Configuring High Availability for Embedded NGX Gateways in SmartCenter

February 2008
# Contents

**Introduction**................................................................................................................... 1

**High Availability Basics and Terminology**......................................................................................... 2

- Active and Passive Gateway States........................................................................................................ 2
- Priority .................................................................................................................................................. 2
- Heartbeats and Synchronization Interface........................................................................................ ..... 4
- Virtual IP Address................................................................................................................................. 5
- High Availability Configuration Types.................................................................................................. 6

**How High Availability Works**........................................................................................................ 9

**Prerequisites** .......................................................................................................................................... 9

**Workflows**.......................................................................................................................................... 10

- Gateway High Availability Workflow .................................................................................................... 10
- WAN High Availability Workflow .......................................................................................................... 11
- WAN High Availability with Virtual WAN IP Address Workflow ......................................................... 12

**Adding UTM-1 Edge Appliances to SmartCenter** ............................................................................... 13

**Configuring the LAN Network's Encryption Domain**.......................................................................... 15

**Configuring a Backup Gateway** ........................................................................................................ 17

**Configuring VPN Communities for Permanent Tunnels** .................................................................... 18

**Simple High Availability Configuration Scenarios** .......................................................................... 19

- Scenario 1: Simple Gateway and WAN HA Configuration with Two Gateways ............................. 19
- Scenario 2: Gateway and WAN HA Configuration with Two Gateways Including Backup Internet Connection .................................................................................................................. 22
- Scenario 3: Gateway and WAN HA Configuration using a Shared WAN Virtual IP Address ........ 25

---

**Introduction**

---
Introduction

It is a well-known fact that in order to keep business transactions working smoothly, it is necessary to have a reliable Internet connection, and keep the network downtime to a minimum, since a period with no Internet connection or access to critical business network resources means loss of business, money, and worker productivity. Therefore, it is important to ensure that your Internet connection is working at all times.

The Check Point UTM-1 Edge appliance's High Availability (HA) feature enables you to create a HA cluster consisting of multiple UTM-1 Edge appliances. All network traffic is routed through one appliance in the cluster, while the rest of the appliances act as backups, so that if the Internet connection fails, the network remains protected and connected to the Internet.

Configuring a HA cluster enables you to:

- Keep your network protected, even in the event of a hardware malfunction
- Ensure that the connection to your email provider is working at all times
- Ensure that remote users and mobile workers have reliable access to internal network resources for business information and transaction
- Allow external users from the Internet to access to your internal Web servers and ASP applications

This document explains how to configure High Availability for a cluster of UTM-1 Edge appliances that are managed by SmartCenter.

Note: This document refers to Check Point UTM-1 Edge appliances version 7.0 or later.
High Availability Basics and Terminology

This section introduces the terms used to discuss HA and explains how HA works.

Active and Passive Gateway States

HA requires the configuration of at least two of identical UTM-1 Edge security appliances. At any given time, one UTM-1 Edge security appliance is in active state, and the other UTM-1 Edge security appliances are in passive state. The currently active appliance is called the Active Gateway, and the currently passive appliances are called Passive Gateways.

A gateway's current state determines its roles:

- The Active Gateway is responsible for processing the current connections and networking tasks. There can be only one Active Gateway in a HA cluster at any given time.
- A Passive Gateway remains in a standby state until the current Active Gateway fails. It then may take over the failed gateway's roles, becoming the new Active Gateway.

The gateways in a HA configuration are collectively called a HA cluster.

Priority

Each UTM-1 Edge security appliance in a HA cluster is configured with a priority: a value that determines whether the gateway is active or passive at a given time. The live gateway with the highest priority on the network is automatically elected as the Active Gateway. If this gateway fails, the gateway with the next-highest priority gateway is elected as the new Active Gateway.

