Palo Alto Networks Firewall Session Overview

by aciobanu (/t5/user/viewprofilepage/user-id/5143) on 03-13-2013 02:03 AM - edited on 04-20-2016 05:30 AM by **reaper** (/t5/user/viewprofilepage/user-id/7608) (57,916 Views)

Labels: Learning (/t5/Learning-Articles/tkb-p/learning_tkb/label-name/learning?labels=learning), Management (/t5/Learning-Articles/tkb-p/learning_tkb/label-name/management?labels=management), Network (/t5/Learning-Articles/tkb-p/learning_tkb/label-name/network?labels=network)

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 enter
  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? (/docs/DOC-3995
- `> 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 cur statistics
- `> show session meter` will display the maximum number of sessions for each VSYS on firewalls with Multiple Virtual Sy capability

Below is an example output from the > `show session id` command:

```
admin@PA-5060> show session id 524342

Session         524342

        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.

In order to have a granular view of the Predict (PRED) sessions on the firewall, use the `> show session all filter type predict` command. The command will display only the predict session that 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.

...g-Articles/Palo-Alto-Networks-Firewall-Session-Overview/ta-p/55633/label-n

Hardware (https://live.paloaltonetworks.com/t5/Learning-Articles/Palo-Alto-Networks-Firewall-Session-Overview/ta-p/55633/label-n

High Availability (https://live.paloaltonetworks.com/t5/Learning-Articles/Palo-Alto-Networks-Firewall-Session-Overview/ta-p/55633/label-n

Integration (https://live.paloaltonetworks.com/t5/Learning-Articles/Palo-Alto-Networks-Firewall-Session-Overview/ta-p/55633/label-n

Learning (https://live.paloaltonetworks.com/t5/Learning-Articles/Palo-Alto-Networks-Firewall-Session-Overview/ta-p/55633/label-n

Logs (https://live.paloaltonetworks.com/t5/Learning-Articles/Palo-Alto-Networks-Firewall-Session-Overview/ta-p/55633/label-n

Management (https://live.paloaltonetworks.com/t5/Learning-Articles/Palo-Alto-Networks-Firewall-Session-Overview/ta-p/55633/label-n

NAT (https://live.paloaltonetworks.com/t5/Learning-Articles/Palo-Alto-Networks-Firewall-Session-Overview/ta-p/55633/label-n

Network (https://live.paloaltonetworks.com/t5/Learning-Articles/Palo-Alto-Networks-Firewall-Session-Overview/ta-p/55633/label-n

Objects & Security Profiles (https://live.paloaltonetworks.com/t5/Learning-Articles/Palo-Alto-Networks-Firewall-Session-Overview/ta-p/55633/label-n

PAN-OS 8.1 (https://live.paloaltonetworks.com/t5/Learning-Articles/Palo-Alto-Networks-Firewall-Session-Overview/ta-p/55633/label-n

Panorama (https://live.paloaltonetworks.com/t5/Learning-Articles/Palo-Alto-Networks-Firewall-Session-Overview/ta-p/55633/label-n

Policies (https://live.paloaltonetworks.com/t5/Learning-Articles/Palo-Alto-Networks-Firewall-Session-Overview/ta-p/55633/label-n

Next (https://live.paloaltonetworks.com/t5/Learning-Articles/Palo-Alto-Networks-Firewall-Session-Overview/ta-p/55633/page/2/show-comments/true)

Contributors

(/t5/user/viewprofilepage/user-id/22095)
snowcrash (/t5/user/viewprofilepage/user-id/22095)

(/t5/user/viewprofilepage/user-id/5143)
aciobanu (/t5/user/viewprofilepage/user-id/5143)

(https://ignite.paloaltonetworks.com/usa/forms/2018_regform.html)

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
```

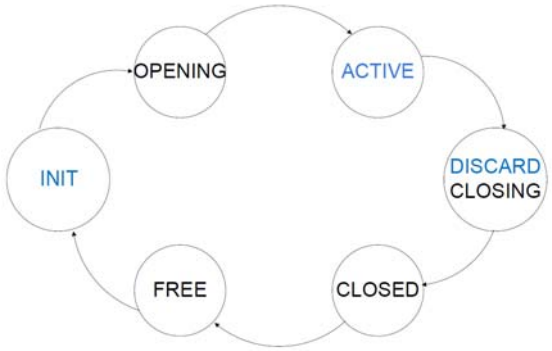
The screenshot above shows the number of packets as 0 for both directions and that the predict session has been triggered by the client.

