Barracuda XDR ATR – Troubleshooting Topics

FortiGate Firewall:

Status '0': Failed to open TCP connection to X.X.X.X:XXX (execution expired)

1. Verify the port used for API calls

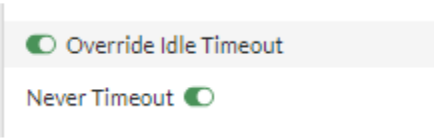
Ask the customer to verify which port is used for API calls. They must input the correct port number in the firewall SOAR settings on the CSD.

1. Navigate to **System** > **Settings > Administration Settings.**
2. Make note of the **HTTPS port**. This will be the port that is used to make API calls for SOAR.
3. The customer must input the port number in the SOAR config settings on the CSD.
4. Please have the customer test the connection from the CSD with the correct port value. If the issue persists, move on to the next troubleshooting step.

2. Check the timeout settings for the XDR admin profile

Ask the customer to enable Override Idle Timeout & Never Timeout.

1. Navigate to **System** > **Admin Profiles** > **(Your REST API Admin Profile)**
2. Scroll down to **Override Idle Timeout** and slide the toggle to **On**. Then slide **Never Timeout** to **On**.



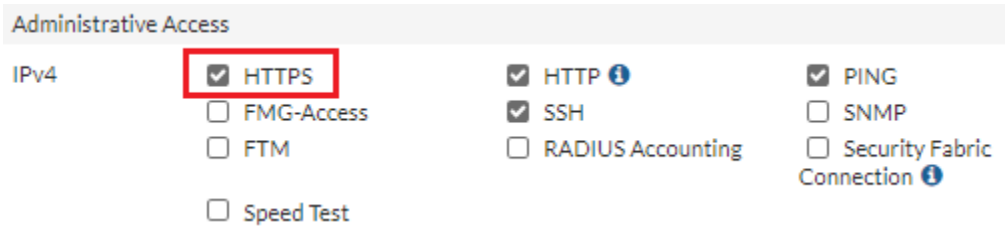
3. Once the customer makes these changes, please have them test the connection again from the CSD.

3. Create a NAT rule to permit traffic from our SOAR endpoint to the firewall

If you have a firewall placed in front of your FortiGate device, you will need to make sure there is a policy in place on that firewall to allow the traffic from our SOAR endpoint to the FortiGate device. The firewall could be blocking API requests if they do not allow admins to log in from the public IP, only the management IP of the device. If this is the case, the customer will need to make sure that they set up a NAT forwarding rule on the firewall to allow traffic from our endpoints (44.239.173.232 & 35.155.74.247) to the management IP.

4. Ensure HTTPS is enabled on the WAN Interface

Admin access from the WAN interface is needed for XDR to have remote access to the firewall device. You can manage these settings by navigating to **Network > Interfaces** and adjusting the administrative access to the interface.

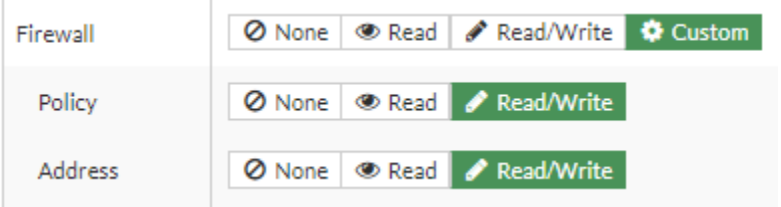


5. Ensure the SOAR IP is added as a trusted host to the system administrator account

The XDR REST API admin needs to be able to communicate and authenticate to the firewall. If you are restricting admin logins to only certain networks, you must add the SOAR IP (44.239.173.232 & 35.155.74.247) as a trusted host to the administrator account.

Error 401: This server could not verify that you are authorized to access the document requested. Either you supplied the wrong credentials (e.g., bad password), or your browser doesn't understand how to supply the credentials required.

