Configuring and Using Dynamic DNS in SmartCenter

This document describes how to configure and use Dynamic DNS for Check Point Embedded NGX gateways, using Check Point SmartCenter R60 and above, with or without the Check Point SmartLSM extension.

Note: Embedded NGX gateways include both VPN-1 Edge, IP40, and IP60 gateways. The Embedded NGX screens that appear in this document relate to VPN-1 Edge gateways.

Note: This document assumes the reader is familiar with the basic concepts of working with SmartCenter.

This document covers the following topics:

The Limitations of Working with Dynamic IP Addresses ...................................................... 2
The Dynamic DNS Solution ................................................................................................. 2
How Does Dynamic DNS Work? .......................................................................................... 4
Overview of DDNS Configuration ....................................................................................... 5
Configuring SmartCenter’s Domain Suffix ......................................................................... 6
Configuring Gateways’ DDNS Settings .............................................................................. 7
Testing the Configuration .................................................................................................... 8
Testing the DDNS Configuration ....................................................................................... 8
Testing the DDNS-Based VPN Mesh Community Configuration .................................... 9
Connecting to SmartCenter .............................................................................................. 9
Viewing VPN Topology Information ................................................................................. 13
The Limitations of Working with Dynamic IP Addresses

Most Internet Service Providers (ISPs) assign dynamic rather than static IP addresses to their subscribers. If a gateway has a dynamic IP address, then each time the gateway connects to the ISP, its IP address may change. This results in the following problems:

- It is not possible to create a fully meshed VPN community with dynamic IP gateways, since gateways will not know how to reach each other.
- The gateway’s owner cannot run public Web servers.
- Remote Access VPN users cannot connect to the gateway’s Remote Access VPN Server.

These limitations do not exist when working with a static IP address; however a static IP address usually entails an additional cost.

The Dynamic DNS Solution

The basic function of a standard DNS (Domain Name Service) is to translate domain names into IP addresses. The DNS does this by maintaining a database of domain names and their corresponding static IP addresses. For example, if you try to surf to “www.sofaware.com”, the DNS server will check its database and direct you to the corresponding IP address, 62.90.136.38. DNS names are helpful because they provide a readable and easy-to-remember reference to IP addresses. However, normally DNS cannot map a domain name to a dynamic IP address, since the IP address might change.

Dynamic DNS (DDNS) solves this problem by allowing you to assign a domain name to a gateway with a dynamic IP address. The DDNS service is constantly updated with changes to gateways’ IP addresses and updates the mapping of domain names to IP addresses accordingly. To facilitate this, SmartCenter NGX can be configured to act as a DDNS server on behalf of the Embedded NGX gateways connected to it. For example, if SmartCenter is registered in the worldwide DNS as the owner of the domain “Mycompany.com”, and the DDNS service is enabled for a gateway named “office”, then the gateway will be accessible at all times using the DNS name “office.Mycompany.com”. Each time the gateway’s IP address changes, the SmartCenter DDNS service will map this DNS name to the new IP address, so that the gateway is always accessible.

As a result:

- It is possible to create a fully meshed VPN community between all dynamic IP gateways, based on the DDNS information.
- External users are able to access a Web server behind the gateway, using the DNS name “office.Mycompany.com”.

Remote Access VPN users are able to communicate with the Remote Access VPN Server, using the DNS name “office.Mycompany.com”, even if the gateway’s IP address often changes.

Administrators can remotely manage their Embedded NGX gateways by accessing the gateways using their domain names. For example: https://office.Mycompany.com:981.

Note: Check Point VPN-1 gateways participating in a meshed VPN community cannot initiate tunnels towards VPN-1 Edge gateways with dynamic IP addresses.

Some Internet tools can only be used if you have a static IP address or domain name. DDNS enables you to use these tools with a dynamic IP address. For example, you can ping an Embedded NGX gateway using its domain name (for example, office.Mycompany.com).

Note: Check Point VPN-1 Pro gateways support DDNS-based link selection, and they can establish VPN tunnels to Embedded NGX gateways with dynamic IP addresses. Likewise, Embedded NGX gateways can establish VPN tunnels to externally managed gateways (such as VPN-1 Pro) with a dynamic IP address that is mapped to a DDNS provider.
How Does Dynamic DNS Work?

1. The enterprise registers SmartCenter's static IP address on a worldwide DNS, under a domain name such as “Mycompany.com”.

   In other words, SmartCenter is registered as the authoritative DNS server for the “Mycompany.com” domain.

   Note: In management High Availability (HA) installations, the secondary management server must be registered as a secondary DNS server for the domain.

2. The enterprise configures DDNS on SmartCenter.

   As part of this configuration, the enterprise enables the DDNS service for SmartCenter. SmartCenter then becomes a DNS server itself, and starts listening to DNS requests on UDP port 53.

