



Support Home

Resources ▼

# PALO ALTO NETWORKS FIREWALL SESSION OVERVIEW

Created On 02/07/19 23:57 PM - Last 15100  
Updated 02/07/19 23:57 PM

## MOBILE NETWORK INFRASTRUCTURE

### Resolution

#### Overview

On a Palo Alto Networks firewall, a session is defined by two uni-directional flows each uniquely identified by a 6-tuple key: source-address, destination-address, source-port, destination-port, protocol, and security-zone.

Besides the six attributes that identify a session, each session has few more notable identifiers:

End hosts - The source IP and destination IP which will be marked as client(source IP) and server(destination IP)

Flow direction - Since each session is identified by a two uni-directional flow, each flow must be properly identified. Palo Alto Networks firewalls will identify the first flow as client-to-server(c2s) and the returning flow as server-to-client(s2c).

#### Show Session command

To view any information related to sessions the user can use the > **show session** command followed by the desired option:

> `show session all` will show all current sessions that are processed by the firewall at the time when command is entered.

**Note:** There is a limit in the number of sessions that can be shown with the > `show session all` command. The limit is based on the byte size of the session which cannot be changed.

Please refer to the following document for more information: [Can the Whole Session Log be Exported?](#)

> `show session id [ID]` will show detailed information on a session based on the entered session ID

> `show session info` will display the general configuration on the firewall regarding session management and their current statistics

> `show session meter` will display the maximum number of sessions for each VSYS on firewalls with Multiple Virtual System capability

Other  
users also  
viewed:

Session  
States  
and  
Types

Packet  
Flow  
Sequence  
in PAN-  
OS

How to  
Monitor  
Live  
Sessions  
in the  
CLI

How to  
View  
Session  
Statistics  
from the  
CLI

#### Actions

[Print](#)

[Copy](#)

[Link](#)

#### Attachments

Choose  
Language

English

```

c2s flow:
  source: 192.168.42.132 [Trust]
  dst:    74.125.136.100
  proto:  6
  sport:  4674      dport: 80
  state:  INIT      type:  FLOW
  src user: unknown
  dst user: unknown

s2c flow:
  source: 74.125.136.100 [Untrust]
  dst:    172.24.12.42
  proto:  6
  sport:  80      dport: 1030
  state:  INIT      type:  FLOW
  src user: unknown
  dst user: unknown

```

In the screenshot below, identify some of the important details of a session:

- `Session ID` - In the example, the session ID is 524342
- `c2s flow` and `s2c flow` - Identifies flow of traffic from Client to Server (c2s) and from Server to Client (s2c).
- `Source` and `dst` (destination) address with zone - Identifies the source and dst addresses for each flow of the session. In the above example, the dst IP in s2c flow does not match the source IP in c2s flow due to a dynamic-ip-and-port source NAT.
- `Source (sport)` and `destination port (dport)` - Identifies source and destination ports for each flow of the session. In the example, the c2s and s2c flows show different ports due to the configured NAT policy.
- `src user` and `dst user` - If User-ID is configured on the firewall, the users would be identified if available.
- `state` - The state of the session. The states are defined below, in the following section.
- `type` - There are 2 types of sessions: `FLOW` and `PREDICT`. The session types are defined below, in the following section.

#### Session types, states and flags

On Palo Alto Networks firewalls there are two types of sessions:

**Flow** - Regular type of session where the flow is the same between c2s and s2c (ex. HTTP, Telnet, SSH).

**Predict** - This type is applied to sessions that are created when Layer7 Application Layer Gateway (ALG) is required. The application has been identified and there is need for a new session to be allowed on the firewall without any additional security rule (ex. FTP active/passive, voice protocols h323/sip etc). These sessions may be created with a 0 as source/destination IP/port, since that information may not be known yet. Packets that match the Predict sessions will then change to normal FLOW session.

are currently active on the firewall. This command might not show many predict sessions on the firewall due to the fact that each predict session will become a FLOW session once it is matched by a single packet. Therefore, the command will show only the predict sessions that are currently pending to be matched by packets.