The following table lists the various values that influence a gateway's priority.
## Table 1: Values Influencing the Gateway Priority

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td></td>
</tr>
<tr>
<td>My Priority</td>
<td>This value represents the priority you assigned to a particular gateway. This must be an integer between 1 and 255.</td>
</tr>
<tr>
<td>Internet Connection</td>
<td></td>
</tr>
<tr>
<td>Internet-Primary</td>
<td>This value is the amount that will be deducted from the My Priority value if the primary Internet connection goes down. This must be an integer between 0 and 255.</td>
</tr>
<tr>
<td>Internet-Secondary</td>
<td>If you configured the gateway with a secondary Internet connection, then this value is the amount that will be deducted from the My Priority value if the secondary Internet connection goes down. This must be an integer between 0 and 255.</td>
</tr>
<tr>
<td>Port Tracking Values</td>
<td></td>
</tr>
<tr>
<td>LAN1/LAN2/LAN3/LAN4</td>
<td>This value is the amount that will be deducted from the My Priority value if the relevant LAN port's Ethernet link is lost. This must be an integer between 0 and 255.</td>
</tr>
<tr>
<td>DMZ</td>
<td>This value is the amount that will be deducted from the My Priority value if the DMZ port's Ethernet link is lost. This must be an integer between 0 and 255.</td>
</tr>
</tbody>
</table>
Normally, the gateway's priority is equal to the **My Priority** value. However, if one or both of the following things happens:

- The primary and/or secondary Internet connection goes down.
- One or more LAN ports and/or the DMZ port stops responding.

Then the gateway's priority is calculated as follows:

\[
\text{Priority} = \text{My Priority} - (\text{Internet-Primary} + \text{Internet-Secondary}) - (\text{LAN1} + \text{LAN2} + \text{LAN3} + \text{LAN4} + \text{DMZ})
\]

*Note:* The appliance detects loss of Internet connectivity based on the Dead Connection Detection (DCD) methods configured for each Internet connection.

**Heartbeats and Synchronization Interface**

The Active Gateway sends periodic signals, or *heartbeats*, to the internal network via a *synchronization interface*. The synchronization interface can be any of the following, except the WLAN (Wireless LAN) interface:

- LAN interface
- DMZ interface
- VLAN interface
- Bridge port

The UTM-1 Edge security appliances' synchronization interface ports must be connected to each other, either directly, or via a hub or a switch. For example, in a HA configuration where the LAN is the synchronization interface, the appliance's LAN ports must be connected to each other.

Heartbeats from the Active Gateway will not reach the internal network, or the Active Gateway will stop sending heartbeats if:

- The Active Gateway is not powered on.
- The Active Gateway is not responding, due to a hardware failure.
- The synchronization interface is disconnected or not working.
- The Active Gateway's priority changed (that is, it was lowered).
• A gateway with a higher priority was added to the network and connected to the synchronization interface.

Virtual IP Address

Normally, all enabled interfaces of a UTM-1 Edge appliance in a HA cluster are assigned a dedicated unique IP address. In addition, cluster gateways can share a virtual IP address (VIP) for each internal interface. The Active Gateway in the cluster always uses virtual IP addresses in the following manner:

• The virtual IP address shared by the internal network interfaces is used as the default gateway for the internal network hosts.

• The virtual IP address assigned to the primary Internet connection is used by the Active Gateway in the cluster to connect to the Internet through the interface assigned to the primary Internet connection.

• The virtual IP address assigned to the secondary Internet connection is used by the Active Gateway in the cluster to connect to the Internet through the interface assigned to the secondary Internet connection.
High Availability Configuration Types

The UTM-1 Edge security appliance allows the following types of High Availability cluster configurations:

Table 2: High Availability Configuration Types

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway High Availability</td>
<td>Hosts on the internal UTM-1 Edge appliance networks use the Active Gateway in the HA cluster as the default gateway to the Internet and other subnets.</td>
<td>If the Active Gateway fails, a Passive Gateway will take control of the virtual IP address and become the new Active Gateway. Thus this configuration provides full redundancy to the Internet and UTM-1 Edge appliance subnets.</td>
<td>The new Active Gateway cannot take over the previous Active Gateway's WAN IP address, because although the previous Active Gateway is now passive, its WAN Internet connection remains active. Therefore, the new Active Gateway will have a different WAN IP address than the old Active Gateway, and external users will be unable to access internal servers at UTM-1 Edge appliance networks without knowing the WAN IP address of the new Active Gateway.</td>
</tr>
<tr>
<td>Type</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WAN High Availability</td>
<td>Only the Active Gateway in the HA cluster is connected to the Internet. Passive Gateways will not connect to the Internet, unless their status changes to Active.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Advantages:**

