cisco Live!

Let's go

The bridge to possible

Knock, knock. Who is there behind your firewall?

All about identity on a Cisco Secure Firewall Threat Defense

Christopher Grabowski
Technical Marketing Engineer, Technical Leader

Your Speaker

- Based in Warsaw, Poland
- With Cisco since May 2012
- Started with TAC Security, then Advanced Services, now Technical Marketing Engineer
- Focusing on Identity Firewall, Integrations and TLS Decryption
- Enjoys cooking and spending time with the family

Christopher Grabowski
Technical Marketing Engineer
CCIE Security #42466

Housekeeping…

It’s a 90 minutes session…

Procedure

Step	Log in to the management c er.
Step 2	Click **Policies** > **Acc Control** > **Identity** and
Step 3	Enter a **Name** , optionally, a **Description**.
Step 4	Clic .
Step 5	T d a ru the policy, click **Add Rule** as d
Step 6	To create a rule ca ory, click **Add Category**.
Step 7	To configure captive port tive authenticatio
Ste	(Optional.) To filter traffic by netw object, cli
Step 9	Click **Save** to save the identity policy.

It won’t be a step by step configuration guide…

Download the PDF version of this deck– there is a ton of reference slides.

All slides = Death by PowerPoint…

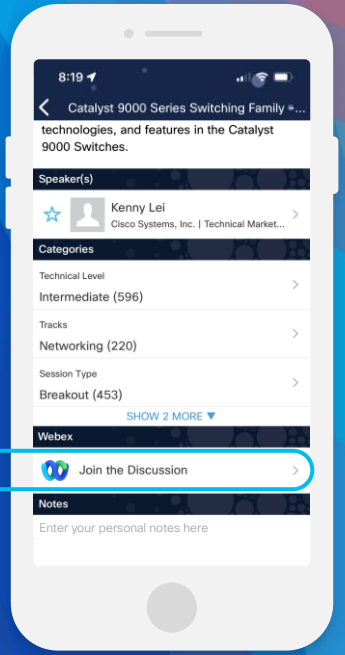
Webex App

Questions?

Use the Webex App to chat with the speaker after the session

How

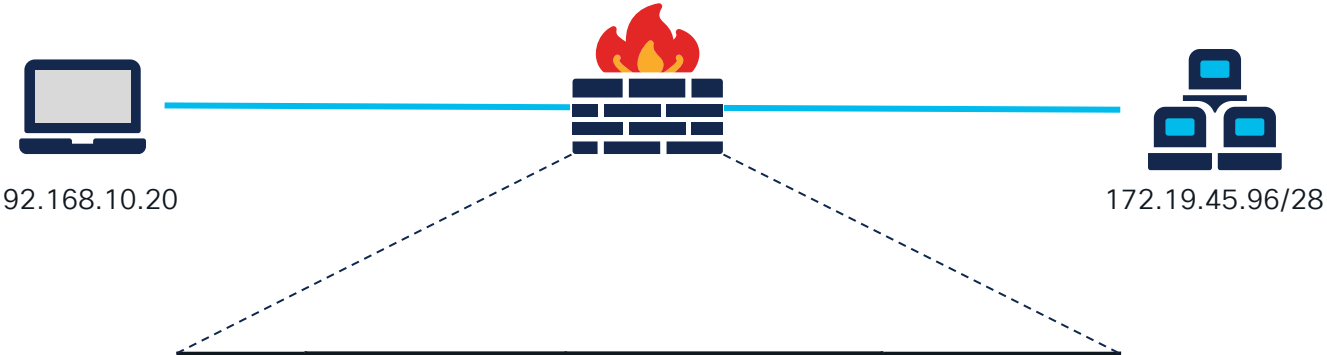
1. Find this session in the Cisco Events Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space



https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2590

Webex spaces will be moderated by the speaker until February 23, 2024.

Traditional Firewall Policy is not Enough



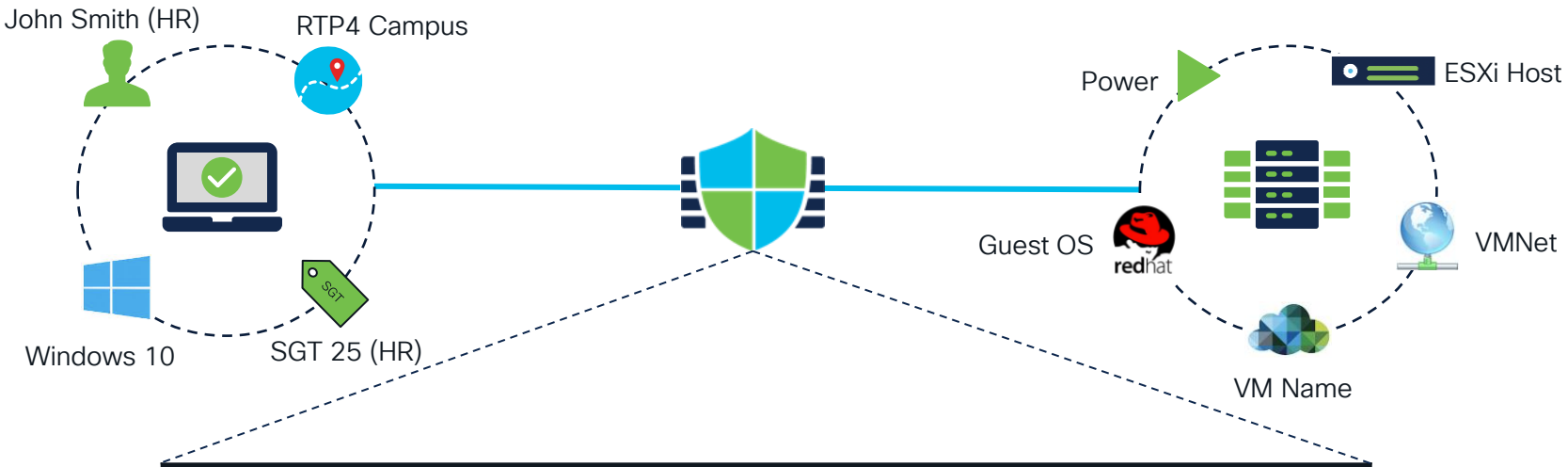
Action	Source	Destination	Service
✔	192.168.10.20	172.19.45.96/28	TCP 80, 443

"Through 2023, 99% of firewall breaches will be caused by firewall misconfigurations, not firewall flaws."

Technology Insight for Network Security Policy Management

Gartner

Shift Towards Intent Based Policy



Action	Source	Destination	Service
✔	HR Users in RTP4 Campus on Windows10	PoweredOn servers in UAT VMNet containing HR-Prod in the VM Name	TCP 80, 443

Agenda

- Introduction – User Identity
- Traffic Based User Discovery
- Passive User Authentication
  - ISE-PIC
  - ISE with RADIUS/802.1x
  - ISE with TrustSec
  - Terminal Services Agent
- Active User Authentication
  - Captive Portal
  - Remote Access
- Server Identity
- Conclusion

Introduction – User Identity

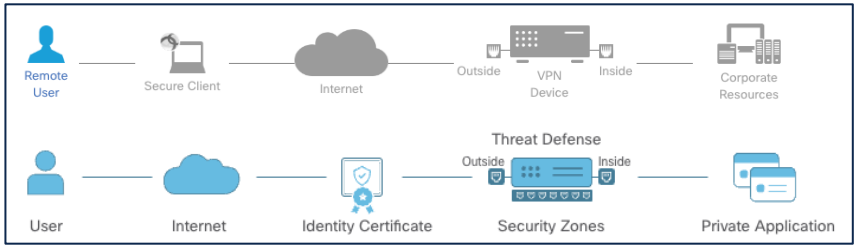
Why do we want to know the identity?

	Time	Event Type	Action	Source IP	Source User	Destination IP	Destination Port / ICMP Code
›	2024-01-10 **13:36:35**	Intrusion	Block	172.16.137.97	lisa simpson (emealab.local\lisa, LDAP)	54.244.207.239	80 (http) / tcp
›	2024-01-10 **13:36:35**	Intrusion	Block	172.16.137.97	lisa simpson (emealab.local\lisa, LDAP)	54.244.207.239	80 (http) / tcp
›	2024-01-10 **13:36:30**	Connection	Block	172.16.137.97	lisa simpson (emealab.local\lisa, LDAP)	54.244.207.239	80 (http) / tcp
›	2024-01-10 **13:36:07**	Connection	Allow	172.16.137.97	lisa simpson (emealab.local\lisa, LDAP)	54.244.207.239	80 (http) / tcp

User Awareness – Visibility

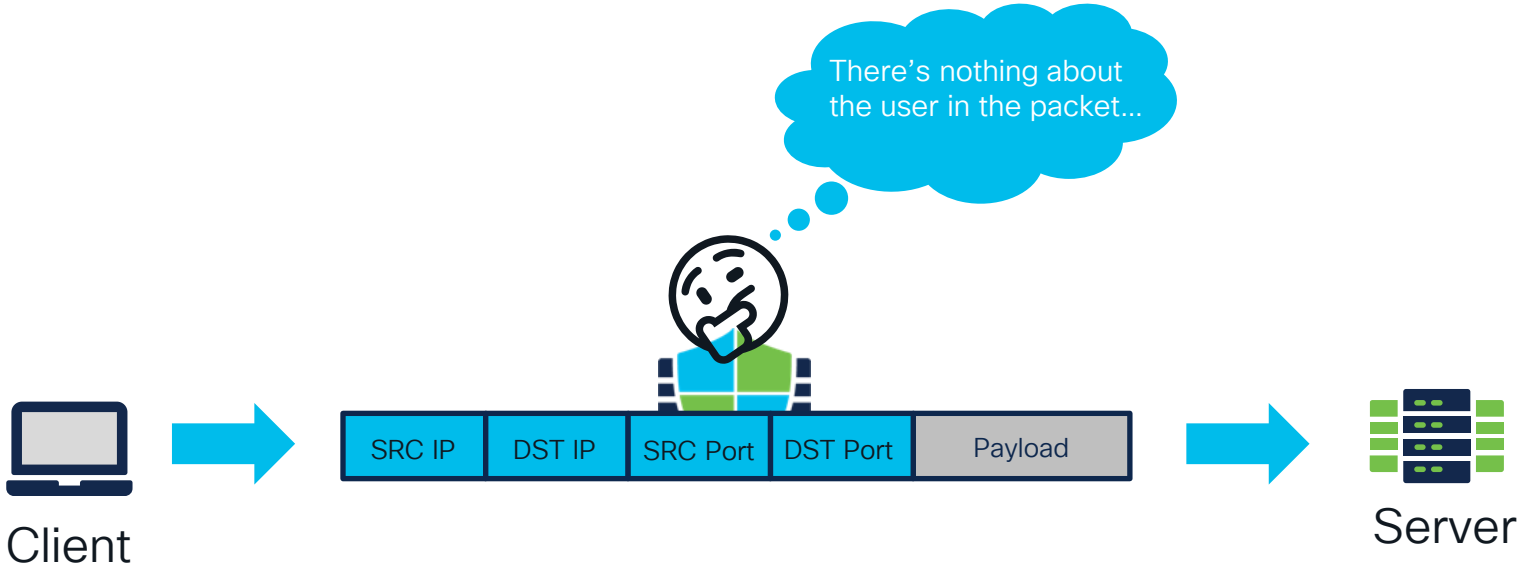
User Control – Identity Based Firewall Enforcement

	Name	Action	Sources	Destinations and Applications
Mandatory (1 - 1)				
1	Block Facebook Access	Block	USER emealab.local/HR, emealab.local/IT, emealab.local/lisa; DYN SGT_HR, SGT_IT	APP Facebook

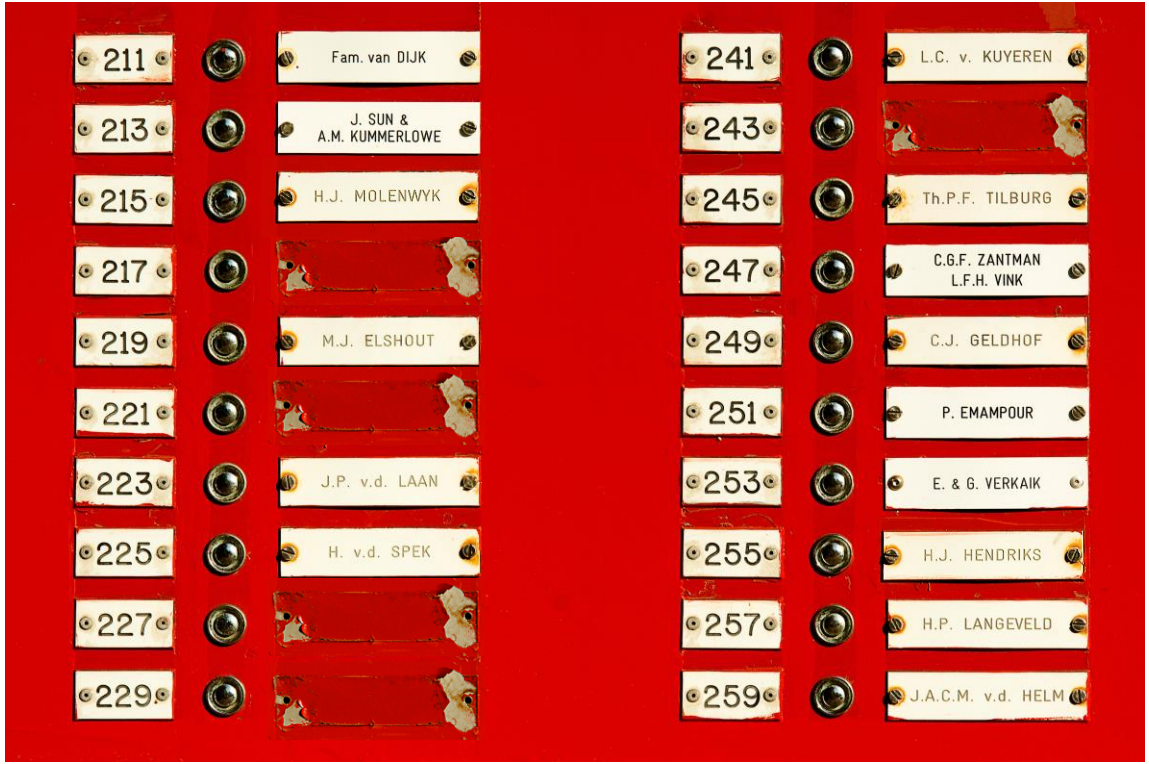


Remote Access – VPN / Zero Trust Access

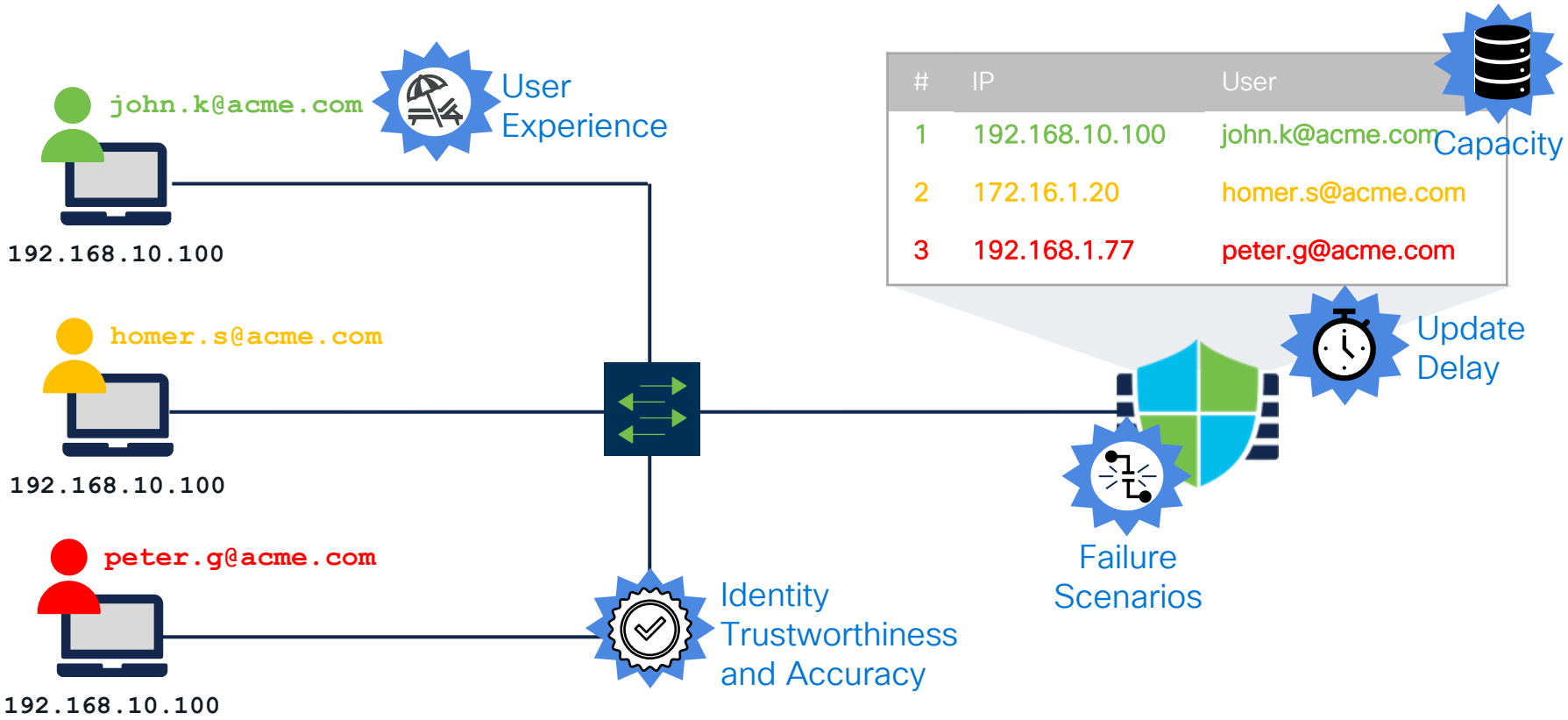
How can the firewall figure out who sent a packet?



It is not easy to find out who lives at a given address…



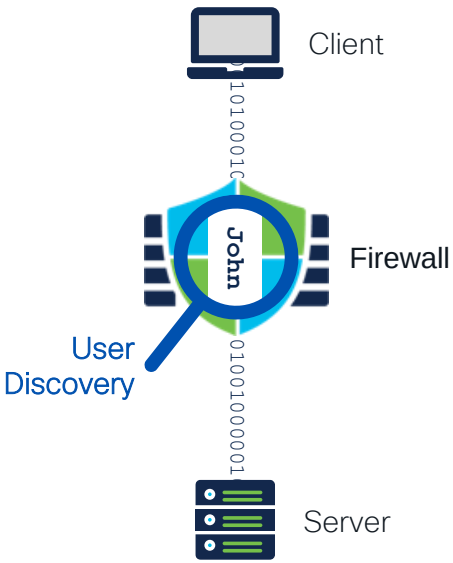
We need to build and maintain a user map



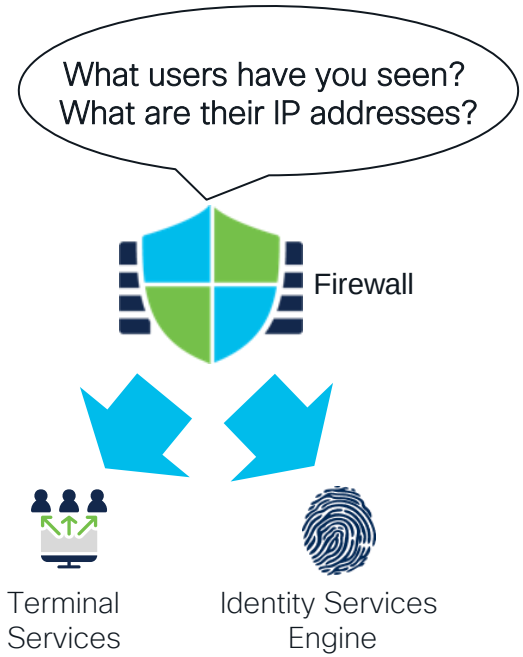
#	IP	User
1	192.168.10.100	john.k@acme.com
2	172.16.1.20	homer.s@acme.com
3	192.168.1.77	peter.g@acme.com

Learning User Mappings

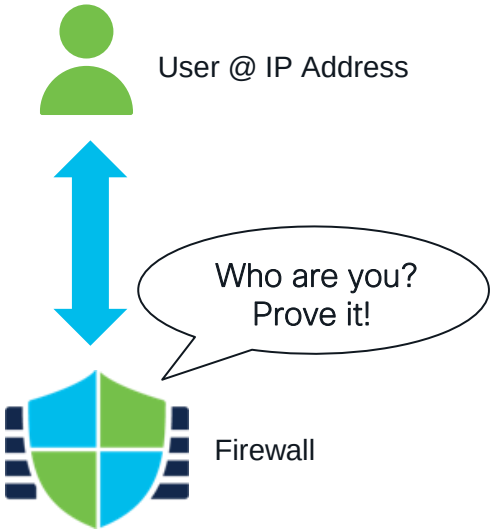
Traffic-Based Detection



Passive Authentication

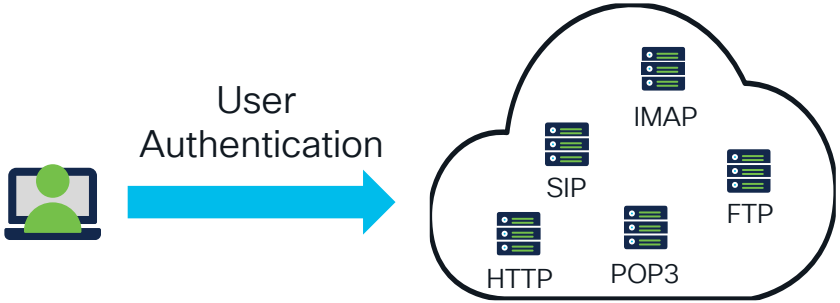


Active Authentication



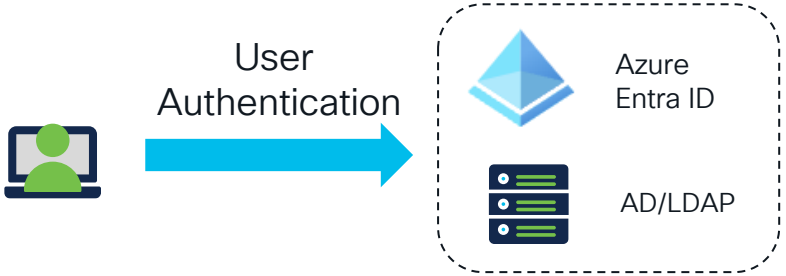
How much do I trust the identity source?

Non-Authoritative Logins



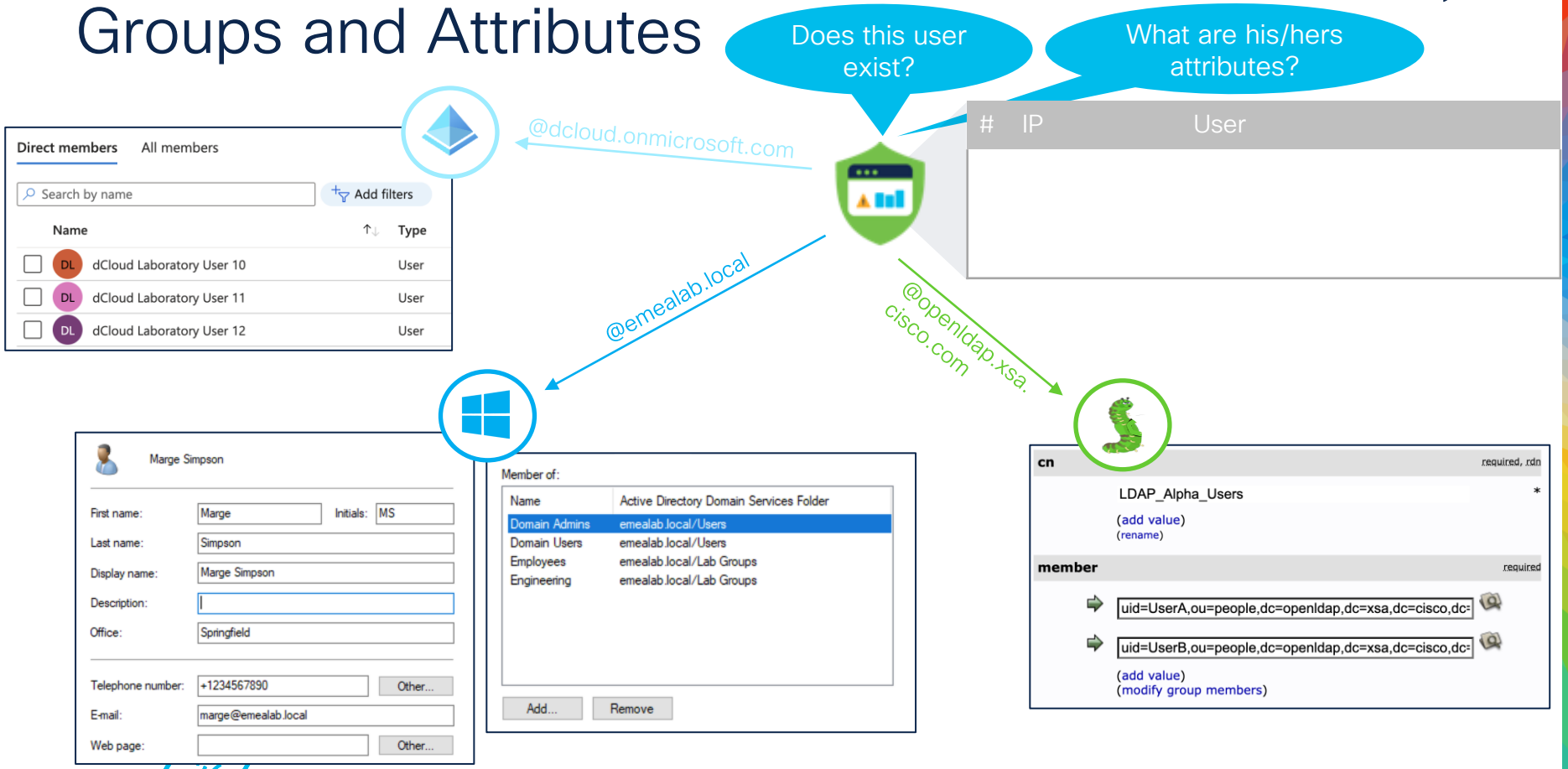
Unknown or untrusted servers

Authoritative Logins



Trusted Identity Stores

Realm makes a store trusted – Download Users, Groups and Attributes



Realm Configuration

Realm Configuration | User Session Timeout

Client ID*
2c13f723-bda7-4db8-a357-523b4053668d

Client Secret*
••••••••

Tenant ID*
b26f4c82-cf2b-40a2-9db0-33c93d3bb072

Event Hubs Host Name*
NetSecTMEs-dCloud.servicebus.windows.net

Event Hub Name*
Cisco-NetSecTMEs-dCloud

Consumer Group Name*
$Default

Event Hub Connection String*
Endpoint=sb://azuremonitor-cisco-netsectme

Excluded User Groups
Enter each group name on a separate line
Group_Name1
Group_Name2

Directory access credentials.

Directory tenant/domain.

Connection details.

Specify which users/groups are cached by Management Center.

Name*
acme.com

Description
ACME AD Realm

Type
AD

AD Primary Domain*
acme.com
E.g. domain.com

Directory Username*
administrator@acme.com
E.g. user@domain.com

Directory Password*
••••••••••

Base DN*
DC=acme,DC=com
E.g. ou=group,dc=cisco,dc=com

Group DN*
CN=GROUPS,DC=acme,DC=com
E.g. ou=group,dc=cisco,dc=com

Directory Server Configuration

ad-dc-server.acme.com:636

Hostname/IP Address*
ad-dc-server.acme.com

Port*
636

Encryption
LDAPS

CA Certificate*
Win-Server-2019-Root-CA

Interface used to connect to Directory server
Resolve via route lookup
Choose an interface
Default: Management/Diagnostic Interface

Test

Cancel | Configure Groups and Users

Putting All Together – Identity Policy

Decide for which network flows, the firewall looks up the user.

For a portion of network traffic, you may request an active authentication with Captive Portal.

For another set of flows, rely on passive identity or VPN user mappings.

Save Cancel

Rules | Active Authentication | Identity Source

+ Add Category + Add Rule Search Rules

	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Source Ports	Dest Ports	Realm	Action	Auth Protocol
Administrator Rules											
1	Authentication Exemption	V137 (Routed)	any	any	Windows_Server_2019	any	any	any	none	No Authentication	none
						any	any	any	emealab.local (AD)	Active Authentication	HTTP Response Page
3	emealab.local	V136 (Routed) V137 (Routed)	any	any	any	any	any	any	emealab.local (AD)	Passive Authentication	HTTP Response Page
4	Remote Users	any	any	AC_Pool_172.16.255.0_28	any	any	any	any	emealab.local (AD)	Passive Authentication	none
Root Rules											

Putting All Together – Identity Policy

For each rule you specify the Authentication Realm.

You can fallback to Captive Portal if passive/VPN identity is unavailable.

Enter Description

Rules | Active Authentication | Identity Source

	Name	Source Zones	Dest Zones	Source Networks	Dest Networks							
Administrator Rules												
1	Authentication Exemption	V137 (Routed) V136 (Routed)	any	any	Windows_Server_2019							
Standard Rules												
					157.240.247.35 212.77.98.9	any	any	any	emealab.local (AD)	Active Authentication	HTTP Response Page	
					any	any	any	any	emealab.local (AD)	Passive Authentication	HTTP Response Page	
4	Remote Users	any	any	AC_Pool_172.16.255.0_28	any	any	any	any	emealab.local (AD)	Passive Authentication	none	
Root Rules												
This category is empty												

Authentication Realm *

emealab.local (AD)

☑ Use active authentication if passive or VPN identity cannot be established

☐ Identify as Special Identities/Guest if authentication cannot identify user

Authentication Protocol

HTTP Response Page

▶ HTTP User Agent Exclusions

Associate Identity with Access Control Policy

Firewall Policy

Packets → Prefilter Rules → Decryption → Security Intelligence → Identity → Access Control | More

Type to search

Total 22 rules

Sources

Identity Policy is a sub-policy of Access Control Policy.

Identity Policy

Identity Policy

Identity Policy Edit

Discard Apply

Default (1 - 22)

USER

1 Block Facebook Access Block

emealab.local/IT

emealab.local/Lab Machines

emealab.local/Management

2 Custom URL List...

ZONE V136

Once you associate the Identity Policy, you can configure user-based firewall rules.

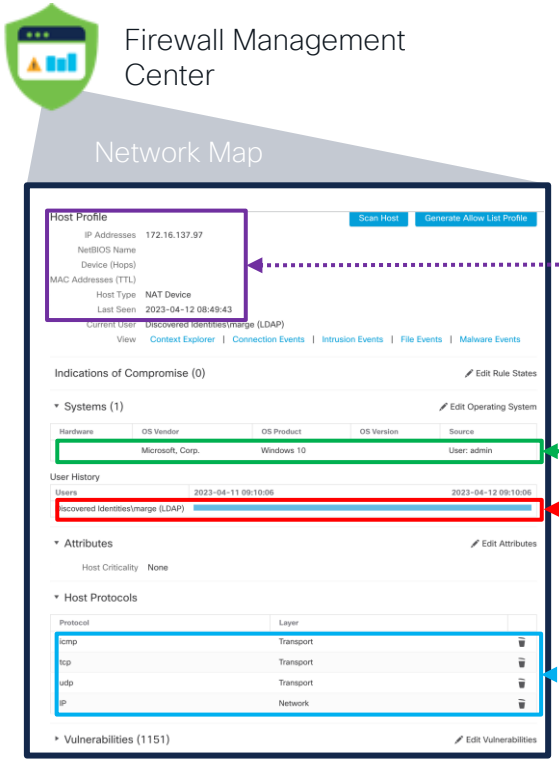
User Identity Sources

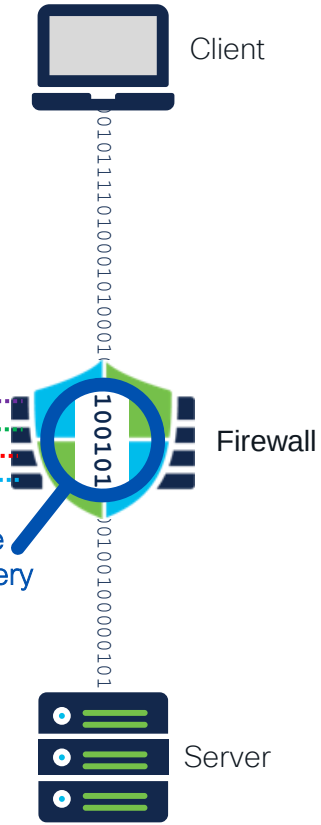
[1] – Access Control Policy
[2] – Zero Trust Access Policy
[3] – Dynamic Access Policy

User Identity Source	Authentication Type	Realm / Server Requirements	Available Firewall Policy Attributes	Enforcement
Traffic-based Detection	N/A	Protocols supported in Discovery Policy	N/A	N/A
ISE-PIC	Passive	Microsoft AD	User, Group	ACP[1]
ISE (802.1x)	Passive	Microsoft AD Azure EntraID	User, Group, ISE profile, NAD IP, User-SGT	ACP
ISE (SXP)	Passive	None	Inline SGT, IP-SGT, Subnet-SGT	ACP
TS Agent	Passive	Microsoft Windows Terminal Server	User, Group	ACP
Captive Portal	Active	Microsoft AD OpenLDAP	User, Group	ACP
Remote Access VPN	Active	Microsoft AD OpenLDAP Azure EntraID Certificate	User, Group	ACP, Traffic-Filter, DAP[3]
ZTNA Clientless	Active	SAML IdP	N/A	ZTA[2]

Traffic-Based User Detection

Traffic-Based User Discovery





Host Profile

Operating System

Users

Applications and Services

Host Profile and User Visibility

Firewall Management Center

Network Map

Host Profile

Scan Host | Generate Allow List Profile

IP Addresses	172.16.137.97
NetBIOS Name	
Device (Hops)	
MAC Addresses (TTL)	
Host Type	NAT Device
Last Seen	2023-04-12 08:49:43
Current User	Discovered Identities\marge (LDAP)
View	Context Explorer | Connection Events | Intrusion Events | File Events | Malware Events

Indications of Compromise (0) — Edit Rule States

Systems (1) — Edit Operating System

Hardware	OS Vendor	OS Product	OS Version	Source
	Microsoft, Corp.	Windows 10		User: admin

User History

Users	2023-04-11 09:10:06	2023-04-12 09:10:06
Discovered Identities\marge (LDAP)		

Attributes — Edit Attributes

Host Criticality None

Host Protocols

Protocol	Layer
icmp	Transport
tcp	Transport
udp	Transport
IP	Network

Vulnerabilities (1151) — Edit Vulnerabilities

User Identity

Last Seen	2024-01-17 21:42:50
Realm	emealab.local
Username	homer
First Name	homer
Last Name	simpson
Email	homer@emealab.local
Department	lab users (lab)
Phone	
Discovery Application	LDAP
Active Session Count	1
View	Context Explorer

Indications of Compromise (2) — Edit Rule States | Mark All Resolved

Category	Event Type	Description	First Seen	Last Seen
Suspicious Activity	Encrypted Visibility Engine	Probable Malware Communication	2023-11-03 13:47:44	2024-02-02 13:09:41
Malware Detected	Threat Detected in File Transfer	The host has encountered malware	2023-03-30 11:52:19	2023-03-30 11:52:19

User History

Users	2024-01-04 12:11:33	2024-01-05 12:11:33
Discovered Identities\marge (LDAP)		
Discovered Identities\homer (LDAP)		
Discovered Identities\lisa (LDAP)		
Discovered Identities\bart (LDAP)		

Discovery Policy Configuration

Enable user discovery.

Edit Rule

Discover

Hosts | Users | Applications

Networks | Zones | Port Exclusions

Available Networks (19)

Search by name or value

any
IPv4-Private-All-RFC1918
any-ipv4
any-ipv6
CSDAC_172.16.135.92
IPv4-Benchmark-Tests
IPv4-Link-Local
IPv4-Multicast

Networks (1)

IPv4-Private-172.16.0.0-12

Select network segments to be discovered.

Enter network address | Add

Networks | Users | Advanced

Traffic-Based Detection

aim	Yes
imap	Yes
ldap	Yes
oracle	
pop3	
sip	
ftp	Yes
http	Yes
mdns	Yes
Capture Failed Login Attempts	Yes

Protocols to scrub the username from.

Key Takeaways

- Traffic-based detection provides user awareness but no control
- Provided by Network Discovery subsystem
- No backend server requirements
- If you have an LDAP/AD Realm configured the system enriches host profiles with user details (department, phone number etc.)

Passive Authentication

Passive Authentication Sources

User:	SGT:	IP:	Source:
-	10	172.16.0.4	TrustSec SXP
Eric	-	172.16.0.22	PassiveID
Ira	15	172.19.1.13	RADIUS

What users have you seen?
What are their IP addresses?

User:	IP:	Port Range
Burns	172.16.0.4	2024-2223
Smithers	172.16.0.4	2224-2423
Moe	172.19.1.13	2424-2623

pxGrid

Management Center

REST

Terminal Services

Microsoft Remote Desktop Services

citrix

Identity Services Engine (Full)
OR
Passive Identity Connector (ISE-PIC)

Users, groups and metadata download

Trusted Identity Stores (Realms)

Passive Identity Connector vs. Identity Services Engine

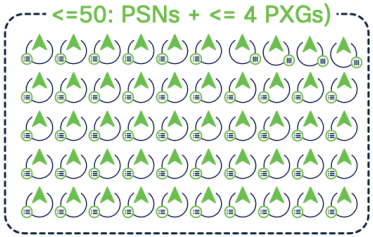
Passive Identity Connector (ISE-PIC)

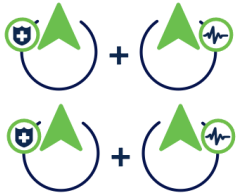
- Limited scale, 2 node deployment
- PassiveID feature set only
- License and support free of charge with Firewall Management Center
  - 3K user sessions (R-ISE-PIC-VM-K9)
  - 300K user sessions (L-ISE-PIC-UPG=)
- Can be promoted to a full ISE install or joined to an existing installation

Identity Services Engine (Full ISE)

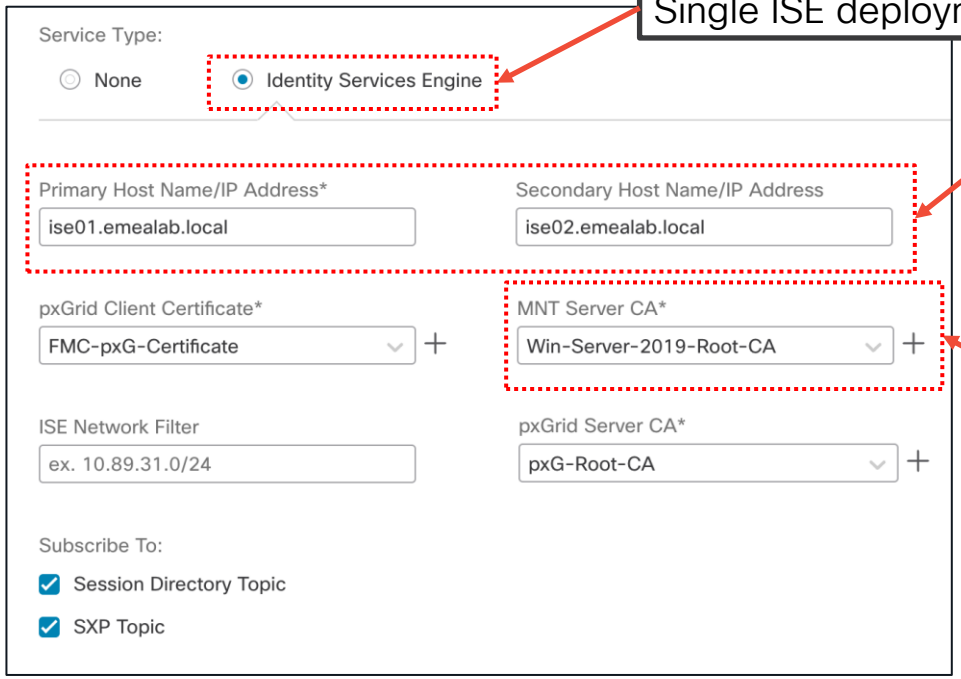
- High scale deployment up to 58 nodes
- RADIUS, 802.1x, TACACS+, Guest/BYOD, MDM, Posture, TrustSec, **PassiveID**

- **PassiveID** is incompatible with 802.1x Machine Authentication





Management Center Integration with ISE



Single ISE deployment supported.

Primary and Secondary pxGrid nodes in ISE deployment (order locally significant).

ISE MnT Root CA certificate for trusted connection. Management Center talks directly to ISE MnT node for bulk session download.

Management Center Integration with ISE

Service Type:

None | Identity Services Engine

Primary Host Name/IP Address*: ise01.emealab.local

Secondary Host Name/IP Address: ise02.emealab.local

pxGrid Client Certificate*: FMC-pxG-Certificate

MNT Server CA*: Win-Server-2019-Root-CA

ISE Network Filter: ex. 10.89.31.0/24

pxGrid Server CA*: pxG-Root-CA

Subscribe To:
- [x] Session Directory Topic
- [x] SXP Topic

Management Center's client certificate to authenticate to pxGrid infrastructure.

