



Identity Awareness Best Practices

PhoneBoy | Cyber Security Evangelist

CheckMates Live Series 2024

YOU DESERVE THE BEST SECURITY

Important Security Update

- Stay protected against CVE-2024-24919
 - Relevant for Remote Access VPN Configurations
- Patches available for:
 - Quantum Appliances (R77.30+): <https://support.checkpoint.com/results/sk/sk182336>
 - Quantum Spark Appliances: <https://support.checkpoint.com/results/sk/sk182357>
- Fixes included in recommended JHF for R81+
- See related discussions on CheckMates:
 - <https://community.checkpoint.com/t5/General-Topics/Important-security-update-stay-protected-against-VPN-Information/m-p/215310/highlight/true#M35533>
 - <https://community.checkpoint.com/t5/Product-Announcements/Best-Practices-to-Patch-and-Remediate-CVE-2024-24919/ba-p/216287>

Housekeeping

- Use Q&A panel for questions, not Chat
- You can upvote there questions from others
- Speak your mind
- Raise a hand to ask a question
- We are recording
- We will share materials and videos

Agenda

- Understanding identity-based security
- Design principles
- Scaling customer scenarios
- Coming next

Drivers & Concepts

“Access must be **authenticated** and **authorized** only when needed, when the **device was checked for compliance** and **for the time it takes to complete the task.**”

CISO of a mid-sized enterprise, Italy

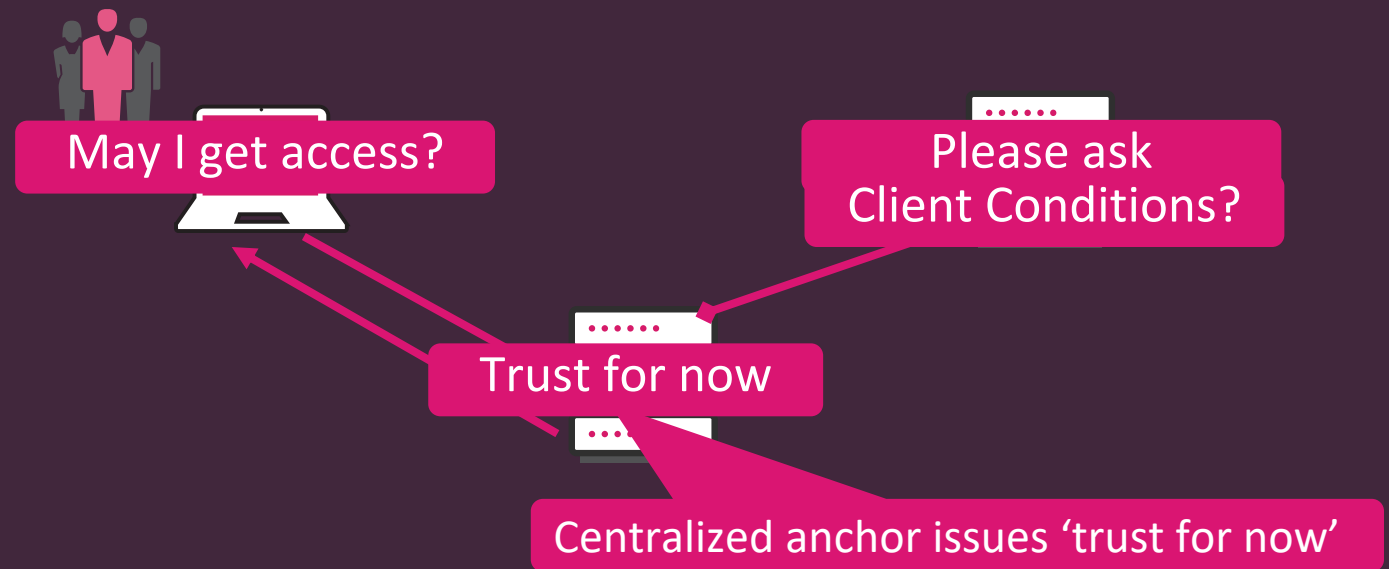
Zero Trust

The Principle

Authentication and Authorization

The 'Explicit Trust Model'

Trust based on continuous verification



For sure you know:

Default lifetime of a **KERBEROS** ticket: **10 hours**

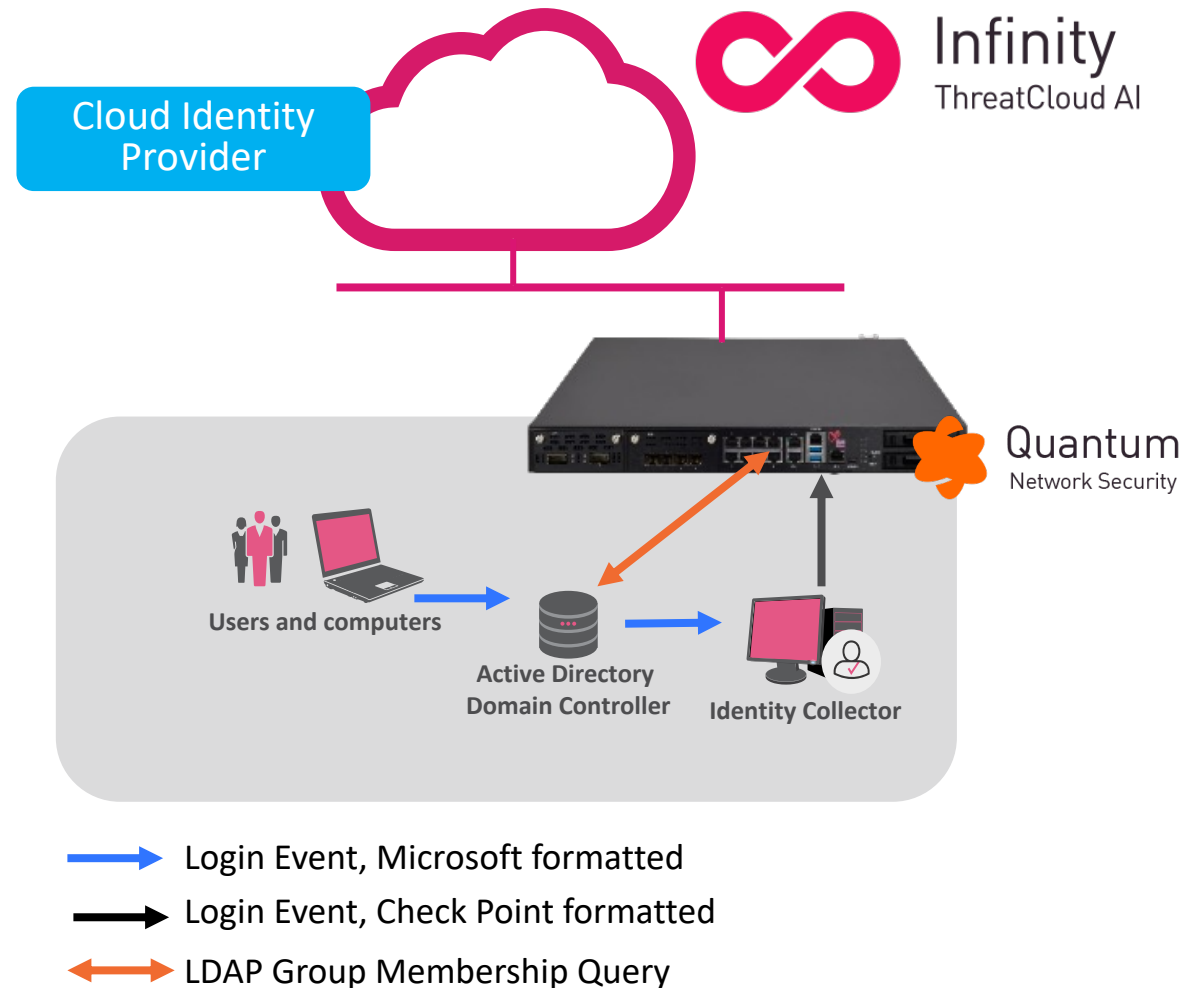
Default lifetime of a **SAML** token: **1 hour**

Identity Providers such as Microsoft Entra ID (Azure AD) support compliance management

Identity Based Security

Achieving visibility about users and machines

- Support for on-prem and cloud centric ID providers
 - User and machine attributes are consumed from identity sources and enforced on the gateway
 - Example of identity sources
 - Active Directory
 - Cisco ISE
 - RADIUS Accounting
 - Web API
 - SAML Identity Providers
 - Identity Agents

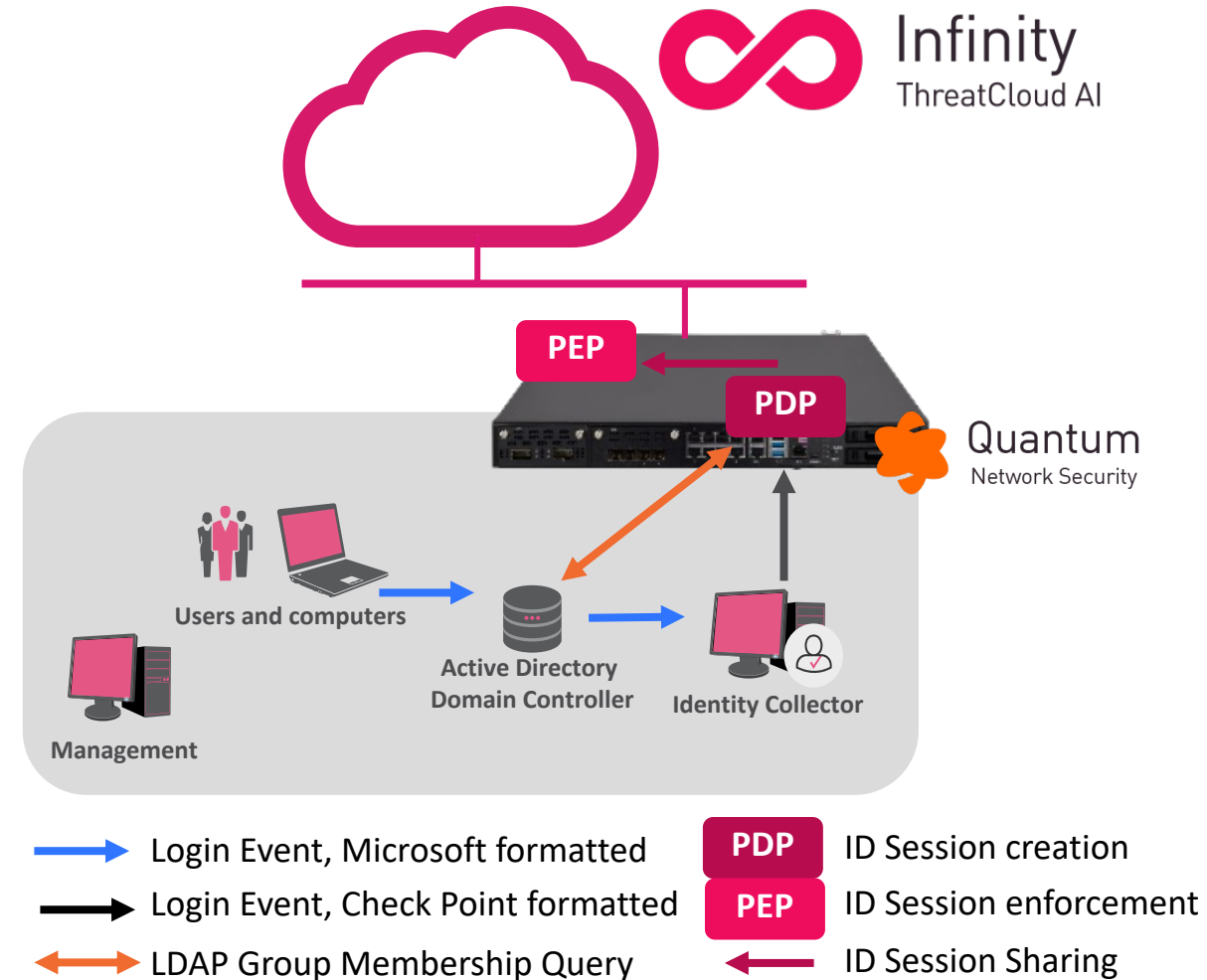


Identity Based Security

On-premises Identity Sources

Mapping IP addresses to users and machines

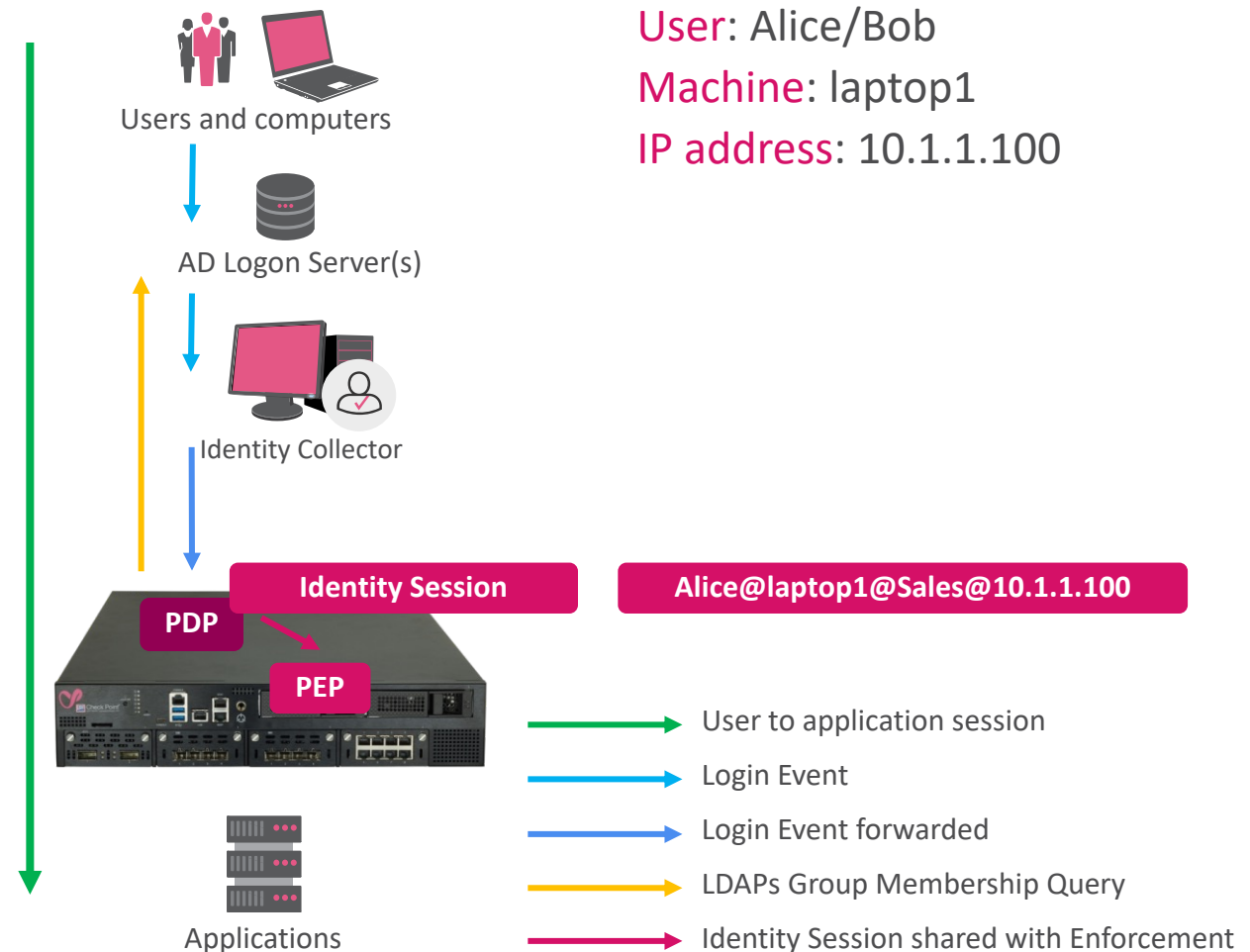
- Security gateway learns...
 - User login event on the computer
 - Group membership of users
- Security gateway maintains...
 - Tables mapping IP addresses to users and machines: Identity Session tables
- Security gateway PDP instance shares...
 - Identity sessions with PEP instance on same and/or remote gateways
- Security gateway enforces ...
 - Security policy based on identity sessions



Identity Based Security

Understanding Identity Sessions

- Users, machines and applications trusted in AD
- Login event taking place
- Learning and forwarding login event
- Learning the group membership
- Creating the identity session
- Sharing the identity session
- Enforcing security



Identity Based Security

Access Control and Threat Prevention based on identities

The security is enforced using an **Access Role** object in the rule base

Name	Source	Destination	Services & Applications	Action	Track
File sharing	EngineeringGroup	adserver	microsoft-ds	Accept	Log

The **Access Role** object has four dimensions

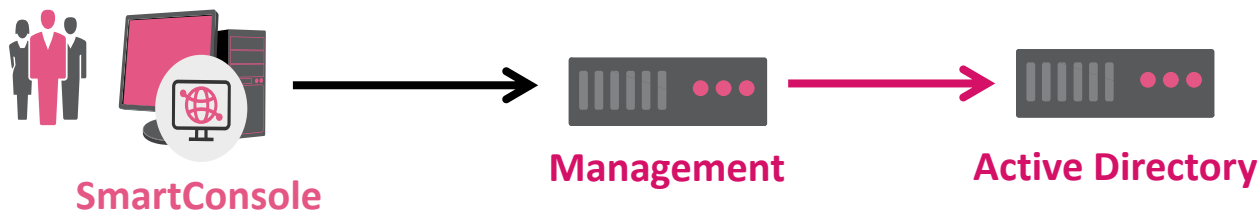
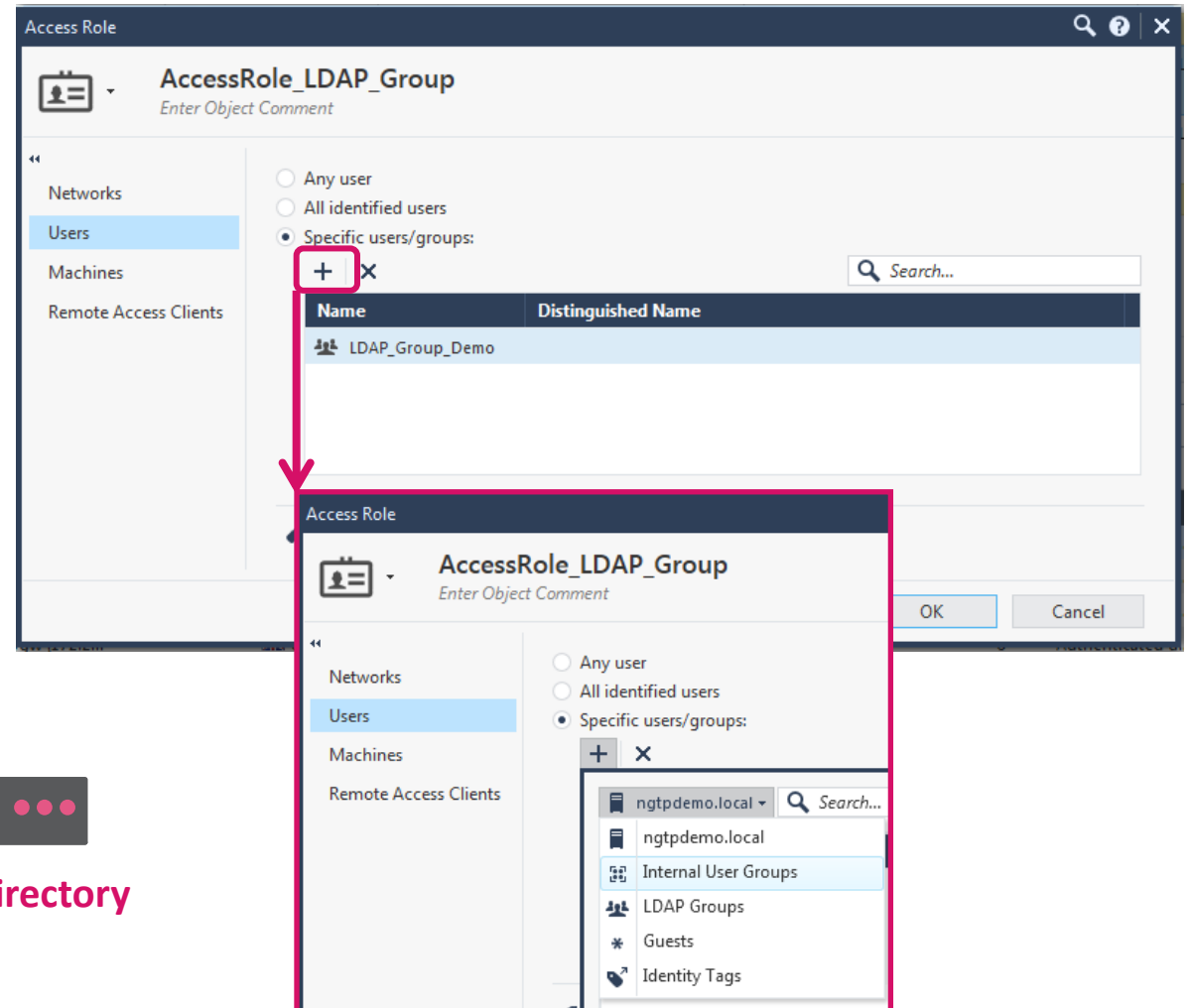
The image displays three sequential screenshots of the 'EngineeringGroup' configuration window in a security management console. Each window shows a different dimension selected in the left-hand navigation pane:

- Left Screenshot:** The 'Networks' dimension is selected. The main area shows radio buttons for 'Any Network' (selected) and 'Specific Networks:'. A table below is empty.
- Middle Screenshot:** The 'Users' dimension is selected. The main area shows radio buttons for 'Any user', 'All identified users', and 'Specific users/groups:'. The 'Specific users/groups:' option is selected, and a table lists one entry: 'EngGroup' with distinguished name 'CN=EngGroup,CN=Users,DC=ngtppdemo,DC=local'. A red arrow points to this entry.
- Right Screenshot:** The 'Machines' dimension is selected. The main area shows radio buttons for 'Any machine' (selected), 'All identified machines', and 'Specific machines/groups:'. The table below is empty and contains the text 'No items found'. A red arrow points to the table area.

