



Register

Login

Cisco Support Community / Security / AAA, Identity and NAC / Sponsor Approved Guest Access

All community

Options

Search the Community



Welcome to Cisco Support Community. We would love to have your feedback.

For an introduction to the new site, [click here](#). If you'd prefer to explore, try our [test area](#) to get started. And see [here for current known issues](#).



Steven Williams New Member

06-13-2016 01:52 PM

✓ Sponsor Approved Guest Access

I have been at this all day and am struggling a bit. Does anyone have a very detailed doc on setting up sponsor approved Guest access with ISE 2.x and WLC code version 8.2.110.0.

I have gone through the process of setting up the portals to best of my ability. I have my users authenticating with ISE with PEAP for corp wireless so I know that works.

How do I tell WLC/ISE which SSID i am using for guest access? Also should my client get an IP address then be redirected?

I am getting this error on the WLC:

```
*apfReceiveTask: Jun 13 20:37:31.136: %APF-3-CLIENT_NO_ACCESS: apf_80211.c:4285 Authentication failed for client: c0:cc:f8:17:de:25. ACL override mismatch from AAA server.
```

And in splunk I am seeing this:

```
Jun 13 15:50:28 10.20.0.60 Jun 13 15:50:28 ise01 CISE_Passed_Authentications 0000157854 4 0 2016-06-13 15:50:28.428 -05:00 0006695154 5200 NOTICE Passed-Authentication: Authentication succeeded, ConfigVersionId=90, Device IP Address=10.20.63.14, DestinationIPAddress=10.20.0.60, DestinationPort=1812, UserName=C0-CC-F8-17-DE-25, Protocol=Radius, RequestLatency=12, NetworkDeviceName=BNA-WLC2500-01, User-Name=c0ccf817de25, NAS-IP-Address=10.20.63.14, NAS-Port=1, Service-Type=Call Check, Framed-MTU=1300, Called-Station-ID=d8-b1-90-08-87-b0:TEST_GUEST, Calling-Station-ID=c0-cc-f8-17-de-25, NAS-Identifier=_GUEST, Acct-Session-Id=575f1c94/c0:cc:f8:17:de:25/23, NAS-Port-Type=Wireless - IEEE 802.11, Tunnel-Type=(tag=0) VLAN, Tunnel-Medium-Type=(tag=0) 802, Tunnel-Private-Group-ID=(tag=0) 142, cisco-av-pair=audit-session-id=0a143f0e000000f575f1c94, Airespace-Wlan-Id=3, OriginalUserName=c0ccf817de25, NetworkDeviceProfileName=Cisco, NetworkDeviceProfileId=8ade1f15-aef1-4a9a-8158-d02e835179db, IsThirdPartyDeviceFlow=false,
```

I cannot join the SSID from my iphone...but it looks like its trying. I assume an ACL is wrong or a policy is wrong. I think I struggling with VLANs that are pushed to the clients.

Any help would be great thanks..

Solved! [Go to Solution.](#)

AAA Identity and NAC

I have this problem too



0 Helpful

Reply

1 ACCEPTED SOLUTION



Francisco Molino ★ VIP Blue

06-17-2016 08:24 AM

✓ Could you send a screenshot

Could you send a screenshot of the configuration of radius server in the WLC (the detail page please).

Did you take a look on the wlc/monitor clients if the ACL was pushed to authenticated clients ? What's the result?

Thanks

Thanks

Francesco

PS: Please don't forget to rate and select as validated answer if this answered your question



0 Helpful

Reply

37 REPLIES



Francisco Molino ★ VIP Blue

06-13-2016 03:56 PM

Hi

Hi

First of all, if you want to have some documentation from Cisco:

- http://www.cisco.com/c/en/us/td/docs/security/ise/2-0/admin_guide/b_ise_admin_guide_20/b_ise_admin_guide_20_chapter_01110.pdf

- http://www.cisco.com/c/en/us/td/docs/security/ise/2-0/admin_guide/b_ise_admin_guide_20/b_ise_admin_guide_20_chapter_011011.html

If you want to see some videos how to configure it, you can take a look on Labminutes:

- http://www.labminutes.com/sec0197_ise_13_guest_access_sponsored_guest_1

The way you do on ISE 2.0 or ISE 1.3, it's quite the same.

