

January 2019

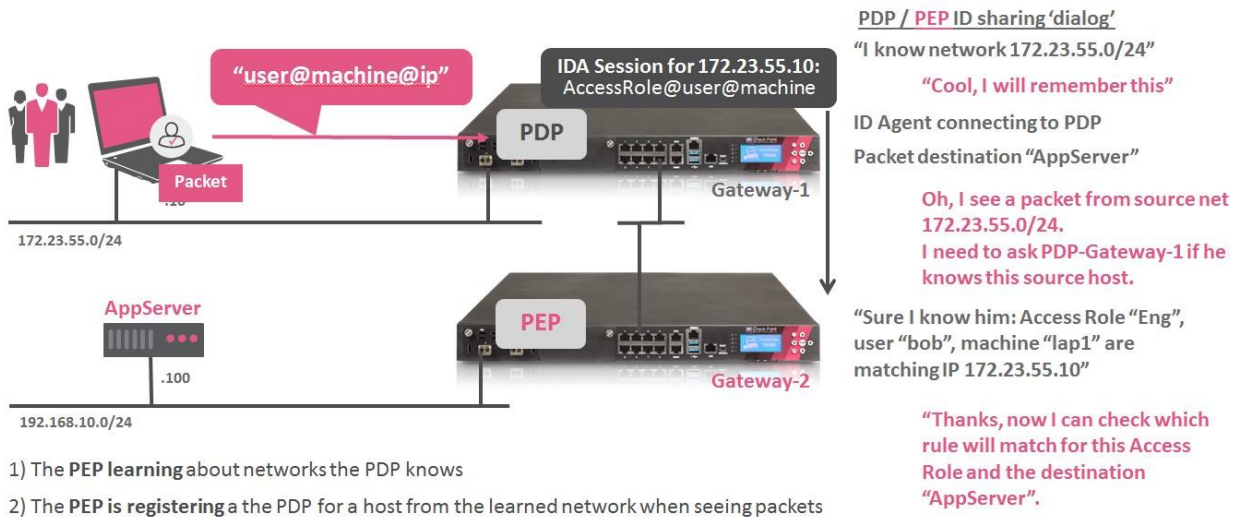
Check Point Identity Sharing

This document outlines some details about Identity Sharing mechanism between the Policy Decision Point (PDP) and Policy Enforcement Point (PEP):

The PEP gateway registers on the PDP gateway asking the list of networks this PDP may have identities for. The PDP sends a list of networks to the PEP gateway in the registration process. The PDP gateway will perform the group membership query once a login event is observed and calculated the Access Role object matching. It will then create an Identity Awareness Session related to the source IP address.

In case a packet sourced by one of the networks learned from the PDP will arrive on the PEP gateway the PEP gateway will query the PDP for the current identities related to this source IP address.

The PDP will provide the relevant Access Role and the PEP will perform the rule base matching allowing or blocking the packet accordingly.



Monitoring Identity Sharing from PDP to PEP

Understand the list of PEP(s) the PDP has a sharing relationship with.

```
[Expert@r8010gw:0]# pdp connections pep
```

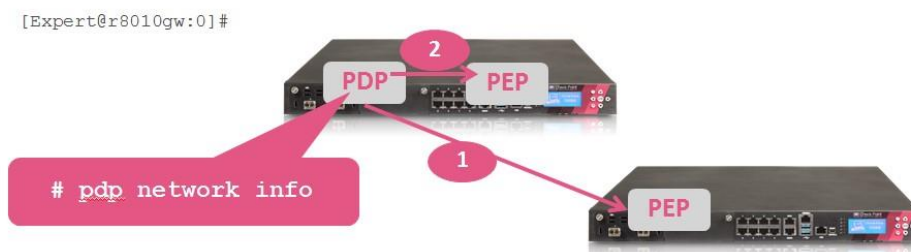
	Direction	IP	Port	Name	Type	Status	Location	IPv6 Supported
1	Incoming	172.23.55.190	28581	R80.10-External	Single Gateway	Connected	Remote	No
2	Outgoing	127.0.0.1	15105	R80.10-Gateway	Single Gateway	Connected	Locally	No
3	Outgoing	172.23.55.190	15105	R80.10-External	Single Gateway	Connected	Remote	No



Understand the list of networks the PDP knows about

```
[Expert@r8010gw:0]# pdp network info
```

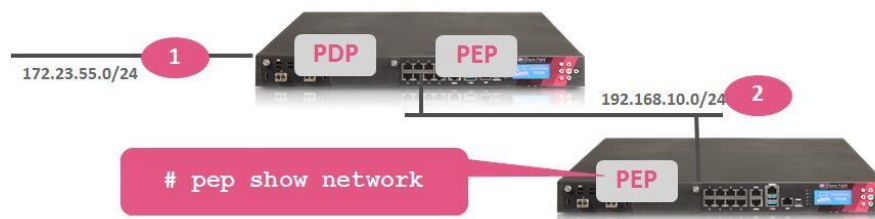
	Network	Mask	Creation Time	Last update time	Last updating IP
1	172.23.55.0	255.255.255.0	Sun Jul 8 16:36:22 2018	Sun Jul 15 15:57:28 2018	172.23.55.190
2	192.168.10.0	255.255.255.0	Sun Jul 8 16:36:11 2018	Sun Jul 15 15:57:34 2018	192.168.10.100



Understand the list of networks the PEP has been made aware of by the PDP

```
Expert@R80.10-External:0]# pep show network pdp
```

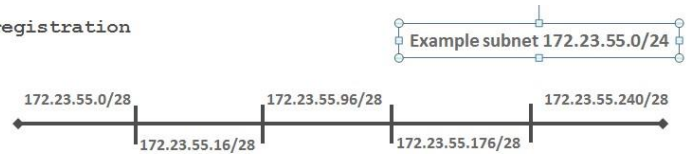
	Network	Mask	Related PDPs
1	172.23.55.0	255.255.255.0	<192.168.10.11,0>;
2	192.168.10.0	255.255.255.0	<192.168.10.11,0>;



Understand the list of networks the PEP has performed a registration process for

```
[Expert@R80.10-External:0]# pep show network registration
```

Network	Mask
172.23.55.0	255.255.255.240
192.168.10.0	255.255.255.240
172.23.55.96	255.255.255.240
192.168.10.96	255.255.255.240
172.23.55.176	255.255.255.240
172.23.55.16	255.255.255.240
172.23.55.240	255.255.255.240



Larger networks are divided into subnets keeping kernel tables small



```
# pep show network registration
```

```
[Expert@R80.10-External:0]#
```

Understand the list of users known on the PEP

```
Expert@R80.10-External:0]# pep sh user all
```

```
Command: root->show->user->all
```

ID (PDP; UID)	Username@Machine	CID (IP, PacketID)	PT
192.168.10.11 :00000000; e70fc1f8	<u>Administrator@win-victim</u>	192.168.10.100	, 00000000 -
192.168.10.11 :00000000; 7a4037ac	<u>Administrator@client-vm</u>	172.23.55.10	, 00000000 -
192.168.10.11 :00000000; 38ea518b	<u>Administrator@win-dc</u>	172.23.55.190	, 00000000 -
192.168.10.11 :00000000; d7bb12cc	<u>Administrator@win-dc</u>	192.168.10.11	, 00000000 -

```
[Expert@R80.10-External:0]#
```



```
# pep show users all
```

[Protected] Distribution or modification is subject to approval