FORCEPOINT

Forcepoint GRE Guide

Forcepoint Web Security Cloud and Hybrid Solutions

2022

Contents

Contents

ii ◄ Forcepoint Web Security Cloud

1

Introduction

Forcepoint GRE connectivity can be used to forward traffic from your network's edge devices to the Forcepoint cloud service over a GRE tunnel. This guide introduces the basics of Forcepoint's GRE solution, and provides information on planning and deploying GRE in your network.

Introduction to the Forcepoint GRE solution

Generic Routing Encapsulation (GRE) is a tunneling protocol used to encapsulate and route data via a virtual point-to-point connection. Forcepoint GRE supports manual end user authentication and transparent identification via NTLM. Transparent authentication allows users to browse the Internet without explicitly providing logon credentials.

Typical uses for the GRE service include providing Forcepoint Web Security Cloud/ Hybrid protection for:

- Remote offices
- Guest Wi-Fi networks
- Organizations that do not want a Group Policy Object (GPO) or browser configuration
- Organizations that are unable to or do not want to install an endpoint on client machines
- Organizations with a "bring your own device" policy.

Benefits

Using GRE to forward traffic to the cloud service can provide a number of benefits. These include:

- Easy to configure
- Connection to two Forcepoint points of presence for redundancy
- No need to install endpoint software on client machines or deploy browser configuration PAC files through Group Policy Objects - ideal for BYOD or guest networks.
- Your network's internal IP addresses are available to the cloud service, so:
    - Policies can be created based on internal IP addresses or address ranges
    - Authentication bypass can be set based on IP addresses or address ranges
    - Reports can be created using internal IP addresses to identify individual users.

Capacity planning

Forcepoint GRE supports up to 5Gbps throughput per tunnel and 1,000,000 concurrent connections.

By default, tunnels are configured for 200Mbps throughput. Customers requiring more than the default can submit a request to Forcepoint Technical Support.

Supported devices

Most devices that support GRE tunneling, and that are able to forward port 80 and port 443 traffic to the tunnel, can be used with the service. Forcepoint recommends using the latest firmware for your device.

Redundancy and failover

By default, two Forcepoint points of presence are provided for GRE connectivity. Forcepoint strongly recommends configuring your device to fail over to a second point of presence (data center or local PoP) cluster to achieve geographic redundancy.

> **Note**
> Connection redundancy is a requirement for the Forcepoint Web Security Cloud SLA. Redundancy can be achieved by configuring connections to both point of presence addresses provided and configuring your device to fail over in the event of network disruption.

Point of Presence locations

Point of Presence (data center or local PoP) IP addresses for Forcepoint's GRE service are listed in the article IP addresses for GRE connectivity in the Forcepoint Knowledge Base.

To decide which points of presence are best for your environment, consider:

- Which points of presence are nearest
- Any geographical or data sovereignty concerns around where users browse or where their reporting data is stored.

> **Note**
>
> Cross-point of presence failover can change an end user's browsing experience. For example, some sites may change localization or presentation between a UK PoP and a German PoP (for example, www.google.co.uk might automatically redirect to www.google.de or www.google.nl, depending on which points of presence users' traffic is directed though).
>
> Bear in mind that point of presence failover should be an exceptional occurrence, so this behavior might be acceptable in emergency circumstances.

Use the **Cloud Service Status** option provided in the banner of the Cloud Security Gateway Portal for tunnel system status. You must first subscribe to the physical data center connected to the Points of Presence configured on the **Web > Device Management** page of the portal.

2 | Configuration steps

This section details the configuration process for setting up your service for GRE connectivity, and covers the following topics:

- *Step 1: Cloud portal configuration*
- *Step 2: device configuration*

Step 1: Cloud portal configuration

Add your GRE device in the cloud portal, via the **Web > Device Management** page (this requires that your administrator account has the Manage Edge Devices permission). To add a device:

1. Define the device name, type, public IP address, and an optional description.
2. Under **Points of Presence (PoPs)**, use the drop-down lists provided to select the two most appropriate points of presence (data center or local PoP) to connect to.
3. Select a default policy to handle traffic from your GRE device.
4. Optionally, define specific policies to apply to different internal networks managed by your device.

