

تايوتحملا

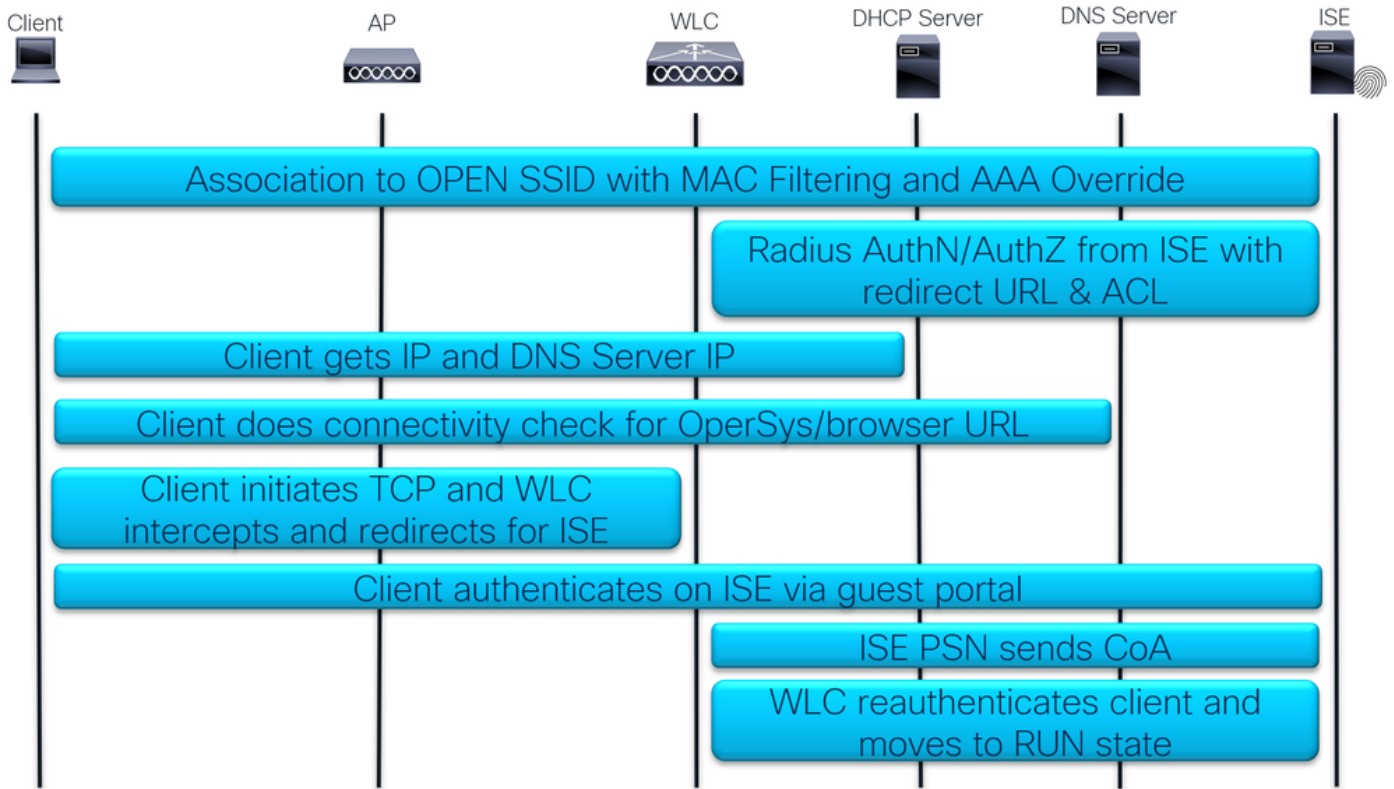
عجاربہ

ەي في ك و، CWA ب ەقل ەتم الم تال ج س ل ا ع ي م ج ت ە ي في ك و، ەي ل م ع ل ل ە م ا ع ل ا ت ا و ط خ ل ا ي ل ا ر ط ن ن ي ف م ك ح ت ل ا ر ص ن ع ي ل ع ە ن م م ض م ە م ز ح ط ا ق ت ل ا ع ي م ج ت ە ي في ك و، ت ا ل ج س ل ا ه ذ ه ل ي ل ح ت

رورمل ةكرح قفدت ديكأتل (WLC) ةيكلسلال ةيلحمل ةكبشلا

ةكبش لاصتالاب ني مدختسملل حمست يتلا تاكرشلل اعويش رثكال دادعإل CWA ربتعي BYOD. مساب اضيأ ةفورعلم، ةيصخشلا مهتزجأ مادختساب ةكرشلا متي يتلا اءال صإو ءاطأل فاشكتسا تاوطخو Gotchas تاوطخلاب متهم ةكبش لوؤسم ي ةينفلا ةدعاسمل زكرم ءلاح حتف لبق مهتالكشم ءالصال اهذيفنت

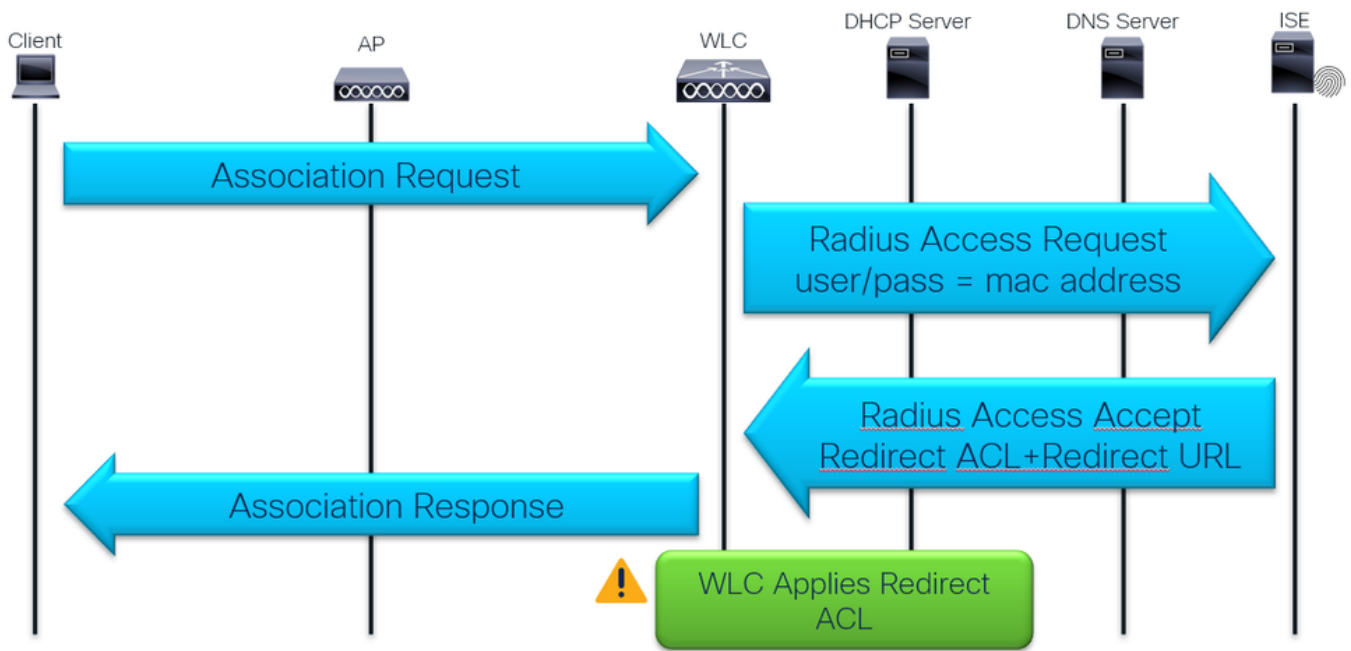
CWA ةمزح قفدت انه



CWA مزح قفدت

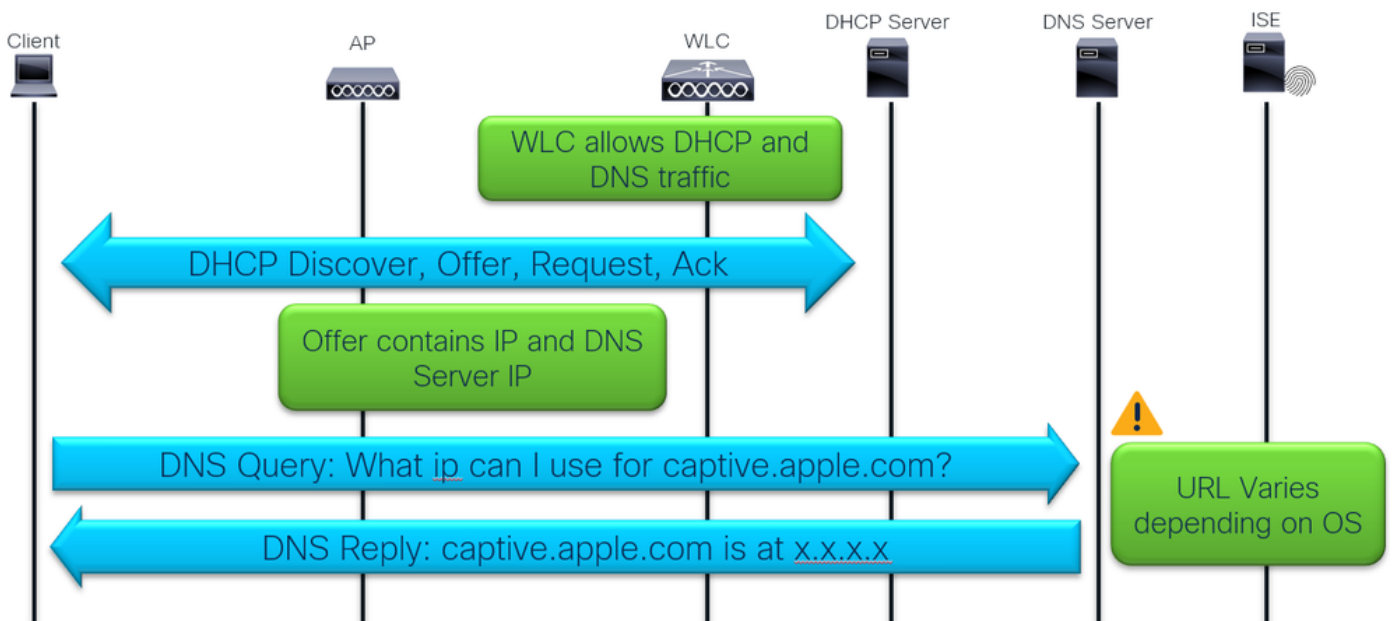
يليصفت نايرج

RADIUS: ةقداصمو لوألا نارتقالا



راديوس مودم و نارتقا لؤا

للاصتالو او DNS و DHCP صحف:



للاصتالو او DNS و DHCP صحف

ليغشت ماظن ةطساوب دي قم لا لخدم لا نع فشكلا مادختساب لاصتالا نم ققحتالا متي
ضرعتسملا و لي عمل زاهاجلا.