- Allows using a single WAN IP address for all gateways in the HA cluster without IP conflicts.
- Inbound communications are enabled through a single IP address, which is handled by the current Active Gateway. Therefore, changes in cluster gateways’ status (active or passive) are transparent to external users.

**Disadvantages:**

- Since only the Active Gateway is connected to the Internet, Passive Gateways are not dynamically updated by SmartCenter in real time. They are only updated when their status changes to active, and they obtain an Internet connection.
- Passive Gateways cannot be remotely configured through the Internet.
<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAN High Availability with Virtual IP Address</td>
<td>All gateways in the HA cluster share an additional virtual IP address on the WAN interface. The Active Gateway uses the WAN virtual IP address for Internet connections, while the Passive Gateways use their original IP addresses.</td>
</tr>
<tr>
<td></td>
<td>Advantages:</td>
</tr>
<tr>
<td></td>
<td>• All cluster gateways can connect to the Internet simultaneously.</td>
</tr>
<tr>
<td></td>
<td>• Inbound communications are enabled through a single IP address, which is handled by the current Active Gateway. Therefore, changes in cluster gateways’ status (active or passive) are transparent to external users.</td>
</tr>
<tr>
<td></td>
<td>• Passive Gateways can be reached via their original IP addresses.</td>
</tr>
<tr>
<td></td>
<td>• Cluster gateways remain connected to SmartCenter and therefore are always updated with the latest software versions, security policies, and SmartDefense signatures.</td>
</tr>
<tr>
<td></td>
<td>Disadvantages:</td>
</tr>
<tr>
<td></td>
<td>• Requires an additional IP address as the shared WAN virtual IP address.</td>
</tr>
<tr>
<td></td>
<td>• This option is supported only when the UTM-1 Edge appliance is configured with an Internet connection of the Local Area Network (LAN) type.</td>
</tr>
</tbody>
</table>
How High Availability Works

High Availability works as follows:

1. Each gateway is assigned a priority, which determines the gateway's state (active or passive).

2. The Active Gateway sends heartbeats to the network via the synchronization interface.

3. If the heartbeat from the Active Gateway stops (indicating that the Active Gateway has failed), the Passive Gateway with the next-highest priority becomes the new Active Gateway and takes over the virtual IP address.

4. When a gateway that was offline comes back online, or a gateway's priority changes, that gateway sends a heartbeat notifying the other gateways in the cluster.

5. If the gateway's priority is now the highest, it becomes the Active Gateway.

6. Internet connection on each of the cluster gateways behaves according to the WAN HA configuration. In any case, traffic to the Internet will flow through the available Internet connection defined on the current Active Gateway.

Prerequisites

Before configuring HA, the following requirements must be met:

- You must have at least two identical UTM-1 Edge security appliances.
- The UTM-1 Edge security appliances must have identical firmware versions and firewall rules.
- The UTM-1 Edge security appliances' internal networks must be the same.
- The UTM-1 Edge security appliances' Internet IP addresses must be different, but they must share the same virtual IP address.
- Each internal network segment must be connected to a separate hub or switch. In other words, the Active and Passive Gateways' LAN segments must be
connected to one hub/switch, and the Active and Passive Gateways' DMZ segments must be connected to another hub/switch, and so on.

- The UTM-1 Edge security appliances' synchronization interface ports must be connected either directly, or via a hub or a switch. For example, if the DMZ is the synchronization interface, then the DMZ/WAN2 ports on the appliances must be connected to each other.

- The UTM-1 Edge security appliances must use the same credentials to connect to SmartCenter.