For each connection, the destination (PoP) inner tunnel address and source (edge device) inner tunnel IP address are provided when the data is saved. You will need these addresses to configure the tunnel on your device.

See Managing Network Devices in the Forcepoint Web Security Cloud help for further details, including information on bulk uploading devices using a CSV file.

> **Note**
> By default, you can create 200 tunnel connections for your account. To add more connections, contact your sales account manager to discuss your requirements.
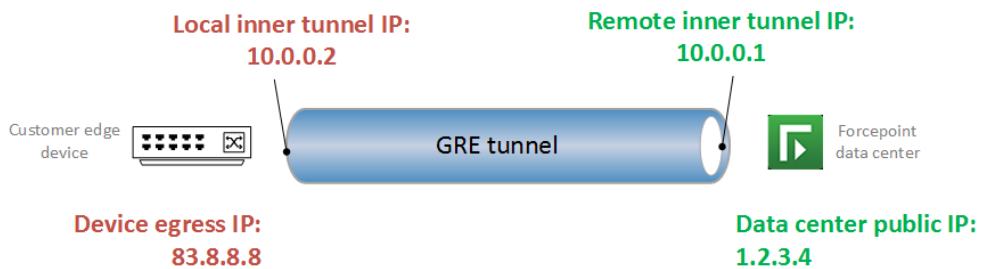
Step 2: device configuration

Configure your device for GRE connectivity based on the manufacturer's guidelines, using the IP addresses provided by Forcepoint. Configure your device to forward port 80 and port 443 traffic through the GRE tunnel.

You will need the destination (PoP) inner tunnel address and source (edge device) inner tunnel address for each connection. These are available in the cloud portal.

Two point of presence (data center or local PoP) connections are provided for each device. Forcepoint **strongly recommends** that you configure your device to fail over to the secondary tunnel to achieve cluster redundancy.

An example GRE configuration is shown in the diagram below. (Note that the addresses used below are examples only.)

Example configuration instructions for Juniper SRX and Cisco ISR are provided in the section *Example device configuration*, page 9.

> **Important**
> Once you have completed device configuration, ensure that the remote inner tunnel IP address can be pinged.

Maximum segment size (MSS)

The encapsulation overhead of the GRE tunnel means that TCP sessions sent over the tunnel must be limited to a lower Maximum Segment Size (MSS) than usual. Most TCP clients will propose an MSS value of 1460 bytes when connecting over an Ethernet network. The GRE encapsulation overhead comprises 24 bytes (4 bytes for the GRE header, and 20 bytes for the inner IP header).

TCP clients must use an MSS value of no more than 1436 bytes for GRE. This can often be achieved by using the MSS clamping feature of a firewall or router, to ensure that any TCP traffic sent down the GRE tunnel is limited to an MSS value of 1436.

Where the WAN connection to Forcepoint's points of presence is using the IPoE or PPPoE protocol, the MSS value may need to be lower still, to account for the encapsulation overhead of the WAN connection.

To display the current MSS setting for your tunnel interface, use the appropriate "show interface" command on your edge device.

Preventing data leakage

As a best practice, Forcepoint recommends that you lock down your firewall to prevent traffic leakage via different protocols and ports. In particular, Google Chrome can default to the experimental QUIC protocol, which uses UDP on port 443. We recommend that you block UDP traffic on port 443 in order to force traffic over TCP. For more information, see the Knowledge Base article Google QUIC protocol is not supported by the Forcepoint cloud service.

Tunnel status

Forcepoint GRE Guide | Forcepoint Web Security Cloud and Hybrid Solutions

After your device has successfully connected to the service, the device status is displayed on the **Web > Device Management** page.

The device status icons are as follows:

Icon	Description	Explanation
✓	Up	The tunnel is successfully connected.
⚠	Unknown	No updates have been received from the device in the last 5 minutes.
✗	Down	No updates have been received from the device in the last hour.
○	Status not available	No connection attempts have been detected for this device.

3 Example device configuration

This section provides an example GRE configuration for the following devices:

- *Cisco ISR* (version 12.4 and higher)
- *Juniper SRX* (version 12.1 R2 and higher)

The table below details the abbreviations used in the configuration examples. Replace these with the appropriate IP addresses for your configuration.

