VPN-1 VPN Interoperability

NGX

Reference Guide

16 November 2010
Important Information

Latest Software
We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Latest Documentation
The latest version of this document is at: http://supportcontent.checkpoint.com/documentation_download?ID=7853
For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>16 November 2010</td>
<td>Fixed Example One (on page 11) subnets in table. Improved formatting and document layout.</td>
</tr>
<tr>
<td>15 November 2007</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

Feedback
Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments (mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on VPN-1 VPN Interoperability NGX Reference Guide).
## Contents

**Important Information** ................................................................................................................... 3  
**Introduction** ....................................................................................................................................... 5  
**IKE Issues** ........................................................................................................................................ 5  
   - Phase 1 IDs ..................................................................................................................................... 5  
   - Phase 2 IDs ..................................................................................................................................... 5  
   - Editing DEF Files ............................................................................................................................ 6  
   - Editing SmartDashboard Objects .................................................................................................... 6  
   - Protocol and Port in IKE Phase 2 ...................................................................................................... 6  
   - Phase 2 Encryption Properties ......................................................................................................... 6  
   - SA Expiration ................................................................................................................................ 6  
   - SA Deletion .................................................................................................................................... 7  
   - Certificate Alternate Name Field ..................................................................................................... 7  
   - IPs Used for VPN Tunnel Establishment ......................................................................................... 8  
   - Dead Peer Detection (DPD) ............................................................................................................ 8  
**IPSec and Other Issues** ...................................................................................................................... 8  
   - Cluster Load Sharing Support ......................................................................................................... 8  
   - Authentication Header Support ...................................................................................................... 8  
   - GRE Tunneling ............................................................................................................................... 9  
   - 3rd Party Dynamic IP GW Dynamically Assigned IP (DAIP) ......................................................... 9  
   - L2TP Client Support ....................................................................................................................... 9  
**Configuring a Subnet** ........................................................................................................................ 10  
   - Configuring the Subnet Per Range ................................................................................................. 10  
   - Example ........................................................................................................................................ 10  
   - Configuring the Subnet Per Peer .................................................................................................... 11  
   - Example One ............................................................................................................................... 11  
   - Example Two .............................................................................................................................. 11  
   - Example Three ........................................................................................................................... 12
Introduction

This document describes interoperability issues between VPN-1 NGX Gateways and VPN solutions of other vendors. It explains how to configure site-to-site tunnels between Check Point VPN-1 and third-party VPN sites.

Supported Products: Check Point management and gateway versions of NGX R60 and higher.

IKE Issues

In This Section

- Phase 1 IDs
- Phase 2 IDs
- Protocol and Port in IKE Phase 2
- Phase 2 Encryption Properties
- SA Expiration
- SA Deletion
- Certificate Alternate Name Field
- IPs Used for VPN Tunnel Establishment
- Dead Peer Detection (DPD)

Phase 1 IDs

IKE Phase 1 negotiation contains an ID payload. The ID payload may contain the IP addresses of the gateways participating in the IKE negotiation. Therefore, VPN-1 uses the main IP address of the gateway as defined in the General Properties of the VPN-1 NGX Gateways object. VPN-1 may use a different IP address for the IKE negotiation and for the VPN tunnel. Some third-party vendors may require the same IP address for the ID payload as for the IKE negotiation and the VPN tunnel. This incompatibility may cause connectivity failure when opening a VPN tunnel between VPN-1 and third-party devices.

To avoid this issue, make sure VPN-1 uses one IP address consistently:
1. In SmartDashboard, in the gateway object properties, open VPN > Link Selection.
2. Select Always use this IP address.
3. Select Main address.
4. Click OK.
5. Install the policy.

Phase 2 IDs

During IKE Quick Mode negotiation, the IP addresses which define the VPN tunnel (also known as IPSec IDs or traffic selectors) are negotiated. The IP addresses can be a set of discrete IP addresses, or a subnet. When negotiating a VPN tunnel between VPN-1 and certain third-party devices, IKE Quick Mode may fail if the subnets are defined differently on each end of the tunnel. One reason is that in VPN-1, the IDs are determined by the encryption domain and in other VPNs, the IDs are derived from the ACLs.