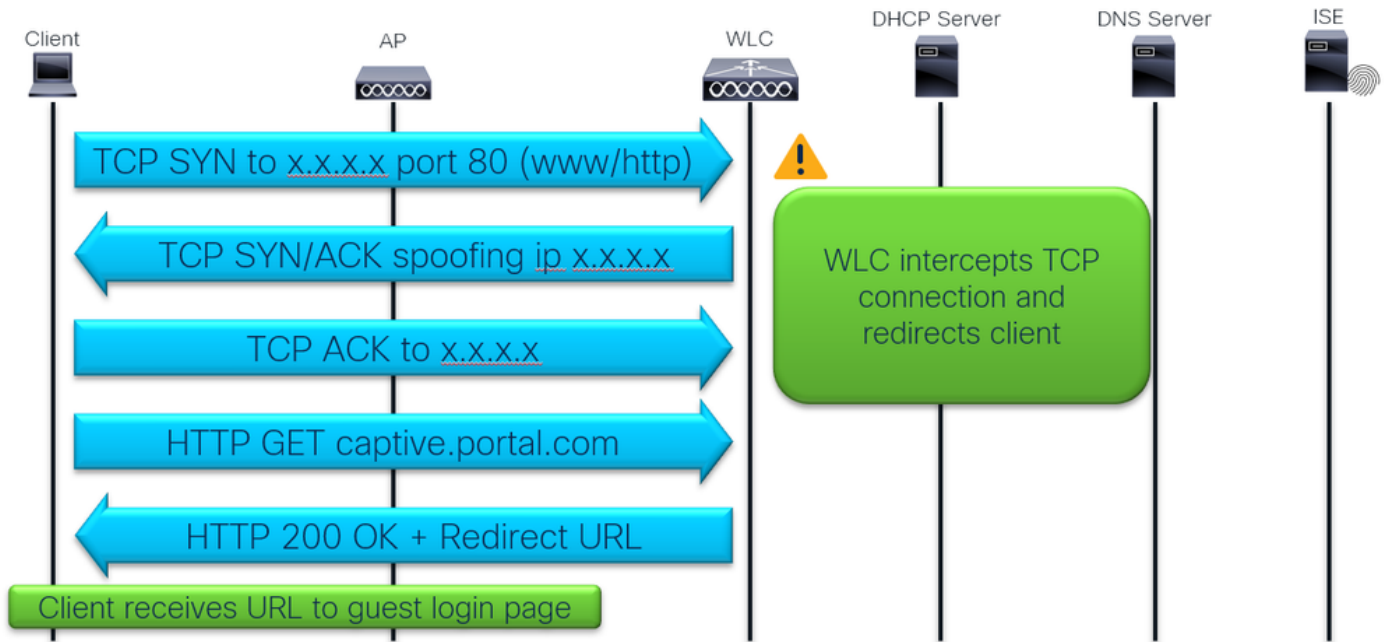
نعم لاجم لا لوصول HTTP ب مايقلل اقبس م هتجرب مت زاهاج ليغشت ماظن دجوي

- أبل = captive.apple.com
- Android = connectivitycheck.gstatic.com
- Windows = msftconnecttest.com

هحتف دن ققحتالا اذهب اضيأ تضرعتسملا موقتو

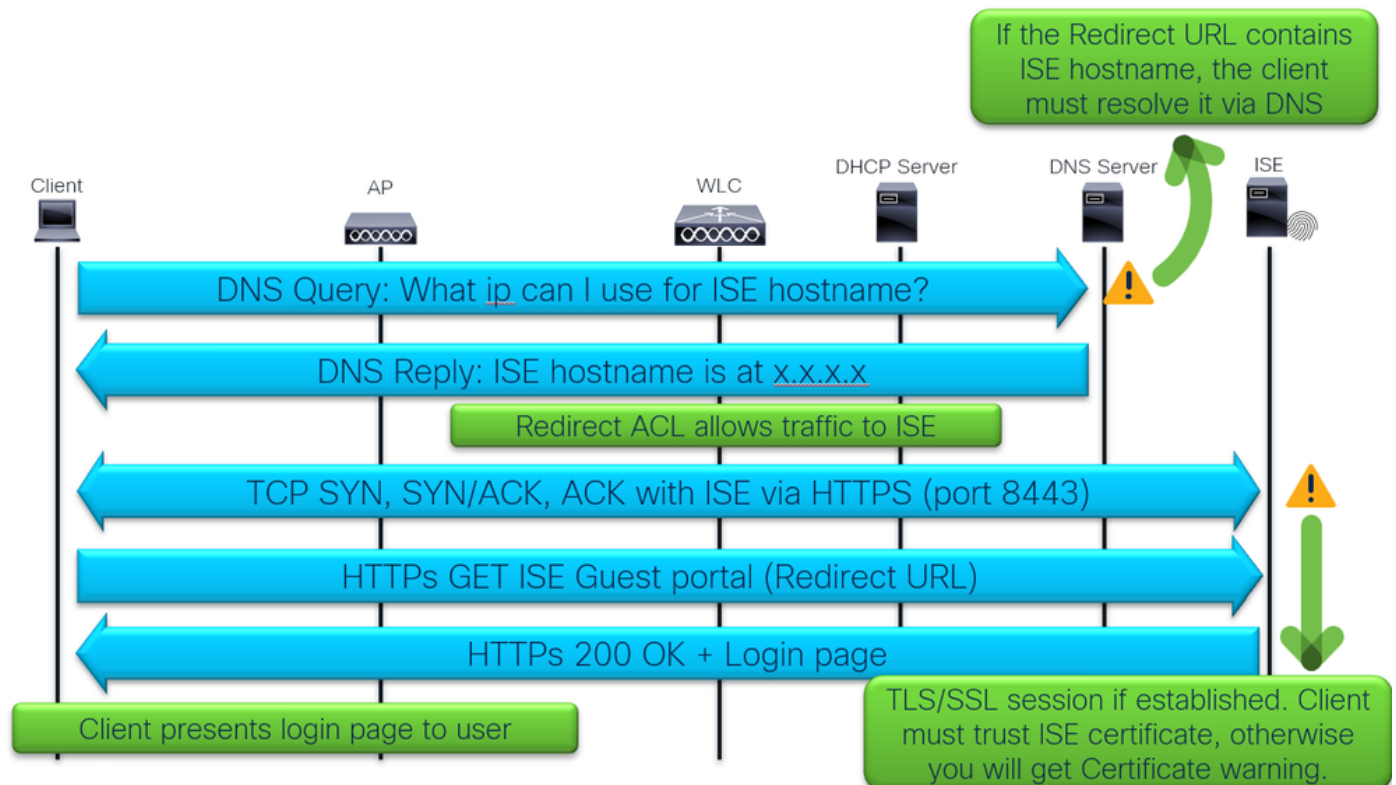
- الموركل = clients3.google.com
- Firefox = detectportal.firefox.com

ههجهوتل ءءاعل ءورمل ءكره ضارءءا:



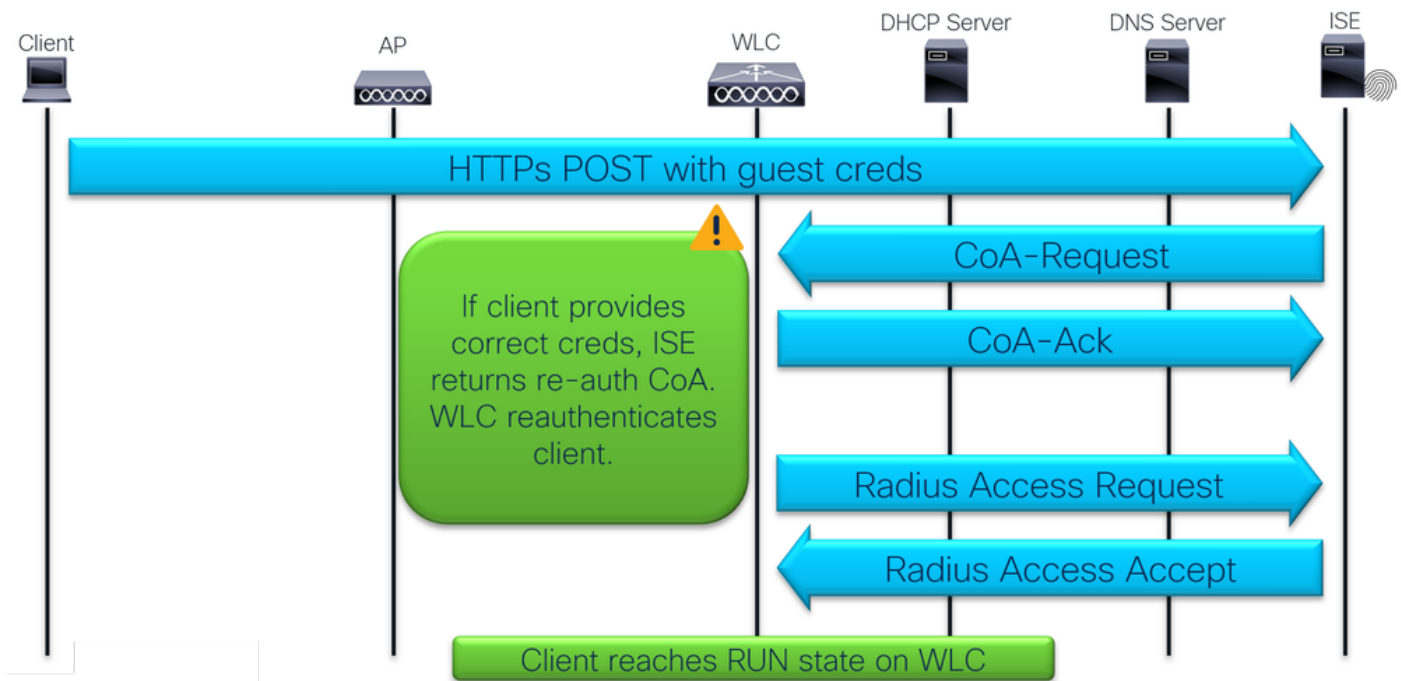
ههجهوتل ءءاعل ءورمل ءكره ضارءءا

ISE: فلفل ءوء ءلءءء ءءاوء ءل ءلفمءل ءوء ءلءءء



ISE: فلفل ءوء ءلءءء ءءاوء ءل ءلفمءل ءوء ءلءءء

CoA: ءلءءء ءوء ءلءءء ءوء ءلءءء

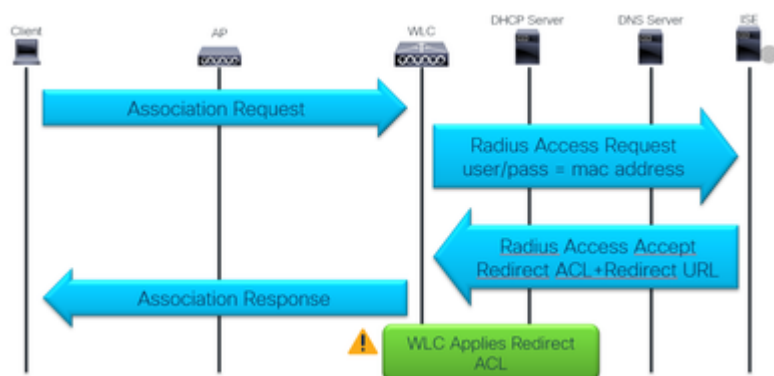


CoA لي جاست و لي عمل ل و خ د لي جاست

اه حال صا و عا ط خ ال فاش ك ت سا

ل و خ د ل ا لي جاست ة ح ف ص ي ل ا م د خ ت س م ل ا ه ي ج و ت ة د ا ع ا م ت ي م ل : ة ع ئ ا ش ل ا ض ا ر ع ا ل ا

ق ف د ت ل ا ن م ل و ا ل ا ع ر ج ل ا ب ا د ب ن ل ف



RADIUS ة ق د ا ص م و ن ا ر ت ق ا ل و ا

ي ل و ا ل a RADIUS ة ق د ا ص م ت ح ج ن ل ه - 1

MAC: ة ي ف ص ت ة ق د ا ص م ة ج ي ت ن م ق ق ح ت

Cisco ISE Operations - RADIUS

Live Logs Live Sessions

Misconfigured Suppliants 0 Misconfigured Network Devices 0

Refresh Reset Repeat Counts Export To

Time	Status	Details	Repea...	Identity	Endpoint ID
Jan 13, 2023 09:42:37.4...				F2:A4:01:57:8D...	F2:A4:01:57:8D:68

Authentication Details

Event: 5400 Authentication failed

Failure Reason: 22056 Subject not found in the applicable identity store(s)

Steps

22056 Subject not found in the applicable identity store(s)

MAC في صف ة قدا صم ة جي تن ره ظت ي الت ISE Live تال جس

يلع مدخت سمل رثعي مل اذا "ة عباتم" يلع ة قدا صم لل مدقت مل رايلخ ل نييعت نم دكأت

Cisco ISE Policy - Policy Sets

Policy Sets -> Default

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
Default	Default policy set			Default Network Access	42

Authentication Policy (2)

Status	Rule Name	Conditions	Use	Hits	Actions
CWA	Wireless_MAB				

Options

If Auth fail: REJECT

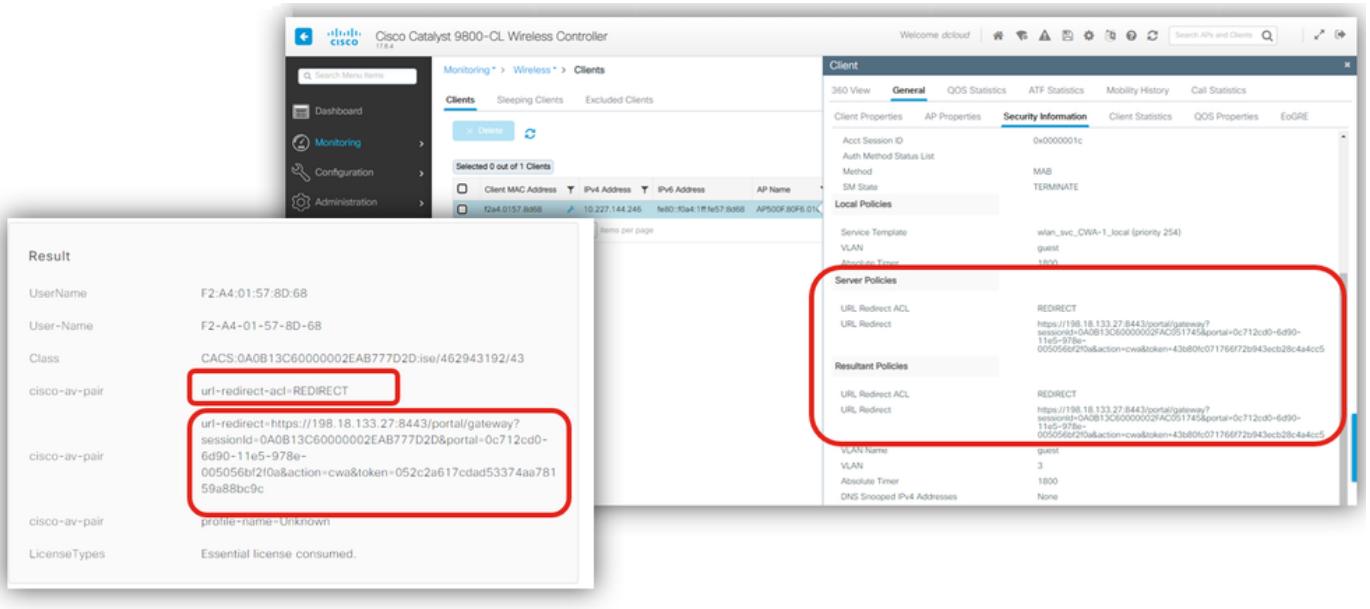
If User not found: CONTINUE

If Process fail: DROP

مدخت سمل لل مدقت مل رايلخ يلع روثعل متي مل

ههيجوت داعمل URL ناو نع ةيكل سلال ةيلحمل ةكبش لل في مكحتل انجل يقلت له - 2 (ACL) لوصول في مكحتل مئاوو

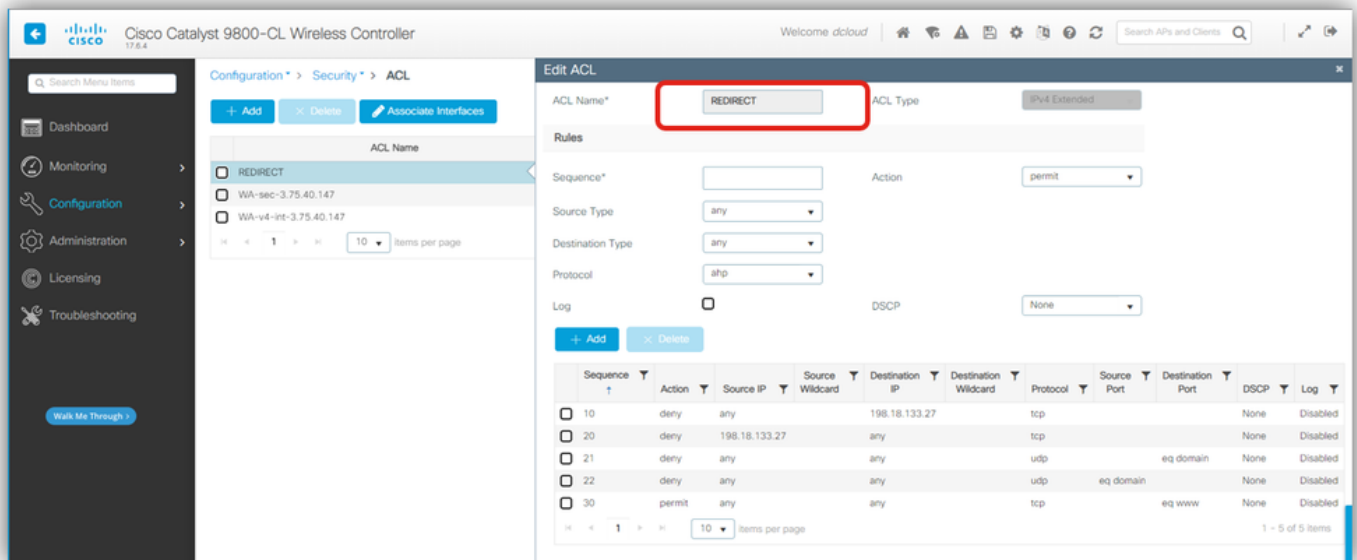
ISE نأ نم ققحت ةبقارمل تحت WLC لي مع نامأ تامولعمو ةرشابم ISE تالجس نم ققحت متي و لوصول لوبق في لوصول في مكحتل ةمئاقو هيجوتل داعل URL ناو نع لسري لي عمل لي صافت في لي عمل يلع هقيبطت متي و WLC ةطساوب همالتسا