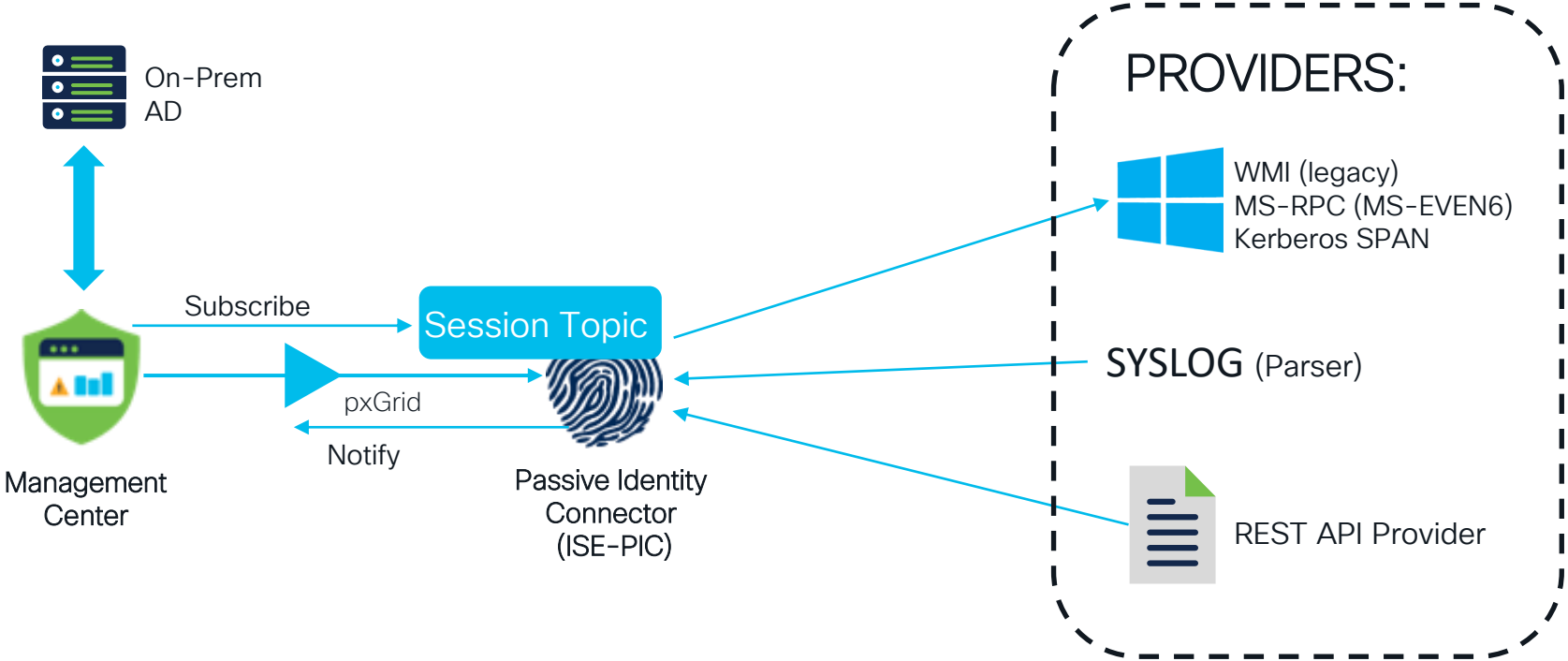
ISE pxGrid Root CA certificate for trusted connection.

pxGrid topic Management Center subscribes to:
- Session Directory – RADIUS and Passive ID user sessions
- SXP – IP-SGT mappings from SXP database

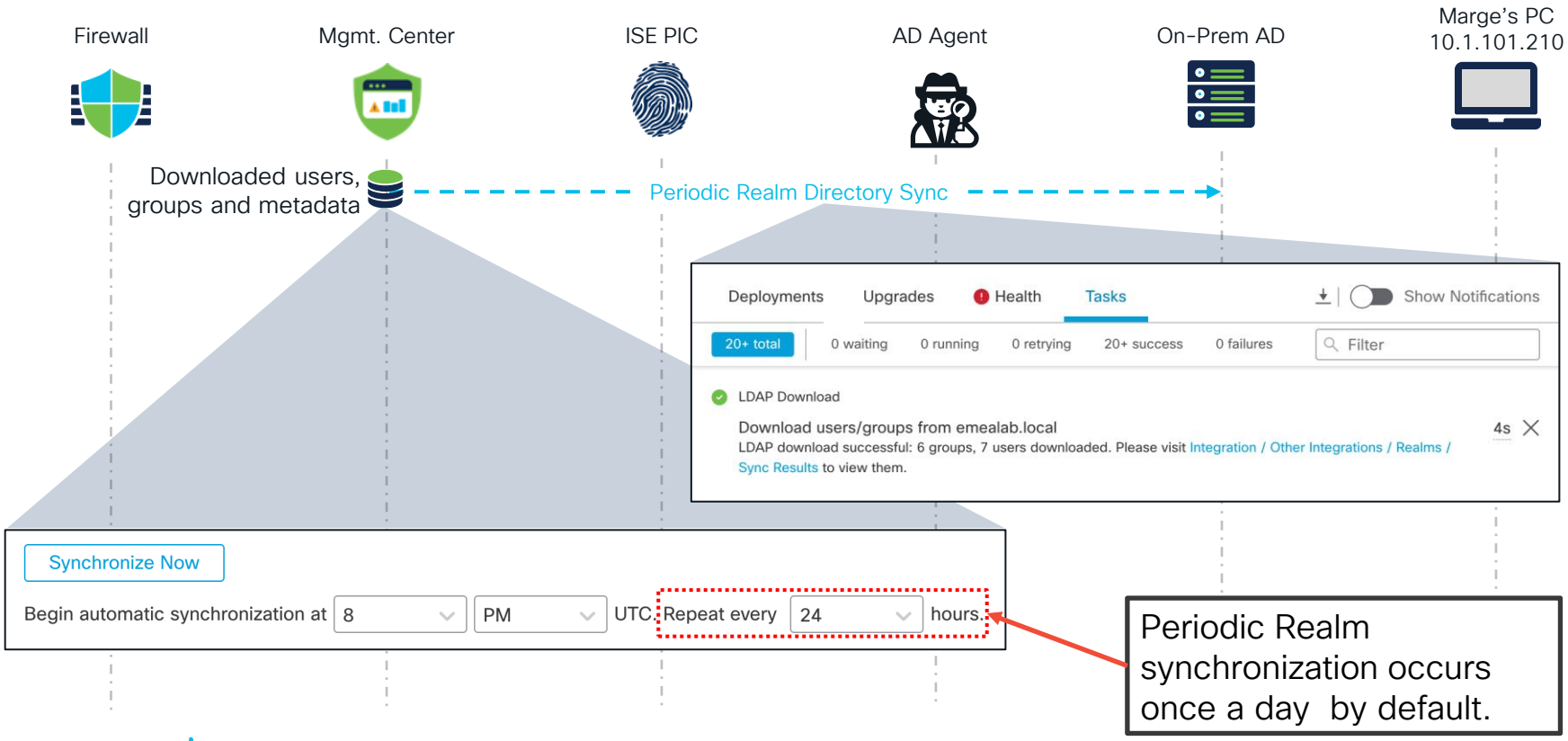
PASSIVE AUTHENTICATION

ISE Passive Identity Connector (ISE-PIC)

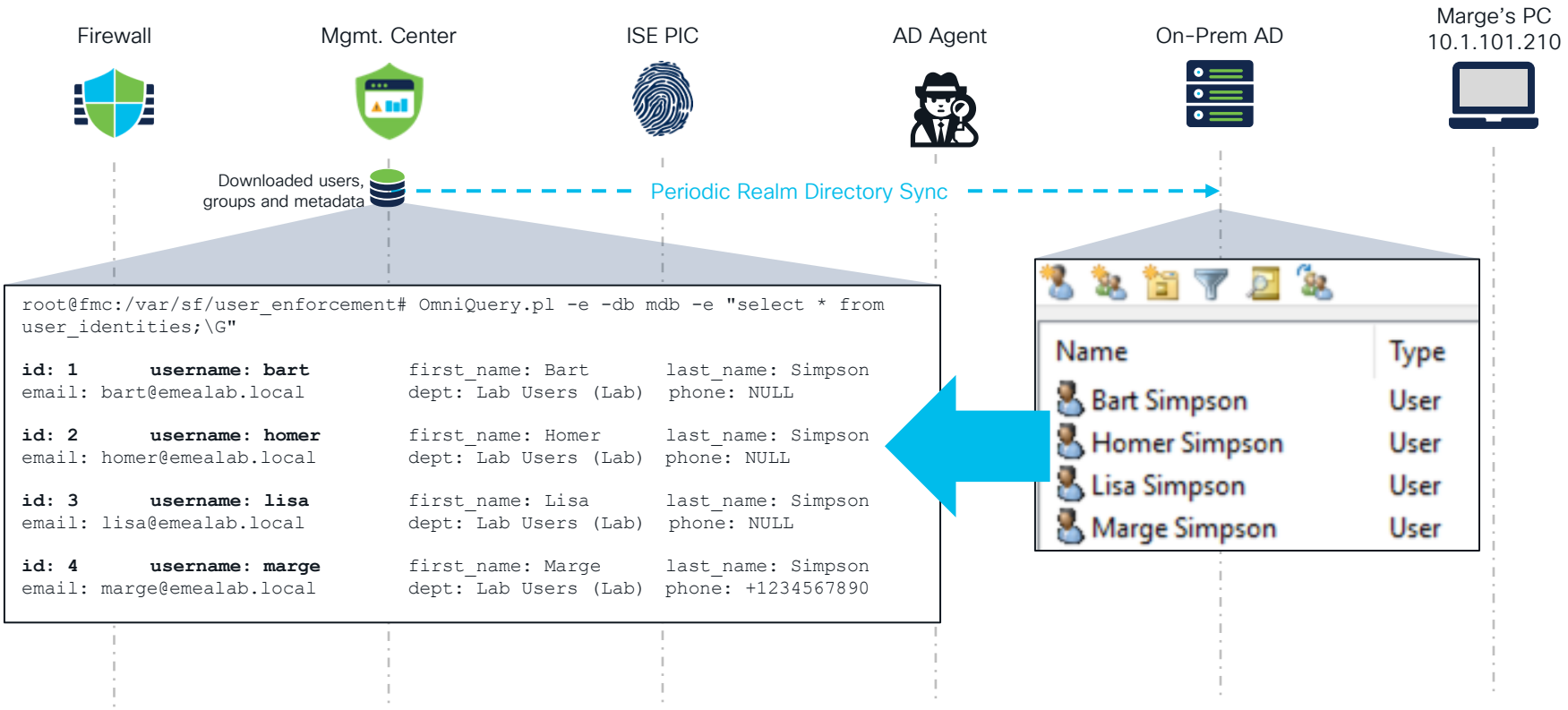
ISE Passive Identity Connector



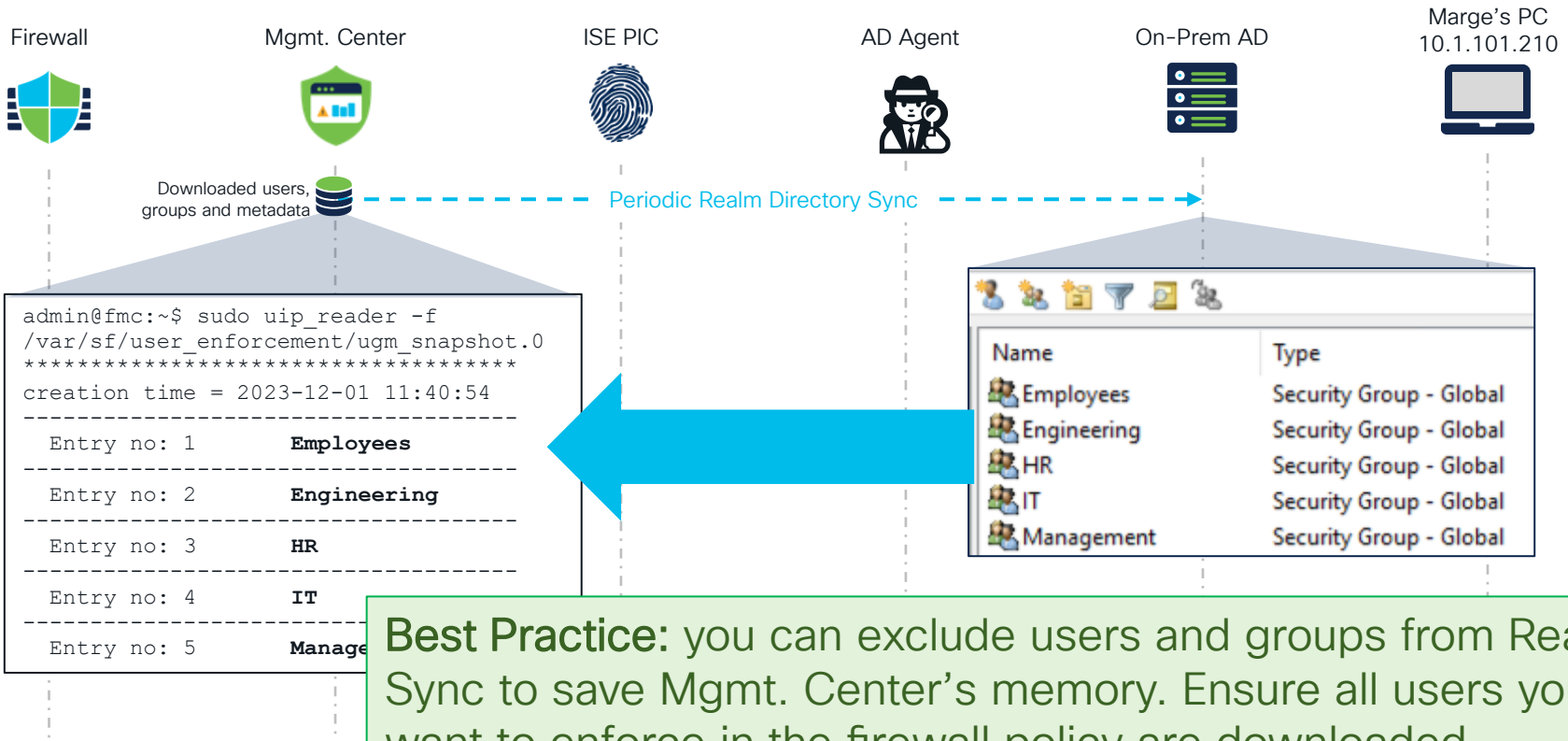
Realm Synchronization



Realm Synchronization – User Download

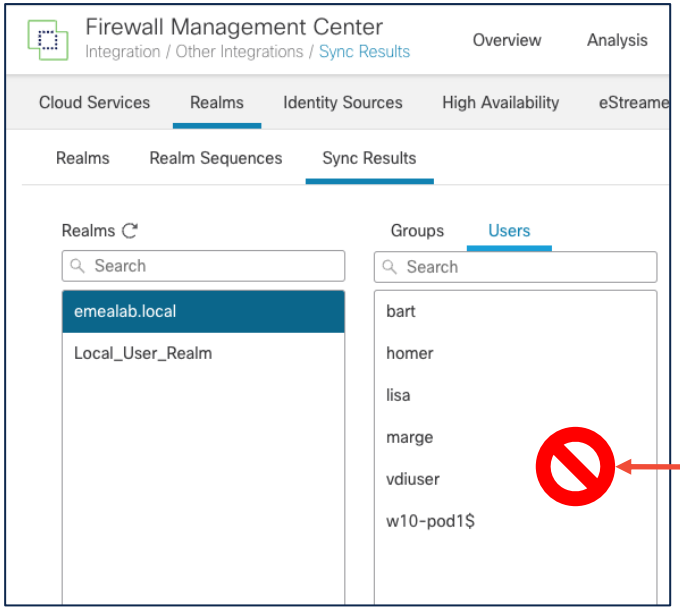


Realm Synchronization – Group Download

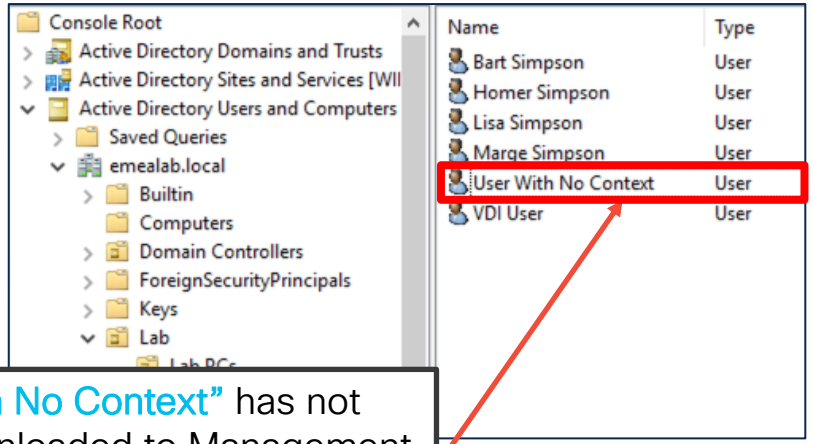


Best Practice: you can exclude users and groups from Realm Sync to save Mgmt. Center's memory. Ensure all users you want to enforce in the firewall policy are downloaded.

Un-synced Realm User = User Not Found



Previous Synch.



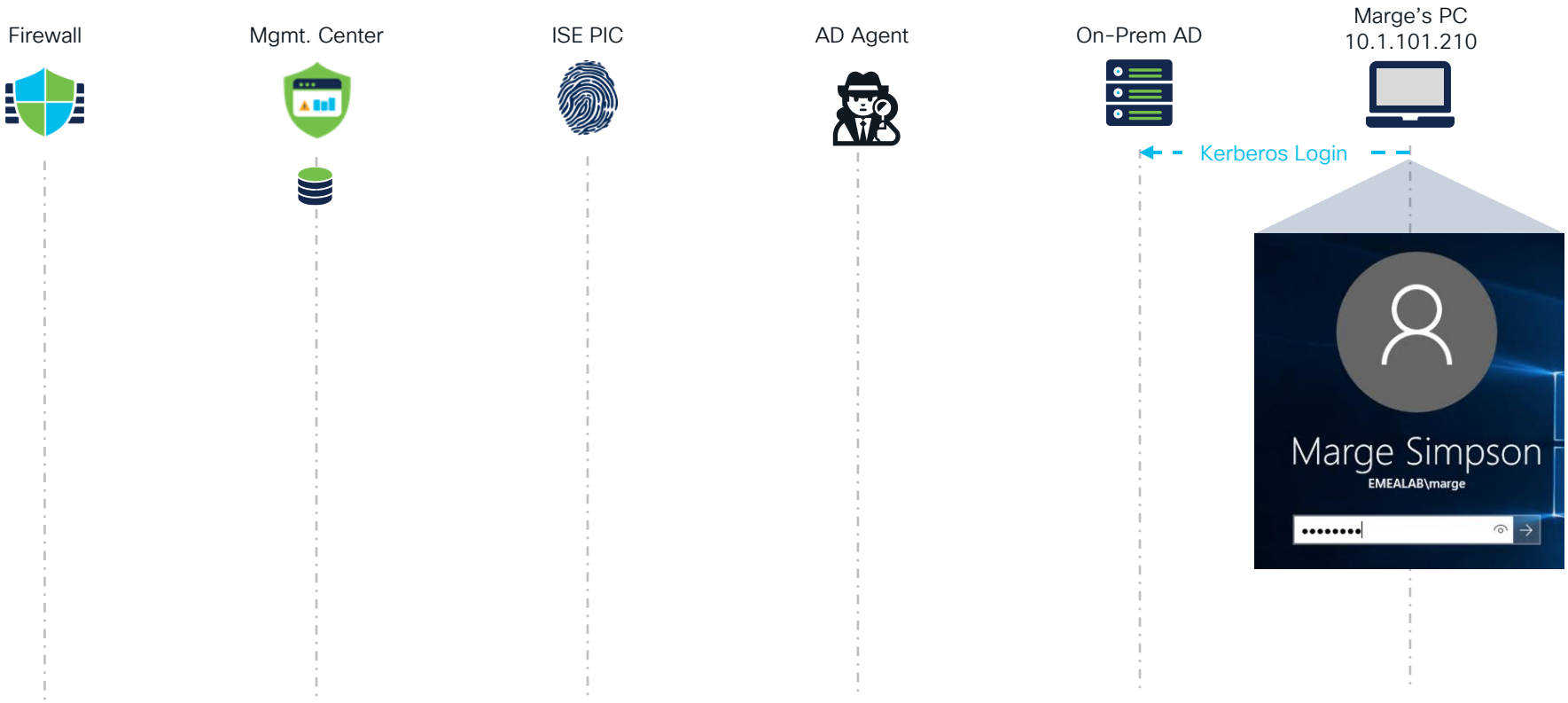
"User with No Context" has not been downloaded to Management Center (e.g. was created after periodic Realm sync).

User Lookup

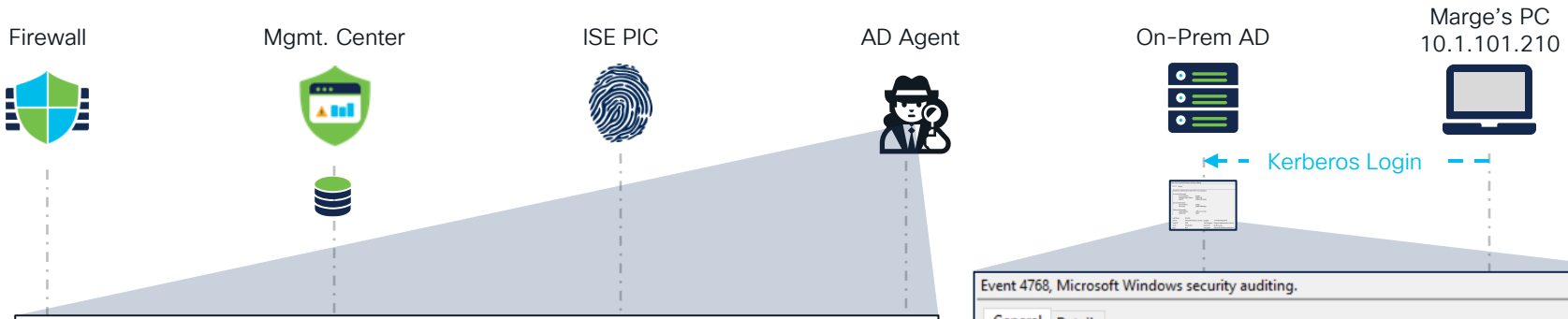
Passive Authentication of non-synced user results in unusable mapping – user is Not Found (Unknown).

Time	Event Type	Action	Source IP	Source User	Acces		
2024-01-17 **14:38:15**	Connection	Allow	172.16.136.96	Not Found	Unknown Users Limited Access	172.16.134.92	0 (No Code) / i...

ISE-PIC: AD Agent Mapping Propagation



ISE-PIC: AD Agent Mapping Propagation



AD Agent looks for any of the two messages in the Event Log:

Event 4768 – Authentication (TGT) Ticket Granted

Usually seen at the beginning of the day when users' workstation requests a TGT from local DC.

Event 4770 – TGT Renewed

Recorded after ticket expires (10h default) and users' workstation requests a renewal from local DC.

Event 4768, Microsoft Windows security auditing.

General | Details

A Kerberos authentication ticket (TGT) was requested.

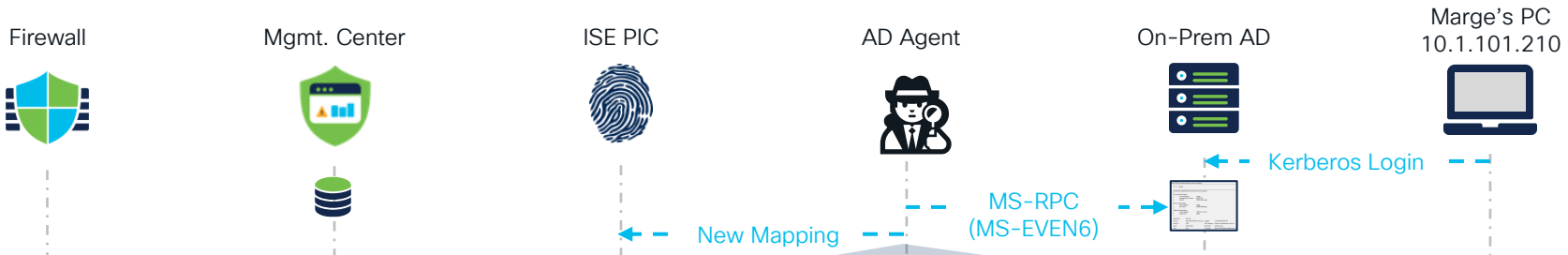
Account Information:
Account Name: marge
Supplied Realm Name: EMEALAB
User ID: EMEALAB\marge

Service Information:
Service Name: krbtgt
Service ID: EMEALAB\krbtgt

Network Information:
Client Address: ::ffff:10.1.101.210
Client Port: 49447

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	1/16/2024 6:06:52 PM
Event ID:	4768	Task Category:	Kerberos Authentication Service
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	WIN-RCI9756298A.emealab.local

ISE-PIC: AD Agent Mapping Propagation




```
***** Reading Event *******
TimeGenerated in DC UTC = 01/16/202
user = marge
domain = EMEALAB.LOCAL
ip = 10.1.101.210
```

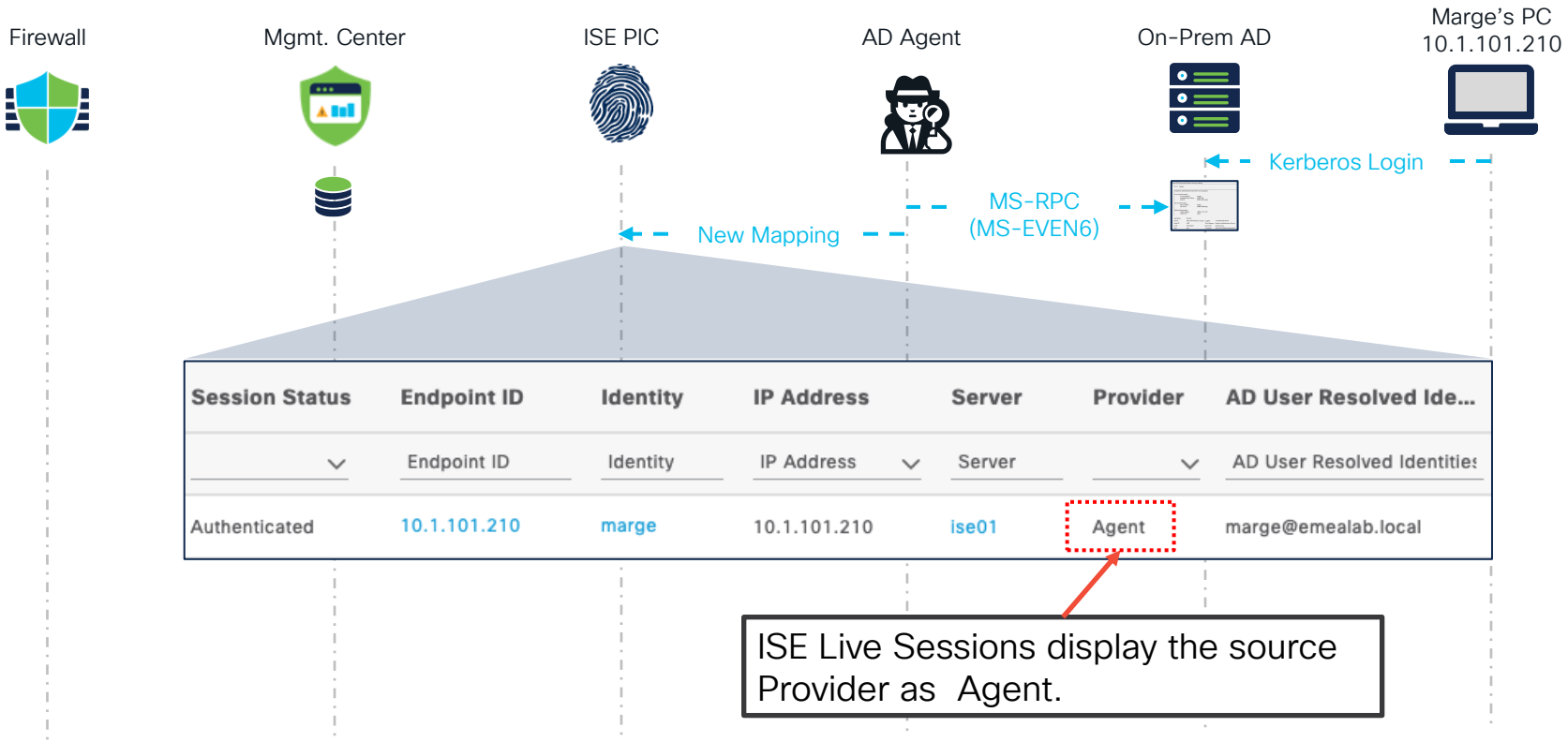
AD Agent scrubs username and IP address from the security event on Domain Controller.

```
Latency = 0.6196513 seconds
AgentTimeUTC , 01/16/2024 18:06:53

Rest Client, Sending mapping to
https://ise01.emealab.local:9095
```

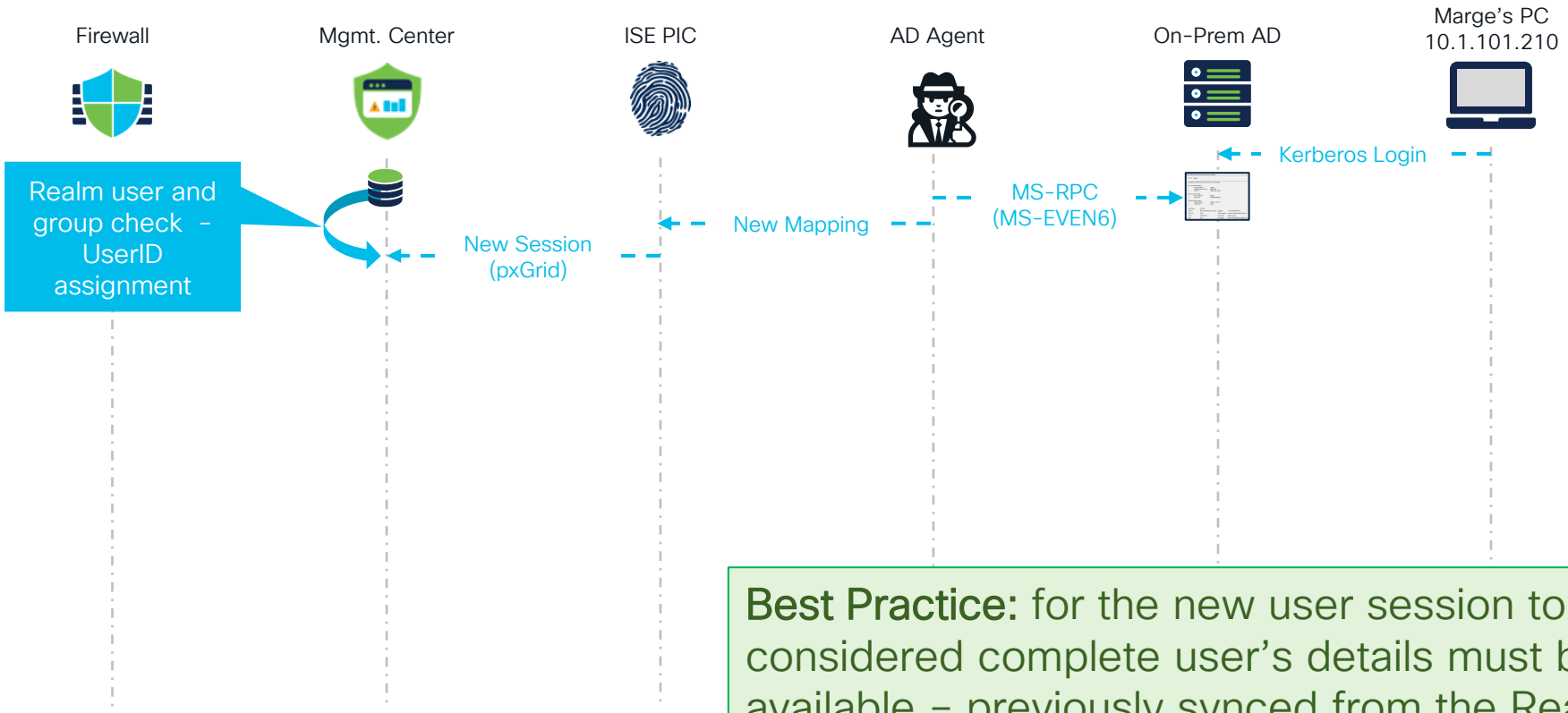
You can check the latency between the actual user login and AD Agent picking up the event.

The new mapping is sent to ISE PassiveID nodes.

ISE-PIC: AD Agent Mapping Propagation

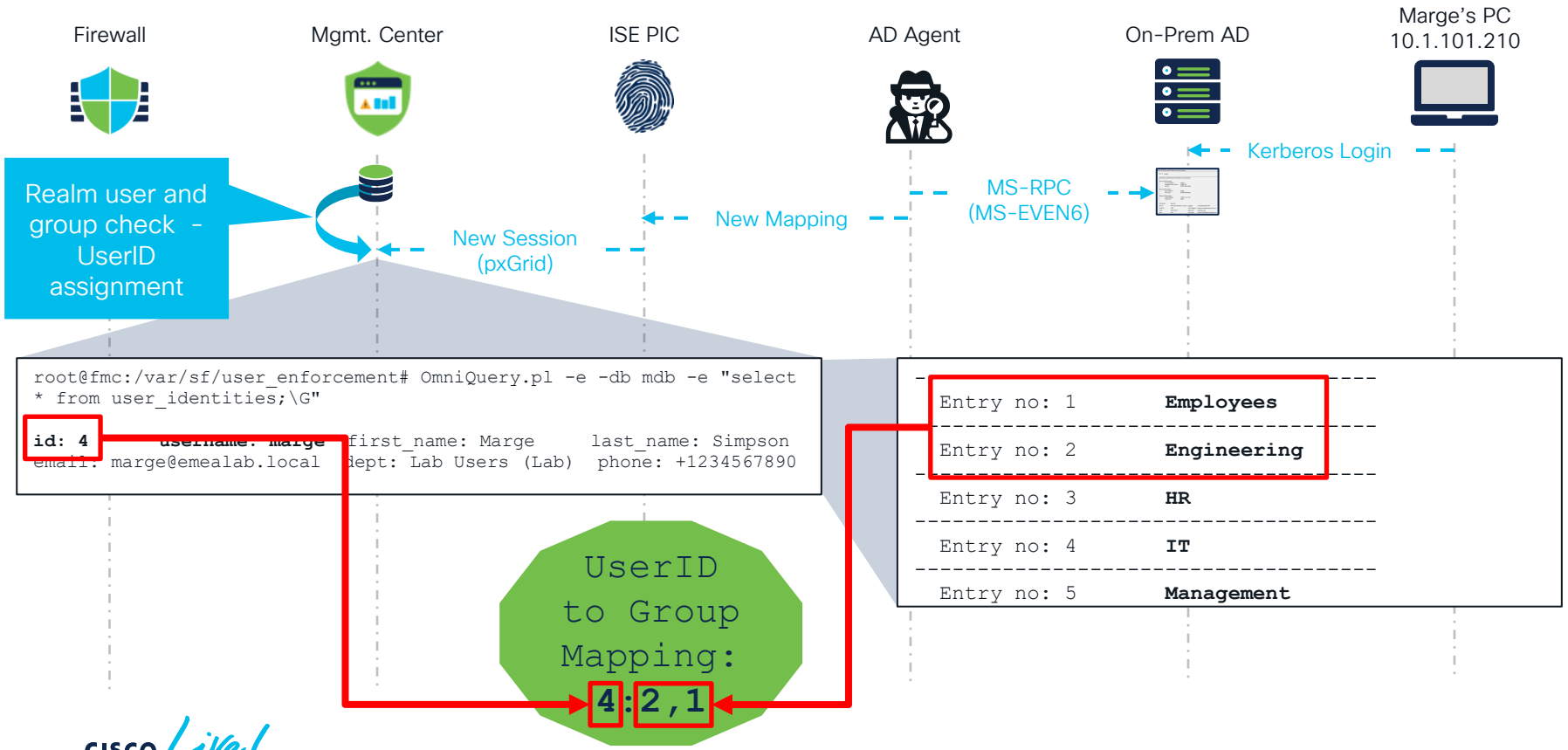


ISE-PIC: AD Agent Mapping Propagation

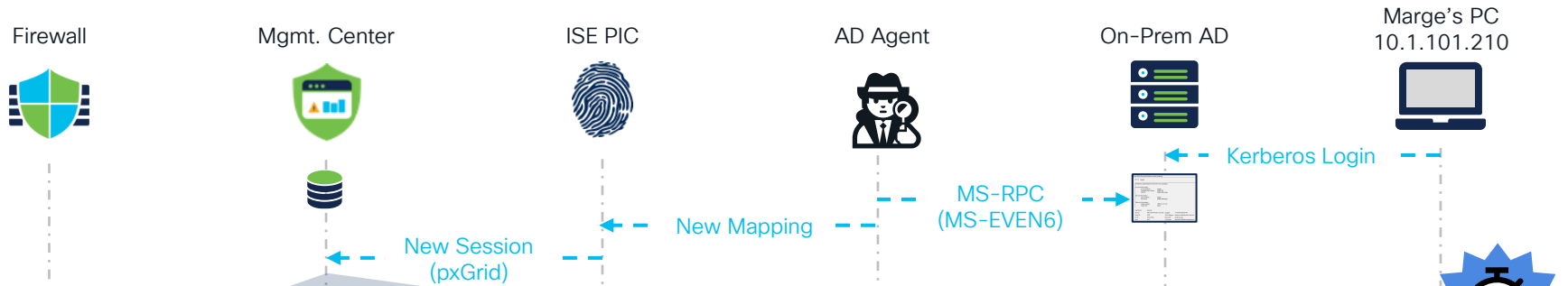


Best Practice: for the new user session to be considered complete user's details must be available – previously synced from the Realm.

ISE-PIC: AD Agent Mapping Propagation



ISE-PIC: AD Agent Mapping Propagation



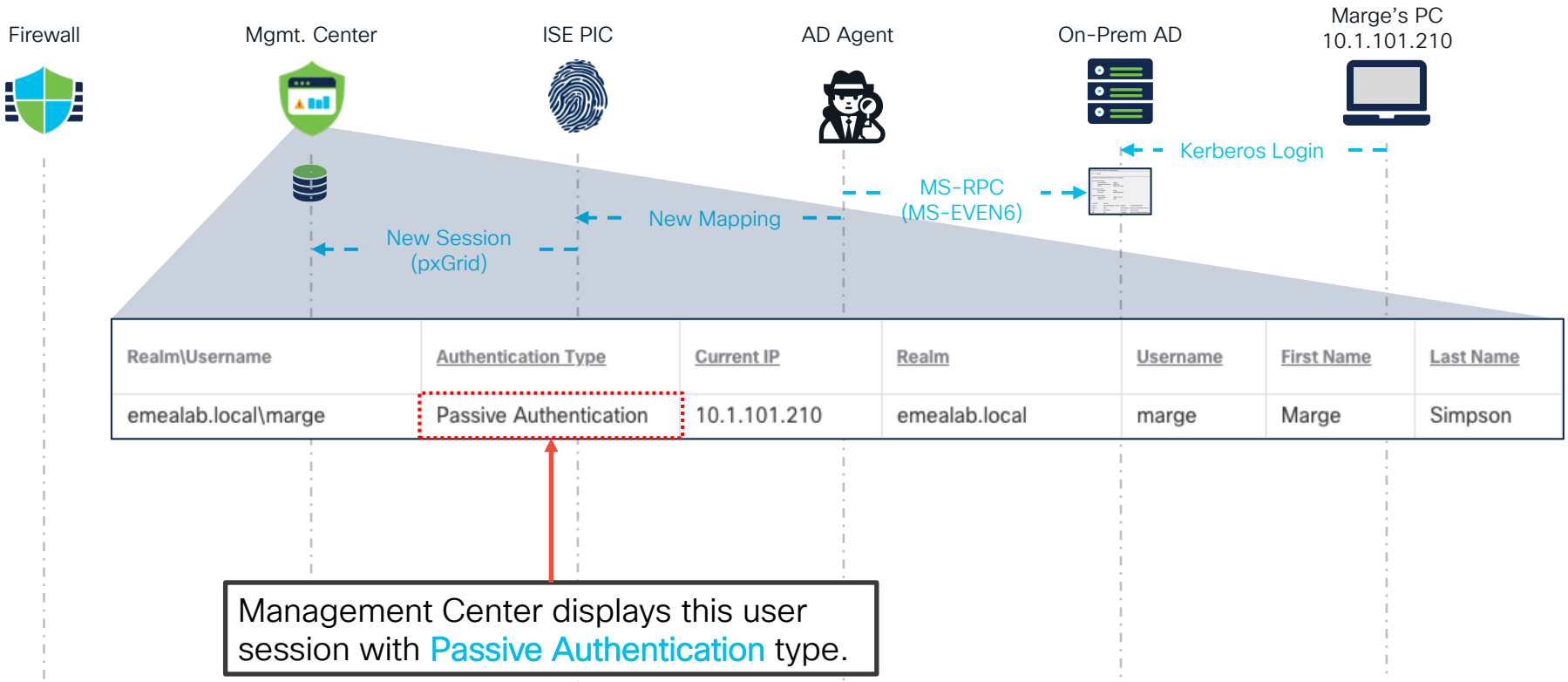

```
admin@fmc:~$ sudo uip_reader -f
/var/sf/user_enforcement/uip_log_entries.1 -p -l
-------------------------------------
Entry no: 287
   SubscriberSession:
     Operation: SESSION_ADD
     Type: IDENTITY_PASSIVE
     Username: marge
     User ID: 4
     Realm ID: 2
     IP Address: ::ffff:10.1.101.210
Timestamp: 2024-01-16 18:06:53
 Hop Timestamps:
      2024-01-16 18:06:57(+4 sec)
```

You can check the delay from Agent reported timestamp in DC's event log.

UserID to Group Mapping: **4:2,1**

Upon cross-check against Realm, the user mapping is complete and may be shared with the firewall for enforcement.

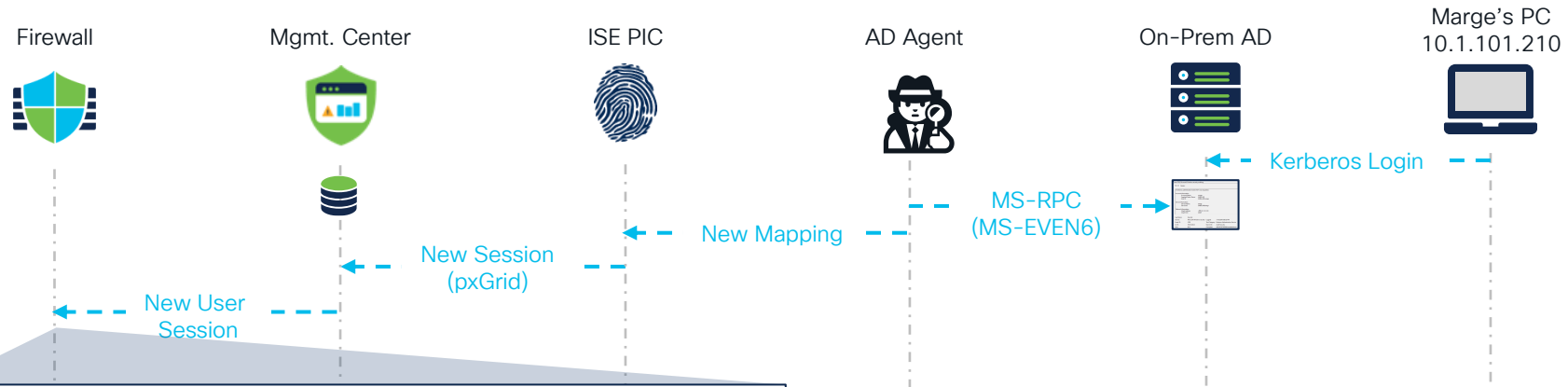
ISE-PIC: AD Agent Mapping Propagation



Realm\Username	Authentication Type	Current IP	Realm	Username	First Name	Last Name
emealab.local\marge	Passive Authentication	10.1.101.210	emealab.local	marge	Marge	Simpson

Management Center displays this user session with Passive Authentication type.

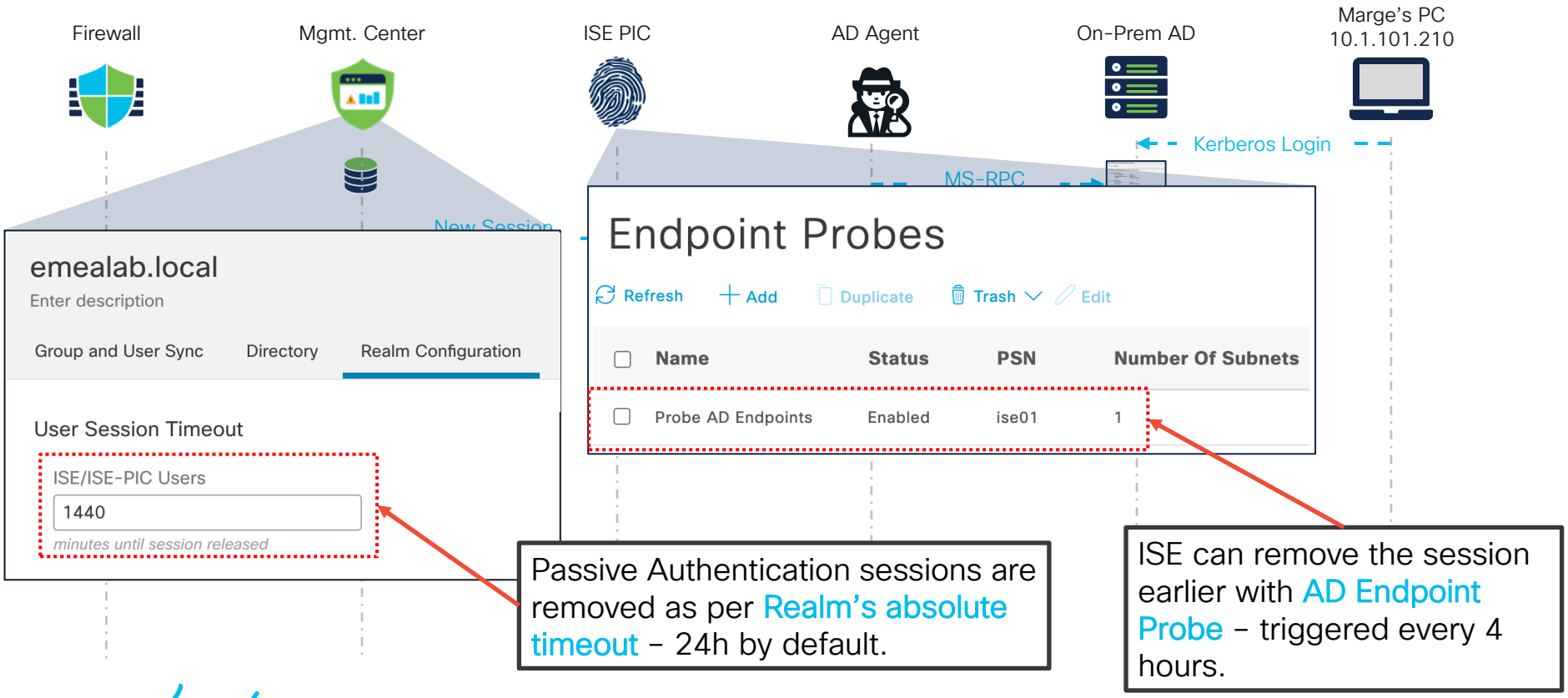
ISE-PIC: AD Agent Mapping Propagation




```
> system support firewall-engine-dump-user-identity-data
> expert
$ sudo cat /ngfw/var/sf/user_enforcement/user_identity.dump

----------------
Host ::ffff:10.1.101.210
----------------
::ffff:10.1.101.210:4 realm 2 type 1, username marge

-------------------
USER:GROUPS
-------------------
4:1,2, (active_sessions: 1)
```

UserID: 4 tells Snort, the user is part of AD groups Employees (1) and Engineering (2).

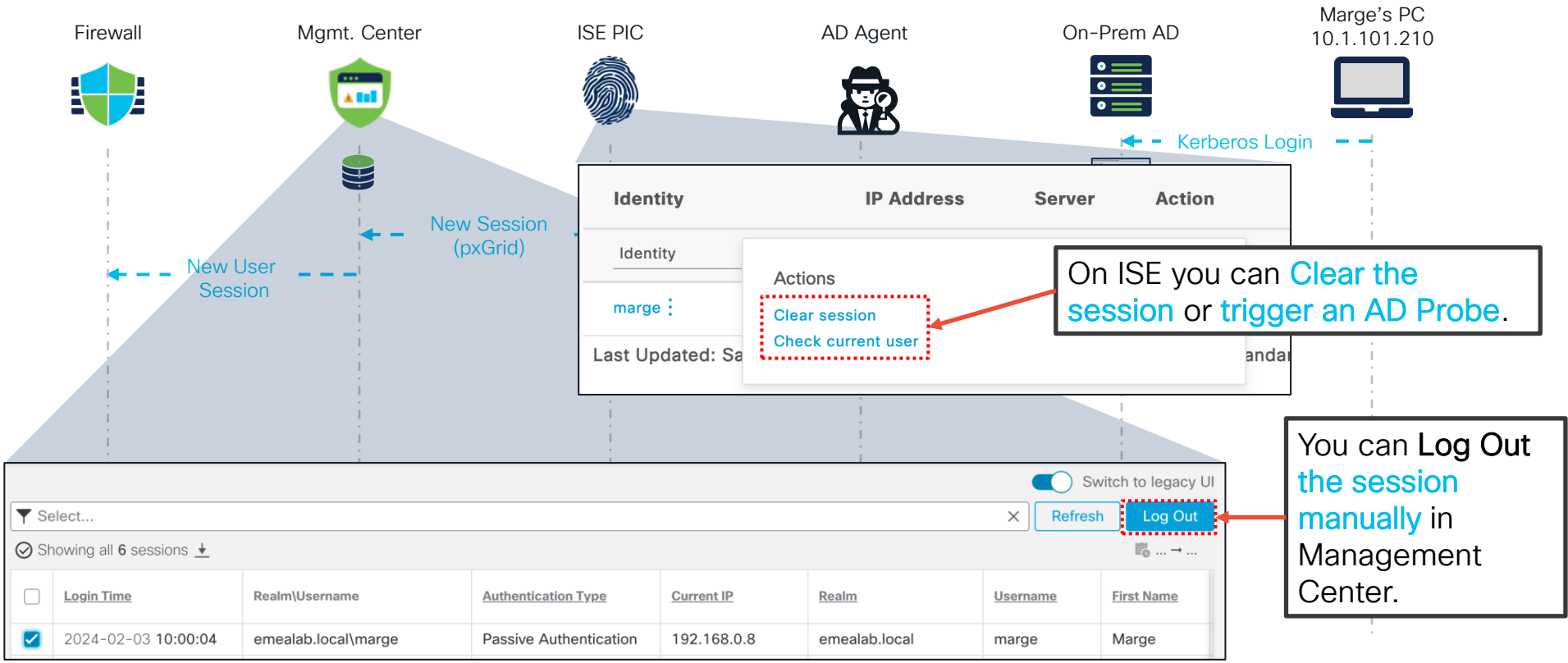
ISE-PIC: Timeout/Probe-Based Session Removal



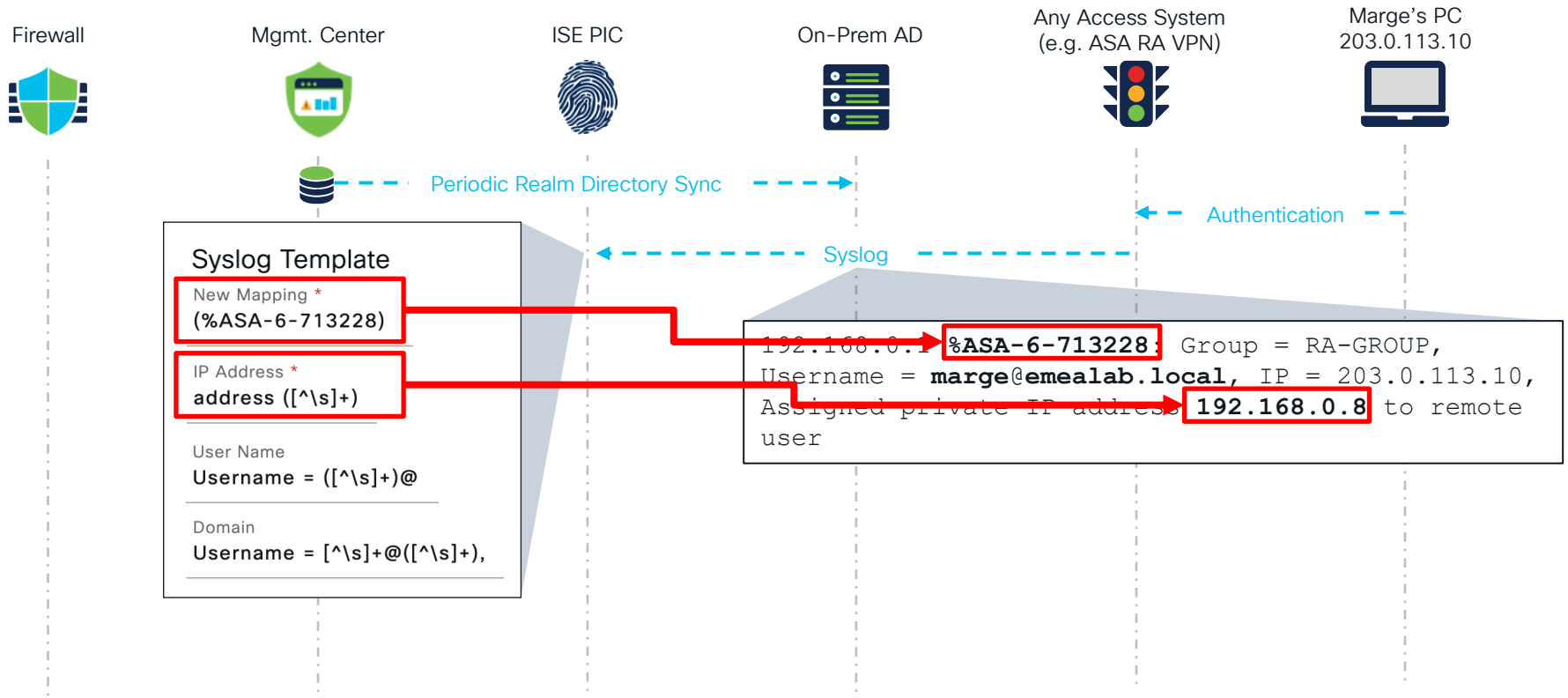
Passive Authentication sessions are removed as per Realm's absolute timeout – 24h by default.

