Net Admin Weekly

53,000 Subscribers Worldwide

November 20, 2002
Issue #17

CramSession StudyGuides InfoCenter Discussions SkillDrill Newsletters

CramSession

Feature

IPSec NAT Traversal

to top

The Network Address Translation (NAT) routing protocol allows multiple internal network clients to access the Internet through a NAT server that only has one or a handful of IP addresses. There are actually several types of NAT. The networking purist would maintain that the term NAT only applies when you map an IP address on the external interface of the NAT server to an IP address on the internal network. This type of NAT is more commonly known as "static NAT". All packets to and from a particular IP address on the external interface of the NAT server are associated with a specific host on the internal network.

The type of NAT we normally work with is sometimes called "PNAT" (Port and Network Address Translation). This allows multiple clients on the internal network to use the same IP address on the external interface of the NAT server as their source address when communicating with Internet servers. The NAT server replaces the original source IP address and TCP/UDP port number (which together represent the original "socket" if you're working with a socket-based application) with a valid public IP address and port number on its own external interface. The NAT server keeps track of the changes it made in its "NAT table" so that it can properly return packets to the internal network clients after the NAT server receives responses from the Internet servers.

NAT works because it can change network and transport layer header information. When the NAT server changes the source IP address on a packet, it changes the network layer header information. When the NAT server changes the UDP or TCP source port number, it changes the transport layer header information. There usually aren't any problems with changing this header information because the NAT server keeps track of the original packet configurations in its NAT table.

How IPSec Breaks NAT

You run into problems when you want to use IPSec-based VPN technology to connect a VPN client behind a NAT server to an IPSec VPN server on the Internet. The reason for this is the IPSec protocols are designed to authenticate and/or encrypt information in the packet. When a NAT server tries to change the information in the packet, it will either cause the packet to be considered invalid by an IPSec protocol, or it will be unable to perform the translation because information the NAT protocol needs to access is encrypted.

The two IPSec protocols causing problems for NAT are the Authentication Header protocol (AH) and the Encapsulating Security Payload protocol (ESP). AH is used to authenticate packets, while ESP can authenticate and/or encrypt packets. Both of these protocols can work in transport or tunnel mode. Transport mode is used when you want to create a host-to-host connection. A host-to-host connection creates a tunnel used only by the machines representing the tunnel endpoints. On the other hand, Tunnel mode allows a tunnel client to connect to a tunnel server to access resources on the tunnel server, and the network or networks behind the tunnel server.

AH in Transport Mode authenticates the entire packet from IP header to the end of the application layer data and trailers. AH in Tunnel Mode also authentications all headers from the IP tunnel header to the application layer data and trailers. ESP in Transport Mode authenticates from the ESP header to the ESP trailer and it encrypts the TCP/UDP header and application data, while leaving the IP header and ESP authentication trailer "in the clear" (no authentication or encryption).

What do you think a NAT server would do to AH in either transport or tunnel mode? AH has authenticated the entire packet from IP header to trailers. When the NAT routing protocol tries to change the IP and UDP/TCP header information, the AH protocol will balk, flag the packet as having its integrity violated, and drop it. This is the case with both AH transport and tunnel mode.

Now what do you think would happen with ESP packets? When using ESP in Transport mode, the IP header is in the clear, so the NAT routing protocol can change that without causing any problems. However, TCP/UDP header is encrypted! The translation will fail because the transport layer header is encrypted, and the NAT server that perform PNAT must be able to access and change this information. ESP in Tunnel Mode is possible from the packet header standpoint, but there are other issues related to IKE security negotiations that make IPSec through NAT fall apart.

NAT Traversal to the Rescue

It's clear something has to change if you want to use an IPSec-based protocol through a NAT server. The change proposed by the IETF is to encapsulate IPSec traffic in a UDP header which is not exposed to ESP (we won't even worry about AH because of its proclivity to authenticate the entire packet). UDP encapsulation allows the ESP-protected packet to "traverse" the NAT server.

This type of UDP tunneling allows the source port and IP address to change because the tunnel headers are not affected by ESP. When the UDP packet arrives at the IPSec VPN server, the UDP header is removed and the VPN server can make an assessment regarding whether the packet is a normal IPSec packet or an IPSec NAT Traversal packet. The entire process is referred to as "IPSec NAT Traversal".

IPSec NAT Traversal actually involves a negotiation of the NAT Traversal protocol between the VPN client and server, as described by the following steps:

1. VPN client and server exchange vendor specific ID string (which is an MD5 hash) to confirm that both sides support IPSec NAT Traversal.

2. NAT Discovery takes place and determines which participant is behind the NAT device. This is important because the VPN client behind the NAT device needs to send keep-alive messages every 9 seconds. NAT Discovery messages compare source and destination IP addresses to determine which host is the VPN client behind the NAT.