1. Check the REST API firewall permissions to ensure the API admin user can make the appropriate changes on the firewall.
    a. Navigate to **System** > **Admin Profiles** > **(Your REST API Admin Profile) > Access Permissions.**
    b. Under **Access Control**, go to the **Firewall** section, and make sure the API admin user can **Read/Write** for **Policy** and **Address** actions.



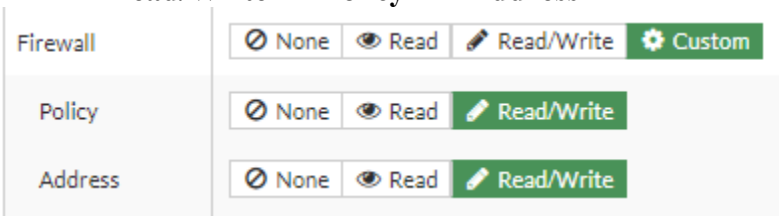
Error 403: This error occurs when the user making the API call does not have the necessary permissions.

1. Verify that the XDR admin user still has the necessary permissions to make API calls to the firewall.

Ask the customer to verify that the XDR admin user still has the necessary permissions to make API calls to the firewall. This would require checking the REST API firewall permissions (similar to the 401 error):

1. Navigate to **System** > **Admin Profiles** > **(Your REST API Admin Profile) > Access Permissions.**

2. Under **Access Control**, go to the **Firewall** section, and make sure the API admin user can **Read/Write** for **Policy** and **Address** actions.



3. Once the customer makes these changes, please have them test the connection from the CSD. If the issue persists, move on to the next troubleshooting step.

2. Regenerate a new REST API KEY

Have the customer regenerate a new API Key for the XDR admin and upload the new value to the SOAR config on the CSD.

1. Navigate to **System** > **Administrators > (Your REST API Administrator).**
2. Go to API Key and click **Regenerate**.
3. Save the new API key in a safe place.
4. Upload the new API key to the SOAR config page on the CSD.
5. Once the customer updates the SOAR data, please have them test the connection again.

Additional FortiGate References:
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/399023
https://community.fortinet.com/t5/FortiGate/Troubleshooting-Tip-Rest-API-response-error-codes/ta-p/202126

Cisco Meraki Firewall:

Error 404: Authentication issue

1. Make sure the Organization ID and Policy Object Group Name are input correctly in the SOAR settings page on the CSD.

Error 401: Invalid API Key

1. Ensure the API Key is input correctly in the CSD.

If the issue persists, they might need to generate a new API key and test the configuration again. They can create the new API key by performing the following steps:

1. Navigate to the profile page by clicking on your account email address in the upper right. Then click **My profile**.
2. Scroll down to **API Access** to generate the API key.
3. Copy, then store the API key in a safe place.
4. Click **Done**.
5. Upload the new API key to the SOAR config page on the CSD.
6. Once the customer updates the SOAR data, please have them test the configuration again.

2. Ensure XDR has the necessary permissions to make API calls to the firewall.

Error 400 (Policy Object): Name already exists, please use a different name

1. The IP has already been added as a Policy Object on the Meraki Dashboard. It could have been manually added by the customer for testing purposes, etc. However, this does not necessarily mean that the IP has already been added to the XDR Blocked IPs Group that the customer is required to set up for SOAR.
    - **Resolution**: Barracuda XDR will attempt to add the existing IP (Policy Object) to the Policy Object Group "XDR Blocked IPs Group". If we get an error when trying to add the IP to the group, then we can confirm if it's because the IP has already been added to the Policy Object Group OR there could be another issue.

Error 400 (Policy Object Group): The Policy Object Group is not found for this organization

1. Please ensure that a Policy Object Group has been created for XDR, and that the group name is input correctly in the SOAR settings page on the CSD.

Additional Meraki References:
https://developer.cisco.com/meraki/api-v1/create-organization-action-batch/

https://developer.cisco.com/meraki/api-v1/authorization/#obtaining-your-meraki-api-key
https://documentation.meraki.com/MX/Firewall_and_Traffic_Shaping/MX_Firewall_Settings#Forwarding_rules
https://documentation.meraki.com/General_Administration/Tools_and_Troubleshooting/Troubleshooting_Group_Policies

Barracuda CloudGen Firewall:

Status '0': Failed to open TCP connection (Connection refused)

1. Ensure the REST API service is enabled on the firewall box level (for both Control Center & Standalone), and that the customer is using the correct Access Token.

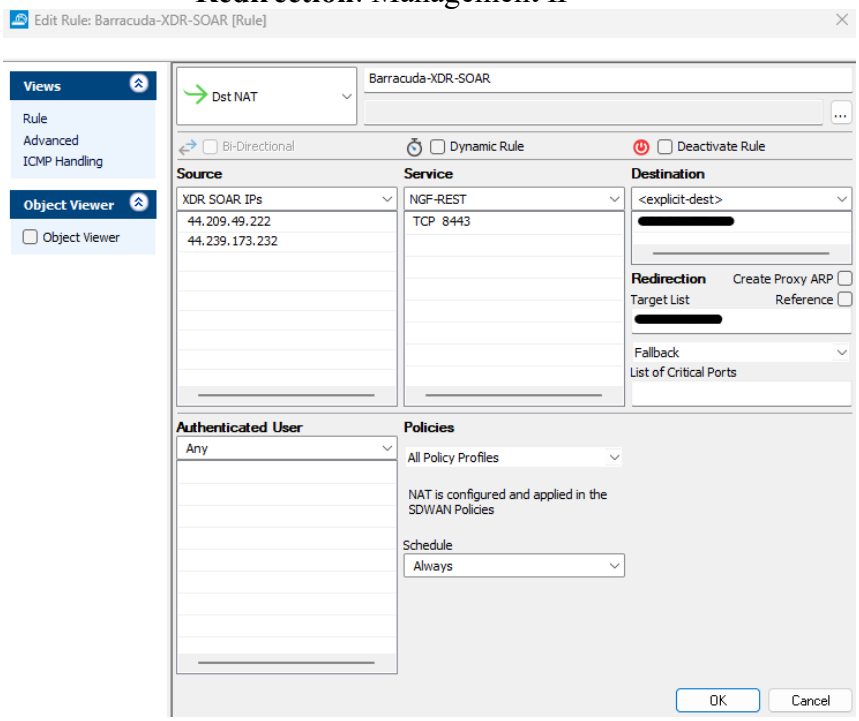
Instructions to enable the REST API and Generate an Access Token:

- Control Center: https://campus.barracuda.com/product/xdr/doc/171507744/setting-up-soar-for-barracuda-cloudgen-control-center-firewall
- Standalone: https://campus.barracuda.com/product/xdr/doc/171509960/setting-up-soar-for-barracuda-cloudgen-standalone-firewall/

2. Ensure communication is allowed from the XDR SOAR IP to the CloudGen firewall

A customer might have a firewall in front of their CloudGen device. If this is the case, a NAT port forward rule will need to be set up on that firewall to allow traffic from our SOAR endpoint to the management IP of the Control Center or (if it's a Standalone FW) the management IP of the box.

- For example, if the firewall in front is also a CloudGen, you could create a destination NAT forwarding rule that would have the source be our SOAR endpoint, the service be TCP 8443, and the destination would be the firewalls public IP address. The Redirection would be the management IP of the Control Center or Standalone.
    - **Type**: Dst NAT
    - **Source**: 44.239.173.232 & 35.155.74.247
    - **Service**: TCP 8443
    - **Destination**: Public IP address of the firewall
    - **Redirection**: Management IP



Status '0': Failed to open TCP connection to X.X.X.X (execution expired)

This typically indicates that the firewall was unable to establish a TCP connection with the target service, and the connection attempt timed out or was aborted before it could be completed. Possible causes for this error include:

1. **Network Connectivity Issues**: There may be network connectivity problems between the firewall and the destination service. This could be caused by issues with routing, DNS resolution, network outages, or physical network problems.
2. **Firewall/Access Control List (ACL) Settings**: The firewall might be blocking the connection based on its configured rules. The destination server or port might be blocked by security policies or access controls on the firewall.
3. **Server/Service Unavailability**: The server trying to connect to might be down, overloaded, or unreachable due to problems such as service crashes, misconfigurations, or capacity limits.
4. **Timeout Configuration**: The TCP connection might take too long to establish, and the configured timeout period may expire before the connection is successfully made.
5. **Overloaded or Unresponsive Proxy or Load Balancer**: If the firewall is acting as a proxy or there is a load balancer between the firewall and the destination service, it could be overwhelmed, misconfigured, or experiencing performance degradation.