For ACL, you'll need to authorize DHCP, DNS and ISE. All the rest should be denied. If you send a quick drawing with all these informations and your WLC, I can tell you if the ACL is correct or not.

For CoA (authorization acl profile), you need to create ACLs on WLC and just type the EXACT name on your ISE authorization profile.

The other thing that can blocks your Apple iDevices to access webportal (while other standard PC can access) is the certificate. Do you have a valide certificate certified by an Authority or it's a self signed?

On ISE, to do rules on ssid, I'm using policy set feature and create a category based on WLAN_ID (you can found this information on your WLC SSID type, close to the SSID name itself).

I've attached to this post some quick screenshots I done 2 years ago for a colleague to show him how to configure Guest portal. Maybe it could help. Again the way Guest portal works is a little bit different between version (more features) but the minding is quite the same.

I'm sorry but I don't have a ISE lab right now to take some screenshots

Let me know if you need more help.


Thanks.

PS: please don't forget to rate and mark as correct answer if this answer solved your issue

Thanks

Francesco

PS: Please don't forget to rate and select as validated answer if this answered your question

[ise_guest_portal_configuration.pdf](#) 



5 Helpful

Reply



Steven Williams New Member

06-14-2016 07:40 AM

Now on my apple device I am

Now on my apple device I am getting a login window, nothing on it, but errors and says "Hotspot login cannot open the page because the server cannot be found"



0 Helpful

Reply



VIP Francesco Molino  VIP Blue

06-14-2016 10:01 AM

Ok. Is the certificate for

Ok. Is the certificate for guest portal a valid signed certificate by a real authority?

But with Windows and/or Android devices, guest is working fine, isn't it?

Thanks

Thanks

Francesco

PS: Please don't forget to rate and select as validated answer if this answered your question



0 Helpful

Reply



Steven Williams New Member

06-14-2016 10:09 AM

I am getting closer and

I am getting closer and closer here. The issue for the guest login page not coming up was DNS. Is there a way to change the URL for the guest portal?

So now I am on a laptop, I get the guest portal, I say I dont have an account. I register as a user, get my request in the sponsor portal, approve it, login and it seems to be successful.

I get to AUP page and click accept. Then the client is redirected to the guest portal again for re-auth. Here is the log event:

Event 5417 Dynamic Authorization failed

Failure Reason 11213 No response received from Network Access Device after sending a Dynamic Authorization request

Resolution

Check the connectivity between ISE and Network Access Device. Ensure that ISE is defined as Dynamic Authorization Client on Network Access Device and that CoA is supported on device.

Root cause No response received from Network Access Device after sending a Dynamic Authorization request

Steps

11204 Received reauthenticate request

11220 Prepared the reauthenticate request

11100 RADIUS-Client about to send request - (port = 1700 , type = Cisco CoA)

11104 RADIUS-Client request timeout expired ([step latency=10016 ms] Step latency=10016 ms)

11213 No response received from Network Access Device after sending a Dynamic Authorization request



0 Helpful

Reply



VIP Francesco Molino ★ VIP Blue

06-14-2016 10:24 AM

the url is based on what it's

the url is based on what it's set on interface with DNS suffix. You can, on your authorization profile, set the IP address instead of taking dynamically the dns name. It's just for test purpose, I don't recommend going with fix IP for guest redirection.

You are talking about laptop only. Put the IP and test it again with mobile.

The error you're getting is related with CoA and seems that there is an issue between your NAD and ISE:

- your WLC is normally ok as you running a recent aireos version
- How did you configured your SSID?
- could you give the output of radius configuration from your WLC?

If you can't give any screenshots, could you ensure that your SSID configuration looks like this step by step documentation: <http://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115732-central-web-auth-00.html>

Thanks

Thanks

Francesco

PS: Please don't forget to rate and select as validated answer if this answered your question



0 Helpful

Reply



Steven Williams New Member

06-14-2016 01:43 PM

It was a deny from my ISE

It was a deny from my ISE server to the WLC for port 1700. Not sure what thats for.

No I am having an issue with my windows PC that is like caching the username and session.