IP address	Description	Abbreviation used
Primary point of presence public IP	Public IP address of the Forcepoint point of presence used for your primary tunnel.	\<primary_dc_public_ip\>
Primary local inner tunnel IP	Inner IP address for the local (edge device) end of the primary tunnel.	\<primary_local_inner_ip\>
Primary remote inner tunnel IP	Inner IP address for the remote (point of presence) end of the primary tunnel.	\<primary_remote_inner_ip\>
Secondary point of presence public IP	Public IP address of the Forcepoint point of presence used for your secondary tunnel.	\<secondary_dc_public_ip\>
Secondary local inner tunnel IP	Inner IP address for the local (edge device) end of the secondary tunnel.	\<secondary_local_inner_ip\>
Secondary remote inner tunnel IP	Inner IP address for the remote (point of presence) end of the secondary tunnel.	\<secondary_remote_inner_ip\>
Edge device public IP	The public egress IP address for your edge device.	\<device_egress_ip\>
Client subnet IP	IP address range for the internal subnet whose traffic will be forwarded to the tunnel.	\<client_subnet\>
Gateway IP	The IP address of your internet gateway.	\<gateway_ip\>

Cisco ISR

The following GRE configuration example is for Cisco ISR version 12.4 or higher.

Use the following commands to configure tunnels to the primary and secondary point of presence.

```
interface Tunnel0
ip address <primary_local_inner_ip> 255.255.255.252
ip tcp adjust-mss 1436
tunnel source <device_egress_ip>
tunnel destination <primary_dc_public_ip>

interface Tunnel1
ip address <secondary_local_inner_ip> 255.255.255.252
ip tcp adjust-mss 1436
tunnel source <device_egress_ip>
tunnel destination <secondary_dc_public_ip>
```

Create a policy-based routing rule to route port 80 and 443 traffic through the tunnel. Access-list commands:

```
access-list 104 permit tcp <client_subnet> 0.0.0.255 any eq
www
access-list 104 permit tcp <client_subnet> 0.0.0.255 any eq
443
```

Route-map commands:

```
route-map Primary_Tunnel permit 11
match ip address 104
set interface Tunnel0

route-map Failover_Tunnel permit 12
match ip address 104
set interface Tunnel1
```

Attach the primary tunnel's route-map to the incoming interface:

```
interface <incoming_interface_name>
ip address <client_subnet> 255.255.255.0
ip nat inside
ip virtual-reassembly in
ip policy route-map Primary_Tunnel
duplex auto
speed auto
```

Create an IP SLA configuration for automatic tunnel failover:

```
ip sla 4
icmp-echo <primary_dc_public_ip> source-interface
<egress_interface_name>
threshold 3000
timeout 30000
frequency 30
ip sla schedule 4 life forever start-time now

track 4 ip sla 4
delay down 10 up 10

event manager session cli username <username>

event manager applet failover_if_primary_tunnel_goes_down
event track 4 state down
action 001 cli command "conf t"
action 002 cli command "interface <incoming_interface>"
action 003 cli command "ip policy route-map Failover_Tunnel"

event manager applet route_back_to_primary_when_available
event track 4 state up
action 001 cli command "conf t"
action 002 cli command "interface <incoming_interface>"
action 003 cli command "ip policy route-map Primary_Tunnel"
```

Useful show commands

Command	Description
show interfaces tunnel 0	Displays connection statistics for the tunnel to the primary point of presence
show interfaces tunnel 1	Displays connection statistics for the tunnel to the secondary point of presence
show track brief	Displays brief IP SLA connection statistics
show track 4	Displays detailed IP SLA connection statistics
show ip sla statistics	Displays IP SLA operation statistics

Juniper SRX

The following GRE configuration example is for Juniper SRX version 12.1 R2 and higher.