URL و (ACL) لوصولو في مكحتل عمئاق هيچوت دءا

ةحجص اههيجوت داعمل (ACL) لوصولو في مكحتل عمئاق له - 3

يتل لثم امامت اهنأ نم دكأت. يعبظم أطخي أل (ACL) لوصولاب مكحتل عمئاق مسا نم ققحت ISE اهلسرأ:



اههيجوت داعمل (ACL) لوصولو في مكحتل عمئاق نم ققحتل

ققلع Web-Auth لىل لىمعل لقن مت له - 4

ةلأل هذه في نكي مل اذإ. "بيو ةقداصم قىلعت" ةلألل لىمعل لىصافت نم ققحت ةسالىسل فيرعت فلم في Radius NAC و AAA زواجت نيكم نم ققحتف:

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

Selected 0 out of 1 Clients

Client MAC Address	IPv4 Address	IPv6 Address	AP Name	SSID	WLAN ID	Client Type	State
f2a4.0157.8d68	198.18.1.11	fe80::f0a4:1ff:fe57:8d68	AP500F.80F6.0168	CWA-1	4	WLAN	Web Auth Pending

10 Items per page

Edit Policy Profile

IPv4 DHCP Required ☐

DHCP Server IP Address

Show more >>>

AAA Policy

Allow AAA Override ☒

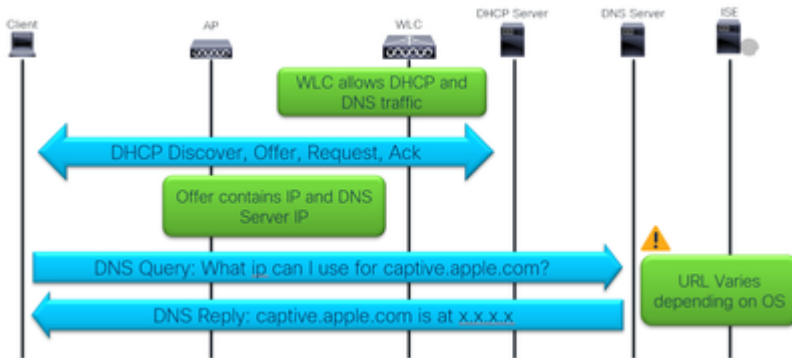
NAC State ☒

NAC Type

RADIUS NAC و AAA) ةبساحم لاوضي وف تال او ةقداصم لا و اج ت و ل لم عمل لي صا فت

لم ع ت ال ت ل ز ام

... ق ف د ت ال ي ف ر ظ ن ال دي ع ن ا ن ع د



ل لاص ت ال او DNS و DHCP ص ح ف

ت ا ن ا ي ب ر و ر م ة ك ر ح ب (WLC) ة ي ك ل س ال ال ة ي ل ح م ال ة ك ب ش ال ي ف م ك ح ت ال ة د ح و ح م س ت ل ه - 5 DHCP و DNS?

ي ف م ك ح ت ال ر ص ن ع ي ف (ACL) ل و ص و ل ال ي ف م ك ح ت ال ة م ئ ا ق ت ا ي و ت ح م ه ي ج و ت ة د ا ع ا ن م ق ق ح ت (WLC): ة ي ك ل س ال ال ة ي ل ح م ال ة ك ب ش ال

Cisco Catalyst 9800-CL Wireless Controller

Configuration > Security > ACL

Edit ACL

ACL Name* REDIRECT ACL Type IPv4 Extended

Rules

Sequence* Action permit

Source Type any

Destination Type any

Protocol http

Log ☐ DSCP None

Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
10	deny	any		198.18.133.27		tcp			None	Disabled
20	deny	198.18.133.27		any		tcp			None	Disabled
21	deny	any		any		udp		eq domain	None	Disabled
22	deny	any		any		udp		eq domain	None	Disabled
30	permit	any		any		tcp		eq www	None	Disabled

(WLC) ةيكل سلالا ةيلحمالا ةكبشلا يف مكحتلا رصنع يف (ACL) لوصولو يف مكحتلا ةمئاق تايوتحم هيوت ةداع

ةداعو اهضارتعا متي يتلا رورملا ةكرح اههيجوت داعمل (ACL) لوصولو يف مكحتلا ةمئاق ددحت
ةداعو ضارتعالا نم اهلهاجت متي يتلا رورملا ةكرحو صيخرتلا نايب ةطساوب اههيجوت
ضفرل نايب مادختساب هيوتلا.

يا ضارتعاو، ISE IP ناونع نم/ىل رورملا ةكرحو DNS تانايب قفدتب حمسن، لاثمل اذه يف
(www) 80 ذفنملا ىل TCP ل رورملا ةكرح.

DHCP بلط/فاش تكا DHCP مداخ لبقتسي له - 6

لثم ةيلخادلا تاحشرملا عم EPC مادختسا نكمي. DHCP لدابت ثدح اذا EPC عم ققحت
ليعمل زاهج MAC ناونع مادختسا اننكمي شيح Internal Filter MAC و/و DHCP لوكوتورب
هيلي اهل اسرا و لي عمل زاهج MAC ناونع ةطساوب اهل اسرا متي يتلا EPC مزح ىل لصحنو
طقف.

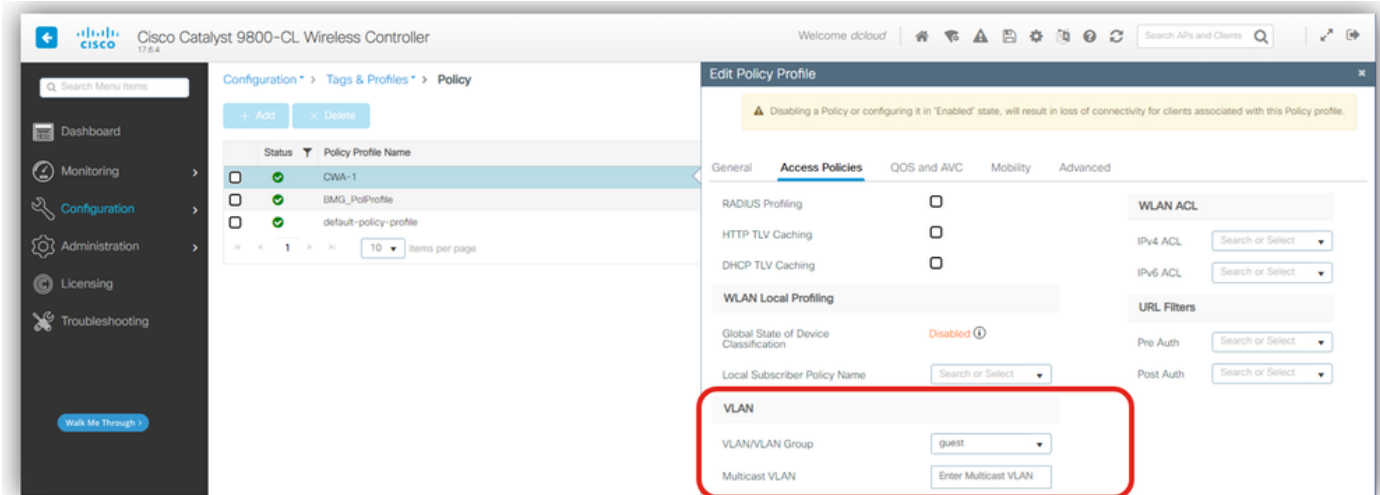
VLAN ةكبش ىل ثبك اهل اسرا متي يتلا DHCP Discover مزحلا ةيؤر اننكمي، لاثمل اذه يف
3: مقر

Inner filters !!

Sent as broadcast on VLAN 3

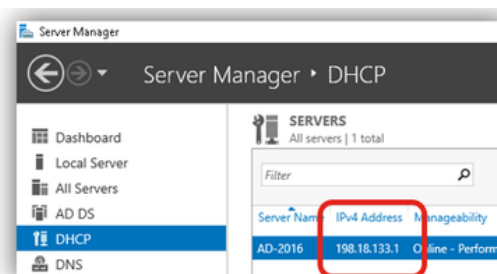
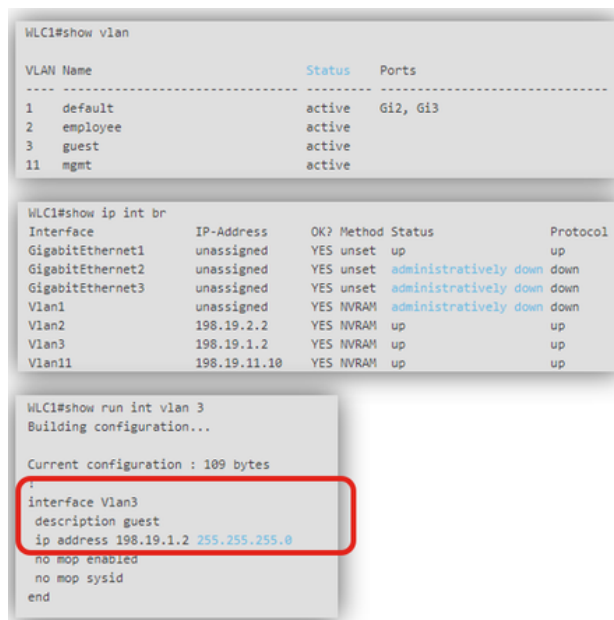
WLC EPC نم ققحتلل DHCP