Workflows

Gateway High Availability Workflow

To configure Gateway HA

1. Configure the UTM-1 Edge appliances for Gateway HA.
   For information, refer to the User Guide.

2. Add each UTM-1 Edge appliance to SmartCenter as a gateway object with a static IP address.
   See Adding UTM-1 Edge Appliances to SmartCenter on page 13.

3. Configure each gateway object with the same LAN network encryption domain.
   See Configuring the LAN Network's Encryption Domain on page 15.

4. On each gateway object, configure the other gateway object as the backup gateway.
   See Configuring a Backup Gateway on page 17.

5. Add the gateway objects as satellites in a single VPN community.
   For information, refer to SmartCenter documentation.
WAN High Availability Workflow

To configure WAN HA

1. Configure the UTM-1 Edge appliances for WAN HA, by doing the following:
   a. Configure the UTM-1 Edge appliances for Gateway HA.
   b. In the Passive Gateway's Network > Internet > Internet Setup page, select the Do not connect if this gateway is in passive state check box.
      For information, refer to the User Guide.

2. Add a single gateway object to SmartCenter, with either a static or dynamic IP address.
   See Adding UTM-1 Edge Appliances to SmartCenter on page 13.

3. Configure the gateway object's LAN network encryption domain.
   See Configuring the LAN Network's Encryption Domain on page 15.

4. Add the gateway object as a satellite in a VPN community.
   For information, refer to SmartCenter documentation.
WAN High Availability with Virtual WAN IP Address Workflow

To configure WAN HA with virtual WAN IP address

1. Configure the UTM-1 Edge appliances for WAN HA with a Virtual WAN IP Address, by doing the following:
   a. Configure the UTM-1 Edge appliances for Gateway HA.
   b. In each appliance's Setup > High Availability page, in the Virtual IP field next to the desired Internet connection, type the shared virtual IP address. For information, refer to the User Guide.

2. Add each UTM-1 Edge appliance to SmartCenter as a gateway object with a dynamic IP address.
   See Adding UTM-1 Edge Appliances to SmartCenter on page 13.

3. Configure each gateway object with the same LAN network encryption domain.
   See Configuring the LAN Network's Encryption Domain on page 15.

4. On each gateway object, configure the other gateway object as the backup gateway.
   See Configuring a Backup Gateway on page 17.

5. Add the gateway objects as satellites in a single VPN community.
   For information, refer to SmartCenter documentation.

6. Configure the VPN community for permanent tunnels.
   See Configuring VPN Communities for Permanent Tunnels on page 18.
Adding UTM-1 Edge Appliances to SmartCenter

To add a UTM-1 Edge appliance to SmartCenter as a gateway object

1. In SmartDashboard, in the left pane under Network Objects, right-click on Check Point and select New Check Point > VPN-1 UTM Edge Gateway.

   The VPN-1 UTM Edge Gateway window opens displaying the General Properties node.

2. In the Name field, type a name for the gateway object that will represent the UTM-1 Edge appliance.
3. Do one of the following:
   - To configure a static IP address, in the **IP Address** field, type the static IP address of the UTM-1 Edge appliance.
   - To configure a dynamic IP address, select the **Dynamic Address** check box.

**Reminder:** For Gateway HA, you must configure a static IP address. For WAN HA, you can configure either a static or dynamic IP address. For WAN HA with Virtual IP Address, you must configure a dynamic IP address.

4. Select the **VPN** check box.
5. Complete the rest of the fields as desired.
   For information, refer to SmartCenter documentation.
6. To close the gateway object, click **OK**.
Configuring the LAN Network's Encryption Domain

Note: When configuring Gateway HA or WAN HA with Virtual WAN IP Address, the gateway objects' LAN networks must have the same encryption domain.

To configure the encryption domain of a gateway object's LAN network

1. In SmartDashboard, in the desired gateway object, click the **Topology** node.
   
   The **Topology** node appears.