Use the following commands to configure tunnels to the primary and secondary point of presence.

```
show interfaces gr-0/0/0
unit 0 {
description primary;
tunnel {
source <device_egress_ip>;
destination <primary_dc_public_ip>;
}
family inet {
address <primary_local_inner_ip>/30;
}
}
unit 1 {
description backup;
tunnel {
source <device_egress_ip>;
destination <secondary_dc_public_ip>;
}
family inet {
address <secondary_local_inner_ip>/30;
}
}

set interfaces gr-0/0/0 unit 0 description primary
set interfaces gr-0/0/0 unit 0 tunnel source
<device_egress_ip>
set interfaces gr-0/0/0 unit 0 tunnel destination
<primary_dc_public_ip>
set interfaces gr-0/0/0 unit 0 family inet address
<primary_local_inner_ip>/30
set interfaces gr-0/0/0 unit 1 description backup
set interfaces gr-0/0/0 unit 1 tunnel source
<device_egress_ip>
set interfaces gr-0/0/0 unit 1 tunnel destination
<secondary_dc_public_ip>
set interfaces gr-0/0/0 unit 1 family inet address
<secondary_local_inner_ip>/30
```

Configure routing instances:

```
show routing-instances
route_to_gre_1 {
instance-type forwarding;
routing-options {
static {
route 0.0.0.0/0 {
next-hop gr-0/0/0.0;
qualified-next-hop gr-0/0/0.1 {
preference 10;
}
}
}
}


set routing-instances route_TO_GRE_1 instance-type
forwarding
set routing-instances route_to_gre_1 instance-type
forwarding
set routing-instances route_to_gre_1 routing-options static
route 0.0.0.0/0 next-hop gr-0/0/0.0
set routing-instances route_to_gre_1 routing-options static
route 0.0.0.0/0 qualified-next-hop gr-0/0/0.1 preference 10
```

Configure routing options:

```
show routing-options
interface-routes {
rib-group inet route_t0_gre_1;
}
static {
route 0.0.0.0/0 next-hop <gateway_ip>;
}
rib-groups {
route_t0_gre_1 {
import-rib [ inet.0 route_to_gre_1.inet.0 ];
}
}


set routing-options interface-routes rib-group inet
route_t0_gre_1
set routing-options static route 0.0.0.0/0 next-hop
<gateway_ip>
```

```
set routing-options rib-groups route_t0_gre_1 import-rib
inet.0
set routing-options rib-groups route_t0_gre_1 import-rib
route_to_gre_1.inet.0
```

Firewall policy configuration:

```
show firewall


filter TO_GRE_1 {
term 0 {
from {
source-address {
<client_subnet>/24;
}
destination-port [ 80 443 ];
}
then {
log;
routing-instance route_to_gre_1;
}
}
term 1 {
then {
log;
accept;
}
}
}


set firewall family inet filter TO_GRE_1 term 0 from source-
address <client_subnet>/24
set firewall family inet filter TO_GRE_1 term 0 from
destination-port 80
set firewall family inet filter TO_GRE_1 term 0 from
destination-port 443
set firewall family inet filter TO_GRE_1 term 0 then log
set firewall family inet filter TO_GRE_1 term 0 then
routing-instance route_to_gre_1
set firewall family inet filter TO_GRE_1 term 1 then log
set firewall family inet filter TO_GRE_1 term 1 then accept
```

Attach the firewall policy to the incoming interface:

```
<incoming_interface_name> {
```

```
unit 0 {
family inet {
filter {
input TO_GRE_1;
}
address <client_subnet>/24;
}
}
}


set interfaces <incoming_interface> unit 0 family inet
filter input TO_GRE_1
set interfaces <incoming_interface> unit 0 family inet
address <client_subnet>/24
```

Security zone configuration:

```
show security zones


security-zone gre {
host-inbound-traffic {
system-services {
all;
}
protocols {
all;
}
}
interfaces {
<egress_interface_name>;
gr-0/0/0.0;
gr-0/0/0.1;
}
}


set security zones security-zone gre host-inbound-traffic
system-services all
set security zones security-zone gre host-inbound-traffic
protocols all
set security zones security-zone gre interfaces
<egress_interface_name>
set security zones security-zone gre interfaces gr-0/0/0.0
set security zones security-zone gre interfaces gr-0/0/0.1
```