This issue can be solved in different ways:
- Edit the DEF files - a more complex solution that is more often effective
- Edit the gateway and community objects - a simpler solution that is sometimes applicable.
Editing DEF Files

The most common method to resolve IP address inconsistencies is to manually configure them ("Configuring a Subnet" on page 10). You define the subnet to use, per range of IP addresses or per peer gateway.

Editing SmartDashboard Objects

In SmartDashboard, configure the subnet on the gateway object or on the Community object. If you configure the Community, the change applies to all gateway members of the community, unless the VPN-1 NGX Gateways was configured explicitly.

To explicitly configure the VPN-1 NGX Gateways object:

1. Open the properties of the VPN Community.
2. Open Tunnel Management > VPN Tunnel Sharing.
3. Choose how tunnel negotiations for the gateway will be done:
   - One tunnel per pair of hosts
   - One tunnel per subnet pair (defined in the Encryption Domain of the gateways)
   - One tunnel per pair of gateways

Protocol and Port in IKE Phase 2

RFC 2407 ((http://www.ietf.org/rfc/rfc2407.txt), section 4.6.2, includes the protocol and port in the system security policy requirement for the association. This information is negotiated as part of the ID payload in IKE Quick Mode. VPN-1 successfully performs Quick Mode negotiation including this information but does not enforce the negotiated port and protocol on subsequent packets. However, some third-party VPN solutions do enforce the negotiated port and protocol on VPN traffic.

To enhance compatibility, configure the third-party device not to negotiate the port and protocol as part of Phase 2 negotiation.

Phase 2 Encryption Properties

When working in Traditional Mode, the IKE Phase two encryption properties are configured in the Action column of the SmartDashboard Rule Base. When responding to an IKE negotiation initiated by a third-party VPN site, these encryption properties are not enforced until after the negotiation, when the first packet of the connection is received. During the IKE negotiation itself, the VPN-1 NGX Gateways will agree to anything it supports. As a result, it may fail the connection because of tunnel misconfiguration.

To avoid this problem, configure the encryption properties in Simplified mode. In this mode, the encryption properties are configured on the community, and are taken into account at the negotiation stage.

Note - In Traditional Mode it was possible to configure different encryption properties for different services, in different rules. In Simplified Mode, because the properties are configured on the Community object, this is not possible.

SA Expiration

In Simplified mode, SA renegotiation by traffic quantity (Kilobytes) cannot be configured. However, this does not constitute a problem, because when a third-party VPN site suggests this, the VPN-1 NGX Gateways accepts the proposal.

If the VPN-1 gateway and the third-party VPN site are both configured for SA expiry by time, but configured for different times, connectivity failures may occur. VPN-1 gateways overcome such misconfigurations by using Delete Notifications and Responder Lifetime Notifications. These notifications are not supported by some third-party vendors.
To avoid this issue, make sure the expiration timeout is defined in the same way on the two sites.

To find the expiration option on the VPN-1 NGX Gateways:

- **In Traditional mode:** In SmartDashboard, in the gateway object properties, go to **VPN > Traditional mode configuration > Advanced > Rekeying Parameters**.
- **In Simplified mode:** In SmartDashboard, in the community object properties, go to **Advanced Settings > Advanced VPN Properties**.

## SA Deletion

When installing a policy on a VPN-1 NGX Gateways, or on restart of VPN-1 or a third-party VPN site, all IKE SAs are deleted (except for SAs for remote access connections). When another site tries to use a SA that has been deleted from a VPN-1 gateway, a Delete Notification is sent and IKE is renegotiated.

Some third-party VPN sites do not send Delete Notifications and cannot receive them. As a result, after installing a policy on a VPN-1 gateway, or after restart of VPN-1 or a third-party VPN site, connectivity may fail.

To solve this problem, configure the VPN-1 gateway not to delete SAs upon policy installation.

### If there are unrecognized SAs in the two sites, treat connections as initial contacts:

1. In SmartDashboard, from the **Policy** menu, select **Global Properties**.
2. In **SmartDashboard Customization**, click **Configure**.
3. Go to **VPN Advanced Properties > VPN IKE Properties**.
4. Select **ike_handle_initial_contact**, **ike_send_initial_contact**, and **keep_IKE_SAs**.
5. Click **OK**.
6. Install the policy.

