How to Configure Inbound SSL Inspection

https://campus.barracuda.com/doc/73703652/

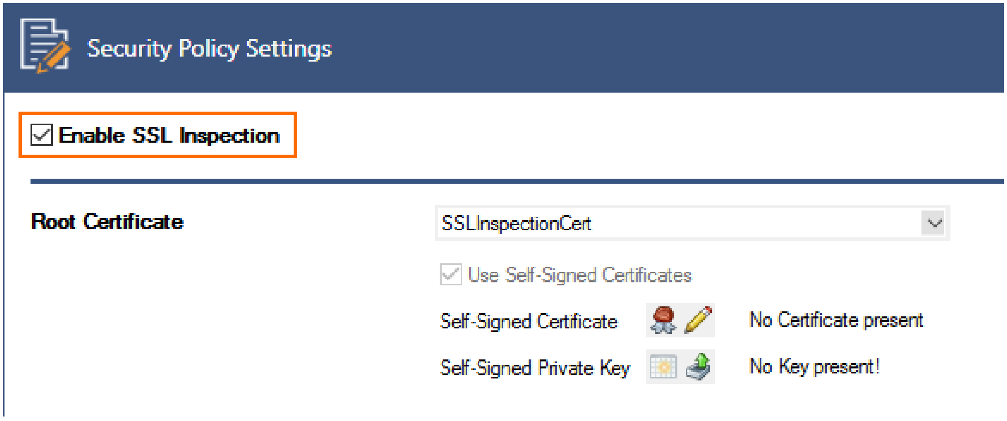
Inbound SSL Inspection allows the firewall to decrypt and secure inbound SSL or TLS connections to servers or services behind the firewall. The firewall uses the server's SSL certificate to terminate the connection. This allows the firewall to define the allowed cipher sets and minimum SSL or TLS version used for the connection. The traffic is then scanned, and the configured policies are applied. The firewall then creates an SSL connection to the server and forwards the traffic to its destination.

Before You Begin

- Verify that the **Firewall Feature** level is set to **7.2** or higher.
- Create an SSL Inspection policy for inbound SSL Inspection. For more information, see How to Create an SSL Inspection Policy for Inbound SSL Inspection.

Step 1. Enable SSL Inspection

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > Firewall > Security Policy**.
2. Click **Lock**.
3. Select the **Enable SSL Inspection** check box.



Security Policy Settings

☑ Enable SSL Inspection

Root Certificate: SSLInspectionCert

☑ Use Self-Signed Certificates

Self-Signed Certificate: No Certificate present

Self-Signed Private Key: No Key present!

4. Click **Send Changes** and **Activate**.

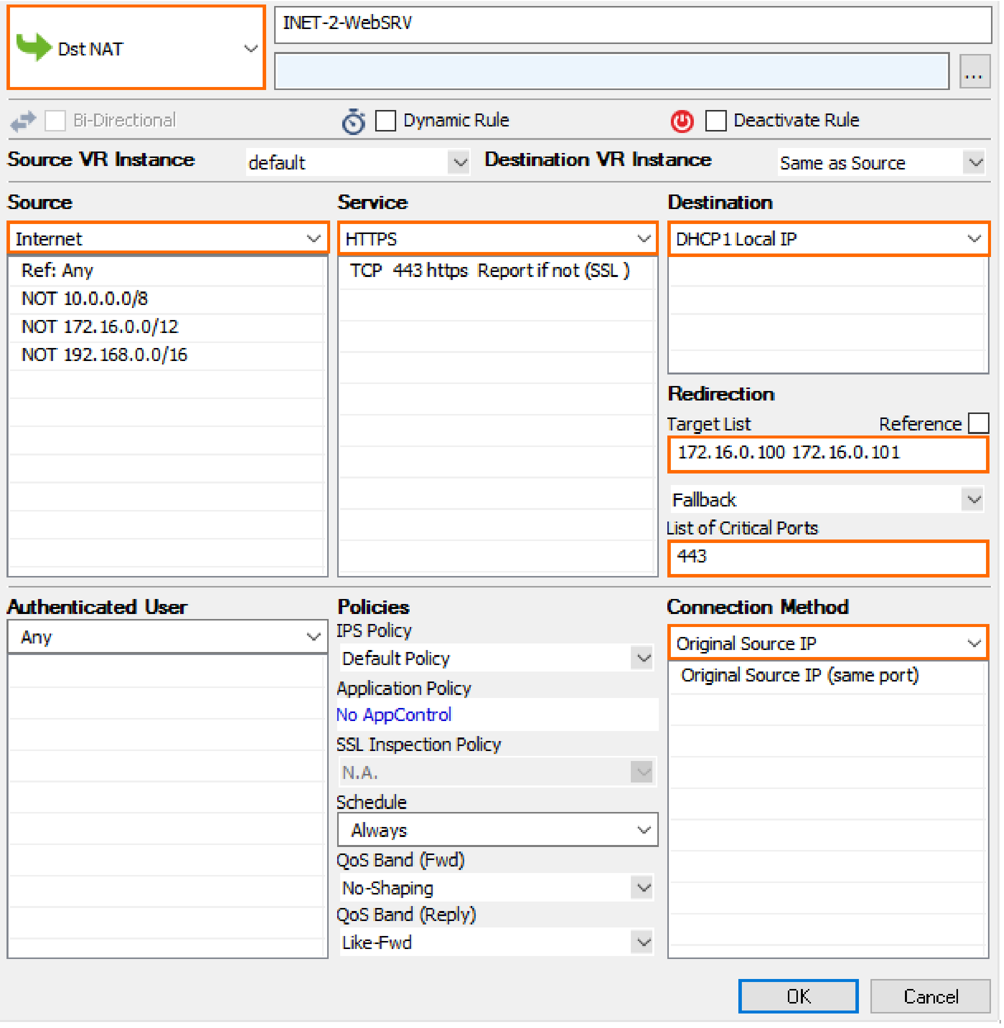
Step 2. Create Access Rule with Inbound SSL Inspection

