VIRTUAL ACCESS

SMART NETWORK SOLUTIONS
FOR SERVICE PROVIDERS

PingFailover VPN Script

Issue: 1.1

Date: 27 February 2014

1 Introduction

This document describes how to use the failover script pingFailoverVpn to enable IPSec tunnels when an interface availability is marked as down by pingFailover script. The pingFailover script uses ping targets to determine primary route availability and is typically used for an Ethernet or Bridged primary link (but can be used for any interface type).

The pingFailoverVpn script waits for the pingFailover script to signal primary interface up or down. When the primary interface is determined to be down, the pingFailover script disables the primary link default to allow other configured default routes to take priority. When this happens the pingFailoverVpn script will enable the required IPsec tunnels for routing over the backup interface.

The pingFailoverVpn script also provides for recovery mechanisms of both primary and backup interfaces. It will optionally try to fix the issue on the primary link by resetting the interface, and also optionally enable a watchdog script, watchdogPPP, for monitoring the backup interface.

1.1 More information

For detailed information on how to operate the pingFailover script, read the ‘PingFailover Script Controlling an Interface Availability using Pings to Test Targets’, guide.

For detailed information on how to operate the watchdogPPP script, read the ‘WatchdogPPP: Watchdog Monitoring of a PPP Interface’ guide

User guides are available to download on our website.

1.2 Example pinFailoverVpn scenario

The pingFailoverVpn script can be used in a scenario as below. The primary connection is from an Ethernet interface to a third-party gateway device (ADSL, Satellite, WiFi, etc.).

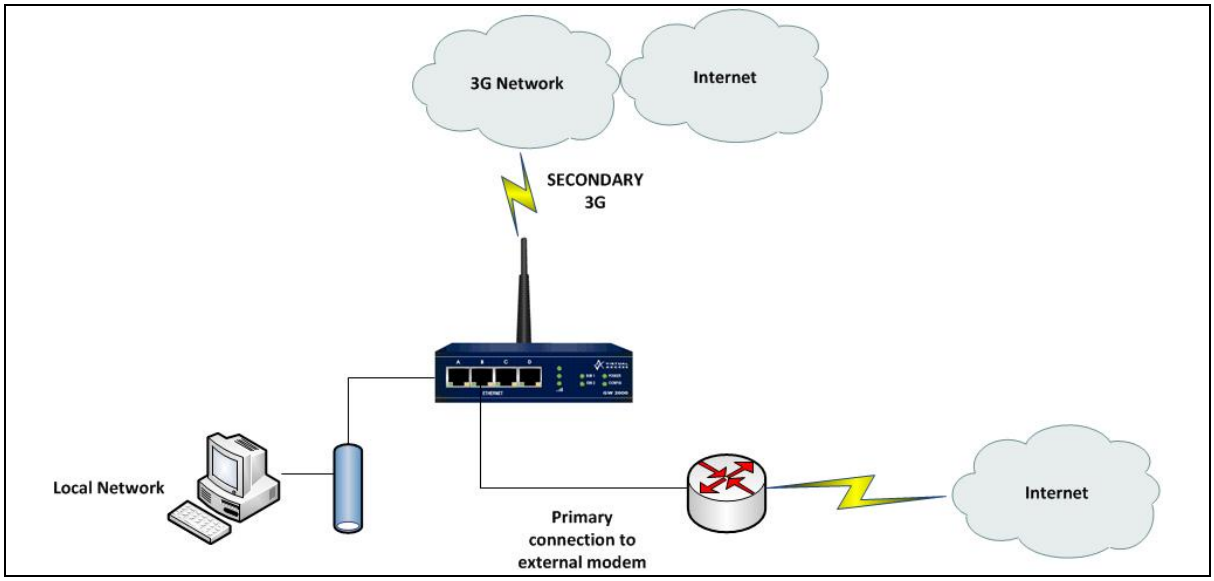

Figure 1: Example network architecture

2 Configuring the pingFailoverVpn script

2.1 pingFailoverVPN Script overview

This script must be run in conjunction with the pingFailover script embedded in firmware. The script can only be run once. It is designed to be run on boot. On boot the script does the following:

