GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Preventing SYN Flooding with Cisco Routers
Jim Phillipo E Mail jphillipo@guardent.com
September 6, 2000

TCP intercept was introduced in IOS Version 11.3 and is available on all Cisco Routers. This feature is designed to prevent known SYN attacks against internal hosts. The attack is simple. The first packet in the TCP three-way handshake sets the SYN bit. When a device receives an initial packet requesting a provided service, the device responds with a packet setting the SYN and ACK bits, and waits for an ACK from the originator of the conversation. If the originator of the request never responds to the host, the host times out the connection. While the host is waiting for the transaction to complete, however, the half open connection consumes resources on the host. This action is the essence of the attack

Thousands of packets with the SYN bit set are sent to a host. The source IP address in these packets however is forged. The source address of the forged packet is an unreachable address. In most cases, the source address will either be an unregistered address or the address of a host the attacker knows does not exist. Therefore, the attacked host will never receive a response to its request to complete the initial three-way handshake and must wait to time out thousands of connections. Eventually, the hosts' resources are consumed, and the host becomes unusable.

The TCP intercept feature works by intercepting and validating TCP connection requests. The feature can operate in two modes: intercept and watch. In intercept mode, the router intercepts incoming TCP synchronization requests and establishes a connection with the client on the server's behalf-and with the server on the clients' behalf. If both connections are successful, the router transparently merges the two connections. The router has aggressive timeouts to prevent its own resources from being consumed by a SYN attack. In watch mode, the router passively watches half-open connections and will actively close connections on the server after a configurable length of time. Access lists are defined to specify which source and destination packets are subject to TCP intercept.

Enable TCP Intercept

The following tasks are used to enable TCP intercept in global configuration mode:

Task	Command
Step 1 Define an IP extended access list.	**access-list** *access-list-number* {**deny** | **permit**} **tcp any** *destination destination-wildcard*
Step 2 Enable TCP intercept.	**ip tcp intercept list** *extended-access-list-number*

Typically the access list will define the source as **any** and define specific destination networks or servers. You do not attempt to filter on the source addresses because you don't necessarily know who to intercept packets from. You identify the destination in order to protect destination servers. You can define an access list to intercept all requests

© SANS Institute 2000 - 2005 Author retains full rights.

or only those coming from specific networks or destined for specific servers. If no access list match is found, the router allows the request to pass with no further action.

Set the Mode

TCP intercept works in either intercept or watch mode. The default is intercept. In this mode, the router responds to the incoming SYN request on the servers' behalf with a SYN-ACK and waits for an ACK from the client. If an ACK is received, the original SYN packet is sent to the server, and the router completes the three-way handshake with the server on behalf of the client.

In watch mode, the router enables SYN requests through to the server. If the session fails to establish itself in 30 seconds (default), the router sends a RST to the server to clear the connection. The amount of time the router waits is configurable with the **ip tcp intercept watch-timeout** command

To set the TCP intercept mode, perform the following task in global configuration mode:

Task	**Command**
Set the TCP intercept mode.	**ip tcp intercept mode** {**intercept** | **watch**}

Aggressive Thresholds

When the router believes a server is under attack as defined by its thresholds, the router will begin actively deleting connections until the number of half-open connections fall beneath this threshold. Oldest connections are dropped first, unless the command **ip tcp intercept drop mode random** is used. When an aggressive threshold is exceeded, the router performs the following actions:

1. Each new connection causes the oldest or random connection to be deleted.
2. The initial retransmission timeout is reduced by half to 0.5 seconds.
3. If in watch mode, the timeout is reduced by half to 15 seconds

Two factors determine aggressive behavior: If either of the thresholds is exceeded, aggressive behavior begins until both values fall below their threshold mark. The parameters and their default values are shown in the following list. The meaning of the parameter is self-explanatory.

ip tcp intercept max-incomplete low number 900
ip tcp intercept max-incomplete high number 1100
ip tcp intercept one-minute low number 900

© SANS Institute 2000 - 2005 Author retains full rights.

ip tcp intercept one minute high number 1100

To display TCP intercept information, perform either of the following tasks in EXEC mode:

show tcp intercept connections
show tcp intercept statistics

Sample Configuration:

The following configuration defines extended IP access list 101, causing the software to intercept packets for all TCP servers on the 192.168.1.0/24 subnet:

```
ip tcp intercept list 101
!
access-list 101 permit tcp any 192.168.1.0 0.0.0.255
```

Sources:
www.cisco.com

www.securityfocus.com **CI-96.02: TCP SYN attack**
Published: Tue Sep 17 1996
Updated: Tue Sep 17 1996

http://packetstorm.securify.com/papers/protocols/tcpflags.txt
TCP/IP Flags by Neon-Lenz®

© SANS Institute 2000 - 2005, Author retains full rights.