ISE can remove the session earlier with AD Endpoint Probe – triggered every 4 hours.

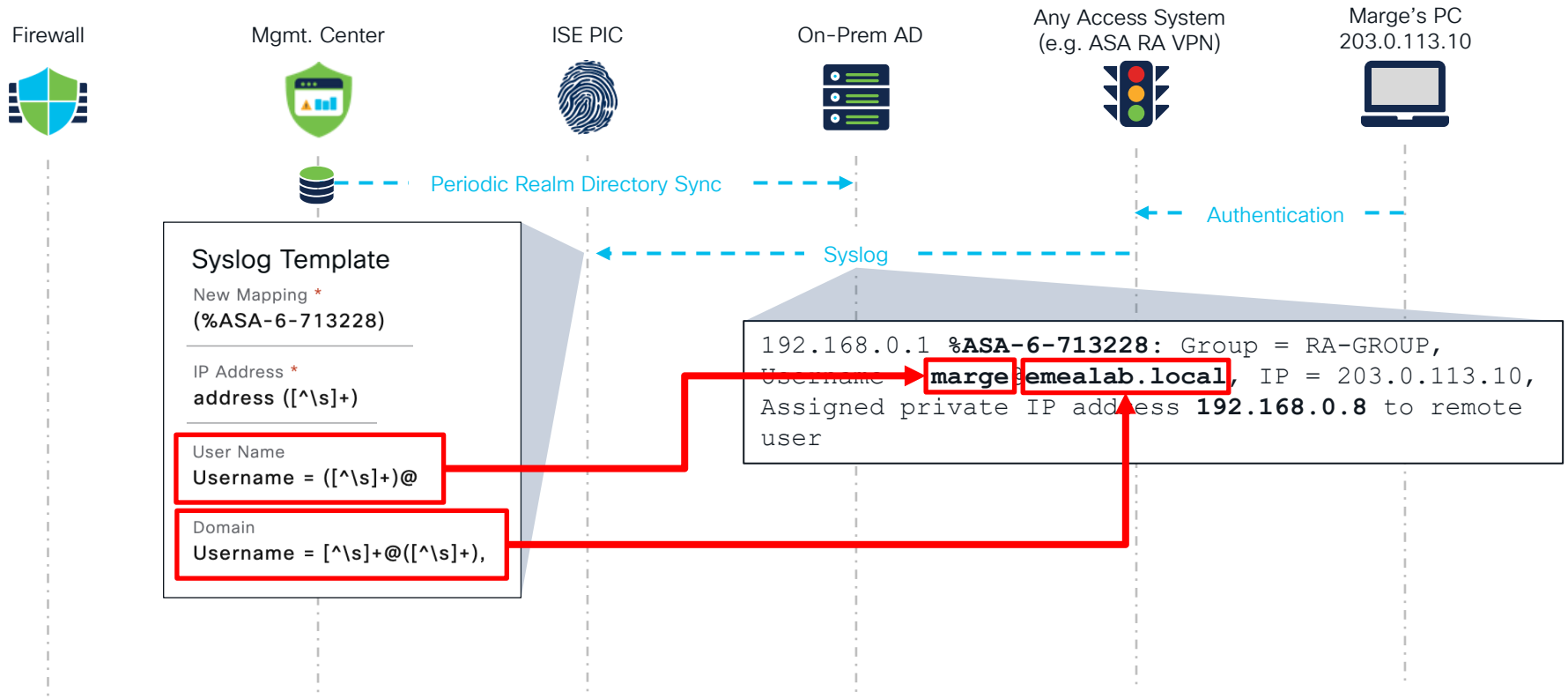
ISE-PIC: Manual Session Removal



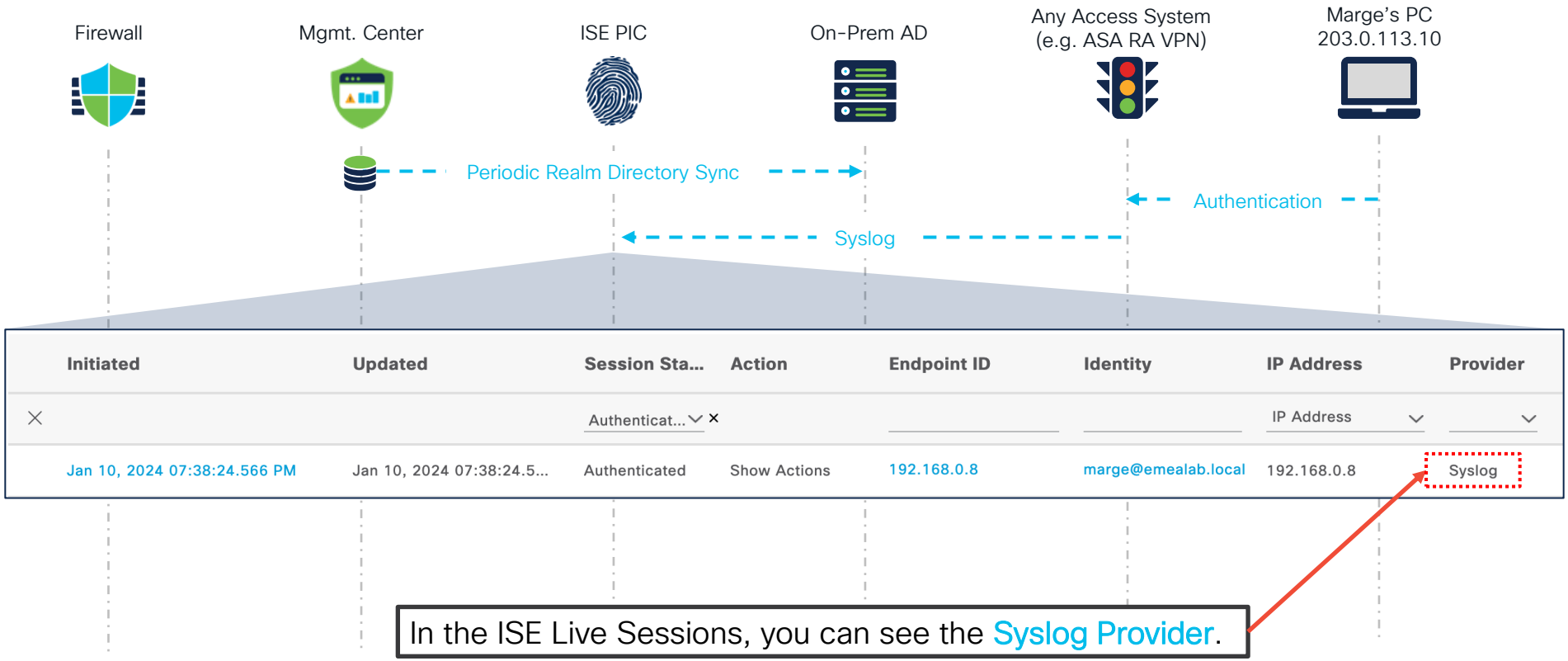
ISE-PIC: Syslog Mapping Propagation



ISE-PIC: Syslog Mapping Propagation

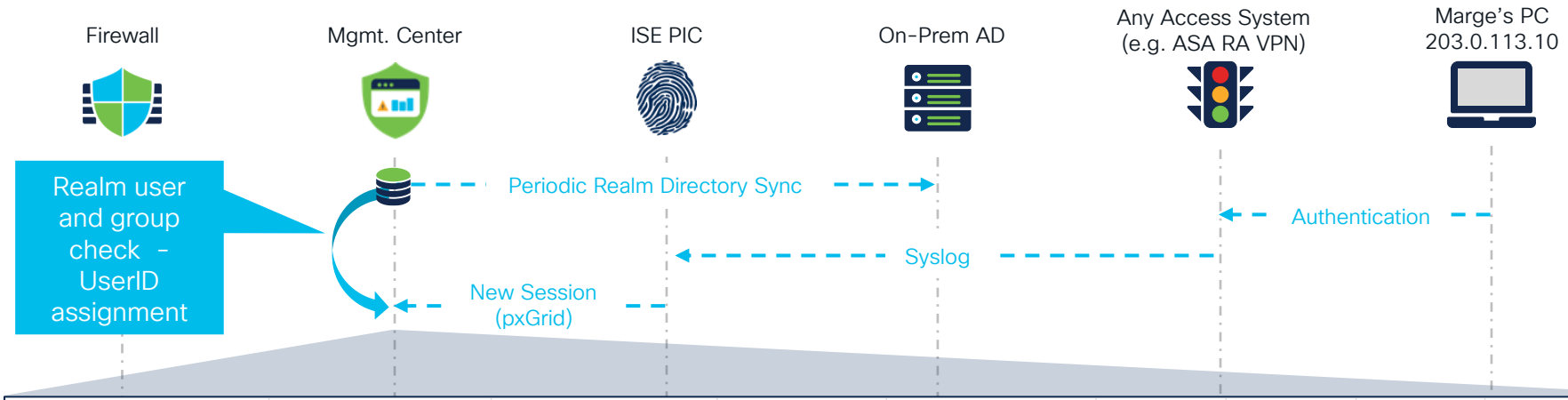


ISE-PIC: Syslog Mapping Propagation



In the ISE Live Sessions, you can see the Syslog Provider.

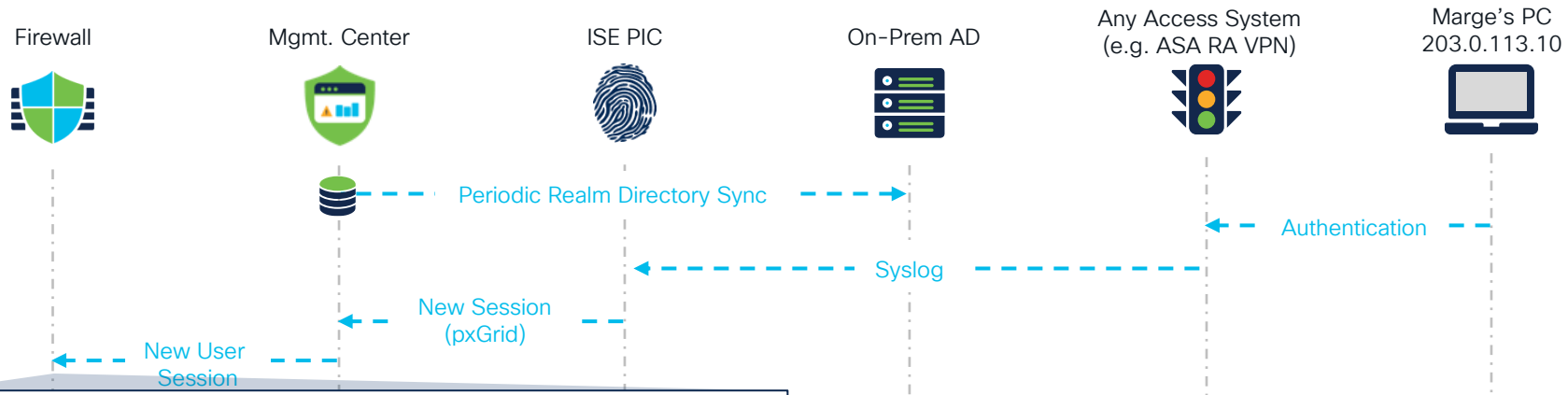
ISE-PIC: Syslog Mapping Propagation



Realm\Username	Last Seen ↓	Authentication Type	Current IP	Realm	Username	First Name	Last Name	Email
emealab.local\marge	2024-01-10 20:38:24	Passive Authentication	192.168.0.8	emealab.local	marge	Marge	Simpson	marge@emealab.local

In the Management Center Active Users, you can see Passive Authentication type, with no indication of Syslog provider.

ISE-PIC: Syslog Mapping Propagation

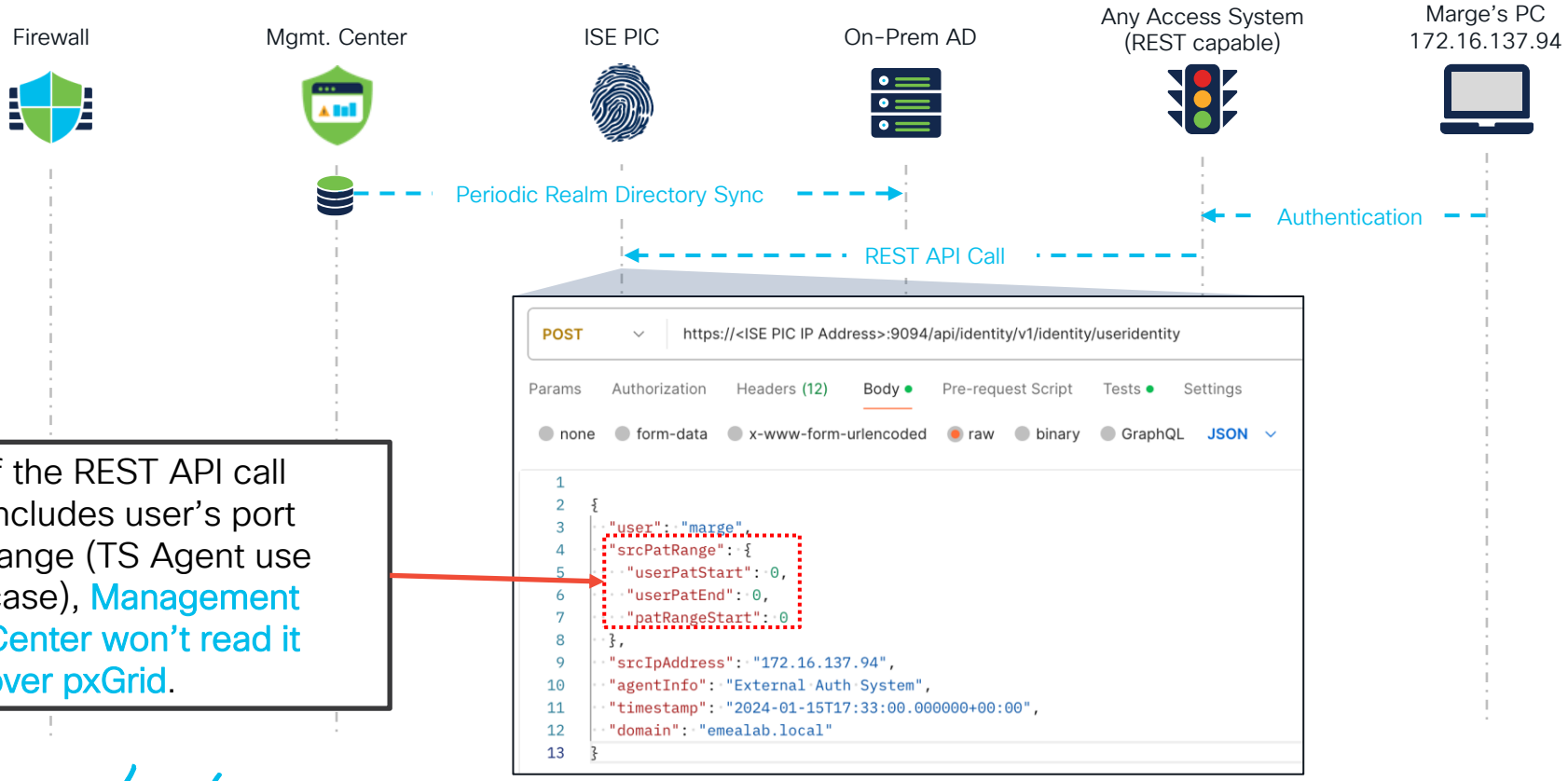



```
> system support firewall-engine-dump-user-identity-data
> expert
$ sudo cat /ngfw/var/sf/user_enforcement/user_identity.dump

----------------
Host ::ffff:10.1.101.210
----------------
::ffff:192.168.0.8:4 realm 2 type 1, username marge

-------------------
USER:GROUPS
-------------------
4:2,1, (active_sessions: 1)
```

Snort gets the User to IP mapping…

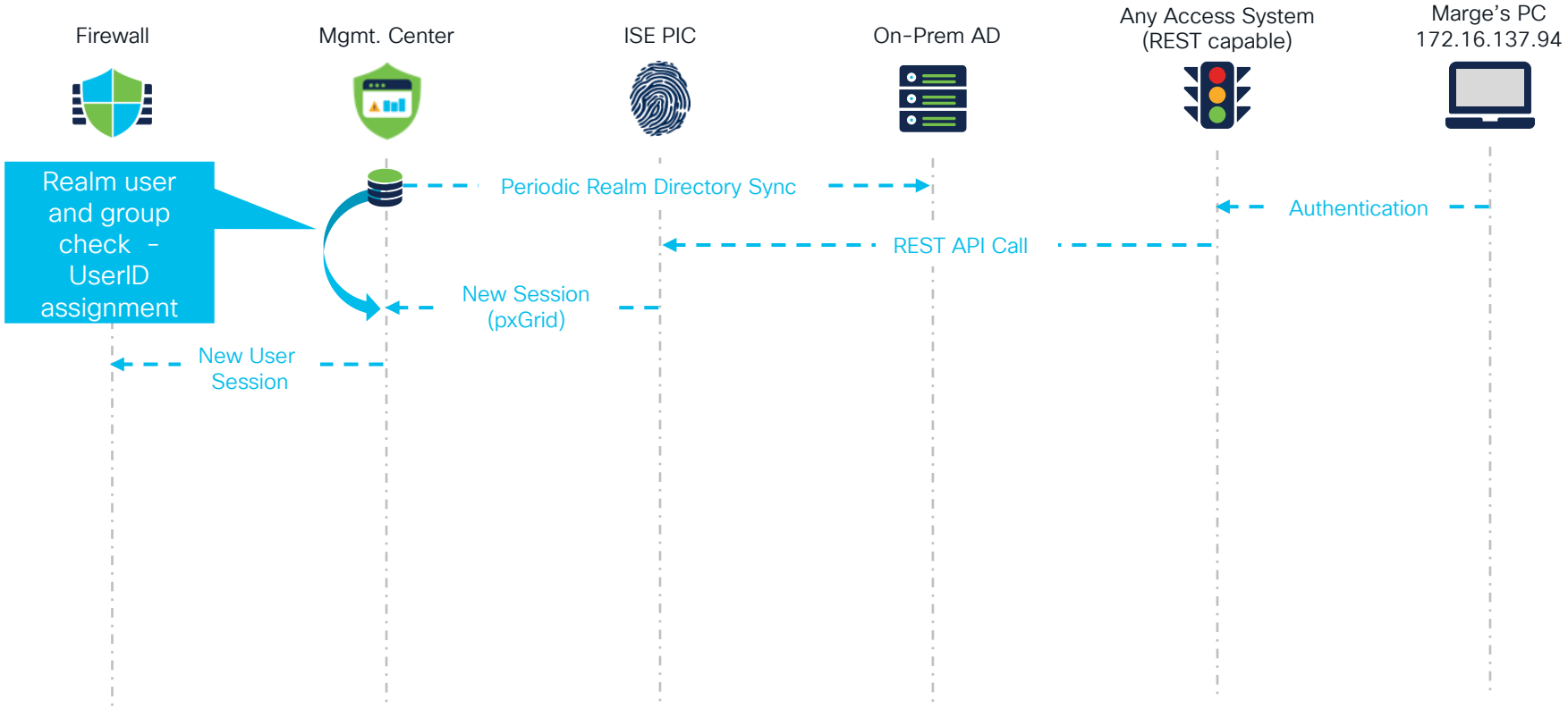
…along with User to Groups mappings.

ISE-PIC: REST API Mapping Propagation



If the REST API call includes user's port range (TS Agent use case), Management Center won't read it over pxGrid.

ISE-PIC: REST API Mapping Propagation



Key Takeaways

- ISE-PIC is a 2-node installation of ISE with feature-set limited to PassiveID
- Client roaming is not supported with with AD Agent passive authentication – Events 4768/4770 are not generated upon client IP change.
- PassiveID is incompatible with 802.1x machine authentication - passive mappings are overridden by unsupported machine auth.

PassiveID and 802.1x Machine Authentication

ISE PassiveID + 802.1x

Updated	Session Status	Endpoint ID	Identity	IP Address	Server	Provider	AD User Resolved Ide...	Auth M...
		Endpoint ID	Identity	IP Address	Server		AD User Resolved I	Auth Meth
Jan 16, 2024 05:13:27.344 PM	Started	00:42:68:6F:50:52	W10-POD1.emealab.local	10.1.101.210	ise01	None		dot1x
Jan 16, 2024 05:06:53.186 PM	Authenticated	10.1.101.210	marge	10.1.101.210	ise01	Agent	marge@emealab.local	

1

2

```
Entry no: 287
   SubscriberSession:
     Operation: SESSION_ADD
     Type: IDENTITY_PASSIVE

     Username: marge
     User ID: 4

     Realm ID: 2
     IP Address: ::ffff:10.1.101.210
```

Management Center

```
Entry no: 288
   SubscriberSession:
     Operation: SESSION_ADD
     Type: IDENTITY_PASSIVE

     Username: W10-POD1.emealab.local
     User ID: 10000010 (UNUSABLE USER ID)

     Realm ID: 2
     IP Address: ::ffff:10.1.101.210
```

Now It’s Time for a Quiz ☺

- You can win a bouncy ball

- There will be 3 quizzes during this session
- Each quiz has 2 questions
- You will have 30, 45 or 60 seconds for a question

A champion of a quiz also wins a QUIZ IMMUNITY until the end of this session.

Join at

slido.com

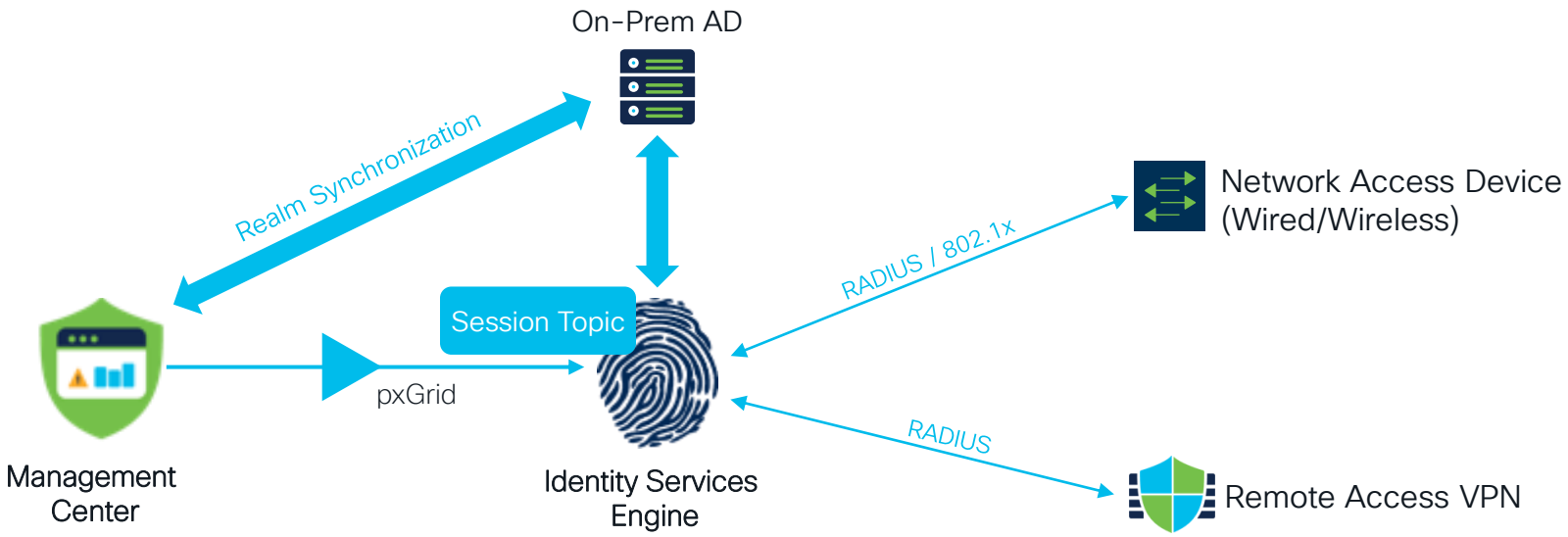
2901 029

QUIZ 1:

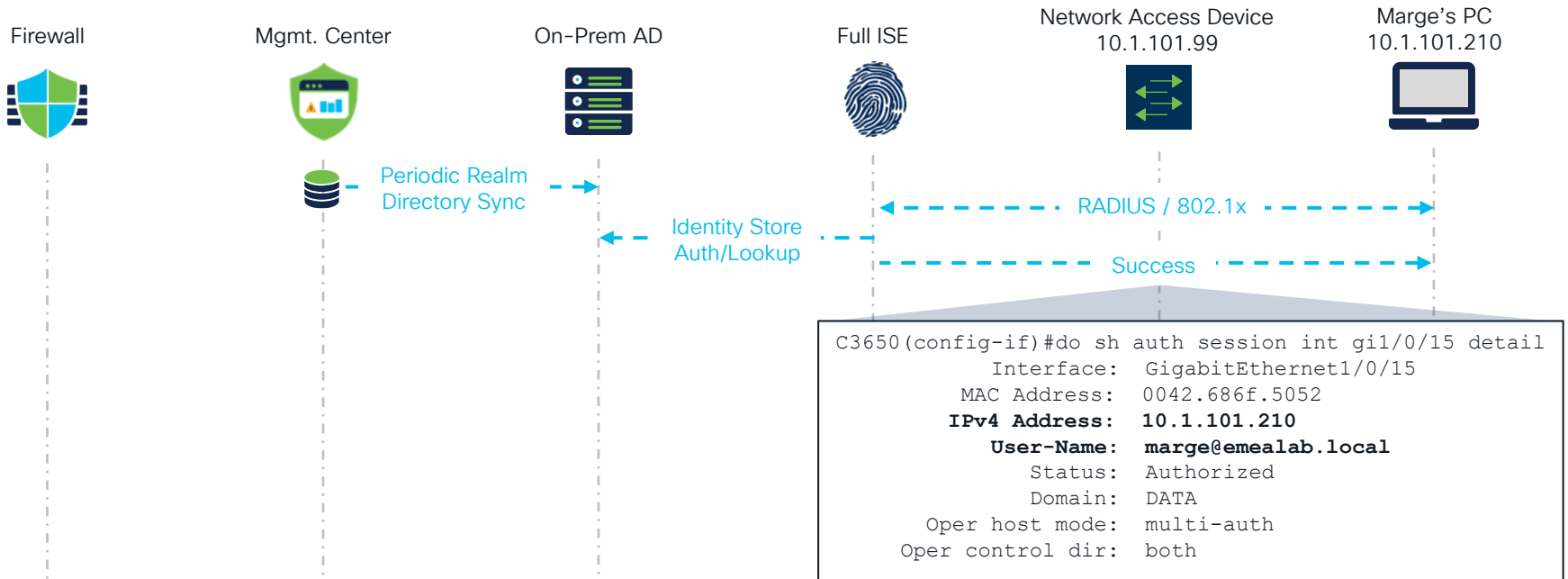
PASSIVE AUTHENTICATION

Identity Services Engine
(RADIUS/802.1x deployment)

Full ISE with 802.1x/RADIUS Features

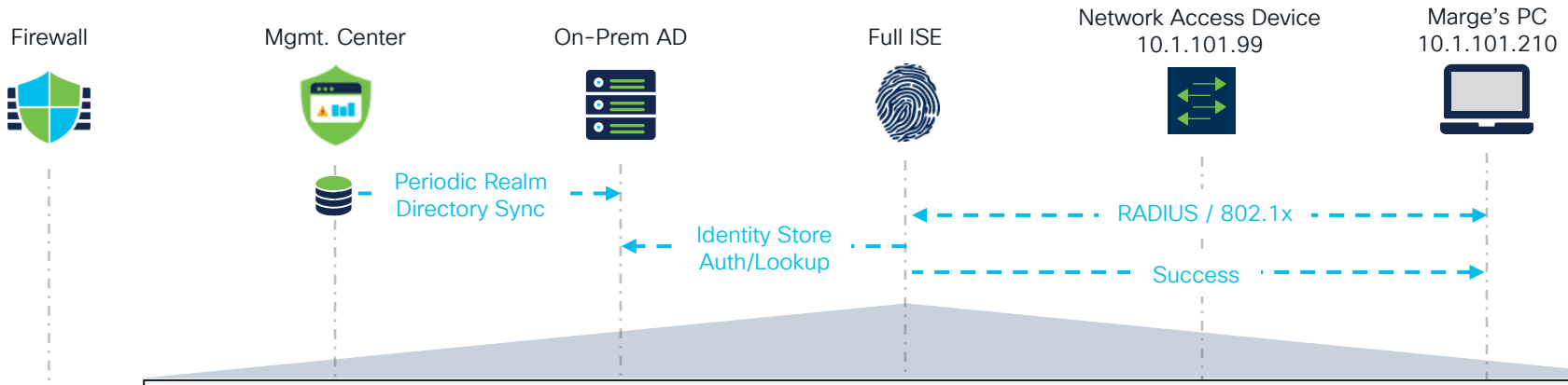


802.1x Sourced Identity Mapping Propagation



User is authenticated and authorized by ISE. The Network Access Device keeps track of the user session.

802.1x Sourced Identity Mapping Propagation

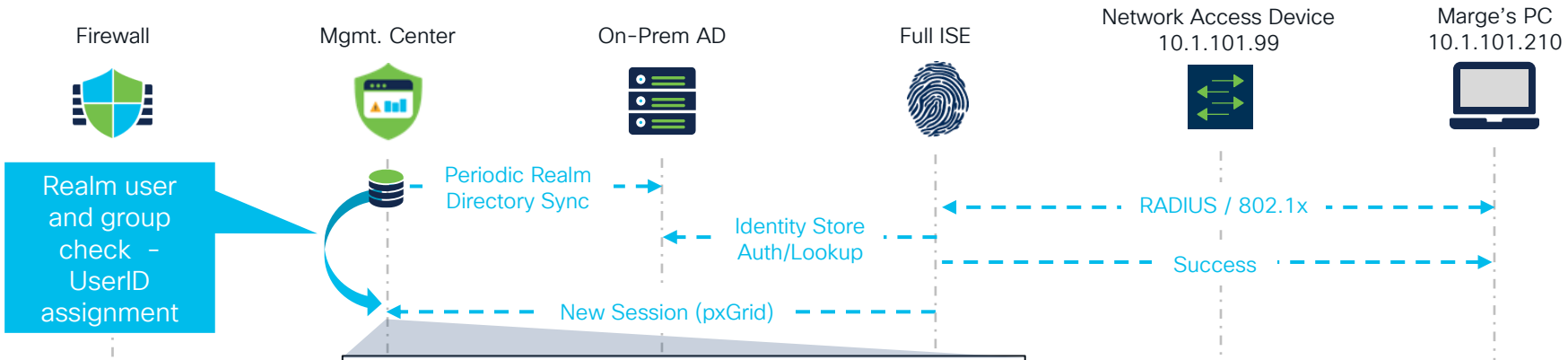


Session...	Action	Auth M...	Authenti...	Endpoint ID	Identity	IP Address	Server
Started	Show CoA Actions	dot1x	EAP-TLS	00:42:68:6F:50:52	marge@emealab.local	10.1.101.210	ise01

ISE Live Sessions display the authentication method as 802.1x.

The user identity is derived depending on authentication method – clear-text user/pass, certificate field, etc...

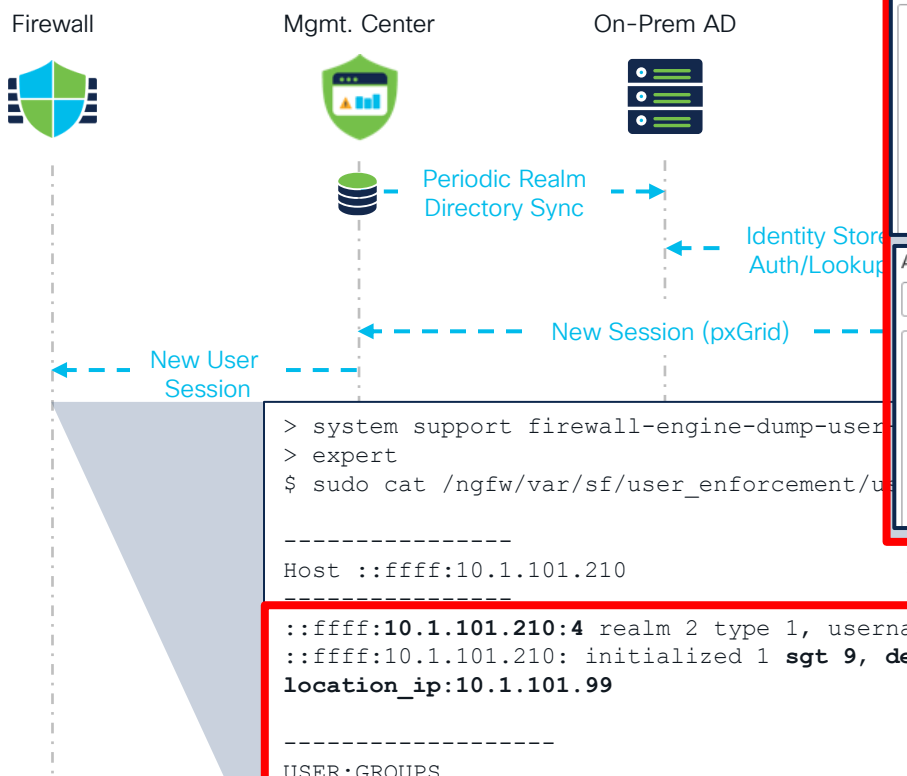
802.1x Sourced Identity Mapping Propagation



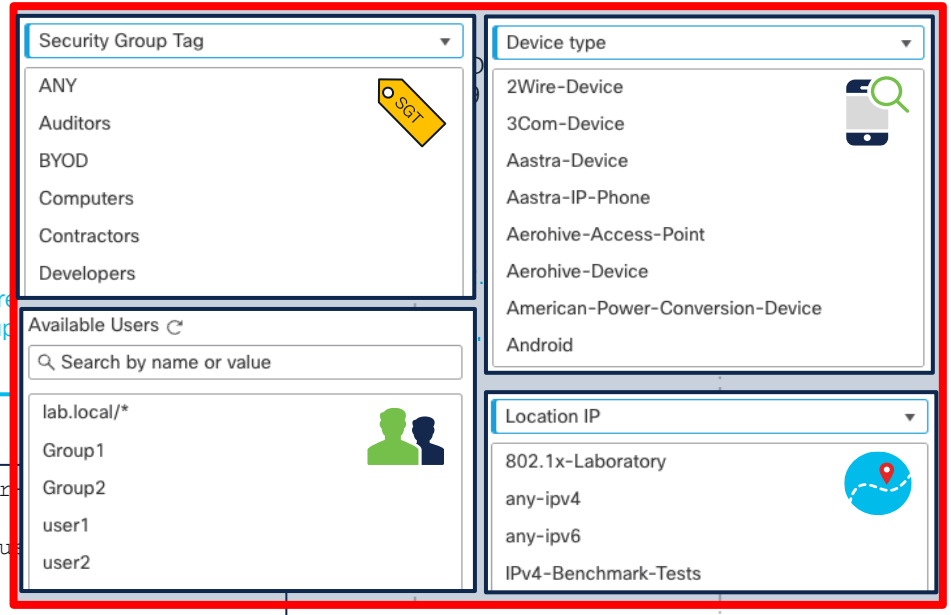

```
admin@fmc:~$ sudo uip_reader -f
/var/sf/user_enforcement/uip_log_entries.1 -p -l
-------------------------------------
  Entry no: 230
   SubscriberSession:
     Operation: SESSION_ADD
     Type: IDENTITY_PASSIVE
     Username: marge
     User ID: 4
     Realm ID: 2
     IP Address: ::ffff:10.1.101.210
     NAS IP Address: ::ffff:10.1.101.99
     Timestamp: 2024-01-16 13:29:58
     Device Profile ID: 450
     Hop Timestamps: 2024-01-16 13:30:02(+4 sec)
```

You can check the delay between ISE authentication and Management Center getting the mapping.

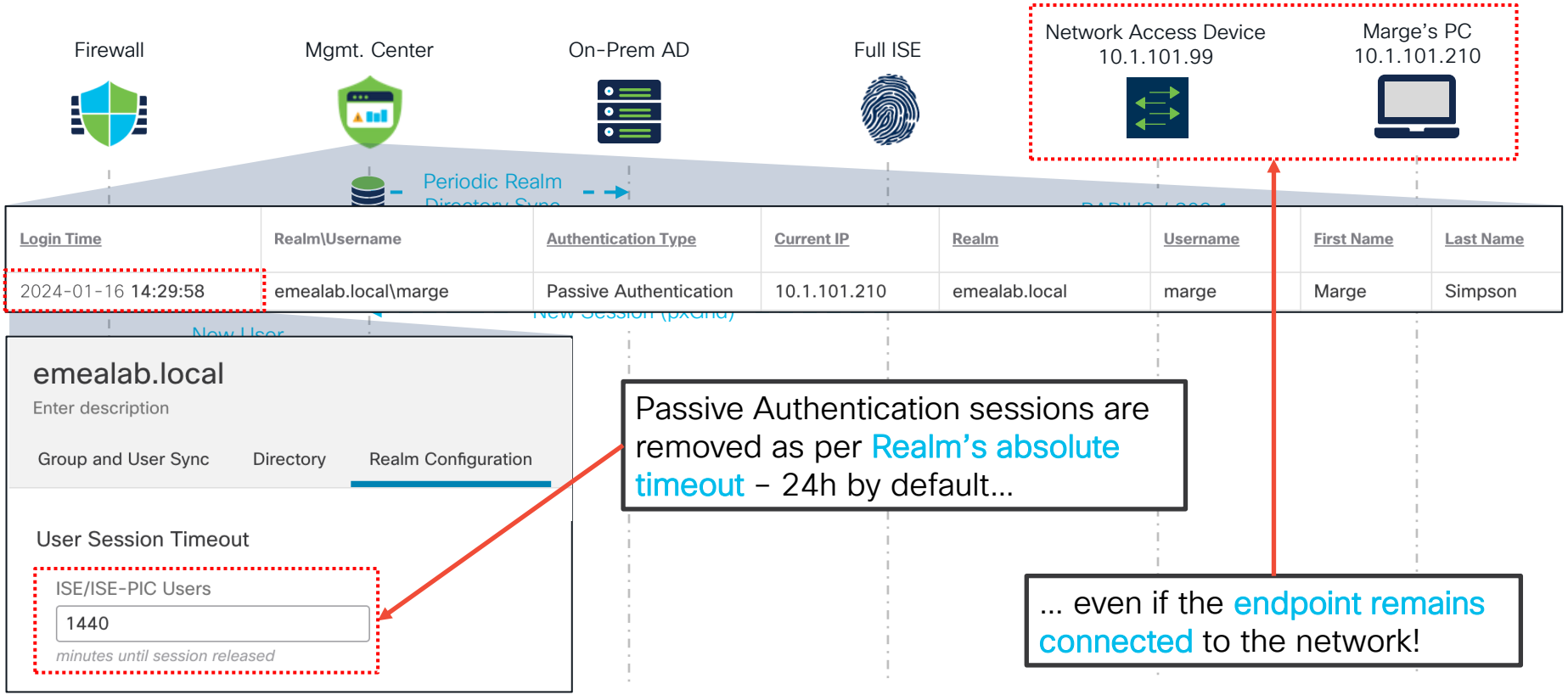
802.1x Sourced Identity Mapping Propagation




```
> system support firewall-engine-dump-user
> expert
$ sudo cat /ngfw/var/sf/user_enforcement/u

----------------
Host ::ffff:10.1.101.210
----------------
::ffff:10.1.101.210:4 realm 2 type 1, username marge
::ffff:10.1.101.210: initialized 1 sgt 9, device_type 450,
location_ip:10.1.101.99

-------------------
USER:GROUPS
-------------------
4:2,1, (active_sessions: 1)
```



802.1x Sourced Identity Mapping Propagation



Passive Authentication Timeout – 802.1x Reauth

ISE ← RADIUS → Network Access Device

Access Type = ACCESS_ACCEPT

Session-Timeout = 180

Termination-Action = Default

```
C3650(config-if)#do sh auth session int gi1/0/15 detail
            Interface:  GigabitEthernet1/0/15
          MAC Address:  0042.686f.5052
        IPv4 Address:  10.1.101.210
           User-Name:  marge@emealab.local
              Status:  Authorized
              Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  180s (server), Remaining: 173s
      Timeout action:  Terminate
```

Time	Session ID	Status	Identity	IP Address	Auth Met...	Authorization Profiles
			marge	IP Address		
Jan 16, 2024 03:51:22.193 PM	0A0163D30000006212F856AF		marge@emealab.local	10.1.101.210	dot1x	PermitAccess,ReAuth180s
Jan 16, 2024 03:51:22.108 PM	0A0163D30000006212F856AF		marge@emealab.local	10.1.1		
Jan 16, 2024 03:48:18.926 PM	0A0163D30000006112F58B2C		marge@emealab.local	10.1.1		
Jan 16, 2024 03:45:17.033 PM	0A0163D30000006012F2C499		marge@emealab.local	10.1.1		

Re-authentication with Terminate action resets RADIUS SessionID – may affect Posture Services.

Key Takeaways

- Machine Authentication sessions are not supported with Session Topic – Mgmt. Center does not resolve machine account group membership (unusable UserID in Snort).

Login Time	Realm\Username	Last Seen ↓	Authentication Type	Current IP	Realm	Username
2024-01-15 16:37:42	emealab.local\W10-POD1.emealab.local	2024-01-15 16:37:42	Passive Authentication	10.1.101.210	emealab.local	W10-POD1.emealab.local
2024-01-15 16:37:42	emealab.local\W10-POD1.emealab.local	2024-01-15 16:37:42	Passive Authentication	fe80::d179:17a3:255b:9555	emealab.local	W10-POD1.emealab.local

- MAC Address Bypass sessions are not supported with Session Topic – you will see them as a “Special Identity”.

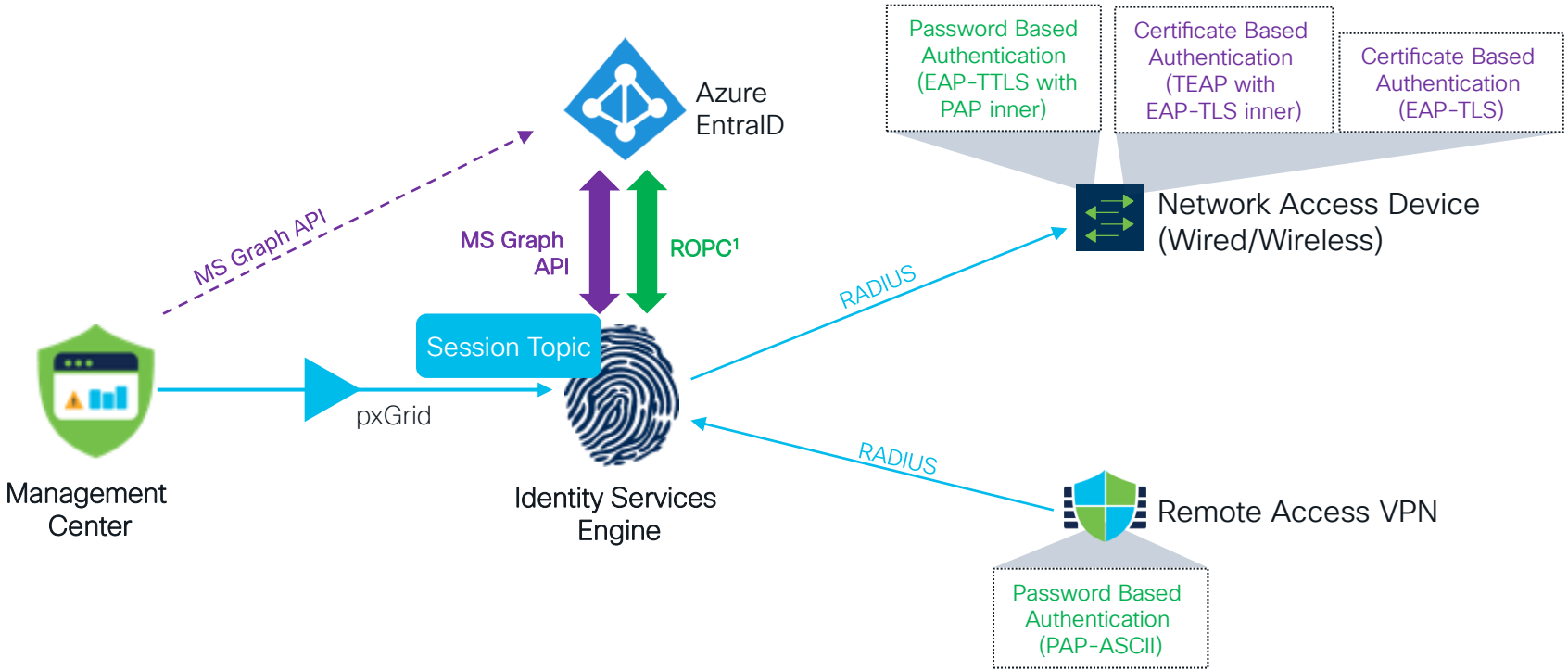
Login Time	Realm\Username	Last Seen ↓	Authentication Type	Current IP	Realm	Username
2024-01-15 16:35:46	Special Identities\00:42:68:6F:5	2024-01-15 16:35:46	Passive Authentication	10.1.101.210	Special Identities	00:42:68:6F:50:52
2024-01-15 16:35:46	Special Identities\00:42:68:6F:5	2024-01-15 16:35:46	Passive Authentication	fe80::d179:17a3:255b:9555	Special Identities	00:42:68:6F:50:52

- With RADIUS sessions, you get more firewall policy attributes than with PassiveID: User, Groups, ISE profiles, NAD IP address and SGTs.
- Realm ISE/ISE-PIC absolute timeout (24h default) will remove a still connected user.

