Deployment Guide

Document version 1.0

What's inside:

Deploying the BIG-IP Data Center Firewall

Welcome to the F5 BIG-IP data center firewall Deployment Guide. This document contains guidance on configuring the BIG-IP Local Traffic Manager (LTM) for deployment as a data center firewall, resulting in a fast, secure and highly available deployment.

For years, the F5 BIG-IP product family has been relied upon to handle high demand application traffic and traffic management. This includes being the traffic manager in front of the firewalls. Now, the data center firewall implementation described in this document will demonstrate how to reduce reliance on a secondary firewall layer, or remove it all together, while still providing protection to the data center.

Why F5

BIG-IP platform provides a unified view of layer 3 through 7 for both general and ICSA required reporting and alerts, as well as integration with SIEM vendors. BIG-IP LTM offers native, high-performance firewall services to protect the entire infrastructure.

BIG-IP LTM is a purpose-built, high-performance Application Delivery Controller (ADC) designed to protect data centers. In many instances, BIG-IP LTM can consolidate existing firewall services while also offering scale, performance, and persistence.

For more information on the F5 BIG-IP system, see *http://www.f5.com/products/big-ip*
For more information on Data Center Firewall solutions, see
http://www.f5.com/solutions/security/data-center-firewall.html

To provide feedback on this deployment guide or other F5 solution documents, contact us at *solutionsfeedback@f5.com*.

Products and versions tested

Product	Version
BIG-IP LTM	11.1 HF-2

Important: *Make sure you are using the most recent version of this deployment guide, found at http://www.f5.com/pdf/deployment-guides/data-center-firewall-dg.pdf.*

What is F5 iApp™?

F5 iApp is a powerful new set of features in the BIG-IP system that provides a new way to architect application delivery in the data center. It includes a holistic, application-centric view of how applications are managed and delivered inside, outside, and beyond the data center.

The Data Center Firewall iApp is meant to help facilitate the deployment and configuration of virtual servers combined with the Data Center Firewall iRule. By combining these two features, the LTM is able to become a Data Center Firewall using Datagroups and the iRule to control incoming traffic.

For more information on iApp, see the White Paper *F5 iApp: Moving Application Delivery Beyond the Network:* http://www.f5.com/pdf/white-papers/f5-iapp-wp.pdf.

Prerequisites and configuration notes

The following are general prerequisites and configuration notes for this guide:

- The BIG-IP system must be running version 11.1 or later.
- You must have the LTM module licensed and provisioned on the BIG-IP system.
- There must be network connectivity between applicable devices.
- If you are configuring this Data Center Firewall iApp to protect an existing application services configured by other iApps, you must disable **Strict Updates** on those iApp Application Services. If you do not, this Data Center Firewall iApp displays and error and does not complete. The Strict Updates feature is meant to prevent users from manually modifying the iApp configuration.

  By disabling Strict Updates, if you use the *Reconfigure* option on iApp application service and modify the configuration within the iApp template, you must make all changes again manually. See *Disabling Strict Updates on page 10* for specific information.
- The iApp template has two functions, creating Source Groups and building the Firewall rules. Before you use the firewall rule builder in the iApp, you must have appropriate BIG-IP Data Groups configured. You can run the iApp and use the Source Group builder option to create the source Data Groups, or you can create Data Groups manually. But you must have source Data Groups configured before running the Firewall Rule builder.
- While this document contains (optional) guidance for using third party security information and event management (SIEM) applications, it does not cover the installation and initial configuration of these systems. Third party systems must be configured and licensed properly. Consult the vendor documentation for specific details.

Configuration overview

The BIG-IP data center firewall deployment can be used in multiple ways. The following diagram illustrates the example used in this deployment guide.

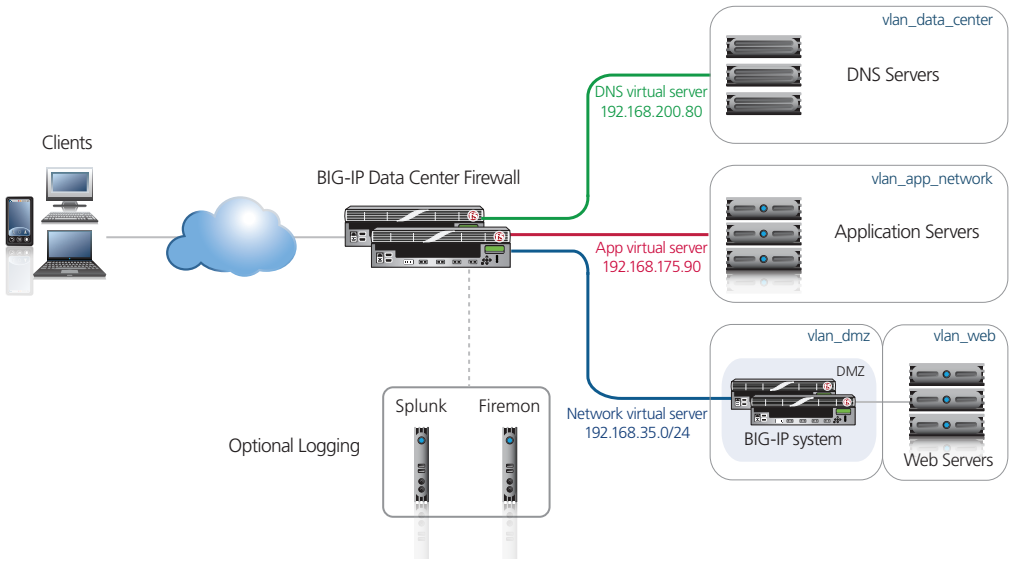


Figure 1: *Configuration example*

In our example, the BIG-IP data center firewall is configured with the following security policies in place:

```
ALLOW SRC 192.168.100.0/24 PORT ANY DST 192.168.200.80 PORT 53
ALLOW SRC 192.168.100.0/24 PORT ANY DST 192.168.175.90 PORT 443
ALLOW SRC 192.168.50.0/24 PORT ANY DST 192.168.35.0/24 PORT 80 443
DENY ALL
```

The example policies above cover the 5-tuples required for essential security.

- Source IP
- Source port
- Destination IP
- Destination port
- Destination protocol

The BIG-IP platform inherently locks down traffic based on the destination IP, port, and protocol. This is because the only traffic that is allowed to pass through the BIG-IP system is traffic destined for a specific IP on a specific port, over a specific protocol.

In this document, we split the 5-tuple into two logical sections, the source and destination.

Another very important aspect of the BIG-IP data center firewall deployment, and firewall systems in general, is logging. The BIG-IP system can be configured to log these messages to third party systems such as Splunk and FireMon. For more information on integrating with these systems see t*Appendix B: Using third-party SIEM and Management applications on page 18*.

Using the BIG-IP system and the iRule ACL

As mentioned, the BIG-IP system inherently locks down the destination portion of the 5-tuples. As such, the iRule provides the source aspects by creating the allow sources, the following rule references Figure 1 as an example.

```
ALLOW SRC srcgrp-1 DST HOST192.168.200.80 PORT 53 PROTOCOL TCP
```

The source group of **srcgrp-1** consists of the following address, **192.168.100.0/24**. This is specified using the data group function within the LTM. Only traffic from 1**92.168.100.0/24** will have access to **192.168.200.80** on port **53** using TCP, all other traffic will be denied.

Destinations are defined using virtual servers. For our example above we create a virtual server with the IP of 192.168.200.80 serving port 53 with a TCP profile. This ensures that only traffic destined for this address on port 53 is allowed.

Going Beyond the 5-tuples

With the example we have above, the destination portion of the 5-tuple is handled by a virtual server. However, virtual servers are not limited to just being a destination. With a virtual server, profiles and additional protocol awareness is provided.

For example, our second sample rule set is:

```
ALLOW SRC 192.168.100.0/24 PORT ANY DST 192.168.175.90 PORT 443
```

The source will be a data group; the destination will be created as a virtual server serving HTTPS with a pool of HTTPS servers behind it.

With this in mind, we can add an HTTP profile to the traffic along with SSL offload. The traffic can then be inspected using the Protocol Security Module or for further depth the Application Security Module. For more information on these Modules please see *http://www.f5.com/products/big-ip/*.

Using Packet Filters

Another tool made available to use for configuring our sources and destinations are Packet Filters. These are configured on the BIG-IP system at a global level. This means that packet filters will impact all traffic traversing the BIG-IP system. This is useful in the case of setting global security for non TCP and UDP traffic such as ICMP.

For more information on using Packet Filters please see the BIG-IP data center firewall Configuration Guide.

Using the Data Center Firewall iApp template

This section describes how to install and use the Data Center Firewall iApp template. Before you can use the Data Center Firewall iApp template to configure the BIG-IP system, you must download and install the template file.

Downloading and importing the Data Center Firewall iApp from DevCentral

The first task is to download the Data Center Firewall iApp from DevCentral and import it onto the BIG-IP system. Ensure you download the file with the latest date in the file name.

To download and import the iApp from DevCentral

1. Open a web browser and go to *https://devcentral.f5.com/wiki/iApp.Data-Center-Firewall-iApp-template.ashx*
2. Download **f5.data_center_firewall.zip** to a location accessible from your BIG-IP system.
   You must download the file, and not copy and paste the contents. F5 has discovered the copy paste operation does not work reliably.

Important →

3. Extract (unzip) the **f5_data_center_firewall.tmpl** file.
4. Log on to the BIG-IP system web-based Configuration utility.
5. On the Main tab, expand **iApp**, and then click **Templates**.
6. Click the **Import** button on the right side of the screen.
7. Click a check in the **Overwrite Existing Templates** box.
8. Click the **Browse** button, and then browse to the location you saved the iApp file.
9. Click the **Upload** button. The iApp is now available for use.

Getting Started with the iApp for the data center firewall

To begin the template, use the following procedure.

1. Log on to the BIG-IP system.
2. On the Main tab, expand **iApp**, and then click **Application Services**.
3. Click **Create**. The Template Selection page opens.
4. In the **Name** box, type a name. In our example, we use **data-center-fw_**.
5. From the **Template** list, select **f5.data_center_firewall**.

Advanced options

If you select **Advanced** from the **Template Selection** list, you see Sync and Failover options for the application. This feature, new to v11, is a part of the Device Management configuration. This functionality extends the existing High Availability infrastructure and allows for clustering, granular control of configuration synchronization and granular control of failover.

1. **Configure Sync/Failover?**
   If you want to configure the Application for Sync or failover groups, select **Yes** from the list.
   a. **Device Group**
      If you select Yes from the question above, the Device Group and Traffic Group options appear. If necessary, uncheck the Device Group box and then select the appropriate Device Group from the list.
   b. **Traffic Group**
      If necessary, uncheck the Traffic Group box and then select the appropriate Traffic Group.

Choosing a template type

As mentioned in the prerequisites, this iApp template has two functions, creating a source data group and building the Firewall rules. If you do not have a source data group currently configured on the BIG-IP system, you ***must*** either use the iApp to create the source data group (recommended), or create source data groups manually (see *Configuring the Data Groups on page 11* for manual configuration procedures).

- If you have not yet created a source data group on the BIG-IP system, select **Source Data Group Builder** from the list, and continue with the following section.
- If you have already configured your source data group, either using the template or manually, select **Data Center Firewall Rule Builder**, and go to *Firewall Rule builder on page 7*.

Source Data Group Builder

The Source Data Group builder creates BIG-IP iRule Data Groups. Data groups contain the source IP address list for addresses to which you want to allow access.

1. **Data Group name**
   Specify a name for the data group. The iApp appends this name to the prefix **dg-dcfw-net-**.
2. **Source IP addresses**
   Specify which source IP addresses should be allowed by the Data Center Firewall. For each IP address, select the appropriate Mask from the list.
   You can optionally include a comment.

   Click the **Add** button to include additional source addresses. Click **Finished**.

If you want to add more source addresses at a later time, simply click **iApp** > **Application Services** > and then the name of your application service. On the Menu bar, click **Reconfigure**, and then add the additional servers.

This completes the source data group builder.

When you have finished creating the Source Data Group, continue with *Firewall Rule builder on page 7*.

Firewall Rule builder

The firewall rule builder creates the Firewall iRule using the source data group you created, and your answers to the template questions. This Data Center Firewall iRule is bound to a BIG-IP LTM virtual server. When client connections are attempted, the connection parameters are compared to the address/virtual server information in the BIG-IP LTM Data Groups you just created.

Firewall settings

1. **Prefix name**
   Specify a prefix that is used for the BIG-IP virtual servers. Objects created by the iApp use this prefix preceded by **dcfw-**.
2. **Enable comments**
   Select whether you want to enable comments or not. If you select Yes, a comment field appears in the BIG-IP Data Center Firewall Rules section.
3. **Action on deny**
   Specify what the BIG-IP system should do with traffic that is denied. You can select Discard or Reject. If you select Discard, the BIG-IP system drops without sending a response. If you select Reject, the BIG-IP system rejects the connection and sends a response.

Syslog settings

In this section, you have the option of configuring the Data Center Firewall to send logs to external logging systems, such as Splunk or FireMon.

1. **Using external logging systems**
   Specify whether you want to configure the Data Center Firewall to send logs to external logging systems. If you select No, the logging questions disappear. Continue with the next section. If you select Yes, continue with #2.
2. **Log all traffic**
   Select whether you want the Data Center Firewall to log all traffic types.
   If you select No, the system only logs matching traffic.

Important →

   If you select Yes, the system logs non-matching as well as matching traffic.
   Use this option with extreme caution, as the BIG-IP system logs all packets, so the volume of log messages could be very large and adversely affect performance.
3. **Logging format**
   Leave this set to the default. There are no options other than Default at this time.
4. **TCP or UDP**
   Specify whether the syslog server is using TCP or UDP. The protocol you choose is used by the BIG-IP system to communicate with the external syslog servers.
5. **IP Address and port of the logging system**
   Specify the IP address and port used by your external logging system. Click add to include additional servers.

BIG-IP Data Center Firewall Rule settings

In this section, you configure the Data Center Firewall rule options.

1. **Configure new rules**
   Select whether you want to create new Firewall rules at this time. If you select No, the rest of the questions in this section disappear; continue with the next section.
   If you select Yes, answer the following questions.
2. **Address translation**
   Select whether you want the BIG-IP to perform address translation. If you select Yes, the Destination NAT and Inside Address and Port fields appear in the BIG-IP Data Center Firewall Rules section. You then have the ability to enable or disable address translation for each rule you create.

Custom name
Select whether you want to include a custom name for the BIG-IP virtual server. If you select Yes, the Custom Name field appears in the BIG-IP Data Center Firewall Rules section. If you select No, the system uses the default name.

3. **VLANs**
   Specify the VLANs on which the rules created by the Data Center Firewall should be run. You must select a VLAN here.
4. **Idle non-TCP and UDP connections**
   Specify the number of seconds you want the BIG-IP system to wait before non-TCP or UDP idle connections time out.
   This and the following two settings determine the default timeout values. You still have the ability to adjust the timeout value of specific rules in the next section.
5. **Idle TCP connections**
   Specify the number of seconds you want the BIG-IP system to wait before idle TCP connections time out.
6. **Idle UDP connections**
   Specify the number of seconds you want the BIG-IP system to wait before idle UDP connections time out.

BIG-IP Data Center Firewall Rules

In this section, you specify the values for the Data Center Firewall rule set. For each row of the ruleset, the BIG-IP system creates a virtual server and applies the Data Center Firewall iRule to it. Note that this row is very long and you have to scroll to the right to complete all of the options.

1. **Custom Name**
   If you chose to enable the Custom Name field, this question appears. Type the name you want to give this virtual server.
2. **Address**
   Specify the IP address for the host or network destination to which you are allowing access.
3. **Mask**
   Select the appropriate mask from the list or type a value in the box.
4. **Protocol**
   Select the appropriate protocol from the list or type a value in the box.

5. **Port**
   Select the appropriate port from the list or type a value in the box.
6. **Destination NAT**
   If you selected to enable address translation, this question appears. Select whether you want to enable destination address translation on this rule.

   If you select No, do not configure the Inside Address or Inside Port. Continue with #9.

   If you select Yes to enable destination address translation, you must complete the Inside Address and Port.

Critical →

*You **cannot** enable address translation if you are using a network address as your destination. The BIG-IP system creates a one-to-one relation between the outside destination and the inside destination.*

7. **Inside Address**
   Type the IP address of the internal resource you want to use for destination NAT. The BIG-IP system creates a pool with this resource as a member.
8. **Inside Port**
   Type the associated port used by the internal resource.
9. **Action**
   Select the action to take for the source data group that you will select in #10.
   - If you select Allow, addresses in the source group are allowed by the Data Center Firewall, and all other traffic dropped.
   - If you select Deny, all addresses in the source group are dropped and all other traffic is allowed.
10. **Source Group**
    From the list, select the source Data Group you created.
11. **Allow iApp Edit**
    Select whether you want to allow iApp edits. If you select Yes, after completing this iApp template, if you re-enter the template to reconfigure the iApp, if you make changes to the rule, the iApp will modify all the relevant objects (virtual server, pool, and/or profiles) to reflect the changes.
    If you select No, the iApp does not modify the object that was originally created, it only updates the source group and destination comments. This allows further modification of the virtual servers created by the iApp.
12. **Timeout**
    Specify a timeout value. You can leave the default, select an option from the list, or type a timeout value. If you leave the default, the iApp uses the timeout values you specified in the previous section.
13. **Mirror**
    If you have a redundant BIG-IP configuration with an active and standby BIG-IP device, select whether you want to mirror connections between the BIG-IP system you are configuring now, and the standby device.
14. **Log**
    If you chose to enable external logging systems, select whether you want to enable logging on this virtual server.

Application Delivery Security

In this section, you specify whether you want to apply the Data Center Firewall ruleset to any of your existing BIG-IP LTM virtual servers. This adds an extra layer of protection for your application deployments.

1. **Apply rule to BIG-IP LTM virtual servers**
   Select whether you want to apply the Data Center Firewall rule produced by the iApp template to any of your existing BIG-IP virtual servers.
   If you select No, continue to the Finish section.
   If you select Yes, additional questions appear.
2. **Configured Ruleset**
   Specify the following information:
   a. *Virtual Server*
      Select the virtual server to which you want to add the Data Center Firewall rule.
   b. *Action*
      Select the action to take for the source data group that you will select in #10.
      - If you select Allow, addresses in the source group are allowed by the Data Center Firewall, and all other traffic dropped.
      - If you select Deny, all addresses in the source group are dropped and all other traffic is allowed.
   c. *Source Group*
      From the list, select the source Data Group you created.
   d. *Logging*
      If you chose to enable external logging systems, select whether you want to enable logging on this virtual server.

Finished

Review your answers to the questions. When you are satisfied, click the **Finished** button. The BIG-IP system creates the relevant objects.

Disabling Strict Updates

If you need to manually modify any of the configuration objects created by the template, or if you are using this Data Center Firewall iApp to protect an existing virtual server that is owned by an iApp application service, you must first disable the Strict Updates feature. By disabling Strict Updates, if you re-enter the iApp template and modify the configuration within the iApp, you must make all changes again manually.

To disable Strict Updates

1. On the Main tab, expand **iApp** and then click **Application Services**.
2. Click the name of your Application service from the list.
3. From the **Application Service** list, select **Advanced**.
4. In the **Strict Updates** row, clear the check from the box to disable Strict Updates.
5. Click the **Update** button.

Apendix A: Manually creating the Data Center Firewall iRule

In this section, we show you how to manually configure the Data Center Firewall iRule, along with the source Data Groups. For detailed information, see the BIG-IP Data Center Firewall Configuration Guide, available on Ask F5 (*http://support.f5.com/kb/en-us.html*).

Configuring the Data Groups

The allowed addresses are a list contained within BIG-IP LTM iRule *data groups*. The data group is used as a static variable in the iRule you will create later in this section.

In this section, we create two data groups, an address data group that contains a list of allowed address, and a string data group that associates the relevant virtual servers to the address group data group.

To configure the address data group

1. On the Main tab, click **Local Traffic > iRules > Data Group List**. The Data Group List screen opens, displaying a list of data groups on the system.
2. Click **Create**.
   The New Data Group screen opens.
3. In the **Name** box, type a name. In our example, we use **`dg-dcf-shownetworks`**. Make note of the name you use here, as it is used in the string data group you create in the following procedure.
4. From the **Type** list, select **Address**.
5. Using the **Address Records** setting, add each IP address that you want to include in the data group:
   a. For the **Type** setting, select **Host** or **Network**.
   b. In the **Address** field, type an IP address.
   c. If the address type is **Network**, type a network mask in the **Mask** field.
   d. In the **Value** field, type **none**.
   e. Click **Add**.
   f. Repeat these steps for each IP address you want to include in the data group.
6. Click **Finished**. The new data group appears in the list of data groups. You now have a data group that lists the source IP addresses for allowed traffic.

After creating this data group, you must create a string data group that associates the relevant virtual servers with the address data group you just created. The virtual servers listed in the string data group are those that you intend to use for access control by assigning an access control iRule to them later.

To create the string data group

Before you create this data group, verify that you have created an address data group named dg-dcfshownetworks.

1. On the Main tab, click **Local Traffic** > **iRules** > **Data Group List**. The Data Group List screen opens, displaying a list of data groups on the system.
2. Click **Create**. The New Data Group screen opens.

3. In the Name field, type a name. In our example, we use **dg-dcf-fwdb**. Make note of the name you use here, as it is used in the iRule you create in the following section.
4. From the **Type** list, select **String**.
5. Using the String Records setting, create entries consisting of a virtual server name and a data group name:
   a. In the **String** field, type the name of the virtual server (using lower-case characters) for which you want to implement access control through data groups and the iRule. The iRule is case sensitive. You also must enter the path (such as /Common/<virtual server name>).
   b. In the **Value** field, type the name you gave the address data group in step 3 of the previous procedure. In our example, we use **dg-dcf-shownetworks**.
   This name must match the name of the other data group exactly.
   You also must enter the path (such as /Common/<virtual server name>).
   c. Click **Add**.
   d. Repeat these steps for each virtual server you want to include in this data group.

   Each specified virtual server can represent the same destination IP address as the others, but must have a unique port name or port number.
6. Click **Finished**.
   The new data group appears in the list of data groups.

You now have a mapping of virtual servers to source IP addresses that the following access control iRule assigned to those virtual servers can reference.

Creating the Data Center Firewall iRule

The F5 Data Center Firewall iRule is bound to a BIG-IP LTM virtual server. When client connections are attempted, the connection parameters are compared to the address/virtual server information. The address lists are defined in BIG-IP LTM Data Groups you just created.

There are two versions of the iRule, one version if you want to send log messages to third party logging servers, and a version if you are not sending log messages. Each rule that has logging enabled generates and sends log messages to the log servers. The log messages are sent using the High Speed Logging interface on the LTM.

Creating the iRule if you are not sending log messages

If you are not configuring the BIG-IP system to send log messages, use the following procedure to create the iRule.

To create the iRule

1. On the Main tab, click **Local Traffic** > **iRules**.
2. Click **Create**.
3. In the **Name** field, type a unique name for the iRule.
4. In the **Definition** section, copy and paste the following iRule, omitting the line numbers.

   Make sure to change the value in red to match the path and name of the String Data Group you created.