**Note:** SecuRemote/SecureClient do not send Initial Contact messages. A VPN-1 NGX Gateways will not send an Initial Contact message if the peer is mobile or a Dynamically Assigned IP (DAIP) Gateway.

## Certificate Alternate Name Field

Some third-party VPN sites require that a received certificate contain an Alternate Name field. Some of these sites require that IKE packets come from the IP address in this field.

When generating a certificate in SmartDashboard from the Internal CA, this field is not automatically created.

To solve this issue:

- When generating the certificate, specify to create the field, for both ICA and OPSEC certificates, and use the main IKE negotiation IP address.

- To have the field created automatically (with the main IP address) with certificate creation:
  a) In SmartDashboard, from the **Policy** menu, select **Global Properties**.
  b) In **SmartDashboard Customization**, click **Configure**.
  c) In **Certificates and PKI properties**, select **add_ip_alt_name_for_opsec_certs** and **add_ip_alt_name_for_ICA_certs**.
  d) Click **OK**.
  e) Install the policy.
IPs Used for VPN Tunnel Establishment

VPN-1 is tolerant to a change of IP addresses during IKE negotiation. In particular, if an IKE packet is sent to one IP address while the return packet is sent from another IP address. However, some third-party VPN sites may fail the negotiation when VPN-1 changes the IP address.

To avoid this issue, make sure the responding source IP address of VPN-1 is the same as the IP address used by the third-party VPN site to address the VPN-1 Gateway.

To make sure the source IP addresses are the same:
1. In SmartDashboard, in the gateway object properties, open VPN > Link Selection.
2. Click Source IP address settings.
4. Select the appropriate option so that the same IP address is used as the one defined in Link Selection > IP Selection by Remote Peer.
5. Click OK.
6. Install the policy.

Dead Peer Detection (DPD)

VPN-1 does not support Dead Peer Detection. When configuring third-party VPN sites to connect to a VPN-1 NGX Gateways, make sure that Dead Peer Detection is disabled.

IPSec and Other Issues

In This Section

Cluster Load Sharing Support 8
Authentication Header Support 8
GRE Tunneling 9
3rd Party Dynamic IP GW Dynamically Assigned IP (DAIP) 9
L2TP Client Support 9

Cluster Load Sharing Support

When VPN-1 is deployed in a Load Sharing cluster configuration, you need to enable the Sticky Decision Function. See “Sticky Connections” in the ClusterXL Administration Guide.

Authentication Header Support

AH (Authentication Header) is not supported on VPN-1. When a VPN-1 NGX Gateways is prompted to use AH during the IKE negotiation, a No Proposal Chosen notification is sent to the peer, and an informative log is displayed in SmartView Tracker.
GRE Tunneling

Some third-party VPN sites support dynamic routing over VPN only with GRE.

To enable GRE when VPN-1’s connections with a third-party device:
1. In SmartDashboard, in the third-party object properties, open VPN > VPN Advanced.
2. Select Custom settings, and One VPN tunnel per Gateway pair.
3. From the list, select GRE on IPSec.
4. Click OK.
5. Install the policy.

3rd Party Dynamic IP GW Dynamically Assigned IP (DAIP)

VPN-1 supports VPN with third-party Dynamically Assigned IP (DAIP) Gateways (such as Netscreen).

To enable VPN connections with third-party DAIP gateways:

- In dbedit, enable the global property ike_allow_unusual_id_types.

L2TP Client Support

VPN-1 supports Windows 2000 and XP L2TP clients, and NGX R65 with HFA01 supports Vista L2TP clients. This includes L2TP routing (packets to the Internet are routed through VPN-1 NGX Gateways).

Supported authentication methods for L2TP clients are:
- EAP: MD5-Challenge and EAP-TLS only. Other EAP methods are not supported.
- PAP with all user-password types of authentication, such as RADIUS and SecureID.
- NAT-T.

