Zscaler Internet Access (ZIA) and
Fortinet SDWAN Deployment Guide

November 2019

Version 1.1
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Document Overview</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>Document Audience</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>Software Revisions</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>Request for Comments</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>Document Prerequisites</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>Document Revision Control</td>
<td>7</td>
</tr>
<tr>
<td>2</td>
<td>Configuring GRE and IPsec Tunnels on ZIA</td>
<td>8</td>
</tr>
<tr>
<td>3</td>
<td>Configuring Fortinet for GRE and IPsec</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>Verify Access to FortiOS</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>Log into FortiOS</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>FortiGate Dashboard</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>Prerequisites to Configuring GRE Tunnels</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>Create GRE Tunnels</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>Configure GRE Tunnel Interfaces</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>Performance SLAs</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>Prerequisites to Configuring Performance SLAs</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>Configuring Performance SLAs</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>Configuring IPsec Tunnels</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td>IPsec Wizard</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td>Configure IPsec - General</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td>Configure IPsec – Phase 1</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>Configure IPsec – Phase 2</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>Verify IPsec Configuration</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>Configuring Firewall Policy</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>Create Firewall Policy</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>Verify Firewall Policies</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>Configuring SD-WAN</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>Create SD-WAN Member for Primary ZEN</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>Create SD-WAN Member for Backup ZEN</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>Verify SD-WAN Members</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td>Configuring SD-WAN Rules</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td>Create SD-WAN Rule</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td>Verify SD-WAN Rule</td>
<td>25</td>
</tr>
<tr>
<td>4</td>
<td>Verify Configuration with Zscaler Test Page</td>
<td>26</td>
</tr>
<tr>
<td></td>
<td>Request Verification Page</td>
<td>26</td>
</tr>
<tr>
<td>5</td>
<td>Requesting Zscaler Support</td>
<td>27</td>
</tr>
<tr>
<td></td>
<td>Gather Support Information</td>
<td>27</td>
</tr>
<tr>
<td></td>
<td>Obtain Company ID</td>
<td>27</td>
</tr>
</tbody>
</table>
5.1.2  Save Company ID.................................................................................................................. 28
5.1.3  Enter Support Section............................................................................................................ 29

6  Appendix A: Zscaler Resources ................................................................................................. 30
7  Appendix B: Fortinet Resources ............................................................................................... 31
# Terms and Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>DPD</td>
<td>Dead Peer Detection <em>(RFC 3706)</em></td>
</tr>
<tr>
<td>GRE</td>
<td>Generic Routing Encapsulation <em>(RFC2890)</em></td>
</tr>
<tr>
<td>IKE</td>
<td>Internet Key Exchange <em>(RFC2409)</em></td>
</tr>
<tr>
<td>IPsec</td>
<td>Internet Protocol Security <em>(RFC2411)</em></td>
</tr>
<tr>
<td>OAM</td>
<td>Operation, Administration, and Management</td>
</tr>
<tr>
<td>PFS</td>
<td>Perfect Forward Secrecy</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Socket Layer <em>(RFC6101)</em></td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security <em>(RFC5246)</em></td>
</tr>
<tr>
<td>XFF</td>
<td>X-Forwarded-For <em>(RFC7239)</em></td>
</tr>
<tr>
<td>ZAPP</td>
<td>Zscaler End-point Client Application</td>
</tr>
<tr>
<td>ZIA</td>
<td>Zscaler Internet Access (Zscaler)</td>
</tr>
<tr>
<td>ZPA</td>
<td>Zscaler Private Access (Zscaler)</td>
</tr>
</tbody>
</table>
1 Document Overview

This Deployment Guide document will provide GUI examples for configuring Zscaler Internet Access (ZIA) and Fortinet. This guide is intended for standing up proof-on-concept topologies and demos, for evaluating interoperability, and joint integration. This guide should not be used to configure either vendor platform for production use. For production deployments, please contact Zscaler or Fortinet for post-sale deployment assistance.

1.1 Document Audience

This document was designed for Network Security Engineers and Network Security Architects. All examples in this guide presumes the reader has a basic comprehension of IP Networking. For additional product and company resources, please refer to the Appendix section.

1.2 Software Revisions

This document was written using Zscaler Internet Access v5.7 and FortiOS 6.2.0 build0866 (GA).

1.3 Request for Comments

We value the opinions and experiences of our readers. To offer feedback or corrections for this guide, please contact partner-doc-support@zscaler.com.
1.4 **Document Prerequisites**

**Zscaler Internet Access (ZIA)**

- A working instance of ZIA 5.7 (or newer)
- Administrator login credentials to ZIA

**Fortinet**

- FortiOS 6.2.0 build0866 (GA) or newer
- Administrator login credentials to Fortinet device
1.5 **Document Revision Control**

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Change Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>October 2019</td>
<td>Initial document created by Zscaler and Fortinet</td>
</tr>
<tr>
<td>1.1</td>
<td>November 2019</td>
<td>Added GRE content</td>
</tr>
</tbody>
</table>
2 Configuring GRE and IPsec Tunnels on ZIA

There are three major steps when configuring GRE or IPsec tunnels to ZIA.