I have removed the registered user from the sponsor portal and removed the client session from the WLC. It still connects to the SSID and is able to access the internet and doesnt require username and password. I was working fine awhile ago.



0 Helpful

Reply



Steven Williams New Member

06-14-2016 02:14 PM

now this.

now this.

Event 5417 Dynamic Authorization failed

Failure Reason 11103 RADIUS-Client encountered error during processing flow

Resolution Do the following: 1) Verify shared secret matches on the ISE Server and corresponding AAA Client, External AAA Server or External RADIUS Token Server. 2) Check the AAA Client or External Server for hardware problems. 3) Check the network devices that connect the AAA peer to ISE for hardware problems. 4) Check whether the network device or AAA Client has any known RADIUS compatibility issues.

Root cause RADIUS-Client encountered an error during processing flow



0 Helpful

Reply



VIP Francesco Molino ★ VIP Blue

06-14-2016 02:32 PM

the port 1700 is a UDP port

the port 1700 is a UDP port and used for CoA.

You have a firewall in between ISE and WLC? Where this port was blocked?

The error message is due to CoA failure.

- How did you configure WLC for radius?
- What's SSID configuration ?
- If there is a firewall do you have still blocking ports?

Thanks

Francesco

PS: Please don't forget to rate and select as validated answer if this answered your question



0 Helpful

Reply



Steven Williams New Member

06-14-2016 02:40 PM

Yes there was a firewall and

Yes there was a firewall and I opened that port and see allows now in splunk.

What specifics are you looking for about the configuration of the WLC and SSID?

Splunk doesnt show any denys at this point between ISE and WLC and ISE and Client.



0 Helpful

Reply



Francisco Molino VIP Blue

06-14-2016 03:47 PM

There are some ports to open

There are some ports to open on your firewall in order to make a full working ISE solution:

http://www.cisco.com/c/en/us/td/docs/security/ise/1-1-1/installation_guide/ise_install_guide/ise_app_e-ports.html

I would like to have advanced tab configuration of your SSID and Security tab/Authentication and Authorization screenshots.

Thanks

Thanks

Francesco

PS: Please don't forget to rate and select as validated answer if this answered your question



0 Helpful

Reply



Steven Williams New Member

06-16-2016 05:25 AM

The screen on these tabs

The screen on these tabs scroll so difficult to screen shot. But the things that I changed were "Allow AAA Override" and "ISE NAC" for NAC state on the advanced tab.

Security AAA Servers is what i assume you mean, that is just the ISE server in the drop box on ports 1812 and 1813. Nothing else was touched.

It connects to the SSID, I get an IP, and the sponsor portion works great. But after logging into the portal it looks like its going to redirect, but then just brings up the guest portal again and even if i open another browser or tab it goes to the same page, so almost like its not authenticating me.



0 Helpful

Reply



VIP Francesco Molino ★ VIP Blue

06-16-2016 05:29 AM

Ok. Did you tried to force

Ok. Did you tried to force ISE to use IP address? You can change it on the CWA authorization profile. When selecting CWA, you have a field named IP address.

Thanks

Francesco

PS: Please don't forget to rate and select as validated answer if this answered your question



0 Helpful

Reply



Steven Williams New Member

06-16-2016 05:39 AM

DNS is working now. There

DNS is working now. There wasnt an entry in DNS for the ISE server. so thats working. THIS really has my stumped and splunk isnt telling me anything is being blocked.



0 Helpful

Reply



Steven Williams New Member

06-16-2016 05:56 AM

Ok I think I have an idea of

Ok I think I have an idea of whats going on here. But how to fix it. When i look at the radius logs on ISE i see the success on the authorization profile called GUEST_REDIRECT...then the next log comes in (the one that has the error) and its also using the GUEST_REDIRECT....so that might explain why the webpage keeps going back to the guest portal.