- Waits for the pingFailover script to detect that the primary route is unavailable.
- When the primary route is unavailable:
    - The required IKE and SPD policies are enabled.
    - The primary interface is optionally reset in an attempt at recovery.
    - A watchdog script, watchdogPPP, is optionally enabled to dynamically monitor the backup interface. When the script is running and the backup interface goes down, it will attempt recovery of the backup interface and then optionally reset as a last resort.
    - An INFO event is generated for visibility that the IPSec tunnels are enabled and also to allow other scripts to fire where required.
- The script then waits for the pingFailover script to detect that the primary route is available again. When this happens:
    - The IKE and SPD policies are disabled.
    - The watchdog script, watchdogPPP, is stopped.
    - An INFO event is generated for visibility that the IPSec tunnels are now disabled and also to allow other scripts to fire where required.

2.2 Dynamic interface recovery

The pingFailoverVpn script has some dynamic recovery mechanisms to help alleviate generic networks issues common in ADSL and GSM networks.

2.2.1 Primary interface recovery

When the primary default route is unavailable, you can configure the pingFailoverVpn script to reset the primary interface. This can overcome a number of network situations from stale L2TP sessions, interoperability issues between vendor ADSL chipsets to undetectable GSM network issues.

2.2.2 Backup interface recovery

When the backup route is the only route now available it is very important to try and recover quickly from any network issue. In many cases the backup interface is a GSM interface where a number of undetectable network issues can arise especially when the PDP layer disappears. If the backup interface cannot be recovered using one of the recovery procedures then the router can be optionally rebooted.

To do this, you can configure the pingFailoverVpn script to dynamically enable the watchdogPPP script to monitor the backup interface. If PPP is found to be down for more than 2 mins the watchdogPPP script will try and recover using the following recovery procedures:

ADSL backup interface recovery procedure

- The script first forces a manual retrain of the ADSL connection. If this does not fix the issue, then the ADSL chip is reset. Finally if this fails to solve the problem, the script will optionally reboot the router.

GSM backup interface recovery procedure

- The script first hard resets the GSM modem. If this fails to solve the problem, the script will optionally reboot the router.

2.3 Script requirements

- You must use this script in conjunction with pingFailover script.
- You must complete any configuration requirements for the pingFailover script. For more information, read section 2.2 of the ‘PingFailover Script Controlling an Interface Availability using Pings to Test Targets’ guide.
- PingFailoverVpn is embedded in firmware versions 9.09.27 and greater; and 10.00.21 and greater. If you are using firmware prior to these releases, use the script editor to configure the script.
- Run the pingFailoverVpn script using the scheduler on boot.
- You must enable IKE in the configuration.
- You must configure the required IKE and SPD policies, but you can leave them as disabled.
- If you are using multiple IKE or SPD, the policy indexes must be consecutive.

2.4 Script parameters

The script name is pingFailoverVpn and it takes in six required parameters and a further three optional parameters:

pingFailoverVpn [ike start] [ike end] [spd start] [spd end] [reset primary if] [watchdog enabled] [watchdog pppif] [watchdogif] [watchdog reload]

These parameters are described in the example and table below.

pingFailoverVpn 1,0,1,0,adsl-0,1,ppp-2,modem-1,1

Parameter	Type	Description	Default
1	Required	The first IKE policy to enable or disable when primary route unavailable or available.	n/a
0	Required	The end IKE policy to enable or disable when primary route unavailable or available. All policies between first and end policy will be enabled. (0 for only first policy to be enabled).	n/a
1	Required	The first SPD policy to enable or disable when primary route unavailable or available.	n/a
0	Required	The end SPD policy to enable or disable when primary route unavailable or available. All policies between first and end policy will be enabled. (0 for only first policy to be enabled).	n/a
adsl-0	Required	The interface to reset when the primary route is detected as down (0 for no interface reset).	n/a
1	Required	Whether to dynamically enable watchdogPPP script to monitor the backup interface when primary is down (0 to not enable; 1 to enable dynamically).	n/a
Ppp-2	Optional	The interface for watchdogPPP to monitor.	Ppp-2
Modem-1	Optional	The interface for watchdogPPP to reset while in recovery procedure.	Modem-1
1	Optional	Whether to reload the router as a last resort of recovery procedure does not bring the monitored interface back online.	1

Table 1: pingFailover parameter descriptions

2.5 pingFailover script

The pingFailoverVpn script is used in conjunction with the pingFailover script embedded in the firmware.