Troubleshooting steps that can potentially help resolve the issue include the following:

1. **Check Network Connectivity**: Verify the network path and connectivity between the firewall and the XDR SOAR service.
2. **Firewall and Security Group Rules**: Check the firewall rules and ensure that the firewall is not blocking outbound connections to the IP address and port of the XDR SOAR service.
3. **Check Server Availability**: Ensure the firewall is up and running, and that there are no outages or maintenance periods affecting it.
4. **Review Timeout Settings**: Review timeout settings and increase them if necessary to account for longer connection establishment times.

Error 404: Network object not found

This typically indicates that the firewall is unable to locate or resolve a specific network object or resource that is being referenced in the configuration. This could be due to a potentially mistyped network name, a deleted network, or an incorrect configuration. Please verify the following:

1. Check the CloudGen firewall's configuration interface to confirm the network object still exists and is properly configured.
2. Review the network object you are using for SOAR and make sure there are no typos in the name.
3. Make sure the XDR team has the appropriate permissions to access the network via API.
    a. The XDR Admin user you created for SOAR will need to have API access to interact with and modify the network object configuration.

Additional CloudGen References:

- https://campus.barracuda.com/product/cloudgenfirewall/api

SonicWall Firewall:

Error 404: Command 'address-group ipv4 name XXX' is not found

1. Please ensure that an Address Group has been created for XDR SOAR, and that the Group name is input correctly in the SOAR settings page on the CSD.
    - Instructions on how to create an Address Group - https://campus.barracuda.com/product/xdr/doc/171509992/setting-up-soar-for-sonicwall-firewall/
2. Make sure the Address Group is considered an ipv4 group

When you create the Address Group, you initially must add something to it (ipv4, ipv6, MAC address, etc.). By default, the customer should add an IPv4 address to the group when creating it.

Error 405: Non config mode

1. Check the Admin Configurations on the firewall

This usually happens when another admin is logged into the firewall at the same time. If they do not have the option set to "preempt another admin user", then we will not be able to login with config mode and perform remediation actions on the firewall.

- Reference: https://www.sonicwall.com/support/technical-documentation/docs/sonicos-7-0-0-0-device_settings/Content/Topics/System_Administration/Multiple_Administrator/multi-administrator-configuration.htm/

Additional SonicWall References:

- https://www.sonicwall.com/support/technical-documentation?language=English&category=Firewalls&product=NSv%20Series&product_model=NSv%20270&resources=Getting%20Started%20Guide
- https://www.sonicwall.com/support/knowledge-base/introduction-to-sonicos-api/200818060121313#Resolution1
- https://www.sonicwall.com/support/knowledge-base/understanding-address-objects-in-sonicos/170504660027820
- https://www.sonicwall.com/support/technical-documentation/docs/sonicos-7-0-0-0-device_settings/Content/Topics/System_Administration/Multiple_Administrator/multi-administrator-configuration.htm
- https://www.sonicwall.com/support/knowledge-base/how-can-i-restrict-admin-access-to-the-device/170503259079248#Resolution1
- https://www.sonicwall.com/support/knowledge-base/troubleshooting-user-cannot-log-in-the-firewall/170503807107288#Resolution1
- https://blog.airbrake.io/blog/http-errors/403-forbidden-error
- https://www.sonicwall.com/support/knowledge-base/what-is-the-maximum-and-optimal-address-object-group-size/210610153801983

3175 Winchester Blvd. | Campbell, CA | 95008 | +1 888 268 4772 | barracuda.com