Tunnel failover configuration:

```
show services
rpm {
probe ping_primary_DC_IP {
test primary_tunnel {
probe-type icmp-ping;
target address <primary_dc_public_ip>;
probe-count 5;
probe-interval 2;
test-interval 2;
thresholds {
successive-loss 5;
total-loss 5;
}
}
}
}

ip-monitoring {

policy failover {
match {
rpm-probe ping_primary_DC_IP;
}
then {
interface gr-0/0/0.1 {
enable;
}
interface gr-0/0/0.0 {
disable;
}
}
}
}

set services rpm probe ping_primary_DC_IP test
primary_tunnel probe-type icmp-ping
set services rpm probe ping_primary_DC_IP test
primary_tunnel target address <primary_dc_public_ip>
```

```
set services rpm probe ping_primary_DC_IP test
primary_tunnel probe-count 5

set services rpm probe ping_primary_DC_IP test
primary_tunnel probe-interval 2

set services rpm probe ping_primary_DC_IP test
primary_tunnel test-interval 2

set services rpm probe ping_primary_DC_IP test
primary_tunnel thresholds successive-loss 5

set services rpm probe ping_primary_DC_IP test
primary_tunnel thresholds total-loss 5


set services ip-monitoring policy failover match rpm-probe
ping_primary_DC_IP

set services ip-monitoring policy failover then interface
gr-0/0/0.1 enable

set services ip-monitoring policy failover then interface
gr-0/0/0.0 disable
```

Useful show commands

Command	Description
show services ip-monitoring status	Displays a summary of the current IP monitoring status for failover
show services rpm probe-results	Displays the result of the most recent real-time performance (RPM) monitoring probes
show interfaces gr-0/0/0	Displays the current status of the GRE interface
show route	Displays active entries in your device's routing tables

4 | Next steps

Once you have completed the setup steps in the preceding section, your next steps are to:

- *Enable notification pages for HTTPS sites* (if required)
- *Configure browsers for NTLM identification* (if required)
- *Using single sign-on*
- Ensure you have configured policies to manage traffic from your network. See Forcepoint Web Security Cloud Help - Defining Web Policies for information on policy configuration.
- *Test your policies*.

Enable notification pages for HTTPS sites

In order for notification pages to be displayed for HTTPS sites - for example, block pages if the website is in a category that is blocked, or the Pre-logon welcome page for authentication - you must configure a root certificate on each client machine. This acts as a Certificate Authority for secure requests to the cloud proxy.

The setting is found on the **Web > Block & Notification Page**s page, under Settings. To enable it, mark the checkbox **Use certificate to serve notifications for HTTPS pages**.

This page also has a link to download the Forcepoint root certificate, which should be installed on client machines. For further details, see Forcepoint Web Security Cloud Help - Configure Block & Notification Pages.

Configure browsers for NTLM identification

If you are using NTLM identification, you must add the authentication URLs for the Forcepoint cloud service to your browsers' local intranet zone.

The following URLs must be trusted:

```
http://proxy-login.blackspider.com

https://ssl-proxy-login.blackspider.com
```

For guidance on adding these URLs for various browsers, see the following article in the Forcepoint Knowledge Base: Configuring browsers for NTLM identification.

Using single sign-on

Single sign-on using the SAML standard is supported for GRE tunneling.

Single sign-on must be configured in the cloud portal. See Configure Single Sign-On settings in the cloud portal Admin Guide for more information.

Test your policies

Your policies can be tested using the proxy query page:

http://query.webdefence.global.blackspider.com/?with=all

Verify that traffic is going through the cloud service and that the correct policies are being applied. The following graphic shows the result of a successful test.

Confirmation Page

✔ Yes: you are using the Filtering Proxy Server

Server Information

Version   7.9.50787.265
Hostname prx32g.srv.mailcontrol.com

Policy chain

Customer name Policy name

Shows your account and policy information.

Connection Information

Your external IP address
Proxy   1.1 hosted.websense 32g

HTTP headers

via   1.1 hosted.websense 32g
accept-language en-US,en;q=0.5
accept-encoding gzip, deflate
x-forwarded-for
accept   text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
user-agent   Mozilla/5.0 (Windows NT 6.1; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0
host   query.webdefence.global.blackspider.com
client-ip

5 | Limitations

The following items are known limitations of the Forcepoint GRE solution.