2.5.1 pingFailover script overview

The pingFailover script is used to control an interface availability using pings to IP targets. This is typically used for an Ethernet or Bridged link but can be used for any interface type.

The pingFailover script sends pings to up to two IP targets at configurable durations. A ping response from either target signifies the primary route is operating as normal.

When a number of configurable consecutive ping failures are detected:

- the monitored interface default route is disabled to allow other default routes to take priority.
- a backup default route is optionally enabled.
- a backup interface is optionally manually connected.
- an INFO event is generated for visibility of the routing change and also to allow other scripts to fire where required.

Pings continue to be sent out the primary route to allow fall back. When a number of consecutive pings are successful:

- the monitored interface default route is enabled.
- a backup default route is optionally disabled.
- a backup interface is optionally manually disconnected.
- an INFO event is generated for visibility of routing change and also to allow other scripts to fire where required.

The pingFailoverVpn script triggers on events:

Severity	Class	Subclass	Text
INFO	49	40	pingFailover primary default route down (index <route_index>).
INFO	49	40	pingFailover primary default route up (index <route_index).

Table 2: PingFailoverVPN script triggers on events

2.5.2 pingFailover script parameters

The pingFailover script takes in three required parameters and a further nine optional parameters:

pingFailover [test-address1] [test-address2] [prim rt index] [sec rt index] [forceBackup] [forceBacupIf] [initwait] [ping failures] [ping wait] [createRouteandFilters] [primaryIf] [ping reply wait]

These parameters are described in the example and table below.

pingFailover 1.1.1.1, 2.2.2.2, 1, 0, 1, ppp-2, 60, 5, 2, 1, ppp-1, 2

Parameter	Type	Description	Default
1.1.1.1	Required	The first ping target.	n/a
2.2.2.2	Required	The second ping target. Set to 0 to signify no second ping target.	n/a
1	Required	The default route index of the interface to be monitored.	n/a
0	Optional	The default route index of the backup interface to automatically enabled or disabled when the monitored interface is unavailable or available (0 for no automatic enable or disable).	0
1	Optional	Whether to force a manual connect or disconnect of the backup interface when the monitored interface is unavailable or available (0 for no manual connect).	1
Ppp-2	Optional	The backup interface to manually enable or disable when the monitored interface is unavailable or available.	Ppp-2
60	Optional	The wait on boot before sending the first ping.	
5	Optional	The number of consecutive pings that signifies the monitored interface as available or unavailable.	5
2	Optional	The wait between pings in seconds. Pings are sent to both ping targets at the same time.	2
1	Optional	Whether to automatically configure static routes and filters for the pings. (0 to not automatically create).	1
ppp-1	Optional	The monitored interface the pings must go out.	ppp-1
2	Optional	The time to wait for a ping reply in seconds (default: 2).	2

Table 3: pingFailover parameter descriptions

For more information, read the guide ‘PingFailover Script: Controlling an Interface Availability using Pings to Test Targets’.

2.6 watchdogPPP script

The pingFailoverVpn script can optionally enable and disable the watchdogPPP script to monitor the backup interface when the primary interface is down.

2.6.1 watchdogPPP script overview

This watchdogPPP script is useful for overcoming generic network problems associated with ADSL or mobile networks.

The script first waits for PPP to establish on the monitored link. If PPP fails to come up within a configurable period of time, the script will start implementing its recovery procedure. If PPP comes up as normal the script will wait for PPP to come down on the monitored link. On PPP down the script will start implementing its recovery procedure. If PPP comes back up on the monitored link then the recovery procedure is terminated.

The recovery procedure is determined by the interface being monitored:

2.6.2 ADSL backup interface recovery procedure

The script first forces a manual retrain of the ADSL connection. If this does not fix the issue, then the ADSL chip is reset. Finally, if this fails to solve the problem, the script will optionally reboot the router.