0 Helpful

Reply



VIP Francesco Molino ★ VIP Blue

06-16-2016 06:19 AM

Maybe a misconfiguration on

Maybe a misconfiguration on authorization rules. If you can send a screenshot I can help to tell you if this correct

Thanks

Francesco

PS: Please don't forget to rate and select as validated answer if this answered your question

 0 Helpful

Reply



Steven Williams New Member


06-16-2016 06:27 AM

This is what splunk is

This is what splunk is telling me:

```
Jun 16 08:20:50 10.20.0.60 Jun 16 08:20:50 bnapinfise01 CISE_Passed_Authentications 0000240113 4 0 2016-06-16
08:20:50.919 -05:00 0010003406 5236 NOTICE Passed-Authentication: Authorize-Only succeeded, ConfigVersionId=94,
Device IP Address=10.20.63.14, DestinationIpAddress=10.20.0.60, DestinationPort=1812, UserName=swilliams,
Protocol=Radius, RequestLatency=16, NetworkDeviceName=BNA-WLC2500-01, User-Name=c0ccf817de25, NAS-IP-
Address=10.20.63.14, NAS-Port=1, Service-Type=Authorize Only, Framed-MTU=1300, Called-Station-ID=d8-b1-90-08-87-
b0:TEST_GUEST, Calling-Station-ID=c0-cc-f8-17-de-25, NAS-Identifier=_GUEST, Acct-Session-
Id=5762a6f1/c0:cc:f8:17:de:25/60, NAS-Port-Type=Wireless - IEEE 802.11, Tunnel-Type=(tag=0) VLAN, Tunnel-Medium-
Type=(tag=0) 802, Tunnel-Private-Group-ID=(tag=0) 142, cisco-av-pair=audit-session-id=0a143f0e00000305762a6f1,
Airespace-Wlan-Id=3, OriginalUserName=c0ccf817de25, NetworkDeviceProfileName=Cisco,
NetworkDeviceProfileId=8ade1f15-aef1-4a9a-8158-d02e835179db, IsThirdPartyDeviceFlow=false,
```

 authpolicy.jpg 

 0 Helpful

Reply



Francisco Molino  VIP Blue

06-16-2016 08:11 AM

I can't say a lot because I


I can't say a lot because I don't see the conditions exactly what there are referring to.

However, the rule with guest_access must become before the rule giving the redirect. Because you want that authenticated users must access instead of getting a redirect again.

Thanks

Francesco

PS: Please don't forget to rate and select as validated answer if this answered your question

 0 Helpful

Reply



Steven Williams New Member

06-16-2016 08:26 AM

correct and I just fixed that

correct and I just fixed that. Also I have two ACLs on the controller now. One for internet only and one for ISE communication.

Here is what i have gathered.

authenticationpolicy.jpg

wlc_acls.jpg

wlans_advanced.jpg

authpolicy_0.jpg

authproinetonly.jpg

authprocwa.jpg



0 Helpful

Reply



Francisco Molino VIP Blue

06-16-2016 08:32 AM

Now it looks correct. Does it

Now it looks correct. Does it works ?

Thanks

Francesco

PS: Please don't forget to rate and select as validated answer if this answered your question



0 Helpful

Reply



Steven Williams New Member

06-16-2016 08:58 AM

No still doesnt work. BUt

No still doesnt work. BUt something did change. After the login is successful by the client it doesnt redirect to the guest portal again, it just fails and the internet doesnt work, then if i open a browser again the guest page comes up again. so it looks like redirect loop is solved.



0 Helpful

Reply



Steven Williams New Member

06-16-2016 09:00 AM

6/16/16 10:15:51.000 AM

6/16/16 10:15:51.000 AM	Jun 16 10:15:51 10.51.100.42 %ASA-6-106015: Deny TCP (no connection) from 10.20.0.60/8443 to 1 • host = 10.51.100.42 • source = udp:514 • sourcetype = cisco:asa
6/16/16 10:15:44.000 AM	
6/16/16 10:15:28.000 AM	
6/16/16 10:15:21.000 AM	
6/16/16 10:15:14.000 AM	
6/16/16 10:15:05.000 AM	



0 Helpful

Reply



Steven Williams New Member

06-16-2016 09:02 AM

the client and ISE are trying

the client and ISE are trying to communicate over port 8443? Why is the client trying to reach into ISE for this? I cant create a rule in the firewall that states allow ISE on 8443 to any destination....



0 Helpful

Reply



Francisco Molino

06-16-2016 10:34 AM

Hi,

Hi,

I'm on meeting all the day and I'll have a look this evening.