- Internet Explorer: version 7 and above is required. Versions earlier than this do not support SNI, which is required for Forcepoint GRE.

- SNI is required for HTTPS traffic when using transparent proxy.

    ■ Windows XP does not support SNI and is, therefore, not supported for Forcepoint GRE.

    ■ Encrypted Client Hello (aka Encrypted SNI) is not supported when using transparent proxy.

- To support PAC file enforcement, you must use the alternate (port 80/443) PAC file address. The standard PAC file address (using port 8082/8087) is not supported.

- Forcepoint Web Security Endpoint is not supported for use with Forcepoint GRE.

- Secure form-based authentication is not supported for use with Forcepoint GRE.

- When using GRE tunneling, Dropbox is not supported for use with the Protected Cloud Apps feature in Forcepoint Web Security Cloud.

- Safari: if the customer policy has authentication enabled, Safari users must change the **Block cookies** setting to **Never** to ensure web pages load properly.

6 Troubleshooting

The following table lists some problems that may be encountered in configuring and establishing your tunnel, with some suggested actions.

Problem	Suggested actions

The GRE tunnel cannot be established	• Check the settings for your tunnel against the recommended settings in the *Configuration steps* and *Example device configuration* sections.
	• Check the tunnel interface status.
	  ■ For Cisco devices, use the command: *show interfaces tunnel <tunnel_id>*
	  ■ For Juniper SRX, use the command: *show interface gr-<interface_id>*
	• Check whether you can ping the Forcepoint point of presence IP address from your firewall or router.
	If yes, check whether you can ping the destination (PoP) inner tunnel address from your edge device.
	If you cannot ping these addresses, ensure the expected GRE packets are leaving your edge device.
	• Check whether you can send a simple HTTP request and receive a response. Check whether you can send an HTTPS request and receive a response.
	If not, ensure the expected GRE packets are leaving your edge device.
	• Check that IP protocol 47 (GRE) is enabled in your network.
	• If the edge device performing GRE encapsulation is behind another firewall, check that GRE packets are leaving the egress firewall and that outbound NAT is being performed.
	If not, modify the firewall's rules to allow GRE traffic to be passed through, and to perform outbound NAT processing.
	After performing these checks, if you have determined that GRE packets are successfully leaving your firewall or router, but no response is being received, contact Technical Support.

Problem	Suggested actions
The GRE tunnel is established, but traffic is not flowing	• Check that the TCP Maximum Segment Size (MSS) setting on your edge device is appropriate for your network configuration. Use the appropriate "show interface" command for your device to find the current MSS setting. For more information on MSS settings, see *Maximum segment size (MSS)*, page 6. • Check that policy-based routing (PBR) is attached to the ingress interface and is configured to allow port 80/443 traffic through the GRE tunnel. • Check the tunnel status in the cloud portal, on the **Web > Device Management** page. This page gives an indication of the visibility of your tunnels to the cloud service.
Your tunnel has successfully established, but your policy settings are not being applied	Use the proxy query page to identify which policy is being applied. If necessary, revisit your policy settings. See *Test your policies*, page 20.
When browsing via HTTPS, the user receives a message saying that the connection was reset, or the site unexpectedly closed the connection	Check that the Forcepoint root CA has been imported to the user's browser.
When NTLM is enabled, the user receives an authentication prompt	Use the proxy query page to identify which policy is being applied. If necessary, revisit your policy settings. See *Test your policies*, page 20. Check your NTLM settings. See *Configure browsers for NTLM identification*, page 19. Ensure that your directory synchronization has successfully imported users and groups.
Block pages are not displaying for HTTPS sites	Ensure you have checked the **Use certificate to serve notifications for HTTPS pages** in the cloud portal, on the **Web > Block & Notification Pages** page, under Settings. See *Enable notification pages for HTTPS sites*, page 19.

If you continue to have issues after checking the items above, please contact Technical Support.

Troubleshooting with HAR files

To help diagnose network issues, you can generate a HAR (HTTP Archive) file to log your browser's interaction with a particular website. HAR files can be generated using Google Chrome's Developer Tools, as well as other software packages.