2.6.3 GSM backup interface recovery procedure

The script first hard resets the GSM modem. If this fails to solve the problem, the script will optionally reboot the router.

2.6.4 watchdogPPP script paramaters

watchdogPPP takes in six optional parameters. These parameters are described in the example and table below.

pingFailover [ppp_port] [ppp_timer] [phy_port] [max_fails] [reload] [init_ppp_wait]

These parameters are described in the example and table below.

watchdogPPP ppp-1, 60, adsl-0, 2, 1, 600

Parameter	Description	Default
ppp-1	The PPP interface to monitor.	ppp-1
60	The frequency of the PPP state check in seconds.	60
adsl-0	The physical port used by recovery procedure.	adsl-0
2	The number of PPP checks before moving to recovery procedure. This number of checks is also used by the recovery procedure before moving to the next stage of recovery.	2
1	Whether to reload the router as a last resort. [0 for no reload, 1 to reload]	1
600	The time to wait in seconds for PPP to establish on boot before initiating PPP state checks.	600

Table 4: Six optional parameters and their descriptions

You can configure the pingFailoverVpn script with parameters 1 (ppp_port), 3 (phy_port) and 5 (reload). It uses watchdogPPP defaults for the remaining parameters.

2.7 Configuring the script

The pingFailoverVpn was introduced into firmware versions 9.09.27 and greater; and 10.00.21 and greater. To use the script on older firmware versions first paste the script from Section 5, ‘pingFailoverVpn script’ into the script editor and then use the scheduler to run the script at boot up.

To open the Expert View menu, from the start page, click **Advanced**.

2.7.1 Pasting the script into the script editor

If you are using 9.09.xx firmware, in the Expert View menu, click **system > scripts->script editor**.

If you are using 10.00.xx firmware, in the Expert View menu, click **system > management > scripts > script editor**.

The Script Editor page appears.

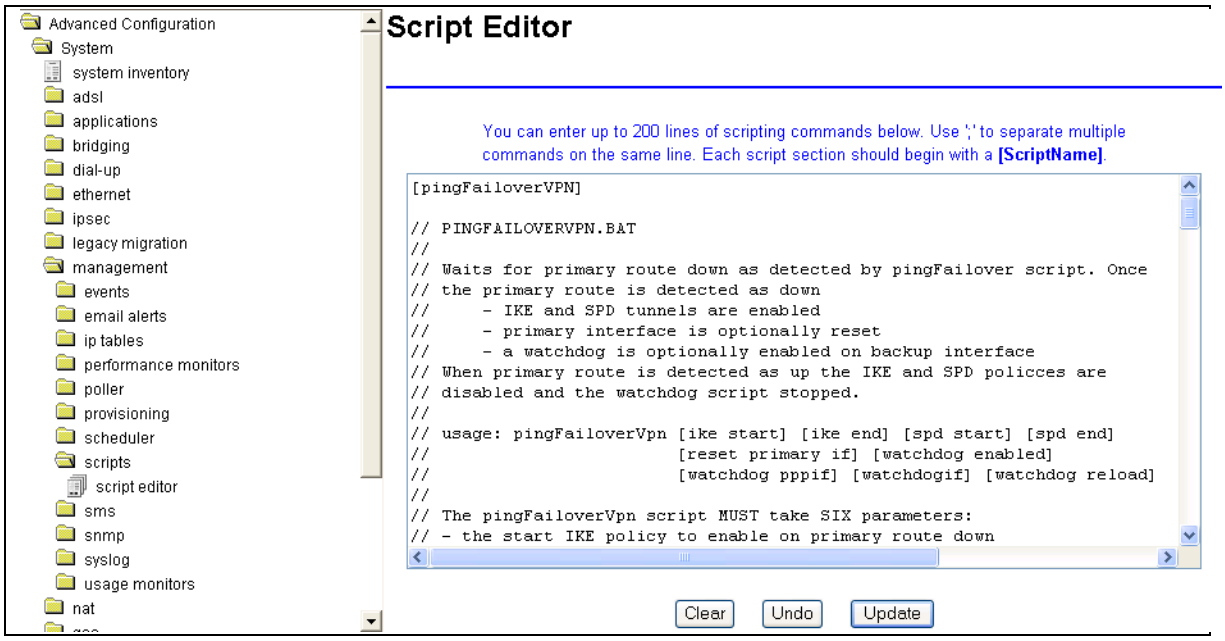

Figure 2: The script editor page in version 9.09.xx

Paste in the script from Section 5, 'pingFailoverVpn Script' The first line of the script should begin with the script name in square brackets, [pingFailoverVpn]. This name will be used to call the script using the scheduler.