A red callout box at the bottom of the screenshots contains the text: "Combining user and machine dimensions allows to describe different use cases: 'User1 on User1Laptop' and 'User1 on Any machine'".

Creating Access Role Objects

- Identity based access control and threat prevention is enforced using the **Access Role** object
 - Clicking on the '+' allows adding users/machines from various sources such as Active Directory domains, LDAP groups or Identity Tags
 - Selecting Active Directory domain(s) initiates the **management server** to contact the **Active Directory logon server** configured in the relevant LDAP Account Unit object



See [sk115677](#) for details

Identity Awareness – Enforcement

- Make sure the **Identity Role** is learned for the given user

Log Details

Log In
Successful Login of eng1 (eng1): User Identity Propagation

Details

Source	192.168.169.115
	eng1 (eng1)
Action	Log In
Blade	Identity Awareness
Time	Today, 18:37:58

Identity

Authentication Sta...	Successful Login
Identity Source	Identity Collector (Active Directory)
User	eng1 (eng1)
Source User Group	ad_group_EngGroup All Users
Roles	EngineeringGroup

Device

Endpoint IP	192.168.169.115
Domain Name	ngtptdemo

Session

Session ID	5c11d9df
Authentication Me...	User Identity Propagation

Actions

Report Log [Report Log to Check Point](#)

More

Type	Log
Origin	gwr8010
Severity	Informational
Confidence Level	N/A

```
[Expert@gwr8010:0]# pep sh us que usr eng1  
Command: root->show->user->query
```

```
PDP: <127.0.0.1, 00000000>; UID: <25e8eba1>
```

```
=====  
Client ID      : <192.168.169.115, 00000000>
```

```
Authentication Key : <Unavailable>
```

```
Brute force counter: 0
```

```
Username       : eng1
```

```
Machine name   :
```

```
User groups    : <Unavailable>
```

```
Machine groups : <Unavailable>
```

```
Compliance    : <Unavailable>
```

```
Identity Role  : <EngineeringGroup>
```

```
Time to live   : 43230
```

```
Cached time    : 86400
```

```
TTL counter    : 43170
```

```
Time left      : 43210
```

```
Last update time : Thu Mar 30 18:37:58 2017
```

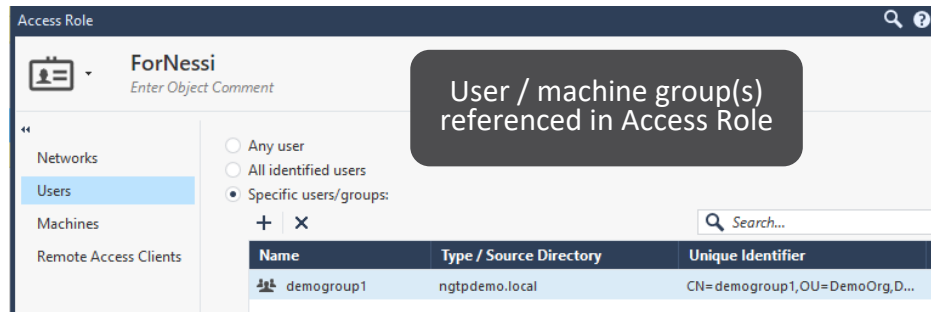
Let's Review

- Login events are learned
- ID Sessions are created
- Access Role objects match

Group Membership

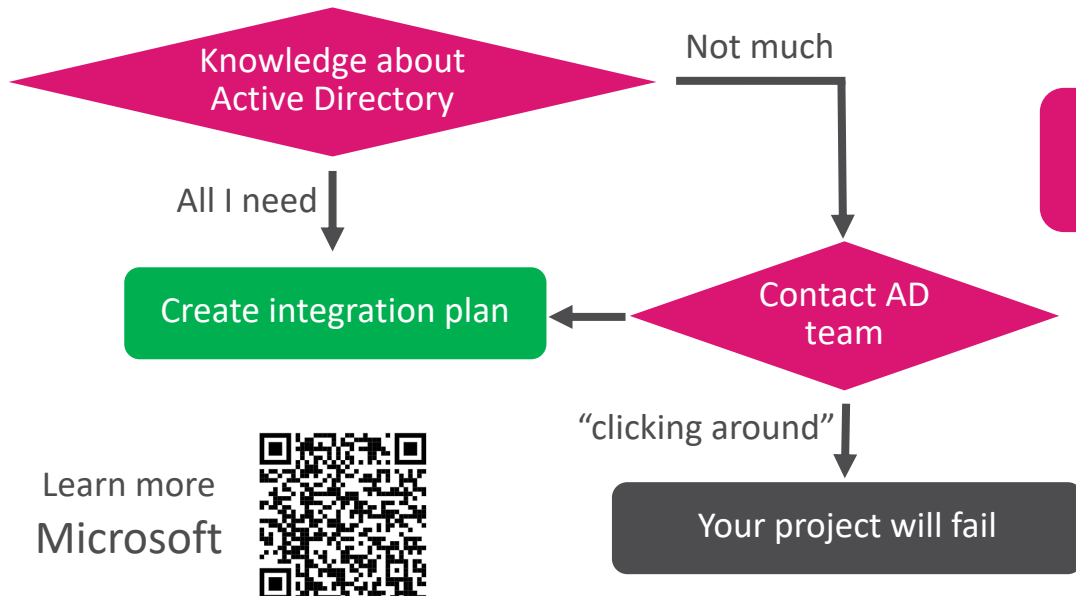
Understanding Group Membership

Access Role objects contain groups

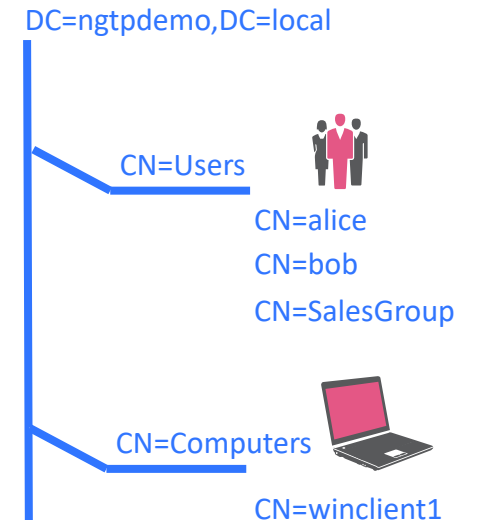
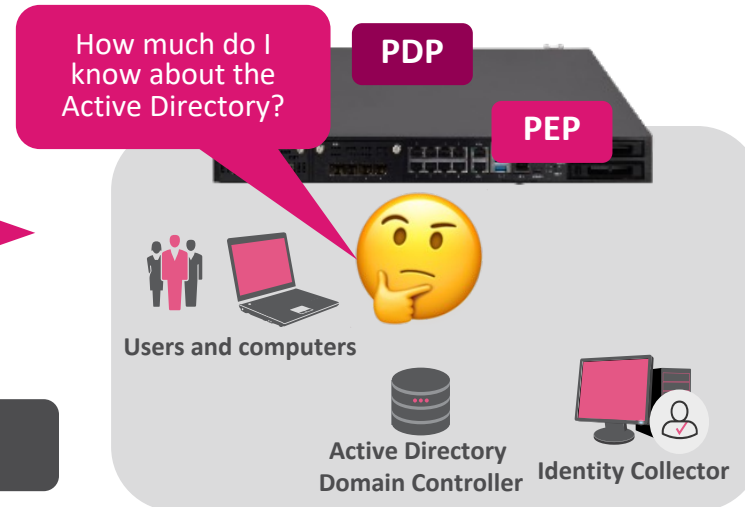


Active Directory Groups have a scope

Scope	Granting permissions
Universal	Any domain in same or trusting forests
Global	< not relevant for integration; read Microsoft documentation and sk134292 >
Local Domain	Within same domain

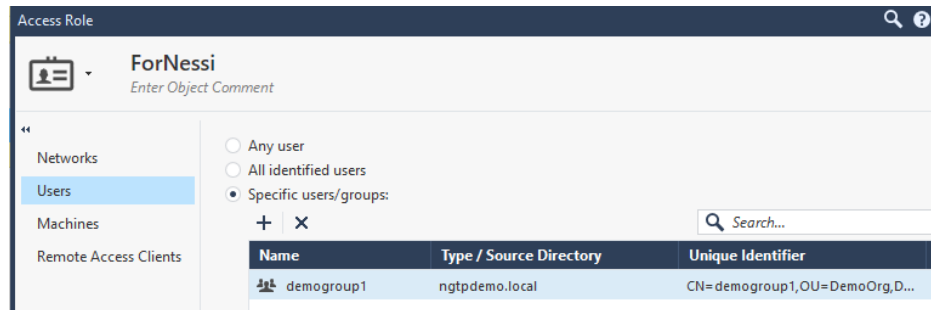


Learn more
Microsoft



Understanding Group Membership

Successful group membership retrieval is required

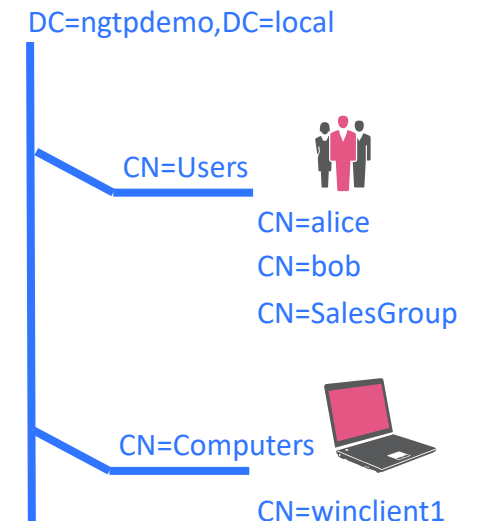
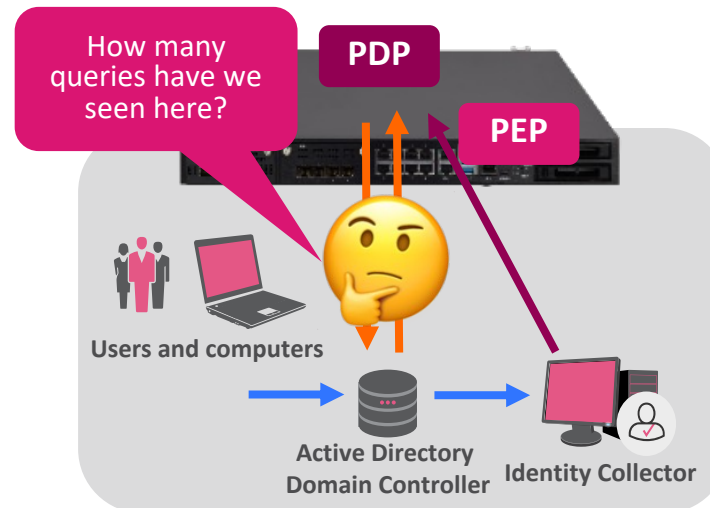


Queries are impacting AD Servers and PDP

- PDP may consume a lot of CPU cycles
- AD Server CPU may get loaded

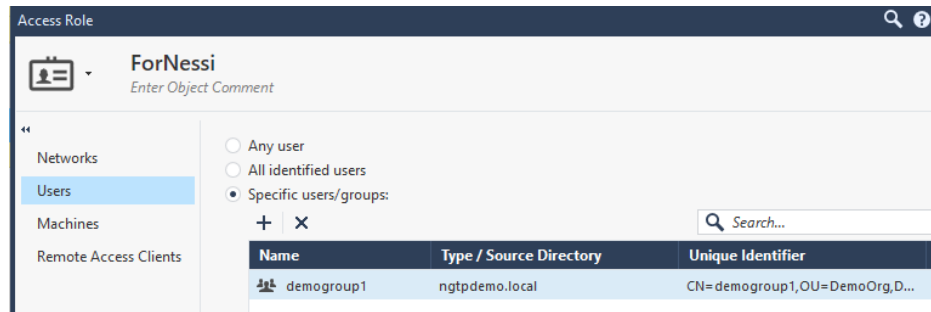
Carefully document these facts:

- How many login events are happening?
- How many groups one user belongs to?
- Are there nested groups?
If yes, what's the nesting level?



Understanding Group Membership

Successful group membership retrieval is required

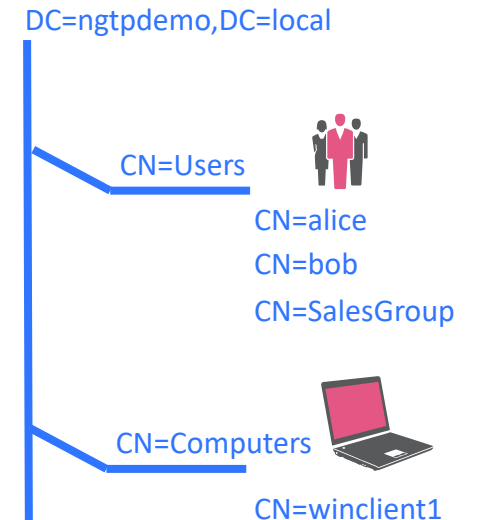
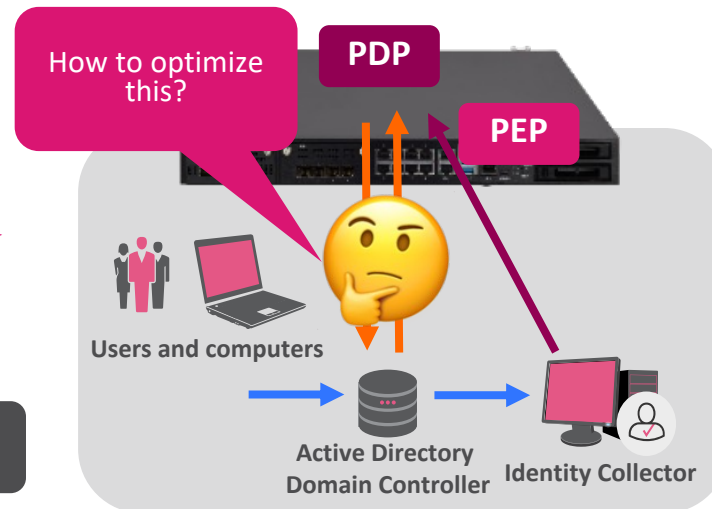
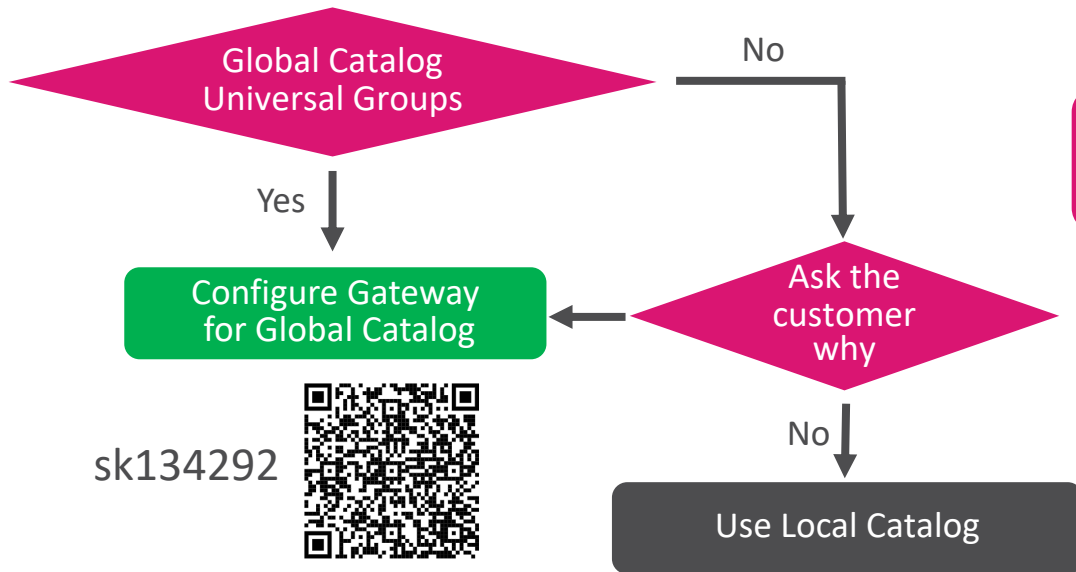


Group information on AD Servers

- Local catalog (holding all attributes of an object)
LDAP TCP/389 – LDAPs TCP/636
- Global catalog (holding a smaller number of attributes)
LDAP TCP/3268 – LDAPs TCP/3269



‘...quickly find objects...’



Understanding Group Membership

Understanding Nested Groups

- By default the gateway raises recursive queries until it has learned all groups

```
# pdp nested_groups status
Nested groups status - Enabled
Nested group mode - 1: Recursive query method. Depth: 20
Auto Tune status - Disabled
```

Access Role object

name	Type / Source Directory	Unique Identifier
demogroup1	ngtpdemo.local	CN=demogroup1,OU=DemoOrg,D...

LDAP queries

```
searchRequest(2) "dc=ngtpdemo,dc=local" wholeSubtree
searchRequest(3) "cn=smartworkersdemo,ou=demoorg,dc=ngtpdemo,dc=local" baseObject
searchRequest(4) "cn=demogroup3,ou=demoorg,dc=ngtpdemo,dc=local" baseObject
searchRequest(5) "cn=demogroup2,ou=demoorg,dc=ngtpdemo,dc=local" baseObject
searchRequest(6) "cn=demogroup1,ou=demoorg,dc=ngtpdemo,dc=local" baseObject
```

Impact?