PASSIVE AUTHENTICATION

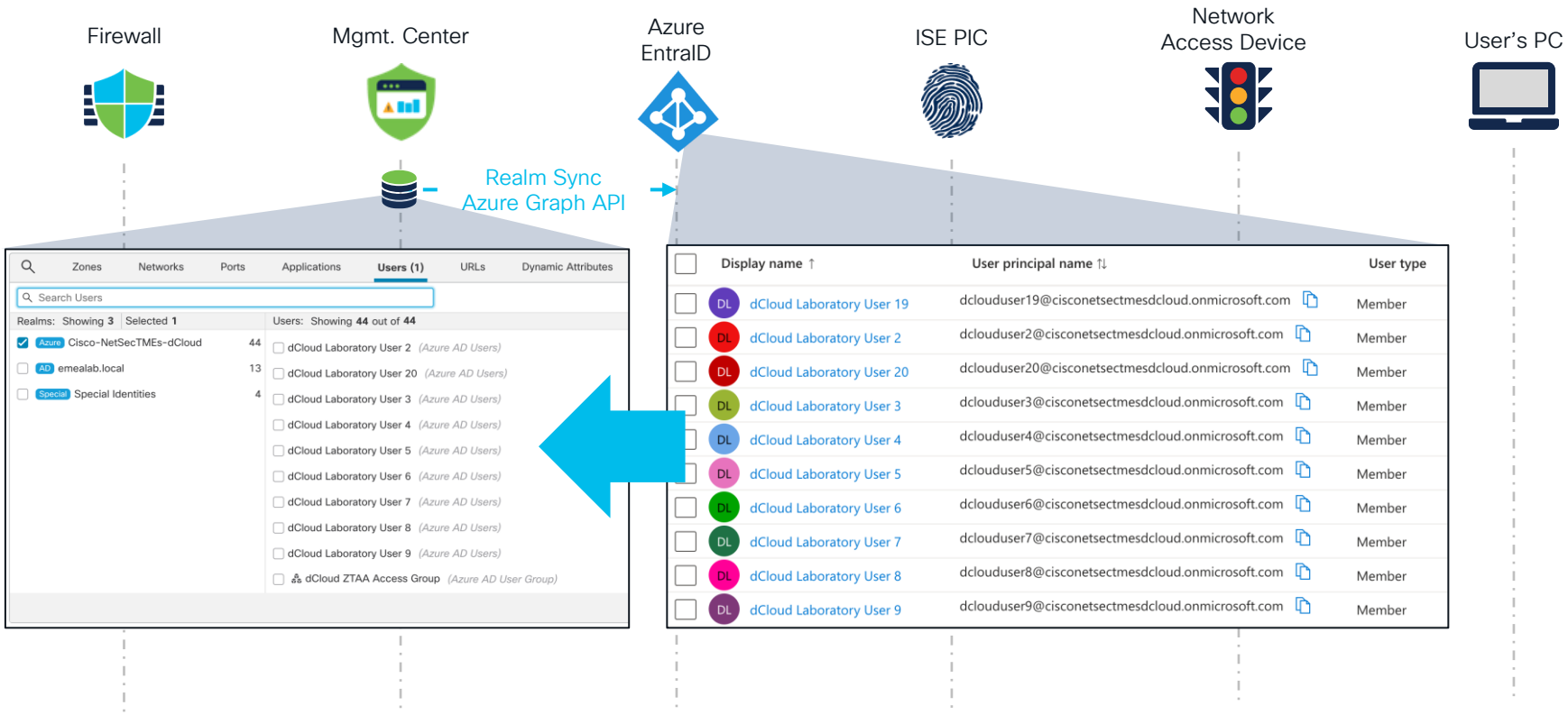
Identity Services Engine
(Azure Entra ID Integration)

ISE Passive Identity Connector

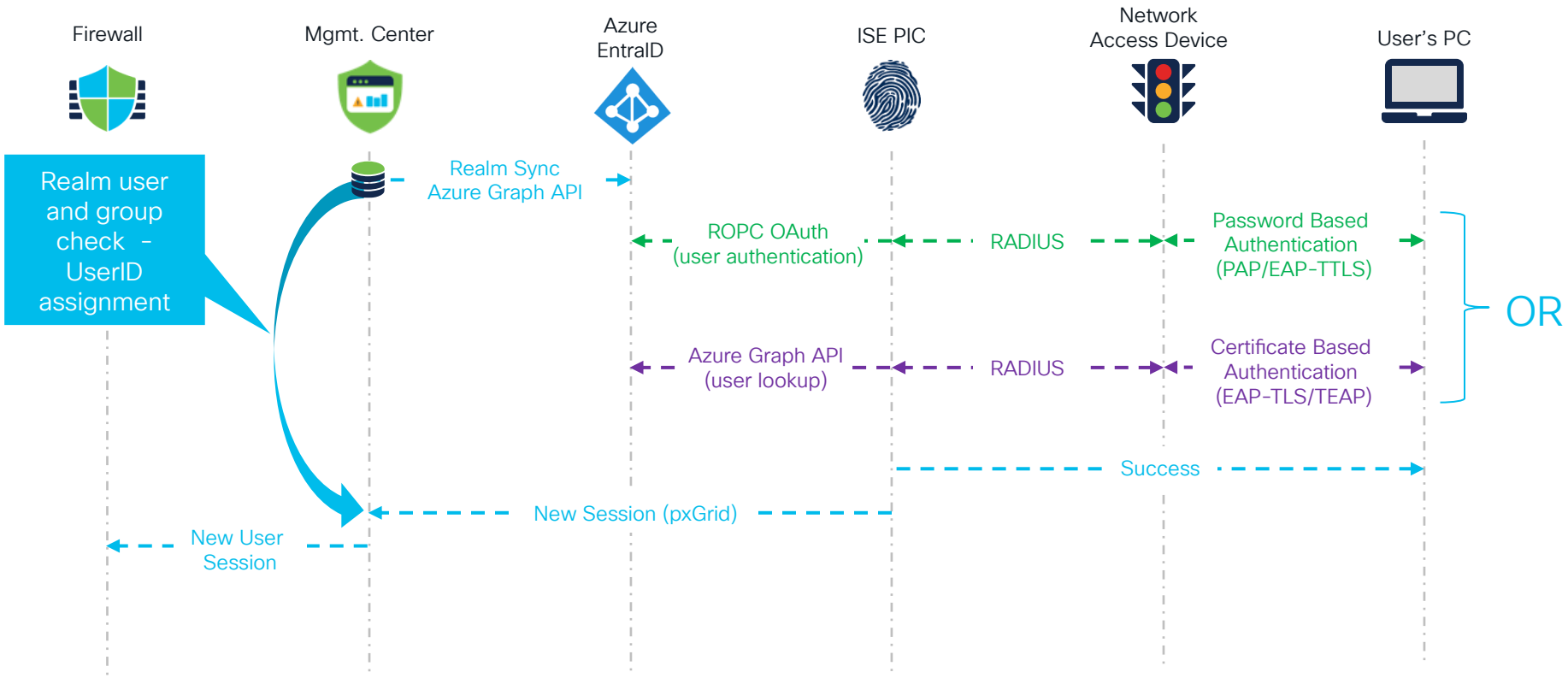


[1] – Resource Owner Password Credentials

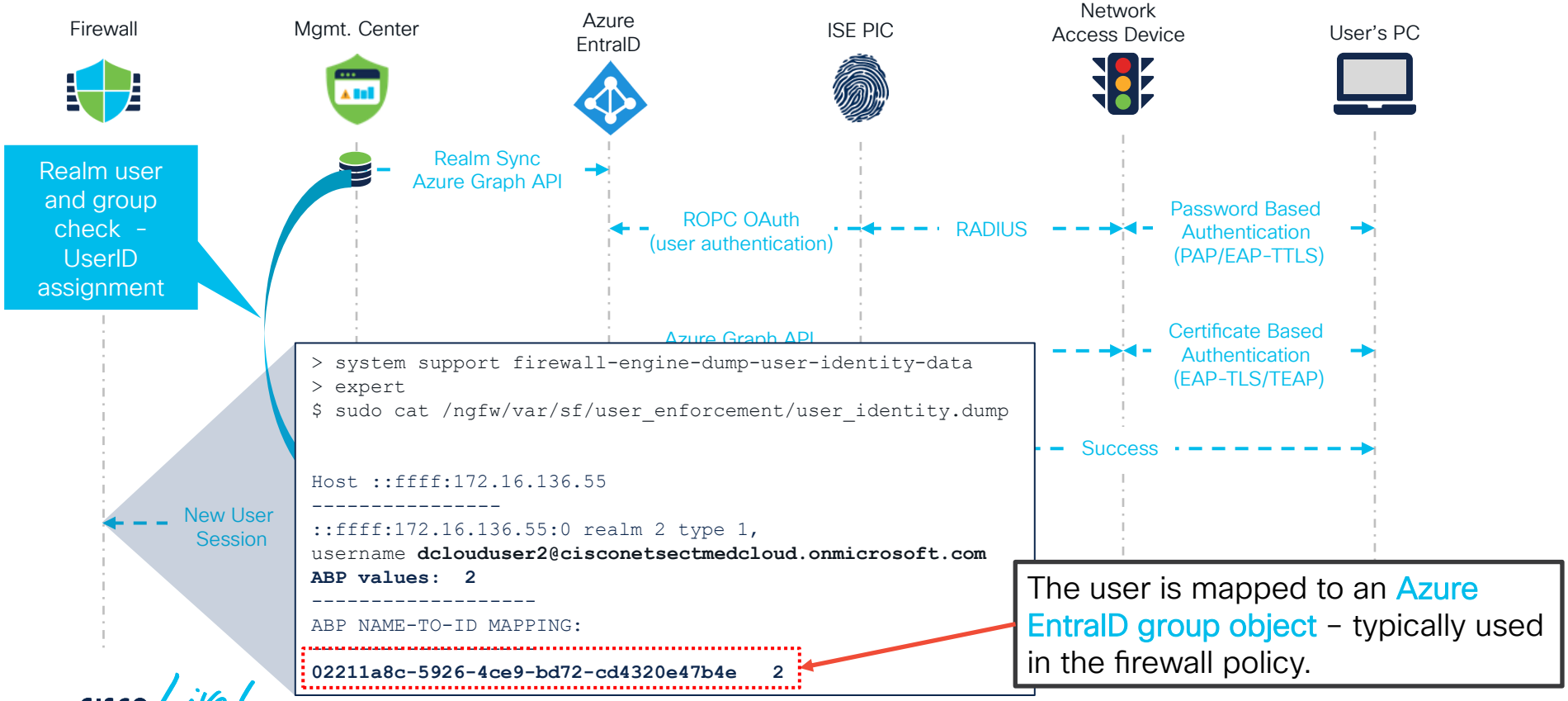
Azure EntraID Realm – User and Group Download



Identity Services Engine with Azure EntraID



Identity Services Engine with Azure EntraID



Key Takeaways

- Azure EntraID store does not provide IP-User mappings – we need passive identity from ISE – authenticated with 802.1x or Remote Access VPN.

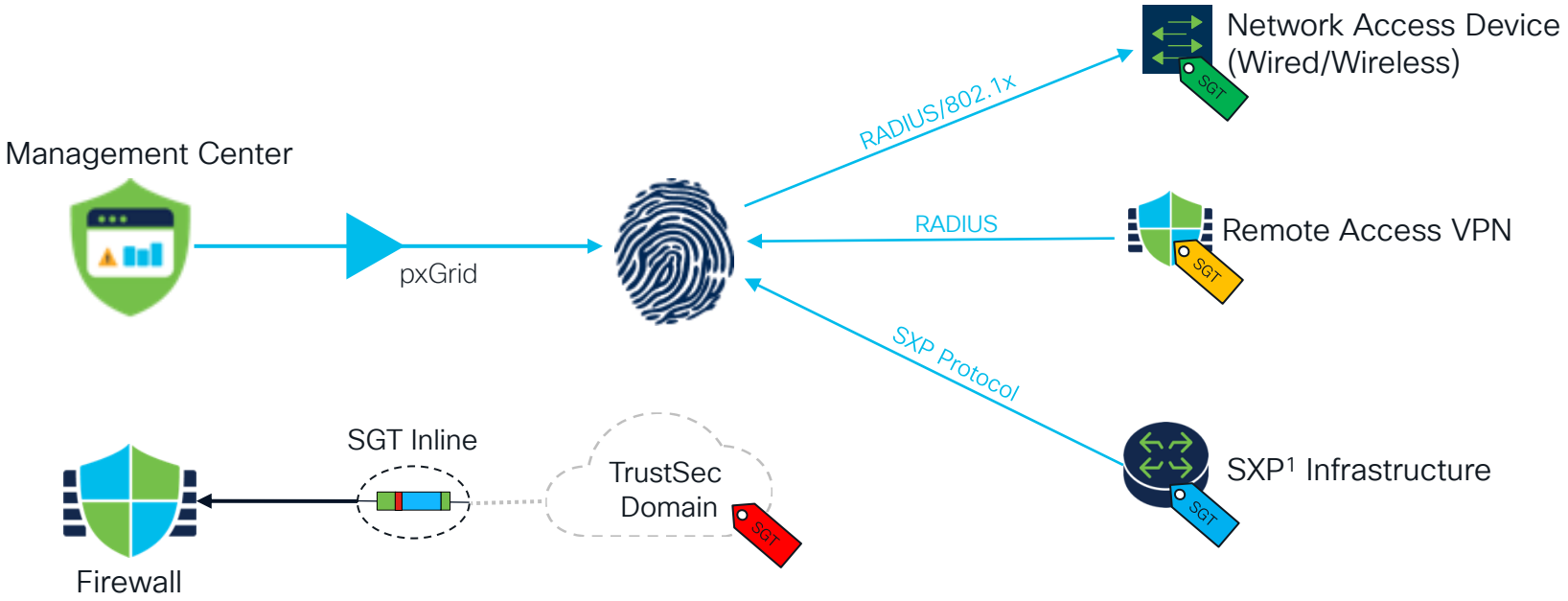
- Due to technical restrictions only specific authentication methods are supported by ISE and EntraID:
  - Resource Owner Password Credentials (ROPC) method requires a plain user password – mandates use of EAP-TTLS (PAP inner) and plain PAP-ASCII (RAVPN)
  - MS Graph API allows meta data lookup only – certificate-based authentication supported only EAP-TLS or TEAP (EAP-TLS inner).

PASSIVE AUTHENTICATION

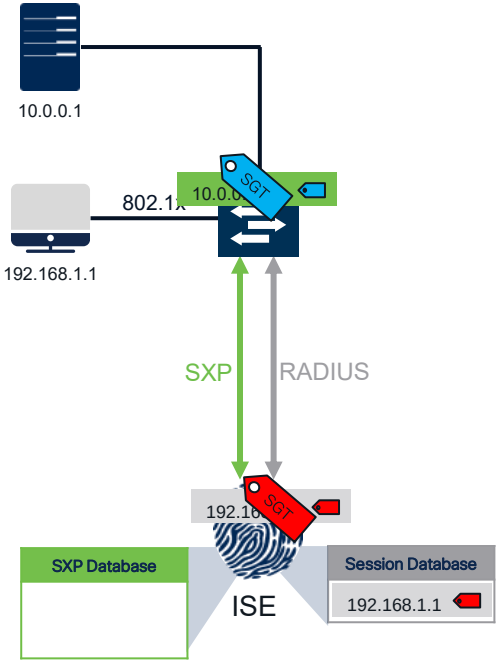
Identity Services Engine
(TrustSec Deployment)

TrustSec Deployment

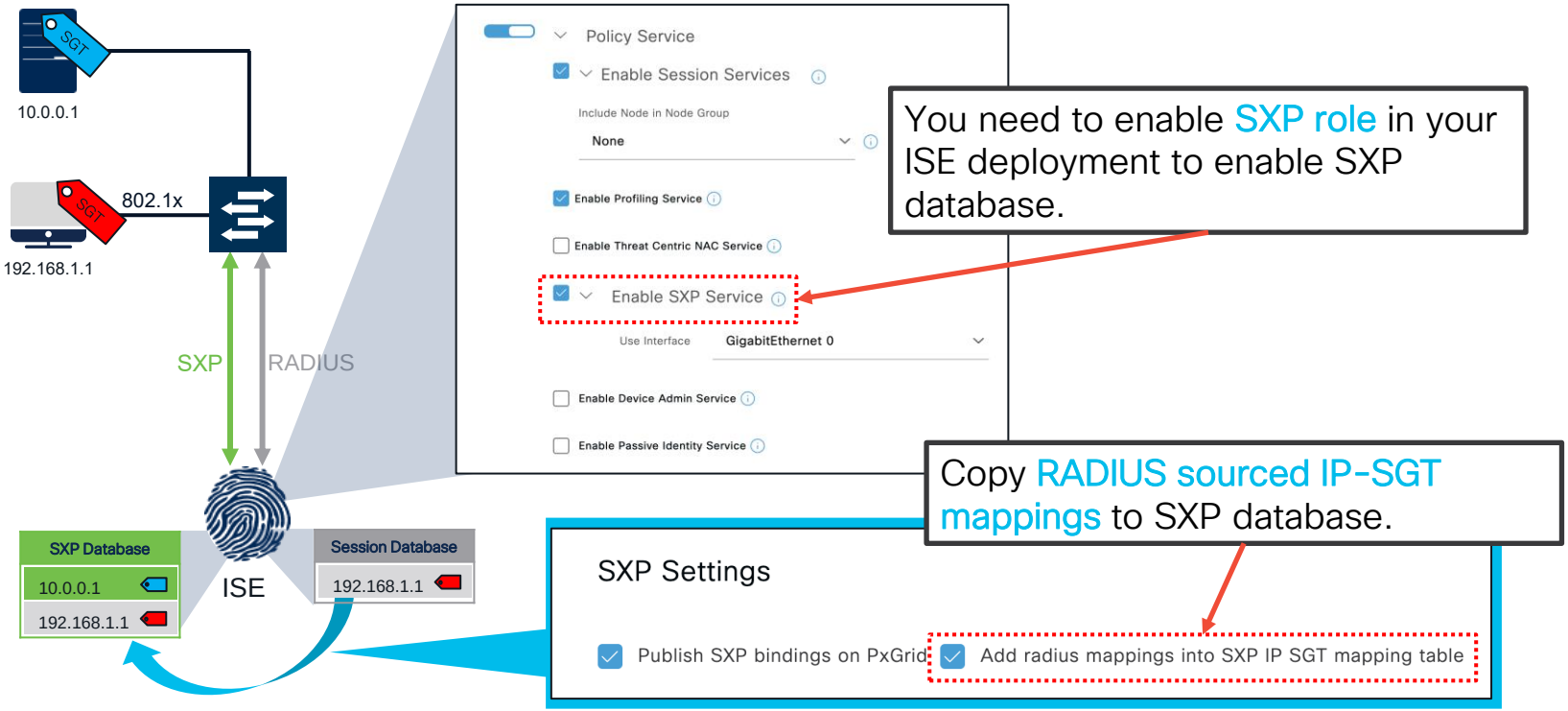
[1] – Scalable Group Tag (SGT) Exchange Protocol



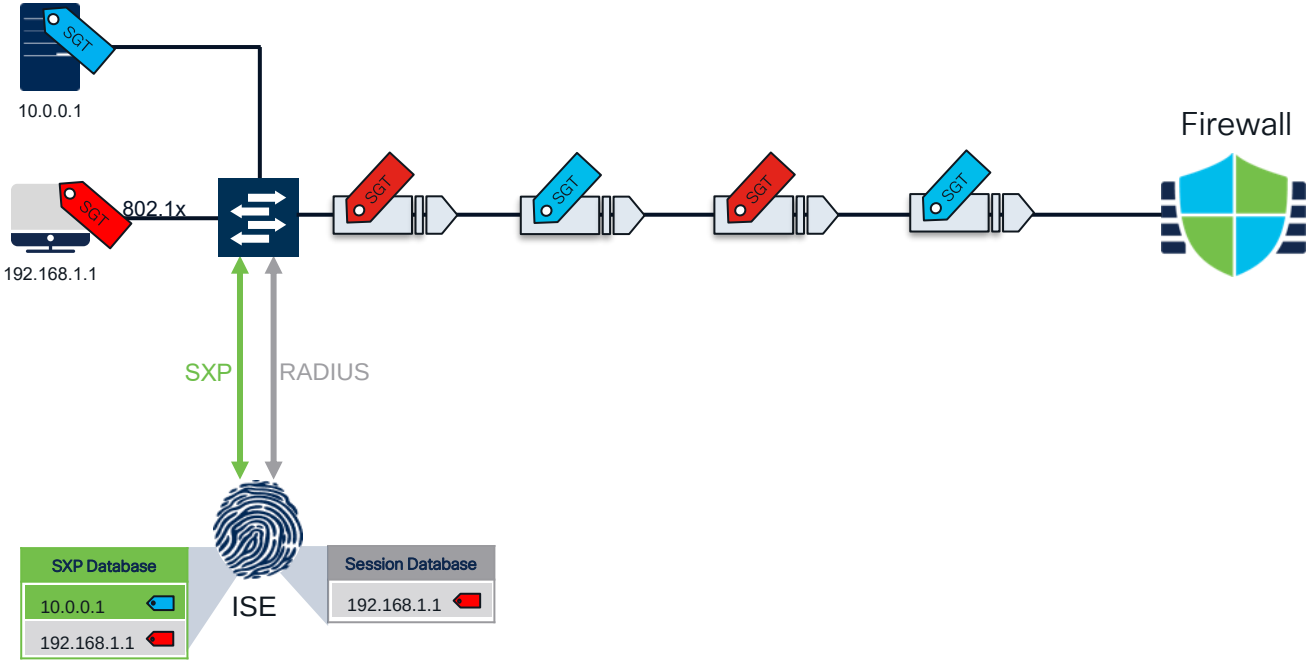
TrustSec Scalable Group Tag (SGT) Assignment



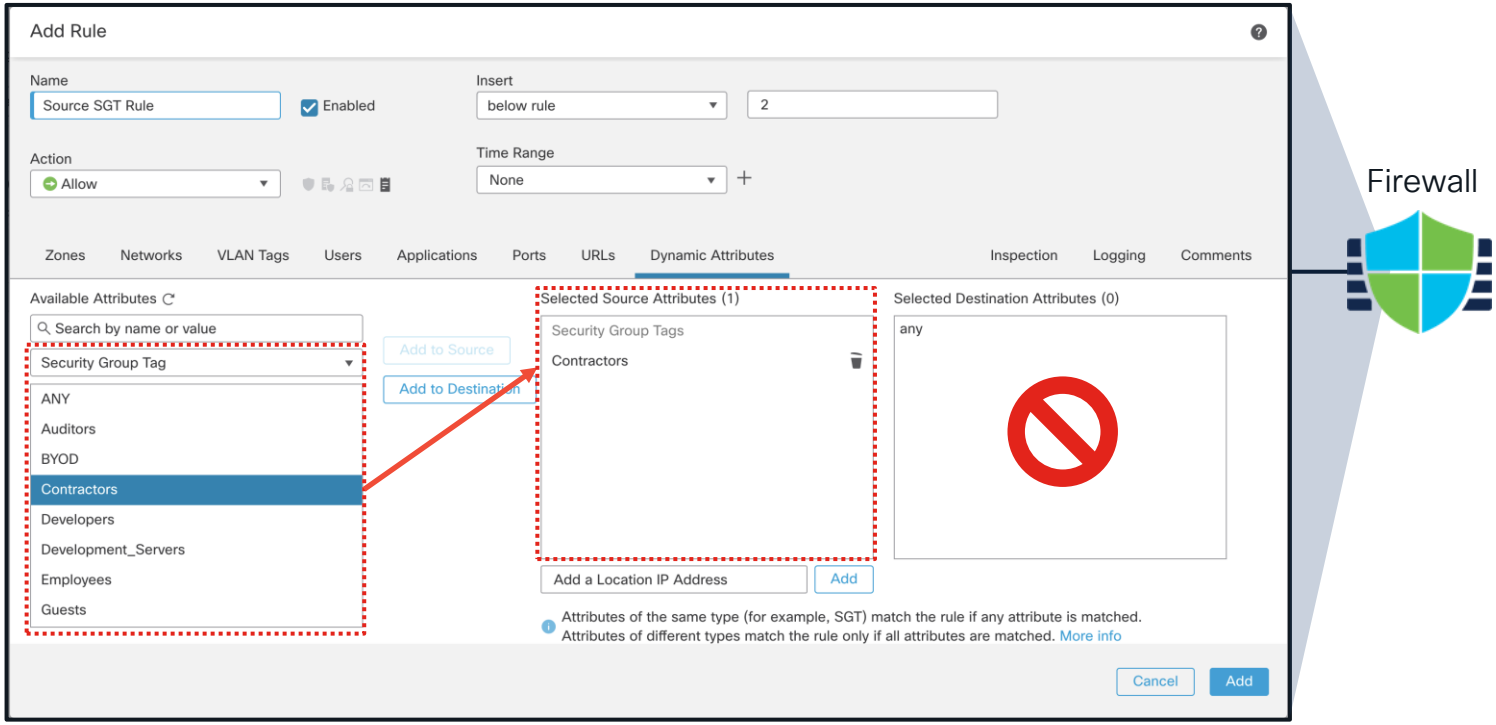
TrustSec Scalable Group Tag (SGT) Assignment



Inline SGT Propagation



Inline SGT Propagation



Note: Inline SGTs applicable for source criteria only

Attribute Based Policy – Inline SGTs

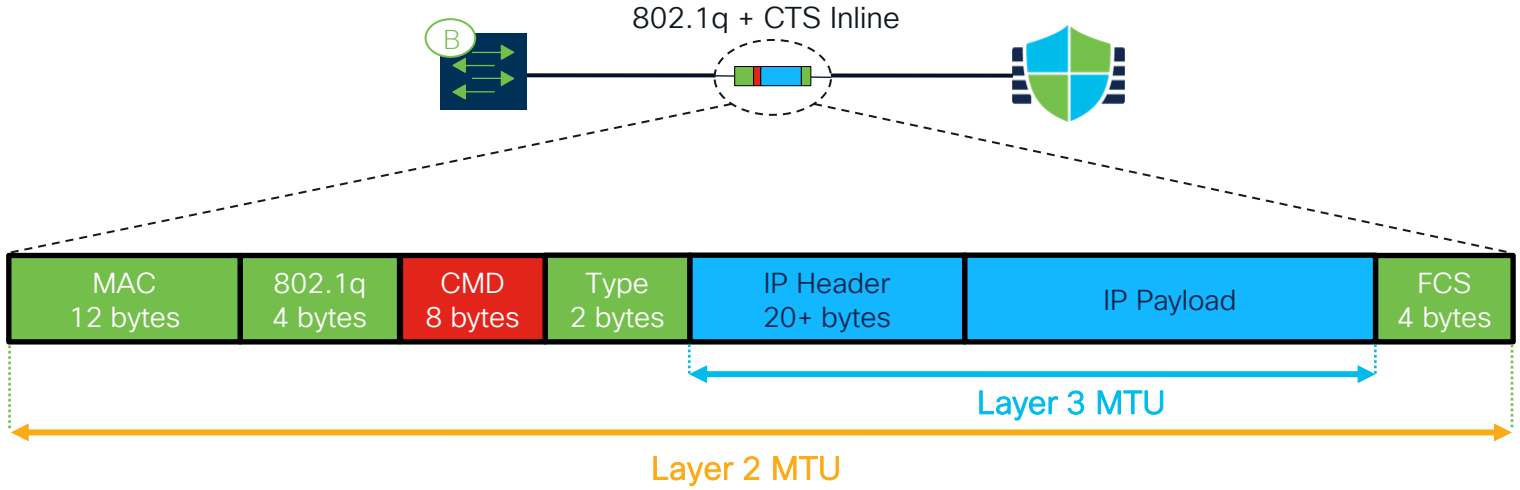
#	Name	Source Zones	Dest Zones	Users	Applications	Dest Ports	Source Dynamic Attributes	Destination Dynamic Attributes	Action
> Mandatory - Attribute-Based Policy (-)									
⌄ Default - Attribute-Based Policy (1-9)									
1	Workload_1	Any	Any	Any	Any	HTTP HTTPS	WorkloadObj_615c486dc9	WorkloadObj_615c8066483	Allow
2	IoT Support Service	External	IoT_VN	Any	Any	HTTPS SSH	IoT_Support	IoT	Allow
3	Machine Authentication	Corporate_VN	Shared_Services	Any	Any	AD_Services	Machine_Auth	VMWare_Active_Directory	Allow
4	Printing Service	Corporate_VN	Data_Center_Edge	Any	Any	SNMP ICMP-PING Spooler_Service	RICOH-Aficio-SP-C410DN RICOH-Aficio-SP-C820DN Xerox-WorkCentre-5030 Xerox-WorkCentre-5135	APIC_A_ESG_Print_Servers	Allow
5	Block Social Media	Corporate_VN	External	Any	Facebook Google+ Instagram Tinder Twitter	Any	Contractors Branch_Locations	Any	Block
6	o365 Access	Corporate_				HTTPS HTTP	Any	o365_Common o365_Exchange o365_SharePoint	Allow
7	SecureX Threat Containment	Corporate_			Any	Any	SecureX_Quarantined_IPs SecureX_Suspicious_IPs	Honeypot_Service	Allow
8	ISE Threat Containment	Corporate_VN	Data_Center_Edge	Any	Any	Any	Quarantined_Systems	Honeypot_Service	Allow
9	Cloud App Access	Corporate_VN	WAN	Any	Any	HTTP HTTPS	Employees	Azure_HR_Workload Azure_Intranet_Service	Allow

TrustSec inline propagated
Scalable Group Tags

Note: Inline SGTs applicable for source criteria only

SGT Inline Propagation Through a Firewall Demo

MTU Considerations

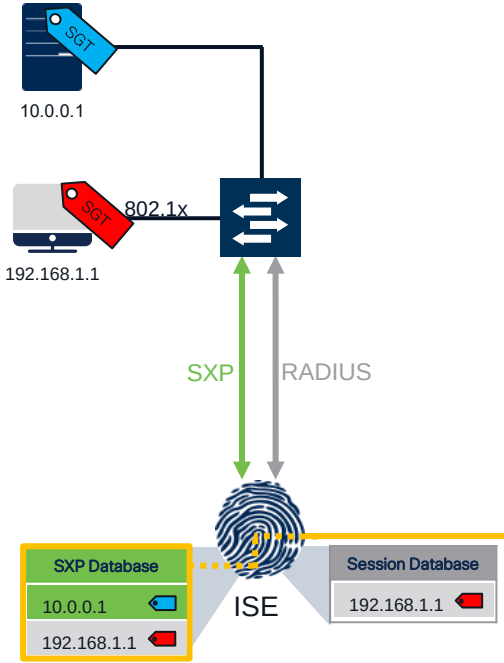


- The MTU on the FTD firewalls the is set up via FMC per interface using Layer 3 MTU.
- For **Firepower 4100/9300** platforms, maximum supported Layer 3 MTU is calculated as follows:

  L3 MTU = 9176 = L2 MTU (9206) – MAC (12B) – 802.1q (4B) – CMD (8B) – Type (2B) – FCS (4B)
- For **Firepower 1100/2100** platforms, maximum supported Layer 3 MTU is calculated as follows:

  L3 MTU = 9186 = L2 MTU (9216) – MAC (12B) – 802.1q (4B) – CMD (8B) – Type (4B) – FCS (4B)

Control Plane Propagation – SXP Topic



Remains in FMC until explicitly deleted by ISE pxGrid SXP topic update.

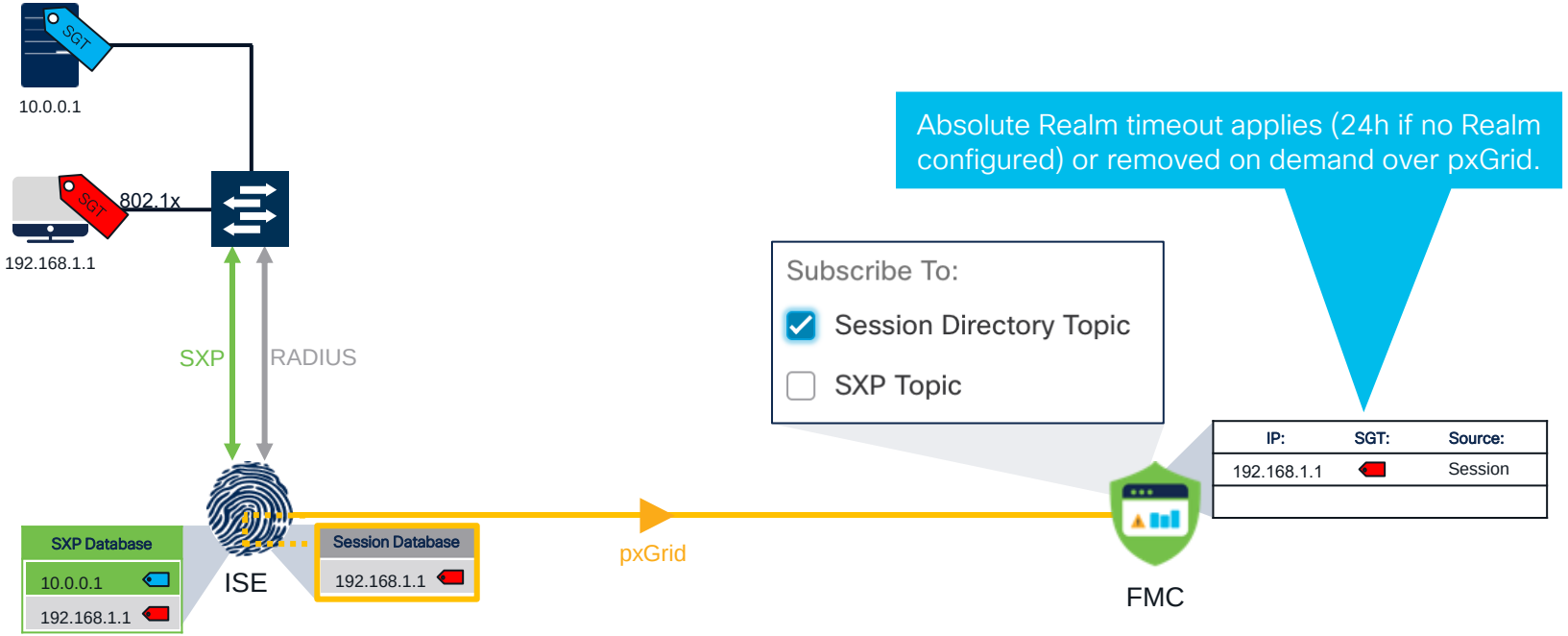
Subscribe To:

- [ ] Session Directory Topic
- [x] SXP Topic

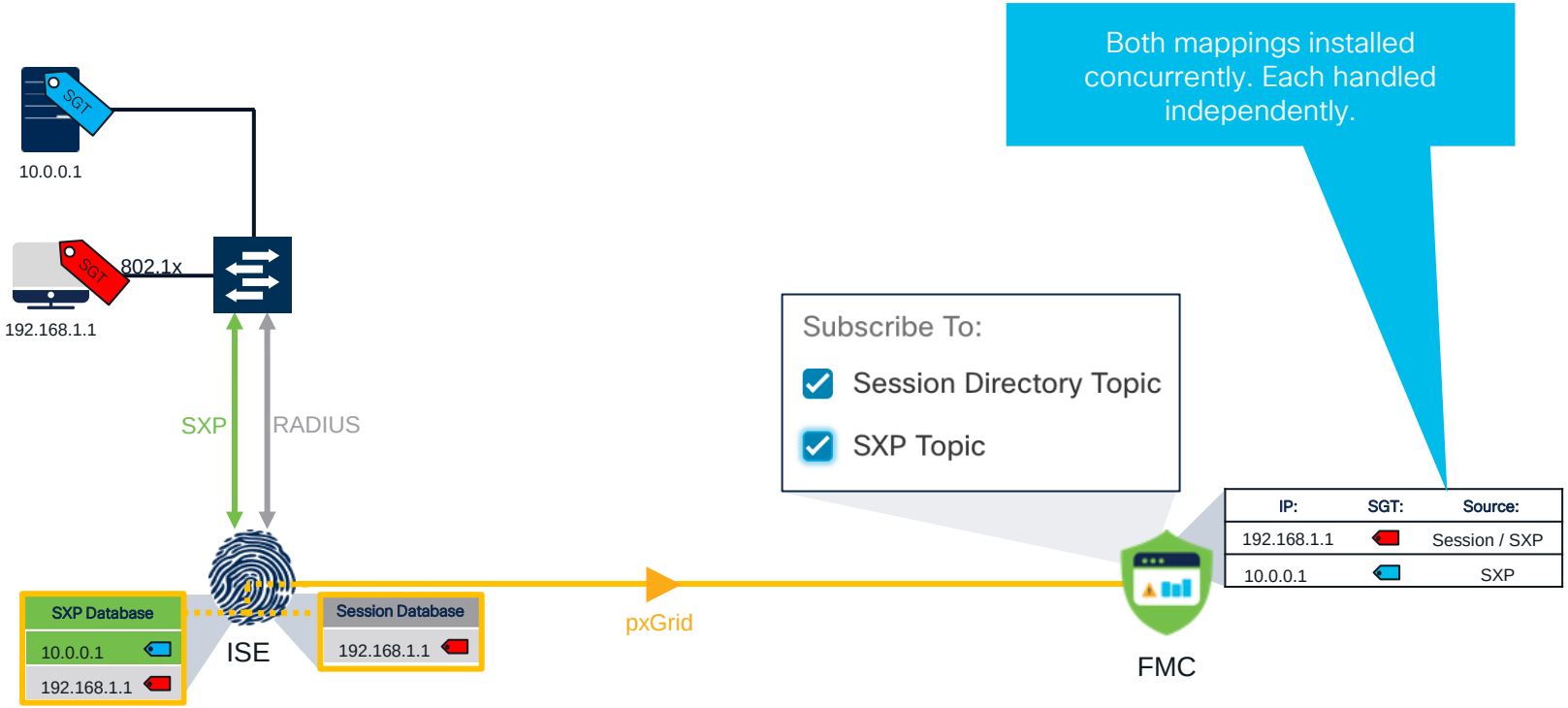
IP:	SGT:	Source:
192.168.1.1		SXP
10.0.0.1		SXP

FMC

Control Plane Propagation – Session Topic



Control Plane Propagation – SXP and Session Topics Concurrently



SXP and Session Topic Sourced Entries Timeout

Firewall

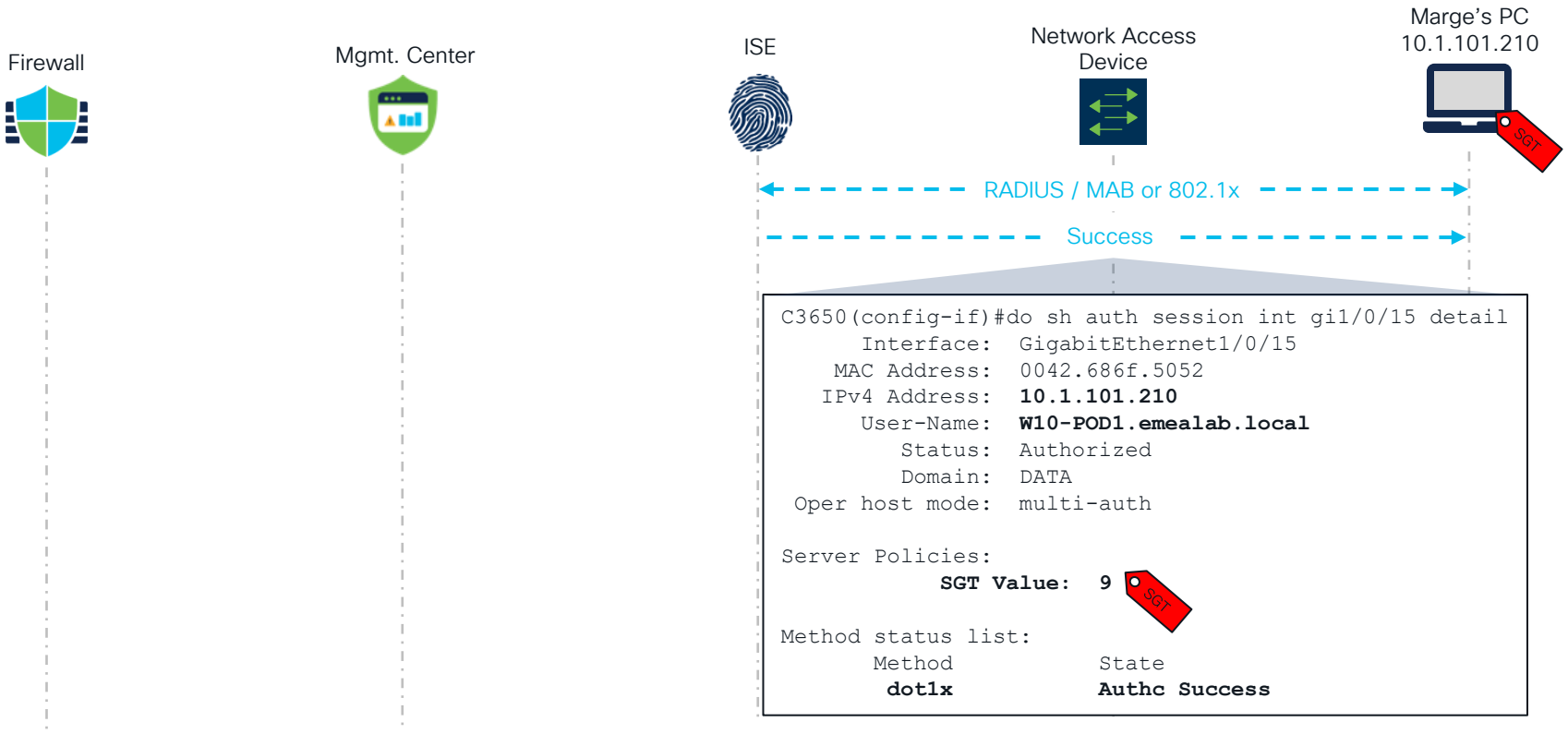
```
----------------
Host ::ffff:10.1.101.210
----------------
::ffff:10.1.101.210:4 realm 2 type 1, username marge
::ffff:10.1.101.210: initialized 1 sgt 6, device_type 450,
location_ip ::ffff:10.1.101.99
::ffff:10.1.101.210: SXP initialized 1 sgt 6

-------------------
USER:GROUPS
-------------------
4:2,1, (active_sessions: 1)
```

```
----------------
Host ::ffff:10.1.101.210
----------------

::ffff:10.1.101.210: SXP initialized 1 sgt 6

-------------------
USER:GROUPS
-------------------
```

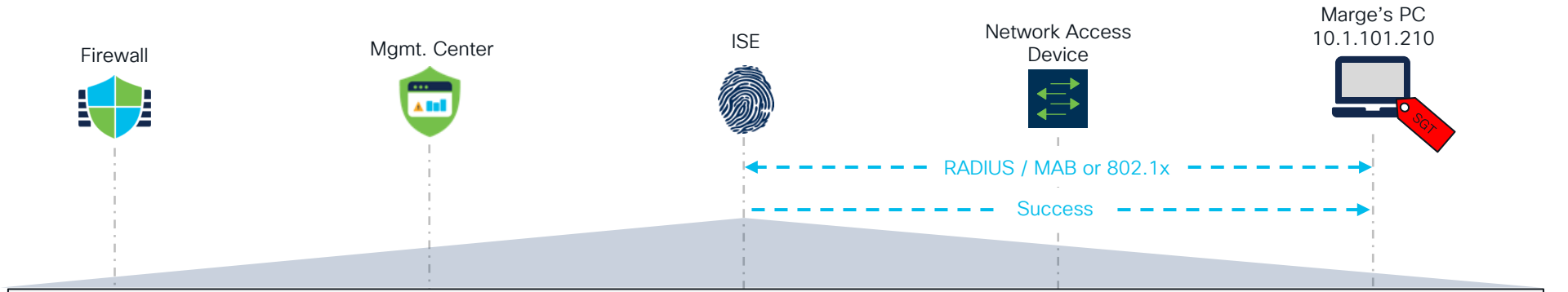
Session Database entry removed due to Realm timeout.

Session Topic Entry
SXP Topic

802.1x Session over SXP Topic Propagation



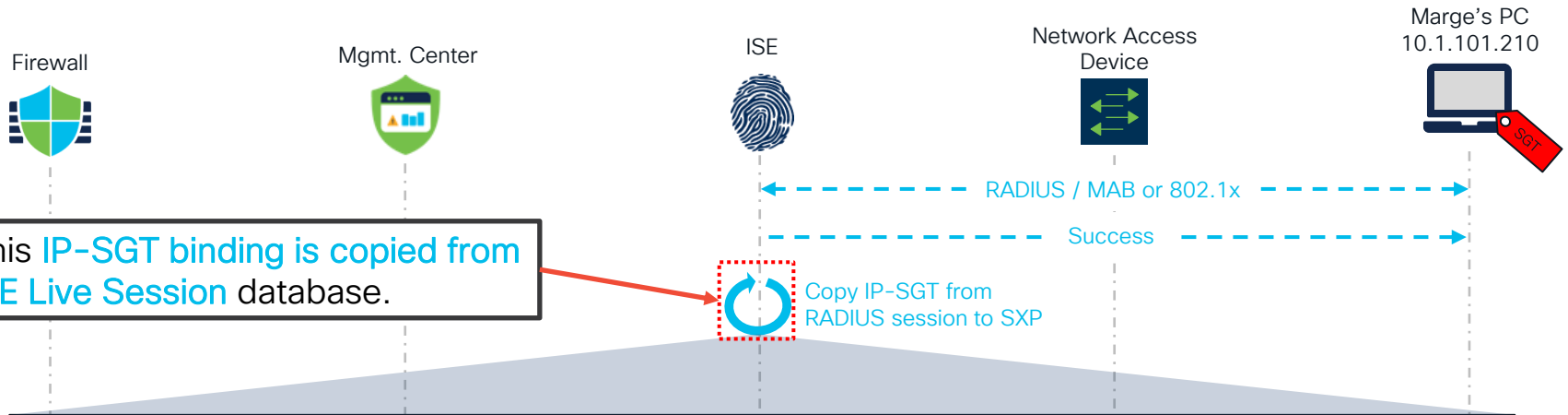
802.1x Session over SXP Topic Propagation



Session...	Action	Auth M...	Authenti...	Endpoint ID	Identity	IP Address	Security G...
Started	Show CoA Actions	dot1x	EAP-TLS	00:42:68:6F:50:52	W10-POD1.emealab.local	10.1.101.210	Machine_SGT

This IP-SGT mapping is now available in the ISE Live Session database. This entry may be shared with Management Center over pxGrid Session topic, or...

802.1x Session over SXP Topic Propagation

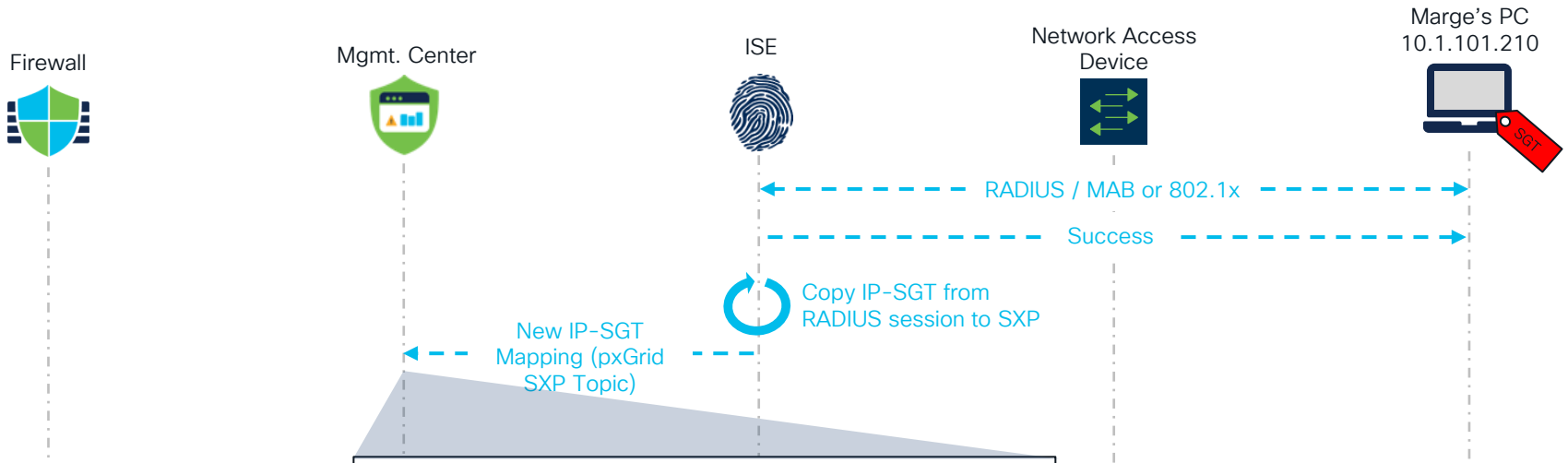


This IP-SGT binding is copied from ISE Live Session database.

IP Address	SGT	Learned From	Learned ...	PSNs Involved
10.1.101.210/32	Machine_SGT (9/0009) SGT	172.16.134.96,10.1.101.99	Session	ise01

This entry may be shared with Management Center over pxGrid SXP topic.
It may be also shared with TrustSec infrastructure using SXP peering.