3. IPSec NAT Traversal will be used between the VPN client and server

after the NAT device is discovered to be in the path. The VPN client and server will use UDP encapsulated transport or tunnel mode ESP.

4. The transport or tunnel mode ESP packets are encapsulated in a UDP packet with a destination port number 500, which is the same port number used for the Internet Key Exchange Protocol (IKE – ISAKMP/Oakley). The VPN server can use the same port number of NAT Traversal packets and non-NAT Traversal packets. The IPSec NAT Traversal-aware VPN server identifies the NAT Traversal packets because the UDP header from the client overwrites the 8 bytes of the IKE initiator cookie field is all zeros.

5. During the active VPN session, the VPN client sends a keep alive packet to the VPN server every 9 seconds. This is important because if the NAT server in front of the VPN client times out the current session and port assignment on the external interface of the NAT server, then when the VPN client starts sending packets again to the VPN server, a new port number is assigned, which breaks the IPSec security associations between the VPN client and server (which are dependent on the source UDP header information). Security associations would break before you want them to if it weren't for the keep alive messages.

While IPSec NAT Traversal does solve most of the major problems with passing IPSec packets through the NAT device, it can't solve all of them. The major problem lies in the fact that poorly designed protocols such as FTP, the H.323 protocol suite, LDAP, and many others embed the actual source IP address in the application layer data.

A NAT device can usually get around this problem by using NAT editors to change the information in the application layer data so that the appropriate public IP address and port numbers are used instead of the actual client. The NAT editor approach can't work with IPSec NAT Traversal because the application layer data is encrypted by ESP while it passes through the NAT device.

Conclusion

NAT is a useful routing protocol that allows us to continue using the venerable IPv4 addressing scheme for hopefully another decade or two. While NAT can easily translate both source IP address and port number, the translation process strikes at the heart of both the AH and ESP protocols. While there's not much hope for AH, the IPSec NAT Traversal Protocol will allow you to use ESP in tunnel mode to connect your VPN clients behind a NAT server to an IPSec VPN server on the Internet. Of course, if you want to make your life easier and almost equally secure, you can use PPTP and take advantage of the NAT editor that comes with the Windows 2000 RRAS to pass PPTP through the NAT and to the PPTP VPN server on the Internet.

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

Q & A

Question: Why WINS?

to top

Question:

Hi Sgt. Deb,

I studied for my Windows 2000 MCSE and I know what a "rogue" DHCP server is and why it's bad to have them on the network (because they might hand out IP addresses to DHCP clients from a range that's different from that assigned to the network). Now I'm hearing the term "rogue Web server". What exactly is that, what's the danger (if any) of having one, and how can I tell if there is one on my network? --Rogue Hunter

Answer:

A "rogue" Web server, like its DHCP counterpart, is one that isn't supposed to be there, i.e. an unauthorized Web server. They come about in different ways. Since Windows desktop operating systems include Web server software (personal web server, peer web services, or IIS, depending on the OS), sometimes users will enable the Web server component, either accidentally when playing with settings, or intentionally with the goal of setting up a Web site hosted on their computers. Also, it's easy for admins to unintentionally install Windows 2000 Server with the Web Services enabled. The biggest problem with these rogue Web servers is the security risk they pose. A Web server, if it isn't properly secured, provides a way for hackers to get into the network, and if you don't know the Web server exists, you're probably not going to take the steps needed to secure it.

There are several ways to determine if a Web server is running. To find out if there's a Web server running on the local machine, you can try to access the loopback URL with a Web browser. The address is http://localhost/. You should get an error message if there's no Web server running. If you see a Web page (including an "under construction" or "coming soon" page), you know the computer is running Web services.

You could also run netstat –na to check if TCP port 80 is listening – this, too, indicates the HTTP service is running. However, the absence of this port listing doesn't guarantee that there's not a Web server; it's possible to set the Web server to listen on a different port. It does indicate there's no Web server running with the default settings. You could also check the Add/Remove Programs applet in Control Panel to see if IIS (or PWS) is installed as a Windows component.

Bottom line: disable or remove the Web server services on all machines that don't need them. You'll make the machine more secure and probably increase performance, as well.

Dazed and Confused over SHTTP and HTTPS

to top

Question:

Dear Sgt. Deb,
In my reading, I run across references to HTTPS (or HTTP/S), which I understand is a security method used with Web browsers for e-commerce and other transactions that need to be secure. But then in other places, I see it abbreviated as SHTTP (or S-HTTP). Which is correct? Or are these even the same thing? --Dazed and Confused

Answer:

Dear Confused,
Join the club – lots of people get confused by this. Although they sound alike, the two are different. HTTP/S is a method of running the HTTP protocol over SSL (Secure Sockets Layer). SSL is a protocol that was created by Netscape to provide secure Web transactions (such as buying something with a credit card). It's supported by most Web browsers, not just Netscape's. It encrypts the network traffic that goes from a client browser to a Web server and uses a different port from regular Web traffic (port 443 instead of port 80).

S-HTTP is Secure HTTP. It was created by Enterprise Integration Technologies and it's an extension to the HTTP protocol. It was designed for the purpose of sending individual messages securely. One big difference is that S -HTTP doesn't require the client to have a public key certificate like HTTP/S does. You won't see S-HTTP as frequently as HTTP/S, and it's not supported by all browsers and Web servers.

Security Advisories

Secure IIS 5 Checklist

to top

It just doesn't seem right to go this many weeks without an IIS security alert. While there aren't any security alerts for IIS this week, that doesn't mean we can let our guard down. Take a breather from installing IIS hotfixes and check out this checklist of procedures for securing IIS 5.

Read more...

New Security Flaws Found in BIND version 4 and 8

to top

You hear a lot of trash talk about the Windows 2000 DNS Server. But when the subject of BIND comes up, you'd think the thing was dropped from Heaven in a state of veritable perfection. Guess not, since some major security holes were recently found in BIND versions 4 and 8. Check out the link for details.

Read more...

FWB Privacy Toolkit v1.5 for MAC Now Available

to top

FWB Privacy Toolkit Volume 1 was released this month. It gives Mac OS 9 and OS X users the ability to encrypt files on their hard disk, folders, and also securely delete files by overwriting the data making it so the data is less likely to be recovered. This is a nice security add-on for the Mac, and a free trial download is available.

Read more...

News Headlines and Resources

MS Win2K Network Security CramSession

▲ to top

Microsoft plans to release its Implementing and Administering Security in a Microsoft Windows 2000 Network exam (70-214) in the early part of next year. You need to hone those security skills if you expect to pass this exam, as it's going to be a tough one! Get a head start on your 70-214 studies with the CramSession study guide for this exam.

Read more...

IntelliMirror Tips and Tricks

▲ to top

Intellimirror was a big thing back when Windows 2000 first saw the light of day. You don't hear so much about it now, but IntelliMirror represents a very powerful collection of technologies. However, they can get a bit tricky to configure. Check out this tips and tricks article by Microsoft to get ahead of the IntelliMirror curve.

Read more...

KNOPPIX 3.1 Linux Released

▲ to top

Aren't all Linii the same? Not when you talk about KNOPPIX! Here's a Debian-based Linux distribution that you can run right off a CD. That's right! NO software has to be installed. It's a great way to demo Linux to the curious without cratering your Windows box. If you've been thinking about migrating to Linux, but not sure if the user experience is acceptable, then you MUST give this a try!

Read more...

Limiting a User's Concurrent Connections in Win2K/NT 4.0

▲ to top

Here's a question that pop's up at least a few times a month: "How can I prevent a user from logging into more than one computer at a time?" The easy way is to limit the user to a single machine. But if you don't want to do that, there's another way. Check out the KB article for more info.

Read more...

Office 2000 Service Pack 3

▲ to top

Office 2000 is still alive and well on personal and corporate desktops. Just to prove that fact, Microsoft presents for your installing pleasure Office 2000 Service Pack 3. You need to install Office SR1 before you install Service Pack 3.

Read more...

Windows .NET 2003 Server to Ship in April

to top

Here's the best news I've heard all week! Win2003 won't be released to the general public until next April. Looks like Microsoft is taking its security push very seriously, and they're not going to release Win2003 until it is rock solid. I suspect that Win2003 will be the best and most secure Windows operating system ever released, and we'll be spending more time with Linux security patches than Windows patches.

Read more...

Support WebCast - .NET Terminal Services: New Features

to top

Win2003 has many new Terminal Server features. These include licensing updates, improved Group Policy support, redirection features, and the Session Directory. This presentation will introduce these new features, discuss how to configure them, and provide troubleshooting tips.

Read more...

Download of the Week

Fire and Water Toolkit

to top

Are you looking for the ultimate assessment and defense toolkit that works on Windows-based operating systems? Sure you are, but you know you have to pay an arm and a leg to get such a toolkit. No way! Try out the TOTALLY FREE Fire & Water Toolkit by NT OBJECTives. The kit contains a powerful port scanner, Web server scanner, traceroute tool, network mapper, and analysis and reporting tool. You could pay tens of thousands for a similar set of tool, but you can get Fire & Water from NT OBJECTives for nothing.

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.