Nest Groups Improved Capabilities

- Administration guide:

Active Directory



sk128212



Name	Active Directory Domain Services Folder
demogroup1	ngtpdemo.local/DemoOrg

Name	Active Directory Domain Services Folder
demogroup2	ngtpdemo.local/DemoOrg

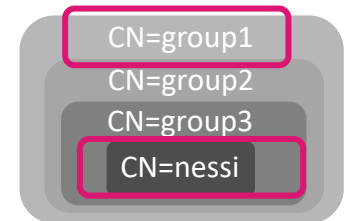
Name	Active Directory Domain Services Folder
demogroup3	ngtpdemo.local/DemoOrg
Domain Users	ngtpdemo.local/Users
SmartWorkersDemo	ngtpdemo.local/DemoOrg

DC=ngtpdemo,DC=local

OU=DemoOrg



CN=nessi



User

Understanding Group Membership

Understanding Nested Groups

- Using “mode 4” allows learning all groups at once
- Consult with Active Directory Administration team before enabling it – it may impact load!

```
[Expert@cpcluster1:0]# pdp nested_groups __set_state 4
```

```
Nested groups status - Enabled
```

```
Nested group mode - 4: One query per-user method (get groups from the branch specified in the LDAP account unit)
```

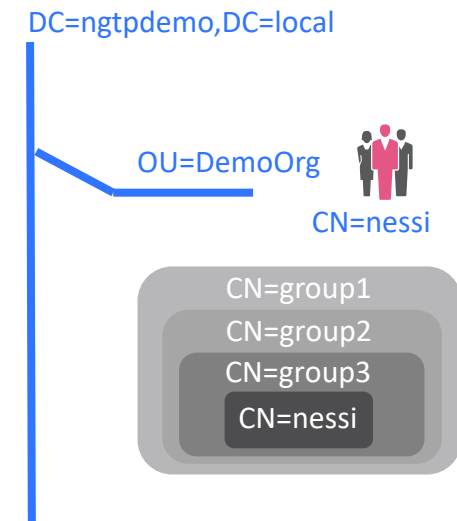
```
Auto Tune status - Disabled
```

No.	Time	Source	Destination	Protocol	Length	Info
7	0.003187	10.0.1.4	10.0.3.4	LDAP	789	searchRequest(2) "dc=ngtpdemo,dc=local" wholeSubtree
9	0.004716	10.0.1.4	10.0.3.4	LDAP	253	searchRequest(3) "DC=ngtpdemo,DC=local" wholeSubtree

Nested Groups – Improved Capabilities – sk128212

- Auto-Tune (disabled by default) allows the PDP finding the most optimal setting for nested group configurations

sk128212



Group Membership

Understanding Active Directory integration

Gaia CLI command to understand group membership of user 'adqueryuser'

```
# ldapsearch -h 10.0.3.4 -p 389 -D "CN=ldapsearch,CN=Users,DC=ngtppdemo,DC=local" -w "P4ssw0rdCP" -b "DC=ngtppdemo,DC=local" -s sub "CN=adqueryuser"
```

Response from Active Directory Domain Controller

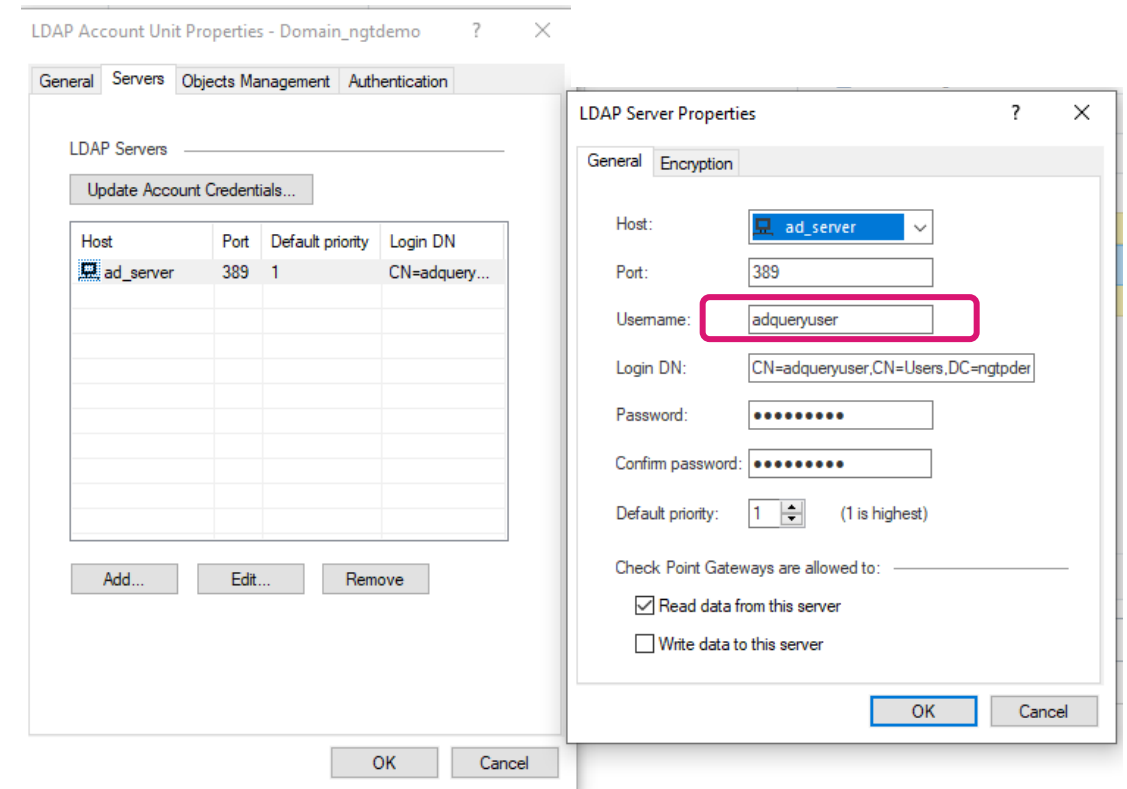
CN=adqueryuser,CN=Users,DC=ngtppdemo,DC=local

[...]

distinguishedName=CN=adqueryuser,CN=Users,DC=ngtppdemo,DC=local

[...]

memberOf=CN=Domain Admins,CN=Users,DC=ngtppdemo,DC=local



Let's Review

- Group membership must be learned
- Learning has cost
- Best Practice: Global Catalog
- Check Group Consolidation

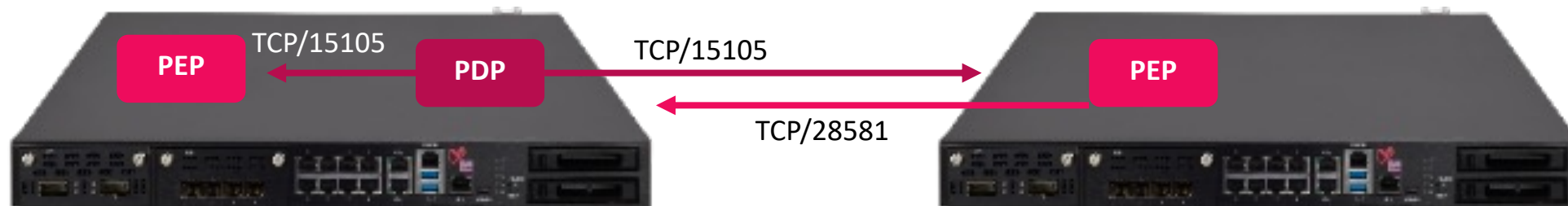
ID Session Sharing

- ID Sessions are maintained in tables
- Associating IP addresses with users, machines, groups and Access Role objects
- ID Sessions can (and often must) be shared

Identity Session Sharing

From PDP to enforcing gateway (PEP) instance

- Gateway running PDP and PEP
 - All identity sessions are shared immediately with enforcing instance (PEP)
 - “Push” Identity Sharing
 - TCP communication via loopback interface
- Across multiple gateways
 - Enforcing gateway subscribes to PDP for learning about ID Sessions (TCP/28581)
 - Requests ID Session based on IP source address, when a packet arrives
 - “Smart-Pull” Identity Sharing



Identity Session Sharing

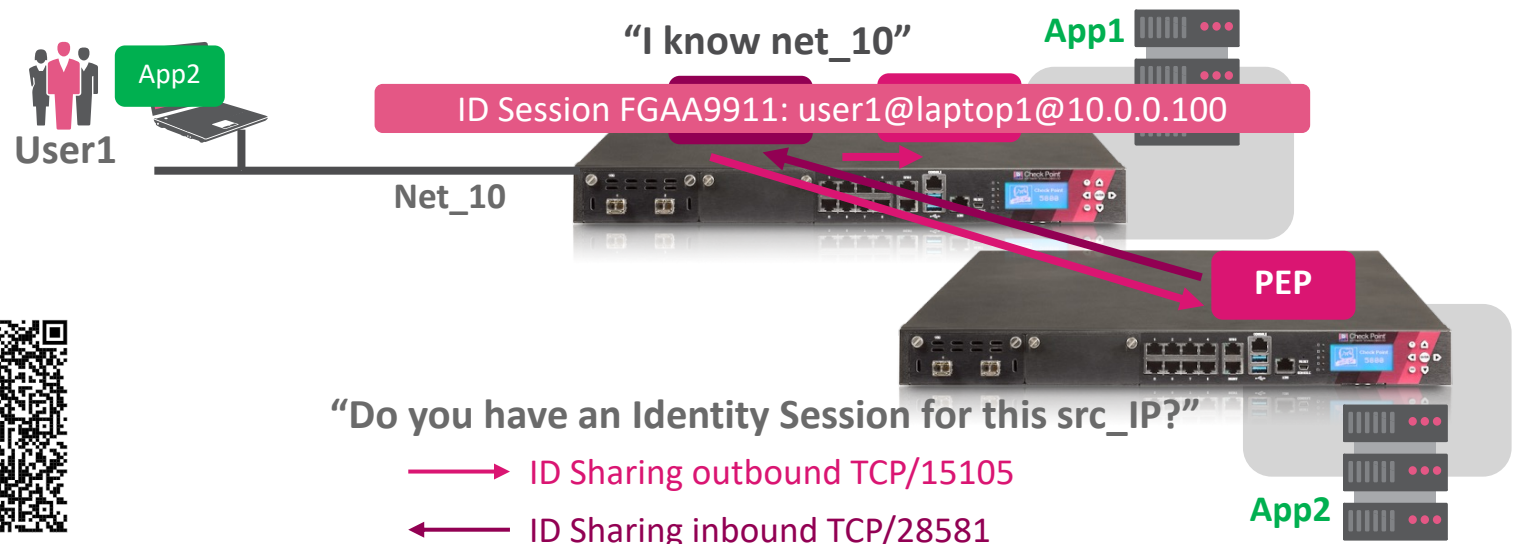
From PDP to enforcing gateway (PEP) instance

- Identity Sessions are created on the PDP instance based on login events
- All Identity Sessions known by a PDP are shared with PEP instance running on the same host
- Remote PEP instances learn Identity Sessions only when required – when seeing a packet of interest
 - Remote PEP registers at PDP and learns which networks this PDP knows about (trust us based on SIC certificates)
 - Packet arriving from source net: Identity Session related information is requested
 - Security is applied based on the Identity Session

ID Sharing sk149255



Identity Awareness Administration Guide



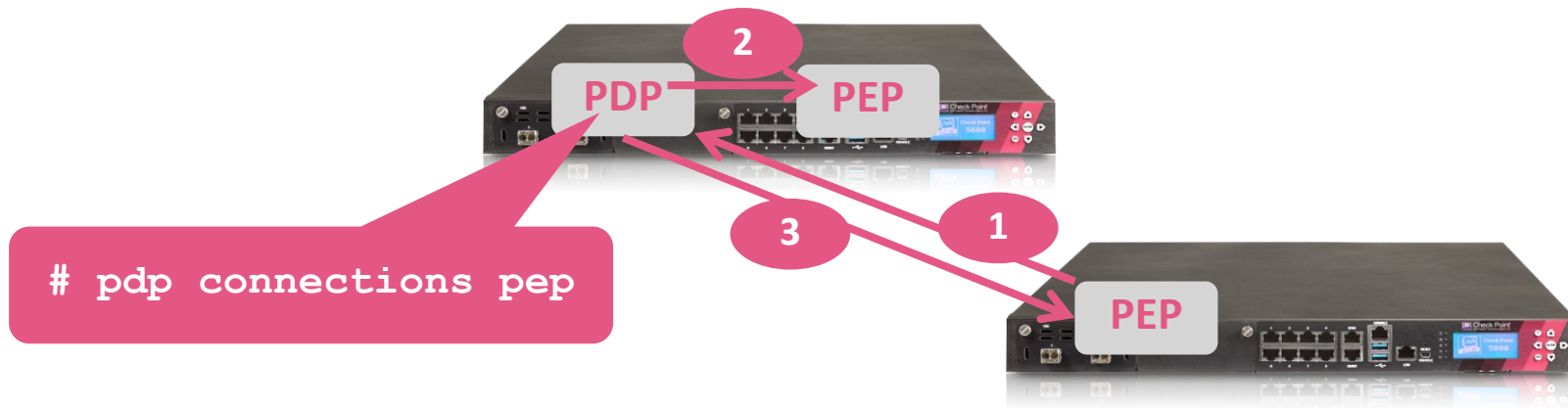
Identity Session Sharing

Two distinct TCP connections

Show the list of PEPs the PDP has a sharing relation 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



Trust between the gateways is based on their SIC certificates

Sharing ID Sessions across domains and long distances

- How can we share ID Sessions between gateways managed by different management servers domains?
- Trust between PDP and PEP is based on the SIC certificate issued by the management server/domain
- ID Broker is sharing identities using TLS

Let's Review

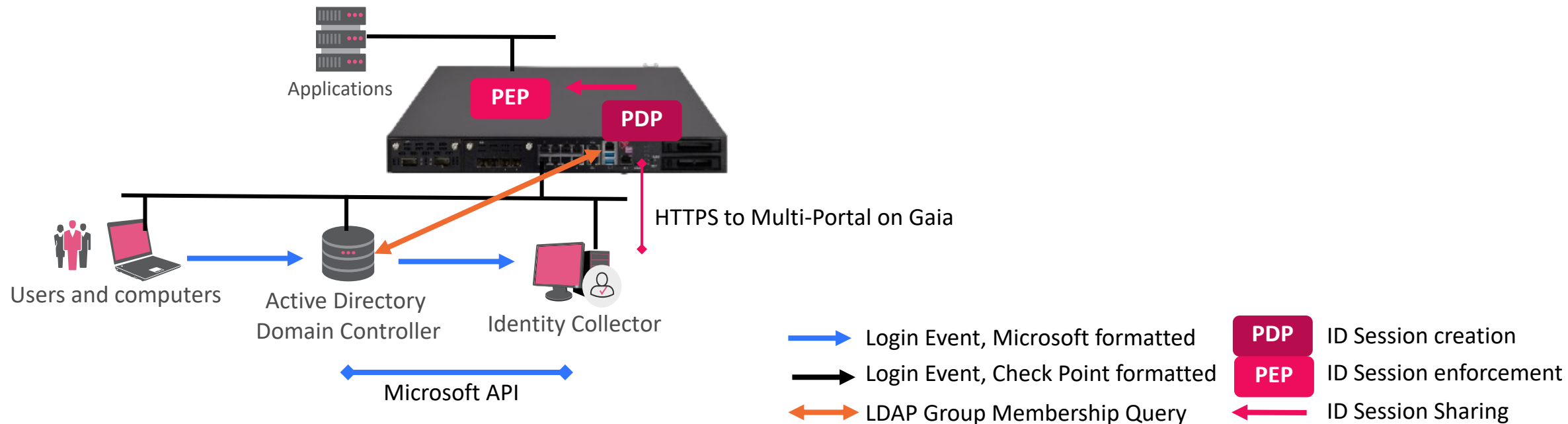
- Enforcing gateway subscribes to PDP
- Request for Identity Sessions on demand
- ID Session is shared from PDP to PEP
- ID Sessions can be shared across domains using ID Broker
- Security is enforced based on identity

Identity Sources

Identity Collector

Best Practices for integrating to on-premises directory services

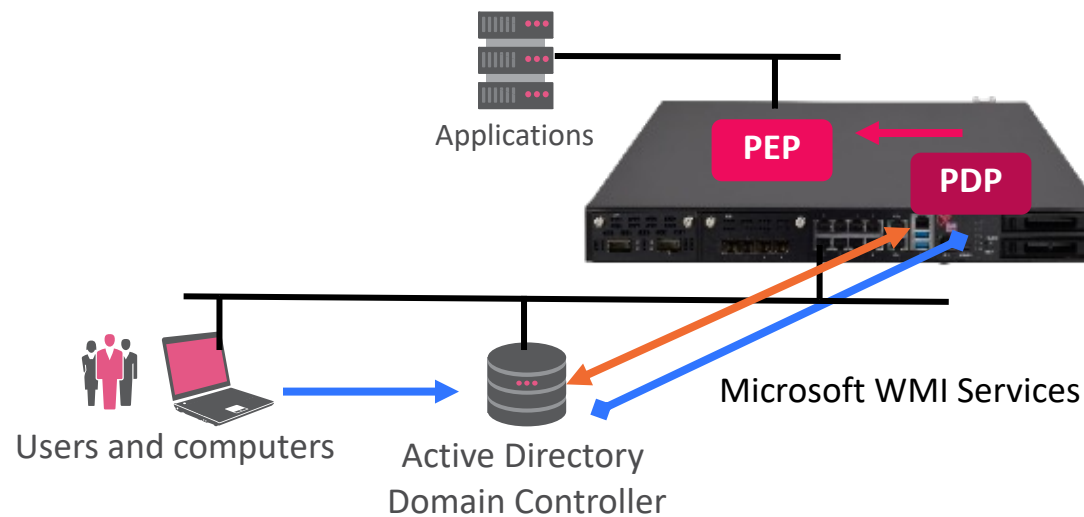
- Application running on a Windows Server
- The Windows server does not need to be part of the domain
- An 'Event Log Reader' account role is sufficient to subscribe to Security Events API on AD Server (remember AD Query requires 'Server Administrator' account role)
- ID Collector consumes login events from Microsoft AD, Cisco ISE, Syslog and NetIQ eDirectory



What About AD Query?

No longer a best practices solution

- Microsoft WMI Services is subscribed by the gateway on the AD Server
- An 'Server Admin' account role required on the gateway
- WMI is a resource intense service on the Windows server: a high rate of login events leads to high load



SmartConsole: LDAP Account Unit

The screenshots show the configuration of an LDAP Account Unit in SmartConsole. The 'General' tab of the 'LDAP Account Unit Properties' window shows the following settings:

- Name: Domain_ngtdemo
- Comment: on premises Active Directory
- Color: Black
- Profile: Microsoft_AD
- Domain: ngtpdemo.local
- Account Unit usage:
 - CRL retrieval
 - User management
 - Active Directory Query
- Additional configuration:
 - Enable Unicode support
 - Active Directory SSO configuration

The 'Servers' tab shows a table of LDAP Servers:

Host	Port	Default priority	Login DN
ad_server	389	1	CN=adqueryuser...

The 'LDAP Server Properties' dialog for 'ad_server' shows:

- Host: ad_server
- Port: 389
- Username: adqueryuser
- Login DN: CN=adqueryuser,CN=Users,DC=ngtpder
- Password: [Redacted]
- Confirm password: [Redacted]
- Default priority: 1 (1 is highest)
- Check Point Gateways are allowed to:
 - Read data from this server
 - Write data to this server

- ➡ Login Event, Microsoft formatted
- ➡ Login Event, Check Point formatted
- ↔ LDAP Group Membership Query
- PDP** ID Session creation
- PEP** ID Session enforcement
- ← ID Session Sharing

Design Guidelines ID Collector

Follow sk179544

- The sk179544 is covering:
- How do I migrate from AD Query to ID Collector
- How can I understand login events?
- What are the CLI commands I need to know?
- Topics are explained in short videos
- Network diagram and packet flow explained

Table of Contents

- (1) Introduction
- (2) Multiple Logons on the same machine
- (3) Advantages of Identity Collector over AD Query
- (4) Integrating to Identity Collector - Learning Login Events
- (5) Migrating to Identity Collector as identity source in addition to AD Query
- (6) Migrating to Identity Collector - Disabling AD Query
- (7) Migrating to Identity Collector - Environments spreading across multiple sites - part I
- (8) Migrating to Identity Collector - Environments spreading across multiple sites - part II
- (9) Understanding Group-Retrieval
- (10) Deployment Guidelines

Find detailed configuration and monitoring guidelines on sk179544

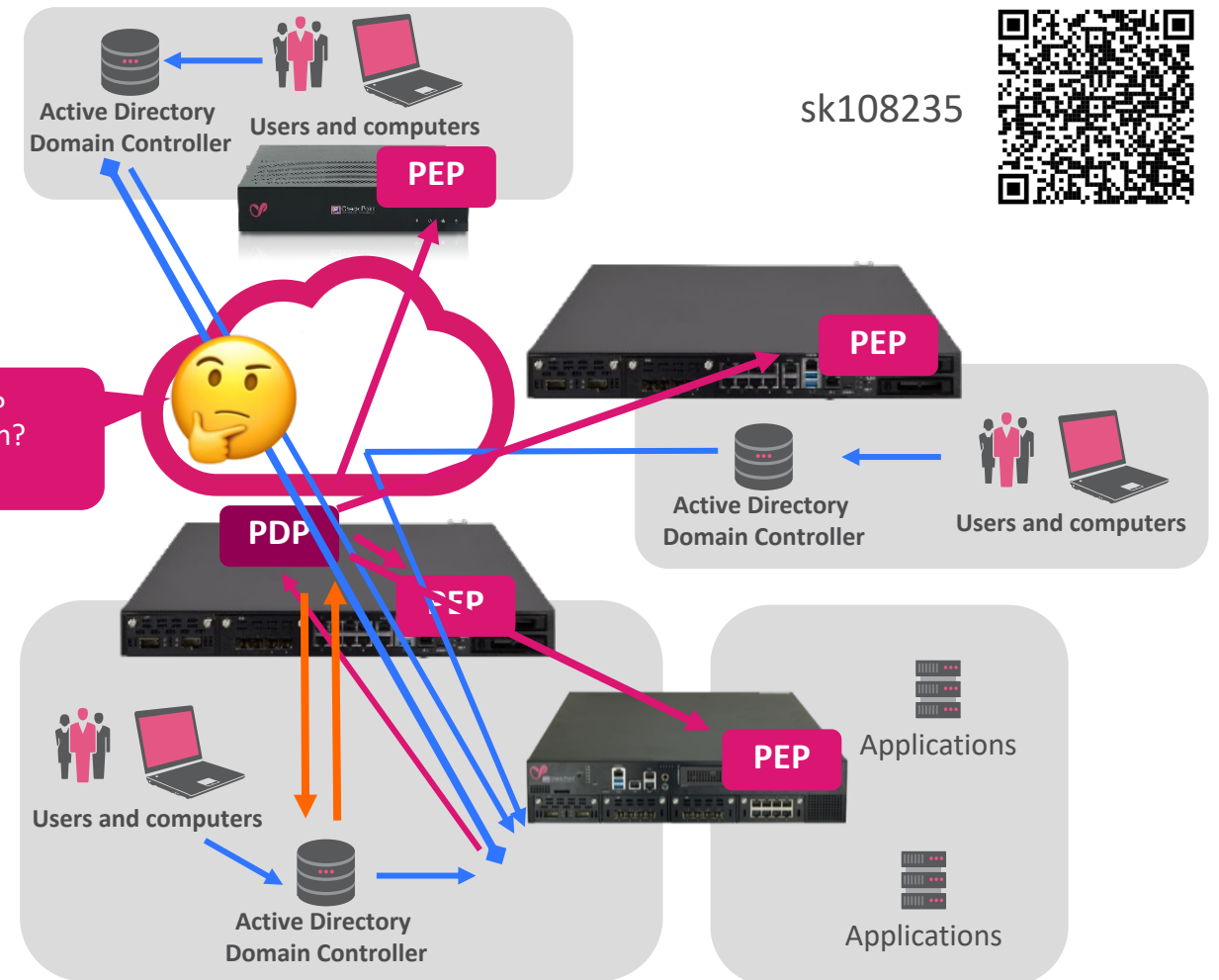
Design Guidelines ID Collector

Follow sk179544

Respect sk108235

- Up to 1900 login events/sec can be learned from up to 35 Active Directory Domain Controllers
- One ID Collector may learn login events from multiple sites
- Communication based on DCE/RPC
- Place ID Collector at site with highest number of login events/sec
- Plan Identity Sharing

NAT is breaking IP address == user / machine mapping of the Identity Session!