802.1x Session over SXP Topic Propagation



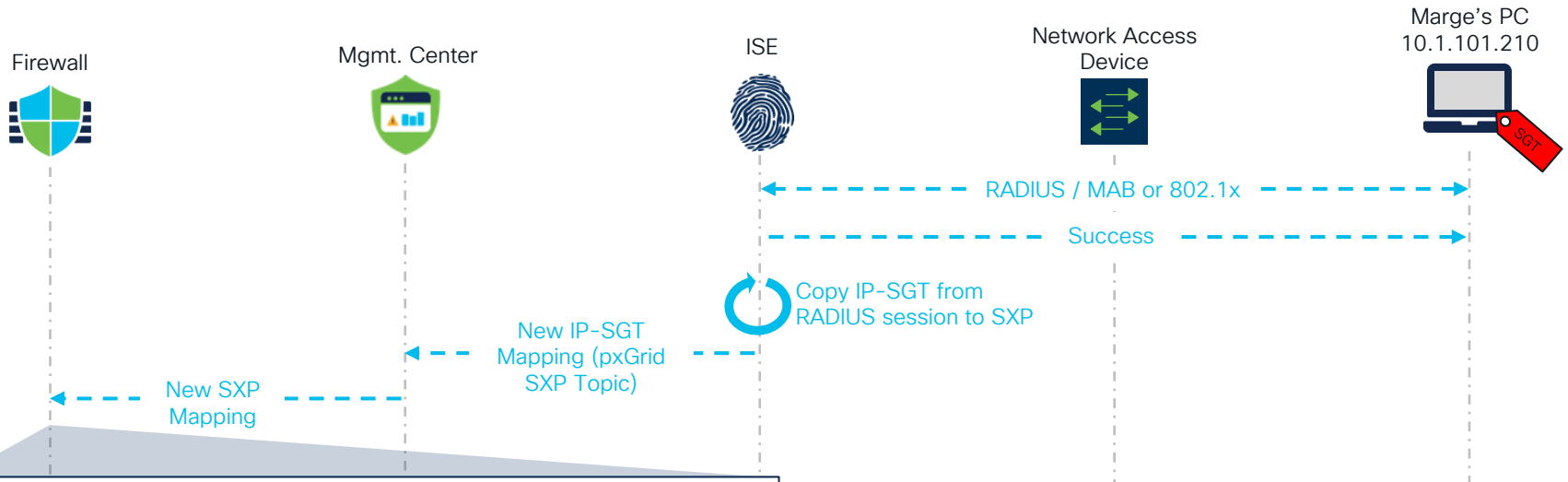

```
admin@fmc:~$ sudo uip_reader -f
/var/sf/user_enforcement/uip_log_entries.1 -p -l
-------------------------------------
 Entry no: 107
   operation_type: SXP_BINDING_ADD
     sxp_binding {
        ipPrefix: "10.1.101.210/32"
        tag: "9"
        source: "10.1.101.99"
        peerSeq: "172.16.134.96,10.1.101.99"
     }
```

SGT

Installing SXP sourced IP-SGT mapping.

PeerSeq lists all SXP nodes involved (ISE and NAD in this case).

802.1x Session over SXP Topic Propagation

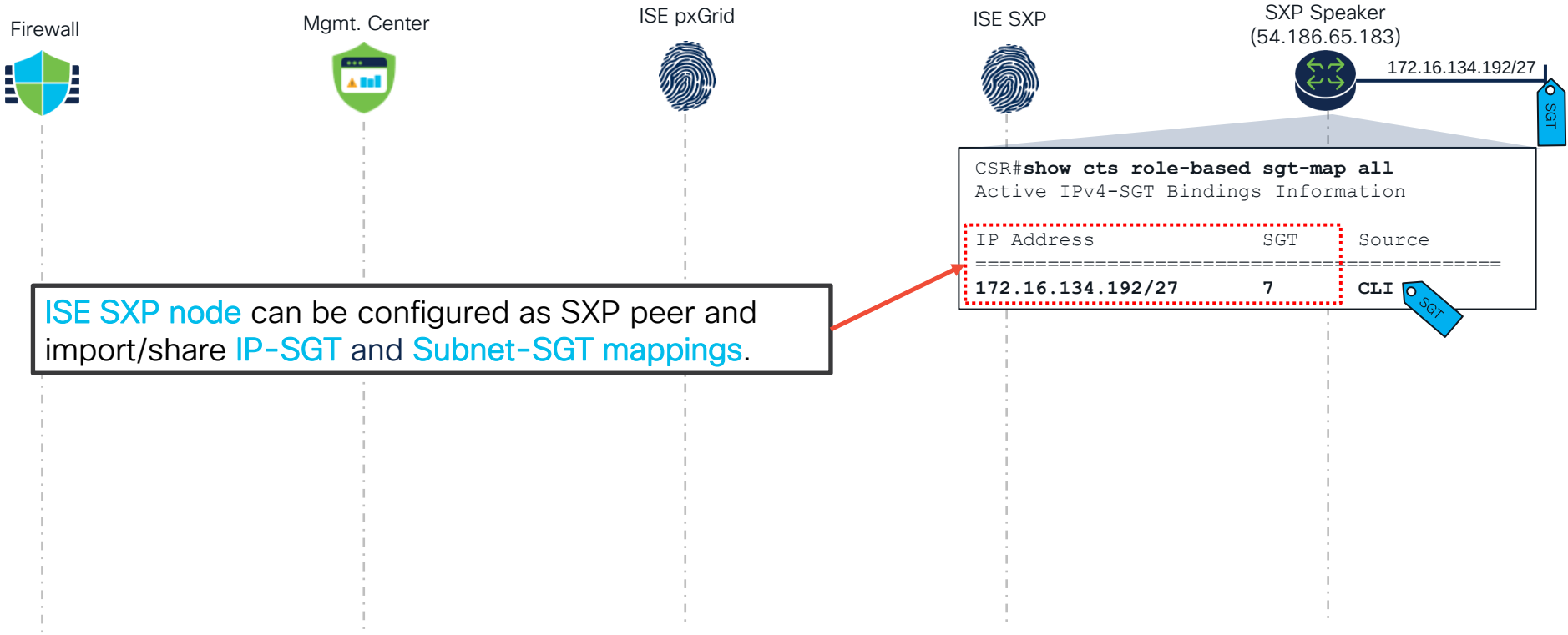



```
> system support firewall-engine-dump-user-identity-data
> expert
$ sudo cat /ngfw/var/sf/user_enforcement/user_identity.dump

----------------
Host ::ffff:10.1.101.210
----------------
::ffff:10.1.101.210: SXP initialized 1 sgt 9
ABP values: None.
```

SGT

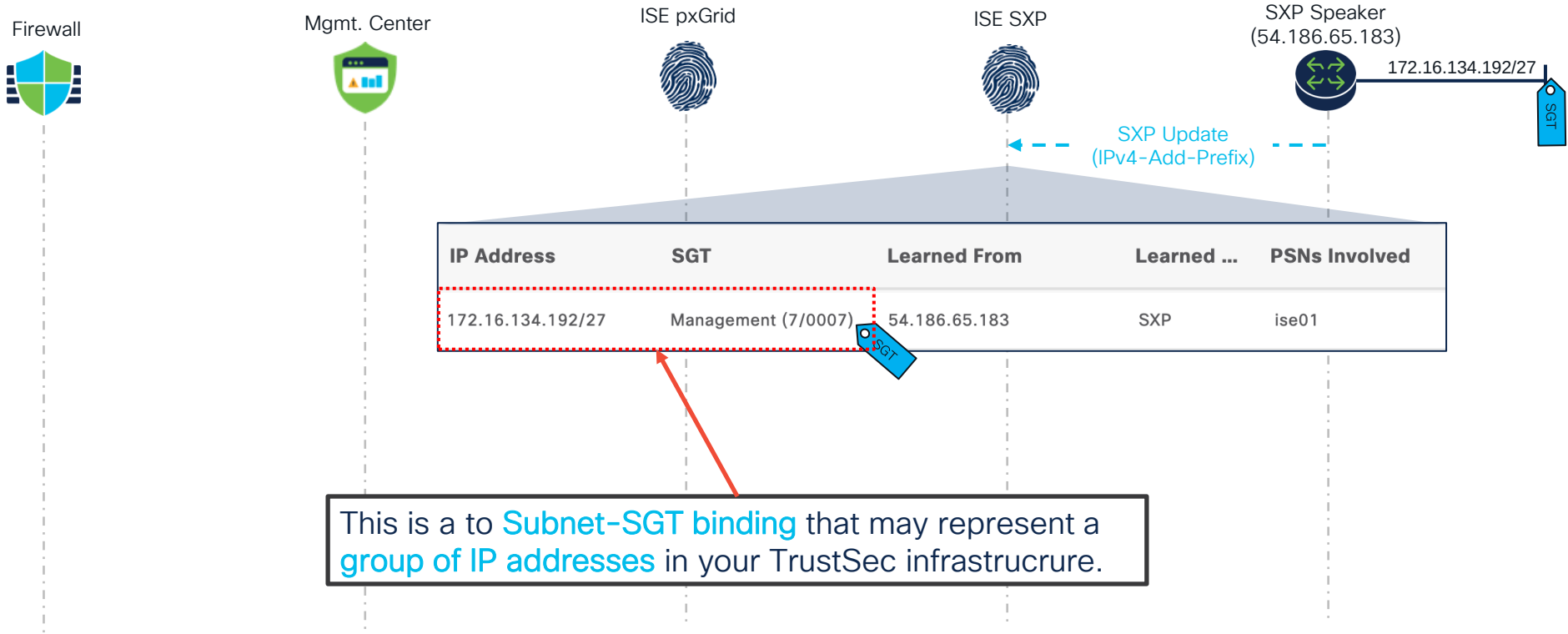
This IP-SGT mapping remains until explicitly removed by ISE over SXP topic. No timeout applies.

SXP Mapping over SXP Topic Propagation



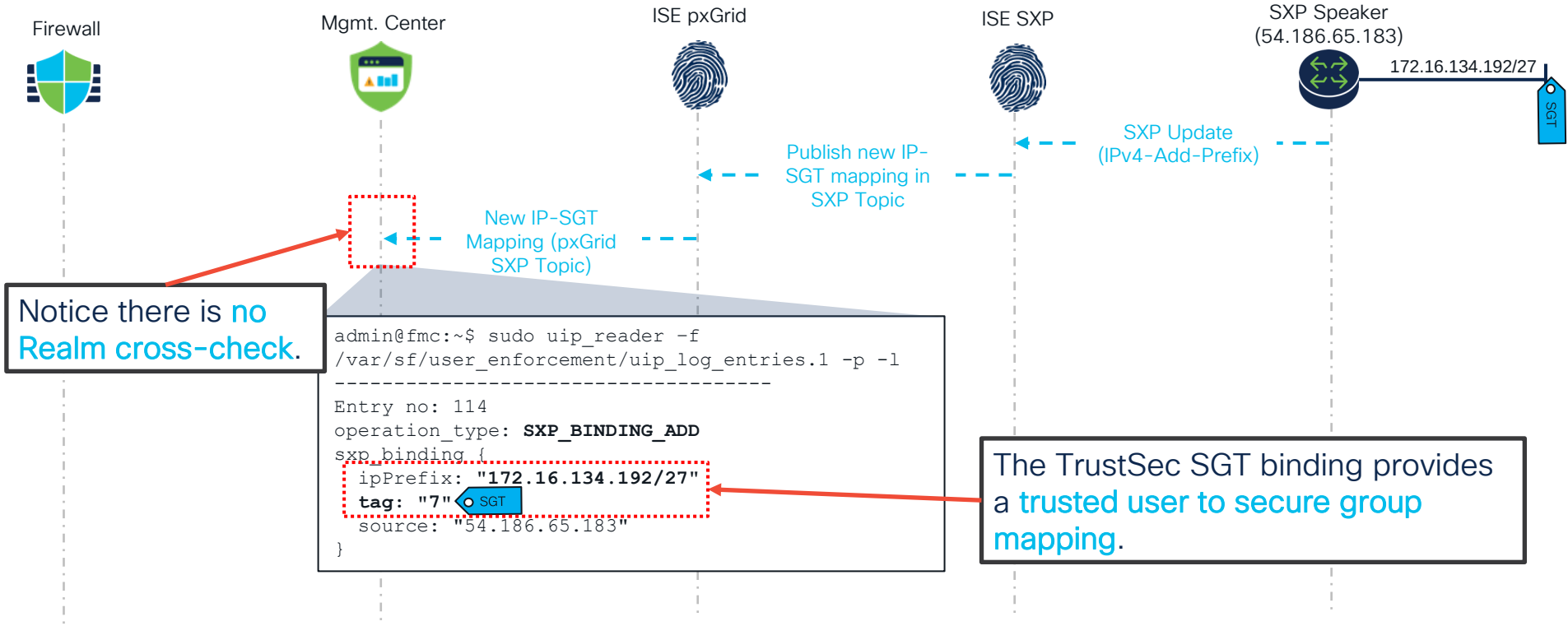
ISE SXP node can be configured as SXP peer and import/share IP-SGT and Subnet-SGT mappings.

SXP Mapping over SXP Topic Propagation



This is a to Subnet-SGT binding that may represent a group of IP addresses in your TrustSec infrastrucrure.

SXP Mapping over SXP Topic Propagation

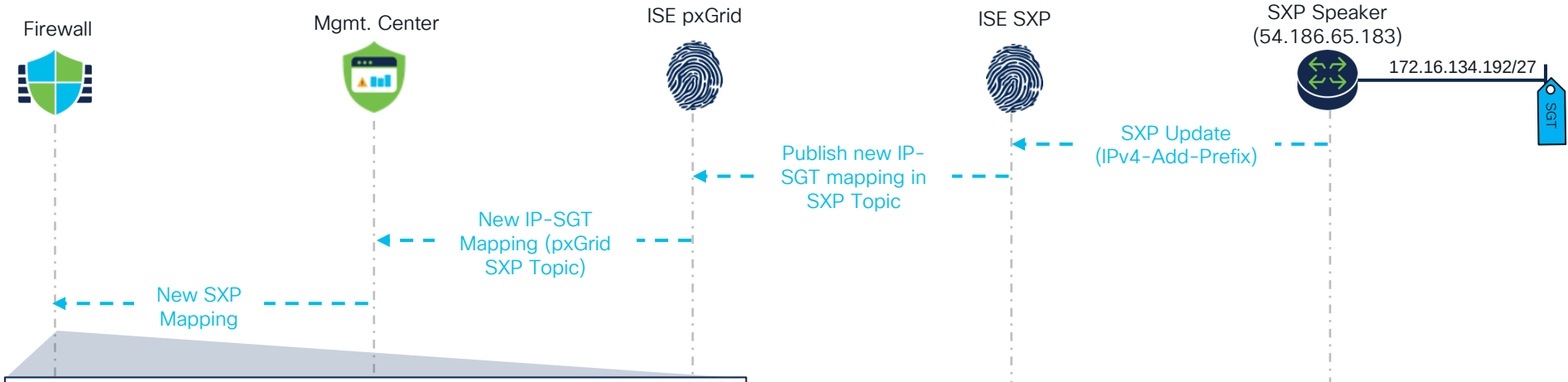


Notice there is no Realm cross-check.

```
admin@fmc:~$ sudo uip_reader -f
/var/sf/user_enforcement/uip_log_entries.1 -p -l
-------------------------------------
Entry no: 114
operation_type: SXP_BINDING_ADD
sxp_binding {
 ipPrefix: "172.16.134.192/27"
 tag: "7"  SGT
  source: "54.186.65.183"
}
```

The TrustSec SGT binding provides a trusted user to secure group mapping.

SXP Mapping over SXP Topic Propagation




```
> system support firewall-engine-dump-user-identity-data
> expert
$ sudo cat /ngfw/var/sf/user_enforcement/user_identity.dump

-------------------
SXP MAPPING:
-------------------
IP : 172.16.134.192/27
SGT : initialized 1, value 7
ABP values: None.
```

SGT

/27 Subnet-SGT entry is now installed in Snort's memory. It will remain installed until explicitly removed. No timeout applies.

MAC Authentication Bypass and Machine Accounts are Supported with SXP

ISE MnT

Live Sessions

Identity	IP Address	Server	Auth M...	Endpoint Profile	Security G...
	IP Address				
94:D4:69:FE:00:B0	172.28.99.201,fe ...	ise01	mab	Cisco-AP-Aironet-1...	AP_SGT
W10-POD1.emealab.local	10.1.101.210,fe8 ...	ise01	dot1x	Workstation	Machine_SGT

MAC Authentication Bypass session with APT_SGT.

ISE SXP

SXP Mappings

IP Address	SGT	Learned From
10.1.101.210/32	Machine_SGT (9/000...	172.16.134.96,10.1.101.99
172.28.99.201/32	AP_SGT (10/000A)	172.16.134.96,10.1.101.99

ISE pxGrid

pxGrid

Management Center

Firewall IP-SGT Mappings

```
# uip_reader -f sxp_log_entries.1 -p -l -t

-------------------------------------
Entry no: 107
operation_type: SXP_BINDING_ADD
sxp_binding {
  ipPrefix: "10.1.101.210/32"
  tag: "9"
}

Entry no: 108
operation_type: SXP_BINDING_ADD
sxp_binding {
  ipPrefix: "172.28.99.201/32"
  tag: "10"
}
```

MAC Authentication Bypass and Machine Accounts are Supported with SXP

ISE MnT

Live Sessions

Identity	IP Address	Server	Auth M...	Endpoint Profile	Security G...
	IP Address				
94:D4:69:FE:00:B0	172.28.99.201,fe ...	ise01	mab	Cisco-AP-Aironet-1...	AP_SGT
W10-POD1.emealab.local	10.1.101.210,fe8 ...	ise01	dot1x	Workstation	Machine_SGT

Machine Auth session with Machine_SGT.

ISE SXP

SXP Mappings

IP Address	SGT	Learned From
10.1.101.210/32	Machine_SGT (9/000...	172.16.134.96,10.1.101.99
172.28.99.201/32	AP_SGT (10/000A)	172.16.134.96,10.1.101.99

ISE pxGrid

pxGrid

Management Center

Firewall IP-SGT Mappings

```
# uip_reader -f sxp_log_entries.1 -p -l -t

-------------------------------------
Entry no: 107
operation_type: SXP_BINDING_ADD
sxp_binding {
  ipPrefix: "10.1.101.210/32"
  tag: "9"
}

Entry no: 108
operation_type: SXP_BINDING_ADD
sxp_binding {
  ipPrefix: ”172.28.99.201/32"
  tag: ”10"
}
```

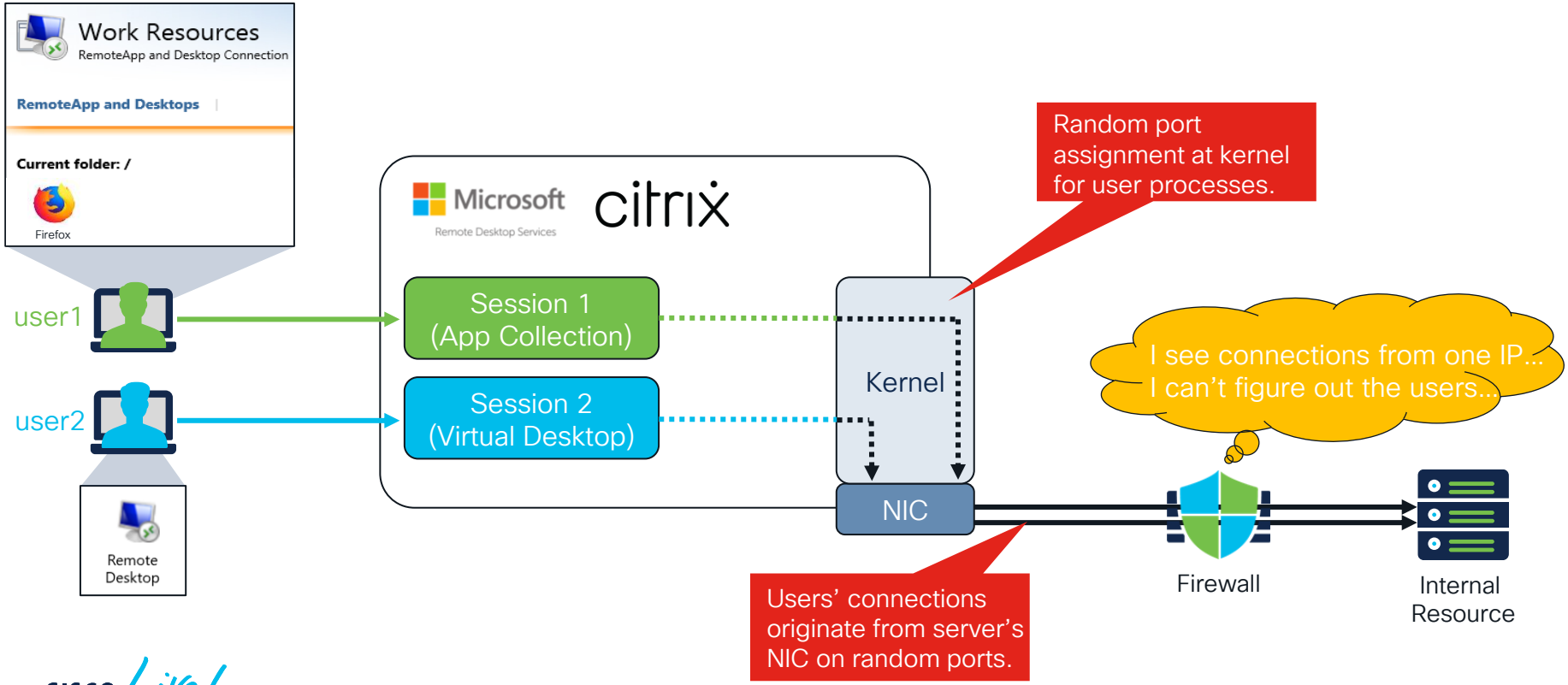
Key Takeaways

- TrustSec deployment does not require Realm configuration – IP-SGT mapping provides group assignment for authorization.
- IP-SGT mappings are not subjected to time-based removal – they must be explicitly removed.
- Machine and MAC Authentication Bypass supported with SXP Topic – IP-SGT abstracts the initial authentication method.
- SXP topic allows firewall integration with wider TrustSec domain e.g. ACI (EPG-SGT mapping by ISE)
- Consider ISE scaling – SXP may require a set of dedicated nodes in ISE deployment with their own IP-SGT binding count limits

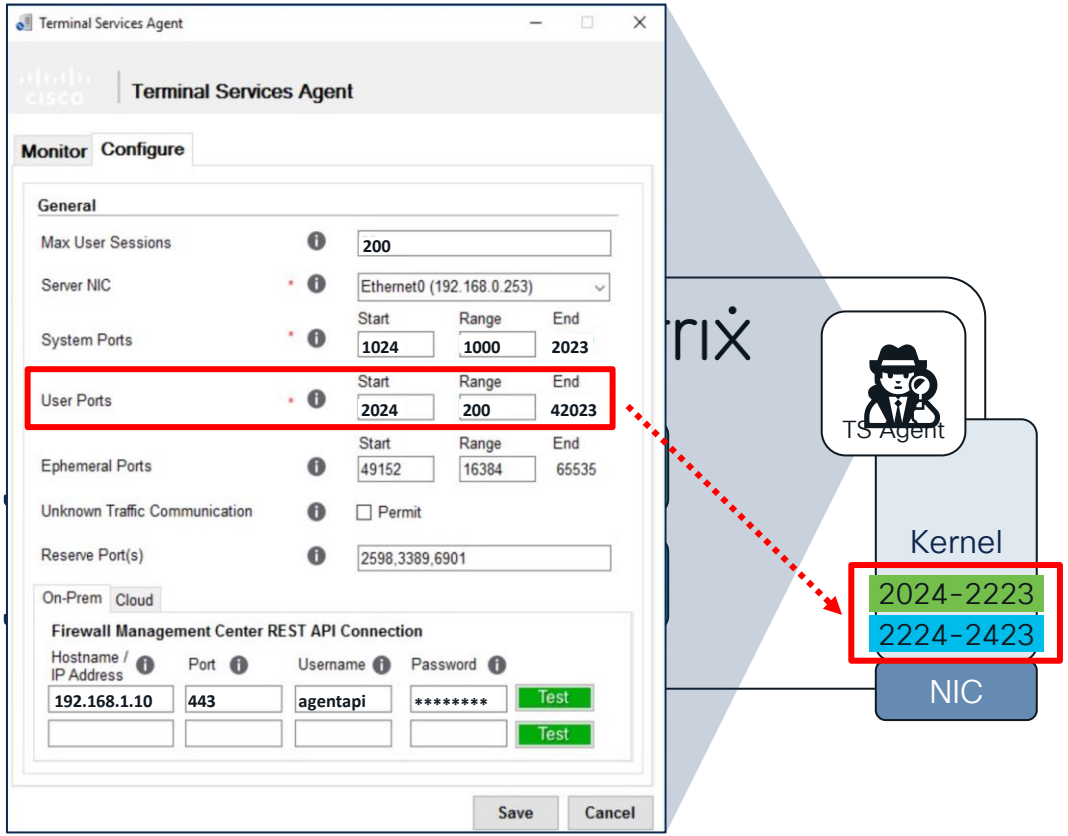
PASSIVE AUTHENTICATION

Terminal Services Agent

Terminal Services – The Challenge



Terminal Services (TS) Agent to The Rescue



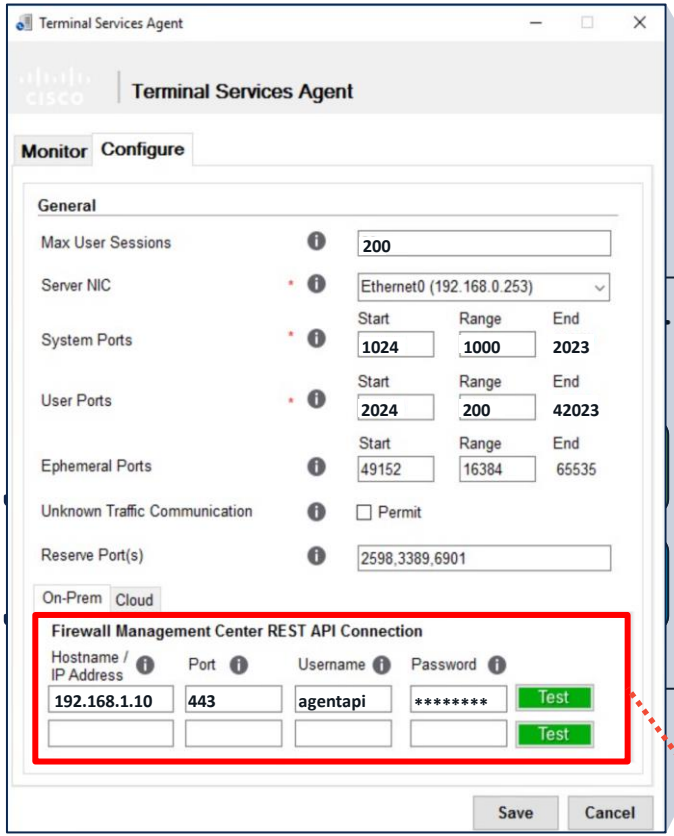
user1

user2

Firewall

Internal Resource

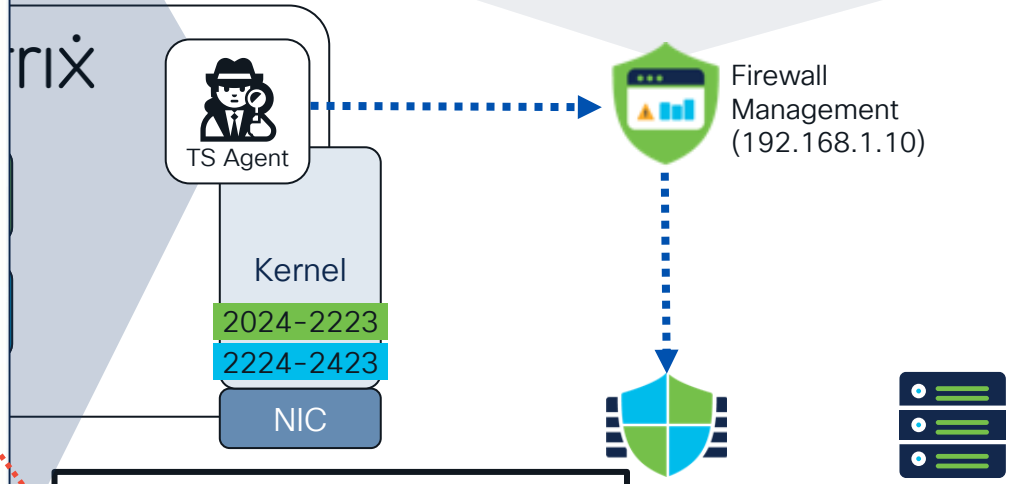
Terminal Services (TS) Agent to The Rescue



user1

user2

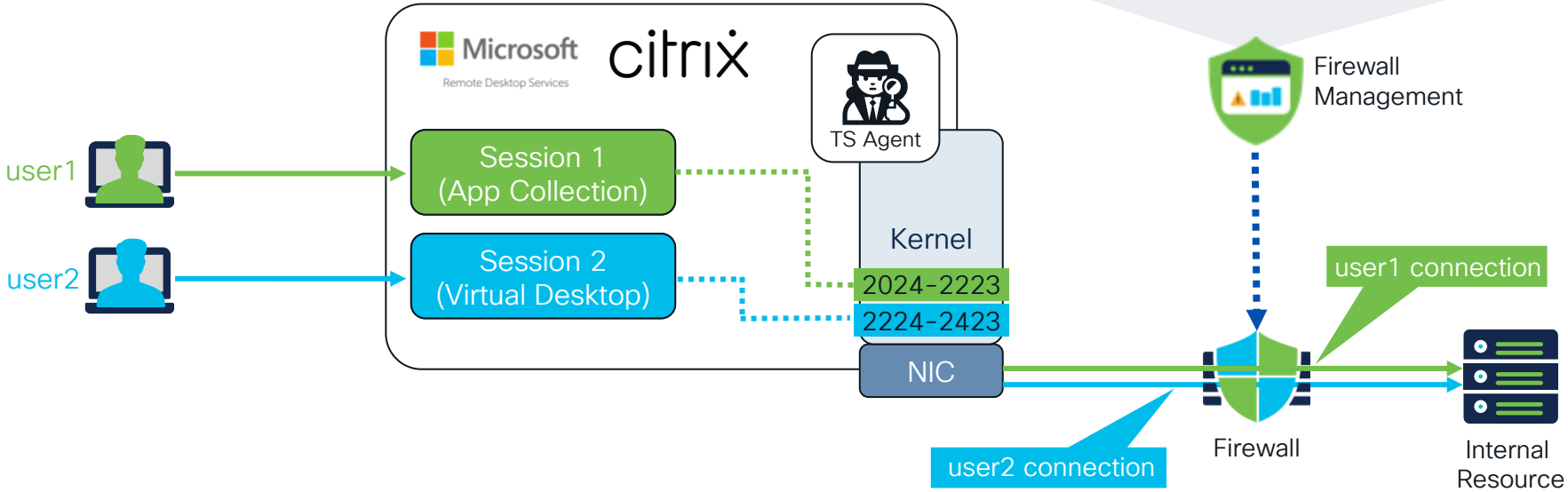
#	User	IP	Port Range
1	user1@acme.com	192.168.0.253	2024-2223
2	user2@acme.com	192.168.0.253	2224-2423



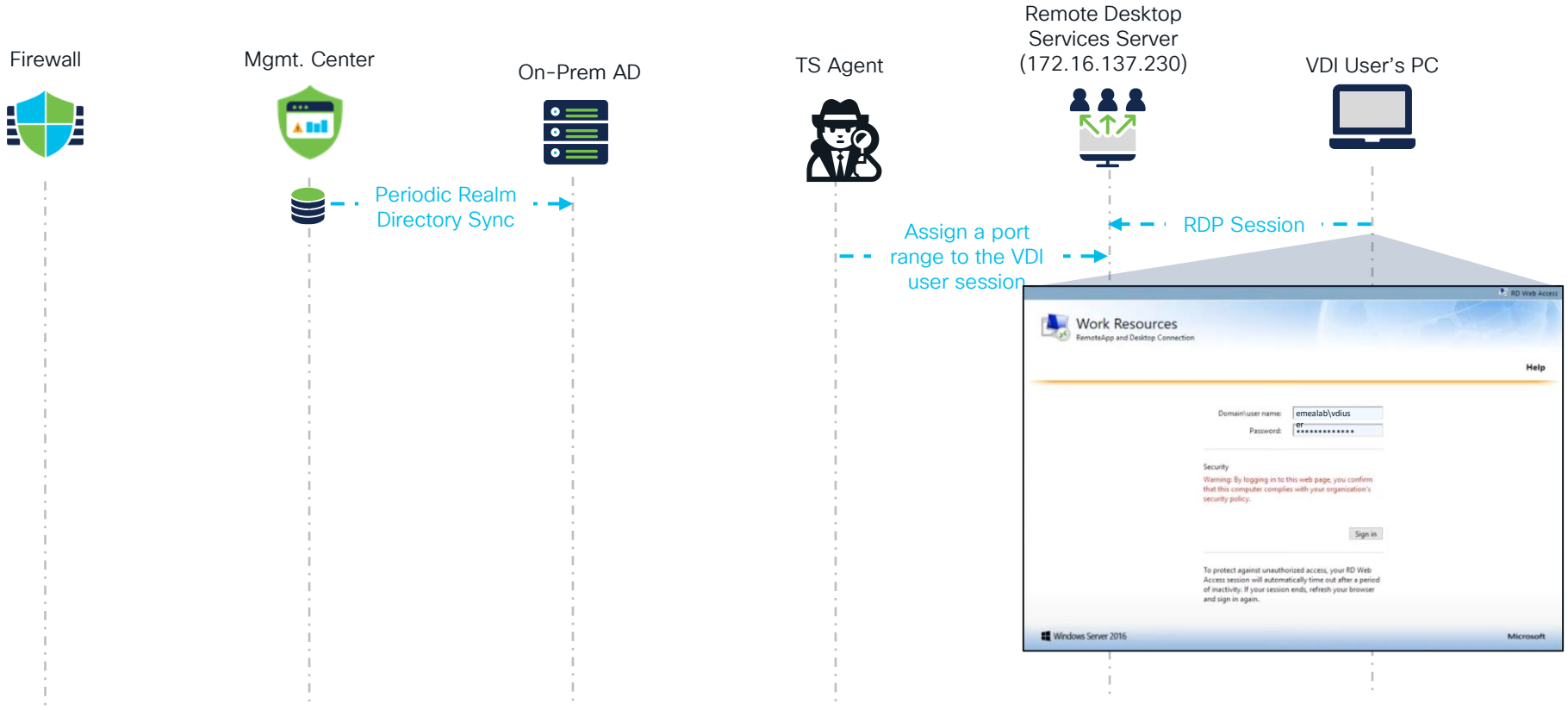
Set TS Agent to Firewall Management Center communication. High Availability and On-Prem/Cloud-Delivered supported.

Remote Desktop Session with TS Agent

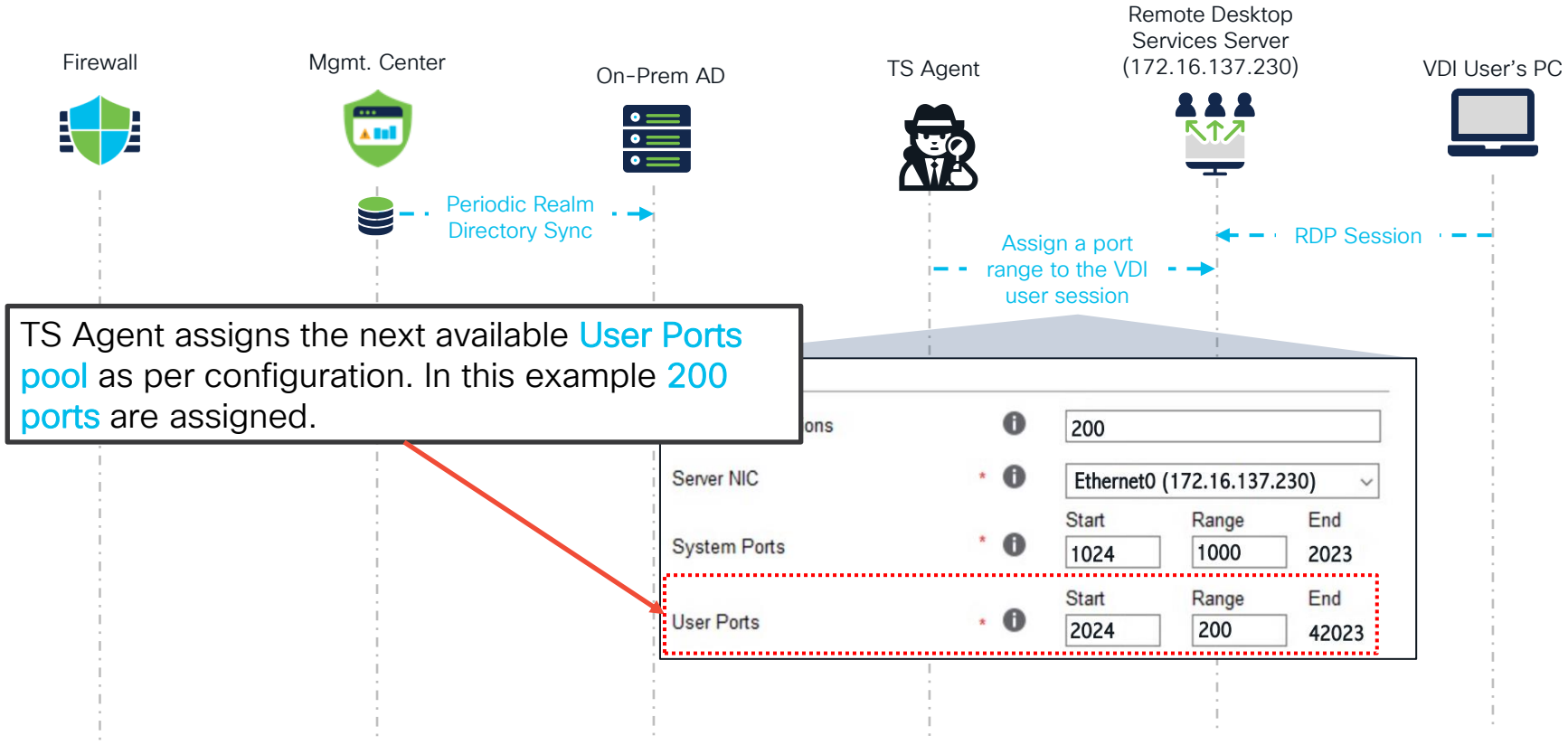
#	User	IP	Port Range
1	user1@acme.com	192.168.0.253	2024-2223
2	user2@acme.com	192.168.0.253	2224-2423



TS Agent Flow

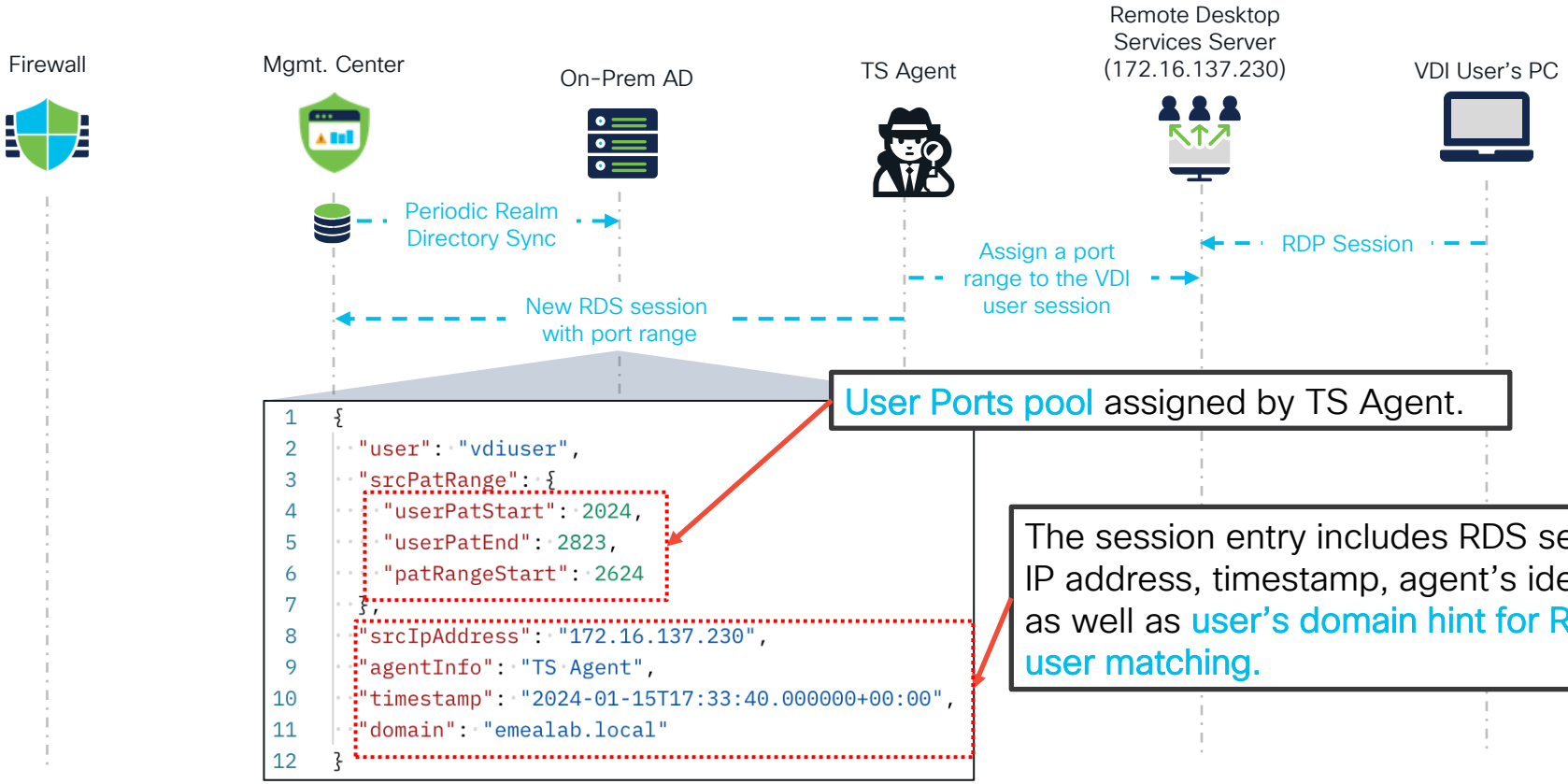


TS Agent Flow



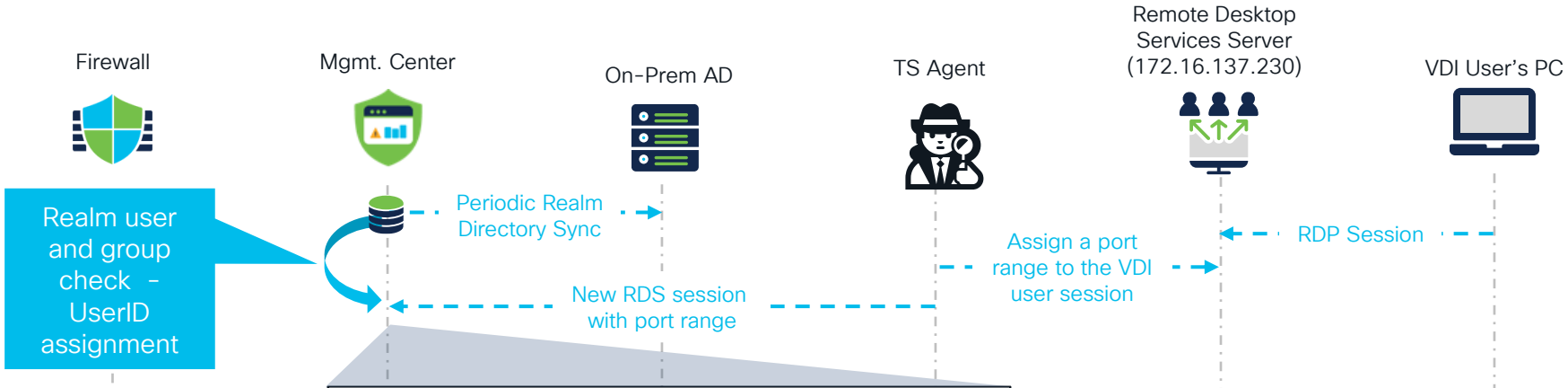
TS Agent assigns the next available User Ports pool as per configuration. In this example 200 ports are assigned.

TS Agent Flow




```
{
  "user": "vdiuser",
  "srcPatRange": {
    "userPatStart": 2024,
    "userPatEnd": 2823,
    "patRangeStart": 2624
  },
  "srcIpAddress": "172.16.137.230",
  "agentInfo": "TS Agent",
  "timestamp": "2024-01-15T17:33:40.000000+00:00",
  "domain": "emealab.local"
}
```

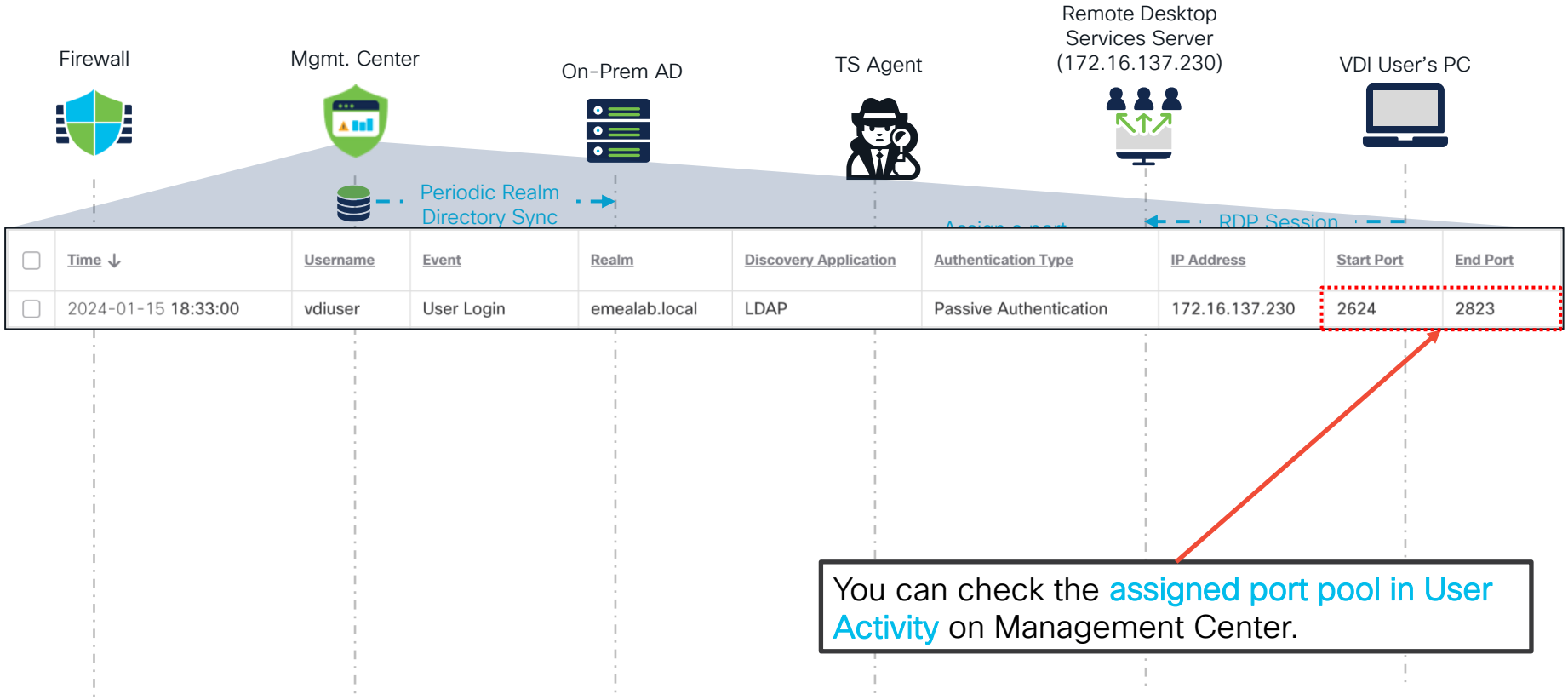
TS Agent Flow




```
admin@fmc:~$ sudo uip_reader -f
/var/sf/user_enforcement/uip_log_entries.1 -p -l
------------------------------------
 Entry no: 191
   SubscriberSession:
     Operation: SESSION_ADD
     Type: IDENTITY_PASSIVE
     Username: vdiuser
     User ID: 5
     Realm ID: 2
     IP Address: ::ffff:172.16.137.230
     Source PAT Range:
        pat range start: 2024
        user pat start: 2624
        user pat end: 2823
 Hop Timestamps: 2024-01-15 17:33:45(+5 sec)
```

You can check the delay from initial user login, as reported by TS Agent.

