

Build-Up and Teardown ASA TCP Connection Flags

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[ASA TCP Connection Flags](#)

[TCP Connection Flag Values](#)

Introduction

This document describes information about Adaptive Security Appliance (ASA) TCP connection flags.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic knowledge of the TCP Communications Protocol
- Basic knowledge of the ASA CLI

Components Used

The information in this document is based on ASA version 8.4.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

ASA TCP Connection Flags

When you troubleshoot TCP connections through the Adaptive Security Appliance, the connection flags shown for each TCP connection provide a wealth of information about the state of TCP connections to the ASA. This information can be used to troubleshoot problems with the ASA, as well as problems elsewhere in the network.

Here is the output of the **show conn protocol tcp** command, which shows the state of all TCP connections through the ASA. These connections can also be seen with the **show conn** command.

```
<#root>
```

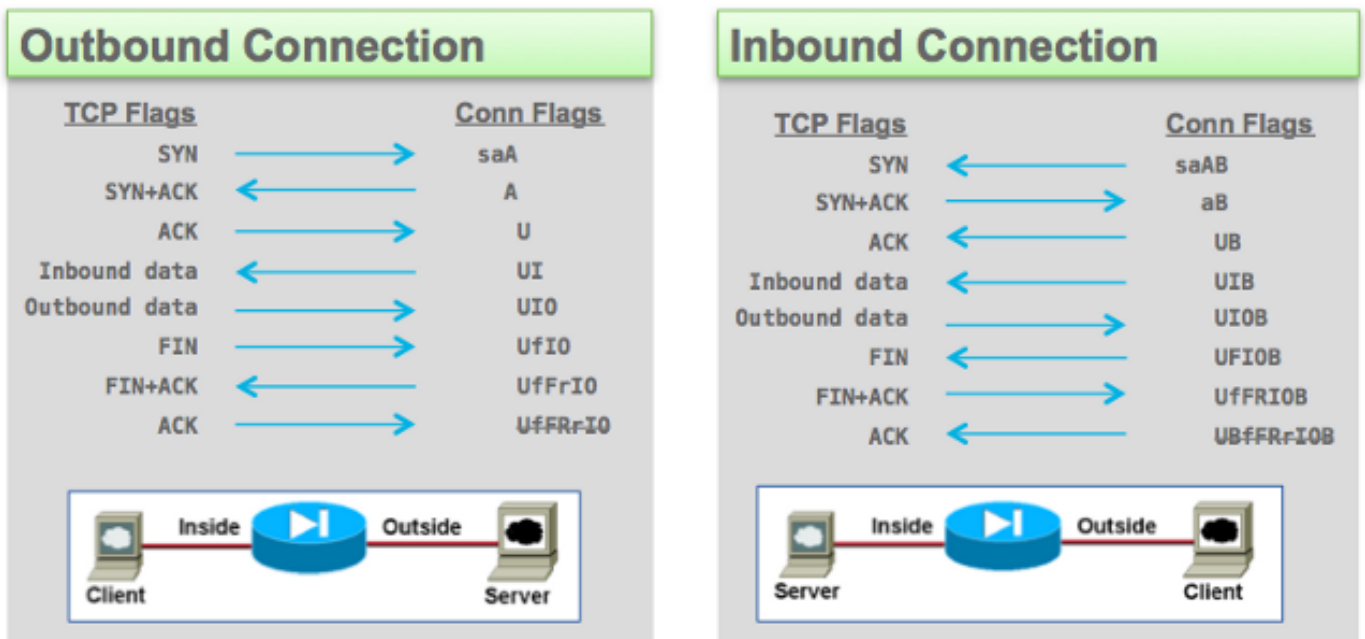
```
ASA#
```

```
show conn protocol tcp
```

