

# Was ist das "x"-Verbindungsflag in der Ausgabe von show xlate in ASA Version 9.0(1) und höher?

## Inhalt

### [Einleitung](#)

[Was ist das "x"-Verbindungsflag in der Ausgabe von show xlate in ASA Version 9.0\(1\) und höher?](#)

[Zugehörige Informationen](#)

## Einleitung

In diesem Dokument wird das "x"-Verbindungsflag beschrieben, das in der Ausgabe des Befehls show xlate in ASA Version 9.0(1) und höher angezeigt wird.

Weitere Informationen zu Dokumentkonventionen finden Sie unter [Cisco Technical Tips Conventions \(Technische Tipps von Cisco zu Konventionen\)](#).

## F. Was ist das 'x'-Verbindungsflag in der Ausgabe von show xlate in ASA Version 9.0(1) und höher?

A. Das 'x'-Flag gibt an, dass die Verbindung eine 'per-session' PAT-Erweiterung verwendet.

Hier ein Beispiel:

```
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 der ASA-Version 9.0(1) und höher gibt die PAT an, dass die verwendete Verbindung standardmäßig sofort aus der Xlate-Tabelle gelöscht wird, wenn eine TCP- oder UDP-basierte DNS-Verbindung geschlossen wird. Dieses Verhalten unterscheidet sich von Softwareversionen vor 9.0(1), bei denen der dynamische Ausdruck nach dem Abbruch der Verbindung für weitere 30 Sekunden in der Tabelle verbleiben würde.

Die Standardbefehle, die dieses Verhalten aktivieren, sind in der Konfiguration mit dem Befehl show run all xlate zu sehen:

```
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#
```

Wenn die ASA von einer Softwareversion vor 9.0(1) auf Version 9.0(1) oder höher aktualisiert wird, wird das bisherige 30-Sekunden-Timeout beibehalten, indem der Konfiguration spezifische Regeln für die Ablehnung von Sitzungen pro Sitzung hinzugefügt werden.

Auf ASAs mit Version 9.0(1) oder höher, die nicht aktualisiert wurden, werden die Standardregeln angewendet (wie in der obigen Beispielausgabe gezeigt). Eine ASA, die auf Version 9.0(1) oder höher aktualisiert wurde, enthält die nicht standardmäßigen expliziten Xlate-Regeln, die wie in dieser Beispielausgabe gezeigt angewendet werden:

```
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
```

Die in dieser Beispielausgabe gezeigten xlate-Befehle werden während eines Upgrades auf Version 9.0(1) hinzugefügt, um Xlates pro Sitzung zu deaktivieren und das Verhalten der vorherigen Version beizubehalten.

## Zugehörige Informationen

- [Technischer Support und Dokumentation für Cisco Systeme](#)

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.