   For information on configuring DDNS, see “Overview of DDNS Configuration,” page 5.

3. An Embedded NGX gateway connects to SmartCenter over an Internet connection and reports its current IP address.

   If the appliance is behind a NAT device, the reported IP address is that of the NAT device.

4. SmartCenter assigns the gateway a domain name using the gateway ID.

   For example, if the gateway ID is “office”, then SmartCenter assigns the gateway the DNS name “office.Mycompany.com”. This domain name is mapped to the IP address reported by the gateway.

5. The gateway can now be contacted via the Internet, using its domain name.

6. If the IP address of the gateway changes, the following things happen:

   a. The gateway reports the change to SmartCenter.

   b. SmartCenter maps the domain name to the new IP address.
Overview of DDNS Configuration

To configure DDNS

1. Configure SmartCenter’s domain suffix.
   See “Configuring SmartCenter’s Domain Suffix,” page 6.

2. If SmartCenter is located behind a firewall, or if you want to configure DDNS for Firewall-1 in a VPN Mesh community, register SmartCenter's public IP address on a worldwide DNS service.
   For information about domain registration, contact your ISP or any domain registration service.

   Note: Since DNS is a distributed system, it takes time until the domain servers are updated with the DNS name.

   Note: If SmartCenter is installed behind a firewall or a NAT device, you must open TCP and UDP port 53 towards SmartCenter, to enable SmartCenter to accept DNS requests.

3. Prepare the gateways for DDNS by doing the following:
   a. Create a gateway object for each gateway for which you want to enable DDNS.
      For information, refer to SmartCenter documentation.
   b. Configure DDNS for each gateway object.

4. (Optional) To configure a DDNS-based VPN Mesh community, do the following:
   a. Create a Mesh or Star community.
      For information, refer to SmartCenter documentation.
   b. Add the gateway objects to the community you created.
      For information, refer to SmartCenter documentation.
   c. Install the policy on each gateway object.
      The Embedded NGX gateway downloads the VPN topology.
      For information, refer to SmartCenter documentation.
5. Test the configuration by doing the following on each gateway:
   
   a. Test the DDNS configuration.
      
   
   b. If you configured a DDNS-based VPN Mesh community, test its configuration by doing the following:
      
      1) Connect each gateway to SmartCenter.
         
         See “Connecting to SmartCenter,” page 9.
      
      2) View the gateway’s VPN topology information.
         

**Configuring SmartCenter’s Domain Suffix**

To configure SmartCenter’s domain suffix

1. In SmartDashboard, in the Policy menu, choose Global Properties.

   The Global Properties dialog box appears.

2. In the menu, expand VPN, and click the Advanced tab.

   The Advanced tab appears.
3. In the **Domain name for DNS resolving** field, type the domain suffix to use for SmartCenter.

4. Click **OK**.

5. In the toolbar, click **Save**.

### Configuring Gateways’ DDNS Settings

**To configure a gateway object's DDNS settings**

1. In SmartDashboard, double-click the desired gateway object.

   The **VPN-1 Edge/Embedded Gateway** dialog box appears displaying the **General Properties** tab.

2. In the menu, expand **VPN**, and click the **Link Selection** tab.

   The **Link Selection** tab appears.

2. Click **Use DNS resolving**.
3. Do one of the following:

- To specify the full hostname for the gateway, click **Full hostname**, and type the desired hostname in the field provided.

- To specify that SmartCenter should automatically create a hostname for the gateway, click **Gateway’s name and domain name** (recommended).

  The hostname is created in the following format: `<gateway’s name>.<domain suffix>`

  For example, if the gateway’s name is “Office”, and the domain suffix you configured in “Configuring SmartCenter’s Domain Suffix,” page 6 is “mycompany.com”, then the gateway’s hostname will be “Office.mycompany.com”.

  

  ![Note: The Outgoing link tracking option is not supported when configuring DDNS.]

4. Click **OK**.

**Testing the Configuration**

**Testing the DDNS Configuration**

**To test the DDNS configuration**

- Open a command line window, and ping the gateway’s domain name (for example, gateway.mycompany.net).

```plaintext
C:\Documents and Settings\user>ping gateway.mycompany.net

Pinging gateway.mycompany.net [212.30.50.12] with 32 bytes of data:

Reply from 212.30.50.12: bytes=32 time=51ms TTL=62
Reply from 212.30.50.12: bytes=32 time=49ms TTL=62
Reply from 212.30.50.12: bytes=32 time=48ms TTL=62
Reply from 212.30.50.12: bytes=32 time=69ms TTL=62

Ping statistics for 212.30.50.12:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 46ms, Maximum = 69ms, Average = 53ms
```

8
Testing the DDNS-Based VPN Mesh Community Configuration

Connecting to SmartCenter

To connect a gateway to SmartCenter

1. Click Services in the main menu, and click the Account tab.

The Account page appears.

