Overview

Event	5434 Endpoint conducted several failed authentications of the same scenario
Username	lab\test
Endpoint Id	24:BE:05:01:5D:C5
Endpoint Profile	HP-Device
Authentication Policy	WIRED_LAB>> WIRED_AUTH
Authorization Policy	WIRED_LAB>> Default
Authorization Result	DenyAccess

Authentication Details

Source Timestamp	2020-01-26 11:42:19.339
Received Timestamp	2020-01-26 11:42:19.339
Policy Server	SRP-01-CISE010
Event	5434 Endpoint conducted several failed authentications of the same scenario
Failure Reason	15039 Rejected per authorization profile
Resolution	Authorization Profile with ACCESS_REJECT attribute was selected as a result of the matching authorization rule. Check the appropriate Authorization policy rule-results.
Root cause	Selected Authorization Profile contains ACCESS_REJECT attribute
Username	lab\test
Endpoint Id	24:BE:05:01:5D:C5
Endpoint Profile	HP-Device
IPv4 Address	xx.xx.xx.xx (address when authentication failed)
Authentication Identity Store	AD_USERS
Identity Group	Profiled 0A0AFF0100001890B9014E9C dot1x
Audit Session Id	PEAP (EAP-MSCHAPv2) Framed
Authentication Method	SWitch01
Authentication Protocol	All Device Types#Switches All Locations
Service Type	
Network Device	
Device Type	
Location	
NAS IPv4 Address	xx.xx.xx.xx
NAS Port Id	GigabitEthernet3/0/27
NAS Port Type	Ethernet
Authorization Profile	DenyAccess
Response Time	4 milliseconds

Steps

11001	Received RADIUS Access-Request
11017	RADIUS created a new session
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15048	Queried PIP
11507	Extracted EAP-Response/Identity
12500	Prepared EAP-Request proposing EAP-TLS with challenge
12625	Valid EAP-Key-Name attribute received
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12301	Extracted EAP-Response/NAK requesting to use PEAP instead
12300	Prepared EAP-Request proposing PEAP with challenge
12625	Valid EAP-Key-Name attribute received
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12302	Extracted EAP-Response containing PEAP challenge-response and accepting PEAP as negotiated
12318	Successfully negotiated PEAP version 0
12800	Extracted first TLS record; TLS handshake started
12805	Extracted TLS ClientHello message
12806	Prepared TLS ServerHello message
12807	Prepared TLS Certificate message
12808	Prepared TLS ServerKeyExchange message
12810	Prepared TLS ServerDone message
12811	Extracted TLS Certificate message containing client certificate
12305	Prepared EAP-Request with another PEAP challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12304	Extracted EAP-Response containing PEAP challenge-response
12305	Prepared EAP-Request with another PEAP challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12304	Extracted EAP-Response containing PEAP challenge-response
12318	Successfully negotiated PEAP version 0
12812	Extracted TLS ClientKeyExchange message
12813	Extracted TLS CertificateVerify message
12804	Extracted TLS Finished message
12801	Prepared TLS ChangeCipherSpec message
12802	Prepared TLS Finished message
12816	TLS handshake succeeded
12310	PEAP full handshake finished successfully
12305	Prepared EAP-Request with another PEAP challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12304	Extracted EAP-Response containing PEAP challenge-response
12313	PEAP inner method started
11521	Prepared EAP-Request/Identity for inner EAP method
12305	Prepared EAP-Request with another PEAP challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12304	Extracted EAP-Response containing PEAP challenge-response
11522	Extracted EAP-Response/Identity for inner EAP method
11806	Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge
12305	Prepared EAP-Request with another PEAP challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session

Other Attributes

ConfigVersionId	78
Device Port	1645
DestinationPort	1645
RadiusPacketType	AccessRequest
UserName	lab\test
Protocol	Radius

12304	Extracted EAP-Response containing PEAP challenge-response
11808	Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP-MSCHAP as negotiated
15041	Evaluating Identity Policy
15013	Selected Identity Source AD_USERS
24430	Authenticating user against Active Directory
24325	Resolving identity
24313	Search for matching accounts at join point
24315	Single matching account found in domain
24323	Identity resolution detected single matching account
24343	RPC Logon request succeeded
24355	LDAP fetch succeeded
24458	Not all Active Directory attributes are retrieved successfully
24100	Some of the expected attributes are not found on the subject record. The default values, if configured, will be used for these attributes
24402	User authentication against Active Directory succeeded
22037	Authentication Passed
11824	EAP-MSCHAP authentication attempt passed
12305	Prepared EAP-Request with another PEAP challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12304	Extracted EAP-Response containing PEAP challenge-response
11810	Extracted EAP-Response for inner method containing MSCHAP challenge-response
11814	Inner EAP-MSCHAP authentication succeeded
11519	Prepared EAP-Success for inner EAP method
12314	PEAP inner method finished successfully
12305	Prepared EAP-Request with another PEAP challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12304	Extracted EAP-Response containing PEAP challenge-response
24715	ISE has not confirmed locally previous successful machine authentication for user in Active Directory
15036	Evaluating Authorization Policy
24432	Looking up user in Active Directory - lab\test
24355	LDAP fetch succeeded
24416	User's Groups retrieval from Active Directory succeeded
15048	Queried PIP
15016	Selected Authorization Profile - DenyAccess
15039	Rejected per authorization profile
12306	PEAP authentication succeeded
11503	Prepared EAP-Success
11003	Returned RADIUS Access-Reject
5449	Endpoint failed authentication of the same scenario several times and was rejected
5434	Endpoint conducted several failed authentications of the same scenario

