SSL VPN Self-Monitoring and Failover Script Readme

June 7, 2007

1 Introduction

The SSL VPN self-monitoring and failover scripts provide automatic monitoring and failover support for the SSL VPN servers that are behind the NetWare Access Gateway or a Linux Access Gateway (SP1). These scripts run on each of the SSL VPN servers.

When the SSLVPN server health status is bad, the scripts the IPTables entries on the SSL VPN server to stop the Access Gateway from sending connection requests to the SSL VPN Web server. When the SSL VPN server health status returns to normal, the scripts remove the IPTables entries and allows Access Gateway to communicate to the SSL VPN Web server and start sending new connections to the SSL VPN server.

2 Access Gateway Configuration

1. Add all the SSL VPN servers as origin Web servers to the proxy service that you have defined.
2. In the administration console, click *Access Gateways* > *Edit* > *[Name of Reverse Proxy]* > *[Name of Proxy Service]* > *Web Servers*.
3. Click *TCP Connect Options* on the *Web Servers* Tab.
4. Select the *Round Robin* option in the *Policy for Multiple Destination IP Addresses* field.
5. Select the *Enable Persistent Connections* check box.

3 Installing the Scripts

1. Copy `sslvpn-heartbeat.sh` to the `/opt/novell/sslvpn/bin` directory.
2. Copy `sslvpn-heartbeat` to the `/etc/init.d/`directory.
3. Enter the following command to change `sslvpn-heartbeat.sh` and `sslvpn-heartbeat` into executable files:

   ```
   chmod
   ```

4. Enter the following command to run the script every time the Access Gateway is started:

   ```
   insserv /etc/init.d/sslvpn-heartbeat
   ```

4 Testing the Scripts

1. Entering the following command to stop SSL VPN:

   ```
   /etc/init.d/novell-sslvpn stop
   ```

2. Enter the following command to verify if the scripts have blocked port 8080:

   ```
   iptables -L
   ```

The following lines are displayed if port 8080 is blocked:

```
Chain       sslvpn-heartbeat-chain (1 reference)
target      prot opt source   destination
REJECT      tcp  --  anywhere anywhere    tcp
dpt:http-alt reject-with icmp-port-unreachable
```

3 In the Administration Console, select *Access Gateways* > *[Name of Server]* > *Health*. The following message is displayed if the SSL VPN server is down:

```
The HTTP Reverse Proxy service <reverse proxy name> might not be
functioning properly. Few of the Web servers being accelerated are
unreachable  <sslvpn server IP Address> :8080
```

NOTE: Click *Update from Server* to get the latest health status of the Access Gateway.

---

4 Connect to SSLVPN. Verify that your connection was sent to SSL VPN that is running and not to the one that is marked as down by the Access Gateway.

5 Execute the following command to start SSL VPN:

```
/etc/init.d/novell-sslvpn start
```

6 Enter the following command to verify if the script has removed the block on port 8080:

```
iptables -L
```

The following lines are displayed if the block on port 8080 is removed:

```
Chain sslvpn-heartbeat-chain (1 references)
target      prot opt source   destination
```

7 In the Administration Console, select *Access Gateways* > *[Name of Server]* > *Health* and check that the SSL VPN server is up.

NOTE: Click *Update from Server* to get the latest health status of the Access Gateway.

---

8 Connect to SSL VPN. Verify if your connection was sent to the SSLV PN server that was restarted. It might require several attempts before you can connect to the desired Access Gateway.

9 Repeat Step 1 to Step 8 to verify if the SSL VPN health scripts are working on all the SSLVPN servers.

5 Documentation Conventions

In this documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

A trademark symbol (®, TM, etc.) denotes a Novell trademark; an asterisk (*) denotes a third-party trademark

6 Legal Notices

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export, or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. Please refer to the Novell International Trade Services Web page (http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Novell, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed on the Novell Legal Patents Web page (http://www.novell.com/company/legal/patents/) and one or more additional patents or pending patent applications in the U.S. and in other countries.

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

All third-party trademarks are the property of their respective owners.