Enable SSL Inspection on the Dst NAT access rule forwarding traffic to the internal server.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual**

server > Assigned Services > Firewall > Forwarding Rules.

2. Click **Lock**.
3. Either click the plus icon (**+**) in the top right of the ruleset, or right-click the ruleset and select **New > Rule**.
4. Select **Dst NAT** as the action.
5. Enter a **Name** for the rule.
6. Specify the following settings that must be matched by the traffic to be handled by the access rule:
    - **Source** – Select **Internet**.
    - **Destination** – Select the network object containing the external IP address of the firewall.
    - **Service** – Select the service(s) for which inbound SSL inspection should be used. For example, select **HTTPS**.
    - **Target List** – Enter the internal IP address(es) of the server, or a select a network object containing the web server IP addresses. For more information, see [How to Create a Destination NAT Access Rule]().
    - **Connection Method** – Select **Original Source IP**.



Dst NAT
INET-2-WebSRV
☐ Bi-Directional ☐ Dynamic Rule ☐ Deactivate Rule
Source VR Instance default **Destination VR Instance** Same as Source

Source
Internet
Ref: Any
NOT 10.0.0.0/8
NOT 172.16.0.0/12
NOT 192.168.0.0/16

Service
HTTPS
TCP 443 https Report if not (SSL)

Destination
DHCP1 Local IP

Redirection
Target List: 172.16.0.100 172.16.0.101
Reference ☐
Fallback
List of Critical Ports: 443

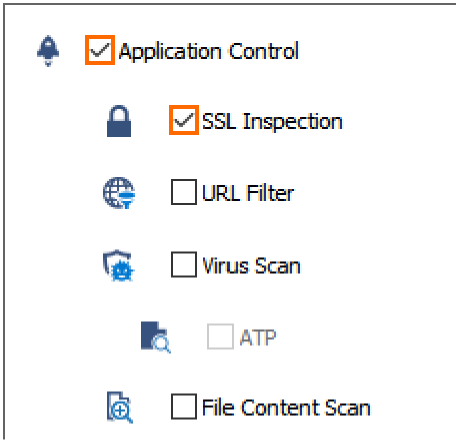
Authenticated User
Any

Policies
IPS Policy: Default Policy
Application Policy: No AppControl
SSL Inspection Policy: N.A.
Schedule: Always
QoS Band (Fwd): No-Shaping
QoS Band (Reply): Like-Fwd

Connection Method
Original Source IP
Original Source IP (same port)

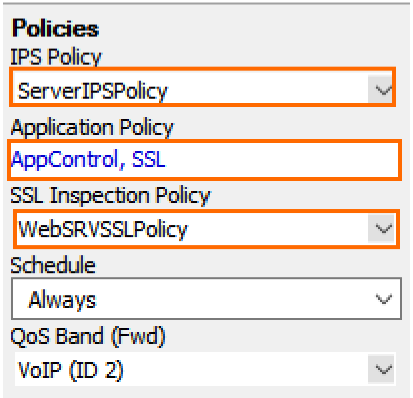
7. From the **IPS Policy** drop-down list, select the IPS policy.
8. Click the **Application Policy** link and select:

  - **Application Control** – Required.
  - **SSL Inspection** – Required.
  - **Virus Scan** – Optional.
  - **ATP** – Optional.
  - **File Content Scan** – Optional.



☑ Application Control
☑ SSL Inspection
☐ URL Filter
☐ Virus Scan
☐ ATP
☐ File Content Scan

9. From the **SSL Inspection Policy** drop down list, select an SSL Inspection policy for inbound inspection. For more information, see How to Create an SSL Inspection Policy for Inbound SSL Inspection.



Policies
IPS Policy: ServerIPSPolicy
Application Policy: AppControl, SSL
SSL Inspection Policy: WebSRVSSLPolicy
Schedule: Always
QoS Band (Fwd): VoIP (ID 2)

10. Click **OK**.
11. Click **Send Changes** and **Activate**.

Incoming SSL or TLS connections are now terminated on the firewall before being forwarded to the internal server.

Monitoring and Troubleshooting

SSL Inspection error messages are written in the Firewall/SSL.log file. On the **FIREWALL > Live** page, the **State** column shows the padlock (🔒) icon for SSL-inspected connections.

Figures

1. inbound_SSL_Inspection_01.png
2. inbound_SSL_Inspection_02.png
3. inbound_SSL_Inspection_03.png
4. inbound_SSL_Inspection_04.png
5. padlock.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.