Each session will be in a certain state at any given time. There are three states, know 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 been used previously, but has now been returned back into the free pool.
- `ACTIVE` - Any session that matches a particular traffic flow, and has been processed for inspection and forwarding.
- `DISCARD` - Traffic that has been matched by a session but is denied due to a security policy, threat detection.

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 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 follo 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 transi to Discard.

Alto-Networks-Firewalls/ta-p/61886)

Palo Alto Networks Application for QRadar (/t5/App-for-QRadar-Articles/Palo-Alto-Networks-Application-for-QRadar/ta-p/118455)

Traceroute and Traceroute6 Through the Palo Alto N... (/t5/Management-Articles/Traceroute-and-Traceroute6-Through-the-Palo-Alto-Networks/ta-p/59230)

When Does Palo Alto Networks Firewall Send a TCP R... (/t5/Learning-Articles/When-Does-Palo-Alto-Networks-Firewall-Send-a-TCP-Reset-RST-to/ta-p/56572)

Palo Alto Networks Management Access through TACAC... (/t5/Configuration-Articles/Palo-Alto-Networks-Management-Access-through-TACACS/ta-p/149144)

Re: Palo Alto Networks Visio Stencils (/t5/Management-Articles/Palo-Alto-Networks-Visio-amp-Omnigraffle-Stencils/ta-p/60547)