NAS-IP-Address	xx.xx.xx.xx
NAS-Port	50327
Framed-MTU	1500
State	37CPMSessionID=0A0AFF0100001890B9014E9C;40SessionID=SRP-01-CISE010/368080779/89132;
IsEndpointInRejectMode	true
NetworkDeviceProfileName	Cisco
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
IsThirdPartyDeviceFlow	false
RadiusFlowType	Wired802_1x
SSID	70-6D-15-0F-96-9B
AcsSessionID	SRP-01-CISE010/368080779/89132
DetailedInfo	Authentication succeed
SelectedAuthenticationIdentityStores	AD_USERS
IdentityPolicyMatchedRule	WIRED_AUTH
AuthorizationPolicyMatchedRule	Default
CPMSessionID	0A0AFF0100001890B9014E9C
EndPointMACAddress	24-BE-05-01-5D-C5
ISEPolicySetName	WIRED_LAB
IdentitySelectionMatchedRule	WIRED_AUTH
AD-User-Resolved-Identities	test@lab.it
AD-User-Candidate-Identities	test@lab.it
AD-User-Join-Point	LAB.IT
StepData	4= DEVICE.Device Type
StepData	65=AD_USERS
StepData	66=AD_USERS
StepData	67=lab\test
StepData	68=lab.it
StepData	69=lab.it
StepData	71=test@lab.it
StepData	72=lab.it
StepData	73=AD_USERS
StepData	74=AD_USERS
StepData	75=AD_USERS
StepData	94=AD_USERS
StepData	95=lab.it
StepData	96=AD_USERS
StepData	97= AD_USERS .ExternalGroups
AD-User-Resolved-DNs	CN=test test
OU	compta
OU	lab.it
DC	lab
DC	it
AD-User-DNS-Domain	lab.it
AD-Groups-Names	lab.it/Users/Domain Users
AD-Groups-Names	lab.it/ lab.it\compta
AD-User-NetBios-Name	false
IsMachineIdentity	

UserAccountControl	512
AD-User-SamAccount-Name	test
AD-User-Qualified-Name	test@lab.it
TLSCipher	ECDHE-RSA-AES256-SHA
TLSVersion	TLSv1
DTLSSupport	Unknown
HostIdentityGroup	Endpoint Identity Groups:Profiled
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types#Switches
IPSEC	IPSEC#Is IPSEC Device#No
ExternalGroups	S-1-5-21-518455919-1689331296-4088792076-513
ExternalGroups	S-1-5-21-518455919-1689331296-4088792076-3790
IdentityAccessRestricted	false
Called-Station-ID	70:6D:15:0F:96:9B
CiscoAVPair	service-type=Framed
audit-session-id	0A0AFF0100001890B9014E9C
method	dot1x
vlan-id	21

Result

RadiusPacketType	AccessReject
EAP-Key-Name	19:5e:2d:6d:0b:60:9b:83:4c:31:de:09:94:d9:2a:9d:cf:41:0a:bc:e1:37:0b:6b:95:9f:4b:5c:d0:27:3c:85:d0:8c:dc:8c:b2:3e:0b:71:84:28:ce:d9:b5:ef:4e:fb:3a:4e:c4:c1:8c:cb:a5:de:ed:28:a9:bf:0f:e1:3a:a7:38

Session Events

2020-01-26 11:43:13.367	RADIUS Accounting watchdog update
2020-01-26 11:42:55.356	RADIUS Accounting watchdog update
2020-01-26 11:42:37.351	RADIUS Accounting watchdog update
2020-01-26 11:42:19.35	RADIUS Accounting watchdog update
2020-01-26 11:22:13.65	RADIUS Accounting watchdog update
2020-01-26 11:21:55.549	RADIUS Accounting watchdog update
2020-01-26 11:21:37.449	RADIUS Accounting watchdog update
2020-01-26 11:21:19.351	RADIUS Accounting watchdog update
2020-01-26 11:21:19.341	Authentication failed
2020-01-26 11:01:14.248	RADIUS Accounting watchdog update