How to Detect and Block DNS Tunneling

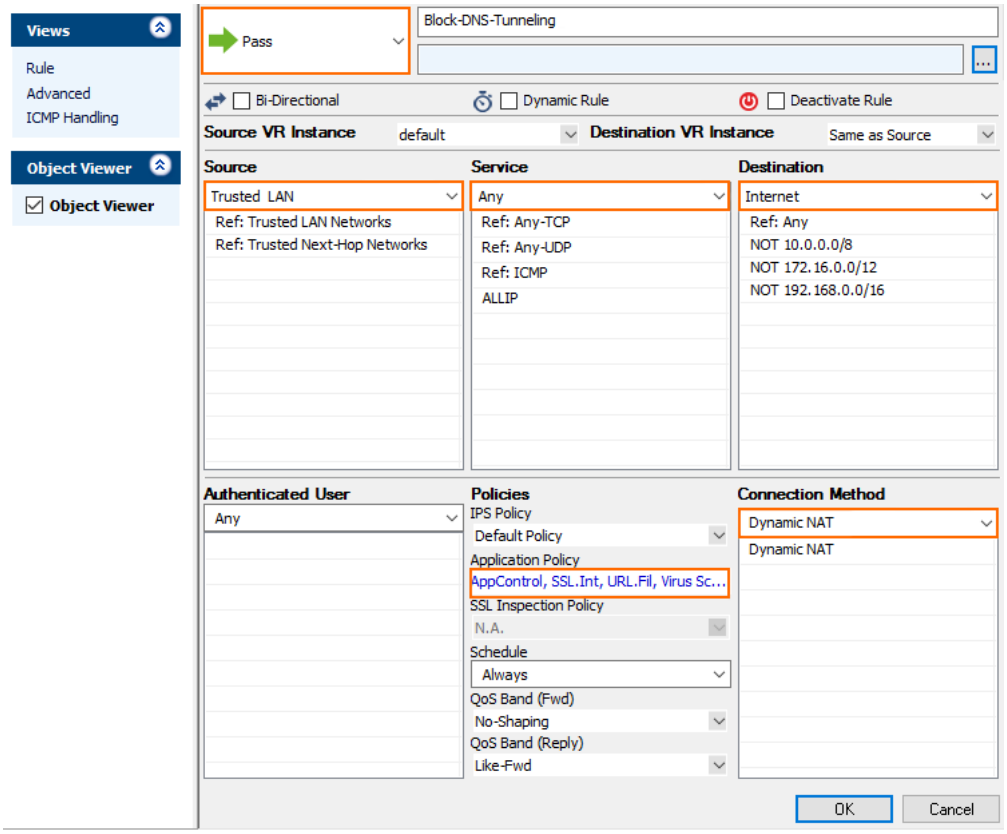
https://campus.barracuda.com/doc/73719262/

DNS tunneling is an attack method that encodes data of other programs or protocols in DNS queries and responses, allowing hackers access to the network using the DNS server. Configure the firewall to detect and block DNS tunneling by creating an application rule that uses a protocol object.

Step 1. Create an Access Rule

Create an access rule to allow traffic from the network to the Internet.

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 (**+**) at the top right of the ruleset, or right-click the ruleset and select **New > Rule**.
4. Select **Pass** as the action.
5. Enter a **Name** for the rule. E.g., `Block-DNS-Tunneling`
6. Specify the following settings:
   - **Source** – Select **Trusted LAN**.
   - **Destination** – Select **Internet**.
   - **Service** – Select **Any**.
   - **Connection Method** – Select **Dynamic NAT**.
   - **Application Policy** – Enable **Application Control**.

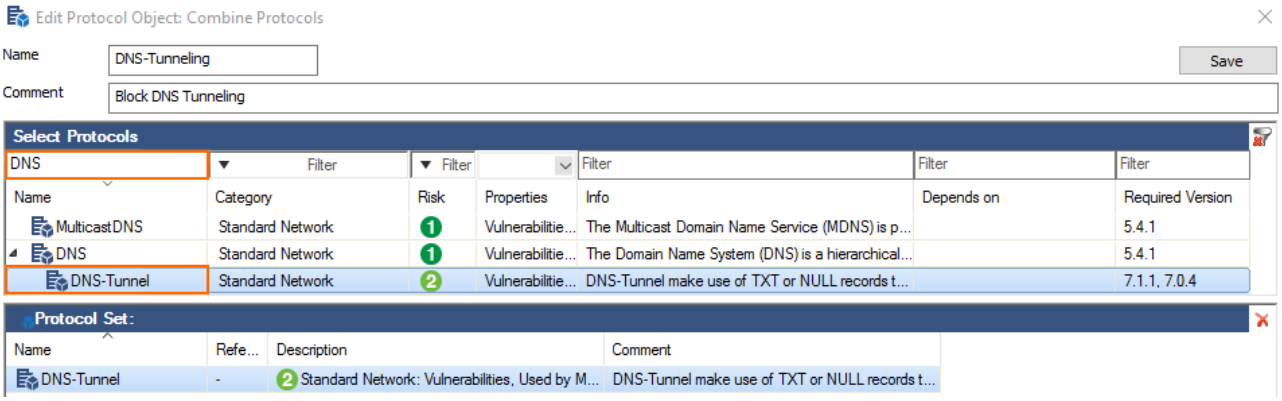


7. Click **OK**.
8. Drag and drop the access rule so that it is the first rule that matches the traffic that you want it to forward. Ensure that the rule is located above the BLOCKALL rule; rules located below the BLOCKALL rule are never executed.
9. Click **Send Changes** and **Activate**.