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

Each session has a defined timeout value which is configurable on the device. There are a few details that can be observed regarding the timer of a session by looking at the output of the > `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):

```
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:       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 **False** value and one created on the peer device and synchronized to the local firewall will have the **True** value.

Additional info

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 identi
  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 (/space/2021)

owner: aciobanu

Everyone's Tags:
cli (/t5/tag/cli/tg-p/board-id/learning_tkb) doc-4785 (/t5/tag/doc-4785/tg-p/board-id/learning_tkb)
learning (/t5/tag/learning/tg-p/board-id/learning_tkb) management (/t5/tag/management/tg-p/board-id/learning_tkb)
packet_flow (/t5/tag/packet_flow/tg-p/board-id/learning_tkb)
View All (8)

7 (/t5/kudos/messagepage/board-id/learning_tkb/message-id/164/tab/all-users)

Article Options

Hide Comments

Comments

by indup089 (/t5/user/viewprofilepage/user-id/29410)
on 04-09-2013 03:27 AM

Very useful, thank you!
We are still missing session timeout flags in the traffic logs (for troubleshooting purposes)
Any news about this?

Permalink (/t5/Learning-Articles/Palo-Alto-Networks-Firewall-Session-Overview/tac-p/55639#M170) 0

by aciobanu (/t5/user/viewprofilepage/user-id/5143)
on 04-09-2013 03:47 AM

Hi,
Do you refer to traffic logs you see in Web-GUI ? There you do not see any session timeout ?
Thanks

Permalink (/t5/Learning-Articles/Palo-Alto-Networks-Firewall-Session-Overview/tac-p/55638#M169) 0

by indup089 (/t5/user/viewprofilepage/user-id/29410)
on 04-09-2013 04:10 AM

Hi,
yes in the traffic logs (web-gui, cli or syslog) is still no flag availble which indicates if the logged session ran into a timeout.
For example a netscreen-firewall shows different close-reasons in the traffic-logs: ageout, fin, rst. That`s very useful for troubleshooting session-issues
Thank you!

Permalink (/t5/Learning-Articles/Palo-Alto-Networks-Firewall-Session-Overview/tac-p/55634#M165) 0

by aciobanu (/t5/user/viewprofilepage/user-id/5143)
on 04-09-2013 04:24 AM

Well you have the Time tab if you open a certain traffic flow in Traffic logs, but also you can use the "show session id" command in CLI and just copy the session ID from the traffic log. Like that you have more details about the session. It is not shown in Web-Gui but you do see it in CLI if you look after the Session ID, which is present in the traffic logs.

Permalink (/t5/Learning-Articles/Palo-Alto-Networks-Firewall-Session-Overview/tac-p/55636#M167)

by indup089 (/t5/user/viewprofilepage/user-id/29410)
on 04-09-2013 05:10 AM

Ok thank you, but "show session id" helps only while the session is active. With troubleshooting connection-issues occured in the p
via the traffic-logs there is no active session available and even no flag in the traffic-logs which indicates if the session was closed f
"normal" reasons or timed-out.

Permalink (/t5/Learning-Articles/Palo-Alto-Networks-Firewall-Session-Overview/tac-p/55635#M166)

by aciobanu (/t5/user/viewprofilepage/user-id/5143)
on 04-09-2013 12:43 PM

Yes are you right... therefore IMO the best troubleshooting method for traffic flow must correlate with CLI...

Permalink (/t5/Learning-Articles/Palo-Alto-Networks-Firewall-Session-Overview/tac-p/55637#M168) 0

by VUGD (/t5/user/viewprofilepage/user-id/33824)
on 04-18-2013 03:04 AM

Let me know if you guys have a good solution for troubleshooting session time-outs. I´m struggling with that too!

Permalink (/t5/Learning-Articles/Palo-Alto-Networks-Firewall-Session-Overview/tac-p/55642#M173) 0

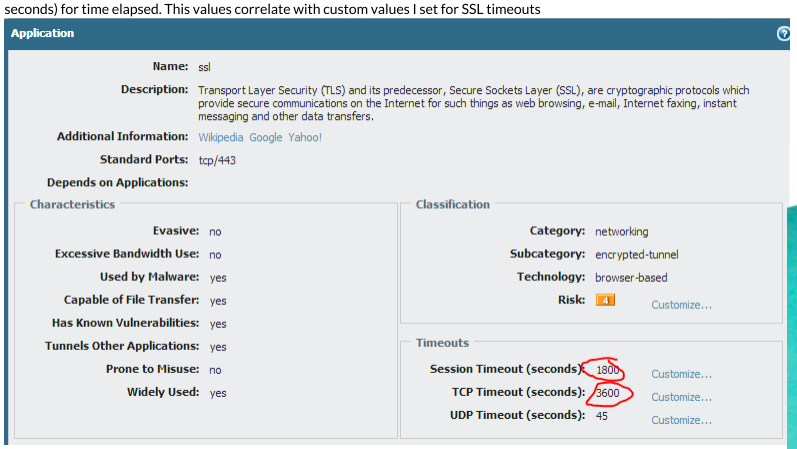
by aciobanu (/t5/user/viewprofilepage/user-id/5143)
on 04-19-2013 02:14 AM

Hi,
What kind of issue are you facing ?
Alex

Permalink (/t5/Learning-Articles/Palo-Alto-Networks-Firewall-Session-Overview/tac-p/55644#M175) 0

by VUGD (/t5/user/viewprofilepage/user-id/33824)
on 04-19-2013 02:39 AM