**STEP #1:** You need to locate which datacenters are available to you and the hostname / IP address of the VIP to establish a tunnel towards:

Locating the Hostname and IP Addresses of ZENs

**STEP #2:** You need to configure the tunnel itself on the ZIA side. Below are steps for configuring a GRE Tunnel and a VPN Credential (for an IPsec tunnel).

Configuring GRE Tunnels
https://help.zscaler.com/zia/configuring-gre-tunnels

Configuring a VPN Credential

**STEP #3:** You need to add the VPN credential to a location. For GRE, the steps are similar, but instead of selecting a VPN Credential, you will select a “Static IP Address”.

Adding VPN Credential to Location
https://help.zscaler.com/zia/configuring-locations

If you have problems with any of these steps, please open a support ticket with Zscaler support:

Submit a Zscaler Support Ticket
https://help.zscaler.com/submit-ticket
3 Configuring Fortinet for GRE and IPsec

3.1 Verify Access to FortiOS

3.1.1 Log into FortiOS

In order to connect to the GUI using a web browser, an interface must be configured to allow administrative access over HTTPS or over both HTTPS and HTTP. If you have not changed the admin account’s password, use the default user name, admin, and leave the password field blank.

Figure 1: FortiOS Login
3.1.2 FortiGate Dashboard

The dashboard displays various widgets that display important system information and allow you to configure some system options. The System Information widget lists information relevant to the FortiGate system, including hostname, serial number, and firmware. The Licenses widget lists the status of various licenses, such as FortiCare Support and IPS.

Figure 2: FortiGate Dashboard
3.2 Prerequisites to Configuring GRE Tunnels

While most of the tasks to configure your FortiGate can be accomplished using the GUI, this configuration guide makes use of advanced features that will require the CLI for portions of the configuration.

3.2.1 Create GRE Tunnels

GRE tunnels are configured using the FortiGate CLI. In the below configuration, “remote-gw” is the IP address of your Zscaler tunnel; “local-gw” is the IP address of your FortiGate’s ISP facing interface.

This step creates the GRE tunnels and adds them as interfaces to the FortiGate:

```
config system gre-tunnel
    edit "GRE-SITE1"
        set interface "wan1"
        set remote-gw 199.168.148.131
        set local-gw 72.52.82.217
    next
    edit "GRE-SITE2"
        set interface "wan1"
        set remote-gw 104.129.194.38
        set local-gw 72.52.82.217
    next
end
```

Figure 3: Example GRE Configuration
3.2.2 Configure GRE Tunnel Interfaces

This next step configures the newly-created FortiGate interfaces. In this config, “ip” is an address in a /30 subnet provided by Zscaler for the express purpose of GRE tunnel connectivity.

```plaintext
config system interface
  edit "GRE-SITE1"
    set ip 172.17.12.12 255.255.255.255
    set allowaccess ping
    set type tunnel
    set interface "wan1"
next
edit "GRE-SITE2"
  set ip 172.17.12.13 255.255.255.255
  set allowaccess ping
  set type tunnel
  set interface "wan1"
next
end
```

Figure 4: Example GRE Configuration
3.3 Performance SLAs

This section will explain how to configure Layer-7 Health Checks (aka “HTTP Ping”).

3.3.1 Prerequisites to Configuring Performance SLAs

If you have not yet done so, please configure SD-WAN interfaces as described in section 3.6. Performance SLAs cannot be configured on your FortiGate unless SD-WAN is enabled and at least one interface is marked as an SD-WAN member interface.

3.3.2 Configuring Performance SLAs

We will need to use the CLI to enable Performance SLA health checks on your new GRE tunnels:

```
config system virtual-wan-link
  config health-check
    edit "Zscaler_VPNTEST"
      set server "gateway.zscalerbeta.net"
      set protocol http
      set http-get "/vpntest"
      set interval 10000
      set failtime 10
      set members 1 2
    config sla
      edit 1
        set latency-threshold 250
        set jitter-threshold 100
        set packetloss-threshold 5
    next
  end
next
end
```

Figure 5: Example GRE Configuration

Note: The rest of this document after this point will only use the HTTP GUI.
3.4 **Configuring IPsec Tunnels**

The remainder of this section will only use the web GUI.

### 3.4.1 IPsec Wizard

To create the VPN, go to VPN > IPsec Wizard and create a new tunnel using a pre-existing template. Name the VPN. The tunnel name cannot include any spaces or exceed 13 characters.

![Figure 6: IPsec Wizard – Step #1](image-url)
3.4.2 Configure IPsec - General

Configure your “Network” settings to make below. The “Dynamic DNS” entry should be the hostname to the Zscaler ZEN you wish to use.