**Note:** Each application's predict session has its own timeout setting.

In the following example is the output of a PREDICT session created for FTP Active mode:

```

c2s flow:
  source:      63.245.215.46 [Untrust]
  dst:         172.24.12.42
  proto:       6
  sport:       0                dport:    41082
  state:       ACTIVE           type:      PRED
  src user:    unknown
  dst user:    unknown

s2c flow:
  source:      192.168.42.132 [Trust]
  dst:         63.245.215.46
  proto:       6
  sport:       2071             dport:    0
  state:       OPENING          type:      PRED
  src user:    unknown
  dst user:    unknown

start time      : Tue Mar 19 01:57:08 2013
timeout         : 60 sec
time to live    : 1 sec
total byte count(c2s) : 0
total byte count(s2c) : 0
layer7 packet count(c2s) : 0
layer7 packet count(s2c) : 0
vsys            : vsys1
application     : ftp-data
rule            :
session to be logged at end : False
session in session ager    : True
session synced from HA peer : False
address/port translation  : source + destination
nat-rule                : All-Traffic(vsys1)
prediction triggered by   : client
prediction matched once   : True
  
```

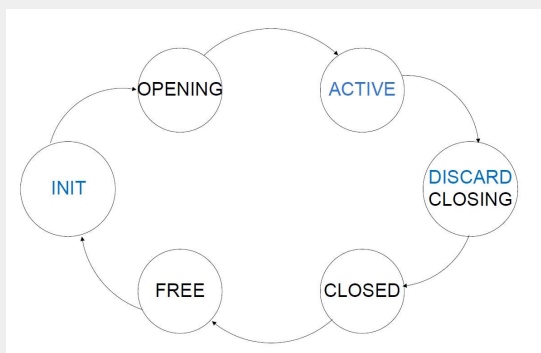
The screenshot above shows the number of packets as 0 for both directions and that the predict session has been triggered by the client.

Each session will be in a certain state at any given time. There are three states, known as the Stable states, that will appear most in the session table:

**INIT** - Every session begins, by default, in INIT state. A session in the INIT state is part of the free pool and can be used at anytime. The session may have been used previously, but has now been returned back into the free pool.

The other states of a session in the Palo Alto Networks firewall are: Opening, Closing, Closed and Free. These states are called *Transient*. Sessions in Transient states are difficult to see as they make the transition to one of the Stable states very quickly.

Under normal conditions, each state will go through the following transition cycle: Init > Opening > Active > Discard/Closing > Closed > Free. From the Free state, the session will move back to the initial session state(INIT) to start the next cycle. The following state transition represents the session life cycle:



The most important state in the life cycle is the Active state. From Active state, the session will transition to either the Discard or Closing state based on the following conditions:

If the session timeout has been reached, the session will timeout and transition to Closing. Session timeout is described in the following section.

If the traffic has been denied due to a security rule or a threat has been detected(with the action set to drop), the session will transition to Discard.

In the output of `> show session all` each session can be identified by a `flag` value. The meaning of each session flag value is described below:

NS - There has been Source NAT applied on the session

ND - There has been Destination NAT applied on the session

NB - There has been Both Source + Destination NAT applied on the session

No flag - There is no NAT applied on the session.