Let's Review

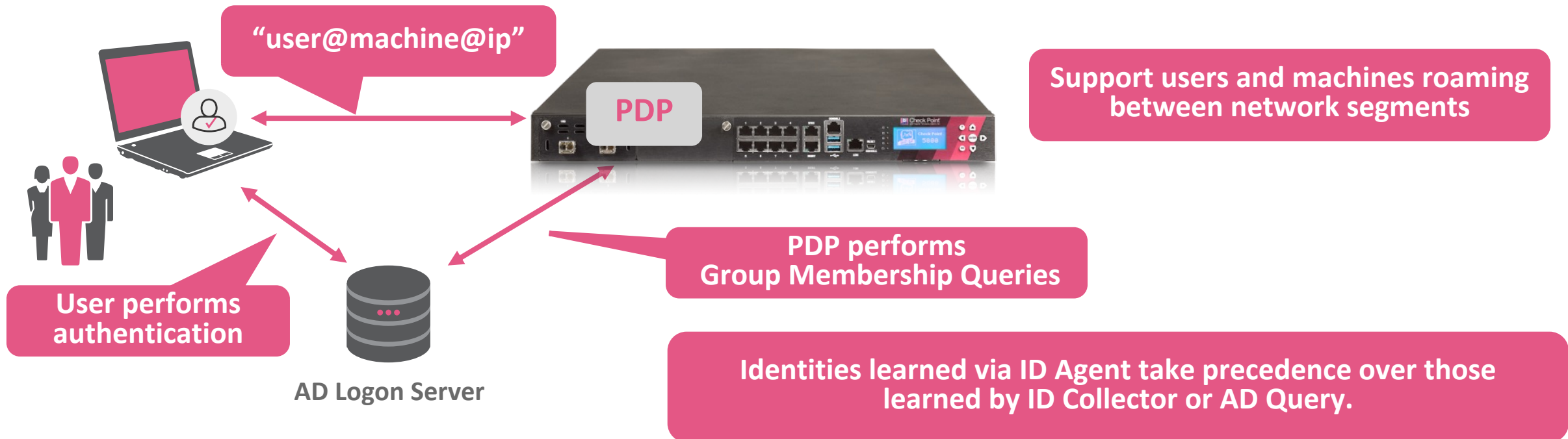
- ID collector is the best practice for integrating to on-prem directory services

Identity Agent

Client based solution for Windows and macOS

Identity Agent

- Using the ID Agent customers can manage roaming users (change of source IP Addresses)
- ID Agents are connecting to the PDP, advising it about the Login Event “user@machine@ip_address”
- “Keep alive” packets are sent from ID Agent to PDP

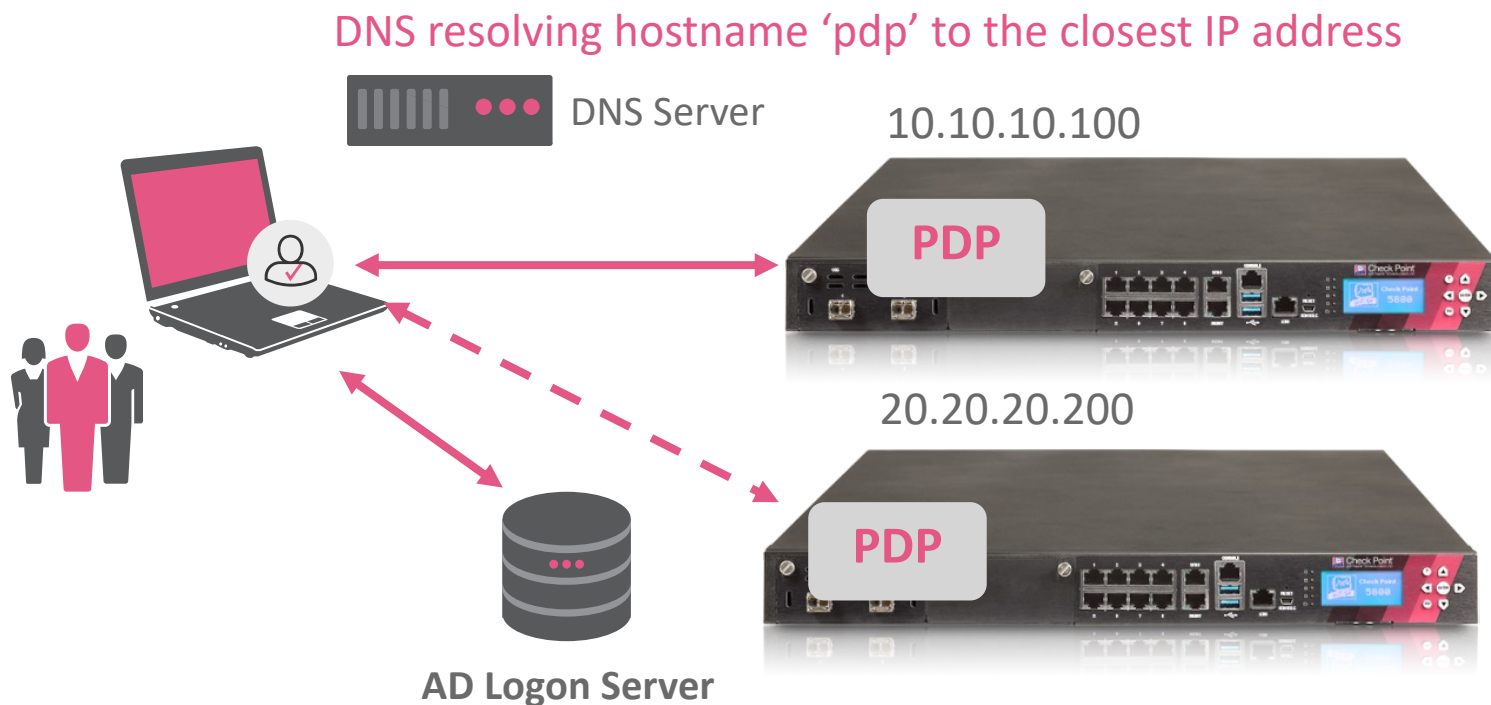


Identity Agent

Client based solution for Windows and macOS

One option to achieve scalability for Identity Agents connecting to the PDP instances is using DNS

- The operating system resolves the IP address of the PDP closest to the regional location

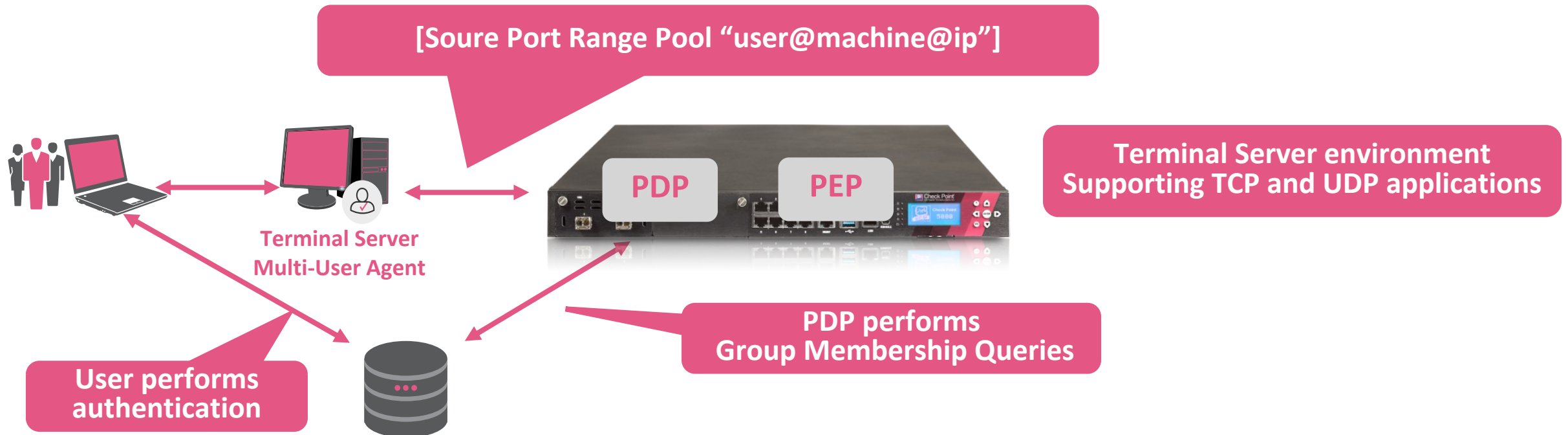


Check Identity Awareness administration guide for more options such as using Service Records

Multi-User Host Agent

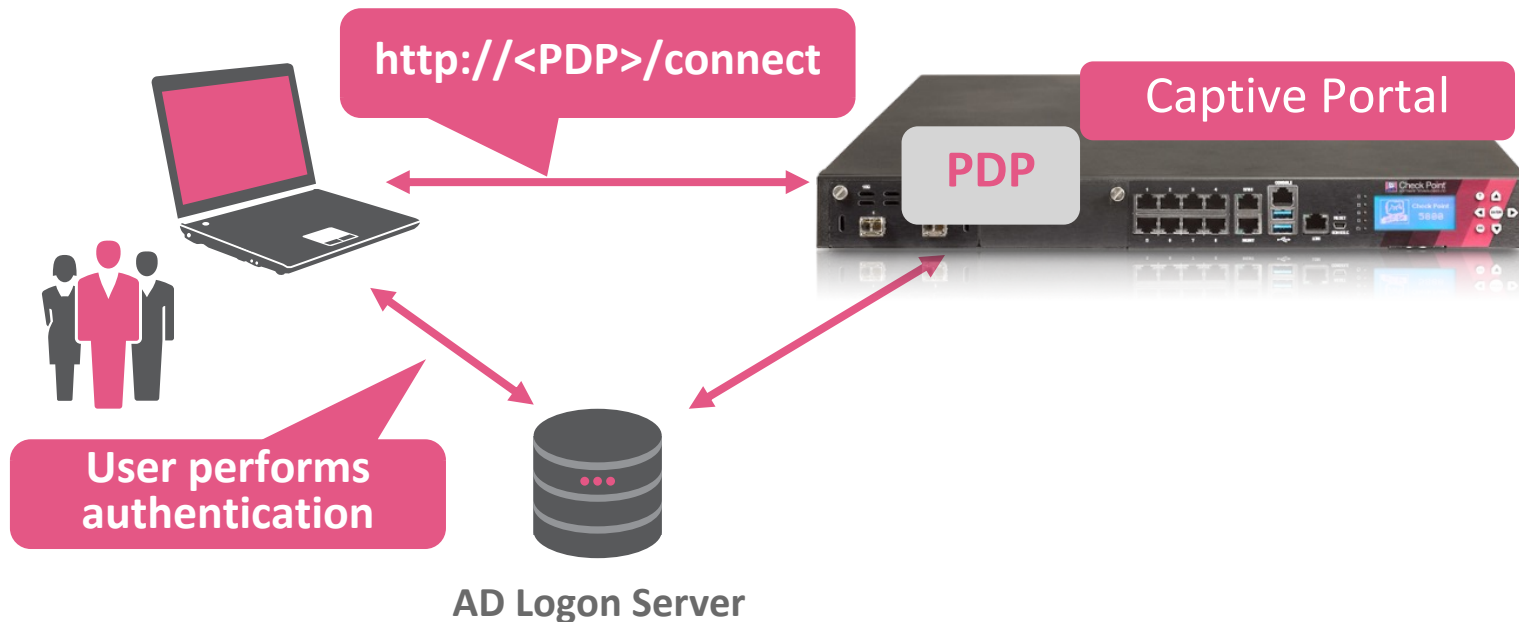
Client based solution for Windows Terminal Servers

- A TDI driver intercepts the users connection
- Source port ranges are allocated per user
- For each user connection a source port from the pool will be allocated allowing the PDP to identify the traffic related to this user



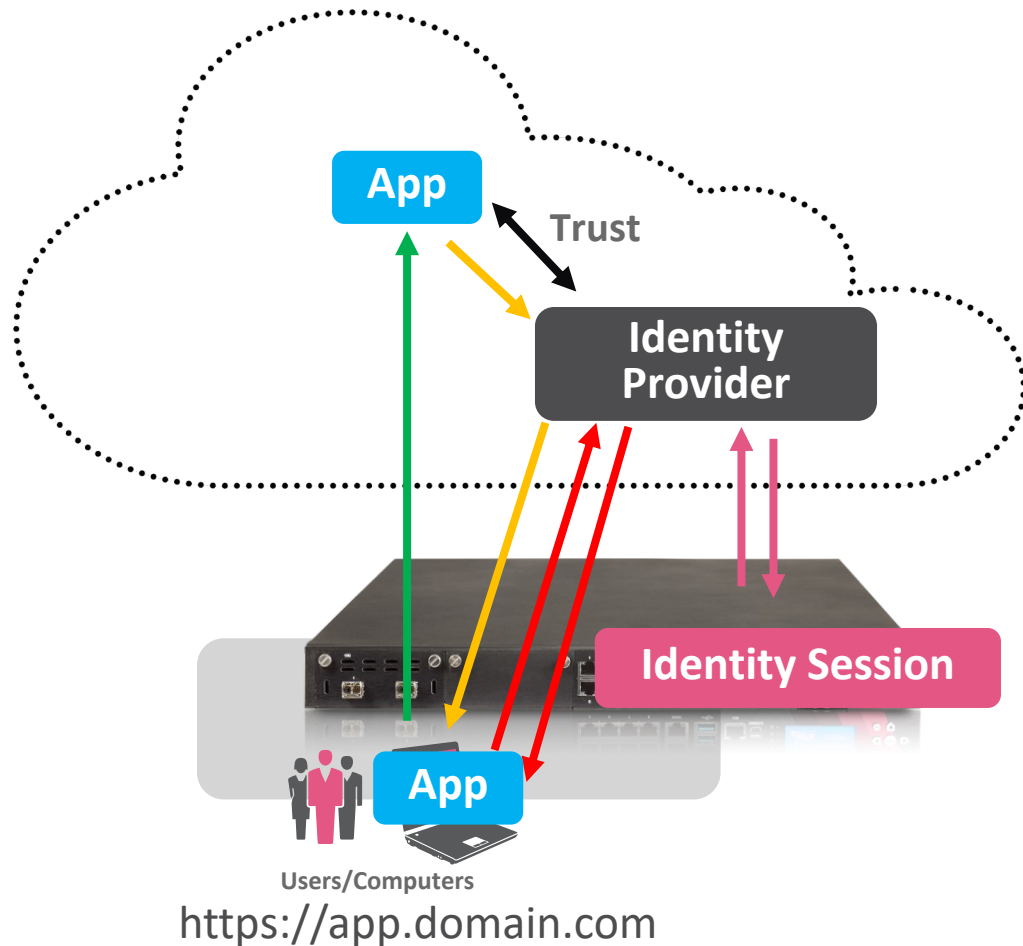
Multi-User Host Agent Captive Portal – Browser Based Authentication

- Users authenticate against the Active Directory and KERBEROS tickets are issued
- The browser presents the ticket to the PDP instance that verifies this ticket
- If verification is successful access is provided
 - The Captive Portal allows users performing a manual logon to the gateway



KERBEROS tickets can be intercepted to achieve transparent authentication

Cloud Based Identity Sources



- Application trusting **Identity Provider**
- Accessing cloud service
- Redirecting to authentication platform
- **Authentication against Identity Provider**
 - Gateway participates in authentication process
 - In SAML terms: **gateway is a Service Provider**
 - Identity Provider issues 'token'
- **Identity Session** is generated
- Access to application is granted
- Application verifies 'token' and provides service

Identity Conciliation

pdp conciliation

Description

Controls the session conciliation mechanism.

Syntax

```
pdp conciliation
  adq_single_user <option>
  api_multiple_users <option>
  idc_multiple_users <option>
  rad_multiple_users <option>
```

What if we learn Login events for the same user/machine from multiple ID Sources?

- Identity Conciliation achieves that only the session learned from highest trust is maintained
- Example:
 - ID Agents have a score of 30
 - ID Collector has a score of 10

Review admin guide



What about Cisco ISE? Cisco TrustSec

Cisco Identity Services Engine and Cisco Digital Network Architecture are commonly used principles achieving network access control

SGTs (Secure/Scalable Group Tags) are assigned to users and machines and used for encapsulating the traffic inside the Cisco DNA segments

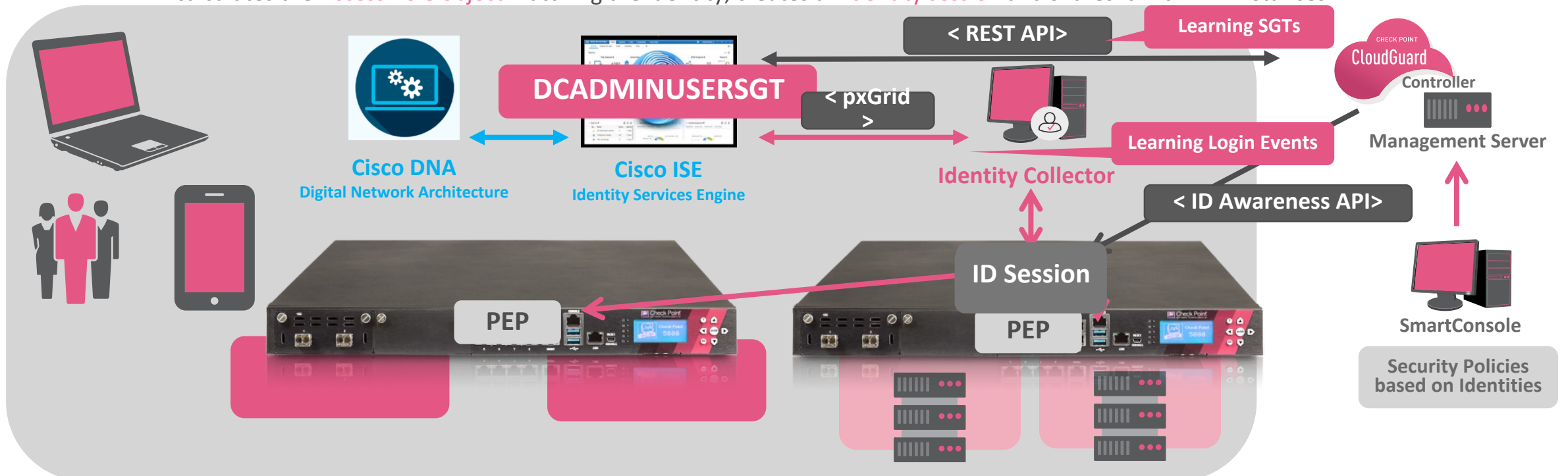
Cisco DNA edge devices transform proprietary data format to regular Ethernet

Check Point Identity Awareness consumes SGTs and enforces security accordingly

Cisco TrustSec Integration

Integrating into Cisco Identity Services Engine (ISE) using pxGrid API


- Cisco ISE is assigning 'Secure Group Tags' to users and machines logging on to the Cisco DNA supported network
 - Configure Identity Tag objects in the Access Role object on the management server to represent these dynamically assigned SGTs
 - CloudGuard Controller imports SGTs via REST API from Cisco ISE (SGTs statically mapped to IP addresses can directly be used in the policy)
- Cisco ISE communicates device/user 'login events' using pxGrid API to the Identity Collector
 - Identity Collector is forwarding 'login event' related identity information to PDP instance on the Check Point Security Gateway
 - PDP calculates the Access Role object matching the identity, creates an identity session and shares it with PEP instances



Controlling Group Membership retrieval

pdp idc

Description

Operations related to [Identity Collector](#) .

