, Microsoft's advanced stateful firewall, ISA Server 2000, is able to block email based on keywords, source/destination address or mail domain, and attachment extension/name/size. ISA Server can also reject SMTP messages that contain certain SMTP command sequences or where the commands are larger than expected. ISA Server 2000 can do this because it has advanced knowledge of the SMTP protocol and can track these elements of an SMTP message's "state".

File Transfer Protocol (FTP)

The File Transfer Protocol (FTP) is considered a "complex" protocol because the FTP client needs to initiate more than just a single outbound connection in order to connect to an FTP server *and* receive data from that server. The FTP protocol uses two types of connections: a primary outbound connection to initiate communications with the FTP server and then secondary connections which are part of the same application layer transaction or session.

PORT (or Active or Standard) mode FTP requires secondary inbound connections. The FTP client sends an outbound request to the FTP server's TCP port 21 to establish the "control" connection. The FTP client and server exchange application layer protocol commands over this command channel. One of these commands informs the FTP server to send data back to a specific port on the FTP client. The FTP server then establishes a *new* inbound connection to send data back to the FTP client via an FTP data channel (using the FTP servers source port TCP 20).

The firewall needs to be aware of how the FTP application protocol works in order to allow the new inbound connection attempt from the FTP server. Since there is no SYN_ACK flag on the packet (only a SYN flag) on the packet, the firewall should detect that this is a new, unsolicited, inbound request. However, an FTP-aware stateful firewall is able to deconstruct the application layer command information and detect that the FTP server needs to send data using new inbound connection (which only contains the SYN flag). The firewall will open the inbound port and allow the data through.

Note that both the initial outbound connection from the FTP client and all subsequent inbound data connections from the FTP server are part of the same FTP session. The stateful firewall that is FTP-aware knows that the primary outbound connection and the subsequent secondary inbound connections are part of the same FTP session, and opens and closes the appropriate ports to allow the communication. The stateful firewall can do this because it places the FTP application layer protocol information in its state table and makes the appropriate allow and deny decisions based on this information.

The FTP application layer protocol-aware stateful firewall can also examine other FTP commands and FTP application layer data. Depending on the level of application layer protocol and data awareness built into the stateful firewall, allow and deny decisions can be made based on FTP file type, file size, file name, and even virus inspection.

Differences between Stateful Filtering and Inspection

Firewall gurus have a hard time coming to an agreement regarding a unified definition of a "stateful firewall". You may have noticed in this article that there seems to be two distinct levels of inspection. One type of stateful firewall looks at OSI layers 4 and below and makes allow and deny decisions based on that information. The other type of firewall is able to use information from the application layer downwards.

The first type of firewall is often thought of as performing "stateful filtering". The second type of firewall performs "stateful inspection". Regardless of whether the firewall performs stateful inspection or stateful filtering, they are both stateful firewalls. Of course, the firewall that's able to perform stateful inspection for a large array of application layer protocols will be able to protect your network from a larger number of attacks, but it will also be more resource intensive because it needs to subject each communication to a higher degree of scrutiny.

Summary

"I'm sorry sir, our application won't work because you do not have a stateful firewall". What will you do when some faux firewall expert on the other side of the phone tells you this? One thing you're not going to do is suck it up and believe this garbage! Now you understand what statefulness is and how firewalls track protocol state. You know the difference between stateful inspection and stateful filtering. You know what a simple protocol is and you know what a complex protocol is. You know that advanced firewalls can examine application layer data and make decisions based on that data.

There's a lot more to the story. We didn't even begin to touch on where firewalls end and proxies begin, and if there is even a difference between a firewall and proxy these days. We'll cover those topics and how they affect your network in future newsletters. But from this point forward,

you should never accept the clueless Help Desk dude telling you that you "need to open ports X, Y and Z" because you know that applications need inbound or outbound access and connections are either primary or secondary. The phrase "opening a port" is entirely meaningless.

Have fun harassing your application vendors regarding the EXACT protocols used by their network applications. You'll be amazed at how many of them don't even know because the developer(s) left the company! :)

This week's feature article by
Thomas W Shinder M.D., etc.
Net Admin Weekly Author

Q & A

Question: Saving Sent Items to an IMAP Server

to top

Question:

Hi Dr. Tom,
Does anyone know how to save the sent items in Outlook to the server and not locally? We are using a Linux mail server called Kerio and also using IMAP. The whole Inbox is being saved to their server but not the sent items. Any ideas? –Schnootz

Answer:

Hey Schnootz! Good question. Poor old IMAP doesn't get used nearly enough. The big question is what version of Outlook are you using? Microsoft has some very clear information on how to save sent items on an IMAP server using Outlook 98 and 2000, but mum's the word when it comes to Outlook XP (2002). There are two procedures to carry out: create a rule that saves the sent item to a specific folder on the IMAP server, and then disable the save sent items in the Sent Items folder on the local Outlook .pst file. You can find the procedures in Microsoft KB articles Q198854 and Q198852.