Session timeout

show session id command. The screenshot below shows the output of a DNS session through the firewall:

```
admin@PA-5060> show session id 2359361

Session      2359361

c2s flow:
  source:    192.168.42.132 [Trust]
  dst:       8.8.8.8
  proto:     17
  sport:     1078           dport:    53
  state:     ACTIVE        type:       FLOW
  src user:  unknown
  dst user:  unknown

s2c flow:
  source:    8.8.8.8 [Untrust]
  dst:       172.24.12.42
  proto:     17
  sport:     53             dport:    47075
  state:     ACTIVE        type:       FLOW
  src user:  unknown
  dst user:  unknown

start time      : Sun Mar 17 09:18:29 2013
timeout         : 30 sec
time to live    : 2 sec
total byte count(c2s) : 5474
total byte count(s2c) : 9290
layer7 packet count(c2s) : 59
layer7 packet count(s2c) : 59
vsys           : vsys1
application    : dns
rule           : Test-Rule
session to be logged at end : True
session in session ager : True
```

Three significant details about the session timeout are:

**Timeout** - The specific timeout configured for the application.

**Time to live** - The time left until the session will expire. In the example, there are 2 seconds left until the session will expire and session state will change.

**Session in session ager** - For each session there is a flow ager, which is an aging process that keeps track of the lifetime of sessions. As long as the session is Active and `time to live` did not reach 0 sec, the `session in session ager` will be marked as `True`.

In the following example, see the output of the same session, but now the session has timed out (due to no traffic matching the session):

```

source:      192.168.42.132 [Trust]
dst:         8.8.8.8
proto:       17
sport:       1078           dport:      53
state:       CLOSED        type:        FLOW
src user:    unknown
dst user:    unknown

s2c flow:
source:      8.8.8.8 [Untrust]
dst:         172.24.12.42
proto:       17
sport:       53           dport:      47075
state:       CLOSED        type:        FLOW
src user:    unknown
dst user:    unknown

start time   : Sun Mar 17 09:18:29 2013
timeout      : 30 sec
time to live : 29 sec
total byte count(c2s) : 5474
total byte count(s2c) : 9290
layer7 packet count(c2s) : 59
layer7 packet count(s2c) : 59
vsys         : vsys1
application  : dns
rule         : Test-Rule
session to be logged at end : True
session in session ager : False
session synced from HA peer : False
address/port translation : source + destination
nat-rule     : All-Traffic(vsys1)
layer7 processing : enabled
URL filtering enabled : False
session via syn-cookies : False
session terminated on host : False
session traverses tunnel : False
captive portal session : False
ingress interface : ethernet1/4
egress interface  : ethernet1/3
session QoS rule  : N/A (class 4)

```

Now see that the session state is Closed and also the session in session ager has turned to False.

#### Session management in HA deployment

In deployments where High Availability is being used, certain active sessions that are not created on the local firewall, but on the peer device must be synchronized between peers. Having these sessions synchronized between peers, in case of fail-over the active sessions will not be lost and the traffic flow will continue on the other device(Active in case of Active/Passive deployment). For details about deployment scenarios involving HA please consult the Admin Guide at HA section.

The user can tell if a session has not been created on the local firewall by looking at the *session synced from HA peer* from `>show session id` output. A session created locally on the firewall will have the

The `> show session id` command displays other information regarding the traffic flow through the firewall. While much of the additional information is for advanced troubleshooting by Palo Alto Networks support representatives, here are three attributes that may be useful for self-troubleshooting:

`Session to be logged at the end` - When configuring the security rules there are 2 options for rule logging: at the end (`True`) or at the start (`False`) of the session.

In this example (see the above screenshot), the configuration has specified that the rule should be logged at the end.

`Offload yes` - Marks the traffic for which the application has been identified already and it will be processed in hardware.

`Layer7 processing` - If enabled, then App-ID has been enabled on the traffic flow and the application is constantly identified. If Layer7 processing is set to complete, then the application has been identified.

See also  
PAN-OS Admin Guides and CLI Reference Guides in [Documentation](#)

owner: aciobanu

#### Attachments



#### COMPANY

[About Palo Alto Networks](#)

[Careers](#)

#### LEGAL NOTICES

[Privacy](#)

[Terms of Use](#)


#### RESOURCES

[Support](#)

[Live Community](#)

[Email Subscription](#)



**CUSTOMER SUPPORT** ▾

What are you looking for?

?

Sign In

© 2018 Palo Alto Networks, Inc. All rights reserved.