

How to Detect and Block DNS Tunneling

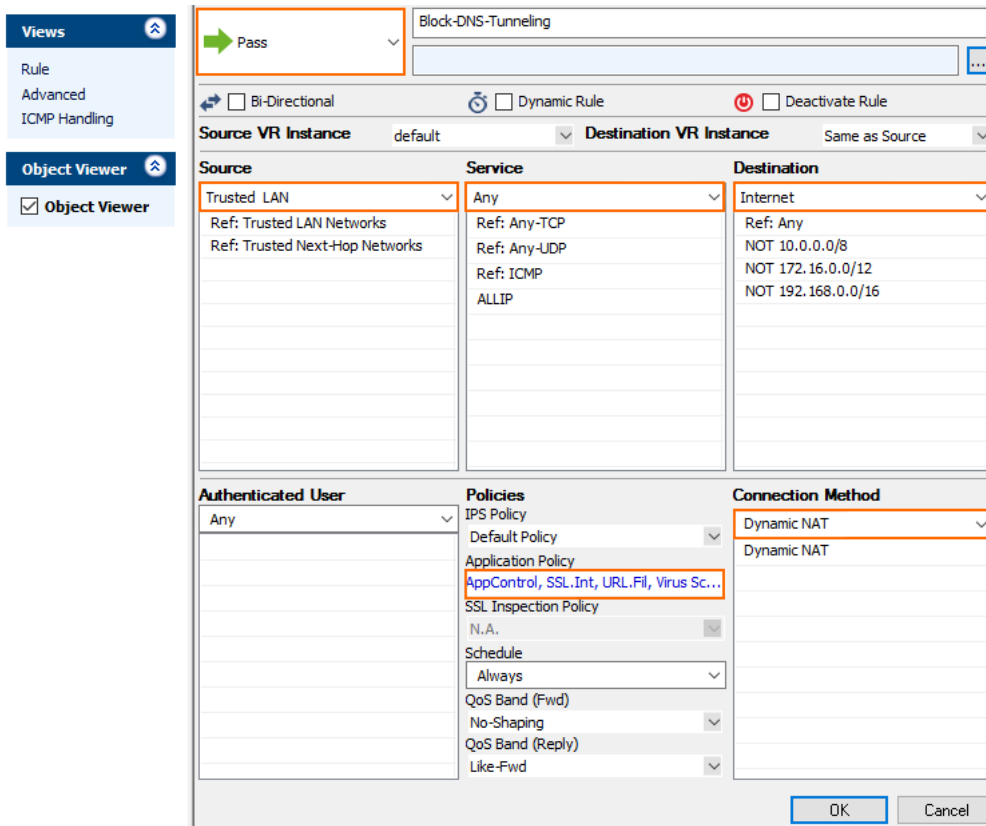
<https://campus.barracuda.com/doc/73719262/>

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**.



The screenshot shows the configuration for a rule named "Block-DNS-Tunneling". The rule is set to "Pass" and is not bi-directional, dynamic, or deactivated. The source is "Trusted LAN" (ref: Trusted LAN Networks, Trusted Next-Hop Networks) and the destination is "Internet" (ref: Any, NOT 10.0.0.0/8, NOT 172.16.0.0/12, NOT 192.168.0.0/16). The service is "Any" (ref: Any-TCP, Any-UDP, ICMP, ALLIP). The authenticated user is "Any". The policies include "AppControl, SSL.Int, URL.Fil, Virus Sc...". The connection method is "Dynamic NAT".

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.

Edit Protocol Object: Combine Protocols

Name: Save

Comment:

Select Protocols						
Name	Category	Risk	Properties	Info	Depends on	Required Version
MulticastDNS	Standard Network	1	Vulnerabilitie...	The Multicast Domain Name Service (MDNS) is p...		5.4.1
DNS	Standard Network	1	Vulnerabilitie...	The Domain Name System (DNS) is a hierarchica...		5.4.1
DNS-Tunnel	Standard Network	2	Vulnerabilitie...	DNS-Tunnel make use of TXT or NULL records t...		7.1.1, 7.0.4