Step 2. Create a Protocol Object

Create a protocol object to detect DNS tunnelling.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Firewall > Forwarding Rules.**
2. Click **Lock**.
3. In the left menu, expand **Firewall Objects** and select **Applications**.
4. Create the protocol object by either right-clicking the table and selecting **New > Protocol Object** or using the icons in the top-right area of the ruleset.
5. Enter a **Name** for the protocol object.
6. Either search or filter for the protocol **DNS**.
7. In the **Select Protocols** list, expand **DNS**, and click the plus sign (**+**) next to **DNS Tunnel**.
8. The protocol appears in the **Protocol Set** section.

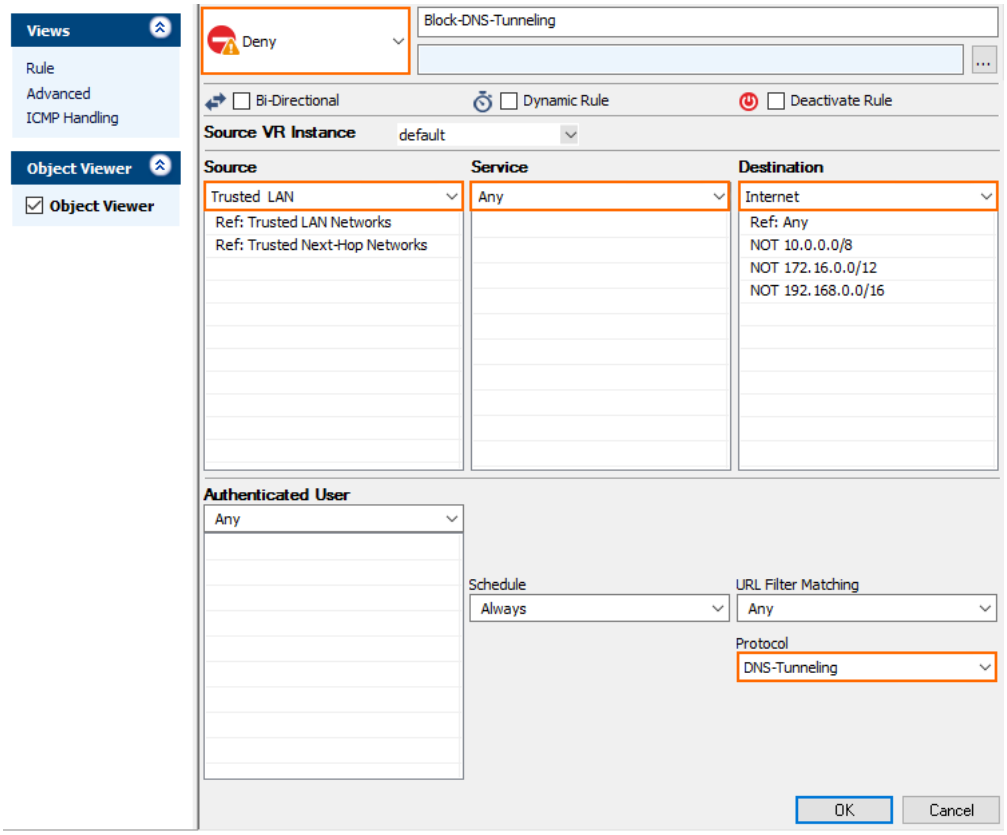


9. Click **Save**.
10. Click **Send Changes** and **Activate**.

Step 3. Create an Application Rule

Create an application rule for traffic between the network and the Internet. Use the protocol object to block the DNS tunnel protocol.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Firewall > Forwarding Rules**.
2. In the left menu, click **Application Rules**.
3. Click **Lock**.
4. Click the green plus sign (**+**) in the top right of the page or right-click the ruleset and select **New > Rule**. An application rule **New Rule** is added to the application ruleset.
5. Double-click on the **New Rule** application rule you just created. The **Edit Rule** window opens.
6. Enter a **Name** for the rule. E.g., `Block-DNS-Tunneling`
7. Specify the following settings:
   - **Action** – Select **Deny**.
   - **Source** – Select **Trusted LAN**.
   - **Destination** – Select **Internet**.
   - **Application** – Select **Any**.
   - **Protocol** – Select the protocol object created in Step 2



8. Click **OK**.
9. Drag and drop the application rule so that it is the first rule that matches the application traffic.
10. Click **Send Changes** and **Activate**.

Figures

1. dns_tunnel_01.png
2. dns_tunnel_02.png
3. dns_tunnel_03.png