If you need to reduce the number of script lines, you can omit any line beginning with //, as this denotes a comment tag. Also, you can enter multiple script lines onto the same script editor line separated by ';' (semi colon). When you have completed the script, click **Update**.

2.7.2 Scheduling the script to run on boot

If you are using 9.09.xx firmware, in the Expert View menu, click **system > scheduler > scheduler tasks**. The Scheduler Task Entry page appears.

Click **add** in the Operation column of the list. The Scheduler Task Form appears.

If you are using 10.00.xx firmware, in the Expert View menu, click **system > management > scheduler > scheduler tasks**. The Scheduler Task Entry page appears.

Click **add** in the Operation column of the list. The Scheduler Task Form appears.

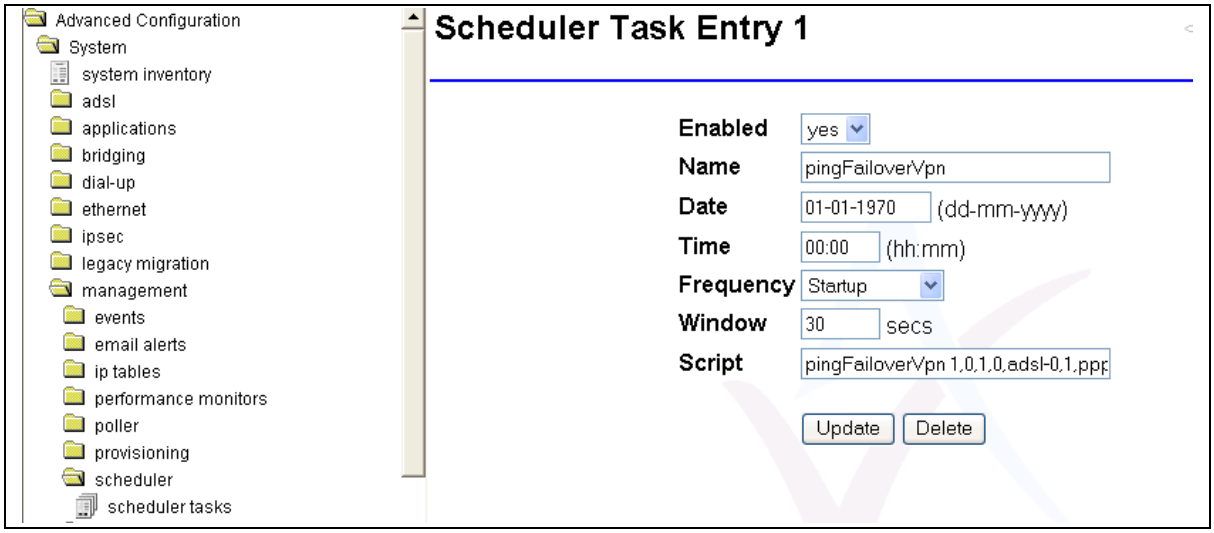

Figure 3: The scheduler task entry page in version 9.09.xx

Field	Description
Enabled	Enables or disables a particular schedule. Set to **Yes**.
Name	The name associated with the schedule. Enter a descriptive name.
Date	The date the script initiates. This field is ignored when frequency is set to start up. Leave at default.
Time	The time the script initiates. This field is ignored when frequency is set to start up. Leave at default.
Frequency	Sets the frequency the script executes. Set to **startup**.
Window	This parameter sets how long the system will wait if it is busy before executing the script. For example if the script is set to execute at 10:00 and the window is set to 30 seconds, the system will try executing the script within this window only. Set to **30**.
Script	The name of the script to be executed. Enter the script name, followed by the relevant parameters as shown in the above image. Separate the parameters by commas. Example: pingFailoverVpn 1,0,1,0,adsl-0,1,ppp-2,modem-1,1

Table 5: The scheduler task fields and their descriptions

3 Debugging commands

Useful debug commands via the command line are described in the table below.