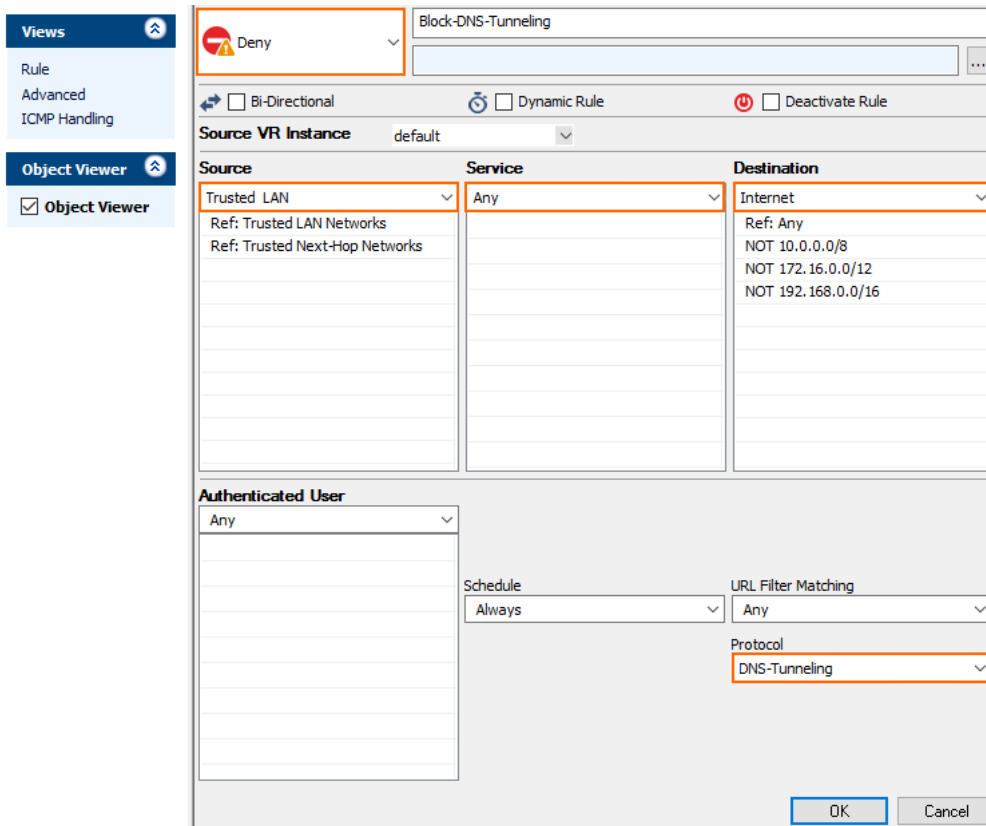
Protocol Set:			
Name	Refere...	Description	Comment
DNS-Tunnel	-	2 Standard Network: Vulnerabilities, Used by M...	DNS-Tunnel make use of TXT or NULL records t...

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:
 - o **Action** – Select **Deny**.
 - o **Source** – Select **Trusted LAN**.
 - o **Destination** – Select **Internet**.
 - o **Application** – Select **Any**.
 - o **Protocol** – Select the protocol object created in Step 2



The screenshot shows the configuration for a firewall rule named "Block-DNS-Tunneling". The rule is set to "Deny". The source is "Trusted LAN" (with references to Trusted LAN Networks and Trusted Next-Hop Networks), the service is "Any", and the destination is "Internet" (with references to Any, NOT 10.0.0.0/8, NOT 172.16.0.0/12, and NOT 192.168.0.0/16). The authenticated user is "Any", the schedule is "Always", the URL filter matching is "Any", and the protocol is "DNS-Tunneling". The rule is not bi-directional, dynamic, or deactivated. The "Object Viewer" is checked in the left sidebar.

Source	Service	Destination
Trusted LAN Ref: Trusted LAN Networks Ref: Trusted Next-Hop Networks	Any	Internet Ref: Any NOT 10.0.0.0/8 NOT 172.16.0.0/12 NOT 192.168.0.0/16

Authenticated User: Any

Schedule: Always

URL Filter Matching: Any

Protocol: DNS-Tunneling

Buttons: OK, Cancel

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

© Barracuda Networks Inc., 2019 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.