![Topology Node](image)

2. In the table, double-click on **LAN**.

![Topology Table](image)
WAN High Availability with Virtual WAN IP Address Workflow

16 Configuring High Availability for Embedded NGX Gateways in SmartCenter

The Interface Properties dialog box appears displaying the General tab.

3. In the IP Address field, type the LAN network's internal IP address.
4. In the Net Mask field, type the LAN network's subnet mask.
5. Click the Topology tab.

   The Topology tab appears.

6. Click Network defined by the interface IP and Net Mask.
7. Click **OK**.
8. To close the gateway object, click **OK**.

### Configuring a Backup Gateway

**To configure a backup gateway**

1. In SmartDashboard, in the desired gateway object, click the **VPN** node.
   
   The **VPN** node appears.

2. Select the **Use Backup Gateway** check box.
3. In the **Use Backup Gateway** drop-down list, select the other gateway object.
4. Click **OK**.
Configuring VPN Communities for Permanent Tunnels

To configure VPN community for permanent tunnels

1. In SmartDashboard, in the desired VPN community, click the **Tunnel Management** node.

   The **Tunnel Management** node appears.

2. Select the **Set Permanent Tunnels** check box.

   Do not change the other settings.

3. Click **OK**.
Simple High Availability Configuration Scenarios

Scenario 1: Simple Gateway and WAN HA Configuration with Two Gateways

Figure 1: Simple Gateway and WAN HA Configuration
GOAL OF THIS CONFIGURATION

The goal of this configuration is to ensure the following:

- The internal networks always have an accessible default gateway for outbound Internet communications, in case the Active Gateway fails (for example, due to a hardware problem).
- Any failure on the Active Gateway is transparent to external users, and access to the internal networks is available at all times through a single IP address.
- Ensure only the Active Gateway is connected to the Internet and using the allocated WAN IP address.

IMPLEMENTING THIS SCENARIO

To implement this scenario

1. Configure Gateway HA.
   
   See *Gateway High Availability Workflow* on page 10

2. Configure WAN HA on the Passive Gateway.

   See *WAN High Availability Workflow* on page 11

CONFIGURATION NOTES

In this configuration, the Passive and Active Gateways can share the same Internet (WAN) IP address. The assumption in this configuration is that only a single WAN IP address can be allocated by the ISP for the cluster gateways to allow Internet connection.

WHAT WE WANT TO HAPPEN

- A failover will take place in the following cases:
SAMPLE CONFIGURATION PARAMETERS

Table 3: Simple Gateway and WAN HA Configuration Parameters

<table>
<thead>
<tr>
<th></th>
<th>Active Gateway</th>
<th>Passive Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAN Network IP Address</td>
<td>192.168.10.1 / 255.255.255.0</td>
<td>192.168.10.100 / 255.255.255.0</td>
</tr>
<tr>
<td>LAN Shared Virtual IP Address</td>
<td>192.168.10.254 / 255.255.255.0</td>
<td>192.168.10.254 / 255.255.255.0</td>
</tr>
<tr>
<td>DMZ Network IP Address</td>
<td>192.168.20.1 / 255.255.255.0</td>
<td>192.168.20.100 / 255.255.255.0</td>
</tr>
<tr>
<td>DMZ Shared Virtual IP Address</td>
<td>192.168.10.254 / 255.255.255.0</td>
<td>192.168.10.254 / 255.255.255.0</td>
</tr>
<tr>
<td>Actual WAN IP Address</td>
<td>62.90.31.1</td>
<td>62.90.31.1</td>
</tr>
<tr>
<td>WAN Shared Virtual IP Address</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>My Priority</td>
<td>30</td>
<td>20</td>
</tr>
<tr>
<td>Track Primary Internet</td>
<td>20</td>
<td>0</td>
</tr>
<tr>
<td>Track Secondary Internet</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Don't connect to the Internet if passive</td>
<td>Unchecked</td>
<td>Checked</td>
</tr>
<tr>
<td>Synchronization Interface</td>
<td>LAN Interface</td>
<td></td>
</tr>
</tbody>
</table>
Scenario 2: Gateway and WAN HA Configuration with Two Gateways Including Backup Internet Connection