Syntax

```
pdp idc
  groups_consolidation <options>
  groups_update <options>
  muh <options>
  service_accounts <options>
  status
```

- In most use cases Cisco ISE and Active Directory co-exist on the network
- Ask you customer from where to learn the group membership: AD or Cisco ISE?
- Configure `groups_consolidation` accordingly
- By default, PDP consolidates what it learns from AD in addition to what is given from Cisco ISE
 - Is there an LDAP Account Unit object? If yes, it will be used by the PDP to learn groups

Enable the consolidation (this is the default):

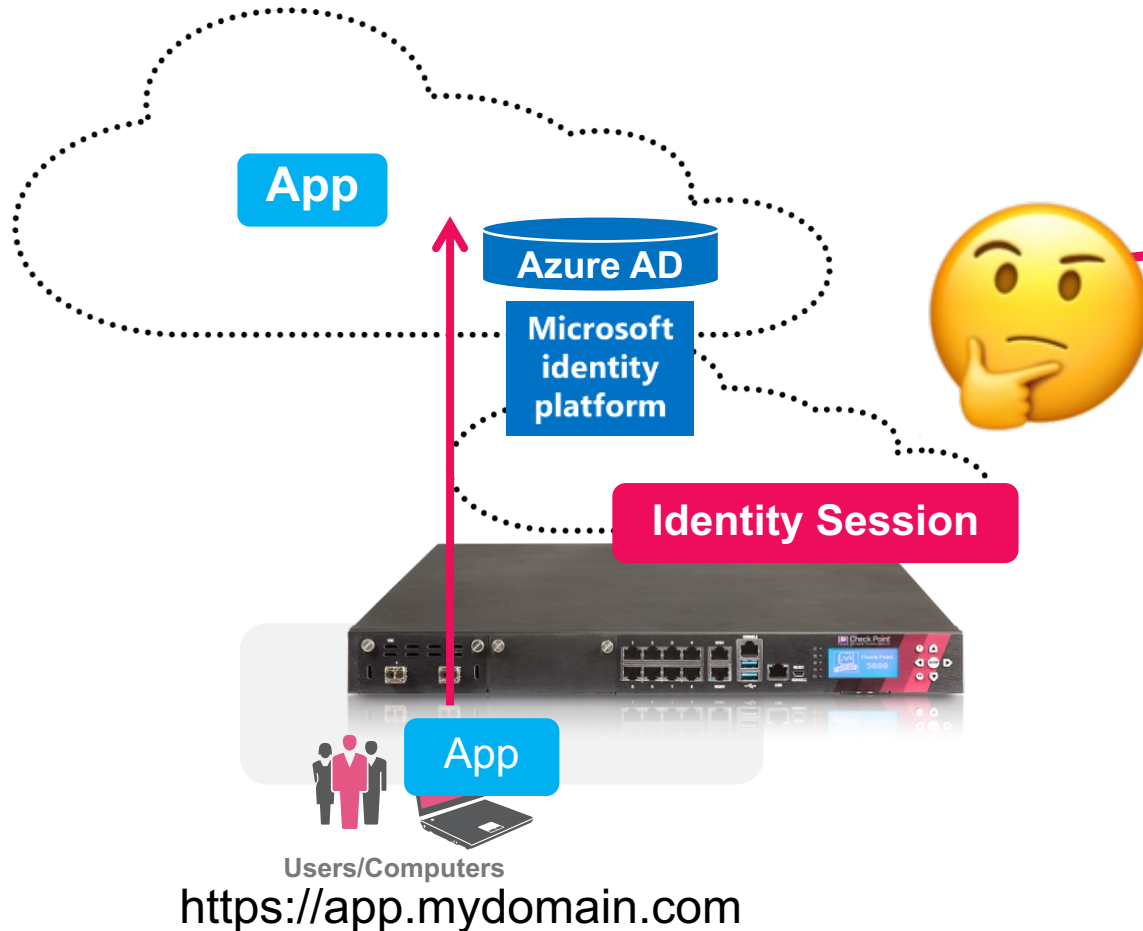
```
pdp idc groups_consolidation enable
```

Cloud Based Identity Sources (SAML)

Authenticating Against Microsoft Identity Platform

Scenario: Accessing Cloud Services registered to Azure AD

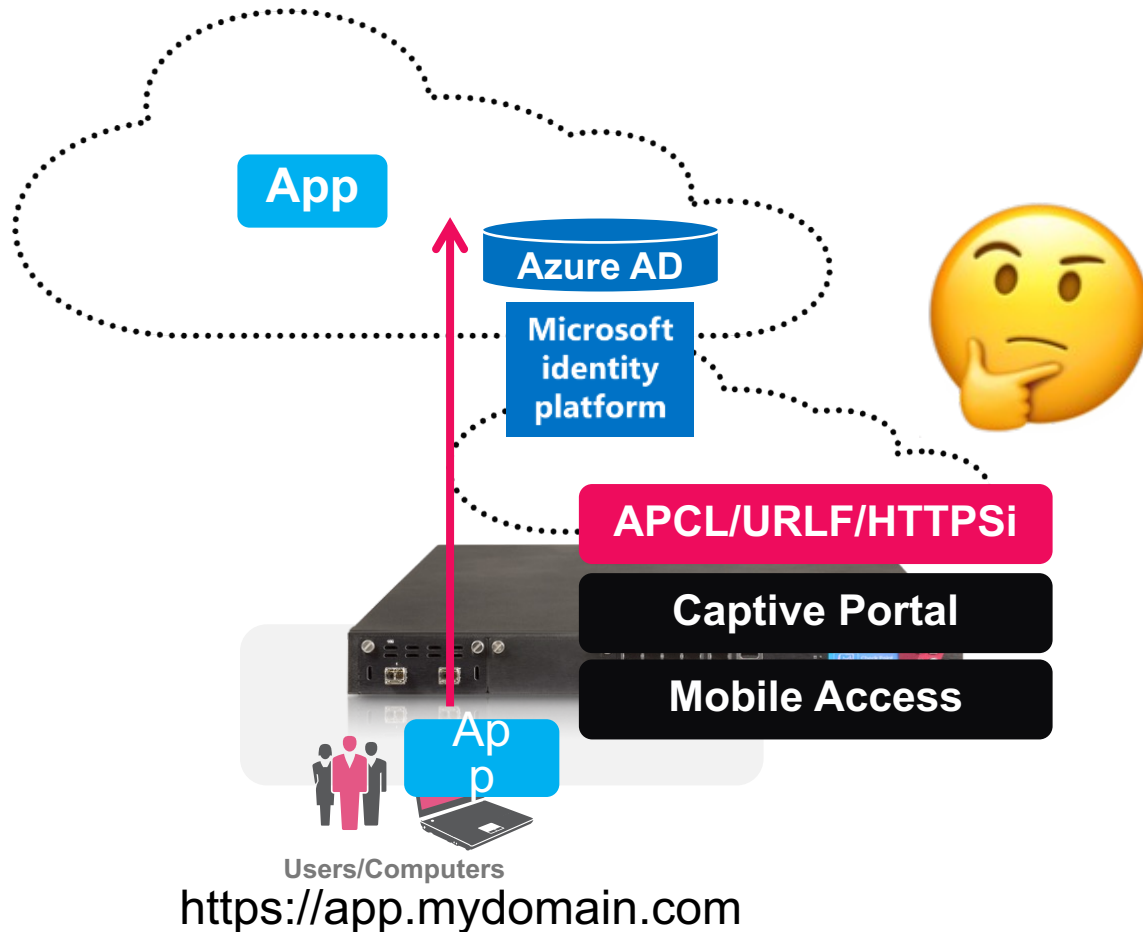
Reviewing the facts until user is working on app



-
-
- HTTP Redirects are passing the gateway
-
-
-
-

Authenticating Against Microsoft Identity Platform

Scenario: Accessing Cloud Services registered to Azure AD



HTTP Redirects passing...

- DNS resolution must work 100%

HTTP Redirects are related to applications...

- Gateway must identify the application/URL accessed by the user
 - Application Control is needed
 - URL Filtering is needed
 - HTTPS inspection might be required to identify Applications/URLs
- An access control rule is required to 'catch' this application traffic
- **Captive Portal** or **Mobile Access Blade** are currently supported for 'catching' the traffic

Authenticating Against Microsoft Identity Platform



'Catching' the traffic with the Access Control Security Rule Base

- Use dedicated Application/Sites as destination with the setting 'Action: Captive Portal'

No.		Name	Source	Destination	Services & Applications	Action
▶ Management (1)						
▶ Network Services (2-4)						
▶ Published Services (5)						
▼ Outbound (6-8)						
6	317	Office 365	NGTPdemo_Azure	Office365 Services	* Any	Accept (display captive portal)
7	12	News	NGTPdemo_Azure	* Any	News / Media	Accept (display captive portal)
8	0	Demo Web Site	NGTPdemo_Azure	* Any	DemoWebSite	Accept (display captive portal)
▶ Clean Up (9-10)						

- Cloud hosted services are based on many TCP connections thus using service objects http/https will not 'catch' the relevant traffic related to the application

Don't use services to 'catch' traffic for SAML authentication

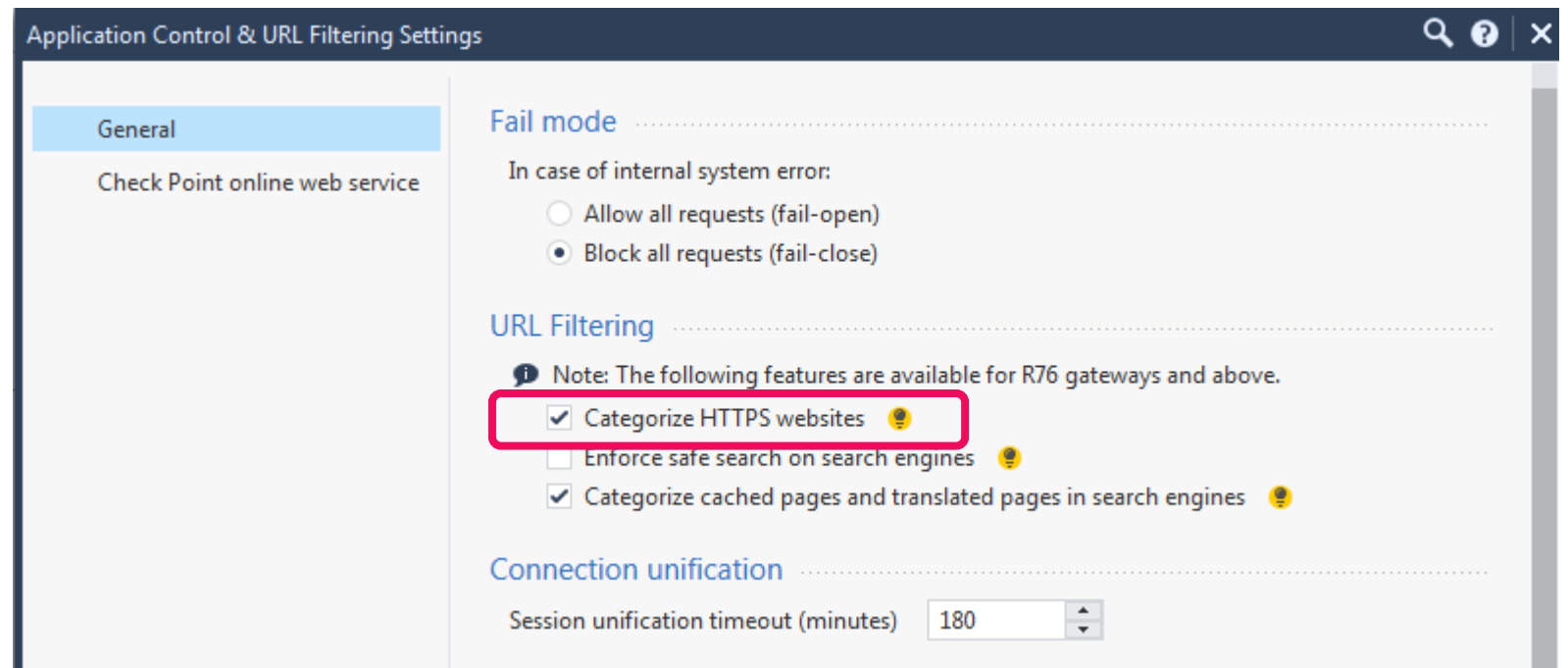
Source	Destination	Services & Applications	Action
NGTPdemo_Azure	* Any	 http  https	Accept (display captive portal)

Depending on the application - you may need to configure HTTPS inspection

'Catching' Traffic Working Without HTTPS Inspection

Make sure categorization of HTTPS websites is enabled

- Enable 'Categorize HTTPS websites' under Manage & Settings > Application Control
 - This functionality allows identifying HTTPS websites based on the SNI
 - Enabled by default in current versions
- Without this function enabled Application/URL Filtering rules will not work as expected



Access Control Security Rule Base

Respect the complexity of Cloud hosted services

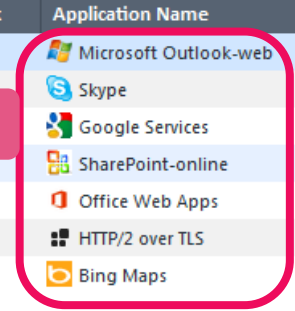
- Rule #3: Online Certificate Service Protocol
- Rule #4: Access to Microsoft Authentication Services
- Rule #6: Authenticated users can access Microsoft Office 365 services hosts and domains

No.	Hits	Name	Source	Destination	Services & Applications	Action	Track
▶ Management (1)							
▼ Network Services (2-4)							
2	888	Network Services	All_Internal_Networks	* Any	dns icmp-proto ntp	Accept	None
3	0	Online Certificate Service	All_Internal_Networks	* Any	OCSP Protocol	Accept	None
4	77	Cloud Authentication Services	All_Internal_Networks	* Any	Microsoft Account	Accept	Detailed Log
▶ Published Services (5)							
▼ Outbound (6-7)							
6	179	Office 365	NGTpdemo_Azure	Office365 Services	* Any	Accept (display captive portal)	Detailed Log
7	11	News	NGTpdemo_Azure	* Any	News / Media	Accept (display captive portal)	Detailed Log

Time	Origin	Source	Source User Name	Destination	Service	Application Risk	Application Name	Primary Category	Access Rule Name
Today, 21:20:39	gateway	WebServer (192.168.170.10)	peter@ngtpdemo.eu	a104-102-28-76.deploy.stati...	https (TCP/443)	Medium	Microsoft Outlook-web	Email	Office 365
Today, 21:20:29	gateway	WebServer (192.168.170.10)	peter@ngtpdemo.eu	68-232-24-200	https (TCP/443)	Medium	Skype	VoIP	Office 365
Today, 21:20:25	gateway	WebServer (192.168.170.10)	peter@ngtpdemo.eu	13.107.136.9	https (TCP/443)	Low	Google Services	Computers / Internet	Office 365
Today, 21:20:24	gateway	WebServer (192.168.170.10)	peter@ngtpdemo.eu	52.109.28.22	https (TCP/443)	Very Low	SharePoint-online	Business / Economy	Office 365
Today, 21:20:23	gateway	WebServer (192.168.170.10)	peter@ngtpdemo.eu		https (TCP/443)	Very Low	Office Web Apps	Business / Economy	Office 365
Today, 21:20:22	gateway	WebServer (192.168.170.10)	peter@ngtpdemo.eu			Very Low	HTTP/2 over TLS	Network Protocols	Office 365
Today, 21:20:14	gateway	WebServer (192.168.170.10)	peter@ngtpdemo.eu			Low	Bing Maps	Search Engines / Por...	Office 365

Only Office 365 home page was opened

SmartLog Filter: type: Session

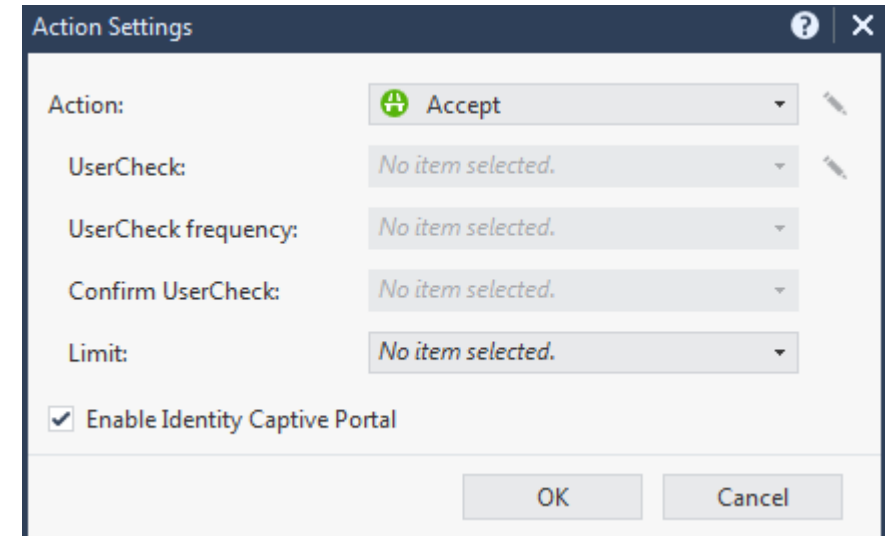
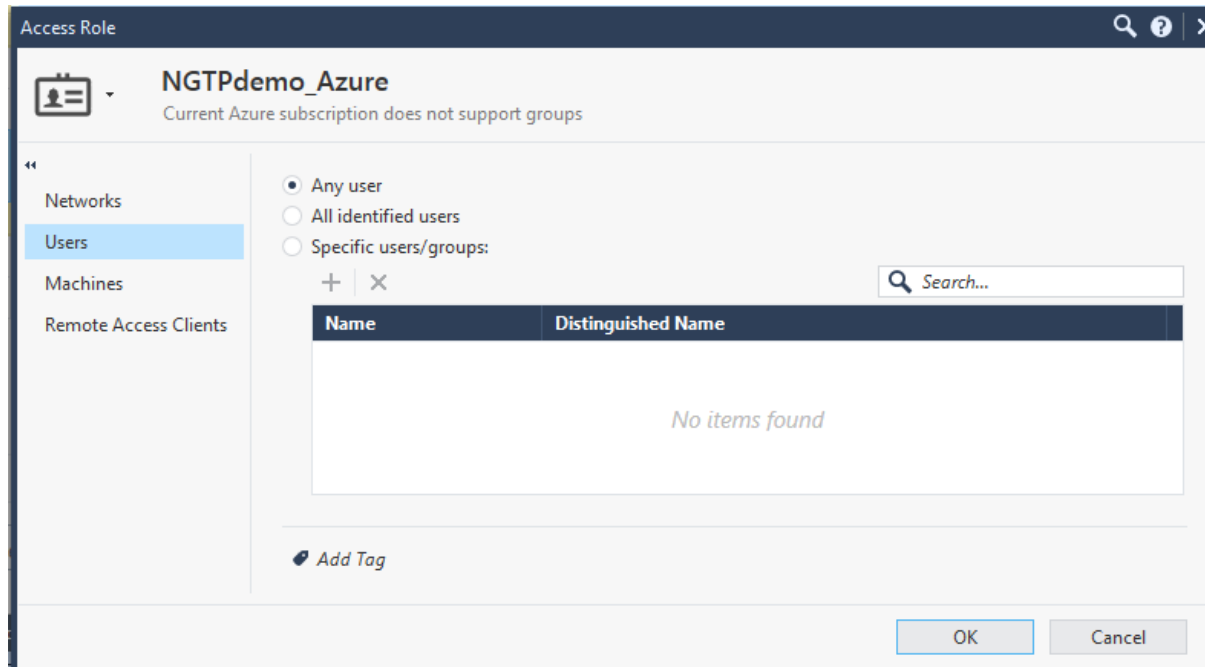