جهنلا فيرعت فلم يف عقوتملا لي عملاب ةصاخلا VLAN ةكبش ديكأت



ةسايسل فيرعت فلم في VLAN

DHCP subnet: و ليكشت ةطنش switchport و VLAN WLC تققد



If DHCP server is on different subnet we need **ip helper address** on SVI

ةيعرفل DHCP ةكش و switchport و VLAN

امدنع نأ ريغ، 3 VLAN ل SVI يقلت في اضيأ وهو WLC ل في دجاوتي 3 VLAN نأ ىرن نأ نكمي دعاسم ip ةجأب نحن كذلذل، فلتخم ةيعرف ةكبش ىلع وه، ناوئع لدان DHCP ل تققد نحن SVI ل ىلع ناوئع

ةيساسألأ ةينبل في ءالمعلل ةيعرفل تاكبشلل SVI نيوكت تاسرامم للضفأ بلطت (WLC). ةيكلسلال ةيحللم ةكبشل في مكحتل رصنع في اهبئجتو ةيكلسل

هءوحو ناكم نع رظنل لضغب SVI ل ip helper-address رملأ ةفاضل مزلي، تالالال نم ي في

ةسايسل فيرعت فلم في DHCP مءاأل IP ناوئع نيوكت وه ليءبل

```
WLC1#show run int vlan 3
Building configuration...

Current configuration : 141 bytes
!
interface Vlan3
description guest
ip address 198.19.1.2 255.255.255.0
ip helper-address 198.18.133.1
no mop enabled
no mop sysid
end
```

SVI can be at the WLC itself or in the Wired network

Edit Policy Profile

Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General Access Policies QoS and AVC Mobility **Advanced**

WLAN Timeout

Session Timeout (sec) 1800

Idle Timeout (sec) 300

Idle Threshold (bytes) 0

Client Exclusion Timeout (sec) 60

Guest LAN Session Timeout

DHCP

IPv4 DHCP Required

DHCP Server IP Address 198.18.133.1

Fabric Profile

Link-Local Bridging

mDNS Service Policy default-mdns-ser...

Hotspot Server

User Defined (Private) Network

Status

Drop Unicast

DNS Layer Security

DNS Layer Security Not Configured

سایس ال فی رت فل و SVI فی IP دعاسم ناوع

DHCP م داخ ناك اذو ق فاوم نال DHCP لدابت ناك اذ EPC م ادخت ساب ق قحت ال ك لذ دع ك نكمي DNS server: (ني وانع) IP رفوي

test3.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter: <Ctrl>

No.	Time	Source	Destination	Protocol	Length	Info
1	2023-01-13 17:27:49.034986	0.0.0.0	255.255.255.255	DHCP	438	DHCP Discover - Transaction ID 0x3c4037c
2	2023-01-13 17:27:49.034986	0.0.0.0	255.255.255.255	DHCP	352	DHCP Discover - Transaction ID 0x3c4037c
3	2023-01-13 17:27:49.035993	198.19.1.2	198.18.133.1	DHCP	348	DHCP Discover - Transaction ID 0x3c4037c
4	2023-01-13 17:27:49.035993	198.19.1.2	198.18.133.1	DHCP	348	DHCP Discover - Transaction ID 0x3c4037c
5	2023-01-13 17:27:49.037992	198.18.133.1	198.19.1.2	DHCP	355	DHCP Offer - Transaction ID 0x3c4037c
6	2023-01-13 17:27:49.037992	198.18.133.1	198.19.1.2	DHCP	355	DHCP Offer - Transaction ID 0x3c4037c
7	2023-01-13 17:27:49.038904	198.19.1.11	198.19.1.11	DHCP	355	DHCP Offer - Transaction ID 0x3c4037c
8	2023-01-13 17:27:49.038904	198.19.1.11	198.19.1.11	DHCP	428	DHCP Offer - Transaction ID 0x3c4037c
9	2023-01-13 17:27:49.254976	0.0.0.0	255.255.255.255	DHCP	448	DHCP Request - Transaction ID 0x3c4037c
10	2023-01-13 17:27:49.254976	0.0.0.0	255.255.255.255	DHCP	362	DHCP Request - Transaction ID 0x3c4037c
11	2023-01-13 17:27:49.254976	198.19.1.2	198.18.133.1	DHCP	358	DHCP Request - Transaction ID 0x3c4037c
12	2023-01-13 17:27:49.255983	198.19.1.2	198.18.133.1	DHCP	358	DHCP Request - Transaction ID 0x3c4037c
13	2023-01-13 17:27:49.255983	198.18.133.1	198.19.1.2	DHCP	355	DHCP ACK - Transaction ID 0x3c4037c
14	2023-01-13 17:27:49.255983	198.18.133.1	198.19.1.2	DHCP	355	DHCP ACK - Transaction ID 0x3c4037c
15	2023-01-13 17:27:49.256975	198.19.1.2	198.19.1.11	DHCP	355	DHCP ACK - Transaction ID 0x3c4037c
16	2023-01-13 17:27:49.256975	198.19.1.2	198.19.1.11	DHCP	421	DHCP ACK - Transaction ID 0x3c4037c

Frame 5: 355 bytes on wire (2840 bits), 355 bytes captured (2840 bits) on Ethernet II, Src: Vmware_f7:7d:8d (08:0c:29:f7:7d:8d), Dst: Cisco_04:06:ff (00:1e:f6:04:00:00), ID: 3

Internet Protocol Version 4, Src: 198.18.133.1, Dst: 198.19.1.2

User Datagram Protocol, Src Port: 67, Dst Port: 67

Dynamic Host Configuration Protocol (Offer)

Message type: Boot Reply (2)

Hardware type: Ethernet (0x01)

Hardware address length: 6

Hops: 0

Transaction ID: 0x03c4037c

Seconds elapsed: 0

Bootp flags: 0x0000 (Unicast)

Client IP address: 0.0.0.0

Your (client) IP address: 198.19.1.11

Next server IP address: 198.18.133.1

Relay agent IP address: 198.19.1.2

Client MAC address: f2:84:01:57:0d:68 (f2:84:01:57:0d:68)

Client hardware address padding: 00000000000000000000000000000000

Server host name not given

Boot file name not given

Magic cookie: DHCP

Option (53) DHCP Message Type (offer)

Length: 1

DHCP: Offer (2)

Option (1) Subnet mask (255.255.255.0)

Option (58) Renewal Time value

Option (59) Rebinding Time value

Option (51) IP Address Lease Time

Option (54) DHCP Server Identifier (198.18.133.1)

Option (1) Router

Option (6) Domain Name Server

Length: 8

Domain name Server: 8.8.8.8

Domain name Server: 198.18.133.1

Option (15) Domain name

Option (255) End

Full DHCP exchange and DHCP server offering IP and DNS servers

DNS م داخ DHCP ضرع لي صافات

قئ اقل لتال هي جوت ل ا دعاع ش دت له - 7

تام ال عت س ال ا ل ع DNS م داخ در اذ EPC WLC م ادخت ساب ق قحت ال

test4.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter: <Ctrl>

No.	Time	Source	Destination	Protocol	Length	Info
31	2023-01-13 17:36:34.034986	198.19.1.11	8.8.8.8	DNS	171	Standard query 0x3c4037c A connectivitycheck.gstatic.com
32	2023-01-13 17:36:34.034986	198.19.1.11	8.8.8.8	DNS	93	Standard query 0x3c4037c A connectivitycheck.gstatic.com
33	2023-01-13 17:36:34.034986	198.19.1.11	8.8.8.8	DNS	156	Standard query 0x73ab A www.google.com
34	2023-01-13 17:36:34.034986	198.19.1.11	8.8.8.8	DNS	78	Standard query 0x73ab A www.google.com
44	2023-01-13 17:36:34.054989	8.8.8.8	198.19.1.11	DNS	189	Standard query response 0x3c4037c A connectivitycheck.gstatic.com A 142.251.163.94
45	2023-01-13 17:36:34.054989	8.8.8.8	198.19.1.11	DNS	175	Standard query response 0x3c4037c A connectivitycheck.gstatic.com A 142.251.163.94
46	2023-01-13 17:36:34.056988	8.8.8.8	198.19.1.11	DNS	174	Standard query response 0x73ab A www.google.com A 172.253.63.147 A 172.253.63.99
47	2023-01-13 17:36:34.056988	8.8.8.8	198.19.1.11	DNS	248	Standard query response 0x73ab A www.google.com A 172.253.63.147 A 172.253.63.99

Frame 31: 171 bytes on wire (1368 bits), 171 bytes captured (1368 bits) on Ethernet II, Src: Vmware_f7:7d:8d (08:0c:29:f7:7d:8d), Dst: Cisco_04:06:ff (00:1e:f6:04:00:00), ID: 11

802.1Q Virtual LAN, PVID: 0, DEI: 0, ID: 11

Internet Protocol Version 4, Src: 198.19.1.11, Dst: 198.19.1.10

User Datagram Protocol, Src Port: 5256, Dst Port: 5247

Control and Provisioning of Wireless Access Points - Data

IEEE 802.11 QoS Data, Flags:T

Logical-Link Control

Internet Protocol Version 4, Src: 198.19.1.11, Dst: 8.8.8.8

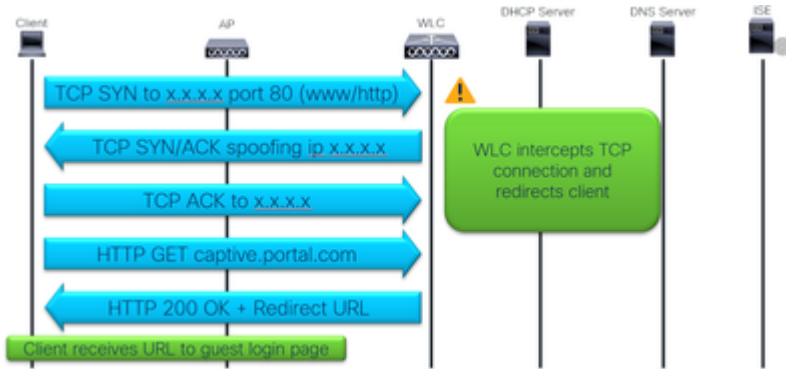
User Datagram Protocol, Src Port: 37404, Dst Port: 53