Diagnostic Command	Description
Show tasks	Shows all running tasks.
Show task <tasknum>	Shows running task. Also indicates position task is currently at.
Show task vars <tasknum>	Shows variables and variable values associated with task.
Show ip route	Shows routing table.
Show ip addresses	Shows all interface IP address.
Show active virtual route hits	Shows active virtual routes and hit counts.
Show active filter hits	Shows active filters and hit counts.
Show events	Shows event log.
Dir scripts	Shows all scripts embedded in the firmware.
Show pingFailoverVpn.bat	Displays pingFailoverVpn script.
Show pingFailover.bat	Displays pingFailover script.
Show watchdogPPP.bat	Displays watchdogPPP script.
Show config script ALL	Displays all scripts in the script editor.
Show config script <scriptname>	Displays the <scriptname> script as configured in script editor. Includes line numbers.
Sh ike table	Displays Phase 1 table for enabled IKE policies.
Sh spd table	Displays Phase 2 SPD table for enabled SPD policies.
Sh ike sas	Displays ISAKMP SA table for currently active Phase 1 IKE SA's.
Sh sad table	Displays IPSec SA table for currently active Phase 2 SA's.

Table 6: Debug command lines and their descriptions

Useful trace commands via the command line are described in the table below.

Trace command	Description
++All 6	Traces all INFO events.
++ip:icmp	Traces ICMP traffic.
++ip:500|:4500	Traces IP packets using port 500 and port 4500
++ip:esp|ah	Traces ESP or AH packets.
++script	Traces script events.
--script	Stops script event tracing.
--	Stops all event tracing.
Trace on <script_name>	Traces each line in a script as it executes.
Trace off <script_name>	Turns off tracing for script.

Table 7: Trace command lines and their descriptions

4 Script events

Severity	Class	Subclass	Text
INFO	49	40	pingFailoverVpn disabling IKE and SPD policies on boot.
INFO	49	40	pingFailoverVpn monitoring IKE:<start to end index> SPD: :<start to end index> reset:<reset primary interface> watchdog:<watchdogPPP enabled>
INFO	49	40	pingFailoverVpn enabling ike <start to end index> spd <start to end index>
INFO	49	40	pingFailoverVpn disabling ike <start to end index> spd <start to end index>