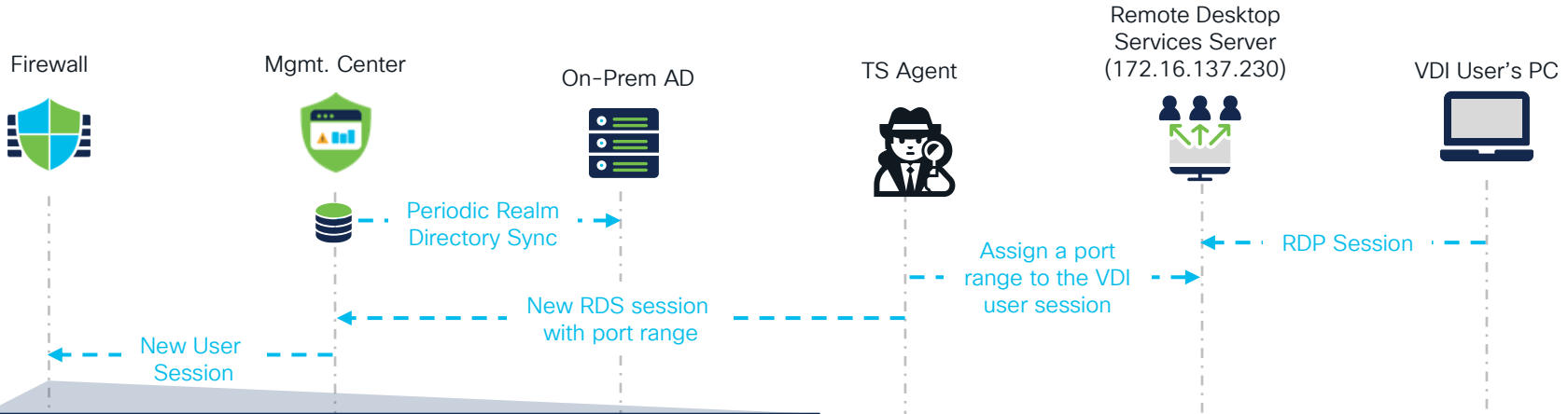
TS Agent Flow



Time ↓	Username	Event	Realm	Discovery Application	Authentication Type	IP Address	Start Port	End Port
2024-01-15 18:33:00	vdiuser	User Login	emealab.local	LDAP	Passive Authentication	172.16.137.230	2624	2823

You can check the assigned port pool in User Activity on Management Center.

TS Agent Flow




```
> system support firewall-engine-dump-user-identity-data
> expert
$ sudo cat /ngfw/var/sf/user_enforcement/user_identity.dump

Host ::ffff:172.16.137.230
---------------
pat_range_start: 2024, pat_blocksize: 200
::ffff:172.16.137.230:5 realm 2 type 1 user_pat_start 2624

USER:GROUPS

5:4, (active_sessions: 1)
```

The user is now mapped to an IP address and a port pool in Snort's memory.

User to group mapping to IT (4) had been provided by Management Center upon checking with Realm.

Key Takeaways

- Consider TS Agent scale numbers:
  - Maximum number of user sessions = 200
  - Ensure sufficient pool of ports is assigned for your users
  - Maximum of 50 TS Agents supported per Cloud/On-Prem Firewall Management Center
- TS Agent does not PAT ICMP traffic
- Terminal services solutions supported:
  - Citrix Provisioning
  - Citrix XenDesktop
  - Citrix XenApp
  - Windows Terminal Services/Windows Remote Desktop Services (RDS)

Join at

slido.com

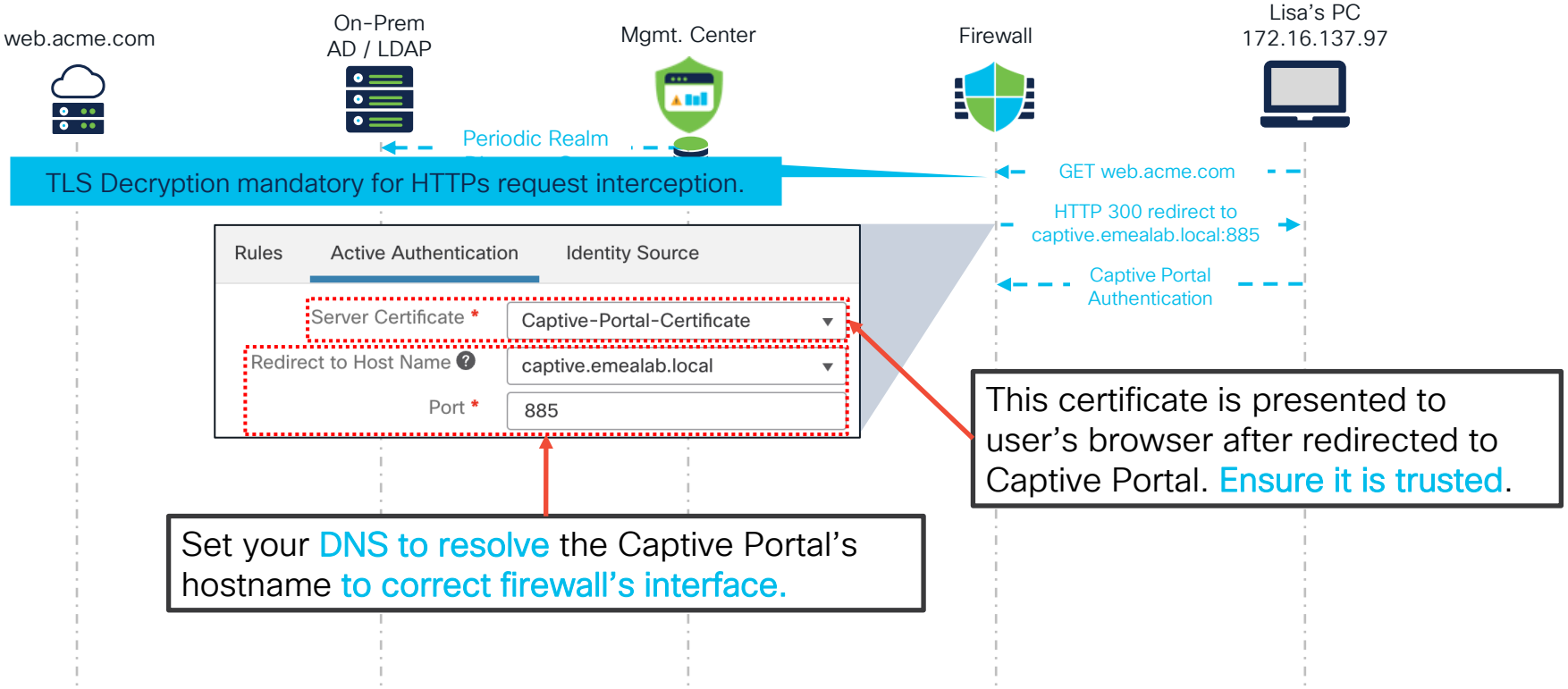
2901 029

QUIZ 2:

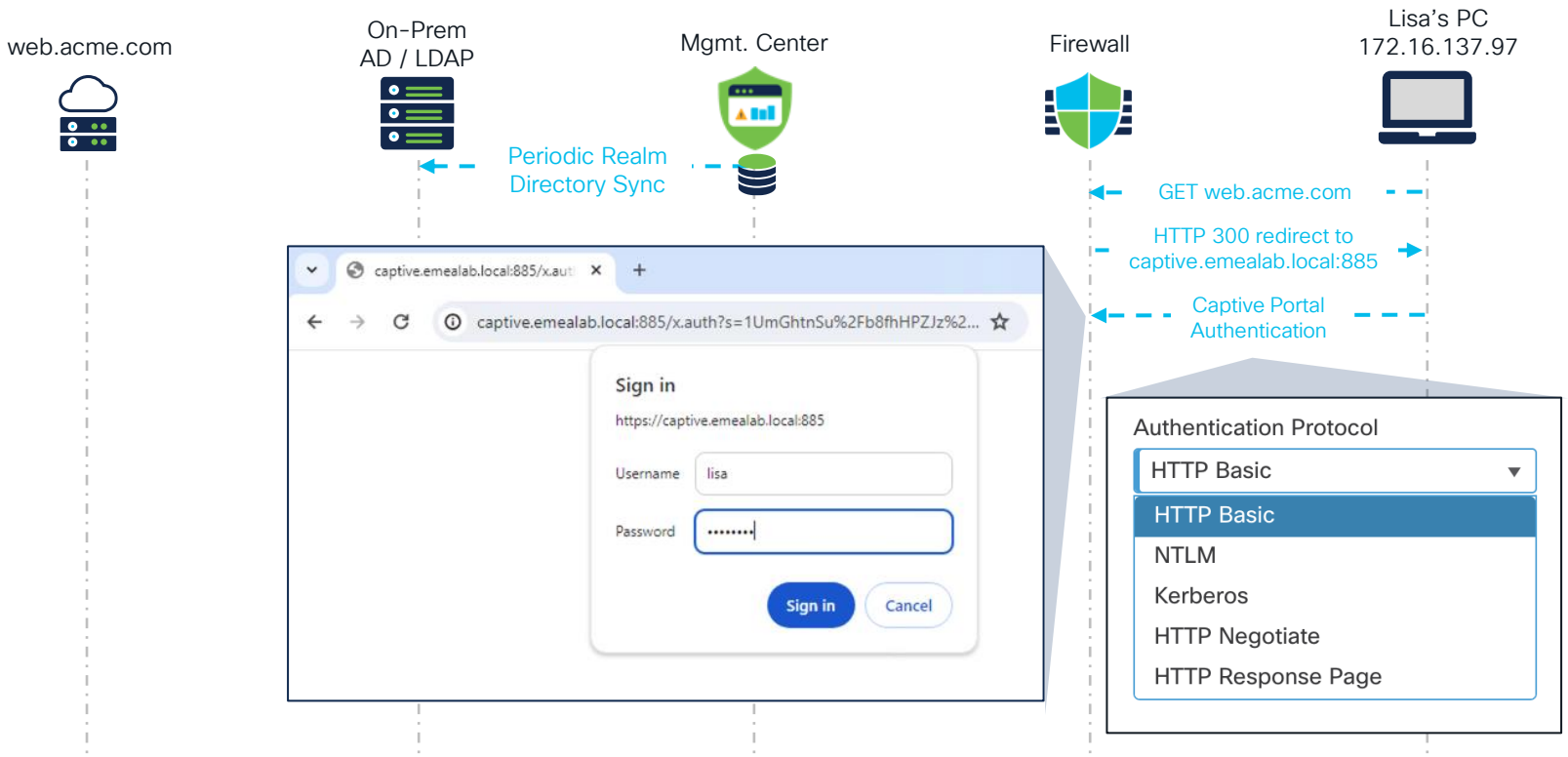
ACTIVE AUTHENTICATION

Captive Portal

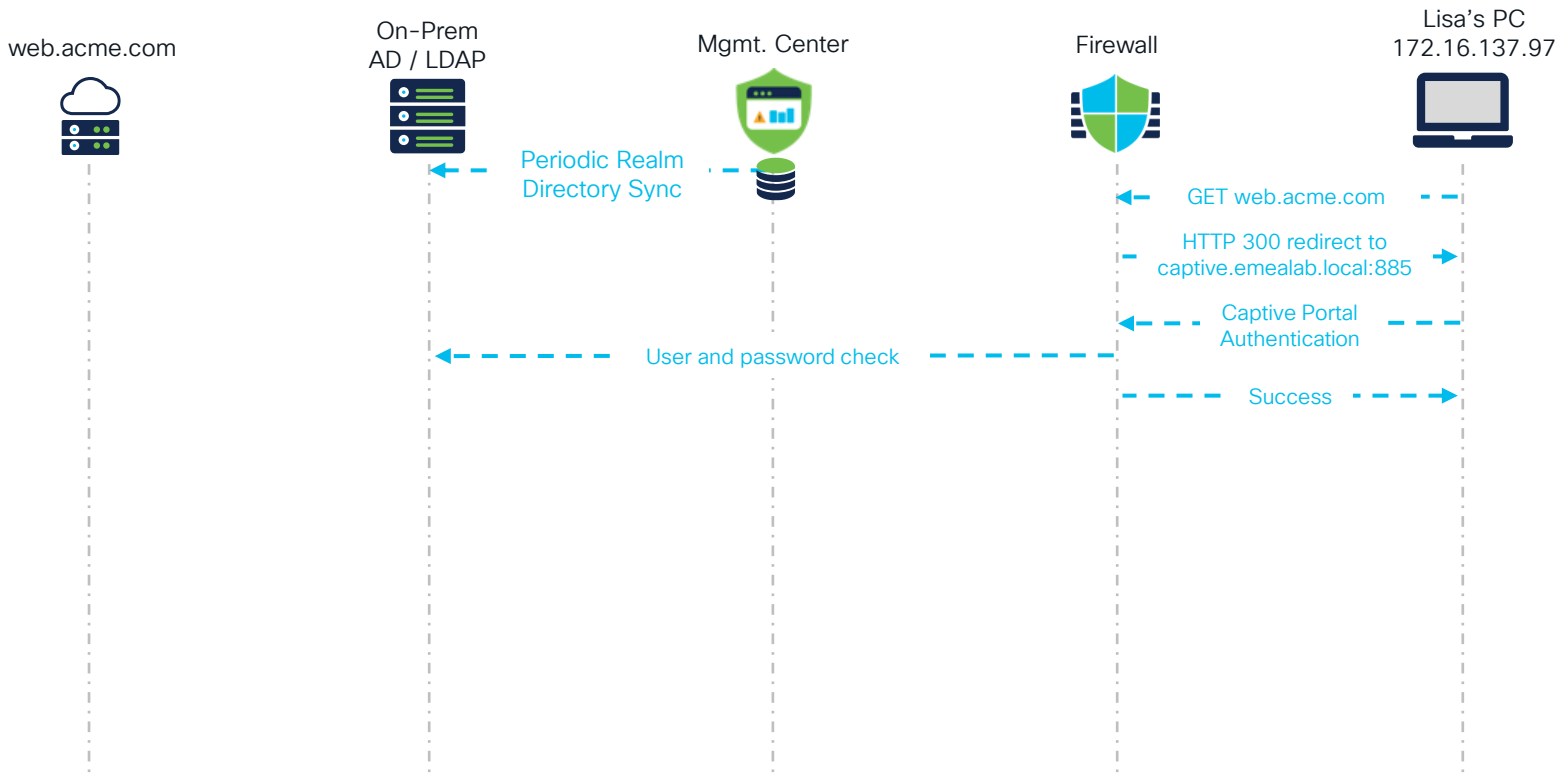
Captive Portal



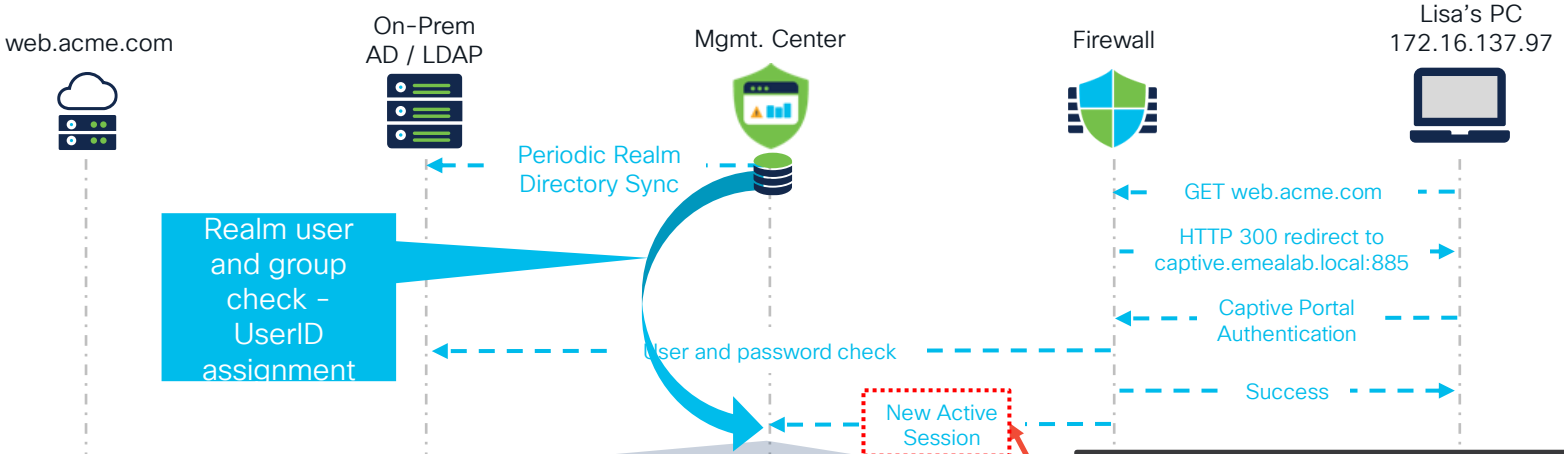
Captive Portal



Captive Portal



Captive Portal

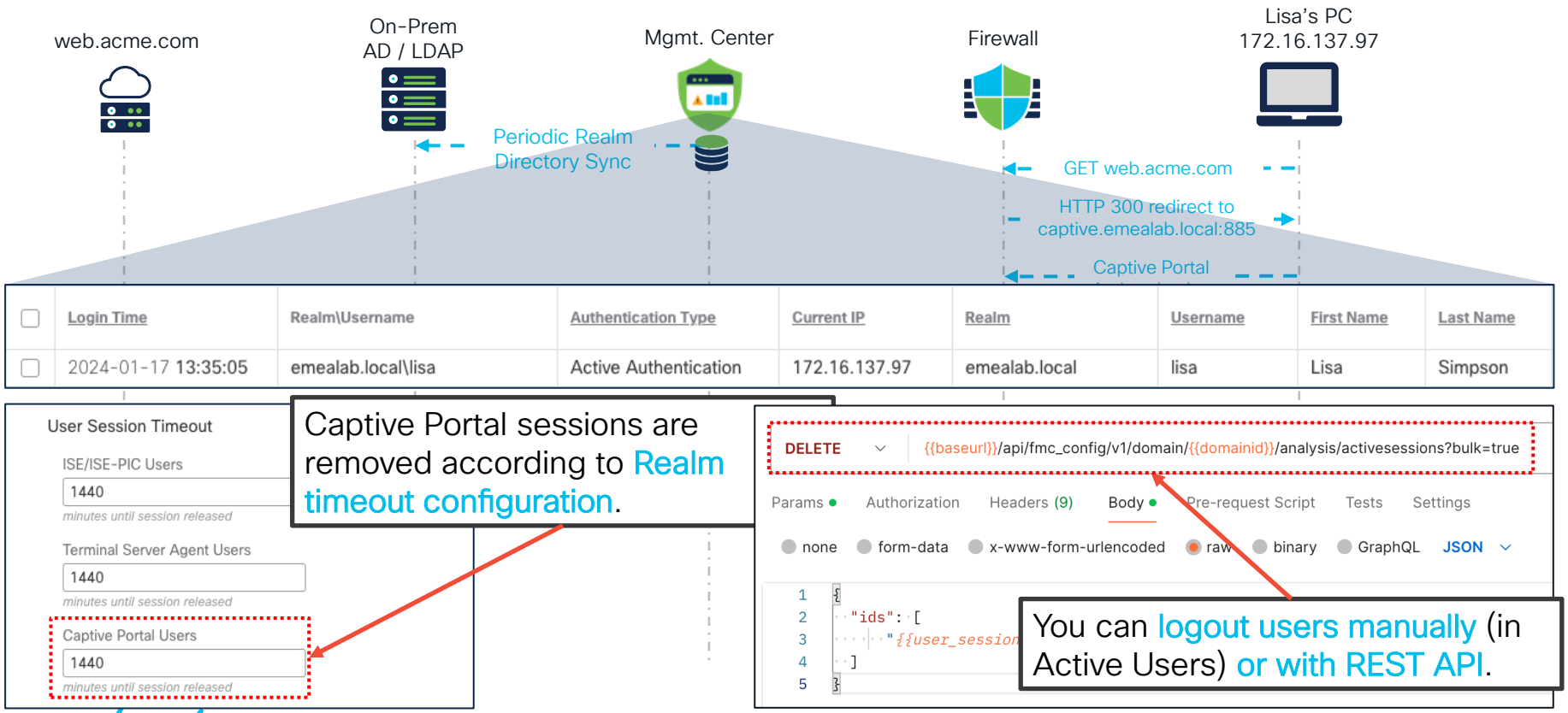



```
admin@fmc:~$ sudo uip_reader -f
/var/sf/user_enforcement/uip_log_entries.1 -p -l
-----------------------------------
Entry no: 322
   SubscriberSession:
     Operation: SESSION_ADD
     Type: IDENTITY_ACTIVE
     Username: lisa
     User ID: 3
     Realm ID: 2
     IP Address: ::ffff:172.16.137.97
   Hop Timestamps:
       2024-01-17 12:35:05(+0 sec)
```

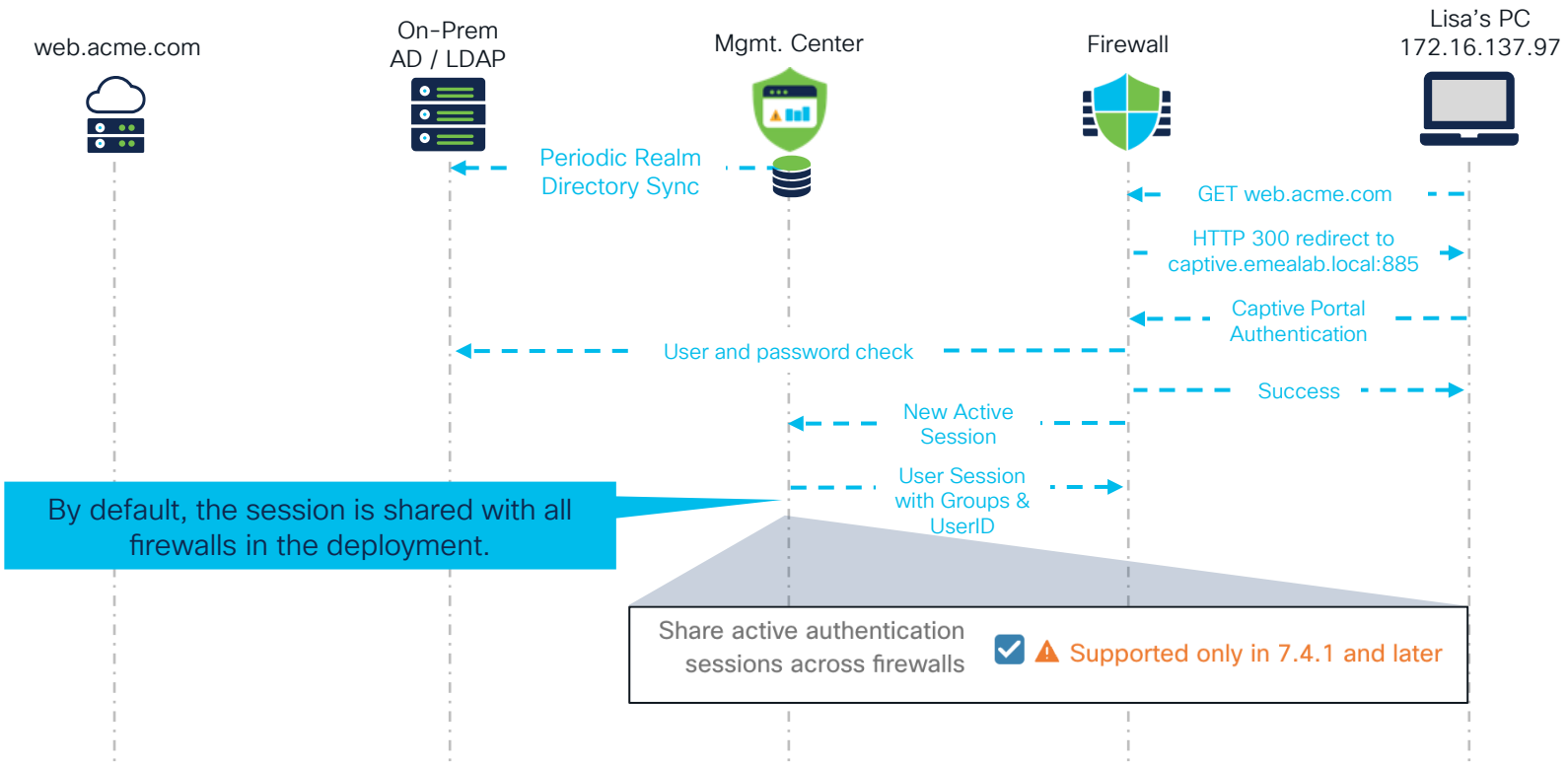
Notice the round-trip to Management Center for Realm cross-check - UserID/group assignment.

This is an Active Authentication type.

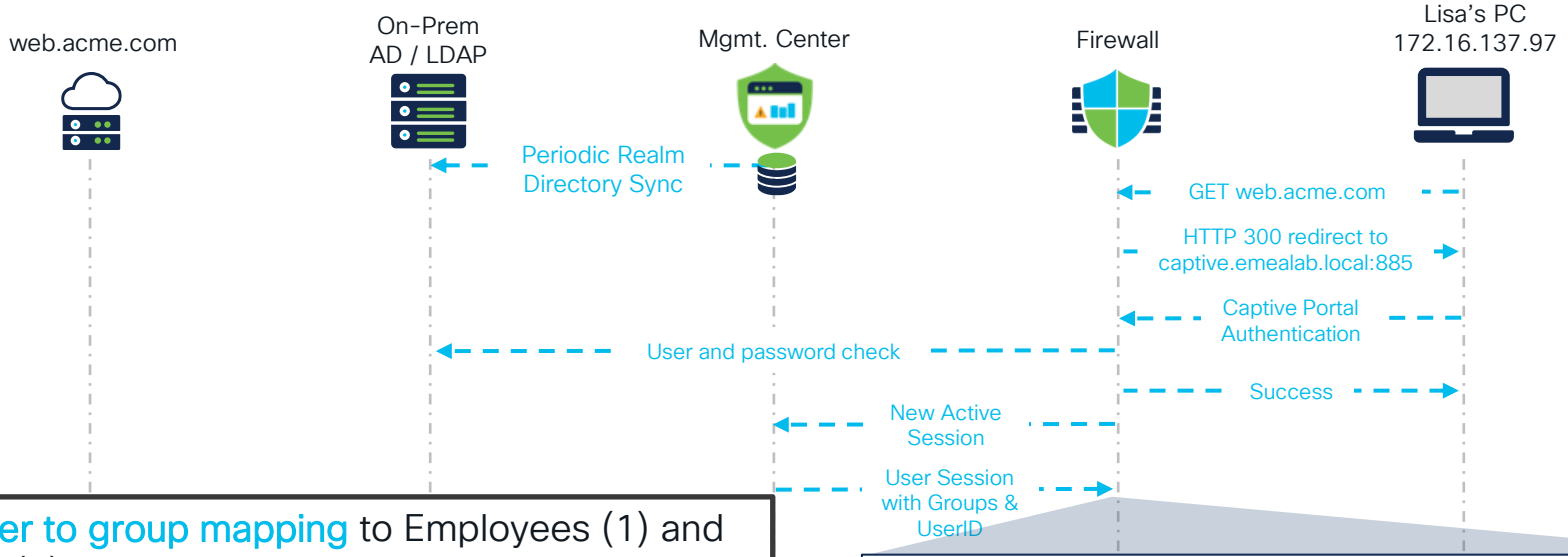
Captive Portal



Captive Portal



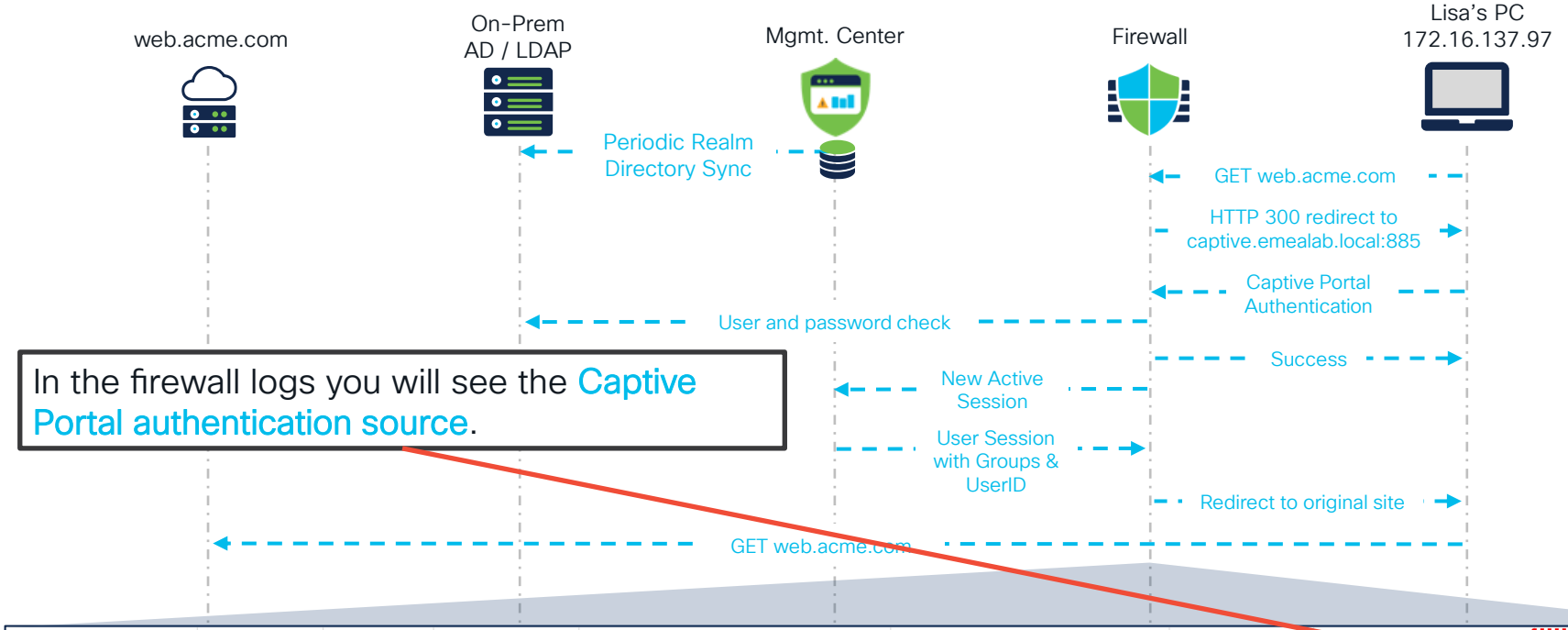
Captive Portal



User to group mapping to Employees (1) and HR (3) had been provided by Management Center upon checking with Realm.

```
----------------
Host ::ffff:172.16.137.97
----------------
::ffff:172.16.137.97:3 realm 2 type 2, username lisa

-------------------
USER:GROUPS
-------------------
3:3,1, (active_sessions: 1)
```

Captive Portal



In the firewall logs you will see the Captive Portal authentication source.

Time	Event Type	Action	Source IP	Source User	Access Control Rule	Destination IP	Destination Port/ICMP Code	Authentication Source
2024-01-17 **13:35:08**	Connection	Allow	172.16.137.97	lisa simpson (emealab.local\lisa, LDAP)	Permit Users	213.19.162.90	**443** (https) / tcp	Captive Portal

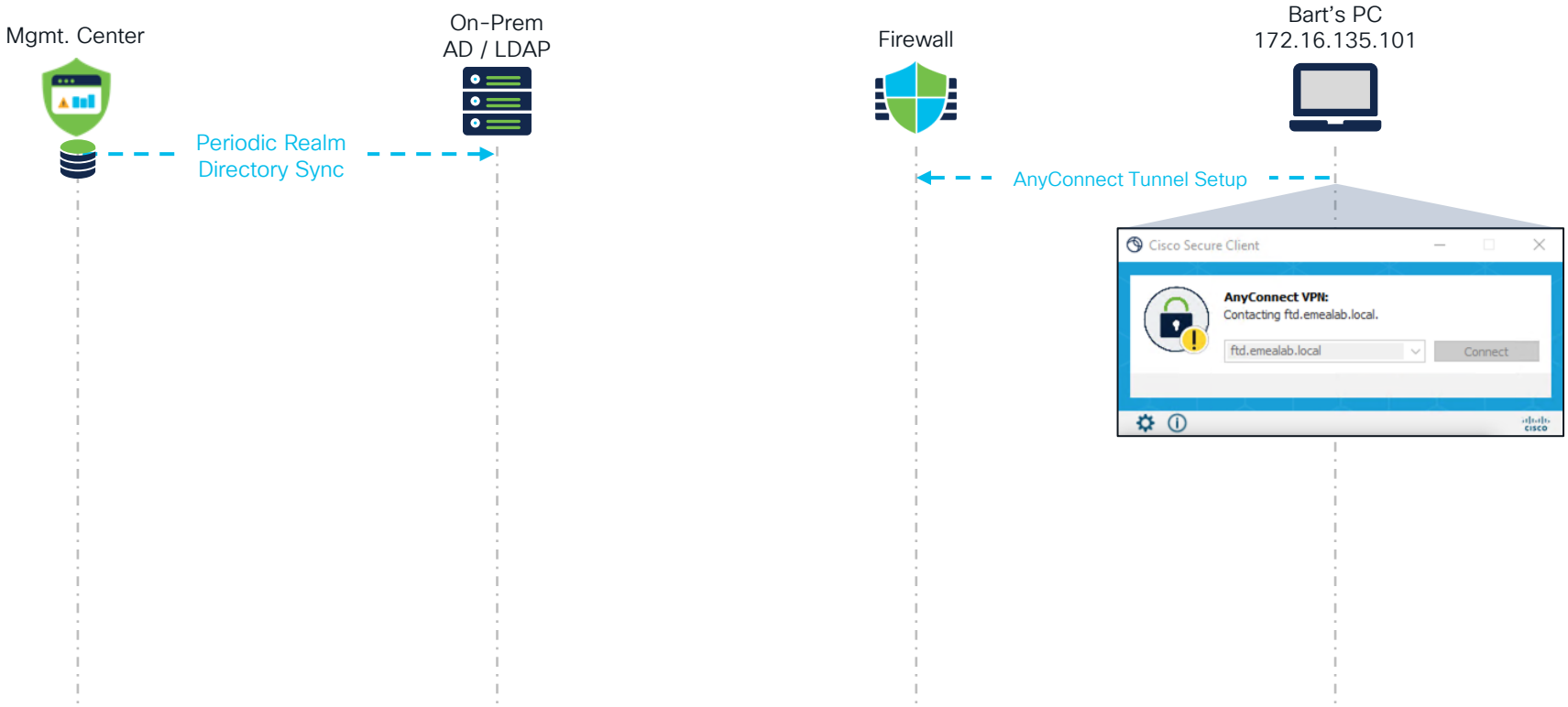
Key Takeaways

- Redirect of HTTPs traffic to Captive Portal requires TLS decryption on the firewall
- A user needs to reach out to a server behind the firewall to get redirected to Captive Portal (you can't authenticate directly to a firewall's interface)
- Ensure Captive Portal certificates are trusted by your clients.
- Set correct DNS entries for Captive Portal's URL – especially with multi-branch deployment.

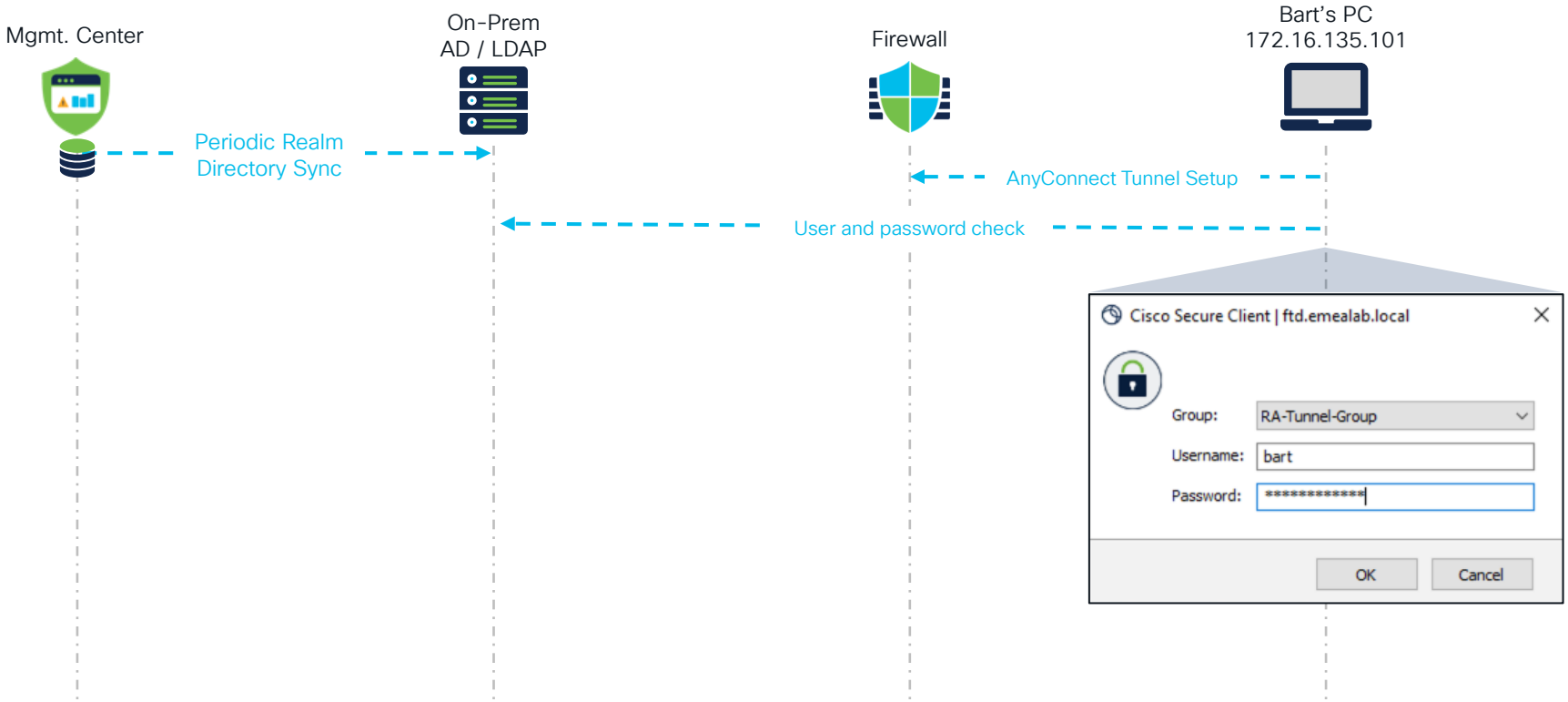
ACTIVE AUTHENTICATION

Remote Access VPN

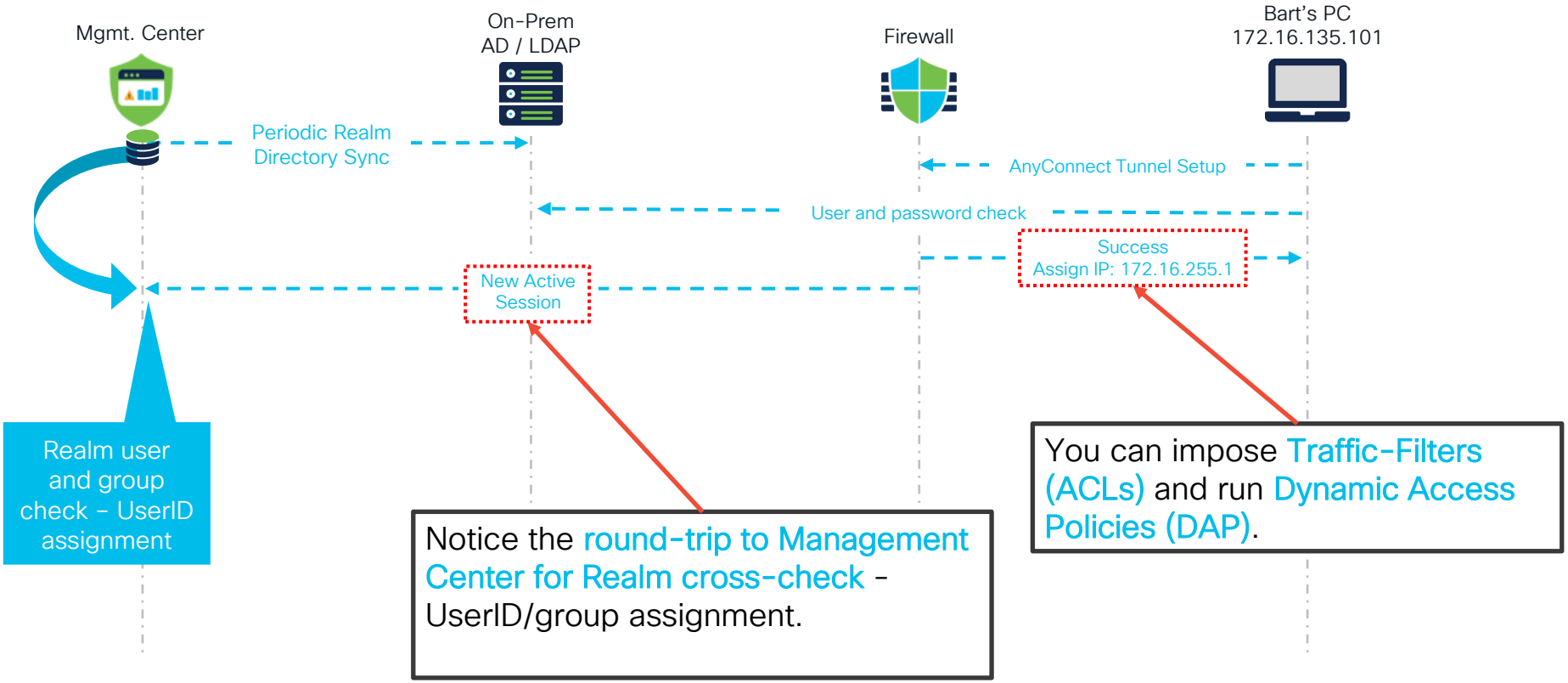
Remote Access



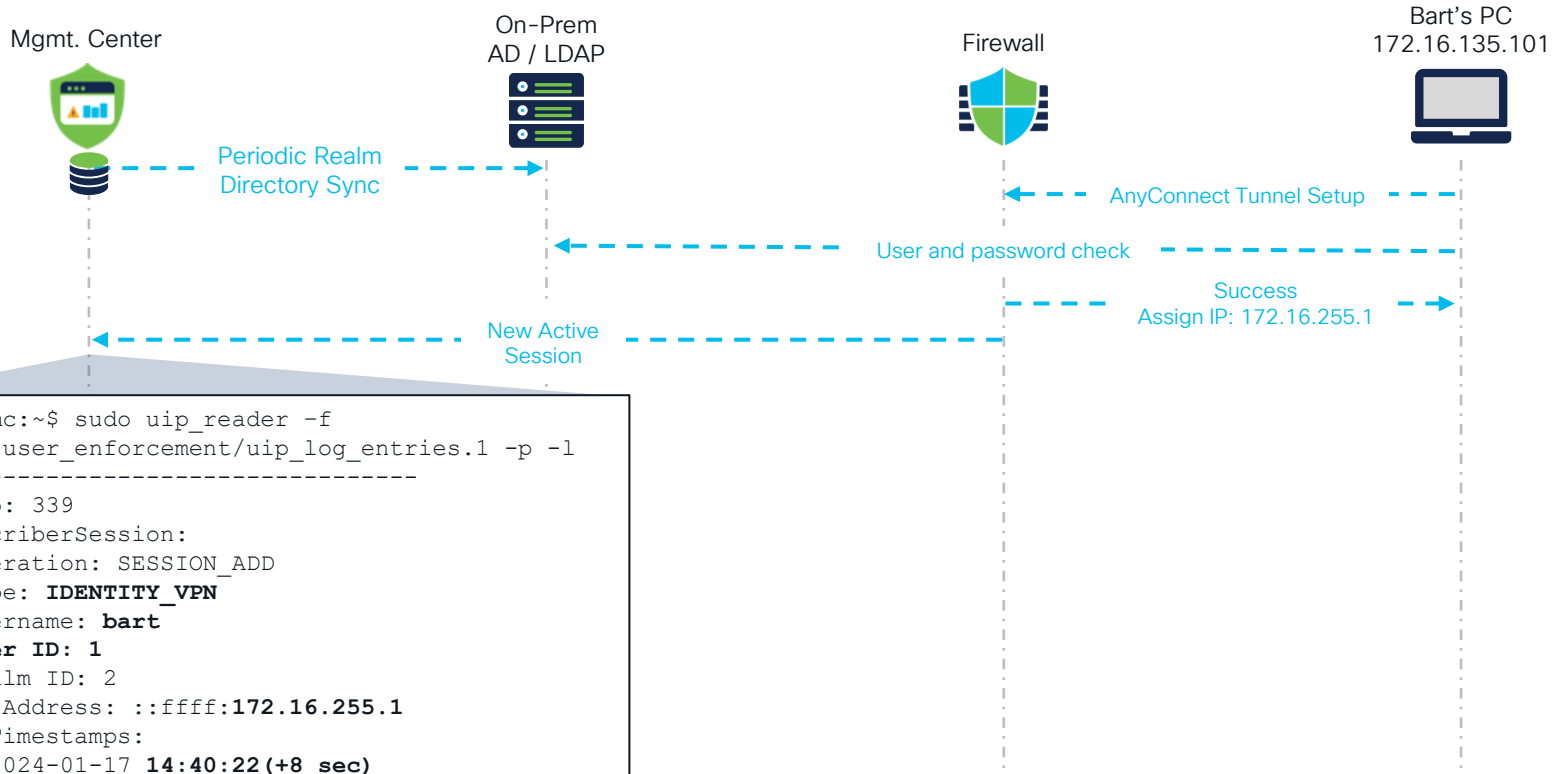
Remote Access



Remote Access

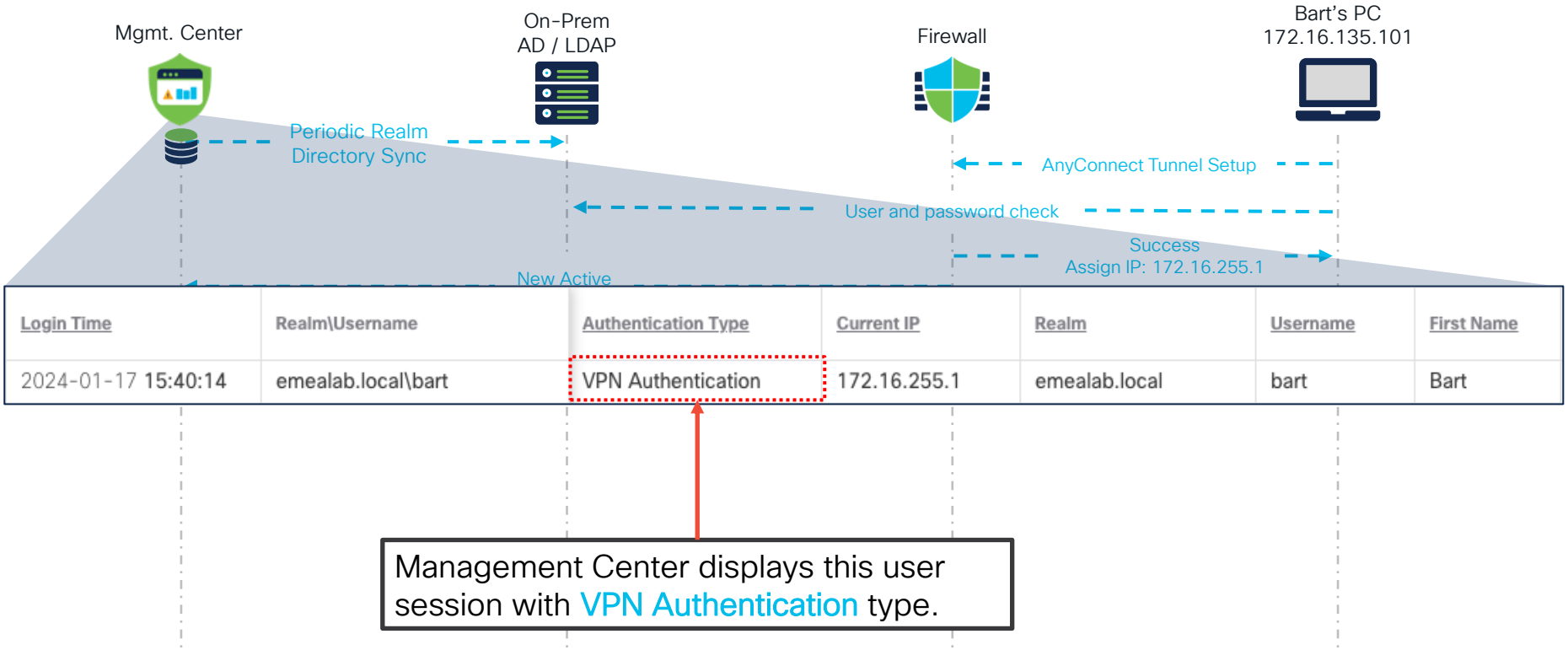


Remote Access




```
admin@fmc:~$ sudo uip_reader -f
/var/sf/user_enforcement/uip_log_entries.1 -p -l
-------------------------------------
Entry no: 339
   SubscriberSession:
     Operation: SESSION_ADD
     Type: IDENTITY_VPN
     Username: bart
     User ID: 1
     Realm ID: 2
     IP Address: ::ffff:172.16.255.1
   Hop Timestamps:
       2024-01-17 14:40:22(+8 sec)
-------------------------------------
```

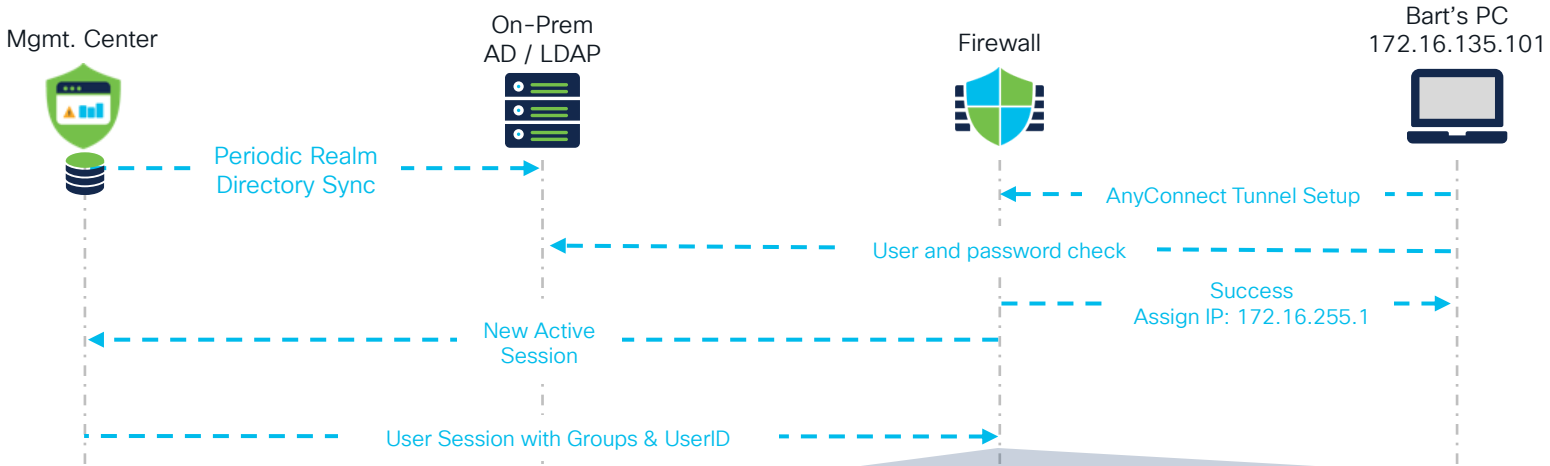
Remote Access



Login Time	Realm\Username	Authentication Type	Current IP	Realm	Username	First Name
2024-01-17 15:40:14	emealab.local\bart	VPN Authentication	172.16.255.1	emealab.local	bart	Bart

Management Center displays this user session with VPN Authentication type.