Figure 2: Gateway and WAN HA Configuration with Backup ISP on Each Gateway
GOAL OF THIS CONFIGURATION
The goal of this configuration is to ensure the following:

- The internal networks always have an accessible default gateway for outbound Internet communications, in case the Active Gateway fails (for example, due to a hardware problem).
- The internal networks are connected to the Internet using the broadband lines as much as possible, and the cheap and slow dialup connection is used only if all broadband connections are down.
- Any failure on the Active Gateway is transparent to external users, and access to the internal networks is available at all times.

IMPLEMENTING THIS SCENARIO

To implement this scenario
1. Configure Gateway HA.
   See Gateway High Availability Workflow on page 10.
2. Configure WAN HA on the Passive Gateway.
   See WAN High Availability Workflow on page 11.
3. Configure a secondary Internet connection for the Active and Passive Gateways, using dialup, ISDN, or GPRS modems to serve as a backup.
   Refer to the UTM-1 Edge appliance's User Guide.

WHAT WE WANT TO HAPPEN

- A failover will take place immediately if the Active Gateway fails to generate heartbeats to the internal network. In this case, all connections will revert to the Passive Gateway, until the Active Gateway is available again.
- If the Active Gateway's primary Internet connection fails, a failover to the Passive Gateway will take place, and its broadband primary connection will be used.
- So long as the broadband primary Internet connection on the Active Gateway has not recovered, the following things will happen:
Scenario 2: Gateway and WAN HA Configuration with Two Gateways Including Backup Internet Connection

- If the Passive Gateway's broadband primary Internet connection also fails, then the Passive Gateway will use its backup dialup Internet connection.
- If the Passive Gateway's dialup backup Internet connection fails, a failover to the Active Gateway will take place, and its dialup backup Internet connection will be used.

**SAMPLE CONFIGURATION PARAMETERS**

**Table 4: Gateway and WAN HA with Backup ISP Configuration Parameters**

<table>
<thead>
<tr>
<th></th>
<th>Active Gateway</th>
<th>Passive Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAN Network IP Address</td>
<td>192.168.10.1 / 255.255.255.0</td>
<td>192.168.10.100 / 255.255.255.0</td>
</tr>
<tr>
<td>LAN Shared Virtual IP Address</td>
<td>192.168.10.254 / 255.255.255.0</td>
<td>192.168.10.254 / 255.255.255.0</td>
</tr>
<tr>
<td>DMZ Network IP Address</td>
<td>192.168.20.1 / 255.255.255.0</td>
<td>192.168.20.100 / 255.255.255.0</td>
</tr>
<tr>
<td>DMZ Shared Virtual IP Address</td>
<td>192.168.10.254 / 255.255.255.0</td>
<td>192.168.10.254 / 255.255.255.0</td>
</tr>
<tr>
<td>Actual WAN IP Address</td>
<td>62.90.31.1</td>
<td>62.90.31.1</td>
</tr>
<tr>
<td>Shared WAN Virtual IP Address</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>My Priority</td>
<td>100</td>
<td>45</td>
</tr>
<tr>
<td>Track Primary Internet</td>
<td>80</td>
<td>20</td>
</tr>
<tr>
<td>Track Secondary Internet</td>
<td>30</td>
<td>10</td>
</tr>
</tbody>
</table>
Scenario 3: Gateway and WAN HA Configuration using a Shared WAN Virtual IP Address

<table>
<thead>
<tr>
<th>Don't connect to the Internet if passive</th>
<th>Unchecked</th>
<th>Checked</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synchronization Interface</td>
<td>LAN Interface</td>
<td></td>
</tr>
</tbody>
</table>

**Scenario 3: Gateway and WAN HA Configuration using a Shared WAN Virtual IP Address**

*Figure 3: Gateway and WAN HA Configuration with Backup ISP on Each Gateway*

**Active UTM-1 Edge:**
- LAN IP: 192.168.10.1
- Subnet Mask: 255.255.255.0
- Virtual LAN IP: 192.168.10.254
- DMZ IP: 192.168.20.1
- Subnet Mask: 255.255.255.0
- Virtual DMZ IP: 192.168.20.254