These authentication methods are not supported:
- SPAP
- CHAP
- MS-CHAP
- MS-CHAPv2
Configuring a Subnet

To enhance interoperability with third-party devices:
- Define the subnet used in the Quick Mode negotiation per range.
- Define the subnet per peer.

Configuring the Subnet Per Range

To configure the subnet per range, create the table `max_subnet_for_range` in the `user.def` file, found under `$FWDIR/conf/`.

**Note** - For VPN-1 gateways of version NG R55, use the `user.def.NGCM` file, in the same location. For VSX gateways, the file is `user.def.VXCM`.

The table syntax is:

```
max_subnet_for_range = {
    <first_IP_of_range, last_IP_of_the_range; subnet_mask>,
    <first_IP_of_range, last_IP_of_the_range; subnet_mask>,
    ...
    <first_IP_of_range, last_IP_of_the_range; subnet_mask>
};
```

When negotiating the quick mode ID for a given connection, VPN-1 will look up the source and destination host IP addressed in the ranges in the above table. Then VPN-1 will apply the entries' specified subnet masks to the host addresses to calculate the network addresses. The quick mode ID is composed of the network addresses for the source and destination.

The table settings take effect after installing policy.

**Note** - Avoid defining overlapping ranges in the table.

Example

If we insert the table:

```
#ifndef __USER_DEF__
#define __USER_DEF__

// User defined INSPECT code

max_subnet_for_range = {
    <0.0.0.0, 194.29.39.255; 255.255.255.0>,
    <194.29.40.0, 194.29.50.255; 255.255.255.255>,
    <194.29.51.0, 255.255.255.255; 255.255.0.0>
};
#endif /* __USER_DEF__ */
```

- For host IP 194.29.23.1, the subnet would be 194.29.23.0/24 (194.29.23.0-194.29.23.255).
- For host IP 194.29.46.45 the subnet would be 194.29.46.45 (just one IP).
- For host IP 194.29.102.1 the network IP would be 194.29.0.0/16 (194.29.0.0-194.29.255.255).
Configuring the Subnet Per Peer

To configure the subnet per peer, create the table `subnet_for_range_and_peer` in the `user.def` file, found under `$FWDIR/conf/`.

Note - For VPN-1 gateways of versions before NGX R60, you cannot configure the subnet per peer.

The table syntax is:

```c
subnet_for_range_and_peer = {
< peerGW_IP, first_ip_of_the_range, last_ip_of_the_range; subnet_mask >,
< peerGW_IP, first_of_at_the_range, last_ip_of_the_range; subnet_mask >,
...< peerGW_IP, first_of_at_the_range, last_ip_of_the_range; subnet_mask >
};
```

The table settings take effect after installing policy.

Note - Avoid defining overlapping ranges in the table.

Example One

For the gateway to negotiate network 10.10.0.0/16 (10.10.0.0 - 10.10.255.255) with peer gateway Peer1 (192.168.10.20), but network 10.10.0.0/24 (10.10.0.0 - 10.10.0.255) with Peer2 (192.168.20.20), the table should be:

```c
#ifndef __user_def__
#define __user_def__

// User defined INSPECT code

subnet_for_range_and_peer = {
< 192.168.10.20, 10.10.0.0, 10.10.255.255; 255.255.0.0 >,
< 192.168.20.20, 10.10.0.0, 10.10.255.255; 255.255.255.0 >
};
#endif /* __user_def__ */
```

Example Two

You can configure the gateway to negotiate a single address instead of a subnet. For example, for connections from 10.10.44.6 behind the gateway to the network behind Peer2, the table should be:

```c
#ifndef __user_def__
#define __user_def__

// User defined INSPECT code

subnet_for_range_and_peer = {
< 192.168.20.20, 10.10.44.6, 10.10.44.6; 255.255.255.255 >
};
#endif /* __user_def__ */
```
Example Three

For further granularity, VPN-1 can narrow the negotiation to a specific host in the Peer2 network:

```c
#ifndef __user_def__
#define __user_def__

// User defined INSPECT code

subnet_for_range_and_peer = {
  < 192.168.20.20, 30.10.9.4, 30.10.9.4; 255.255.255.255 >
};
#endif /* __user_def__ */
```