

Defining Strategies to Protect Against TCP SYN Denial of Service Attacks

Document ID: 14760

Abstract

Prerequisites

Requirements

Components Used

Conventions

Problem Description

The TCP SYN Attack

Defending Against Attacks on Network Devices

Devices Behind Firewalls

Devices Offering Publicly Available Services (Mail Servers, Public Web Servers)

Preventing A Network from Unwittingly Hosting an Attack

Preventing Transmission of Invalid IP Addresses

Preventing Reception of Invalid IP Addresses

Related Information

Abstract

There is a potential denial of service attack at internet service providers (ISPs) that targets network devices.

- **TCP SYN attack:** A sender transmits a volume of connections that cannot be completed. This causes the connection queues to fill up, thereby denying service to legitimate TCP users.

This paper contains a technical description of how the potential TCP SYN attack occurs and suggested methods for using Cisco IOS software to defend against it.

Note: Cisco IOS 11.3 software has a feature to actively prevent TCP denial of service attacks. This feature is described in the document [Configuring TCP Intercept \(Prevent Denial-of-Service Attacks\)](#).

Prerequisites

Requirements

There are no specific prerequisites for this document.

Components Used

This document is not restricted to specific software and hardware versions.

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

Problem Description

The TCP SYN Attack

When a normal TCP connection starts, a destination host receives a SYN (synchronize/start) packet from a source host and sends back a SYN ACK (synchronize acknowledge). The destination host must then hear an ACK (acknowledge) of the SYN ACK before the connection is established. This is referred to as the "TCP three-way handshake."

While waiting for the ACK to the SYN ACK, a connection queue of finite size on the destination host keeps track of connections waiting to be completed. This queue typically empties quickly since the ACK is expected to arrive a few milliseconds after the SYN ACK.

The TCP SYN attack exploits this design by having an attacking source host generate TCP SYN packets with random source addresses toward a victim host. The victim destination host sends a SYN ACK back to the random source address and adds an entry to the connection queue. Since the SYN ACK is destined for an incorrect or non-existent host, the last part of the "three-way handshake" is never completed and the entry remains in the connection queue until a timer expires, typically for about one minute. By generating phony TCP SYN packets from random IP addresses at a rapid rate, it is possible to fill up the connection queue and deny TCP services (such as e-mail, file transfer, or WWW) to legitimate users.

There is no easy way to trace the originator of the attack because the IP address of the source is forged.

The external manifestations of the problem include inability to get e-mail, inability to accept connections to WWW or FTP services, or a large number of TCP connections on your host in the state SYN_RCVD.

Defending Against Attacks on Network Devices

Devices Behind Firewalls

The TCP SYN attack is characterized by an influx of SYN packets from random source IP addresses. Any device behind a firewall that stops inbound SYN packets is already protected from this mode of attack and no further action is needed. Examples of firewalls include a Cisco Private Internet Exchange (PIX) Firewall or a Cisco router configured with access lists. For examples of how to set up access lists on a Cisco router, please refer to the document *Increasing Security On IP Networks*.

Devices Offering Publicly Available Services (Mail Servers, Public Web Servers)

Preventing SYN attacks on devices behind firewalls from random IP addresses is relatively simple since you can use access lists to explicitly limit inbound access to a select few IP addresses. However, in the case of a public web server or mail server facing the Internet, there is no way to determine which incoming IP source addresses are friendly and which are unfriendly. Therefore, there is no clear cut defense against an attack from a random IP address. Several options are available to hosts:

- Increase the size of the connection queue (SYN ACK queue).

- Decrease the time-out waiting for the three-way handshake.
- Employ vendor software patches to detect and circumvent the problem (if available).

You should contact your host vendor to see if they have created specific patches to address the TCP SYN ACK attack.

Note: Filtering IP addresses at the server is ineffective since an attacker can vary his IP address, and the address may or may not be the same as that of a legitimate host.

Preventing A Network from Unwittingly Hosting an Attack

Since a primary mechanism of this denial of service attack is the generation of traffic sourced from random IP addresses, we recommend filtering traffic destined for the Internet. The basic concept is to throw away packets with invalid source IP addresses as they enter the Internet. This does not prevent a denial of service attack on your network, but will help attacked parties rule out your location as the source of the attacker. In addition, it makes your network less attractive as a base for this class of attack.

Preventing Transmission of Invalid IP Addresses

By filtering packets on your routers that connect your network to the Internet, you can permit only packets with valid source IP addresses to leave your network and get into the Internet.

For example, if your network consists of network 172.16.0.0, and your router connects to your ISP using a serial 0/1 interface, you can apply the access list as follows:

```
access-list 111 permit ip 172.16.0.0 0.0.255.255 any
access-list 111 deny ip any any log

interface serial 0/1
ip access-group 111 out
```

Note: The last line of the access list determines if there is any traffic with an invalid source address entering the Internet. It is not crucial to have this line, but it will help locate the source of the possible attacks.

Preventing Reception of Invalid IP Addresses

For ISPs who provide service to end networks, we highly recommend the validation of incoming packets from your clients. This can be accomplished by the use of inbound packet filters on your border routers.

For example, if your clients have the following network numbers connected to your router via a serial interface named "serial 1/0", you can create the following access list:

```
The network numbers are 192.168.0.0 to 192.168.15.0, and 172.18.0.0.

access-list 111 permit ip 192.168.0.0 0.0.15.255 any
access-list 111 permit ip 172.18.0.0 0.0.255.255 any
access-list 111 deny ip any any log

interface serial 1/0
ip access-group 111 in
```

Note: The last line of the access list determines if there is any traffic with invalid source addresses entering the Internet. It is not crucial to have this line, but it will help locate the source of the possible attack.

This topic has been discussed in some detail on the NANOG [North American Network Operator1s Group] mailing list. The list archives are located at: <http://www.merit.edu/mail.archives/nanog/index.html>

For a detailed description of the TCP SYN denial of service attack and IP spoofing, see:
<http://www.cert.org/advisories/CA-1996-21.html>

<http://www.cert.org/advisories/CA-1995-01.html>

Related Information

- **Technical Support – Cisco Systems**

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Jul 13, 2007

Document ID: 14760