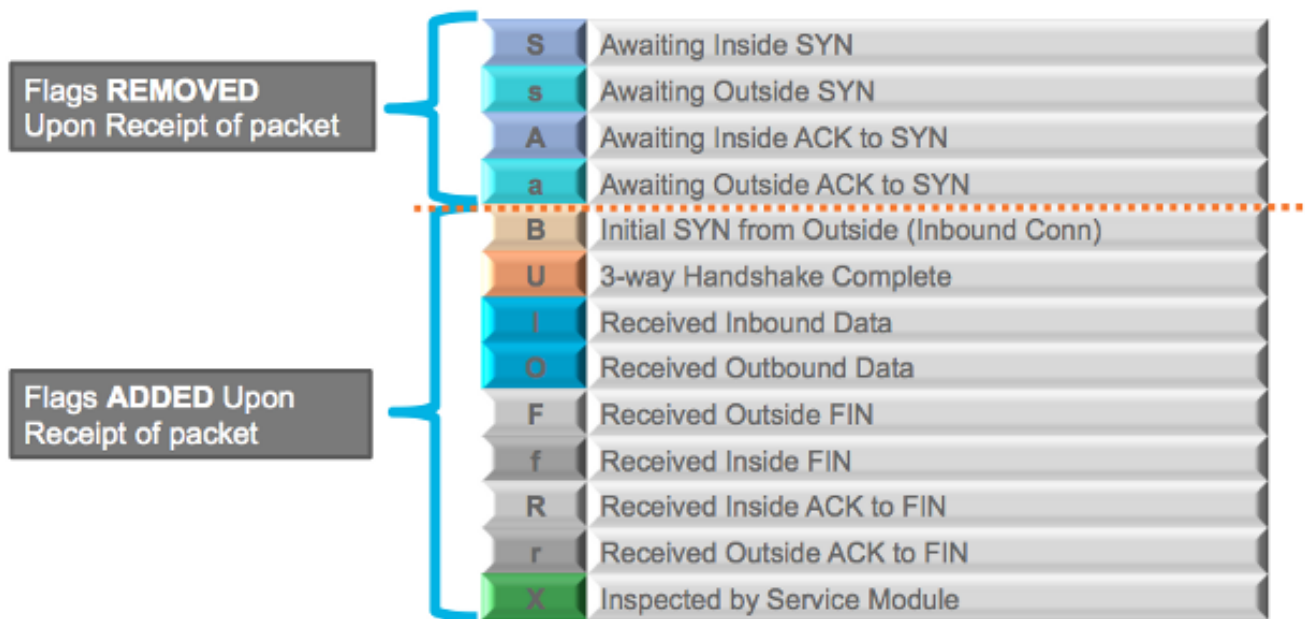
101 in use, 5589 most used.

```
TCP outside 10.23.232.59:5223 inside 192.168.1.3:52419, idle 0:00:11, bytes 0, flags saA
TCP outside 192.168.3.5:80 dmz 172.16.103.221:57646, idle 0:00:29, bytes 2176, flags UIO
TCP outside 10.23.232.217:5223 inside 192.168.1.3:52425, idle 0:00:10, bytes 0, flags saA
TCP outside 10.23.232.217:443 inside 192.168.1.3:52427, idle 0:01:02, bytes 4504, flags UIO
TCP outside 10.23.232.57:5223 inside 192.168.1.3:52412, idle 0:00:23, bytes 0, flags saA
TCP outside 10.23.232.116:5223 inside 192.168.1.3:52408, idle 0:00:23, bytes 0, flags saA
TCP outside 10.23.232.60:5223 inside 192.168.1.3:52413, idle 0:00:23, bytes 0, flags saA
TCP outside 10.23.232.96:5223 inside 192.168.1.3:52421, idle 0:00:11, bytes 0, flags saA
TCP outside 10.23.232.190:5223 inside 192.168.1.3:52424, idle 0:00:10, bytes 0, flags saA
```

This picture shows the ASA TCP Connection flags at different stages of the TCP state machine. The connection flags can be seen with the **show conn** command on the ASA.



TCP Connection Flag Values



Additionally, in order to view all of the possible connection flags issue the **show connection detail** command on the command-line:

```
<#root>
```

```
ASA5515-X#
```

```
show conn detail
```

```
35 in use, 199 most used
```

```
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
      B - initial SYN from outside, b - TCP state-bypass or nailed,
      C - CTIQBE media, c - cluster centralized,
      D - DNS, d - dump, E - outside back connection, F - outside FIN, f - inside FIN,
      G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
      i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
      k - Skinny media, M - SMTP data, m - SIP media, n - GUP
      O - outbound data, P - inside back connection, p - Phone-proxy TFTP connection,
      q - SQL*Net data, R - outside acknowledged FIN,
      R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
      s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
      V - VPN orphan, W - WAAS,
      X - inspected by service module,
      x - per session, Y - director stub flow, y - backup stub flow,
      Z - Scansafe redirection, z - forwarding stub flow
```