2. In the Service Account area, click Connect.
The Services Wizard opens, with the Service Center dialog box displayed.

3. Make sure the Connect to a different Service Center check box is selected.

4. Select Specified IP and then in the Specified IP field, enter SmartCenter’s IP address, as given to you by your system administrator.

5. Click Next.
   - The Connecting… screen appears.
   - If the Service Center requires authentication, the Service Center Login dialog box appears.

Enter your gateway ID and registration key in the appropriate fields, as given to you by your enterprise, then click Next.

- The Connecting… screen appears.
The **Confirmation** dialog box appears with a list of services to which you are subscribed. Make sure that the Dynamic DNS service appears in the list.

6. Click **Next**.

The **Done** screen appears with a success message.

7. Click **Finish**.
On the **Account** page, the **Dynamic DNS** service's status is "Connected", and the gateway’s domain name is displayed in the **Information** column.

<table>
<thead>
<tr>
<th>Service</th>
<th>Subscription</th>
<th>Status</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Updates</td>
<td>Subscribed</td>
<td>Connected</td>
<td>Automatic</td>
</tr>
<tr>
<td>Remote Management</td>
<td>Subscribed</td>
<td>Connected</td>
<td></td>
</tr>
<tr>
<td>Web Filtering</td>
<td>Subscribed</td>
<td>Connected</td>
<td>On</td>
</tr>
<tr>
<td>Email Antivirus</td>
<td>Subscribed</td>
<td>Connected</td>
<td>On</td>
</tr>
<tr>
<td>Spam</td>
<td>Subscribed</td>
<td>Connected</td>
<td>On</td>
</tr>
<tr>
<td>VirusStream Antivirus Signature Updates</td>
<td>Subscribed</td>
<td>Connected</td>
<td></td>
</tr>
<tr>
<td><strong>DNS</strong></td>
<td>Subscribed</td>
<td>Connected</td>
<td><strong>gbw495.mysoftware.net</strong></td>
</tr>
<tr>
<td>Dynamic VPN</td>
<td>Not Subscribed</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Logging &amp; Reporting</td>
<td>Subscribed</td>
<td>Connected</td>
<td></td>
</tr>
<tr>
<td>Vulnerability Scanning</td>
<td>Not Subscribed</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>
Viewing VPN Topology Information

To view VPN topology information


The VPN network topology appears.

<table>
<thead>
<tr>
<th>Topology by Gateways</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site Index:</td>
</tr>
<tr>
<td>Site Name:</td>
</tr>
<tr>
<td>Topology Version:</td>
</tr>
<tr>
<td>Gateway Name:</td>
</tr>
<tr>
<td>Gateway Main IP:</td>
</tr>
<tr>
<td>Gateway Active Interface:</td>
</tr>
<tr>
<td>RDP Resolution Mechanism:</td>
</tr>
<tr>
<td>Gateway Resolution Name:</td>
</tr>
<tr>
<td>Interfaces:</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Networks:</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>0.0.0.4</td>
</tr>
<tr>
<td>192.168.10.10</td>
</tr>
</tbody>
</table>

The RDP Resolution Mechanism field displays “DNS Lookup”.

The Gateway Resolution Name field displays the gateway’s hostname, as configured in “Configuring Gateways’ DDNS Settings,” page 7.

2. From another gateway, ping the second IP address listed in the Interfaces field.

In our example, the IP address to ping is 192.168.10.10.
The **Gateway Dynamic IP** field appears displaying the gateway’s current IP address.

<table>
<thead>
<tr>
<th>Topology by Gateways</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site Index:</td>
</tr>
<tr>
<td>Site Name:</td>
</tr>
<tr>
<td>Topology Version:</td>
</tr>
<tr>
<td>Gateway Name:</td>
</tr>
<tr>
<td>Gateway Main IP:</td>
</tr>
<tr>
<td>Gateway Active Interface:</td>
</tr>
<tr>
<td>RDP Resolution Mechanism:</td>
</tr>
<tr>
<td>Gateway Resolution Name:</td>
</tr>
<tr>
<td><strong>Gateway Dynamic IP:</strong></td>
</tr>
<tr>
<td>Interfaces:</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Networks:</th>
<th>Net Start</th>
<th>Net End</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.4</td>
<td>0.0.0.4</td>
<td></td>
</tr>
<tr>
<td>192.168.10.10</td>
<td>192.168.10.255</td>
<td></td>
</tr>
</tbody>
</table>

Note: The Embedded NGX gateway will try to resolve the remote gateway’s external IP address every time an IKE or IPSEC security association is established.