Domain Name System (Query)

- IP ناونع مَادخِستِ لِوَاوِوِ ضِرْعَتِ سَمَلِ حَتَفَافِ، ةِيئِاقِلَتِ هِيچَوَتِ لِدَاعِ ةِيْلَمَعِ نَكْتِ مَلِ اِذَا 10.0.0.1، لاثَمَلِ لِيْبَسِ لَعِ. يِئِاوشِ عِ
- DNS. لِحِ يِفِ ةَلِكْشِمِ كِيْدَلِ نَوَكْتِ نَأْ لَمَلِ حَمَلِ نَمَفِ، لَمَعَتِ هِيچَوَتِ لِدَاعِ ةِيْلَمَعِ تِنَاكْ اِذَا

لمعت التلزام

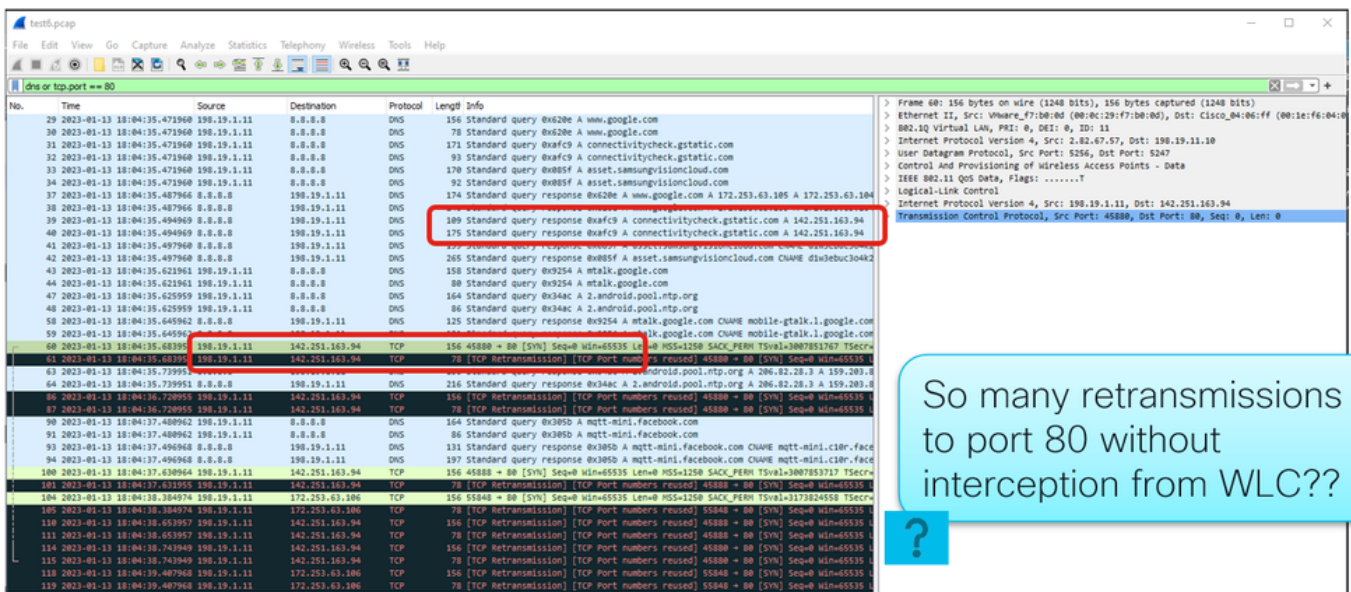
...قفت لاي ف رظن لاي عن انعد



اههيجوت ةداعإو رورملا ةكرح ضارتعا

8 - لو خدلا لي جست ةحفص ضرعت سملا رهظي ال -

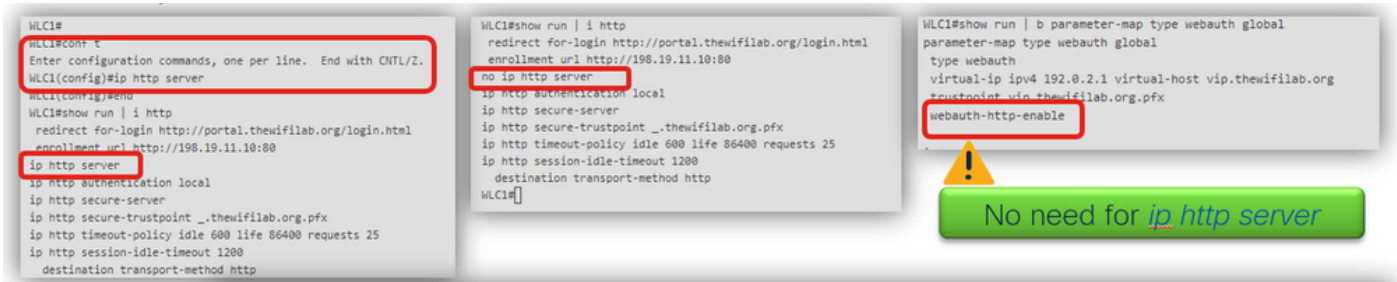
ه:ضارتع اب WLC موقيو 80 ذفنملا ىلإ TCP ماضن لسري ليمعلا ناك اذا امم ققحت



80 ذفنم الى TCP لوكوتورب لاسرا ةداع تاي لمع

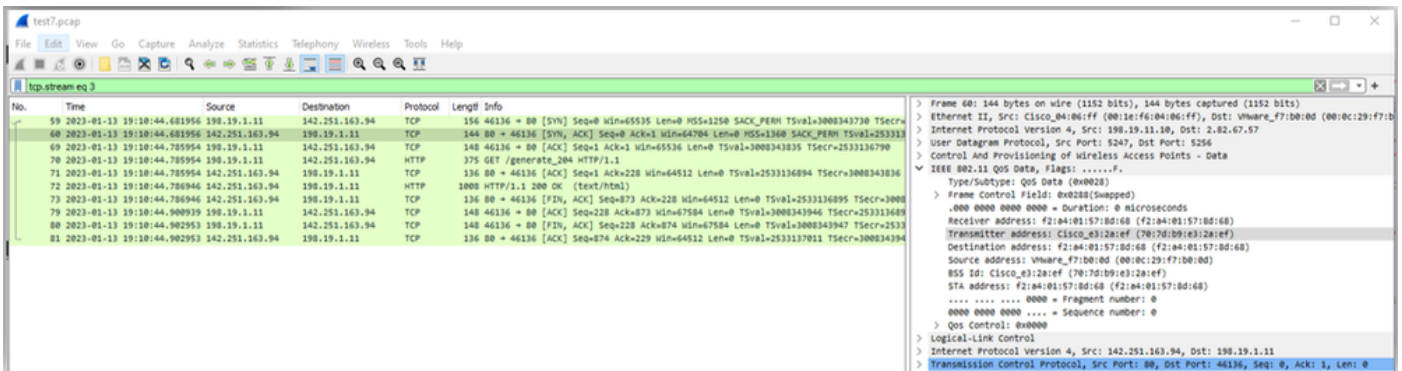
در يلى لصحي ال ه نكلو 80 ذفنم الى TCP syn مزح لسري ليمعلا نأ ىرن نأ اننكمي انه TCP لاسرا ةداعإ موقيو.

parameter-
map global في webAuth-http-enable وأماعل نيوكتل في ip http server رمال كي دل نأ نم دكأت



HTTP ضارعتا رماو

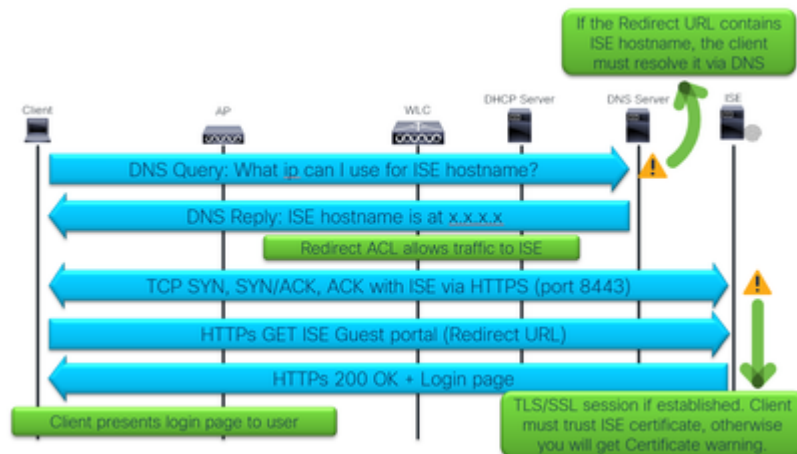
ةداعاو لي م ع ل ا ي ل ع د ر ل ل ة ه ج و ل ل IP ن ا و ن ع ك ة ه ن ت و TCP ل و ك و ت و ر ب WLC ض ر ت ع ت ، ر م ا ل د ع ب ه ي ج و ت ل ل .



WLC ة ط س ا و ب TCP ض ا ر ت ع ا

؟ ل م ع ت ا ل ت ل ز ا م

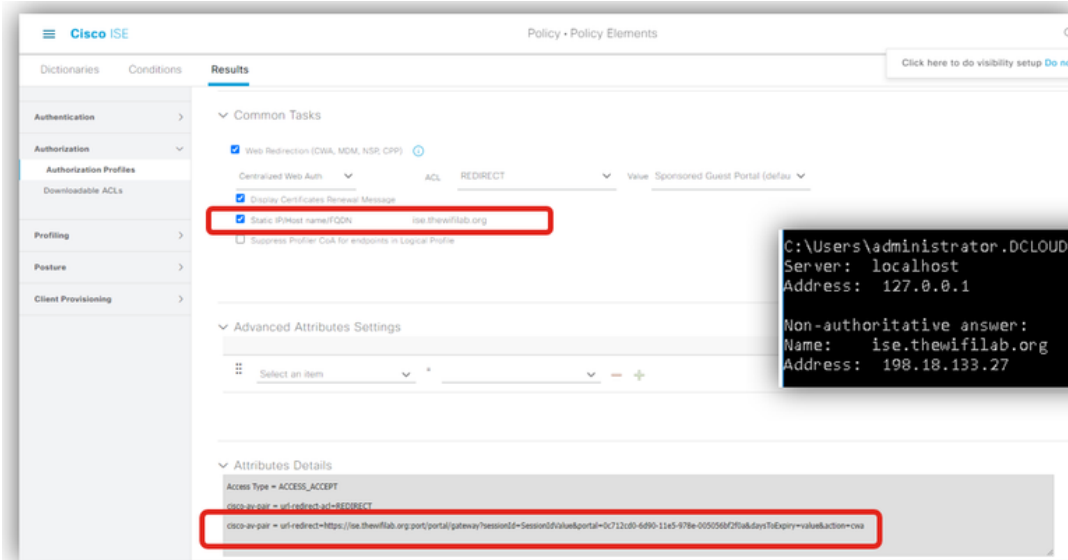
... ق ف د ت ل ا ي ف د ي ز م ل ا ك ا ن ه



ISE في ض لو خ د ل ي ج س ت ة ب ا و ب ل ا ي م ع ل ا ل و خ د ل ي ج س ت

؟ ISE في ض م ل ا م س ا ل ح ل ي م ع ل ل ن ك م ي ل ه - 9

ل ي م ع ل ا ن ا ك ا ذ ا ا م و ف ي ض م ل ا م س ا و IP م د خ ت س ي ه ي ج و ت ل ا ة د ا ع ا ل URL ن ا و ن ع ن ا ك ا ذ ا ا م ق ق ح ت ISE في ض م ل ا م س ا ل ح ب م و ق ي :

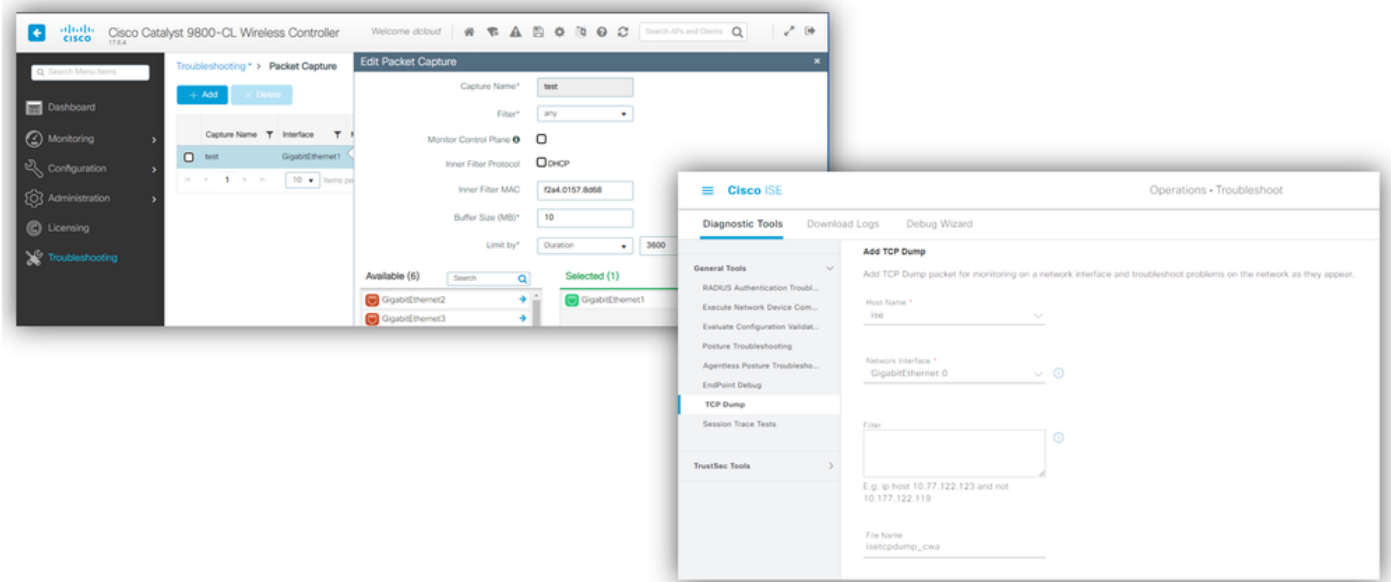


ISE ل فيض الم مسا عقد

عمو، ISE فيض الم مسا لى لع هي جوت ال اداع ال URL ناو نع يوتحي ام دن ع كرت شم ة لك شم ره ظت مادختسا مت اذا. ISE ب صاخ ال IP ناو نع لى اذه فيض الم مسا لى لى لمع ال زا ه لى لع رذعتي ك لى DNS ربع لى L

لمحت ال لو خ دل لى ج ست ة ح فص ت ل ا ز ام له - 10

نيوكت. ISE PSN لى لى لى لمع ال رورم ة ك رح ت ل ص و اذ ISE TCPdump و WLC EPC لى لى نم ق قحت ISE و WLC لى لى لى لى غ ش ت ع د ب و ط ا ق ت ل ل ال ت ا ي ل م ع



WLC EPC و ISE TCPDump

ISE ىرن نأ نكمي انه. رورم ال ة ك رح ط ب ر و ط ا ق ت ل ل ال ت ا ي ل م ع م ج ب م ق ، ة لك شم ال خ س ن د ع ب 8443 ء ا ن ي م لى لى ISE و لى لى لمع ال ن ي ب ل ا ص ت ال ك لى لى د ع ب و ت ل ل ل hostname

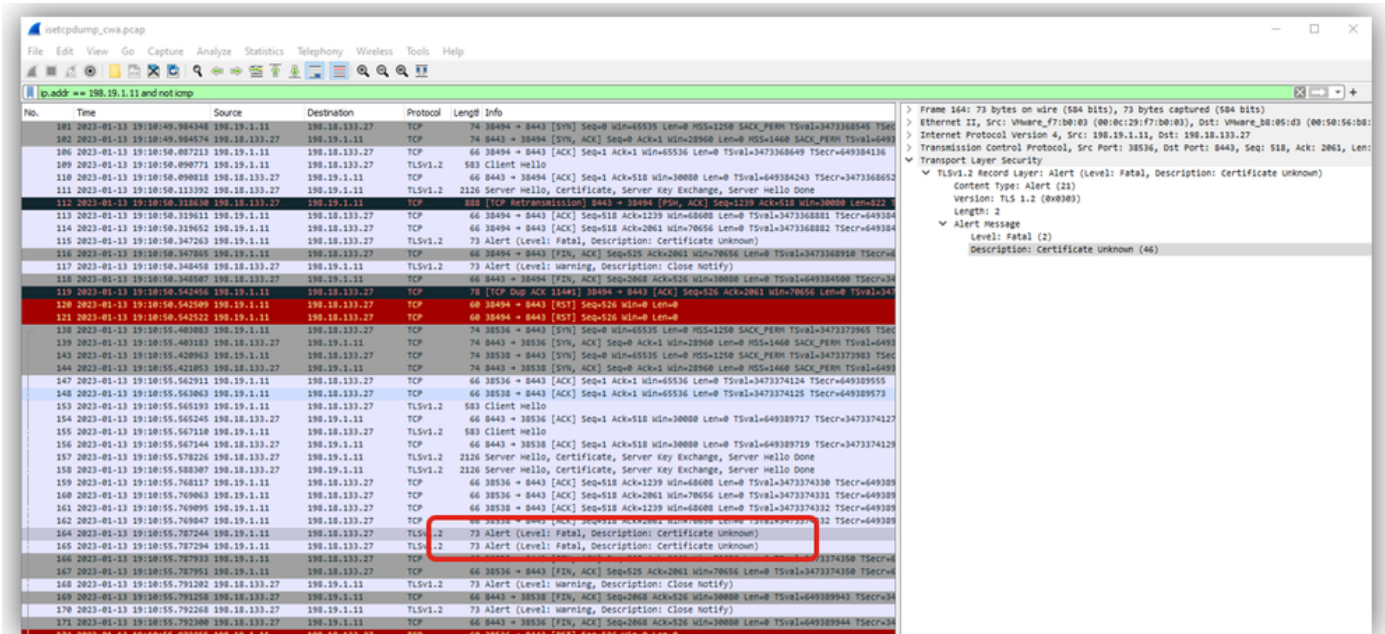
رورم وكح

قدهاشل ب بسب نامألل كهاتنا لىل لصحن اذامل - 11

ريذحت هي جوتب لي عمل موقري نأ عقوتم لم نمف ، ISE لىل اي تاذ عقوتم قدهاش مدخستت اذإ رى ISE Portal لوخذ لي جست ءحفص مي دقت ءلواحم دنع نامأ

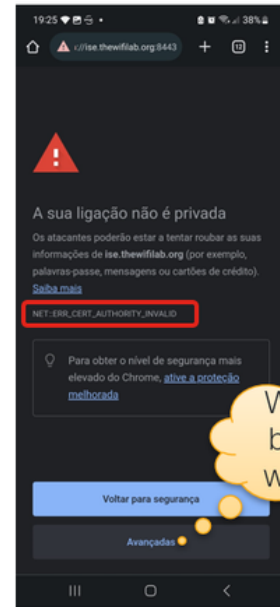
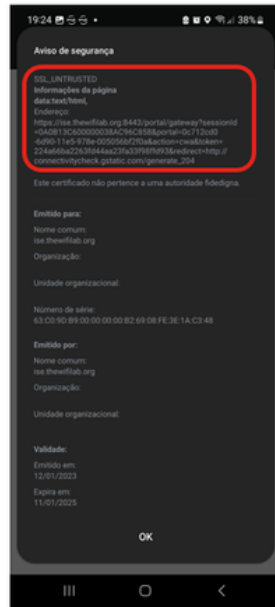
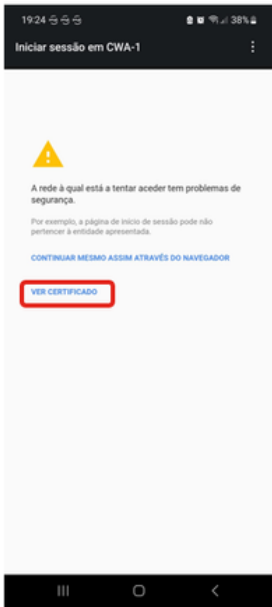
اب قو Thom ISE قدهاش تناك اذإ امم ققحتال ان نكمي ISE TCPdump وأ EPC WLC لىل