KB Q198854
KB Q198852

Allow Inbound NetBIOS Access?

to top

Question:

Dear Dr. Tom,
I have a computer performing network address translation on a network. I have set up port mappings so that port 80 on the gateway maps to 80 on a machine behind the gateway. Is it possible to set up a special port mapping so that I can connect to a machine behind the gateway using a UNC path (i.e., so \\gateway\sharname would actually make you connect to \\machine_behind_gatweay\sharename ? Can this be done by mapping the NetBIOS session port (137)? –Hacker Bait

Answer:

You're darned right about that, Mr. Hacker Bait. Why in the world would you want to open NetBIOS ports through your "firewall" (NAT Server) into the internal network? Do you wear t-shirts that say "kick me" on the back? Do you stand in the corner with a "dunce cap" (you might not remember dunce caps – they were used to hurt dumb kids self-esteem). NetBIOS requires access to TCP 137 for name resolution, TCP 138 for NetBIOS datagram service (used for things like browsing) and TCP 139 for data transfer. Whiles you're at it, make sure you allow inbound TCP 445 (Direct Access) and TCP 135 (RPC endpoint mapper). After you get things set up, let me know what you public IP address is so that I can let all our readers test your security. :-) A better solution is to create a Web site or FTP site that maps to your NetBIOS share. Configure the appropriate permissions to secure the directory and your IIS Server. You'll have a more secure solution and you'll be able to upload and download files if you need to. For details on IIS security measures, **click here**.

Security Advisories

E-mail Header Processing Flaw Could Cause Outlook 2002 to Fail

to top

There's a vulnerability in Outlook 2002 relating to how it processes e-mail header information. An attacker who exploits the vulnerability could send a malformed e-mail to a user of Outlook 2002 that would cause Outlook to fail. The Outlook 2002 client would continue to fail as long as the malformed e-mail message remained on the e-mail server. The e-mail message has to be deleted by the e-mail server administrator at the server, or by the user via another e-mail client such as Outlook Web Access or Outlook Express. This bug isn't a problem if you connect to Exchange via MAPI.

Read more...

Cumulative Patch for Internet Explorer

to top

Has it been a month already? Yep, it's time to update your Internet Explorer patches. The cumulative patch brings you up to date as of December 4, 2002. Both Internet Explorer 5.5 and 6.0 fixes are included in this offering.

Read more...

Definitions and Value of Honeypots

to top

Do you know what a Honeypot is? Do you use a Honeypot for security or research? Honeypots are a great way to catch those cruising losers who spend their time trying to break into your network. Honeypots can also be used to collect valuable forensic data you can use to put the script kiddie into a jail cell where he will become Bruno's new "wife". Check out this article on how you can leverage Honeypots to protect your network.

Read more...

News Headlines and Resources

Tis the Season for High Tech Toys

to top

What better excuse than the year's biggest gift-giving holiday to purchase all of those high tech toys you've been pining for all year? Vendors save up many of their coolest new hardware offerings for release during this time of the year, tempting us to overspend our budgets and come home with all manner of new computer-related gadgets. Deb Shinder walks you through a holiday toy store of high tech gadgets.

Read more...

Product Documentation for Windows .NET Server 2003 (Win2003)

to top

While Windows .NET 2003 (Win2003) won't see the light of day until next April, you can't start studying too early for your Win2003 exams. What better study material than the Help files? This page includes links to the Win2003 Standard, Enterprise, and Datacenter versions. No Help for those of you who want to use the Win2003 Web version.

Read more...

Microsoft Sees Threat from Linux Desktop

to top

The next few years will be interesting. Microsoft marketing and business guys are acting like Hatters with mercury poisoning as they alienate enterprises with Licensing 6.0, scare off national governments with the threat of "turning off" rented software, hack off consumers with the Windows XP RegWorm, torpedo the success of Windows XP Media Edition with copy protection, and continue work on Palladium, which ultimately will put their stock in the tank. And they wonder why Linux on the desktop could become a real threat? Desktop Linux could cause a new high tech boom, as companies and individuals spend money on low-cost software and hardware to run with their new desktop Linux boxes.

Read more...

Check out how Palladium will crater the Microsoft Government market...

The Complete IP Addressing and Subnetting Web Site

to top

Need to bone up on your IP addressing and subnetting? Then head on over to subnetonline.com. Your first impression is that you've mistakenly gone to a porno site due to the pop-ups. Once you recover from the pop-up offensive, check out the subnet calculators and subnetting guides. There are even wall posters of the OSI model and security exploits.

Read more...

Windows .NET Server RC1 Administration Tools Pack: adminpak.msi for Windows XP Users

to top

If you're running Windows XP, you've probably discovered that your old Windows 2000 admin tools won't work any more. No problem! Download the latest and greatest .NET RC1 admin tools. They work great managing Windows 2000 Servers too.

Read more...

Sign Up for Windows .NET Server 2003 Release Candidate 2 (RC2)

to top

Get hands-on experience with an "almost" final version of Win2003. Release Candidate 2 (RC2) can be yours when you become a Customer Preview Program members. Check out the sign for the details and pick the CD or download option.

Read more...

Support WebCast - Microsoft Windows .NET Server 2003 DNS: Stub Zones and Conditional Forwarding

to top

This session will cover two new features introduced in Windows .NET Server 2003 DNS: stub zones and conditional forwarding. We will discuss the technical details and recommended usage of these new features.

Read more...

Download of the Week

Holiday Lights

to top

Here's an old program we used to run in Windows 3.1. Holiday Lights puts festive holiday light bulbs around the edges of your screen. Break out of your on-call doldrums by giving yourself the gift of light and cheery music. I'm usually an old sour puss about this stuff, but I found the Holiday Lights desktop garnish and screen saver just what the doctor ordered. The free version has a subset of all the lights and works for ten days. Don't be a grinch - pay the lousy twenty bucks so your kids and use it throughout the holidays without reinstalling.

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.