Access Control Security Rule Base

Define Access Role object

- Using specific groups in the Access Role object requires an Azure Premium subscription
 - If you are using a trial Office 365 subscription for testing assign even 'Any user'

- Don't forget to enable the 'Identity Captive Portal' in the 'Action: Accept' column



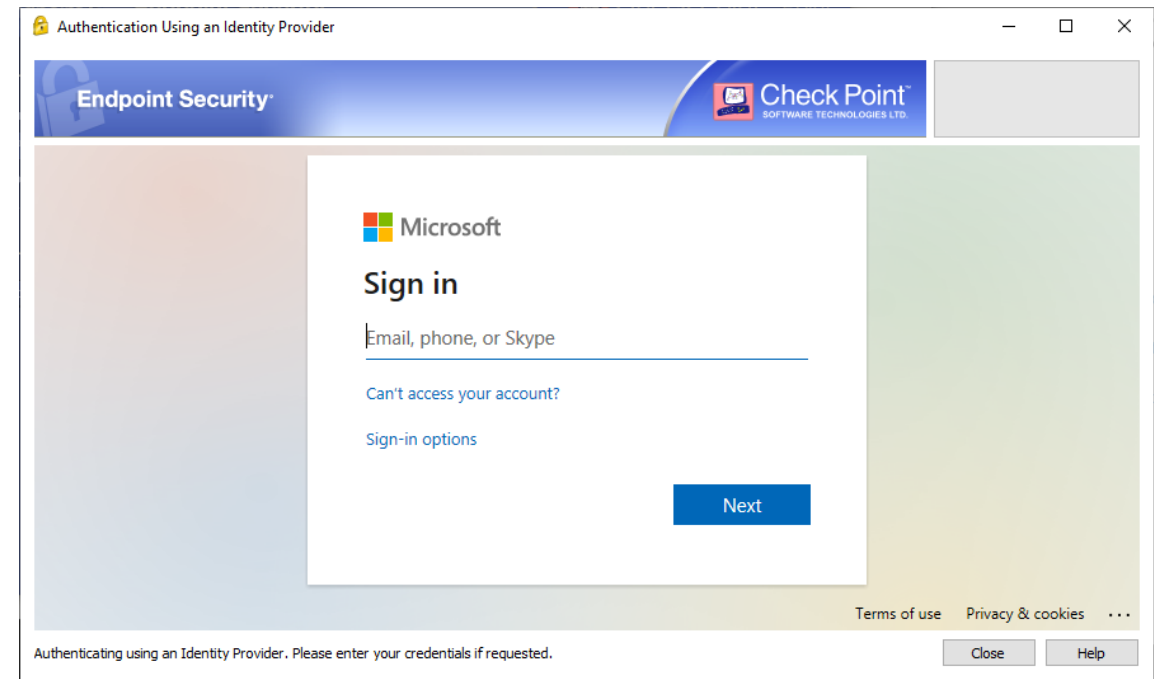
Configuration Video

-

https://sc1.checkpoint.com/documents/R80.40/Videos/EN/IDA/IDA_SAML_IdP.mp4

Remote Access VPN with SAML Authentication

- Allows authentication with ADFS and other SAML-based services.
- Version Requirement (GW):
 - R81.20
 - R80.40 JHF 114 or above
 - R81 JHF 42 or above
 - R81.10 JHF 9 or above
- Version Requirement (Client):
 - E84.70 or above
- More details in [sk172909](#) and [sk177267](#)
- [Video on CheckMates](#)



Identity Awareness Enhancements in R81.20

Service Accounts Overview

- In Microsoft Active Directory, a user account created explicitly to provide a security context for services running on Microsoft Windows Server
- Administrators often don't want to monitor service accounts
- Problem: Service accounts consume unnecessary CPU and kernel table space
- Hence, we want to have the option to exclude them from PDP

Service Accounts Overview – cont

- Suspected service accounts are accounts who logged in more than 10 machines by default.
- Currently suggested solution for customers: filter service accounts in collector side
- Important note - In ADQuery, we have option to automatic exclude service accounts. This option is called “**prevention**”.
- In IDC source (PDP side) this option is not automatic and we had to develop it.

IDC New Mechanism – On the fly detection & prevention

How it works internally?

- When logins arrives via the collector, we add it to a new map (username count): username->[IPs]
 - If [IPs].size() is equal/passed the threshold, we report it as service account
 - If in addition prevention is on – we revoke all it's sessions right away (and delete from our map) & won't create session for it
 - If session is revoked (in same logic for MUH) – we reduce the list.
- When we get user association, we first check if we know this as service account and prevention (auto exclude) is on. If so, we won't create session.

Improvements in IDA Infrastructure

- Multi-threaded PDP for improved resiliency, stability, and scalability
- Extract heavy operations to reduce the hard work from the PDP
- Remove the usage of Id tables and move to GHTAB in PDP and PEP daemons to remove sync between instances overhead and work with optimized KISS APIs
- Integrate with a side task made by the framework group to allow improved IOCTLs which also required for IDA improved performance
- Two or more connected PDPs will be able to recover identities from other PDPs for the same host IP address for improved redundancy
- End result: **Improved resiliency and stability in Identity Awareness, improved performance in Kernel and especially in USFW mode**

Monitoring

Monitoring: SmartLog

- Accessing only the home page of Microsoft Office 365 results in a large number of TCP connections to different services
- Filtering the logs for 'type: Session' provides an overview of the complexity
 - Developing a granular rule base may take time

★ Queries | < > ↻ 🔍 Last Hour ▾ rule:6 AND type:Session

Found 12 results (261 ms)

Time	Origin	Source	Source User Name	Destination	Service	Application Risk	Application Name	Primary Category	Access Rule N...
Today, 21:20:39	gateway	WebServer (192.168.170.10)	peter@ngtpdemo.eu	a104-102-28-76.deploy.static.akamaitechnologie...	https (TCP/443)	3 Medium	Microsoft Outlook-web	Email	Office 365
Today, 21:20:29	gateway	WebServer (192.168.170.10)	peter@ngtpdemo.eu	68.232.34.200	https (TCP/443)	3 Medium	Skype	VoIP	Office 365
Today, 21:20:25	gateway	WebServer (192.168.170.10)	peter@ngtpdemo.eu	mil04s03-in-f14.1e100.net (216.58.198.14)	https (TCP/443)	2 Low	Google Services	Computers / Internet	Office 365
Today, 21:20:24	gateway	WebServer (192.168.170.10)	peter@ngtpdemo.eu	13.107.136.9	https (TCP/443)	2 Low	SharePoint-online	Business / Economy	Office 365
Today, 21:20:23	gateway	WebServer (192.168.170.10)	peter@ngtpdemo.eu	52.109.28.22	https (TCP/443)	1 Very Low	Office Web Apps	Business / Economy	Office 365
Today, 21:20:22	gateway	WebServer (192.168.170.10)	peter@ngtpdemo.eu	52.109.28.34	https (TCP/443)	1 Very Low	HTTP/2 over TLS	Network Protocols	Office 365
Today, 21:20:14	gateway	WebServer (192.168.170.10)	peter@ngtpdemo.eu	13.107.21.200	https (TCP/443)	2 Low	Bing Maps	Search Engines / Portals	Office 365
Today, 21:20:14	gateway	WebServer (192.168.170.10)	peter@ngtpdemo.eu	13.107.21.200	https (TCP/443)	2 Low	Bing	Search Engines / Portals	Office 365
Today, 21:20:14	gateway	WebServer (192.168.170.10)	peter@ngtpdemo.eu	52.114.76.34	https (TCP/443)	2 Low	MSN-web	Search Engines / Portals	Office 365
Today, 21:20:11	gateway	WebServer (192.168.170.10)	peter@ngtpdemo.eu	13.107.6.156	https (TCP/443)	2 Low	Microsoft Services	Computers / Internet	Office 365
Today, 21:20:11	gateway	WebServer (192.168.170.10)	peter@ngtpdemo.eu	a23-79-91-153.deploy.static.akamaitechnologies...	https (TCP/443)				Office 365
Today, 21:18:39	gateway	WebServer (192.168.170.10)		40.101.137.98	https (TCP/443)	1 Very Low	Office365-Outlook-web	Email	Office 365

Monitoring - SmartLog

- The login event includes information about
 - Identity Provider
 - Identity Source
 - User

Identity	
Authentication Status	Successful Login
Identity Source	Captive Portal
User	peter@ngtpdemo.eu
Source User Group	All Users
Roles	NGTPdemo_Azure

Log Details

Log In
Successful Login of peter@ngtpdemo.eu: Identity Provider (boxNGTPdemo)

Details

Source: WebServer (192.168.170.10)
peter@ngtpdemo.eu

Action: Log In
Blade: Identity Awareness
Time: Today, 21:19:57

Device

Endpoint IP: WebServer (192.168.170.10)

Client Information

Client Name: Identity Awareness Captive Portal
Product Version: R80.40

Session

Session ID: 6bdbbeab3
Authentication Method: Identity Provider (boxNGTPdemo)

Identity

Authentication Status: Successful Login
Identity Source: Captive Portal
User: peter@ngtpdemo.eu
Source User Group: All Users
Roles: NGTPdemo_Azure

Actions

Report Log: Report Log to Check Point

More

Id: c0a8a9fc-b607-3696-5df3-f26d000000...
Marker: @A@@B@1576231394@C@4024
Log Server Origin: mgnt (192.168.169.40)
Id Generated By Indexer: false
First: false
Sequencenum: 4
Last Update Time: 2019-12-13T20:19:57Z
Type: Log
Origin: gateway
Logid: 131073
Description: Successful Login of peter@ngtpdemo.eu: Identity Provider (boxNGTPdemo)

Monitoring – Command Line On The Gateway

pdp monitor all

- The CLI command allows viewing the Identity Session
 - This **Identity Session can be shared** with PEP instances (Gateways enforcing security based on identities)
 - This **Identity Session can be published** (shared) using PDP Broker functionality to PDP Broker gateways configured as subscriber

```
[Expert@gw:0]# pdp m a
```

```
Session: 342bc3fb
```

```
Session UUID: {D621127A-2721-9BCF-02A0-1242FDBF1561}
```

```
Ip: 192.168.170.10
```

```
Users:
```

```
peter@ngtpeu {6bdbbeab3}
```

```
Groups: All Users
```

```
Roles: NGTpeu_Azure
```

```
Client Type: portal
```

```
Authentication Method: Identity Provider (boxNGTpeu)
```

```
Distinguished Name:
```

```
Connect Time: Fri Dec 13 21:19:26 2019
```

```
Next Reauthentication: Sat Dec 14 09:19:57 2019
```

```
Next Connectivity Check: Sat Dec 14 09:19:57 2019
```

```
Next Ldap Fetch: -
```

```
Packet Tagging Status: Not Active
```

```
Published Gateways: Local
```

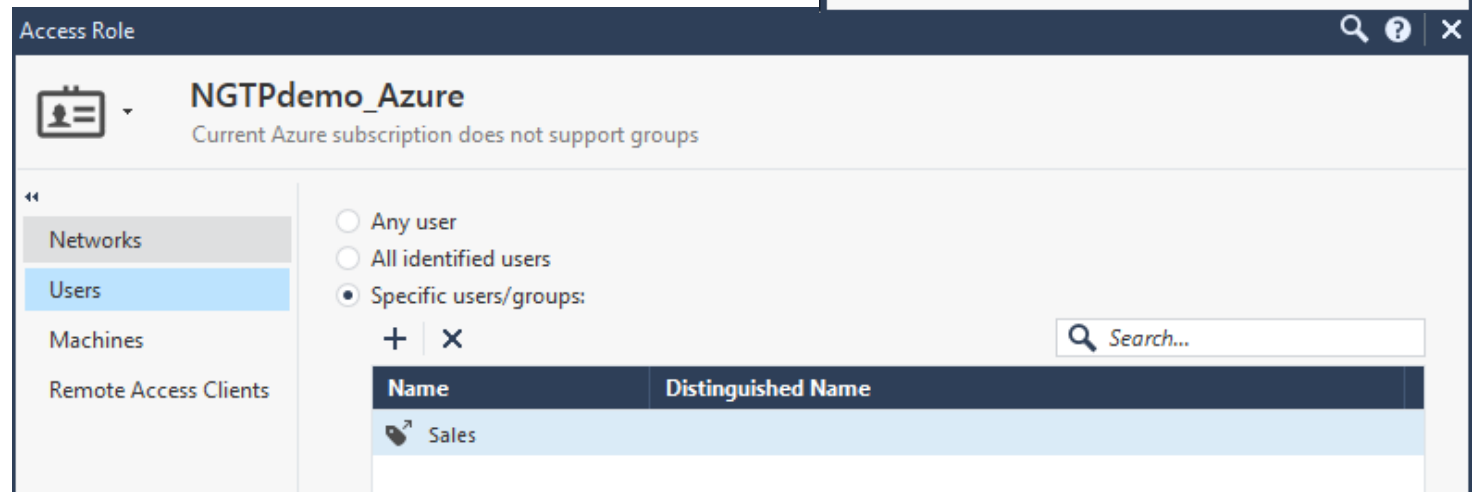
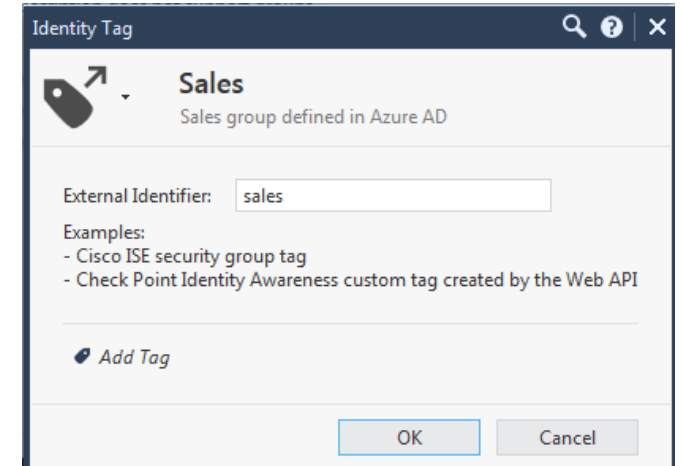
Working With Azure AD Groups

R80.40 requires Identity Tags to represent these on the management

- Microsoft Azure supports restricting access to applications for users and groups



- R80.40 supports Azure AD groups
 - Existing groups need to be configured in SmartConsole as Identity Tag object and associated with the Access Role object



Working With Azure AD Groups

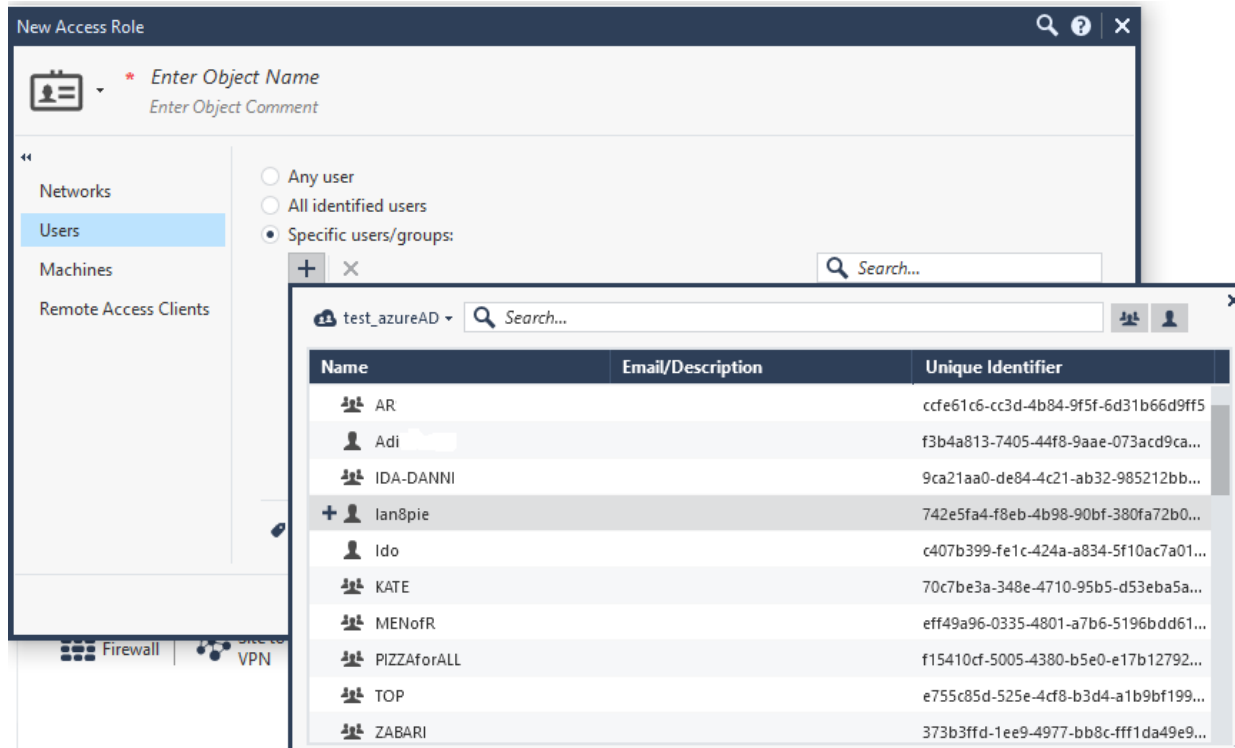
R80.40 requires Identity Tags to represent these on the management

- It is important that the Identity Tag carries the same spelling of the group name than in the Azure AD

The screenshot displays the 'sales - Properties' page in the management console. The 'Group name' field is highlighted with a red box and contains the text 'sales'. A blue line connects this field to the 'Identity Tag' dialog box. The dialog box, titled 'Sales', shows the 'External Identifier' field also containing 'sales'. Below the dialog box, the 'Group description' is 'sales team ngtpdemo', the 'Group type' is 'Office', the 'Membership type' is 'Assigned', and the 'Object Id' is 'a97ad640-9aec-4ae8-8ff2-60fdea400636'.