**Passive UTM-1 Edge:**
- LAN IP: 192.168.10.100
- Subnet Mask: 255.255.255.0
- Virtual LAN IP: 192.168.10.254
- DMZ IP: 192.168.20.100
- Subnet Mask: 255.255.255.0
- Virtual DMZ IP: 192.168.20.254

**Virtual LAN IP:** 192.168.10.254
**Virtual DMZ IP:** 192.168.20.254

**LAN Segment Switch**
- LAN IP: 192.168.10.0
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.10.254

**DMZ Segment Switch**
- DMZ IP: 192.168.20.0
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.20.254

**Shared Virtual WAN IP:** 62.90.31.3
GOAL OF THIS CONFIGURATION

The goal of this configuration is to ensure the following:

- The internal networks always have an accessible default gateway for outbound Internet communications, in case the Active Gateway fails (for example, due to a hardware problem).

- Enable sharing the same IP address on the WAN interface of active and passive gateways with no IP conflicts.

- Enable inbound communications for VPN and internal Web server access from the Internet for external users and teleworkers through a single IP address.

- Any failure on the Active Gateway is transparent to external users, and access to the internal networks is available at all times.

- All cluster gateways must be connected to a SMART management server to get security and software updates.

IMPLEMENTING THIS SCENARIO

To implement this scenario

1. Configure Gateway HA.
   
   See Gateway High Availability Workflow on page 10.

2. Configure WAN HA with Virtual IP Address.

   See WAN High Availability with Virtual WAN IP Address Workflow on page 12.

WHAT WE WANT TO HAPPEN

- A failover will take place immediately if the Active Gateway fails to generate heartbeats to the internal network. In this case, all connections will revert to the Passive Gateway, until the Active Gateway is available again.

- Only the active gateway answers the virtual shared WAN IP address, enabling the passive gateway to remain connected to the Internet, for central management and updating.
### Scenario 3: Gateway and WAN HA Configuration using a Shared WAN Virtual IP Address

**SAMPLE CONFIGURATION PARAMETERS**

#### Table 5: Gateway and WAN HA with Backup ISP Configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Active Gateway</th>
<th>Passive Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LAN Network IP Address</strong></td>
<td>192.168.10.1 / 255.255.255.0</td>
<td>192.168.10.100 / 255.255.255.0</td>
</tr>
<tr>
<td><strong>LAN Shared Virtual IP Address</strong></td>
<td>192.168.10.254 / 255.255.255.0</td>
<td>192.168.10.254 / 255.255.255.0</td>
</tr>
<tr>
<td><strong>DMZ Network IP Address</strong></td>
<td>192.168.20.1 / 255.255.255.0</td>
<td>192.168.20.100 / 255.255.255.0</td>
</tr>
<tr>
<td><strong>DMZ Shared Virtual IP Address</strong></td>
<td>192.168.10.254 / 255.255.255.0</td>
<td>192.168.10.254 / 255.255.255.0</td>
</tr>
<tr>
<td><strong>Actual WAN IP Address</strong></td>
<td>62.90.31.1</td>
<td>62.90.31.1</td>
</tr>
<tr>
<td><strong>Shared WAN Virtual IP Address</strong></td>
<td>62.90.31.3</td>
<td>62.90.31.3</td>
</tr>
<tr>
<td><strong>My Priority</strong></td>
<td>30</td>
<td>20</td>
</tr>
<tr>
<td><strong>Track Primary Internet</strong></td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><strong>Track Secondary Internet</strong></td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><strong>Don't connect to the Internet if passive</strong></td>
<td>Unchecked</td>
<td>Unchecked</td>
</tr>
<tr>
<td><strong>Synchronization Interface</strong></td>
<td>LAN Interface</td>
<td></td>
</tr>
</tbody>
</table>