5 pingFailoverVpn script

```
[pingFailoverVpn]

// PINGFAILOVERVPN.BAT
//
// Waits for primary route down as detected by pingFailover script. Once
// the primary route is detected as down
//     - IKE and SPD tunnels are enabled
//     - primary interface is optionally reset
//     - a watchdog is optionally enabled on backup interface
// When primary route is detected as up the IKE and SPD polices are
// disabled and the watchdog script stopped.
//
// usage: pingFailoverVpn [ike start] [ike end] [spd start] [spd end]
//                        [reset primary if] [watchdog enabled]
//                        [watchdog pppif] [watchdogif] [watchdog reload]
//
// The pingFailoverVpn script MUST take SIX parameters:
// - the start IKE policy to enable on primary route down
// - the end IKE policy to enable on primary route down
// - the start SPD policy to enable on primary route down
// - the end SPD policy to enable on primary route down
// - the primary interface to reset on route down (0 for no reset)
// - whether to dynamically enable a watchdogPPP script to monitor
//   the backup interface when primary route is down (0 for no watchdog]
//
// It can optionally take THREE parameters:
// - the watchdog PPP interface to monitor (def: ppp-2)
// - the watchdog interface to reset when in recovery procedure (def:
modem-1)
// - whether the watchdog will reload the router in recovery procedure
//   (def: 1) (0 for no reload)
//
// CONFIGURATION
// -------------
```

```
//This script MUST be used in conjunction with pingFailover.bat
// that is embedded in the firmware.
// Both pingFailover and pingFailoverVpn MUST be run on boot.
//
// EXAMPLES
// --------
// pingFailoverVpn 1,0,1,0,adsl-0,1,ppp-2,modem-1,1
// (On default route down enable IKE 1, SPD 1, reset adsl-0 and enable
//  watchdogPPP monitoring ppp-2, modem-1 and reloading on continued
//  failure of ppp-2).

!echo off
!unique
!arg ikeStart, ikeEnd, spdStart, spdEnd, resetPrimary, enableWatchdog

$watchdogPPP = $7
$watchdogIf = $8
$watchdogReload = $9

//set defaults
!if watchdogPPP = ''
  $watchdogPPP = ppp-2
!endif
!if watchdogIf = ''
  $watchdogIf = modem-1
!endif
!if watchdogReload = ''
  $watchdogReload = 1
!endif

//checking VPN policy numbers
!if $ikeEnd < $ikeStart
   $ikeEnd = $ikeStart
!endif
!if ikeEnd > 100
  $ikeEnd = 100
```

```
!endif
!if $spdEnd < $spdStart
   $spdEnd = $spdStart
!endif
!if spdEnd > 200
  $spdEnd = 200
!endif

//logging
$logikestr = $ikeStart
!if $ikeEnd > $ikeStart
  $logikestr = $ikeStart to $ikeEnd
!endif
$logspdstr = $spdStart
!if $spdEnd > $spdStart
  $logspdstr = $spdStart to $spdEnd
!endif
$logwatchdogstr = none
!if $enableWatchdog <> 0
  $logwatchdogstr = $watchdogPPP $watchdogIf
!endif
$logresetstr = none
!if $resetPrimary <> 0
  $logresetstr = $resetPrimary
!endif

// Check invalid save of SPD policies
$changed = 0
$index = $ikeStart
!while index <= ikeEnd
  !if `sh ike policy enabled $index` = yes
    $z = `set ike policy enabled $index, no`
    $changed = 1
  !endif
  !inc index
!endwhile
```

```
$index = $spdStart
!while index <= spdEnd
  !if `sh spd policy enabled $index` = yes
    $z = `set spd policy enabled $index, no`
    $changed = 1
  !endif
  !inc index
!endwhile
!if $changed > 0
  !log pingFailoverVpn disabling IKE and SPD policies on boot
  $z = `commit`
  $z = `vpnreset`
!endif

!log pingFailoverVpn monitoring IKE:$logikestr SPD:$logspdstr
reset:$logresetstr watchdog:$logwatchdogstr

!while 1

  !waitevent script.40:pingFailover_primary_default_route_down
  !endevent

  !label PRIMARY_DOWN
    !log pingFailoverVpn enabling ike $logikestr spd $logspdstr
    !call changeIKE $ikeStart, $ikeEnd, yes
    !call changeSPD $spdStart, $spdEnd, yes
    $z = `commit`
    $z = `vpnreset`

    //ADSL reset
    !if $resetPrimary = "*adsl-"
      $z = `reset adsl $resetPrimary `
    !endif

    //3G modem reset
    !if $resetPrimary = "*modem-"
```

```
        $z = `reset modem $resetPrimary`
    !endif

    !if $enableWatchdog <> 0
      watchdogPPP $watchdogPPP, 60, $watchdogIf, 2, $watchdogReload, 600
    !endif

    !waitevent script.40:pingFailover_primary_default_route_up
    !endevent

  !label PRIMARY_UP
    !log pingFailoverVpn disabling ike $logikestr spd $logspdstr
    !if $enableWatchdog <> 0
      $z = `kill watchdogPPP`
    !endif

    !call changeIKE $ikeStart, $ikeEnd, no
    !call changeSPD $spdStart, $spdEnd, no
    $z = `commit`
    $z = `vpnreset`

!endwhile

[changeIKE]
!arg ikeStart, ikeEnd, value
$index = $ikeStart
!while index <= ikeEnd
  $z = `set ike policy enabled $index, $value`
  !inc index
!endwhile

[changeSPD]
!arg spdStart, spdEnd, value
$index = $spdStart
!while index <= spdEnd
  $z = `set spd policy enabled $index, $value`
```

```
  !inc index
!endwhile
```