In R81 and above

Configure Access Role with Azure directory without creating IDA tag

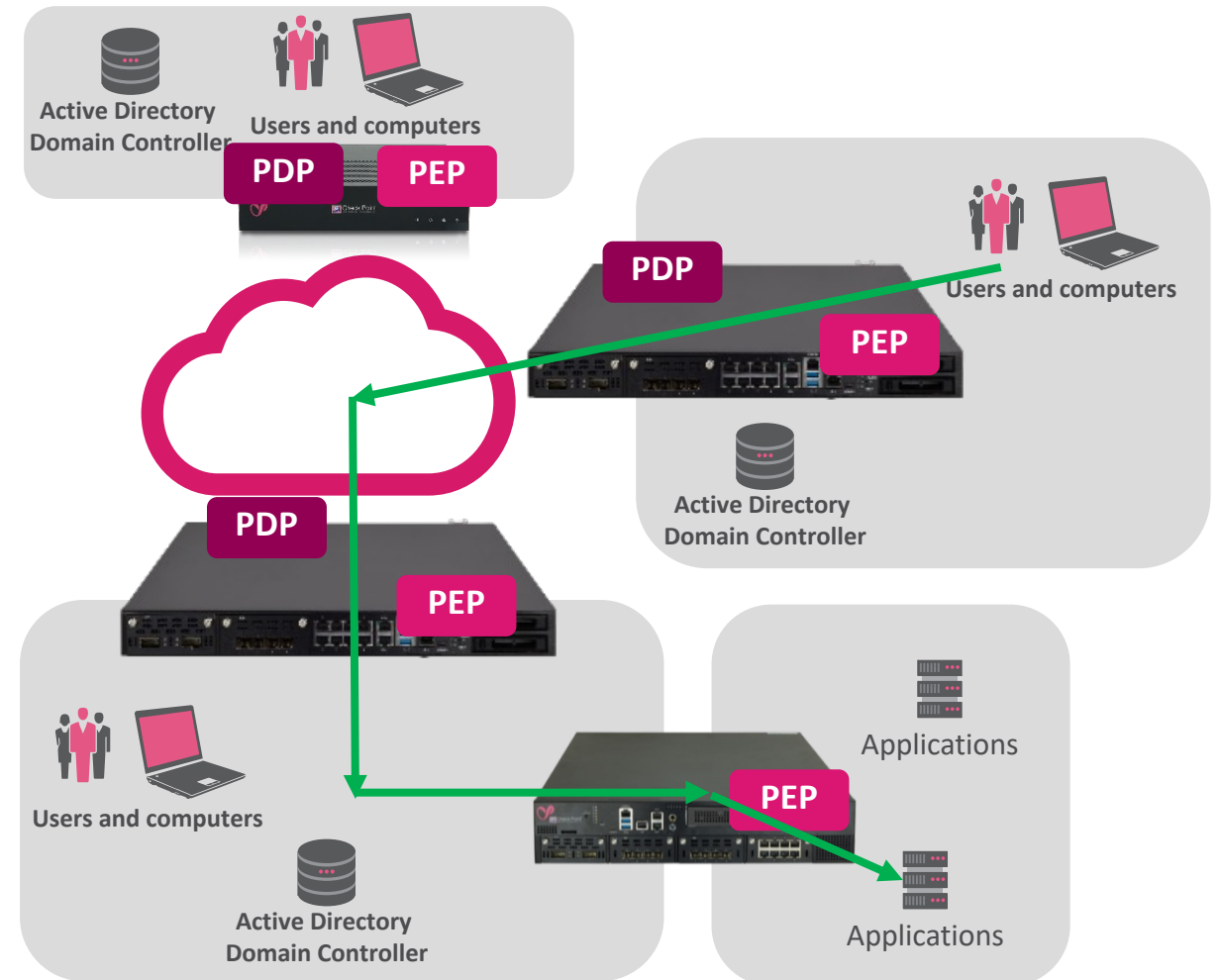
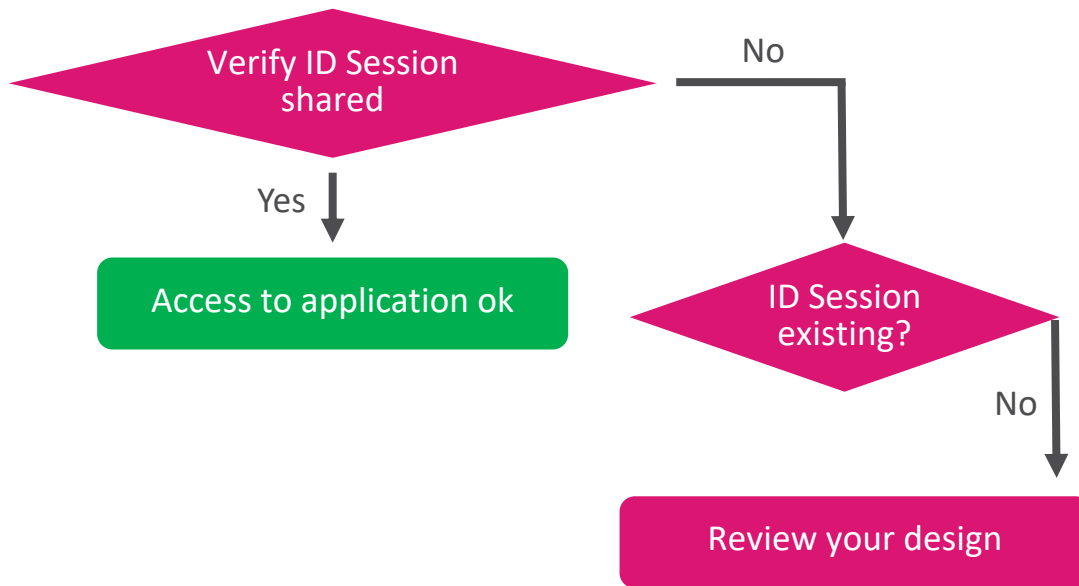


Design & Scale

Design Guidelines

Identity Sharing

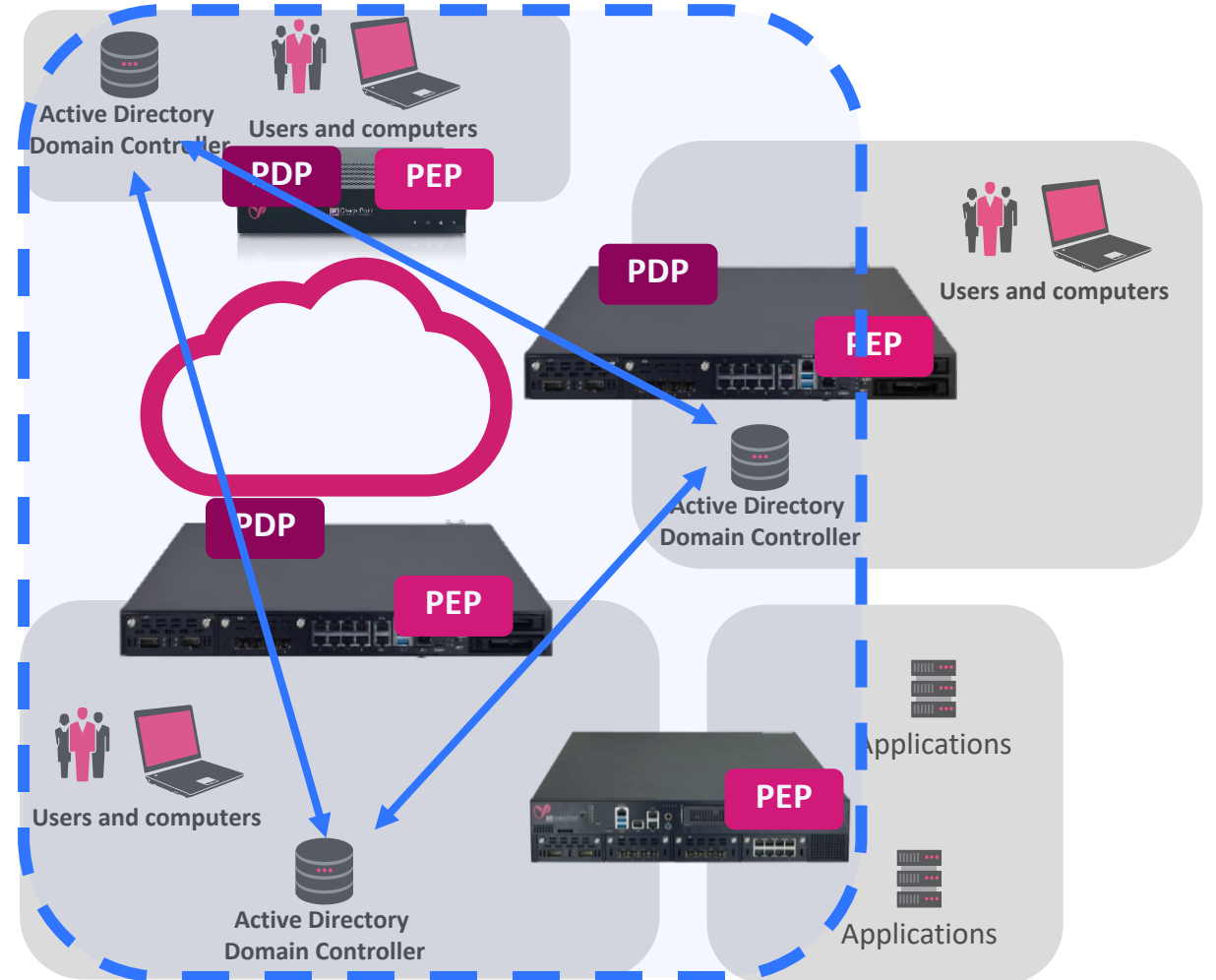
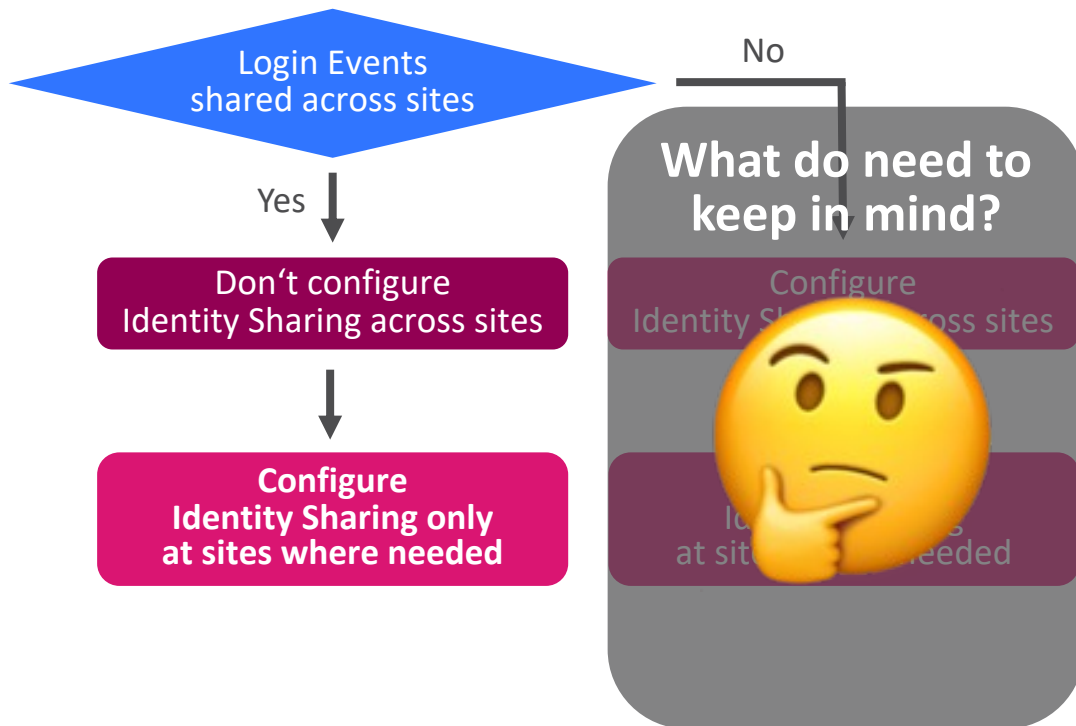
- Understand user to application flow requires Identity Session being known at multiple PEPs



Design Guidelines

Identity Sharing

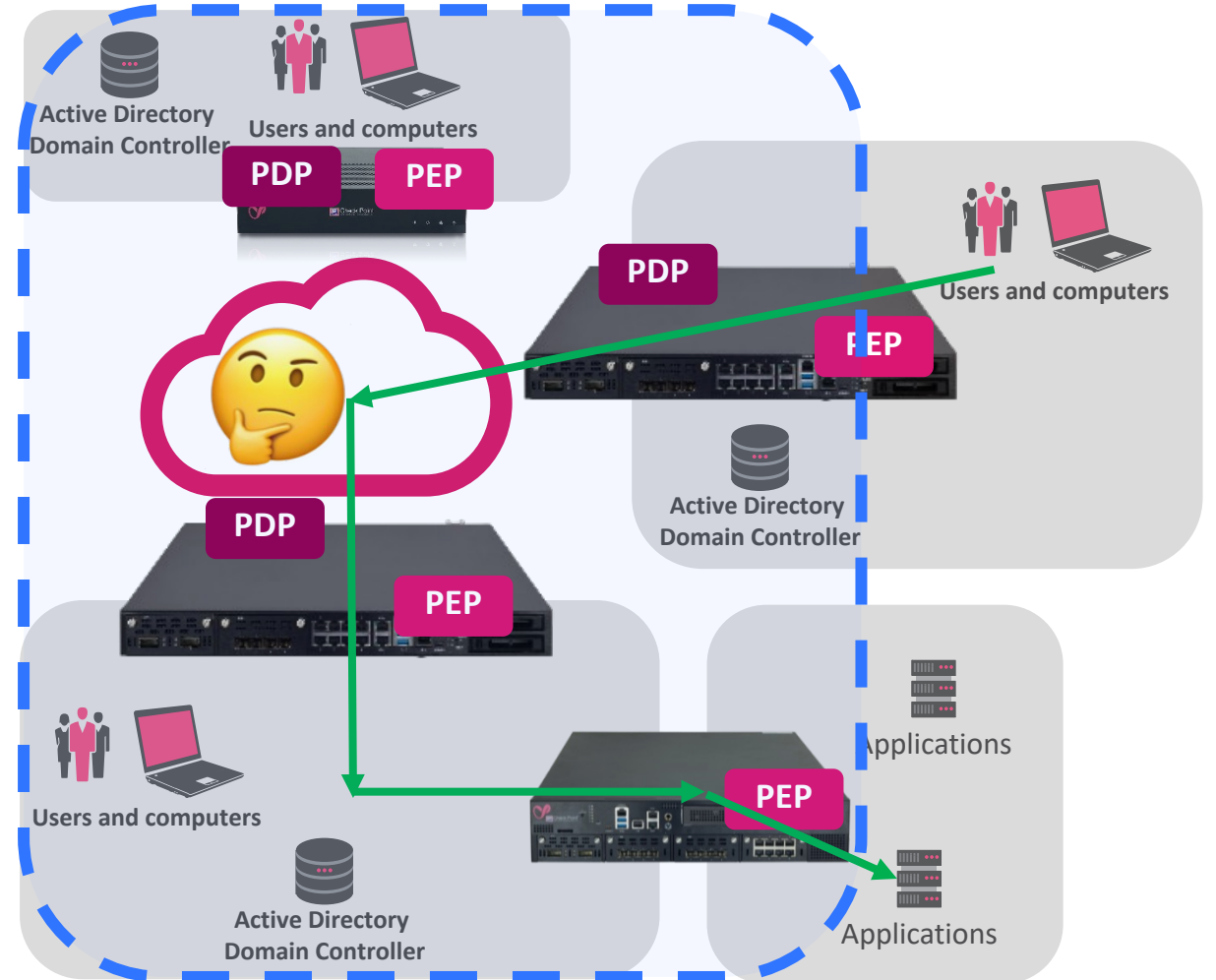
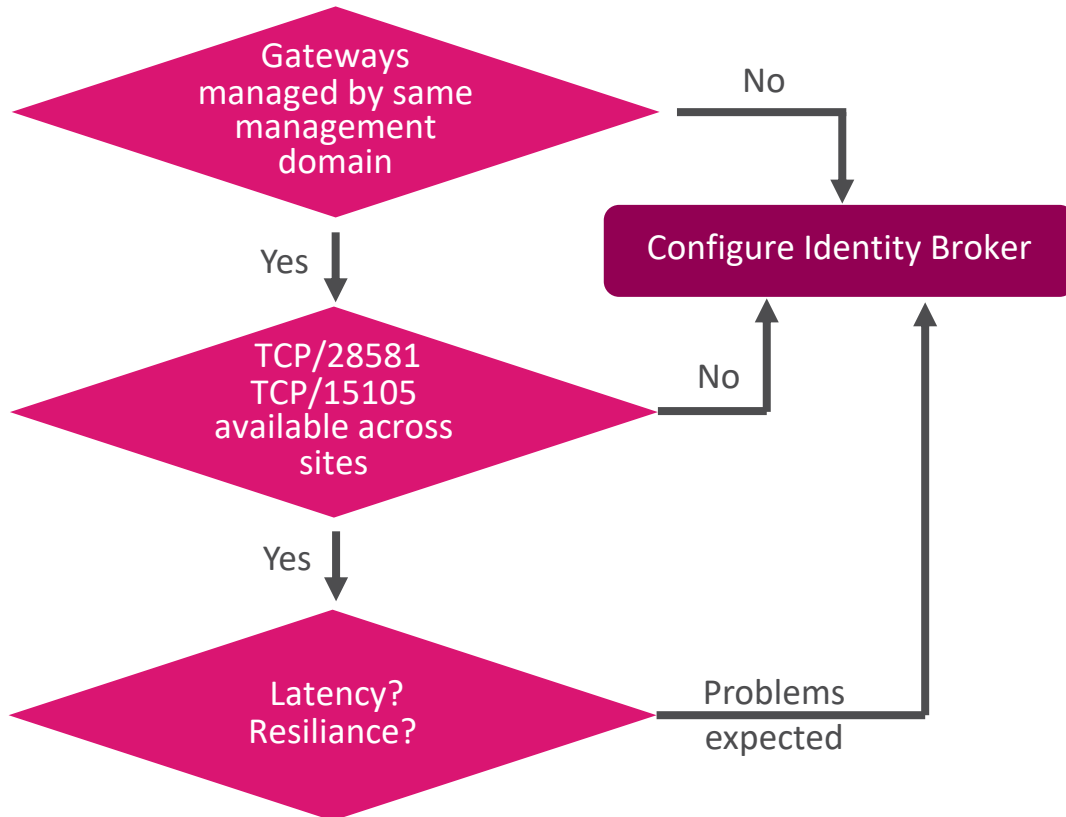
- Understand trust relationship between distributed AD logon servers



Design Guidelines

Identity Sharing

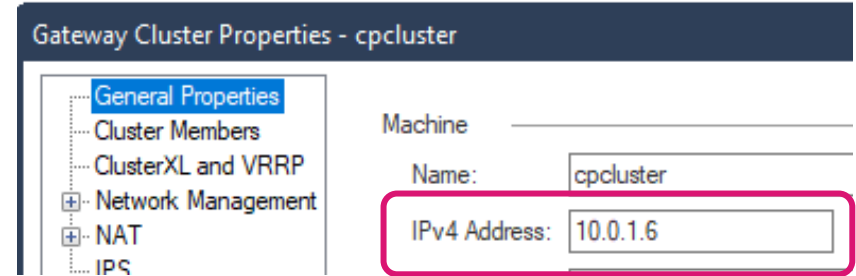
- Is ID sharing from PDP to PEP applicable?



Design Guidelines

Main IP address is used for ID Sharing TCP connections

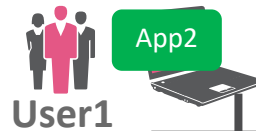
- Routing constrains may require configuring a different IP address for the identity sharing connections



Configure alternate IP address for Identity Awareness communication channel sk60701

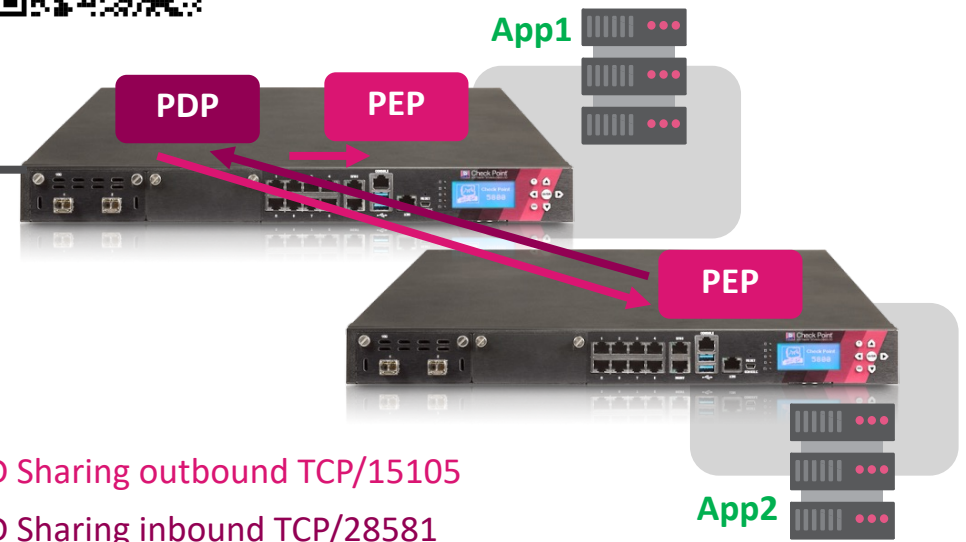


ID Sharing sk149255



Net_10

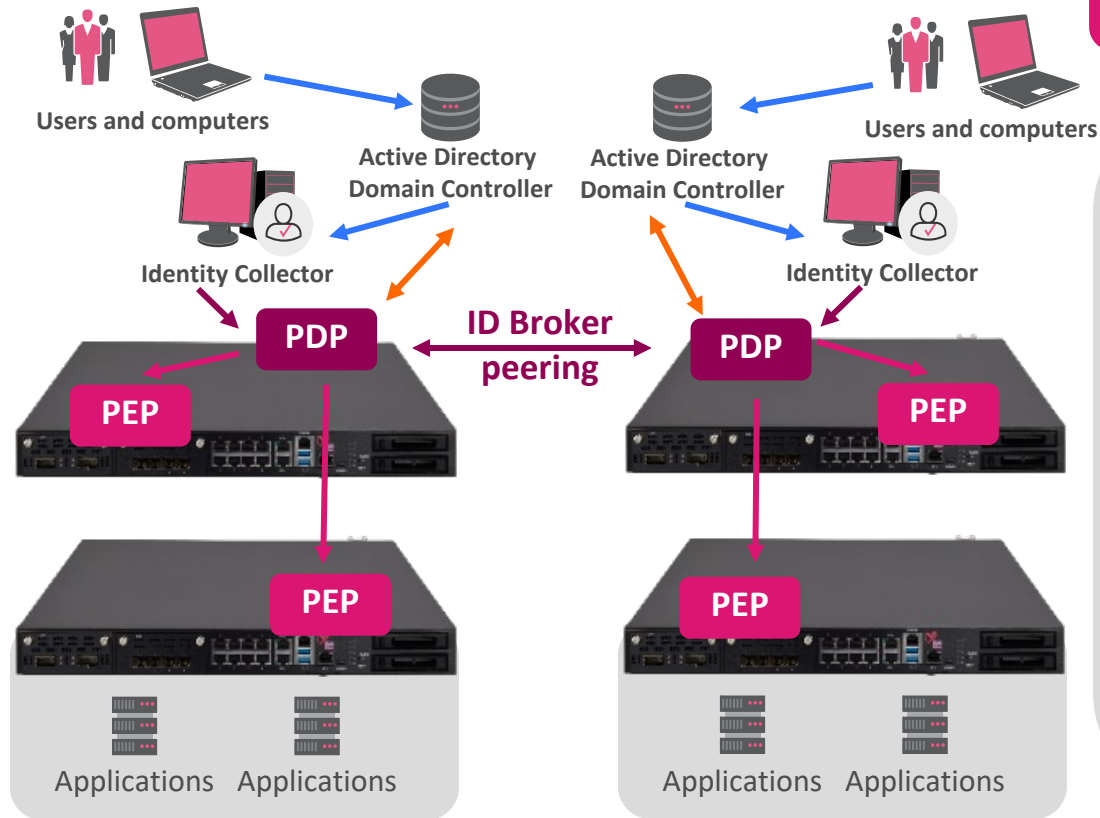
Identity Awareness Administration Guide



How To Scale?

