

Qual è il flag di connessione 'x' nell'output show xlate in ASA versione 9.0(1) e successive?

Sommario

[Introduzione](#)

[Qual è il flag di connessione 'x' nell'output show xlate in ASA versione 9.0\(1\) e successive?](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto il flag di connessione 'x' che viene visualizzato nell'output del comando show xlate in ASA versione 9.0(1) e successive.

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

D. Qual è il flag di connessione 'x' nell'output del comando show xlate in ASA versione 9.0(1) e successive?

R. Il flag 'x' indica che la connessione utilizza un'estensione PAT 'per sessione'.

Di seguito è riportato un esempio:

```
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 versione 9.0(1) e successive, l'estensione PAT usata per la connessione viene eliminata immediatamente dalla tabella xlate per impostazione predefinita quando si chiude una connessione DNS basata su TCP o UDP. Questo comportamento è diverso dalle versioni software precedenti alla 9.0(1) in cui l'estensione dinamica rimarrebbe nella tabella per un ulteriore periodo di timeout di 30 secondi dopo l'interruzione della connessione.

I comandi predefiniti che abilitano questo comportamento possono essere visualizzati nella configurazione con il comando show run all xlate:

```
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#
```

Se l'ASA viene aggiornata da una versione software precedente alla 9.0(1) alla versione 9.0(1) o successive, il comportamento di timeout precedente alla versione 30 secondi viene mantenuto con l'aggiunta di specifiche regole di rifiuto per sessione xlate nella configurazione.

A un'appliance ASA che esegue la versione 9.0(1) o successive non aggiornata vengono applicate le regole predefinite (come mostrato nell'output di esempio riportato sopra). Un'appliance ASA che è stata aggiornata alla versione 9.0(1) o successive includerà le regole di estensione esplicita non predefinite applicate, come mostrato nell'output di esempio:

```
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
```

I comandi xlate mostrati in questo output di esempio vengono aggiunti durante un aggiornamento alla versione 9.0(1) per disabilitare gli xlate per sessione e mantenere il comportamento della versione precedente.

Informazioni correlate

- [Documentazione e supporto tecnico – Cisco Systems](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).