However to answer your question, about port 8443, this is the standard ISE port for Guest, sponsor, device portal

Thanks

Francesco

PS: Please don't forget to rate and select as validated answer if this answered your question

 0 Helpful

Reply



VIP Francesco Molino  VIP Blue

06-16-2016 01:44 PM

Ok i read your last posts. We

Ok i read your last posts. We are moving to the next step.

When user is authenticated, do you see on ISE that it's pushing the right authorization profile?


On the wlc, do you see the right acl placed for this particular guest?

Could you drop a screenshot of your acl internet-only?

Thanks

Francesco

PS: Please don't forget to rate and select as validated answer if this answered your question

 0 Helpful

Reply



Steven Williams New Member

06-16-2016 02:02 PM

Here is the internet only acl 

Here is the internet only acl

 internetonlyacl.jpg 

 0 Helpful

Reply



VIP Francesco Molino  VIP Blue

06-16-2016 02:55 PM

Why are you denying dns and

Why are you denying dns and dhcp?

Thanks

Francesco

PS: Please don't forget to rate and select as validated answer if this answered your question

 0 Helpful

Reply



Steven Williams New Member

06-17-2016 06:05 AM

Fixed that, it was because

Fixed that, it was because when you create the rule its automatically set to deny, so I always forget that. Everything else seems to be ok though no?

 0 Helpful

Reply



Francesco Molino  VIP Blue

06-17-2016 06:31 AM


I don't know your exact

I don't know your exact design. However I will add as permit the next hop (Gateway IP of the Guest vlan) as inbound.

Thanks

Francesco

PS: Please don't forget to rate and select as validated answer if this answered your question

 0 Helpful

Reply



Steven Williams New Member

06-17-2016 07:37 AM

the guest vlan is 142 (10.20

the guest vlan is 142 (10.20.42.0) so wouldnt the last rule accomplish this?

also from the client i can ping the controller IP but not the SVI

 0 Helpful

Reply

ASA NAT 8.3+ - NAT Operation and Configuration Format (CLI)

Created by Jouni Forss on 03-20-2013 12:55 PM

40 161

Table of ContentsIntroductionVersion HistoryPossible Future UpdatesDocuments PurposeNAT Operation in ASA 8.3+ SectionsRule Types Network Object NATtwice NAT / Manual NATRule Types used per SectionNAT Types used with Twice NAT / Manual NAT and Network Obje... [view more](#)

How Does NAT-T work with IPSec?

Created by athukral on 05-23-2011 01:20 AM

22 150

Table of Contents Introduction:This document describes details on how NAT-T works. Background: ESP encrypts all critical information, encapsulating the entire inner TCP/UDP datagram within an ESP header. ESP is an IP protocol in the same sense that TCP an... [view more](#)

ASA Pre-8.3 to 8.3 NAT configuration examples

Created by Magnus Mortensen on 05-12-2010 09:06 AM

52 86

Static NAT/PAT Pre-8.3 NAT8.3 NATRegular Static NAT static (inside,outside) 192.168.100.100 10.1.1.6 netmask 255.255.255.255 object network obj-10.1.1.6 host 10.1.1.6 nat (inside,outside) static 192.168.100.100 Regular Static PAT static (inside,outside) t... [view more](#)



569
VIEWS



5
HELPFUL



37
REPLIES

Recommended

Cisco ISE Guest Sponsor Portal Issue

Pranav Gade

ISE 1.3 Sponsor Portal.

graham.harper

ISE1.3でのSponsor/Guest Portal URLの変更

hiryokoy

ISE 1.4 Sponsor Portal Guests Accounts

James Davies

Add Approved URLs on SA540 Security App...

smallbusiness

Popular Blogs

AnyConnect Certificate Based Authentication.

Created by Marvin Ruiz on 08-27-2012 05:20 PM

36 60

BLOG (No Title)

Created by athukral on 06-14-2011 04:23 AM

15 35

Wireless Hacking

Created by Anim Saxena on 01-24-2013 07:56 AM

2 20



[Contacts](#)
[Feedback](#)
[Site Map](#)
[Terms & Conditions](#)

[Privacy Statement](#)
[Cookie Policy](#)
[Trademarks](#)
[Help](#)

