NEW How To Exclude Microsoft Lync traffic from a VPN Tunnel

Nino Pasalic
Dec 14, 2014
Revision: 1.2.2

Objective

This document gives a step by step procedure for excluding Microsoft Lync traffic from a VPN Tunnel. Since Microsoft Lync traffic is already encrypted there is a known issue with latency when it is tunneled through the client-to-site VPN.

Details

Supported Versions

- Client side – Endpoint Connect E80.xx. Tested with E80.41
- Management Server – R77.xx. Tested with R77.10
- Gateway – R77.xx. Tested with R77.10

Supported OS

- Gaia, SecurePlatform, and IPSO.

Supported Appliances

Any R77.xx Security Gateway appliance that supports Gaia, SecurePlatform or IPSO.

Read the R77.xx Release Notes on the Support Center (https://supportcenter.checkpoint.com/supportcenter/).
Before You Start

Related Documentation and Assumed Knowledge

- R77.10 iPad Release notes
  http://downloads.checkpoint.com/dc/download.htm?ID=30257
- R77.10 VPN Administration Guide

You must have a basic knowledge of:

- Installing Check Point releases and Hotfixes
- Administering rules and changes in the Security Management Server.
Excluding Microsoft Lync traffic from a VPN Tunnel

Create a Group with Exclusion

1. Create a Simple Group with Lync servers (NAT to a public IP address is already set up):

   ![Diagram of creating a simple group with Lync servers]

   For example, make a group is called “Excluded_IP”:

   ![Image of a group named Excluded_IP]

   **Important**: You must add private and public Lync server IP addresses to this group. This ensures that clients do not encrypt traffic destined for Lync servers.
2. Create a **Simple Group** that includes an “All Internet” object. For example, make a group called “Everything”:

![Simple Group](image1)

3. Create a **Group With Exclusion**:

![Group With Exclusion](image2)
4. Add the group “Everything” to the left side and “Excluded_IP” on the right:

5. Edit the Check Point Gateway properties
6. Open the Topology page,
7. Select Set domain for Remote Access Community.
8. Add the Group with Exclusion that you created earlier
Set up DNS servers for Endpoint Clients
1. Edit the Check Point Gateway properties
2. Open the VPN Clients > Office Mode page.
3. Select Optional parameters.

4. In the DNS Servers section, define the Primary DNS Server for the VPN clients. Only VPN clients will use this DNS server and only Microsoft Lync servers will be resolved on this DNS server. This DNS Server must point the VPN clients to the public IP addresses of the Microsoft Lync servers. This forces VPN clients to go to public IP addresses instead of private addresses of the Lync Servers.
5. For the First backup and Second backup add other existing DNS servers or commonly used internal or external servers.
Disable Hub Mode in the Global Properties:
1. Select Policy > Global Properties
2. Open the Remote Access > Endpoint Connect page.
3. For Route all traffic to gateway, select No.
Disable Hub Mode on the Gateway:
1. Edit the **Check Point Gateway** object.
2. Open the **VPN Clients > Remote Access** page.
3. Unselect **Allow VPN clients to route traffic through this gateway**.

Install the Policy
Install the policy and test the setup.

Setting Up Rules
In some situations the clients may still attempt to establish connection to Lync servers over VPN and vice versa. To make sure this does not happen, we recommend that you configure these rules:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Port</th>
<th>Action</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client VPN Subnets</td>
<td>Corporate VPN network</td>
<td>1024-65535 TCP/UDP</td>
<td>accept</td>
<td>Allow Lync client media traffic to all other internal clients</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(These are the default ports. Can be modified.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client VPN Subnets</td>
<td>All Lync Servers, including the Edge Server internal interface</td>
<td>All TCP/UDP ports</td>
<td>drop</td>
<td>Block Lync client traffic to Lync Servers (public and private IP addresses)</td>
</tr>
</tbody>
</table>

Additional notes: There are some great articles about this topic that are helpful to understand how Microsoft Lync solution works such as “Enabling Lync Media to Bypass a VPN Tunnel” written by Kevin Peters and Randy White.

References: