



This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

Integration Reference Manual

Configuring the BIG-IP LTM

12/14/2025

Configuring the BIG-IP LTM

The following table provides an overview of the main steps that are required in order to configure the BIG-IP LTM. Complete all steps in the order in which they are listed.

Integrating with BIG-IP LTM

1. Check Prerequisites.

Verify that BIG-IP LTM is working

The procedures in this topic assume that the BIG-IP LTM is properly licensed and fully functional, with login and password access configured. For more information, see BIG-IP LTM specific documentation.

2. Configure VLANs.

Configuring VLANs

Purpose

To configure two VLANs (Virtual Local Area Networks): one VLAN for the external interface (physical interface 1.3) and one VLAN for the internal (SIP Server side) interface (physical interface 1.1). VLANs are used to logically associate Self IP interfaces with physical interfaces on the BIG-IP LTM.

Prerequisites

- You are logged in to the BIG-IP LTM web interface.

Start

1. Go to **Network > VLANs > VLAN List**.
2. Click **Create**.
3. In the dialog box that appears, specify the following properties (see the following figure):
 - a. **Name**: Enter the VLAN name for the external interface--for example, `vlanSipExternal`.
 - b. **Tag**: 503 (it is set automatically).

- c. Resources > Interfaces > Untagged: Select 1.3 in the Available section and click the left-pointing arrow button to move it into the Untagged section.

Network >> VLANs >> vlanSipExternal

Properties Layer 2 Static Forwarding Table

General Properties

Name	vlanSipExternal
Tag	503

Resources

Interfaces

Untagged	Available	Tagged
1.3	1.1 1.2 1.4 2.1 2.2	

Configuration: Basic

Source Check ☐

MTU 1500

Update Cancel Delete

Configuring a VLAN for the External Interface

4. Click Finished.
5. Click Create.
6. In the dialog box that appears, specify the following properties (see the following figure):
 - a. Name: Enter the VLAN name for the internal interface--for example, vlanSipInternal.
 - b. Tag: 103 (it is set automatically).
 - c. Resources > Interfaces > Untagged: Select 1.1 in the Available section and click the left-pointing arrow button to move it into the Untagged section.

The screenshot shows the configuration page for a VLAN named 'vlanSipInternal'. The breadcrumb trail is 'Network >> VLANs >> vlanSipInternal'. There are two tabs: 'Properties' (selected) and 'Layer 2 Static Forwarding Table'. The 'General Properties' section shows 'Name' as 'vlanSipInternal' and 'Tag' as '103'. The 'Resources' section shows a list of interfaces on the left and three columns for 'Untagged', 'Available', and 'Tagged' resources. The 'Untagged' column contains '1.1'. The 'Available' column contains a list of IP addresses: 1.2, 1.3, 1.4, 2.1, and 2.2. The 'Tagged' column is empty. Below the resources, the 'Configuration' section is set to 'Basic'. It includes a 'Source Check' checkbox (unchecked) and an 'MTU' field set to '1500'. At the bottom are 'Update', 'Cancel', and 'Delete' buttons.

Configuring a VLAN for the Internal Interface

7. Click Finished.

End

Next Steps

- [Configuring Self IP addresses](#)

3. Configure Self IP addresses.

Configuring Self IP addresses

Purpose

To configure two Self IP addresses--one for the external interface and one for the internal interface--and associate them with the VLANs, to access hosts in those VLANs.

Prerequisites

- [Procedure: Configuring VLANs](#)

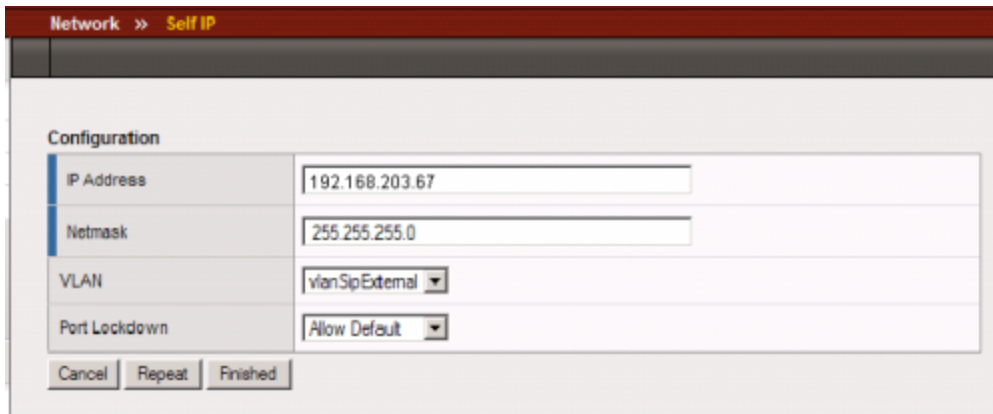
Start

1. Go to Network > Self IPs.
2. Click Create.
3. In the dialog box that appears, specify the following properties (see the following figure):
 - a. IP Address: Enter the IP address for the internal interface--for example, 192.168.63.1.
 - b. Netmask: Enter the netmask--for example, 255.255.255.240.
 - c. VLAN: Select the name of the VLAN to which you want to assign the self IP address--for example, vlanSipInternal.

The screenshot shows a web-based configuration interface for a Self IP. The title bar at the top reads 'Network >> Self IP'. Below this is a 'Configuration' section with four rows of input fields. The first row is 'IP Address' with the value '192.168.63.1'. The second row is 'Netmask' with the value '255.255.255.240'. The third row is 'VLAN' with a dropdown menu showing 'vlanSipInternal'. The fourth row is 'Port Lockdown' with a dropdown menu showing 'Allow Default'. At the bottom of the configuration area are three buttons: 'Cancel', 'Repeat', and 'Finished'.

Configuring a Self IP Address for the Internal Interface

4. Click Finished.
5. Click Create.
6. In the dialog box that appears, specify the following properties (see the following figure):
 - a. IP Address: Enter the IP address for the external interface--for example, 192.168.203.67.
 - b. Netmask: Enter the netmask--for example, 255.255.255.0.
 - c. VLAN: Select the name of the VLAN to which you want to assign the self IP address--for example, vlanSipExternal.
 - d. Click Finished (see the following figure).



Configuration	
IP Address	192.168.203.67
Netmask	255.255.255.0
VLAN	vlanSipExternal
Port Lockdown	Allow Default

Cancel Repeat Finished

Configuring a Self IP Address for the External Interface

End

Next Steps

- [Configuring the Default IP route](#)

4. Configure the Default IP route.

Configuring the Default IP route

Purpose

To configure the default IP route.

Prerequisites

- [Configuring Self IP addresses](#)

Start

1. Go to Network > Routes.
2. Click Add.
3. In the dialog box that appears, specify the following properties (see the following figure):
 - a. Type: Select Default Gateway.
 - b. Resource > Use Gateway: Enter the IP address for this default IP route--for example, 192.168.203.1.

- c. Click Finished.



Configuring Default IP Route

End

Next Steps

- [Configuring SIP Server nodes](#)

5. Configure SIP Server nodes.

Configuring SIP Server nodes

Purpose

To configure two SIP Server nodes, primary and backup.

Prerequisites

- [Configuring the Default IP route](#)

Start

1. Go to Local Traffic > Nodes.
2. Click Create.
3. In the dialog box that appears, specify the following properties (see the following figure):
 - a. Address: Enter the IP address for the primary SIP Server node--for example, 192.168.63.201.
 - b. Name: Enter the node name--for example, nodeHa01Primary.

- c. Health Monitors: Select Node Specific.
- d. Select Monitors > Active: Select icmp.

The screenshot shows the 'New Node...' configuration window in the BIG-IP LTM interface. The breadcrumb trail at the top reads 'Local Traffic >> Nodes >> New Node...'. The window is divided into two main sections: 'General Properties' and 'Configuration'.

General Properties:

- Address:** 192.168.63.201
- Name:** nodeHa01Primary

Configuration:

- Health Monitors:** Node Specific (dropdown)
- Select Monitors:** A list of monitors is shown. In the 'Active' column, 'icmp' is selected. In the 'Available' column, the following monitors are listed: gateway_icmp, https_443, real_server, snmp_dca, and tcp_echo. Navigation buttons '<<' and '>>' are between the columns.
- Availability Requirement:** All (dropdown) Health Monitor(s)
- Ratio:** 1
- Connection Limit:** 0

At the bottom of the configuration section are three buttons: 'Cancel', 'Repeat', and 'Finished'.

Configuring a Primary SIP Server Node

- 4. Click Finished.
- 5. Click Create.
- 6. In the dialog box that appears, specify the following properties (see the following figure):
 - a. Address: Enter the IP address for the backup SIP Server node--for example, 192.168.63.203.
 - b. Name: Enter the node name--for example, nodeHa01Backup.
 - c. Health Monitors: Select Node Specific.
 - d. Select Monitors > Active: Select icmp.

The screenshot shows the 'New Node...' configuration window in the BIG-IP LTM GUI. The 'General Properties' section has 'Address' set to '192.168.83.203' and 'Name' set to 'nodeHa01Backup'. The 'Configuration' section has 'Health Monitors' set to 'Node Specific'. Under 'Select Monitors', the 'Active' list contains 'icmp' and the 'Available' list contains 'gateway_icmp', 'https_443', 'real_server', 'snmp_dc', and 'top_echo'. The 'Availability Requirement' is set to 'All', 'Ratio' is '1', and 'Connection Limit' is '0'. At the bottom are 'Cancel', 'Repeat', and 'Finished' buttons.

Configuring a Backup SIP Server Node

7. Click Finished.

End

6. Configure a health monitor.

Configuring a health monitor

Overview

In general, the BIG-IP LTM uses health monitors to determine whether a server to which messages can be routed is operational (active). Servers that are flagged as not operational (inactive) will cause the BIG-IP LTM to route messages to another server if one is present in the same server pool. However, primary and backup SIP Servers must be configured as the only members of the same server pool—one member active (primary) and one member inactive (backup).

In this procedure, the BIG-IP LTM is configured to use the health monitor of SIP type in UDP mode. This means that the OPTIONS request method will be sent to both primary and backup SIP Servers.

Any response to OPTIONS is configured as Accepted Status Code.

SIP Server always starts in backup mode, establishes a permanent connection with the Genesys Management Layer, and changes its role to primary only if a trigger from the Management Layer is received. Such trigger is only generated if no other primary SIP Server is currently running. After switching to primary mode, SIP Server responds to UDP packets received on the SIP port specified by the sip-port configuration option. Therefore, after receiving the OPTIONS request from the BIG-IP LTM, SIP Server responds to the health check, and the BIG-IP LTM marks SIP Server as active.

When running in backup mode, SIP Server ignores UDP messages. Since the BIG-IP LTM does not receive any response to the OPTIONS request, it marks the backup SIP Server as inactive. If SIP Server does not respond because of network latency or other reasons, the BIG-IP LTM will mark SIP Server as inactive, and continue sending ping messages periodically.

The Interval setting defines how often pool members (primary and backup) are checked for presence. The Timeout setting defines the waiting time before an unresponsive member of the pool is marked as inactive. Regardless of the member's status (or SIP Server status), the BIG-IP LTM will always check servers for presence. When an inactive member responds to the health check, it is marked as active. In this configuration, the Interval parameter is set to one second and Timeout to four seconds in order to minimize a possible delay that might result from a switchover.

Start

1. Go to Local Traffic > Monitors.
2. Click Create.
3. In the dialog box that appears, specify the following properties (see the following figure):
 - a. Name: Enter the name for this health monitor--for example, monSipUdp.
 - b. Type: Select SIP.
 - c. Configuration: Select Basic.
 - d. Interval: Enter 1.
 - e. Timeout: Enter 4.
 - f. Mode: Select UDP.
 - g. Additional Accepted Status Codes: Select Any.

Local Traffic >> Monitors >> New Monitor...

General Properties

Name	monSipUdp
Type	SIP
Import Settings	sip

Configuration: Basic

Interval	1 seconds
Timeout	4 seconds
Mode	UDP
Additional Accepted Status Codes	Any

Cancel Repeat Finished

Configuring a Health Monitor

4. Click Finished.

End

Next Steps

- [Configuring a server pool](#)

7. Configure a server pool.

Configuring a server pool

Purpose

To configure a server pool with which the BIG-IP LTM will communicate.

Start

1. Go to Local Traffic > Pools.

2. Click Create.
3. In the dialog box that appears, specify the following properties (see the following figure):
 - a. Name: Enter the name for this server pool--for example, the poolHa01.
 - b. Health Monitors > Active: Select monSipUdp.
 - c. Action On Service Down: Select Reselect.
 - d. Load Balancing Method: Select Round Robin.
 - e. Priority Group Activation: Select Disabled.

Local Traffic >> Pools >> New Pool...

Configuration: **Advanced**

Name	poolHa01	
Health Monitors	<div>Active</div> <div>monSipUdp</div>	<div>Available</div> <div>gateway_icmp http https https_443 tcp</div>
Availability Requirement	All	Health Monitor(s)
Allow SNAT	Yes	
Allow NAT	Yes	
Action On Service Down	Reselect	
Slow Ramp Time	0 seconds	
IP ToS to Client	Pass Through	
IP ToS to Server	Pass Through	
Link QoS to Client	Pass Through	
Link QoS to Server	Pass Through	

Resources

Load Balancing Method	Round Robin	
Priority Group Activation	Disabled	
New Members	<input checked="" type="radio"/> New Address <input type="radio"/> Node List	
	Address: <input type="text"/>	
	Service Port: <input type="text"/> <input type="button" value="Select..."/>	
	<input type="button" value="Add"/>	
<input type="text"/>		<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Configuring a Server Pool

4. Click Finished.

End

8. Add server pool members.

Adding server pool members

Purpose

To add primary and backup SIP Servers to the server pool. Note that they must be the only members of this server pool.

Start

1. Go to Local Traffic > Pools > poolHa01 > Members.
2. Click Add.
3. In the dialog box that appears, specify the following properties (see the following figure):
 - a. Address > Node List: Select the primary server node you created in [Configuring SIP Server nodes](#). In our example, it would be 192.168.63.201 (nodeHa01Primary).
 - b. Service Port: Enter 5060.

The screenshot shows the 'New Pool Members...' dialog box. The 'Address' field has a dropdown menu with the selected option '192.168.63.201 (nodeHa01Primary)'. The 'Service Port' field is set to '5060'. The 'Configuration' section is set to 'Basic' and includes fields for 'Ratio' (1), 'Priority Group' (1), and 'Connection Limit' (0). At the bottom are 'Cancel', 'Repeat', and 'Finished' buttons.

Adding the Primary SIP Server to the Server Pool

4. Click Finished.
5. Click Add.
6. In the dialog box that appears, specify the following properties (see the following figure):
 - a. Address > Node List: Select the backup server node you created in the [Configuring SIP Server nodes](#). In our example, it would be 192.168.63.203 (nodeHa01Backup).
 - b. Service Port: Enter 5060.

Local Traffic >> Pools >> poolHa01

New Pool Members...

Address: ☐ New Address ☒ Node List
192.168.63.203 (nodeHa01Backup)

Service Port: 5060

Configuration: Basic

Ratio: 1

Priority Group: 1

Connection Limit: 0

Adding the Backup SIP Server to the Server Pool

7. Click Finished.
8. Go to Local Traffic > Pools. The status of the poolHa01 server pool displays as available (green) (see the following figure).

Local Traffic >> Pools

Pool List Statistics

Search Create...

<input checked="" type="checkbox"/>	Status	Name	Partition	Members
<input type="checkbox"/>		poolHa01	Common	2

Delete...

The Server Pool of Two Members

End

9. Configure data groups.

Configuring data groups

Purpose

To configure data groups that will be used by the iRule. One data group (dataGroupHa) contains physical IP addresses of primary and backup SIP Server nodes. The second data group (dataGroupSnatExcluded) contains IP addresses of the groups that will be excluded from applying SNAT, such as the Genesys Configuration Server group and Genesys T-Library Clients group (see the [Device Communication Groups](#) figure).

Start

1. Go to Local Traffic > iRules > Data Group List.
2. Click Create.
3. In the dialog box that appears, specify the following properties (see the following figure):
 - a. Name: Enter the name for this data group--for example, dataGroupSnatHa.
 - b. Type: Select Address.
 - c. Address Records > Type Host > Address: Enter the host IP address of the primary server node--for example, 192.168.63.201.
 - d. Click Add.
 - e. Address Records > Type Host > Address: Enter the host IP address of the backup server node--for example, 192.168.63.203.
 - f. Click Add.

Local Traffic >> Data Groups >> New Data Group...

General Properties

Name: dataGroup SnatHa

Type: Address

Records

Type: ☒ Host ☐ Network

Address: 192.168.63.203

Add

Address Records

192.168.63.201

192.168.63.203

Edit Delete

Cancel Repeat Finished

Configuring a Data Group for SNAT

4. Click Finished.
5. Click Create.
6. In the dialog box that appears, specify the following properties (see the following figure):
 - a. Name: Enter the name for this data group--for example, dataGroupSnatExcluded.
 - b. Type: Select Address.
 - c. Address Records > Type Host > Address: Enter the host IP address of Genesys Configuration Server--for example, 172.21.226.73.
 - d. Click Add.
 - e. Address Records > Type Network > Address: Enter the IP address and net mask--for example, 192.168.89.0/255.255.255.0.
 - f. Click Add.

Local Traffic >> Data Groups >> New Data Group...

General Properties

Name: dataGroupSnatHa

Type: Address

Records

Type: ☒ Host ☐ Network

Address: 192.168.63.203

Add

192.168.63.201

192.168.63.203

Edit Delete

Cancel Repeat Finished

Configuring a Data Group for SNAT Exclusions

7. Click Finished.

End

10. Configure a SNAT pool.

Configuring a SNAT pool

Purpose

To configure a SNAT pool that specifies the Virtual IP address to be used as a source IP address for any packet that originates from the primary or backup SIP Server to which SNAT is applied (with the exception of the devices specified in the dataGroupSnatExcluded data group). SNAT is the mapping of one or more original IP addresses to a translation address.

Start

1. Go to Local Traffic > SNAT Pools.
-

2. Click Create.
3. In the dialog box that appears, specify the following properties (see the following figure):
 - a. Name: Enter the name for this SNAT pool--for example, snatPoolVip.
 - b. Configuration > Members List > IP Address: Enter the IP address to be used as a source IP address--for example, 192.168.203.164.

The screenshot shows the 'New SNAT Pool' configuration window. The breadcrumb trail at the top is 'Local Traffic >> SNAT Pools >> New SNAT Pool...'. The 'General Properties' section has a 'Name' field with the value 'snatPoolVip'. The 'Configuration' section has an 'IP Address' field with the value '192.168.203.164'. Below this is an 'Add' button, and the 'Member List' contains the IP address '192.168.203.164'. There are also 'Edit' and 'Delete' buttons for the member list. At the bottom of the dialog are 'Cancel', 'Repeat', and 'Finished' buttons.

Configuring a SNAT Pool

4. Click Finished.

End

11. Configure an iRule.

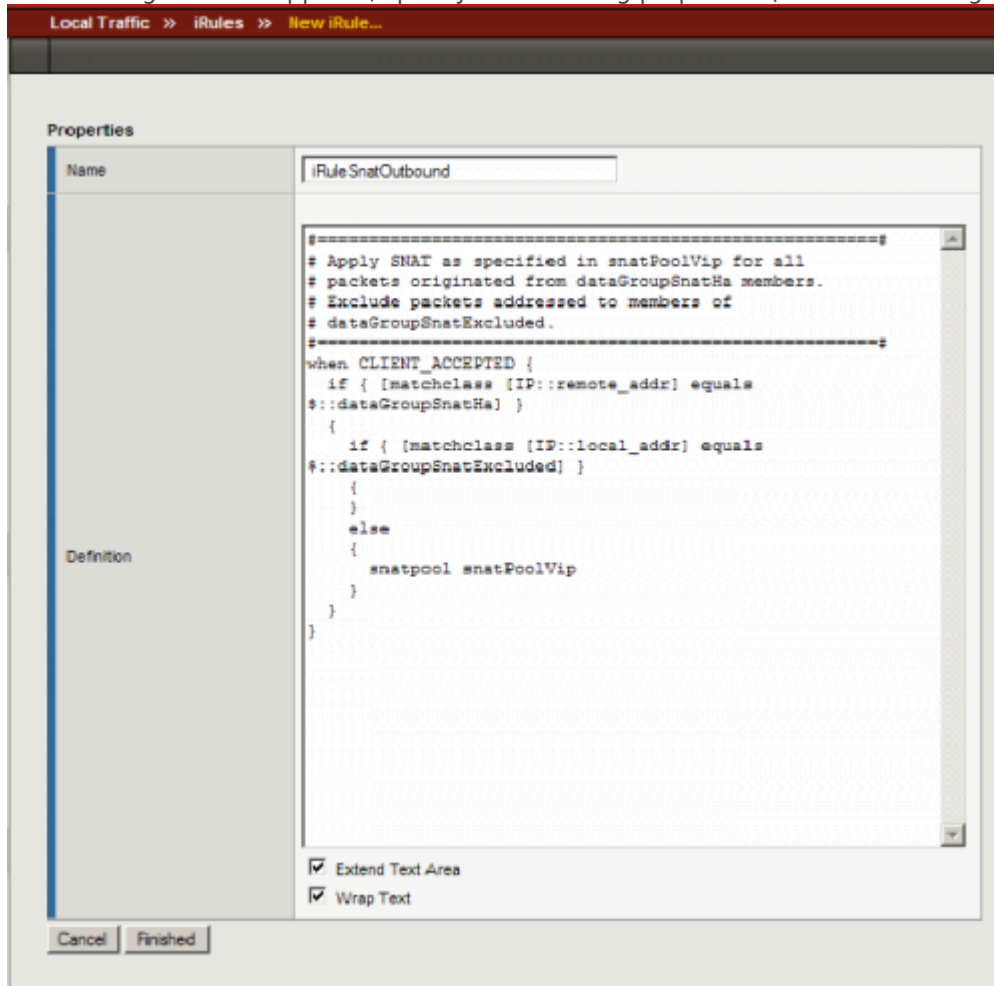
Configuring an iRule

Purpose

To configure an iRule that is used to perform SNAT to the Virtual IP address to any packets that originate from the primary or backup SIP Server (with the exception of the packets addressed to Configuration Server and the Genesys T-Library Clients group). This iRule will then be associated with a Virtual Server for the outbound traffic, vsWildCardOutbound. In this deployment architecture, the HA synchronization traffic between primary and backup SIP Servers does not pass through the BIG-IP LTM, that is why it is excluded from applying SNAT.

Start

1. Go to Local Traffic > iRules.
2. Click Create.
3. In the dialog box that appears, specify the following properties (see the following figure):



Configuring an iRule

- a. Name: Enter the name for this iRule--for example, iRuleSnatOutbound.
- b. Definition: Enter the following text:

```
#=====#
# Apply SNAT as specified in snatPoolVip for all
# packets originated from dataGroupSnatHa members.
# Exclude packets addressed to members of
# dataGroupSnatExcluded.
#=====#
when CLIENT_ACCEPTED {
    if { [matchclass [IP::remote_addr] equals $::dataGroupSnatHa] }
    {

```

```
        if { [matchclass [IP::local_addr] equals $::dataGroupSnatExcluded] }
        {
        }
        else
        {
            snatpool snatPoolVip
        }
    }
}
```

4. Click Finished.

End

12. Configure a Virtual Server.

Configuring a Virtual Server

Complete the following steps:

[+] Configuring a Virtual Server for outbound traffic

Purpose

To configure a Virtual Server to be used for outbound traffic. It is associated with a VLAN that is configured for the internal interface (see [Configuring VLANs](#)) and it has iRule assigned to Resources, which applies SNAT to all packets (except for packets addressed to Configuration Server).

Prerequisites

- [Configuring an iRule](#)

Start

1. Go to Local Traffic > Virtual Servers.
2. Click Create.
3. In the dialog box that appears, specify the following properties (see the following figure):
 - a. Name: Enter the name for this Virtual Server--for example, vsWildcardOutbound.
 - b. Destination > Type: Select Network.
 - c. Destination > Address: Enter 0.0.0.0.
 - d. Destination > Mask: Enter 0.0.0.0.
 - e. Service Port: Enter * (asterisk).
 - f. Configuration: Select Basic.

- g. Type: Select Forwarding (IP).
- h. Protocol: Select All Protocols.
- i. VLAN Traffic: Select Enabled on...
- j. VLAN List Selected: Select vlanSipInternal.
- k. Resources > iRules > Enabled: Select iRuleSnatOutbound.

Local Traffic >> Virtual Servers >> New Virtual Server...

General Properties

Name	vsWildCardOutbound
Destination	Type: <input type="radio"/> Host <input checked="" type="radio"/> Network Address: 0.0.0.0 Mask: 0.0.0.0
Service Port	* All Ports
State	Enabled

Configuration: Basic

Type	Forwarding (IP)
Protocol	All Protocols
VLAN Traffic	Enabled on...
VLAN List	<div>Selected: vlanSipInternal</div> <div>Available: vlanSipExternal</div>

Resources

Rules	<div>Enabled: iRuleSnatOutbound</div> <div>Available: _sys_auth_sel_cc_idap, _sys_auth_krbdelegate</div>
-------	--

Up Down

Cancel Repeat Finished

Configuring a Wildcard Virtual Server for Outbound Traffic

- 4. Click Finished.

End

[+] Configuring a Virtual Server for inbound traffic

Purpose

To configure a Virtual Server for inbound traffic. In Layer 3/ Routing configuration mode, the BIG-IP LTM passes through only those packets that have a destination matching a virtual server. Having the

Virtual Server for inbound traffic allows packets with a destination that matches the physical IP address of the primary or backup SIP Server to pass through.

Start

1. Go to Local Traffic > Virtual Servers.
2. Click Create.
3. In the dialog box that appears, specify the following properties (see the following figure):
 - a. Name: Enter the name for this Virtual Server--for example, vsWildcardInbound.
 - b. Destination > Type: Select Network.
 - c. Destination > Address: Enter 0.0.0.0.
 - d. Destination > Mask: Enter 0.0.0.0.
 - e. Service Port: Enter * (asterisk).
 - f. Configuration: Select Basic.
 - g. Type: Select Forwarding (IP).
 - h. Protocol: Select All Protocols.
 - i. VLAN Traffic: Select Enabled on....
 - j. VLAN List Selected: Select vlanSipExternal.

Configuring a Wildcard Virtual Server for Inbound Traffic

4. Click Finished.

End

[+] Configuring Virtual Servers for UDP and TCP SIP communications

Purpose

To configure two virtual servers to handle traffic directed to a Virtual IP address: one virtual server for SIP communications using the UDP as a transport protocol and one virtual server for SIP communications using the TCP as a transport protocol. The Virtual IP address is used by SIP clients to contact SIP Server. In other words, the Virtual IP address hides two physical IP addresses (used by the primary and backup servers) and presents the SIP Server HA pair as a single entity for all SIP-based communications.

Start

1. Go to Local Traffic > Virtual Servers.
2. Click Create.
3. In the dialog box that appears, specify the following properties (see the following figure):
 - a. Name: Enter the name for this Virtual Server--for example, vsVip.
 - b. Destination > Type: Select Host.
 - c. Destination > Address: Enter the IP address for this Virtual Server--for example, 192.168.203.164.
 - d. Service Port: Enter 5060 and select Other.
 - e. State: Select Enabled.
 - f. Configuration: Select Basic.
 - g. Type: Select Standard.
 - h. Protocol: Select UDP.
 - i. SMTP Profile: Select None.
 - j. SIP Profile: Select sip.
 - k. VLAN Traffic: Select Enabled on....
 - l. VLAN List Selected: Select vlanSipExternal.
 - m. Resources > Default Pool > Select poolHa01.

Local Traffic » Virtual Servers » New Virtual Server...

General Properties

Name	vsVip	
Destination	Type:	<input checked="" type="radio"/> Host <input type="radio"/> Network
	Address:	192.168.203.164
Service Port	5060	Other: <input type="text"/>
State	Enabled	

Configuration: Basic

Type	Standard	
Protocol	UDP	
SMTP Profile	None	
SIP Profile	sip	
VLAN Traffic	Enabled on...	
VLAN List	<div>Selected</div> <div>vlanSipExternal</div>	<div>Available</div> <div>vlanSipInternal</div>

Resources

iRules	Enabled	Available
		_sys_auth_ssl_cc_ldap _sys_auth_krbdelegate iRuleSnatOutbound
Up Down		
Default Pool	poolHa01	
Default Persistence Profile	None	
Fallback Persistence Profile	None	

Cancel Repeat Finished

Configuring a Virtual Server for UDP-Based Communications

4. Click Finished.
5. Click Create.

6. In the dialog box that appears, specify the following properties (see the following figure):
 - a. Name: Enter the name for this Virtual Server--for example, vip_tcp.
 - b. Destination > Type: Select Host.
 - c. Destination > Address: Enter the IP address for this Virtual Server--for example, 192.168.203.164.
 - d. Service Port: Enter 5060 and select Other.
 - e. State: Select Enabled.
 - f. Configuration: Select Basic.
 - g. Type: Select Standard.
 - h. Protocol: Select TCP.
 - i. SMTP Profile: Select None.
 - j. SIP Profile: Select sip.
 - k. VLAN Traffic: Select Enabled on....
 - l. VLAN List Selected: Select vlanSipExternal.
 - m. Resources > Default Pool > Select poolHa01.

General Properties	
Name	vip_tcp
Destination	Type: <input checked="" type="radio"/> Host <input type="radio"/> Network Address: 192.168.203.164
Service Port	5060 Other: <input type="text"/>
State	Enabled <input type="button" value="v"/>

Configuration: <input type="button" value="Basic"/>	
Type	Standard <input type="button" value="v"/>
Protocol	TCP <input type="button" value="v"/>
OneConnect Profile	None <input type="button" value="v"/>
HTTP Profile	None <input type="button" value="v"/>
FTP Profile	None <input type="button" value="v"/>
SSL Profile (Client)	None <input type="button" value="v"/>
SSL Profile (Server)	None <input type="button" value="v"/>
SMTP Profile	None <input type="button" value="v"/>
SIP Profile	sip <input type="button" value="v"/>
VLAN Traffic	Enabled on... <input type="button" value="v"/>
VLAN List	<div> <div>Selected</div> <div>var SoExternal</div> <div>Available</div> <div>vlanSp Internal</div> </div> <div> <input type="button" value="v"/> <input type="button" value="v"/> </div>

Resources	
IRules	<div> <div>Enabled</div> <div>Available</div> </div> <div> <input type="button" value="v"/> <div> _sys_auth_ssl_cc_idap _sys_auth_krbdelegate iRuleSmtOutbound </div> </div> <div> <input type="button" value="v"/> <input type="button" value="v"/> </div>
HTTP Class Profiles	<div> <div>Enabled</div> <div>Available</div> </div> <div> <input type="button" value="v"/> <div>httpclass</div> </div> <div> <input type="button" value="v"/> <input type="button" value="v"/> </div>
Default Pool	poolHs01 <input type="button" value="v"/>
Default Persistence Profile	None <input type="button" value="v"/>
Failback Persistence Profile	None <input type="button" value="v"/>

Creating a Virtual Server for TCP-Based Communications

7. Click **Finished**.

End

<verttabber>