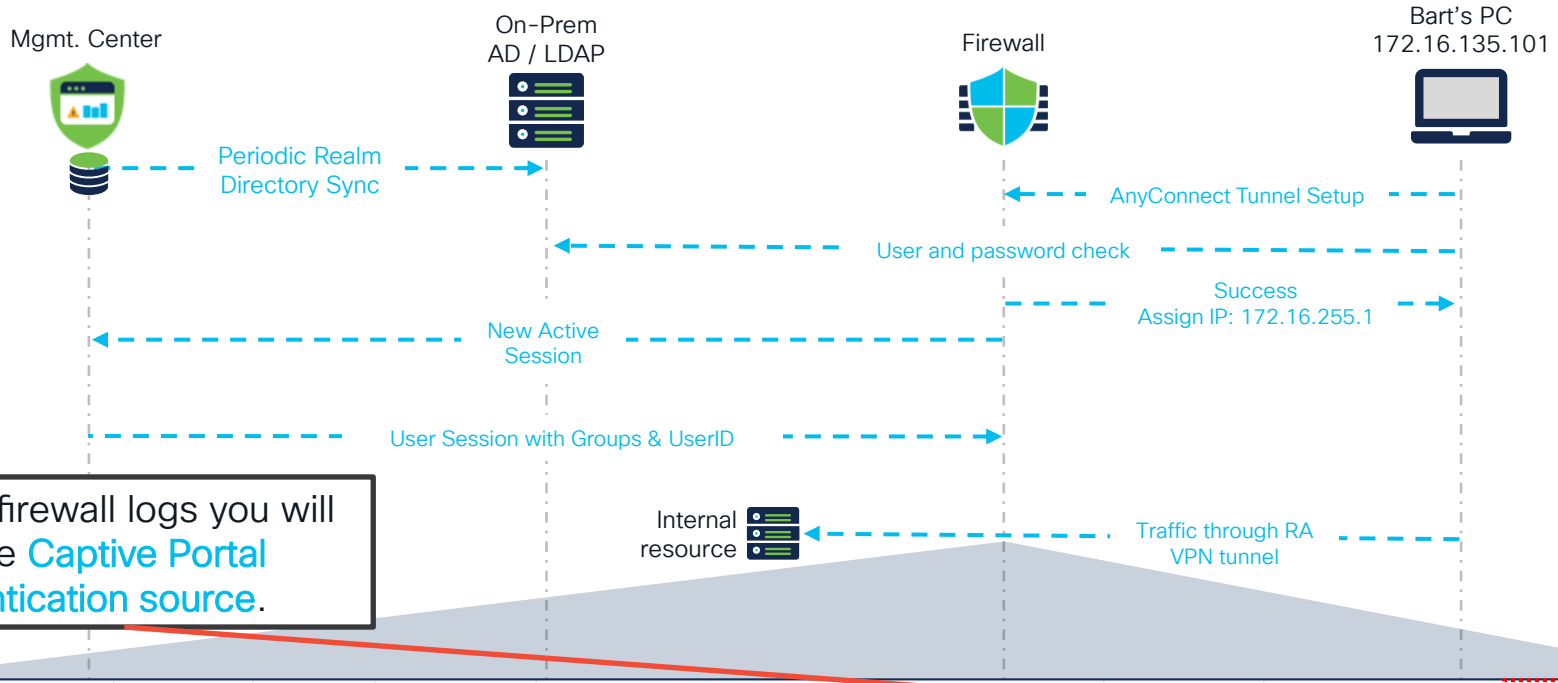
Remote Access



User to group mapping to Employees (1) and Management (5) had been provided by Management Center upon checking with Realm.

```
> system support firewall-engine-dump-user-identity-data
  expert
  sudo cat /ngfw/var/sf/user_enforcement/user_identity.dump

--------------
st ::ffff:172.16.255.1
--------------
ffff:172.16.255.1:1 realm 2 type 5, username bart

-------------------
USER:GROUPS
-------------------
1:5,1, (active_sessions: 1)
```

Remote Access



In the firewall logs you will see the Captive Portal authentication source.

	Time	Event Type	Action	Source IP	Source User	Access Control Rule	Destination IP	Destination Port / ICMP Code	Authentication Source
>	2024-01-17 **15:42:15**	Connection	Allow	172.16.255.1	bart simpson (emealab.local\bart, LDAP)	Permit Any Log	172.16.137.97	**0** (No Code) / icmp	RA-VPN

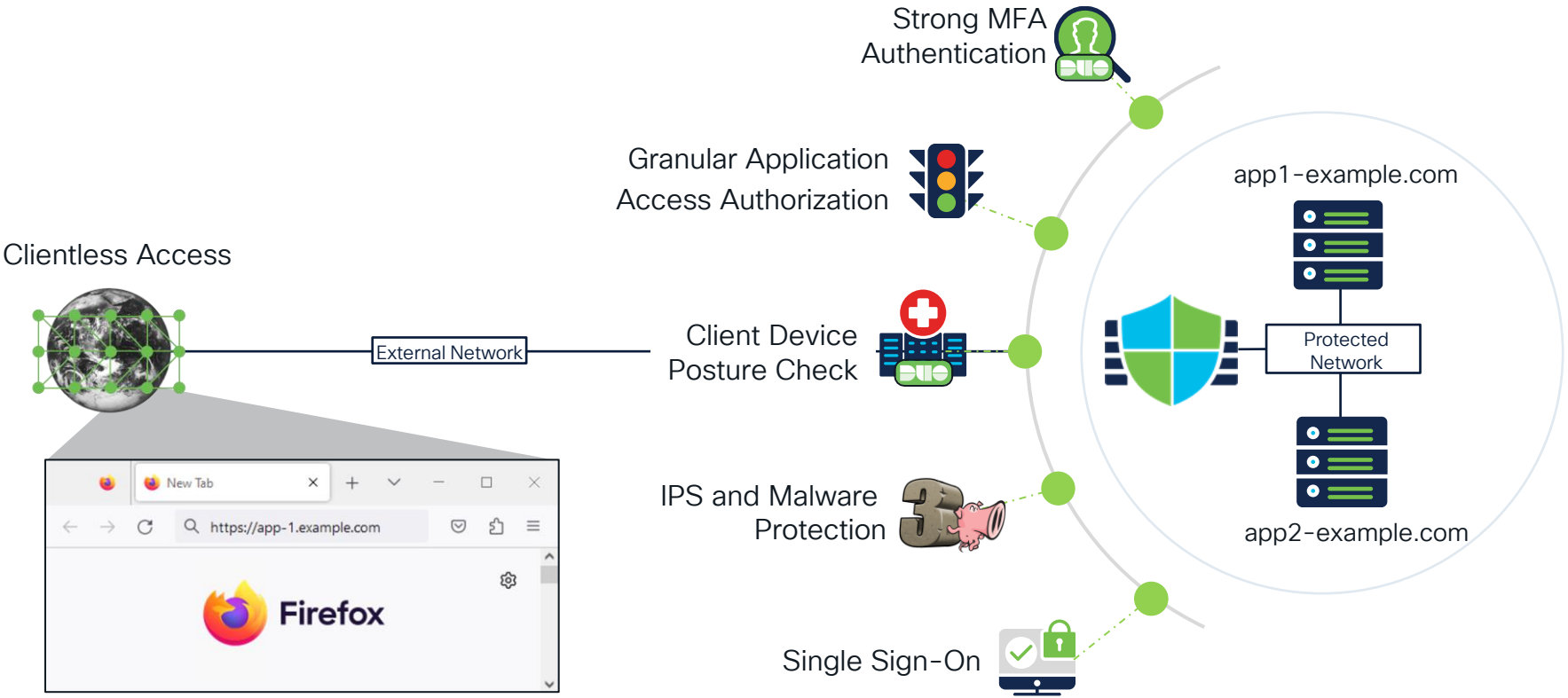
Remote Access Remarks

- Realm consideration for RA VPN authentication methods:
  - **RADIUS** – associate AD/LDAP realm in AAA server setup
  - **SAML** – on-prem AD/LDAP realm must match SAML user domain
  - **Certificate** – username extracted from the certificate must include a domain indication e.g use UPN username@domain maching on-prem AD/LDAP
  - **Local Realm** – firewall identity enforcement policy is not supported

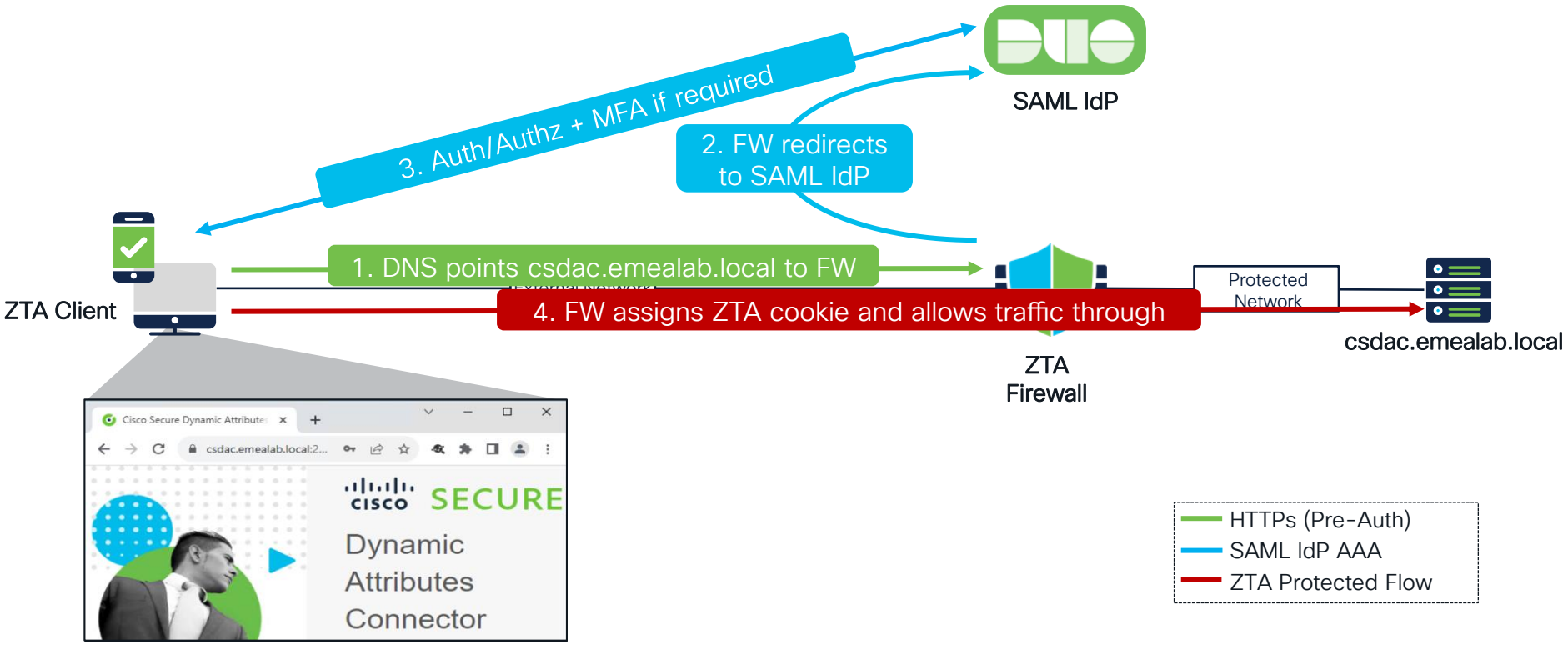
- For the first-time user connection to a firewall, a round-trip to FMC is required for Realm cross-ceck UserID/group mapping.

Zero Trust Access (Clientless)

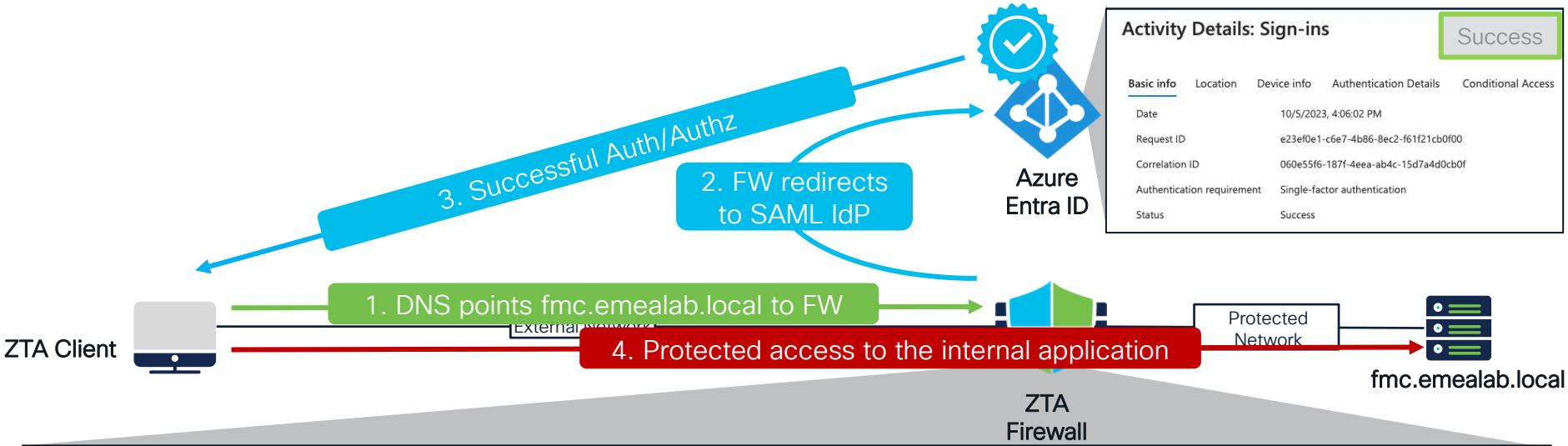
Zero Trust Access (ZTA) - Overview



Zero Trust Access – Basic Flow



Zero Trust Access – Successful Auth/Authz



Firewall Management Center
Analysis / Unified Events

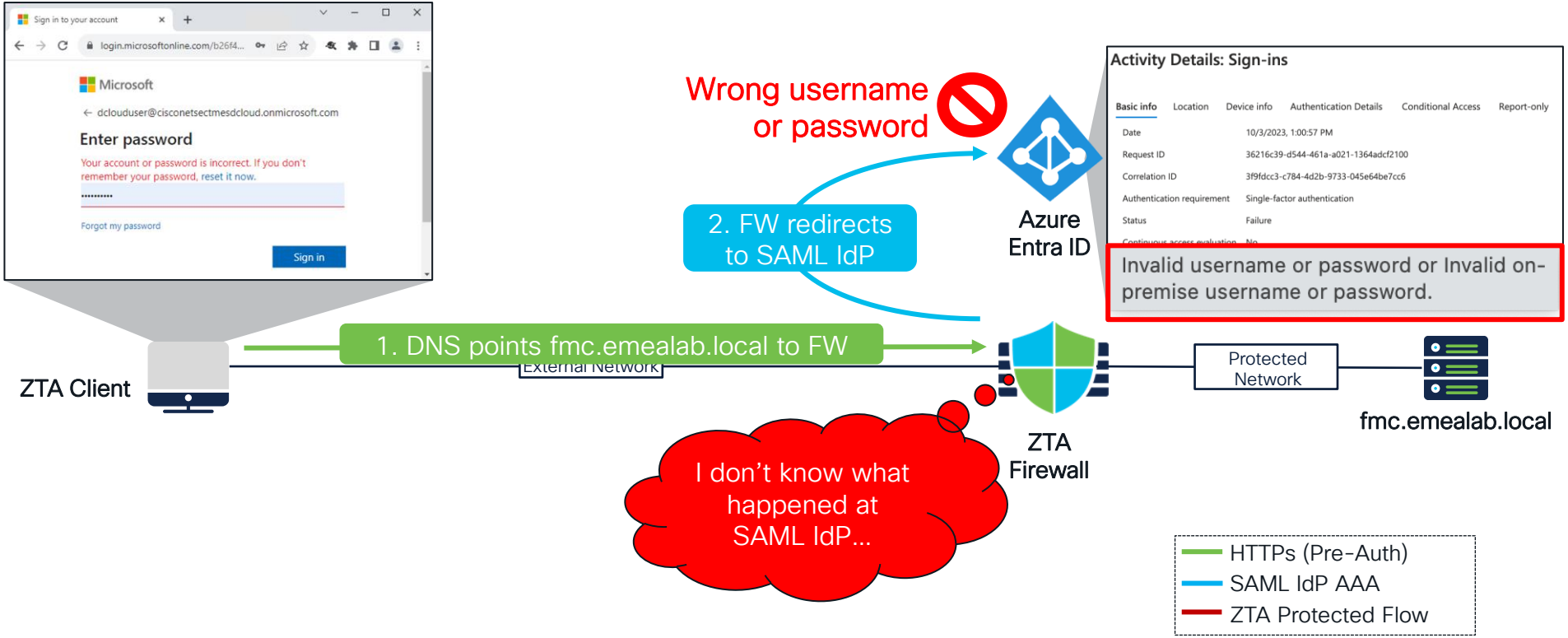
Overview | Analysis | Policies | Devices | Objects | Integration | Deploy | admin | SECURE

Zero Trust Application IN/A | Refresh

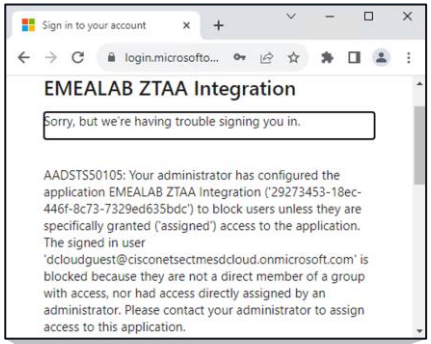
Showing all 4 events (4) | Last 30 minutes | Go Live

Time	Event Type	Action	Source IP	Destination IP	Destination Port / ICMP Code	Zero Trust Application	Zero Trust Application Group	Zero Trust Application Policy	Source User
2023-10-06 13:31:48	Connection	Allow	172.16.135.101	172.16.134.97	443 (https) / tcp	ZTAA_FMC_GUI_Access	EMEALAB-ZTAA-Group	ZTAA_EMEALAB_Policy	dclouduser@cisconetsectmesdcloud.onmicrosoft.com
2023-10-06 13:26:20	Connection	Allow	172.16.135.101	172.16.134.97	443 (https) / tcp	ZTAA_FMC_GUI_Access	EMEALAB-ZTAA-Group	ZTAA_EMEALAB_Policy	dclouduser@cisconetsectmesdcloud.onmicrosoft.com
2023-10-06 13:21:37	Connection	Allow	172.16.135.101	172.16.134.97	443 (https) / tcp	ZTAA_FMC_GUI_Access	EMEALAB-ZTAA-Group	ZTAA_EMEALAB_Policy	dclouduser@cisconetsectmesdcloud.onmicrosoft.com
2023-10-06 13:16:29	Connection	Allow	172.16.135.101	172.16.134.97	443 (https) / tcp	ZTAA_FMC_GUI_Access	EMEALAB-ZTAA-Group	ZTAA_EMEALAB_Policy	dclouduser@cisconetsectmesdcloud.onmicrosoft.com

Zero Trust Access – Failed Authentication

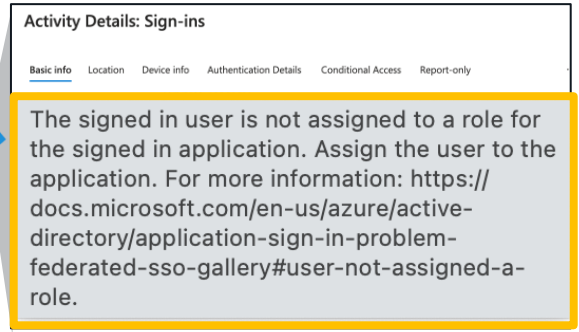


Zero Trust Access – Failed Authorization



User not granted access to the application

Azure Entra ID



2. FW redirects to SAML IdP

1. DNS points fmc.emealab.local to FW

ZTA Client

External Network

ZTA Firewall

Protected Network

fmc.emealab.local

I don't know what happened at SAML IdP...

HTTPs (Pre-Auth)
SAML IdP AAA
ZTA Protected Flow

Zero Trust Access - Recommendations

- Only SAML IdPs are supported e.g. Azure AD, Duo, Ping ID, One Login, Okta
- DNS needs to be configured to attract application traffic to the ZTA firewall's interface.
- ZTA application protection supported for Internet and internal access use-case (with proper DNS configuration)
- ZTA is supported on routed mode in HA/Cluster*/Multi-Instance deployments
- License requirements:
  - Essentials license for basic ZTA access
  - IPS and/or Malware Defense for application traffic inspection
  - ZTA does not work in evaluation mode
- ZTA traffic is not subjected to Access Control Policy (ZTA policy takes precedence)

* - not supported on individual mode cluster

Zero Trust Access - Recommendations

- Supports HTTPs applications only (HTTP, RDP, SSH not supported)
- ZTA supports interactive web applications (requires user SAML login)
- ZTA is not a reverse-proxy:
  - Firewall does not rewrite HTTP requests
  - The flow is based on HTTP redirects
  - TLS decryption is mandatory – Snort validates ZTA HTTP cookie in the HTTP request
- ZTA will not work for non-HTTP traffic tunneled through TCP 443 interface.
- ZTA preserves original client IP address – ensure symmetric traffic between client and application through the firewall (superseded by Source-NAT in 7.4.1)
- A pre-auth certificate matching FQDNs of protected applications is required
- Not supported if protected application redirects between ports or does strict HTTP Host Header validation

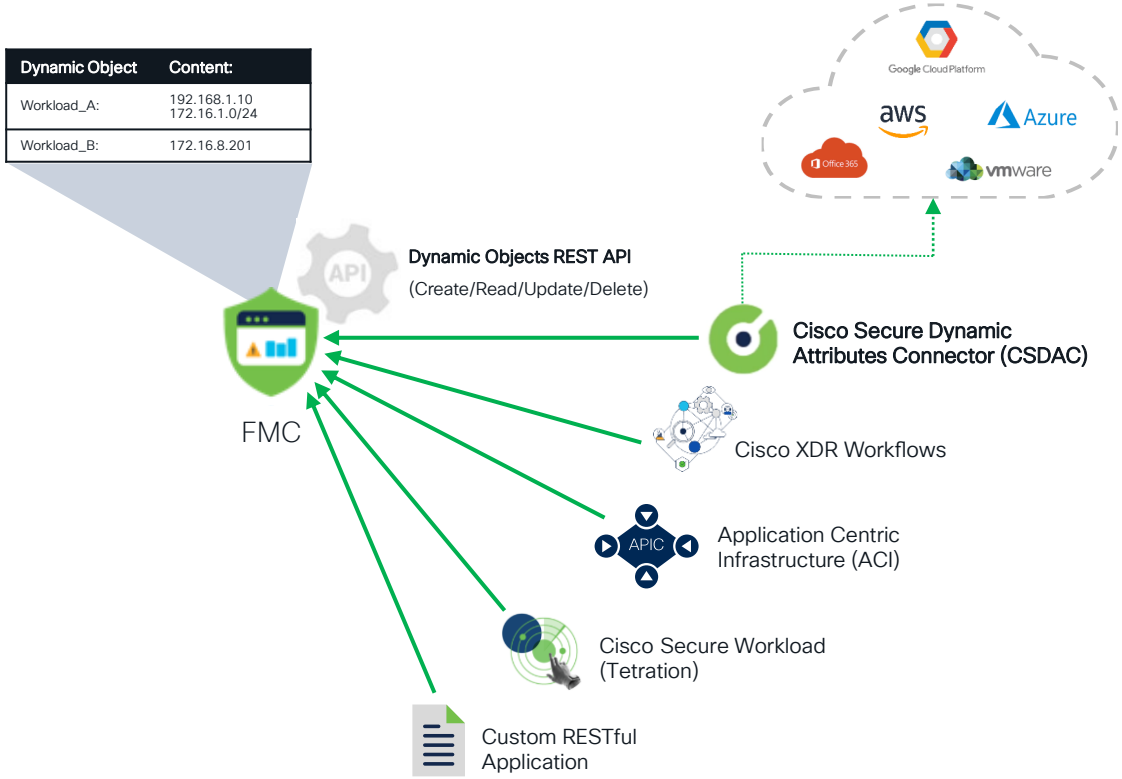
Zero Trust Access Demo

Key Takeaways

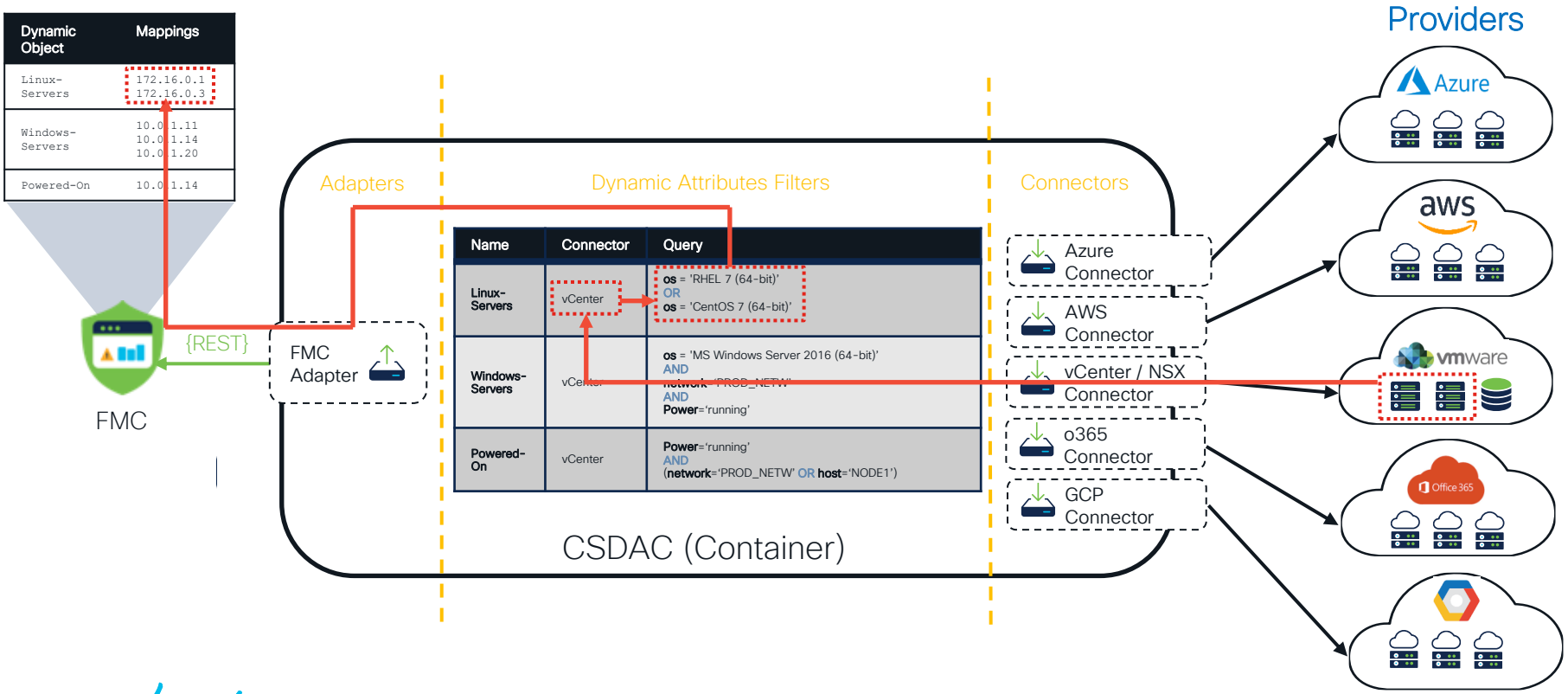
- Browser based application access (no agent)
- Reduce attack surface by enforcing per-application security controls
- Leverage SAML SSO for applications with common IdP
- ZTA traffic is not subjected to Access Control Policy

Server Identity

Dynamic Objects



Architecture of the Dynamic Attributes Connector



Dynamic Objects in Action

Cisco Secure Dynamic Attributes Connector

REST API
(Add 10.0.0.5 to Workload_A)

FMC

SFtunnel Update

(Without policy deployment)

Managed Firewall

```
----------------
Host ::ffff:10.0.0.4
----------------
ABP values:  1

----------------
Host ::ffff:10.0.0.5
----------------
ABP values:  1

-------------------
ABP NAME-TO-ID MAPPING:
-------------------
Workload_A   1
```

#	Name	Source Networks	Dest Networks	Dest Ports	Source Dynamic Attributes	Destination Dynamic Attributes	Action
Mandatory - Secure Policy (1-1)							
1	Worklaod A	Any	Any	HTTPS	Any	Workload_A	Allow

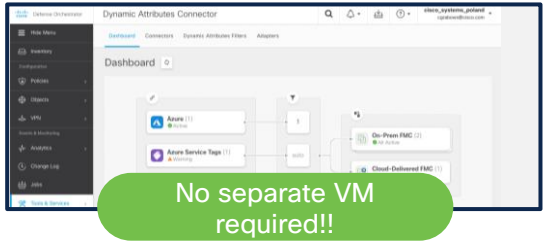
Dynamic Object	Content:
Workload_A:	10.0.0.4 10.0.0.5

Workload A

Dynamic Feed Update

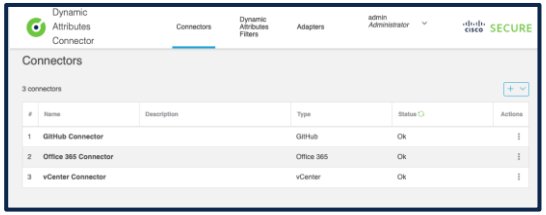
CSDAC Form Factors

CSDAC in CDO's Tools & Services



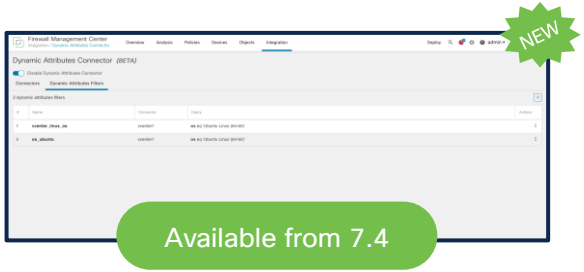
Cloud Delivered

CSDAC (Linux Machine)



Standalone

CSDAC in FMC



Built In

Supported Connectors

Cloud Connectors

- Azure
- Azure Service Tags
- vCenter/ NSX-T
- Google Cloud
- AWS

Public Feeds Connectors

- Office365
- GitHub
- Webex
- Zoom
- Generic TXT

Attribute Based Policy – CSDAC Attributes

#	Name	Source Zones	Dest Zones	Users	Applications	Dest Ports	Source Dynamic Attributes	Destination Dynamic Attributes	Action
> Mandatory - Attribute-Based Policy (-)									
⌄ Default - Attribute-Based Policy (1-9)									
1	Workload_1	Any	Any	Any	Any	HTTPS	WorkloadObj_615c486dc9	WorkloadObj_615c8066483	Allow
2	IoT Support Service	External	IoT_VN	Any	Any	HTTPS SSH	IoT_Support	IoT	Allow
3	Machine Authentication	Corporate_VN	Shared_Services	Any	Any	AD_Services	Machine_Auth	VMWare_Active_Directory	Allow
4	Printing Service	Corporate_VN	Data_Center_Edge	Any	Any	SNMP -PING ler_Service	RICOH-Aficio-SP-C410DN RICOH-Aficio-SP-C820DN Xerox-WorkCentre-5030 Xerox-WorkCentre-5135	APIC_A_ESG_Print_Servers	Allow
5	Block Social Media	Corporate_VN	External	Any	Tinder Twitter		Contractors Branch_Locations	Any	Block
6	o365 Access	Corporate_VN	External	lab-local/Domain Users	Any	HTTPS HTTP	Any	o365_Common o365_Exchange o365_SharePoint	Allow
7	SecureX Threat Containment	Corporate_VN	Data_Center_Edge	Any			SecureX_Quarantined_IPs SecureX_Suspicious_IPs	Honeypot_Service	Allow
8	ISE Threat Containment	Corporate_VN	Data_Center_Edge	Any			Quarantined_Systems	Honeypot_Service	Allow
9	Cloud App Access	Corporate_VN	WAN	Any	Any	HTTP HTTPS	Employees	Azure_HR_Workload Azure_Intranet_Service	Allow

vCenter / NSX Dynamic Objects

vmware

o365 Public Feeds

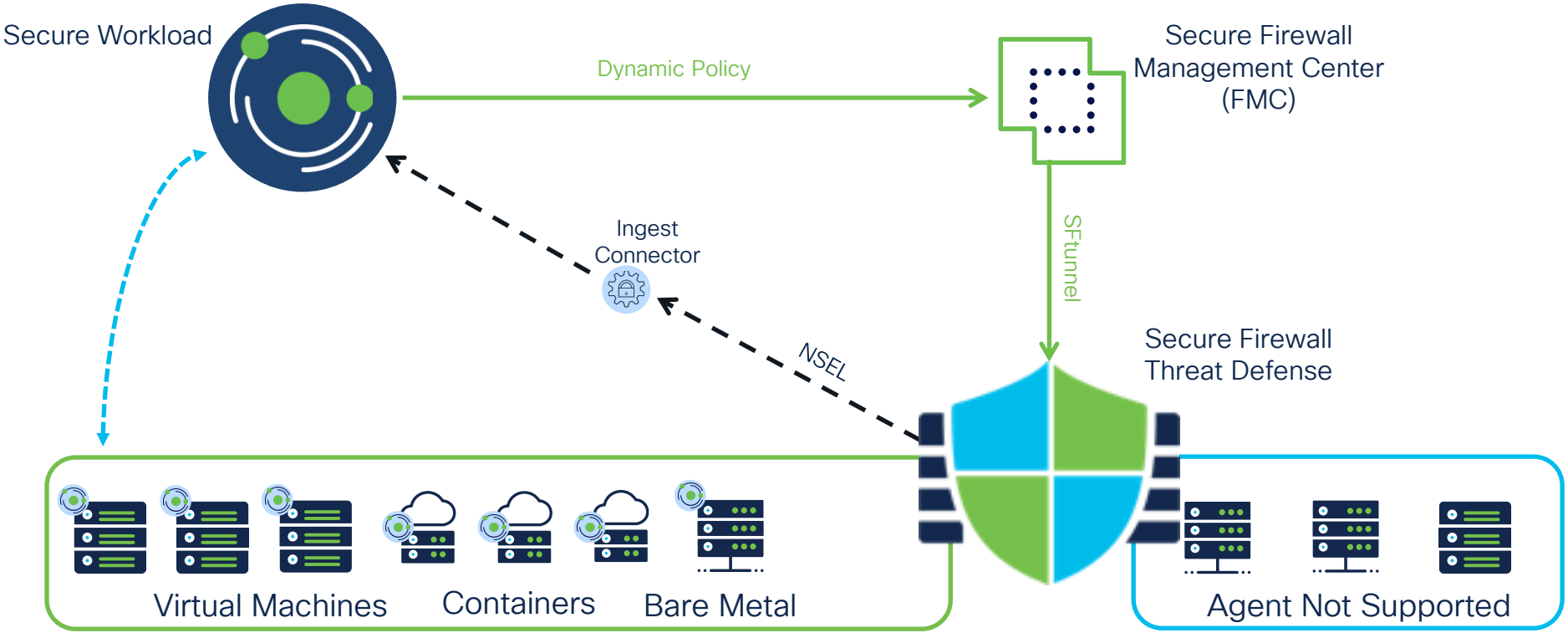
Office 365

Public Cloud Tags

aws Azure

CSDAC Demo

Cisco Secure Workload Dynamic Policy Push



Segmentation policies enforcement
at workloads

Segmentation policies enforcement
at firewall

Accurate and Validated Dynamic Policy

Invoice-App-Firewall PRIMARY

... : DC : DC-1 : Applications : Prod : Invoice-App | Version: v1 | Last Run: Apr 26, 9:59 PM

Switch Application | Start ADM Run

Activity Log | Matching Inventories 8 | Conversations 208 | Filters 4 | Policies 16 | Provided Services | Enforcement Status | Policy Analysis | Enforcement

16 / 16 policy changes selected for enforcement

Filter Policies ...

Absolute No matching changes

Default Added 15 Removed 0

Priority	Action	Consumer	Provider	Protocols and Ports
100	ALLOW	siwapp-front-end-haproxydb	siwapp-db-tier	TCP : 3306 (MySQL)
100	ALLOW	siwapp-front-end-haproxy	siwapp-app-tier	TCP : 8081
100	ALLOW	siwapp-db-tier	Default : EMEAR	UDP : 53 (DNS)
100	ALLOW	siwapp-db-tier	siwapp-db-tier	TCP : 4567
100	ALLOW	siwapp-db-tier	siwapp-front-end-haproxydb	TCP : 32768-60800

Enforced Policy Version: disabled

Enforce Policies

Enforcement is disabled for this application.
Traffic in, out and within this application's scope may still be enforced by policies from other enforced applications.

Select time range
Apr 27 3:34am - Apr 27 9:34am

10/1 1/1 4/1 7/1 10/1 1/1 4/1 7/1 10/1 1/1 4/1 7/1 10/1 1/1 4/1

18,098,412 total observations
Showing Flow Observations

1. Generate an accurate micro-segmentation policy based on NSEL firewall flow events with Application Dependency Mapping.

2. ADM automatically discovers relationships between services and suggests Zero Trust policy.

3. Run What-If policy analysis using real-time or historical data for pre-enfocement validation.

4. Enforce the normalized micro-segmentation on the workloads and the Cisco Secure Firewall protected segments.

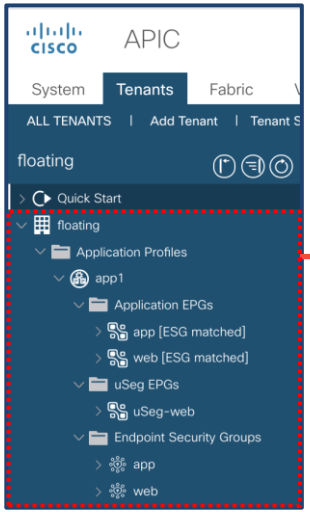
Attribute Based Policy – Cisco Secure Workload Rules and Dynamic Objects

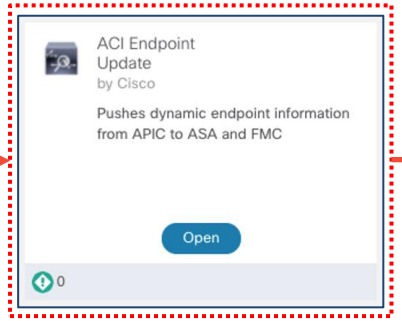
#	Name	Source Zones	Dest Zones	Users	Applications	Dest Ports	Source Dynamic	Destination Dynamic	...tion
> Mandatory - Attribute-Based Policy (-)									
⌄ Default - Attribute-Based Policy (1-9)									
1	Workload_1	Any	Any	Any	Any	HTTP HTTPS	WorkloadObj_615c486dc9	WorkloadObj_615c8066483	Allow
2	IoT Support Service	External	IoT_VN	Any	Any	HTTPS SSH	IoT_Support	IoT	Allow
3	Machine Authentication	Corporate_VN	Shared_Services	Any	Any	AD_Services	Machine_Auth	VMWare_Active_Directory	Allow
4	Printing Service	Corporate_VN	Data_Center_Edge	Any	Any	SNMP ICMP-PING Spooler_Service	RICOH-Aficio-SP-C410DN RICOH-Aficio-SP-C820DN Xerox-WorkCentre-5030 Xerox-WorkCentre-5135	APIC_A_ESG_Print_Servers	Allow
5	Block Social Media	Corporate_VN	External	Any	Facebook Google+ Instagram	Any	Contractors Branch_Locations	Any	Block
6	o365 Access	Corporate_VN	Exte			PS	Any	o365_Common o365_Exchange o365_SharePoint	Allow
7	SecureX Threat Containment	Corporate_VN	Data_Center_Edge	Any	Any	Any	SecureX_Quarantined_IPs SecureX_Suspicious_IPs	Honeypot_Service	Allow
8	ISE Threat Containment	Corporate_VN	Data_Center_Edge	Any	Any	Any	Quarantined_Systems	Honeypot_Service	Allow
9	Cloud App Access	Corporate_VN	WAN	Any	Any	HTTP HTTPS	Employees	Azure_HR_Workload Azure_Intranet_Service	Allow

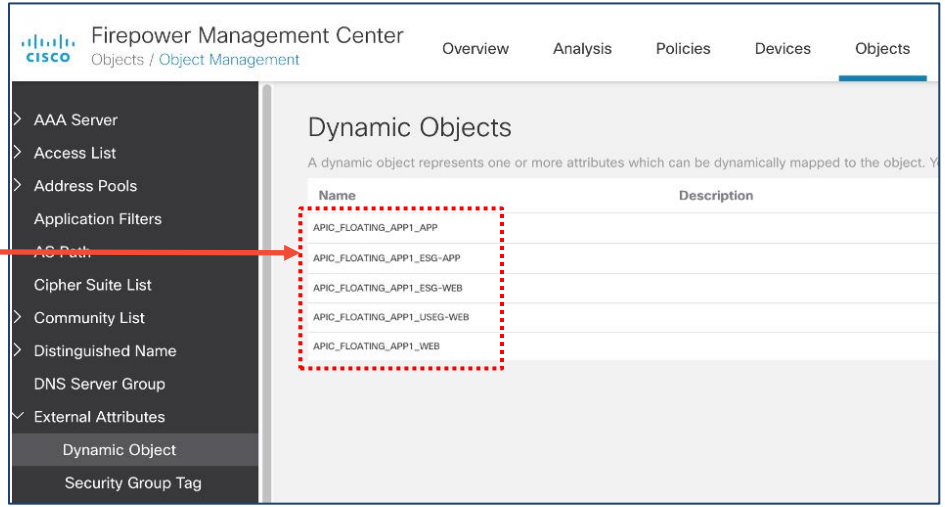
Cisco Secure Workload pushed Dynamic Objects

Cisco Secure Workload deployed Access Control Policy Rule

ACI Endpoint Update App 2.x







ACI Endpoint Update App is Compatible with FMC 6.7 and above:

- With FP 7.0+, use Dynamic Objects – no Deployment Needed
- With FP 6.7, use Network Group Objects – Deployment Required

Attribute Based Policy – ACI EPG and ESG

#	Name	Source Zones	Dest Zones	Users	Applications	Dest Ports	Source Dynamic Attributes	Destination Dynamic Attributes	Action
> Mandatory - Attribute-Based Policy (-)									
⌄ Default - Attribute-Based Policy (1-9)									
1	Workload_1	Any	Any	Any	Any	HTTP HTTPS	WorkloadObj_615c486dc9	WorkloadObj_615c8066483	Allow
2	IoT Support Service	External	IoT_VN	Any	Any	HTTPS SSH	IoT_Support	IoT	Allow
3	Machine Authentication	Corporate_VN	Shared_Services	Any	Any	AD_Services	Machine_Auth	VMWare_Active_Directory	Allow
4	Printing Service	Corporate_VN	Data_Center_Edge	Any	Any	SNMP ICMP-PING Spooler_Service	RICOH-Aficio-SP-C410DN RICOH-Aficio-SP-C820DN Xerox-WorkCentre-5030 Xerox-WorkCentre-5135	APIC_A_ESG_Print_Servers	Allow
5	Block Social Media	Corporate_VN	External	Any	Facebook Google+ Instagram Tinder Twitter	Any	Contractors Branch_Locations	Any	Block
6	o365 Access	Corporate_VN	External	lab-local/Domain Users	Any	HTTPS HTTP	Any	o365_common o365_exchange	Allow
7	SecureX Threat Containment	Corporate_VN	Data_Center_Edge	Any	Any	Any	[illegible]	[illegible]	[illegible]
8	ISE Threat Containment	Corporate_VN	Data_Center_Edge	Any	Any	Any	Quarantined_Systems	Honeypot_Service	Allow
9	Cloud App Access	Corporate_VN	WAN	Any	Any	HTTP HTTPS	Employees	Azure_HR_Workload Azure_Intranet_Service	Allow

ACI Endpoint Groups (EPG) and Endpoint Security Group (ESG)

Dynamic Objects REST API is Straight Forward

Connect to your FMC at ”https://<FMC IP>/api/api-explorer” to browse the REST API documentations

GET	/api/fmc_platform/v1/domain/{domainUUID}/object/**dynamicobjects**	Retrieves the list of all Dynamic Objects or creates a new Dynamic Object.
POST	/api/fmc_platform/v1/domain/{domainUUID}/object/**dynamicobjects**	
GET	/api/fmc_platform/v1/domain/{domainUUID}/object/**dynamicobjects/{objectIdOrName}**	Retrieves, deletes or modifies an existing Dynamic Object with the specified ID.
PUT	/api/fmc_platform/v1/domain/{domainUUID}/object/**dynamicobjects/{objectIdOrName}**	
DELETE	/api/fmc_platform/v1/domain/{domainUUID}/object/**dynamicobjects/{objectIdOrName}**	
GET	/api/fmc_platform/v1/domain/{domainUUID}/object/**dynamicobjects/{objectIdOrName}/mappings**	Retrieves, adds or removes IP addresses mapped to an existing Dynamic Object with the specified ID.
PUT	/api/fmc_platform/v1/domain/{domainUUID}/object/**dynamicobjects/{objectIdOrName}/mappings**	
POST	/api/fmc_platform/v1/domain/{domainUUID}/object/**dynamicobjectmappings**	Adds or removes IP addresses mapped to existing Dynamic Objects in bulk.