![IPsec Wizard – Step #2](image)

Figure 7: IPsec Wizard – Step #2
3.4.3 Configure IPsec – Phase 1

Now we will configure Phase 1 of IPsec. Configure your settings to match below. The “Pre-shared Key” (PSK) should be unique per site. The “Local ID” should be the FQDN you configured in the previous sections.

![IPsec Wizard – Step #3](image)

**Figure 6: IPsec Wizard – Step #3**
3.4.4 Configure IPsec – Phase 2

Now we need to configure Phase 2 of IPsec. Configure your settings to match the screen capture below. Once completed, save these settings.

Figure 7: IPsec Wizard – Step #4
3.4.5 Verify IPsec Configuration

After saving your settings, you should see your tunnels “Up”. If they do not establish, recheck your Pre-Shared Key.

Figure 8: Verify IPsec Configuration
3.5 Configuring Firewall Policy

3.5.1 Create Firewall Policy

Next you will create a Firewall policy. Your settings should match what is configured below. Your “Outgoing Interface” may have a different name, so please adjust this setting to match your Internet facing link.

![Configure Firewall Policy]

**Figure 9: Configure Firewall Policy**
3.5.2 Verify Firewall Policies

Next you need to repeat the steps in the following section as shown below.

![Figure 10: Verify Firewall Policies](image-url)
3.6  Configuring SD-WAN

In this section, we will the primary and secondary Zscaler ZEN to be a member of the SD-WAN

3.6.1  Create SD-WAN Member for Primary ZEN

First, we will configure the primary ZEN, as a SD-WAN member, with a cost of 5.

![Figure 11: Config SD-WAN for Primary ZEN](image-url)
3.6.2 Create SD-WAN Member for Backup ZEN

Next, we will configure the primary ZEN, as a SD-WAN member, with a cost of 10. By having a higher cost than the prior SD-WAN member will determine this SD-WAN member to be secondary.

![Figure 12: Config SD-WAN for Secondary ZEN](image)
3.6.3 Verify SD-WAN Members

Once both SD-WAN members are configured, verify the configuration. Your screen should look similar to the screen below.

Figure 13: Verify SD-WAN Members
3.7 Configuring SD-WAN Rules

In this section, we will configure a SD-WAN rule. This will tie the Performance SLA probe to each SD-WAN member for the primary and secondary ZEN.

3.7.1 Create SD-WAN Rule

By using a “strategy” of “Lowest Cost (SLA)”, this will determine which ZEN will be the active primary and which ZEN will be the standby secondary.

Figure 14: Configure SD-WAN Rule
### 3.7.2 Verify SD-WAN Rule

Once you have configured your SD-WAN rule, please verify your configuration. Your screen should look similar to what is shown below.

![Verify SD-WAN Rule](image)

**Figure 15: Verify SD-WAN Rule**
4 Verify Configuration with Zscaler Test Page

4.1 Request Verification Page

The URL https://ip.zscaler.com can be used to validate if you are transiting ZIA. This is what you will see if you are not transiting ZIA.

![Non-working Example](image)

Figure 20: Non-working Example

If you are transiting ZIA, you should see the following:

![Working Example](image)

Figure 21: Working Example
5 Requesting Zscaler Support

5.1 Gather Support Information

5.1.1 Obtain Company ID

The navigation is: Administration -> Settings -> and then click Company profile

Figure 30: Collecting details to open support case with Zscaler TAC
5.1.2 Save Company ID

Figure 31: Company ID
5.1.3 Enter Support Section

Now that we have our company ID, we are ready to open a support ticket. The navigation is: “?” and then click **Submit a Ticket**.

![Submit a Ticket](image)

**Figure 32: Submit ticket**
6 Appendix A: Zscaler Resources

Zscaler: Getting Started
https://help.zscaler.com/zia/getting-started

Zscaler Knowledge Base:
https://support.zscaler.com/hc/en-us/?filter=documentation

Zscaler Tools:
https://www.zscaler.com/tools

Zscaler Training and Certification:
https://www.zscaler.com/resources/training-certification-overview

Zscaler Submit a Ticket:
https://help.zscaler.com/submit-ticket

ZIA Test Page
http://ip.zscaler.com/
7 Appendix B: Fortinet Resources

FortiOS Handbook:
https://docs.fortinet.com/document/fortigate/6.0.0/handbook

FortiOS Cookbook:
https://docs.fortinet.com/document/fortigate/6.2.0/cookbook

FortiOS Knowledge Base:
https://kb.fortinet.com/kb/microsites/microsite.do

FortiOS CLI Reference:
https://docs.fortinet.com/document/fortigate/6.2.2/cli-reference

FortiOS Best Practices:
https://docs.fortinet.com/document/fortigate/6.2.0/best-practices/587898/best-practices

FortiOS Hardening Guide:
https://docs.fortinet.com/document/fortigate/6.2.0/hardening-your-fortigate/612504/hardening-your-fortigate

Fortinet Training & Certification:
https://training.fortinet.com/course/index.php

Fortinet Support:
https://support.fortinet.com