Scaling – ID Broker + ID Sharing

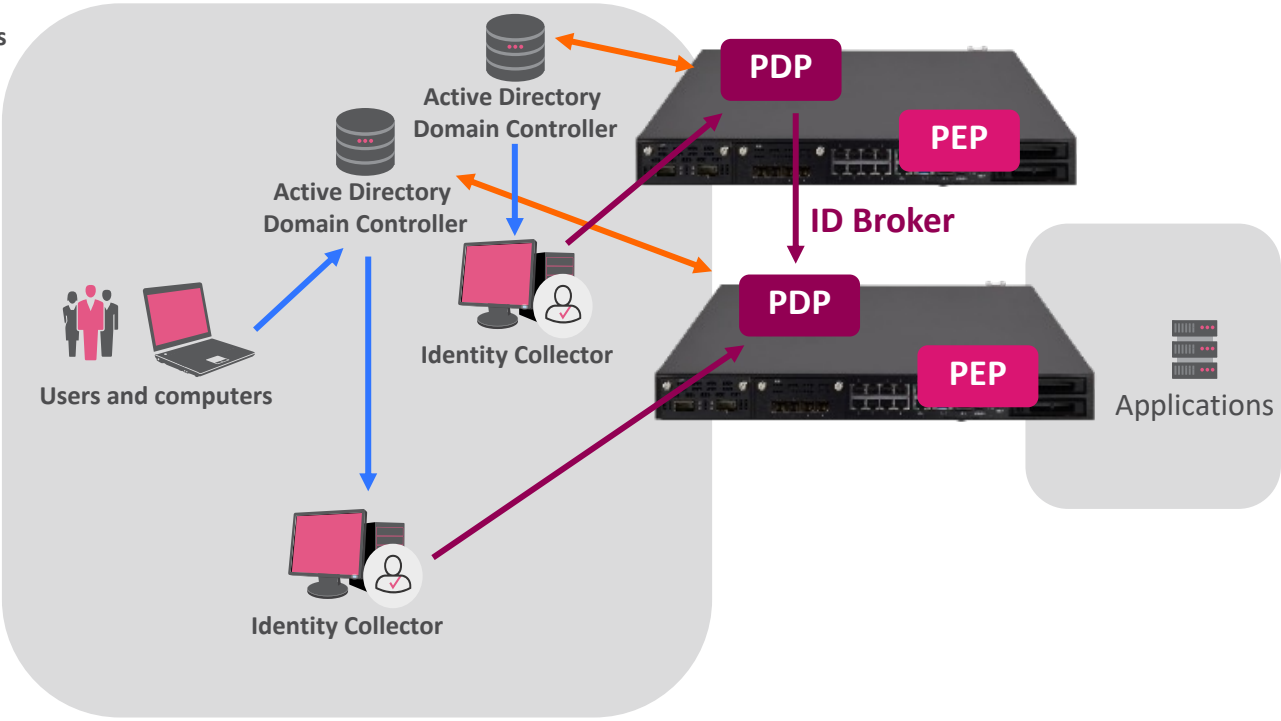
- User to application flow – planning for scale



What if there are more ...
...than 1900 login events / sec?
...than 35 AD logon servers?



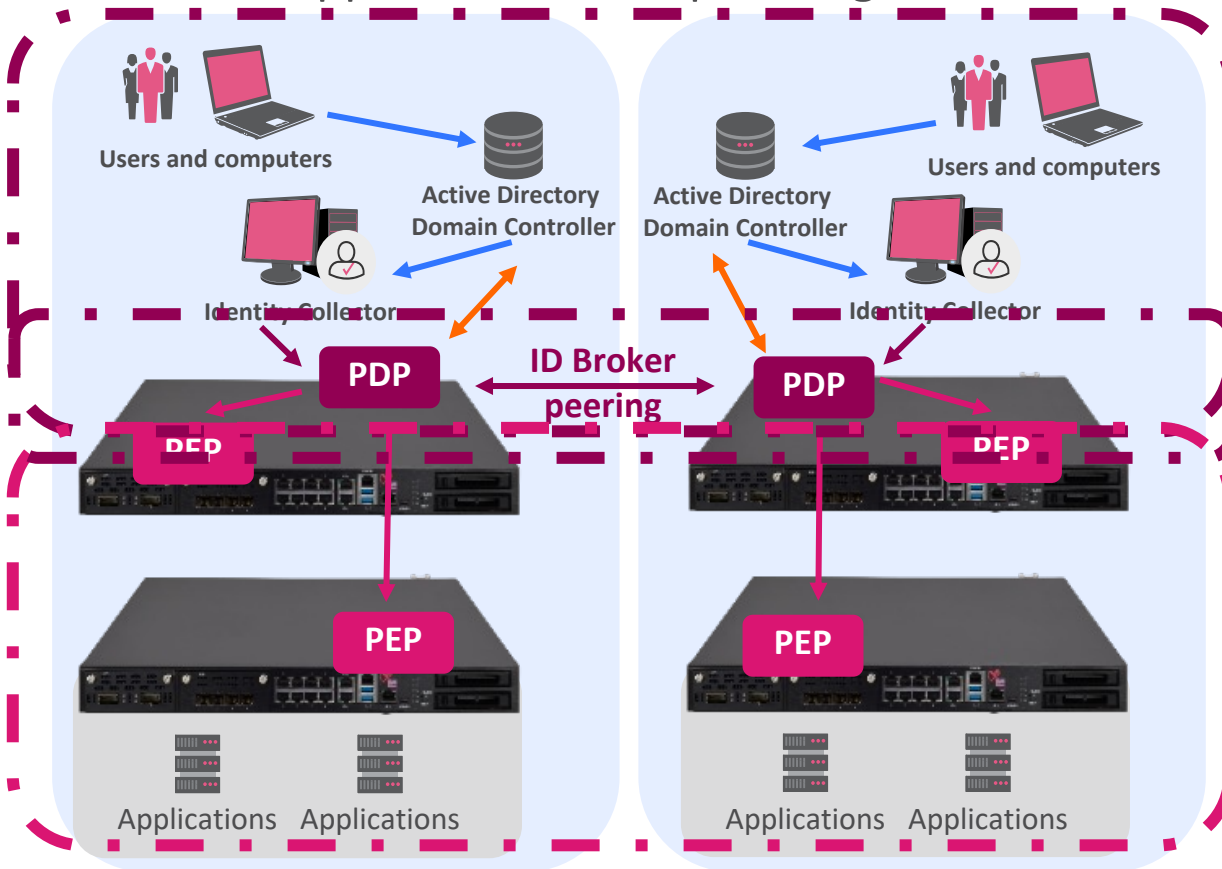
Admin Guide
ID Broker



How To Scale?

Scaling – ID Broker + ID Sharing

- User to application flow – planning for scale

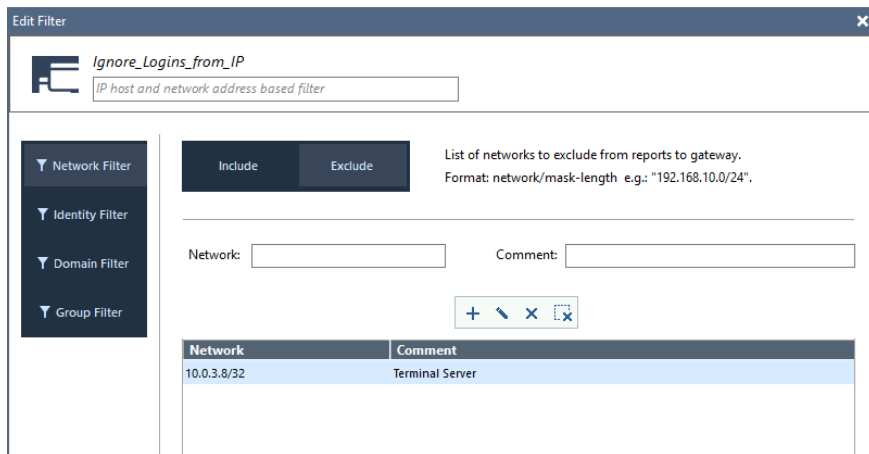


Vertical flow – user to application traffic

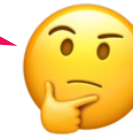
- Users accessing applications should be documented as a vertical flow
- Login events learned in most upper layer
- ID Session are shared vertical towards lower layers – closer to applications
- Horizontal scale provided by ID Broker peering

How To Scale?

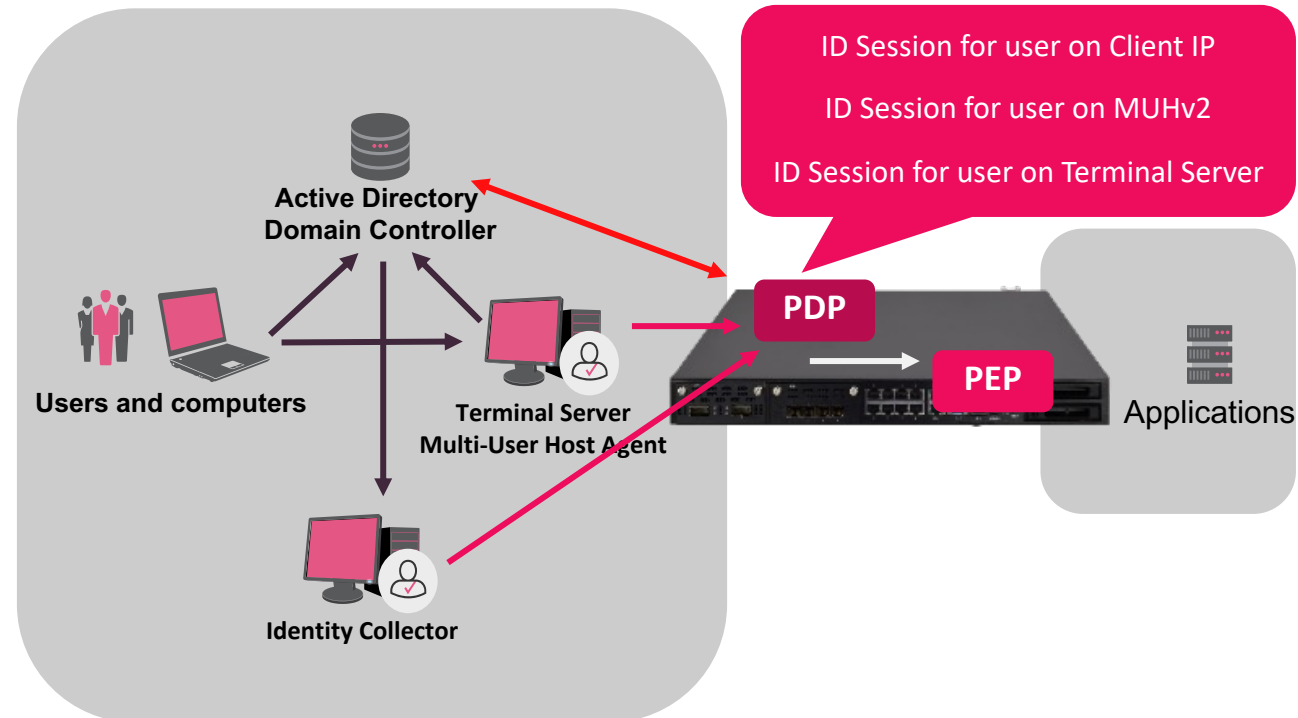
- Filtering login events
- Important when using multiple ID sources
 - Exclude/include domains, identities or networks
- Create a filter excluding login events related to the IP address of the Terminal Server



Do I need all these ID sessions?



Admin Guide
Filtering

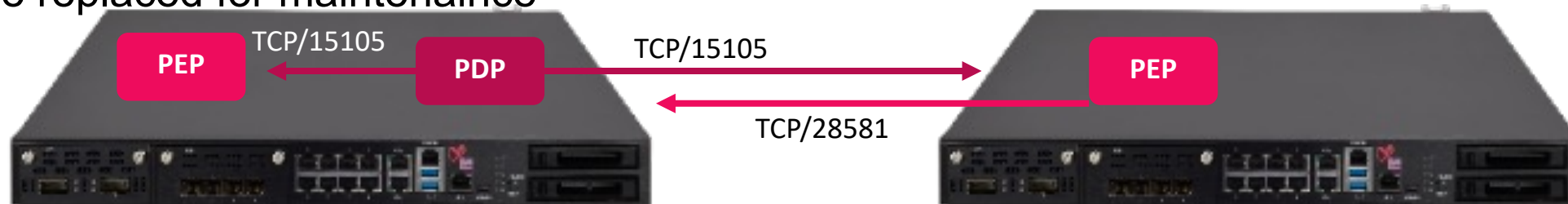


What's next?

Improving Resilience Cache Mode

Coming soon in R81.20 JHF – sk181613

- What if the PEP does not “hear anymore” from the PDP or and ID Broker from it’s peer?
- After 10 min all ID Sessions are deleted
- PDP/PEP aims to reconnect and initiates ID Session synchronization
- In large scale environments or WAN scenarios this may lead to traffic outage and high CPU load
- Cache Mode (available since R81.20 JHF 38, disabled by default, currently evaluated by key customers)
- Principle ‘prefer to keep’ maintains ID Sessions allowing traffic to flow
- Example: 120k ID Sessions are maintained across 8 ID Broker peers while cluster members are replaced for maintenance



Improving Scale Upcoming Release

Content subject to change as it relates to work in-progress
Please work with local Check Point Sales representative for updates

- **Sharing of Identity Sessions**
 - Single identity core gateway (PDP) sharing with hundreds enforcing gateways (PEPs)
 - **How is this possible?**
 - Change of communication infrastructure
 - Use of HTTPS instead of two distinct TCP connections
 - New PDP auto-scaling infrastructure benefitting from multiple CPUs and using REST API for internal communication
 - **What's the impact for customers?**
 - Simplified ID sharing architecture for new projects
 - Saving resources for existing ID sharing architecture
 - Scaling up existing
- **Identity Agent scenarios**
 - Increase number of ID Agents terminating on PDP
 - **How is this possible?**
 - PDP infrastructure becoming multi-processed
 - Gaia OS infrastructure is improved
 - **What's the impact for customers?**
 - Simplified architecture
 - Scaling up "login events/second" on PDP
 - Scaling up number of ID Agents terminating on PDP

Target delivery: EA scheduled H2'24

ID Agent Support For SAML

- An RFE version of ID Agent is available
- Supporting Microsoft Entra ID
- Reach out your local Check Point Sales contact

SAML Authentication Support for Identity Agent

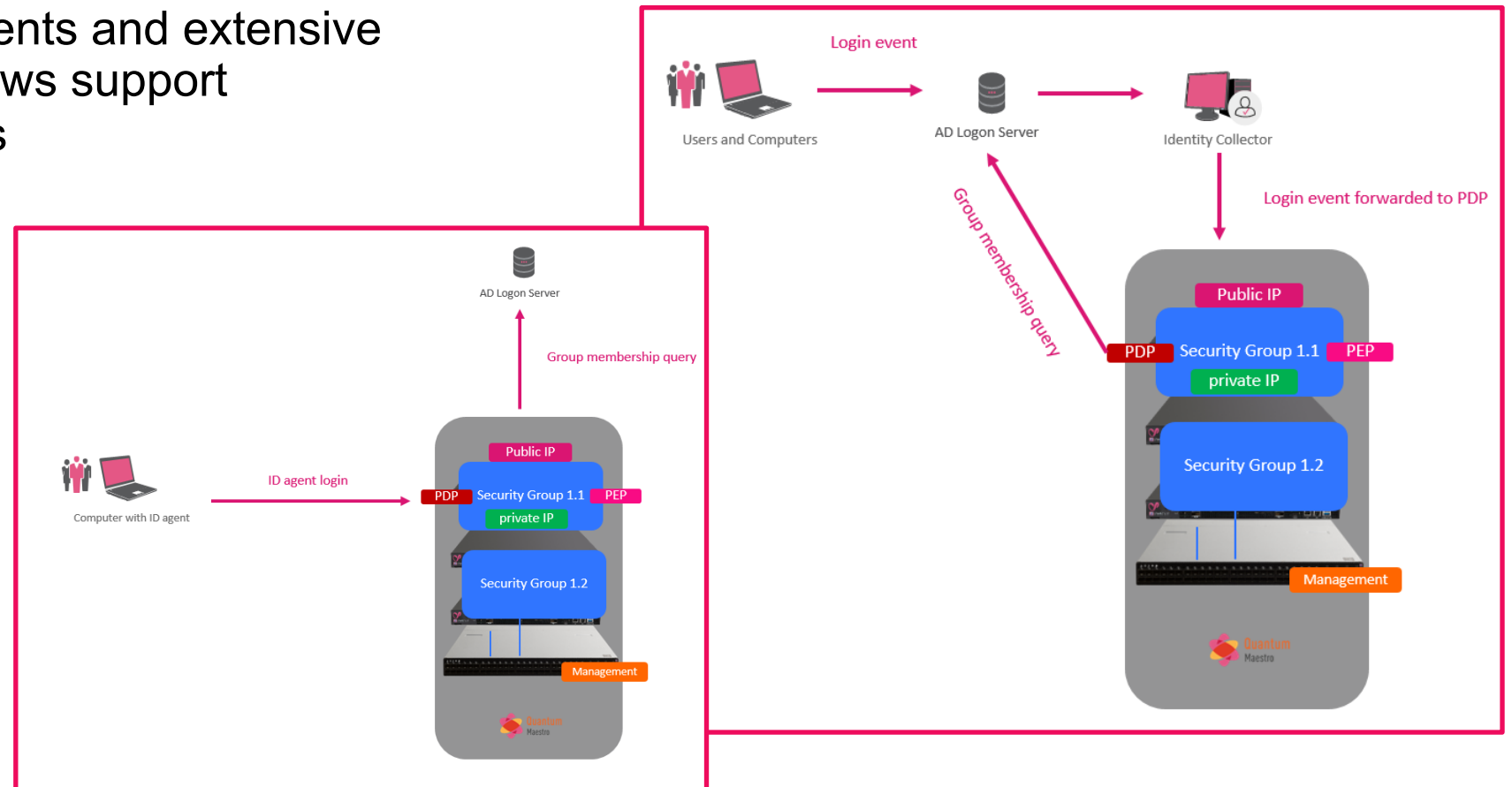
This release adds SAML support for Microsoft Entra ID user authentication using Identity Agent on top of Gaia R81.20 with Jumbo Hotfix Accumulator Take 26 installed.

Prerequisites

- Security Gateway R81.20 with the R81.20 Jumbo Hotfix Accumulator Take 26.

Maestro Supporting PDP sk175587 is getting updated

- Maestro load sharing presented challenges when terminating ID Sources
- Software improvements and extensive tests in QA labs allows support for certain scenarios
 - ID Collector
 - ID Agents
 - Web API





Thank You

YOU DESERVE THE BEST SECURITY