Configure Dynamic Objects with the REST API

Environment Variables:

X-auth-access-token =
c830333c-614e-44a7-b6ca-dca7b8be605d

Domain UUID =
e276abec-e0f2-11e3-8169-6d9ed49b625f

Workload_A Object ID =
005056AF-6E04-0ed3-0000-021474843199

POST /api/fmc_platform/v1/auth/**generatetoken**

HEADER Authorization : Basic cnWzdFAcdDovcW86RFfTMU==

Status: 204

HEADER X-auth-access-token : c8303…605d
Domain_UUID : e276abec…b625f

POST /api/fmc_platform/v1/domain/e276abec…b625f/object/**dynamicobjects**

HEADER X-auth-access-token : c830333c-614e-44a7-b6ca-dca7b8be605d

BODY {
"name": "Workload_A",
"type": "DynamicObject",
"objectType": "IP"
}

Status: 201

BODY
[…]
"id": "005056AF…199",
"name": "Workload_A",
"type": "DynamicObject",
[…]

POST /api/fmc_platform/v1/domain/e276abec…b625f/object/**dynamicobjectmappings**

HEADER X-auth-access-token : c830333c-614e-44a7-b6ca-dca7b8be605d

BODY {
"add": [
{
"mappings": [
"172.16.11.100"
],
"dynamicObject": {
"id": "005056AF-6E04-0ed3-0000-021474843199"
}
}
]
}

Status: 201

FMC

Dynamic Object	Content:
Workload_A	172.16.11.100

REST Allows You to Design your Own Use-Cases

#	Name	Source Zones	Dest Zones	Users	Applications	Dest Ports	Source Dynamic Attributes	Destination Dynamic Attributes	Action
> Mandatory - Attribute-Based Policy (-)									
⌄ Default - Attribute-Based Policy (1-9)									
1	Workload_1	Any	Any	Any	Any	HTTP HTTPS	WorkloadObj_615c486dc9	WorkloadObj_615c8066483	Allow
2	IoT Support Service	External	IoT_VN	Any	Any	HTTPS SSH	IoT_Support	IoT	Allow
3	Machine Authentication	Corporate_VN	Shared_Services	Any	Any	AD_Services	Machine_Auth	VMWare_Active_Directory	Allow
4	Printing Service	Corporate_VN	Data_Center_Edge	Any	Any	SNMP ICMP-PING Spooler_Service	RICOH-Aficio-SP-C410DN RICOH-Aficio-SP-C820DN Xerox WorkCentre-5030 Xerox WorkCentre-5135	APIC_A_ESG_Print_Servers	Allow
5	Block Social Media	Corporate_VN	External	Any	Facebook Google+ Instagram Tinder Twitter	Any	Contractors	Any	Block
6	o365 Access	Corporate_VN	External	lab-local/Domain Users	Any	HTTP HTTP	Any	o365_Common o365_Exchange o365_SharePoint	Allow
7	SecureX Threat Containment	Corporate_VN	Data_Center_Edge	Any	Any	Any	SecureX_Quarantined_IPs SecureX_Suspicious_IPs	Honeypot_Service	Allow
8	ISE Threat Containment	Corporate_VN	Data_Center_Edge	Any	Any	Any	Quarantined_Systems	Honeypot_Service	Allow
9	Cloud App Access	Corporate_VN	WAN	Any	Any	HTTP HTTPS	Employees	Azure_HR_Workload Azure_Intranet_Service	Allow

REST API pushed
Dynamic Object

Key Takeaways

- FMC syncs dynamic objects to the FTDs without policy deployment
- Dynamic Attributes Connector imports attribute maps from a dynamic environment and translates into firewall dynamic objects
- Dynamic Objects REST API opens doors for various integrations – ACI, XDR, Secure Workload, REST API, public-feeds, and more to come!

Join at

slido.com

#2901 029

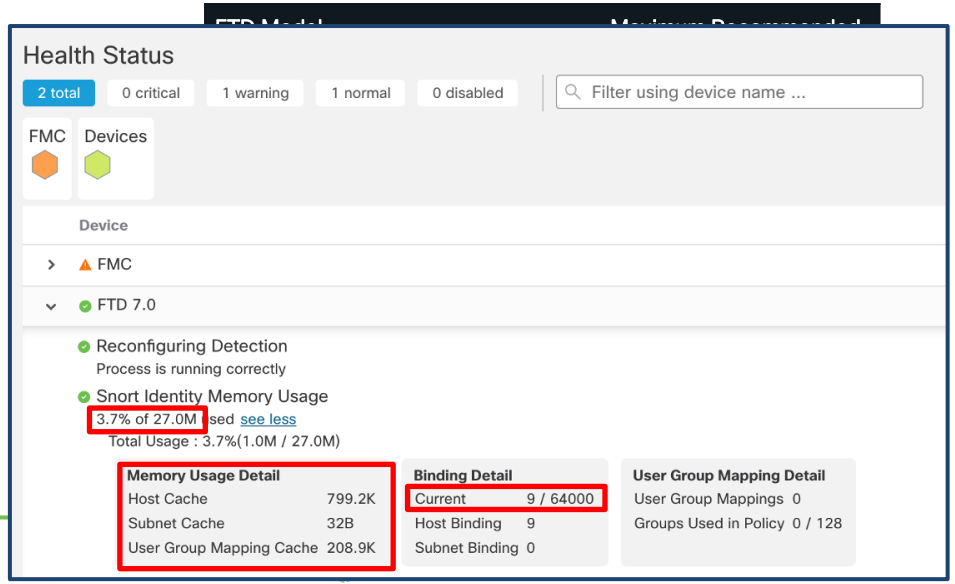
QUIZ 3: Dynamic Objects

Scaling and Redundancy

Scaling Firewall Identity Mappings

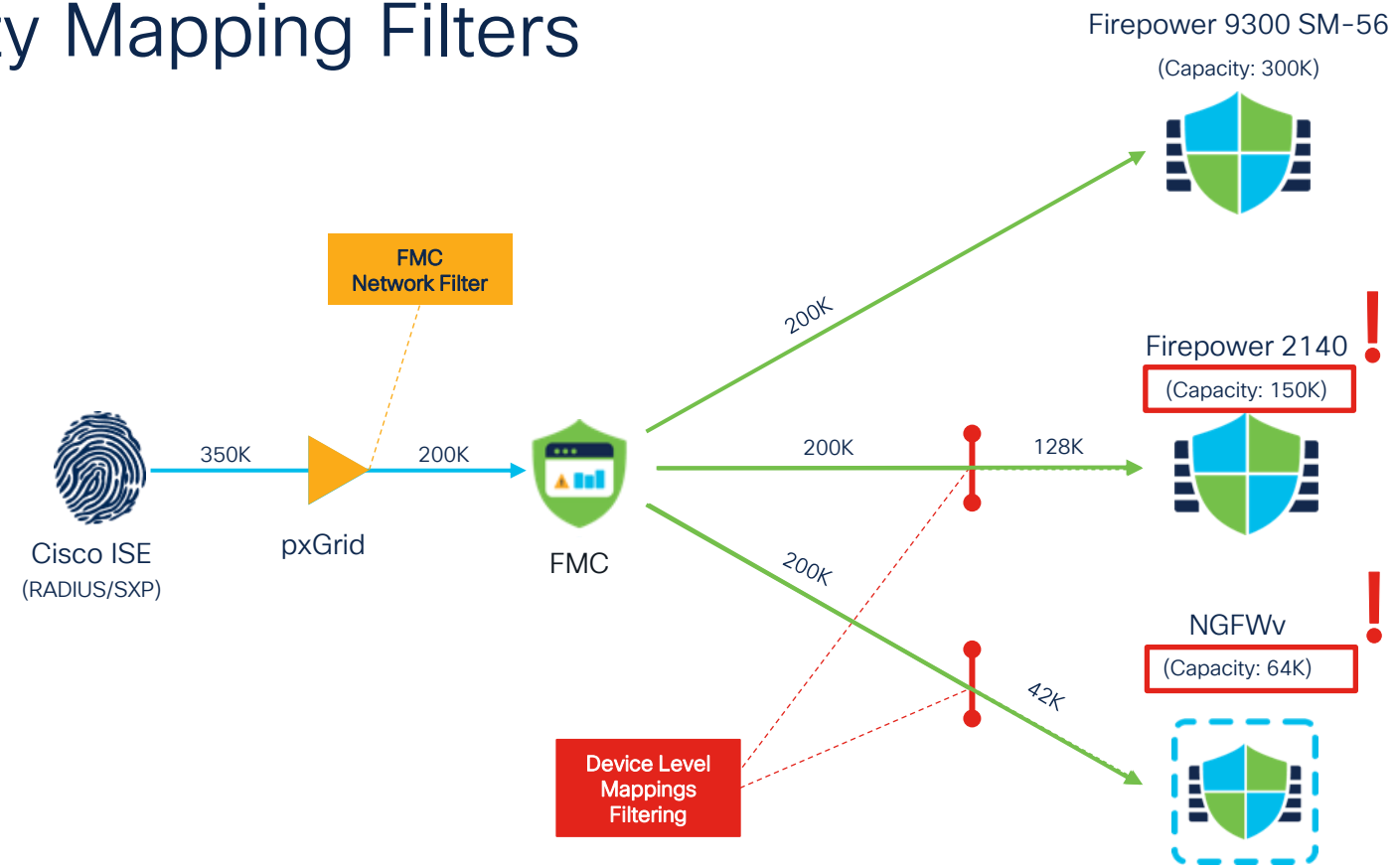
FMC Model	Maximum Downloaded Realm Users
FMC1600, FMC1700	50,000
FMC2600, FMC2700	150,000
FMC4600, FMC 4700	600,000
FMCv	50,000
FMCv 300	150,000

Management Center



Managed Device

Identity Mapping Filters



Identity Propagation Considerations

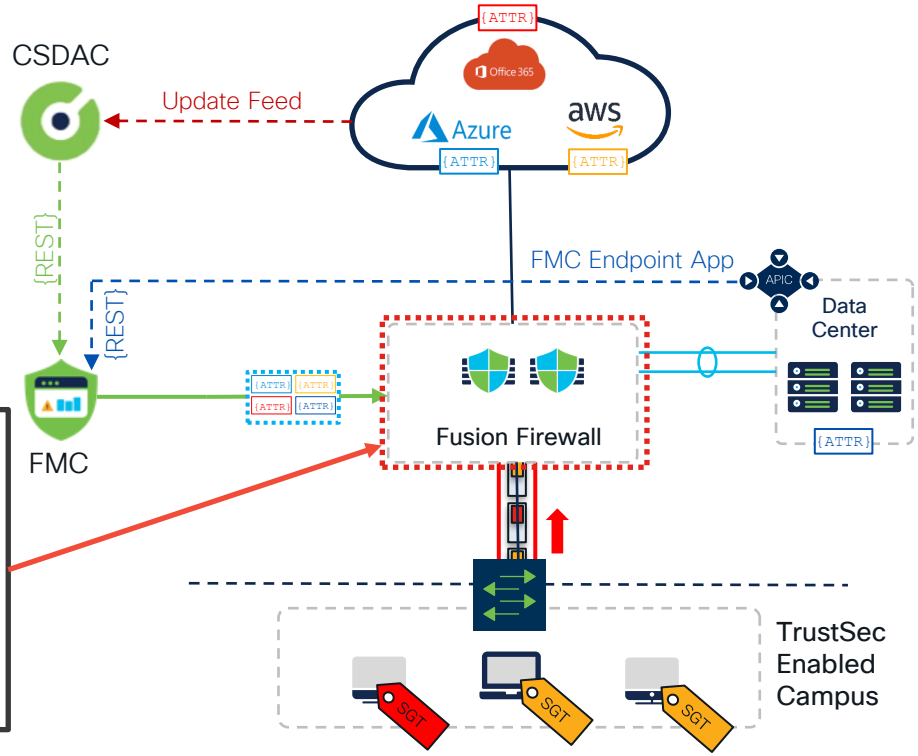
(Mapping Availability for Enforcement)

- Consider identity availability on the firewall when making enforcement decision
- Ensure your firewall can ingest the number of required identity mappings

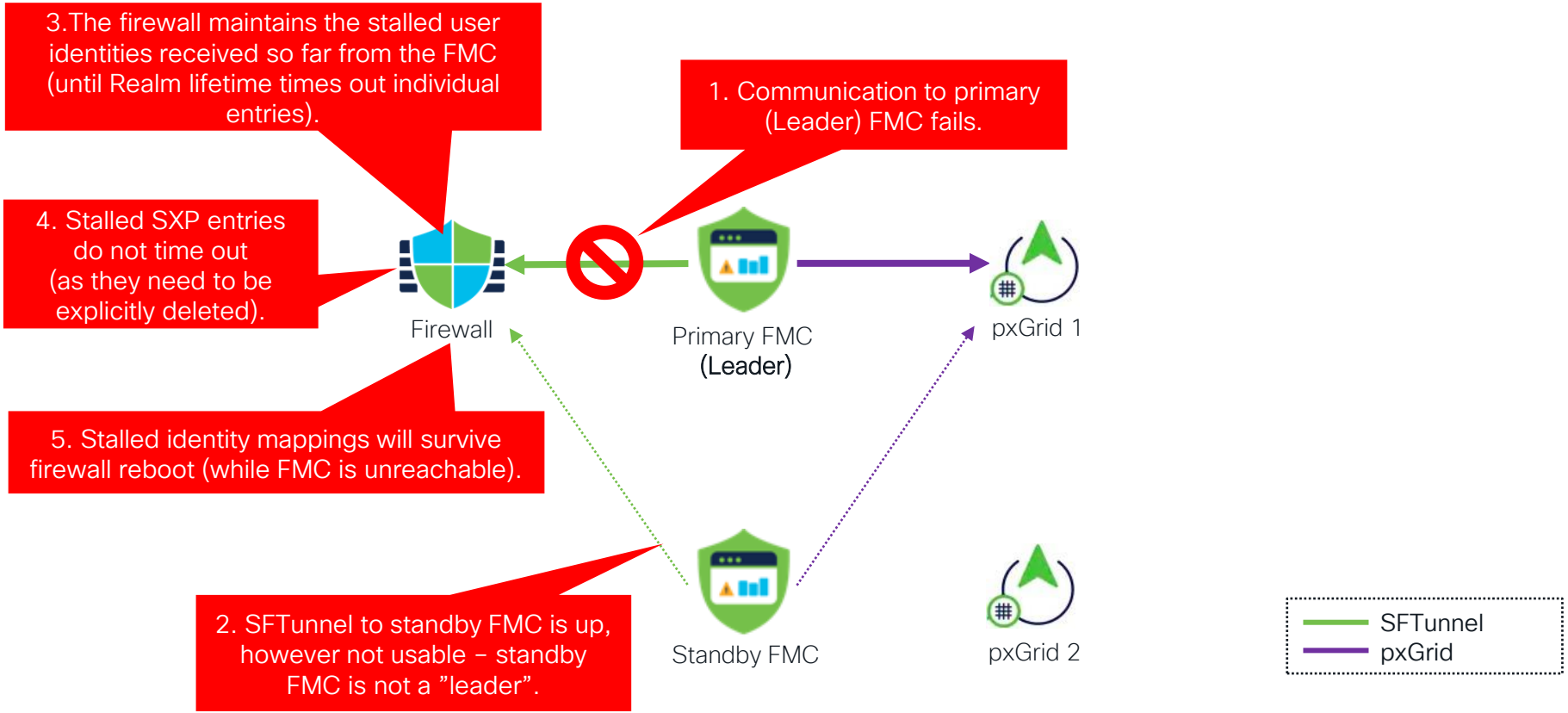
Enforcement Strategy: Site Egress

Egress Enforcement Capabilities:
Source SGT (Campus) -> EPG/ESG Dynamic Attribute (ACI)
Source SGT (Campus) -> CSDAC Dynamic Attribute (Public Cloud)

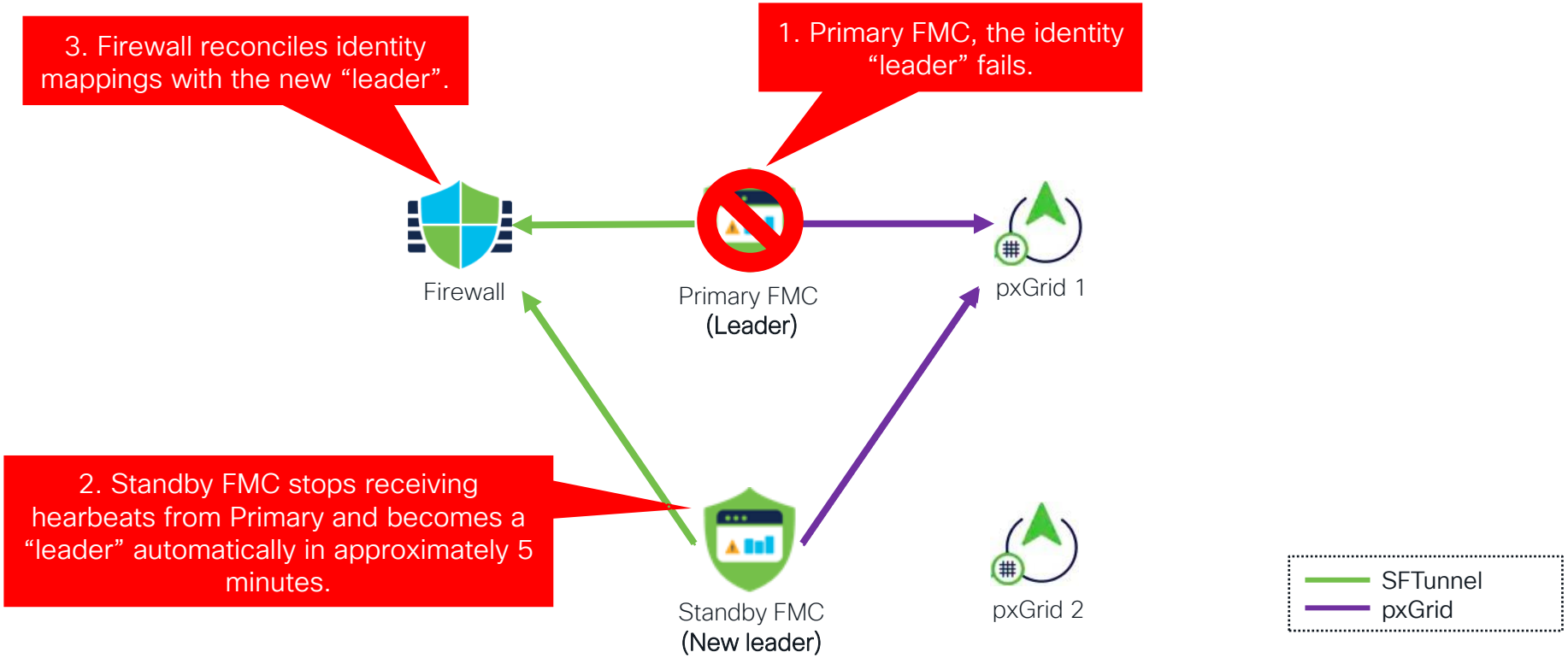
Ingress Enforcement Capabilities:
EPG/ESG Dynamic Attribute (ACI) -> Destination IP (Campus)
CSDAC Dynamic Attribute (Public Cloud) -> Destination IP (Campus)



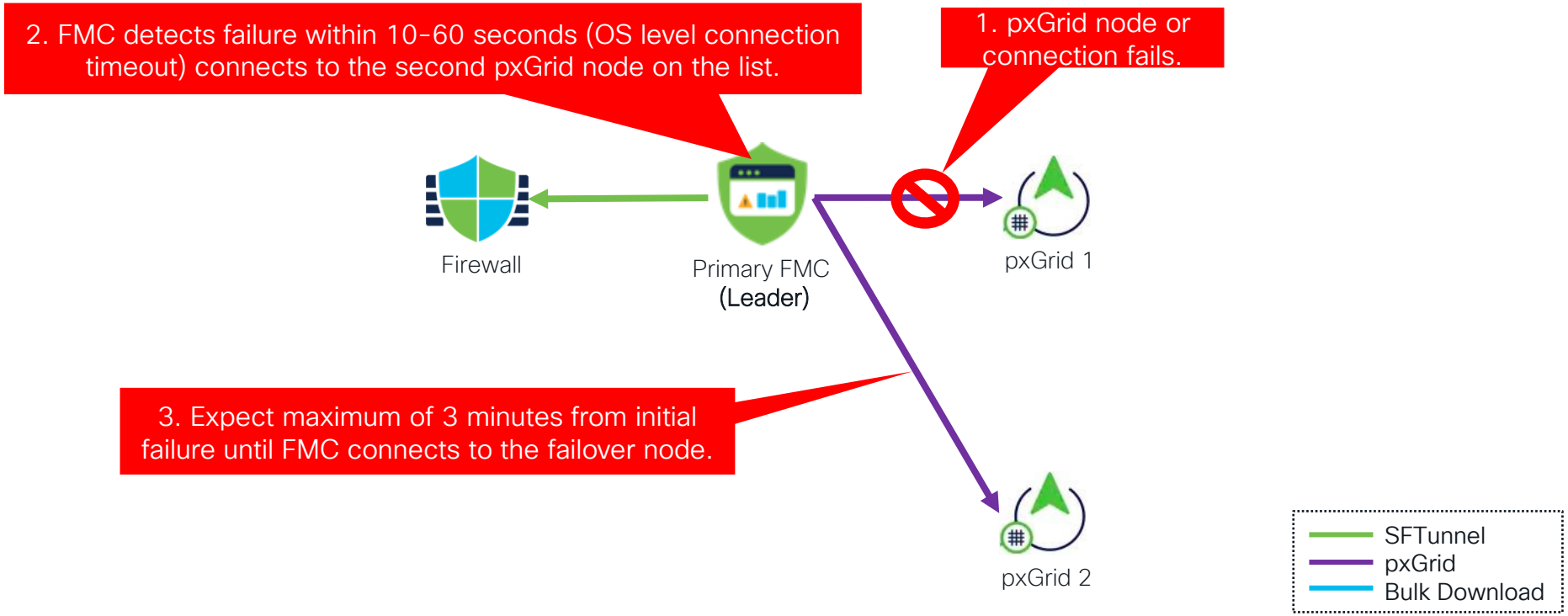
Failure Scenarios: SFTunnel to Primary FMC Down



Failure Scenarios – Primary FMC Down



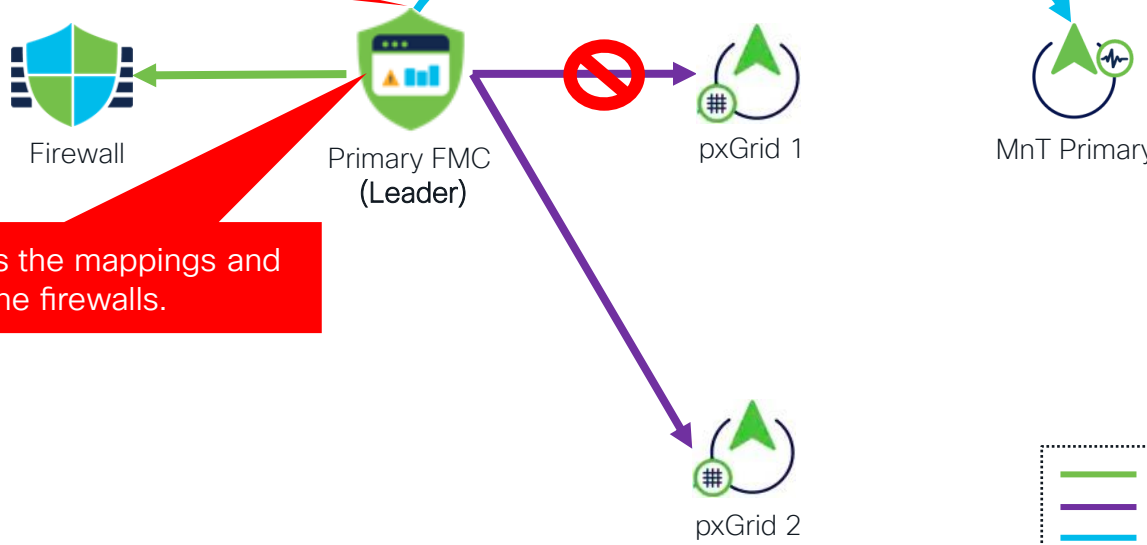
Failure Scenarios – pxGrid Node Down



Failure Scenarios – pxGrid Node Down (cont.)

4. Once pxGrid 2 connection to secondary pxGrid node is operational, the FMC does Session Bulk Download from Primary MnT.

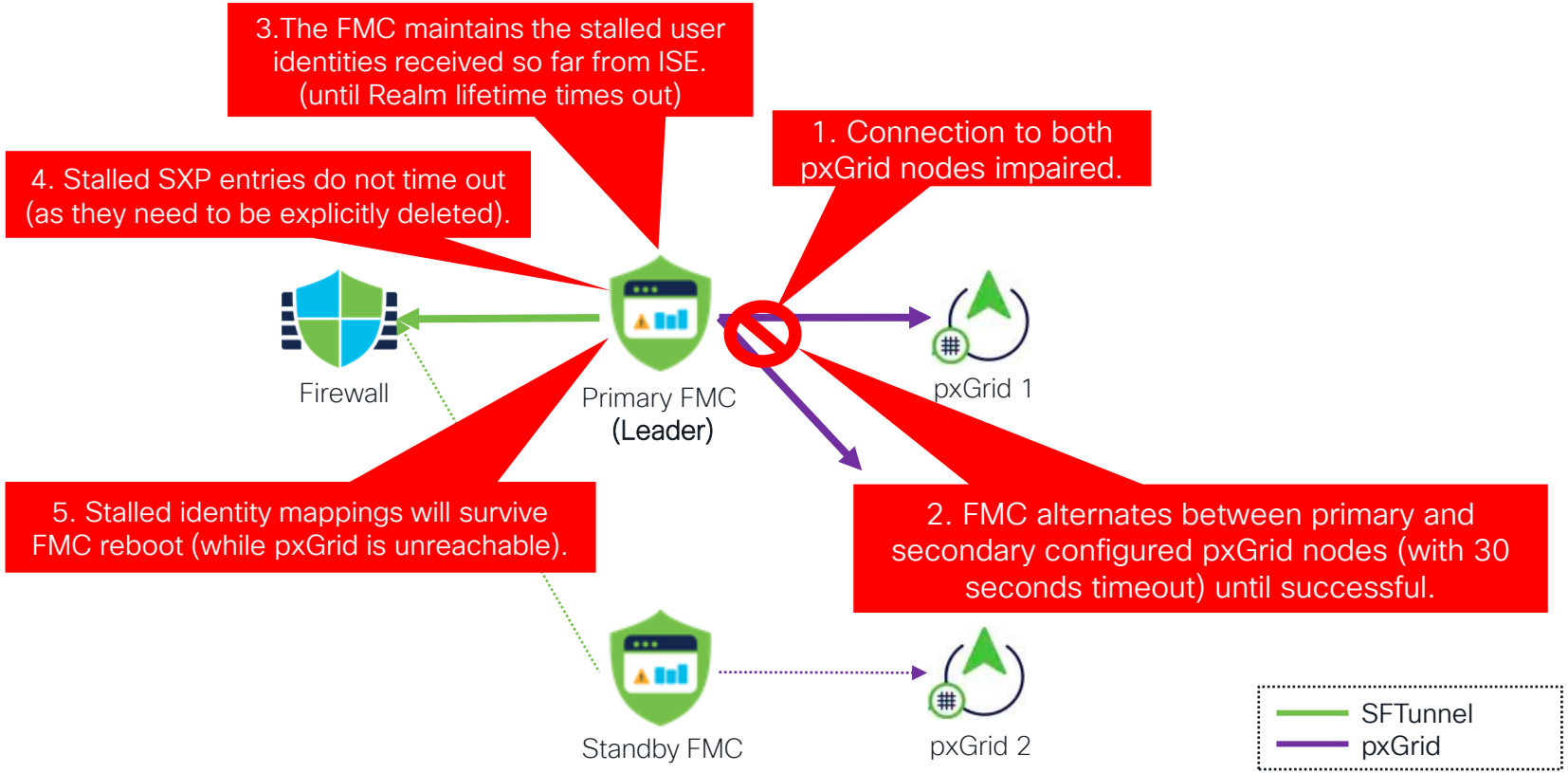
5. Bulk download time depends on the number of sessions (approx. 20K sessions / minute).



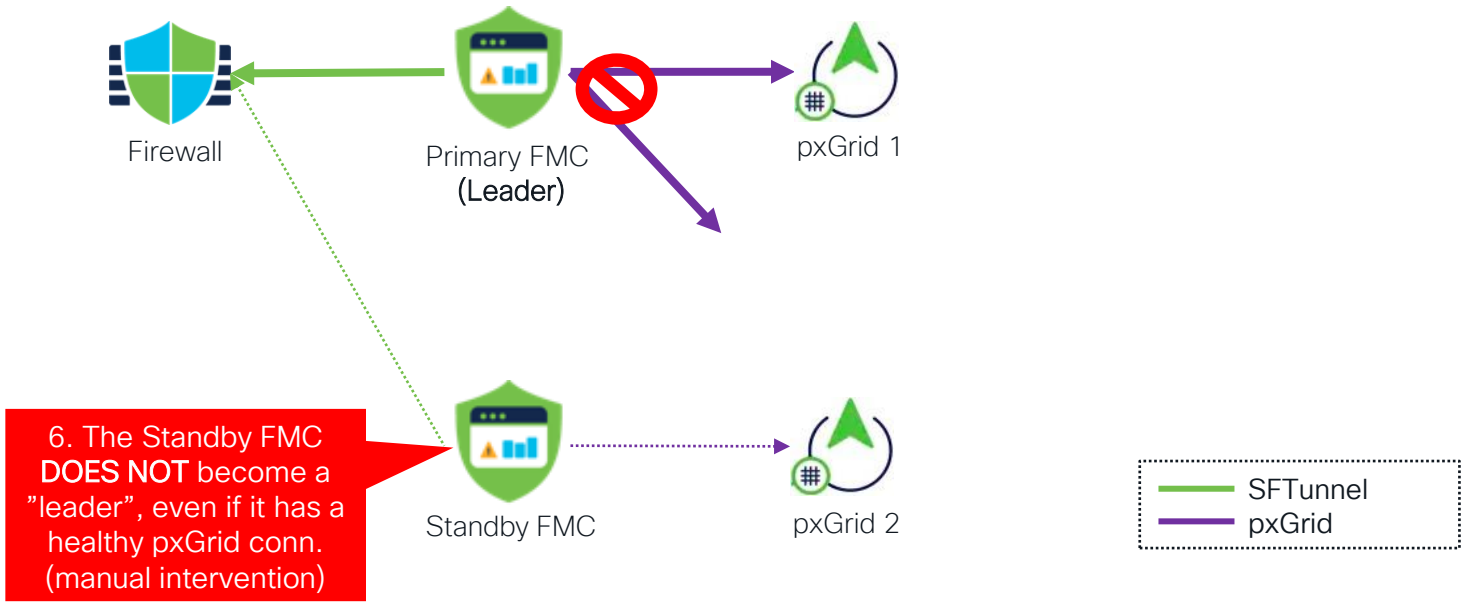
6. FMC reconciles the mappings and updates the firewalls.

SFTunnel
pxGrid
Bulk Download

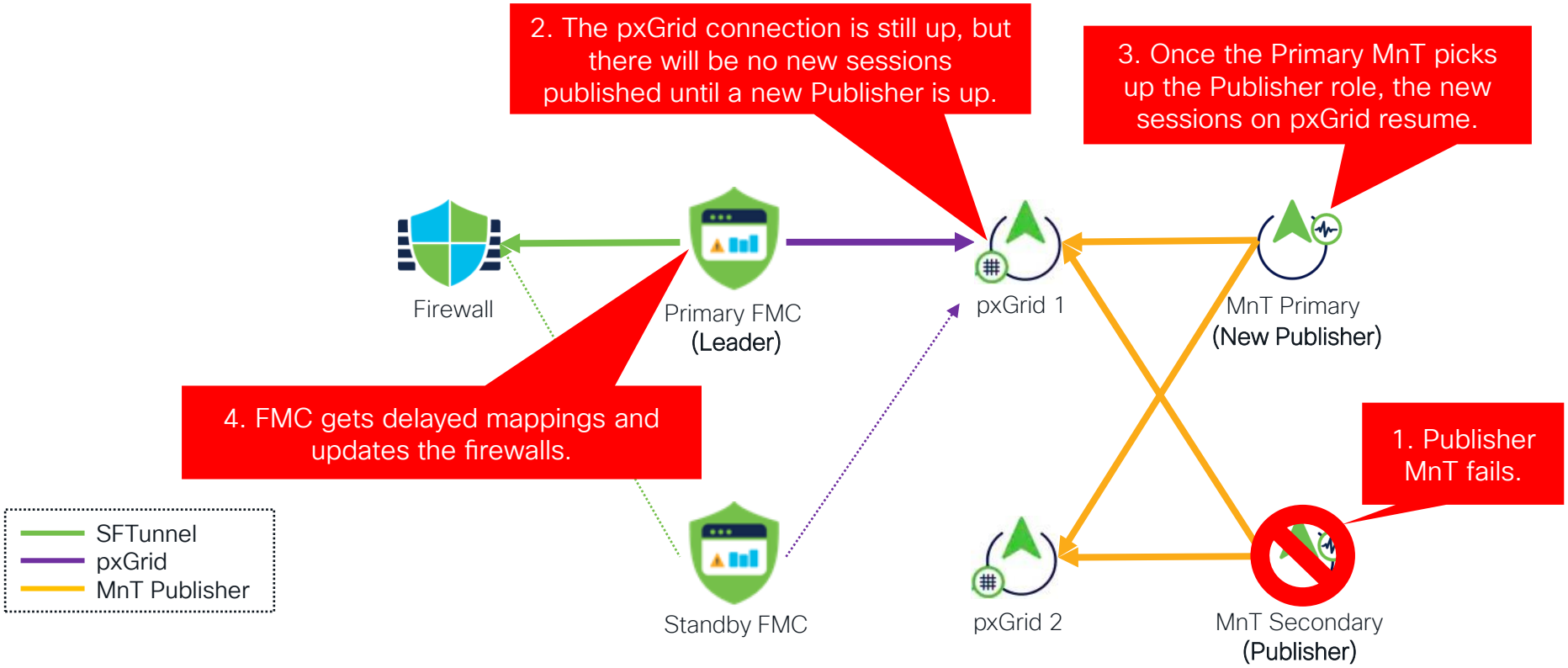
Failure Scenarios – Both pxGrid Nodes Unreachable



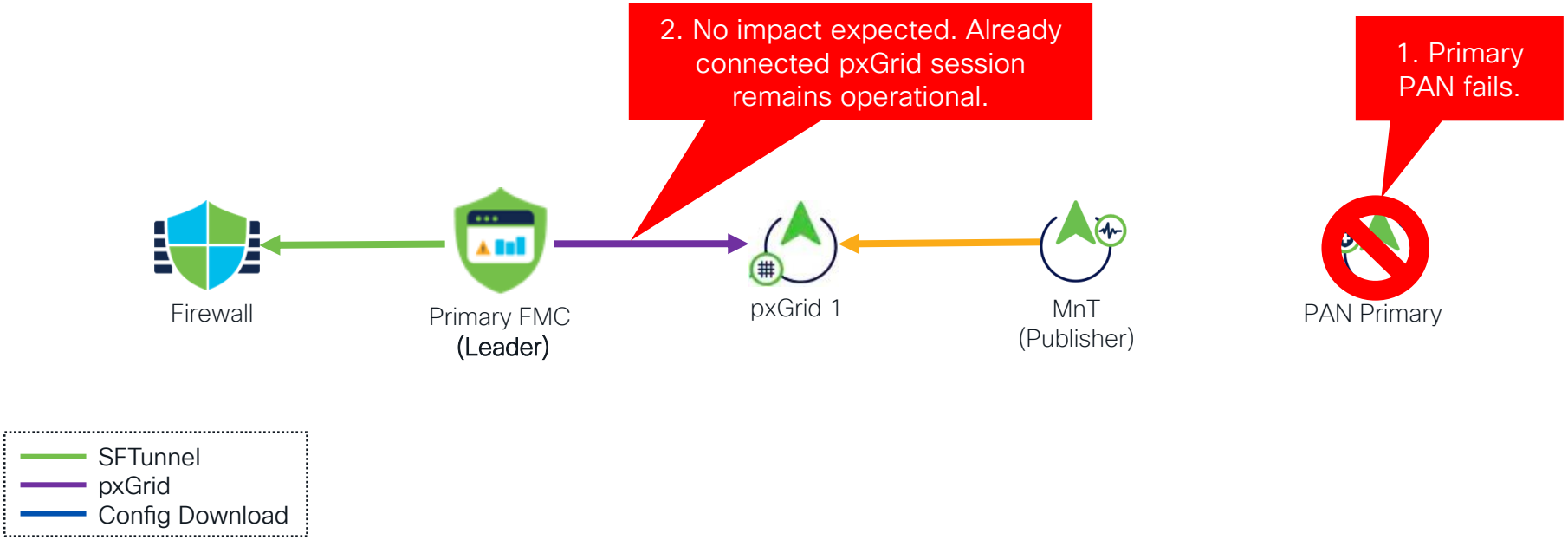
Failure Scenarios – Both pxGrid Nodes Unreachable



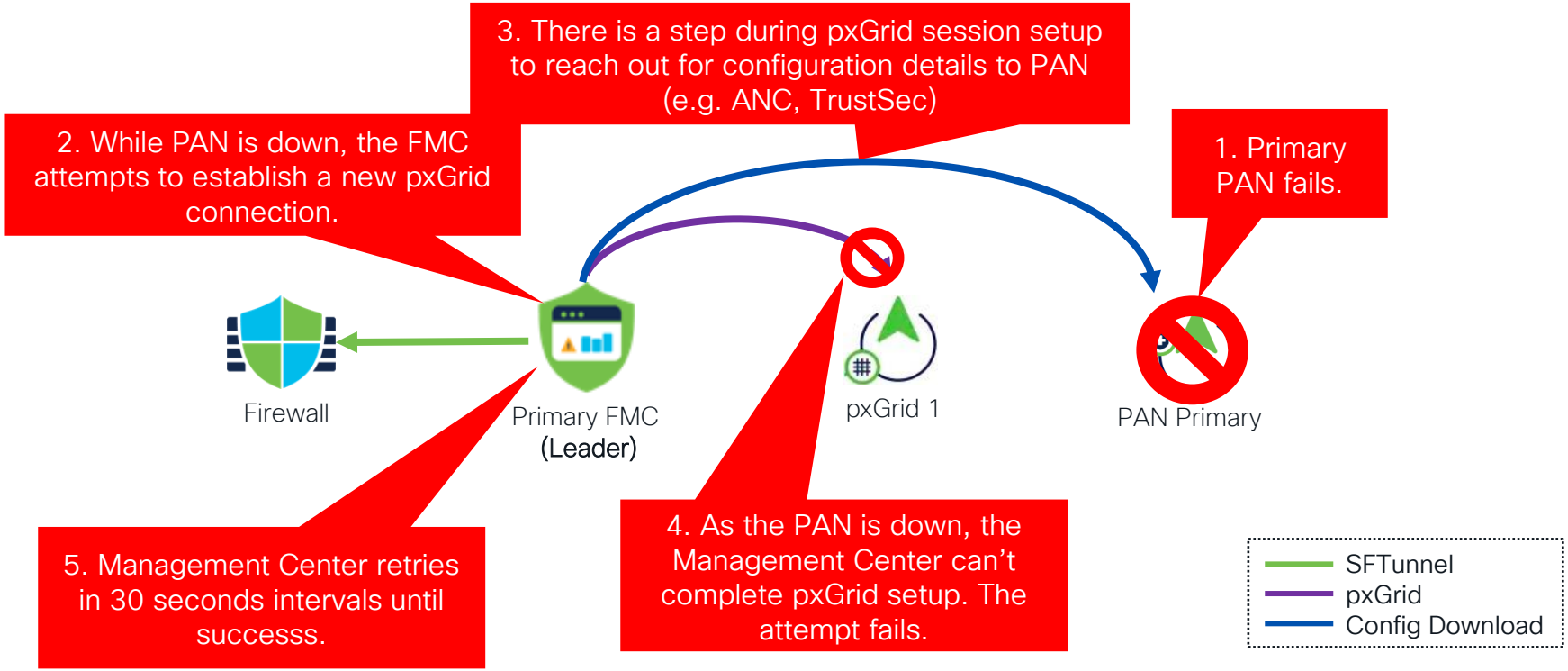
Failure Scenarios – MnT Publisher Down



Failure Scenarios – ISE Primary PAN Down – Existing pxGrid Connection

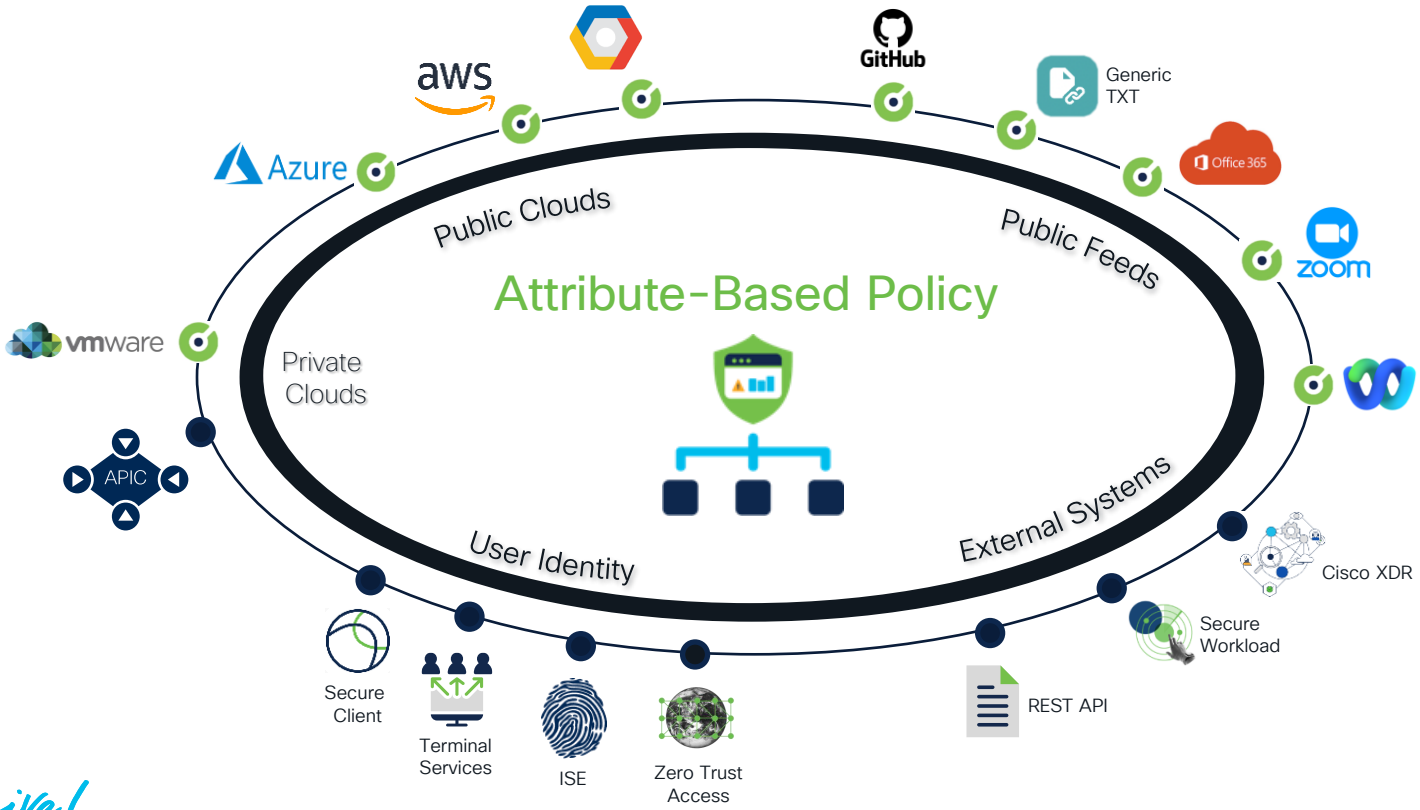


Failure Scenarios – ISE Primary PAN Down – New pxGrid Connection



Conclusions

Attribute-Base Policy makes your firewall rules dynamic, more secure and easier to manage



Attribute Based Policy with User and Server Identity

#	Name	Source Zones	Dest Zones	Users	Applications	Dest Ports	Source Dynamic Attributes	Destination Dynamic Attributes	Action
> Mandatory - Attribute-Based Policy (-)									
⌄ Default - Attribute-Based Policy (1-9)									
1	Workload_1	Any	Any	Any	Any	HTTP HTTPS	WorkloadObj_615c486dc9	WorkloadObj_615c8066483	Allow
2	IoT Support Service	External	IoT_VN	Any	Any	HTTPS SSH	IoT_Support	IoT	Allow
3	Machine Authentication	Corporate_VN	Shared_Services	Any	Any	AD_Services	Machine_Auth	VMWare_Active_Directory	Allow
4	Pri	Corporate_VN	Data_Center_Edge	Any	Any	SNMP ICMP-PING Spooler_Service	RICOH-Aficio-SP-C410DN RICOH-Aficio-SP-C820DN Xerox-WorkCentre-5030 Xerox-WorkCentre-5135	APIC_A_ESG_Print_Servers	Allow
5	Block Social Media	VN	External	Any	Facebook Google+ Instagram Tinder Twitter	Any	Contractors Branch_Locations	Any	Block
6	o365 Access	Corporate_VN	External	lab-local/Domain Users	Any	HTTPS HTTP	Any	o365_Common o365_Exchange o365_SharePoint	Allow
7	SecureX Threat Containment	Corporate_VN	Data_Center_Edge	Any	Any	Any	SecureX_Quarantined_IPs SecureX_Suspicious_IPs	Honeypot_Service	Allow
8	ISE Threat Containment	Corporate_VN	Data_Center_Edge	Any	Any	Any	Quarantined_Systems	Honeypot_Service	Allow
9	Cloud App Access	Corporate_VN	WAN	Any	Any	HTTP HTTPS	Employees	Azure_HR_Workload Azure_Intranet_Service	Allow

Complete your Session Survey

Before leaving the room, please share your feedback on this session!

- It is very important for me personally and …
- … based on your feedback I will improve slides, add more relevant content and influence engineering decisions.

The bridge to possible

Thank you

cisco Live!