We have different scenarios where it seems like the PAN is dropping the sessions (the time elapsed always shows the specified value for the application timeout setting).
To give a more particular scenario: Some days ago a co-worker was reporting problems with managing ESX Server in "outside" Zones ever since we migrated from CISCO ASA to PAN. Basically the ESX Management server is initiating SSL Sessions to ESX Servers in different remote Zones. My co-worker extracted a log from one of the remote ESX that shows 321 open sessions to the ESX-Management server (321 connections is maximum for open sessions for the deamon, that´s why no more management is possible). However, at the same time there are only 4 active sessions on the ESX-Management Server.
Checking the connections in the traffic tab showed that the majority of the sessions had values of 1,800 (+/- 2 seconds) or 3600 (+/- 2 seconds) for time elapsed. This values correlate with custom values I set for SSL timeouts



This let me came to the conclusion:

- The PAN is dropping sessions because they run into a timeout.
- The remote host doesn´t recognize that the session is dropped - and as a result - probably tries to communicate with old sess IDs which the PAN is not accepting.

However, I´m still a newbie when it comes to PAN troubleshooting and really unsure if this way of troubleshooting leads me to the conclusions...
Thanks for your help,
Heiko

Permalink (/t5/Learning-Articles/Palo-Alto-Networks-Firewall-Session-Overview/tac-p/55643#M174) 0

by indup089 (/t5/user/viewprofilepage/user-id/29410)
on 04-19-2013 05:40 AM

Hi Heiko,
thank you! Your conclusion is absolutely right. What we need in the PaloAlto to deal with such issues is the following:
- Session timeout / ageout - flags in the traffic logs
- Send TCP RST on non-syn-Traffic on zone level (like the Juniper/Netscreen boxes).
The last feature would definitely prevent your hosts running in such issues because the firewall would send a TCP reset if the session is timed out and the client come back with his old session-flow (of coures this feature should only used on trusted/internal zones)
Regards,
Ulrich

Permalink (/t5/Learning-Articles/Palo-Alto-Networks-Firewall-Session-Overview/tac-p/55641#M172) 0

by gwesley (/t5/user/viewprofilepage/user-id/2128)
on 09-16-2014 06:01 AM

good news! In version 6.1, session end logging has been added:
Session End Reason Logging—When troubleshooting connectivity and application availability issues, knowing what caused a session to terminate can be useful. PAN-OS now provides a new session end reason field in traffic logs, reports, syslogs, SNMP traps, and email alerts.

Permalink (/t5/Learning-Articles/Palo-Alto-Networks-Firewall-Session-Overview/tac-p/55640#M171) 0

(http://www.paloaltonetworks.com)

Latest Blogs

New App-IDs for May are ready! (https://live.paloaltonetworks.com/t5/Community-Blog/New-App-IDs-for-May-are-ready/ba-p/213496)
New App-IDs for May are ready now. Palo ...

Ignite: What's in it for me? (https://live.paloaltonetworks.com/t5/Ignite-Blog/Ignite-What-s-in-it-for-me/ba-p/213292)
Ignite. What's all the fuss? You've got ...

Got Questions? #GetAnswers (https://live.paloaltonetworks.com/t5/Community-Blog/Got-Questions-GetAnswers/ba-p/213291)
Our community Sentinel offers tips and t...

Events

Ignite: What's in it for me? (https://live.paloaltonetworks.com/t5/Ignite-Blog/Ignite-What-s-in-it-for-me/ba-p/213292)
Ignite. What's all the fuss? You've got ...

We've got a bigger board at Ignite '18 (https://live.paloaltonetworks.com/t5/Ignite-Blog/We-ve-got-a-bigger-board-at-Ignite-18/ba-p/212139)
Does this crowded board look familiar to...

Ignite '18 Call for Papers Extended 'til February 12 (https://live.paloaltonetworks.com/t5/Ignite-Blog/Ignite-18-Extended-til-February-12/ba-p/196088)
Haven't quite put the finishing touches ...

Connect

(https://www.linkedin.com/company/palo-alto-

(https://twitter.com/PaloAltoNetworks) (https://www.youtube.com/user/PaloAltoNetworks) (https://www.slideshare.net/PaloAltoNetworks) (https://www.facebook.com/PaloAltoNetworks)

(https://ignite.paloaltonetworks.com/usa/forms/2018_regform.html)