What is the 'x' connection flag in the show xlate output in ASA version 9.0(1) and later?

Document ID: 115993

Contributed by Cisco TAC Engineers.
Mar 08, 2013

Contents

Introduction

This document describes the 'x' connection flag that appears in the output of the show xlate command in ASA version 9.0(1) and later.

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

Q. What is the 'x' connection flag in the show xlate output in ASA version 9.0(1) and later?

A. The 'x' flag indicates that the connection uses a 'per−session' PAT xlate.

Here is an example:

```
ASA# show conn address 10.107.84.210
55 in use, 108 most used
TCP outside  10.107.84.210:443 dmz  10.36.103.86:53613,
    idle 0:00:30, bytes 18155, flags UxIO
TCP outside  10.107.84.210:80 dmz  10.36.103.86:52723,
    idle 0:00:57, bytes 2932, flags UxIO
ASA#
```

In ASA version 9.0(1) and later, the PAT xlate that the connection utilized is immediately deleted from the xlate table by default when any TCP or UDP−based DNS connection is closed. This behavior differs from software versions earlier than 9.0(1) in which the dynamic xlate would stay in the table for an additional 30−second timeout period after the connection was torn down.

The default commands that enable this behavior can be seen in the configuration with the show run all xlate command:

```
ASA# show run all xlate
xlate per−session permit tcp any4 any4
xlate per−session permit tcp any4 any6
xlate per−session permit tcp any6 any4
xlate per−session permit tcp any6 any6
xlate per−session permit udp any4 any4 eq domain
xlate per−session permit udp any4 any6 eq domain
xlate per−session permit udp any6 any4 eq domain
xlate per−session permit udp any6 any6 eq domain
```

```
ASA#
```

If the ASA is upgraded from a software version earlier than 9.0(1) to version 9.0(1) or later, the legacy 30−second timeout behavior is maintained by adding specific xlate per−session deny rules in the configuration.

An ASA that runs version 9.0(1) or later that was not upgraded will have the default rules applied (as shown in the sample output above). An ASA that has been upgraded to version 9.0(1) or later will include the non−default explicit xlate rules applied as shown in this sample output:

```
ASA# show run xlate
xlate per−session deny tcp any4 any4
xlate per−session deny tcp any4 any6
xlate per−session deny tcp any6 any4
xlate per−session deny tcp any6 any6
xlate per−session deny udp any4 any4 eq domain
xlate per−session deny udp any4 any6 eq domain
xlate per−session deny udp any6 any4 eq domain
xlate per−session deny udp any6 any6 eq domain
```

The xlate commands shown in this sample output are added during an upgrade to version 9.0(1) in order to disable per−session xlates and preserve the behavior of the previous version.

Related Information

- **Technical Support & Documentation − Cisco Systems**

Updated: Mar 08, 2013 Document ID: 115993