

設定したタイムアウトより長いアイドル状態の値の xlate エントリが ASA にある理由

目次

[はじめに](#)

[設定したタイムアウトより長いアイドル状態の値の xlate エントリが適応型セキュリティ アプライアンス \(ASA \) にある理由](#)

[関連情報](#)

概要

このドキュメントでは、設定したタイムアウトより長いアイドル状態の値の xlate エントリが存在する理由について説明します。また、conn および xlate 値を関連付け、表示する方法についても説明します。

ドキュメント表記の詳細は、『[シスコテクニカルティップスの表記法](#)』を参照してください。

Q. 設定したタイムアウトより長いアイドル状態の値の xlate エントリが適応型セキュリティ アプライアンス (ASA) にある理由

A. 次に、設定したタイムアウトより長いアイドル状態の値の xlate エントリの例を示します。

```
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
```

接続が ASA での変換 (xlate) の対象となる場合、先に変換が構築されて、次に接続が確立され、最終的に接続がその変換と関連付けられます。 xlate のアイドル タイムアウトは、その xlate

に関連付けられたすべての接続が終了した場合にのみ開始されます。

show xlate と **show conn** の出力を関連付けると、conn の値が設定されたタイムアウトよりも長くアイドル状態になっている xlate の値と一致を確認できます。次に例を示します。

Port Address Translation (PAT) **show xlate command** を入力します。

```
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
```

次に、**show conn** コマンドでポートを指定し、関連する接続エントリを見つけます。

```
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
```

この接続は、変換と関連付けられています。ローカルポート 54676 は、接続エントリおよび変換エントリの両方で同じです。この TCP 接続はプロトコル (TCP FIN またはリセット パケット) によって閉じられるか、ASA によってタイムアウトされる (1 時間のデフォルトのタイムアウト後) まで存続します。接続がダウン状態になると、変換も削除されますが、この削除は「タイムアウト」の秒数だけ遅延されます。

関連情報

- [Cisco ASA 5500 シリーズ Next Generation Firewalls](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)