فصلو ، تيم (ىوتسم ل) هي بنت عم ليم نم قالغإ لاصتا ءيؤر ان نكمي ، لاثم ل اذه ي (اب قو Thom) ءفورعم ريغ ISE قدهاش نأ ينع ي امم (ءفورعم ريغ قدهاش ل)



اب قو Thom ل ريغ ISE قدهاش

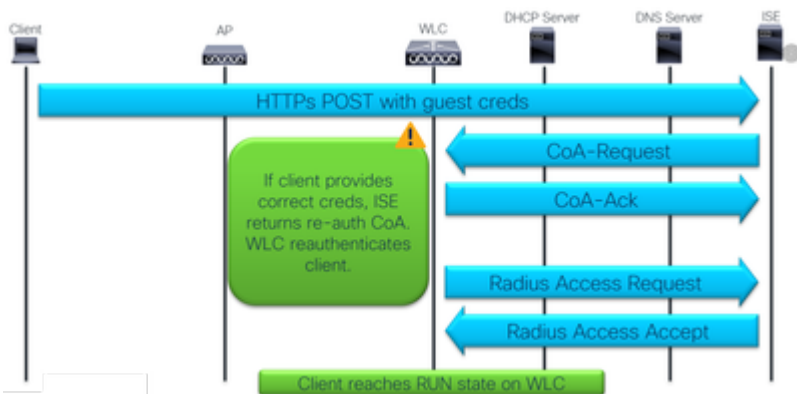
تاجر خم لل ءي لل اتال اى رن س ف ، لي عمل ا بن ا ج نم ققحتال اب انم ق اذإ



ISE ةداهشب قثي ال يذل لي مغل زاهج

...لش في لوخدل لي جس ت نكل !! لمعت هي جوتل ةداع، اريخأ

...ققفدتل نم ققحتل اهي متي ةرم رخآ



CoA لي جس ت و لي مغل ال لوخد لي جس ت

؟فويضل ال لوخد لي جس ت لش ف - 12

دامت عال تانايب ةحص نم دكأت . ةلشاف ةقداصم نع اثحب ISE تالجس نم ققحت

Overview		Steps	
Event	5418 Guest Authentication Failed	5418	Guest Authentication Failed
Username	Cwa		
Endpoint Id	F2-A4:01:57:8D:68 @		
Endpoint Profile			
Authorization Result			

Authentication Details	
Source Timestamp	2023-01-13 21:32:29.201
Received Timestamp	2023-01-13 21:32:29.201
Policy Server	ise
Event	5418 Guest Authentication Failed
Failure Reason	22040 Wrong password or invalid shared secret
Resolution	Check the Device shared secret in Administration > Network Resources > Network Devices and user for credentials.
Root cause	Wrong password or invalid shared secret
Username	Cwa

Make sure you using correct credentials 😊

ةحج حص ريغ دامتعا تانايب ببسب فيضال ةقداصم تلشف

RUN؟ الى لقتنت مل مأ لوخدل ليحست ةيلمع تحجن له - 13

ةحجتنل او ةقداصم ل لوصافات يلع لوصحلل ISE تالچس نم ققحت

Overview		Steps	
Event	5236 Authorize-Only succeeded	11001	Received RADIUS Access-Request
Username	cwa	11017	RADIUS created a new session
Endpoint Id	F2-A4:01:57:8D:68 @	11027	Detected Host Lookup UseCase (Service-Type = Call Check (10))
Endpoint Profile	Android	15049	Evaluating Policy Group
Authentication Policy	Default	15008	Evaluating Service Selection Policy
Authorization Policy	Default >> Redirect-to-Portal	24715	ISE has not confirmed locally previous successful machine authentication for user in Active Directory
Authorization Result	CWAredirect	15036	Evaluating Authorization Policy
		24209	Looking up Endpoint in Internal Endpoints IDStore - cwa
		24211	Found Endpoint in Internal Endpoints IDStore
		15016	Selected Authorization Profile - CWAredirect
		24210	Looking up User in Internal Users IDStore - cwa
		24212	Found User in Internal Users IDStore
		11002	Returned RADIUS Access-Accept

Authentication Details	
Source Timestamp	2023-01-13 21:36:01.8
Received Timestamp	2023-01-13 21:36:01.8
Policy Server	ise
Event	5236 Authorize-Only succeeded
Username	cwa
User Type	User

Result	
User-Name	cwa
Class	CACS:0A0B13C60000003BAD0BF3E4:ise/462943192/128
cisco-av-pair	url-redirect-act=REDIRECT
cisco-av-pair	url-redirect=https://ise.thewifilab.org.8443/portal/gateway?sessionId=0A0B13C60000003BAD0BF3E4&portal=0c712cd0-6d90-11e5-978e-005056b2f0a&action=cwa&token=92eb9963bc6f70c9f82d32ed8a072c6c
cisco-av-pair	profile-name=Android
LicenseTypes	Essential license consumed.

Still getting Redirect-to-Portal ????

هيجوتل ةداع ةقلا

يوتحي يذل ليوختل فيرعت فلم يلع ىرخأ ةرم لصحي ليمعلا ةيؤر اننكمي، لاثملا اذه في في جتني اذه. هيجوتل ةداعل (ACL) لوصول في مكحتل مئاوقو هيجوتل ةداعل URL يلع ةطوشنأ هيجوت ةداعل.

هيجوتل ةداعل لبق Guest_Flow ةدعاقلا صحتف نوكتي نأ بجي. جهنل ةعومجم نم ققحت

Authorization Policy (3)

Status	Rule Name	Conditions	Results
			Profiles Security Groups Hits Actions
✓	Redirect-to-Portal	AND Wireless_MAB Radius-Called-Station-ID CONTAINS CWA	Profiles: CWAredirect x Security Groups: Hits: Actions: PermitAccess x
✓	Guest-Flow	AND Wireless_MAB Guest_Flow	Profiles: PermitAccess x Security Groups: Hits: Actions: DenyAccess x
✓	Default		Profiles: DenyAccess x Security Groups: Hits: Actions:

Other Attributes

ConfigVersionId	83
DestinationPort	1812
Protocol	Radius
NAS-Port	1115
Framed-MTU	1485
OriginalUserName	12a401578d68
NetworkDeviceProfileId	8ade1115-ae11-4a9a-8158-c02e835179db
IsThirdPartyDeviceFlow	false
AuthSessionId	16a1467943192/118
UseCase	Guest Flow
AuthorizationPolicyMatched...	Guest-Flow
EndPointMACAddress	F2-A4-01-57-8D-68
ISEPolicySetName	Default
DTLSSupport	Unknown
HostIdentityGroup	Endpoint Identity Groups: GuestEndpoints

```

client 10.48.39.28

vrf

Mgmt-intf

server-key cisco123

interface GigabitEthernet0
vrf

forwarding

Mgmt-intf

ip address x.x.x.x x.x.x.x

!if using aaa group server:
aaa group server radius group-name
server name nicoISE

ip

vrf

forwarding

Mgmt-intf

ip

radius

source

-interface GigabitEthernet0

```

رارقلا

ةفئاتسملا ةيعجرملا CWA ةمئاق يه هذو:

- DNS و IP ناونع ىلع لصحيو ةحيصل VLAN ةكبش ىلع سلجي ليمعل نا نم دكأت
 - ةلحمل ةكبشلا ي مكحتل رصنع ي ليمعل لىصافت ىلع لصحا

DHCP. لوكوتورب لدابت ضرعل مزحل طاقتل لىغشتب مقو (WLC) ةيكلسلال

- DNS. ربع فيضمل اامسأ لىمعلل نكمي هنا نم ققحت
 - cmd. نم لاصتالا رابتخا فيضم مسا
- 80 ذفنملىل ع WLC تصنت نأ بجي
 - webAuth-http-enable. ةماعل ةململ ةطيرخ رمأ وأ ip http server ماعل رملأ نم ققحت
- ISE. لىل اهب قوئوم ةداهش تيبتب مق ،ةداهشل ريذحت نم صلختلل
 - CWA. في WLC لىل اهب قوئوم ةداهش تيبتتل ةجاح دجوت ال
- مدختسمل لىل روئعل متي مل اذا "ةعباتم" ISE Advanced رايل لىل ةقداصلما جهن
 - مئووقو URL هيجوت ةداعإو لاصتالاب نيوموعدمل فويضلل نيومدختسملل حامسلل (ACL). لوصولل في مكحتلل

اهالصلإو اطاخال فاشكتسأ في ةمدختسمل ةيساسأل تاودألأو

- WLC EPC
 - MAC. ناونع ، DHCP لوكوتورب :ةيلخادل ةيفصللل لماع
- WLC ةشاش
 - لىمعلل نامأ لىصافت نم ققحت
- WLC RA عبتت
 - WLC. بئاح لىل ةيلىصفت تامولعمب اطاخال لىحصت
- ةرشابم ال ISE تالچس
 - ةقداصلل لىصافت
- ISE TCPDump
 - ISE PSN. ةهجاو في مزحل طاقتل لىمجتب مق

عجارملا

[ISE و Catalyst 9800 WLC لىل \(CWA\) بىولل ةيكلرمل ةقداصلل نيوكت](#)

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م ج ر ت
م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م ج ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م م ج ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م ج ر ت ل ا ع م ل ا ح ل ا و ه
ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م ج ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems
(ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا