Why Does the ASA have xlate Entries with Idle Values Longer than the Configured Timeouts?

Contents

Introduction

This document explains why xlate entries with idle values are longer than the configured timeouts. It also provides information how you can correlate and see the conn and xlate values.

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Q. Why does the Adaptive Security Appliance (ASA) have xlate entries with idle values longer than the configured timeouts?

A. Here is an example that shows the xlate entries with idle values longer than the configured timeouts:

```
ASA#show xlate 26 in use, 16665 most used Flags: D - DNS, e - extended, I - identity,
I - dynamic, r - portmap, s - static, T - twice, N - net-to-net TCP PAT from
inside:10.20.33.2/54676 to outside: 192.0.2.3/54676 flags ri idle 1:48:12 timeout
0:00:30 TCP PAT from inside:10.20.33.2/54397 to outside: 192.0.2.3/54397 flags ri
idle 2:03:59 timeout 0:00:30 TCP PAT from inside:10.20.33.2/54369 to outside:
192.0.2.3/54369 flags ri idle 2:04:26 timeout 0:00:30 TCP PAT from
inside:10.20.33.3/56695 to outside: 192.0.2.3/56695 flags ri idle 0:09:22 timeout
0:00:30 TCP PAT from inside:10.20.33.3/55880 to outside: 192.0.2.3/55880 flags ri
idle 0:33:12 timeout 0:00:30 TCP PAT from inside:10.20.33.3/54431 to outside:
192.0.2.3/54431 flags ri idle 2:03:23 timeout 0:00:30
```

If a connection is subjected to translation (xlate) on the ASA, first the translation is built, then the connection is built, and finally, the connection is associated with that translation. The xlate idle timeout only starts when all of the associated connections for that xlate are terminated.

If you correlate the output of **show xlate** and **show conn**, you can see that the conn values match xlate values that have been idle for longer than the configured timeout. Here is an example.

Enter the Port Address Translation (PAT) **show xlate** command:

```
ASA# show xlate local port 54676 TCP PAT from inside:10.20.33.2/54676 to
outside:192.0.2.3/54676 flags ri idle 1:48:12 timeout 0:00:30
```

Then, Specify the port in the **show conn** command to find the associated connection entry:

```
ASA# show conn port 54676 TCP outside 192.168.22.3:443 events
inside:10.20.33.2:54676, idle 0:03:52, bytes 1807, flags UIO
```

This connection is associated with the translation. Local port 54676 is the same for both the connection and the translation entry. This TCP connection is present until it is closed by the protocol (TCP FINs or reset packets), or until it times out by the ASA (after the default timeout of 1 hour). When the connection is taken down, the translation is also deleted, but this deletion is delayed for "timeout" seconds.

Related Information

- **Cisco ASA 5500 Series Next Generation Firewalls**
- **Technical Support & Documentation - Cisco Systems**