   The following iRule configures the BIG-IP system to DENY by default and only allow what's in the data groups. If you want to ALLOW by default, see the note following the iRule code.

```
1  when CLIENT_ACCEPTED {
2     while {1} {
3        set dcfw_vdg [ class match -value [virtual name] equals /Common/STRING_DATA_GROUP ]
4        if { ! [ class exists $dcfw_vdg ] } { break }
5        if { ! [ class match [IP::remote_addr] equals $dcfw_vdg ]
6     }
7     {
8        break
9     }
10    return
11    }
12    discard
13 }
```

If you want to default to ALLOW and only DENY what's in the data group, change line 5 in the iRule above to the following:

```
if { [ class match [IP::remote_addr] equals $dcfw_vdg ]
```

5. Click **Finished**.

Attaching the iRule to virtual servers

The final task is to associate this iRule with a virtual server that you want to protect with the Data Center iRule.

To attach the iRule to a virtual server

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
2. On the Menu bar, click **Resources**.
3. In the iRule section, click **Manage**.
4. From the **Available** box, click the name of the iRule you just created, and then click the Add (**<<**) button to move it to the **Enabled** box. If you created two iRules, add them both to the Enabled box.
5. Click **Finished**.

This completes the configuration if you are not logging.

Creating the iRule if you are sending log messages

Use this section if you want to send log messages to third party applications.

Before you create the iRule, you must create a BIG-IP pool for the logging servers that is referenced in the Data Center Firewall iRule. If you want to send traffic to multiple logging servers, you must have a pool for each server.

To create the HSL pools

1. On the Main tab, click **Local Traffic** > **Pools**. The Pool List screen opens.
2. Click **Create**. The New Pool screen opens.
3. In the **Name** field, type a unique name for the pool. In our example, we type **splunk_hsl**.
4. From **Health Monitors Available** list, select a monitor (such as **tcp**) and the click the Add (**<<**) button to move it to the Active list.
5. From the **Load Balancing Method** list, select how the system distributes traffic to members of this pool.
6. In the New Members section, make sure the **New Address** option button is selected.
7. In the **Address** box, type the IP address of a logging server.
8. In the **Service Port** box, type the appropriate port number.
9. Click the **Add** button to add the member to the list.
10. Click **Finished**.
11. If you want to send traffic to more than one logging server, repeat this entire procedure for each server. Each pool must only contain one logging server.

Before creating the iRule on the BIG-IP system, you need modify the values for three objects in the iRule code. These are clearly marked in red text in the iRule.

- The **hostname** variable should be set to the shared name of both the active and standby unit.
- The **hsl_dst** variable contains the name of the LTM pool(s) you created for the logging servers.
- The **MAPPING_DATA_GROUP** must be the name of the string data group you created. In our example, this is **dg-dcf-fwdb**.

The following iRule works for two virtual server types: Forwarding or Performance (Layer 4). If you want to use this functionality for a TCP or UDP virtual server, you must create an additional virtual server with different switch statement. Instructions

To create the iRule

1. On the Main tab, click **Local Traffic** > **iRules**.
2. Click **Create**.
3. In the **Name** field, type a unique name for the iRule.
4. In the **Definition** section, copy and paste the following iRule.

   Make sure to change the values in red to match your environment.

```
when RULE_INIT {
   set static::dbg 0
   set static::hsl_dst {{hslpool1}{hslpool2}}
   set static::hostname "hostname"
   set static::module "F5-LTM"
   set static::msgid "1"
   set static::mapping_dg "<MAPPING_DATA_GROUP>"
}

when CLIENT_ACCEPTED {
   set src [IP::remote_addr]
   set dst [IP::local_addr]
   set vdg "default_deny"
   switch [IP::protocol] {
      6 {
         set srcp [TCP::remote_port]
         set dstp [TCP::local_port]
      }
      17 {
         set srcp [UDP::remote_port]
         set dstp [UDP::local_port]
      }
      default {
         set srcp 0
         set dstp 0
      }
   }
   while {1} {
      set vdg [ class match -value [virtual name] equals $mapping_dg ]
      if { ! [ class exists $vdg ] } { break }
      if { ! [ class match [IP::remote_addr] equals $vdg ] } { break }
      return
   }
   set msg "[clock format [clock seconds] -format "%Y-%m-%d %H:%M:%S" ] \
   $static::hostname \
   $static::module \
   $vdg \
   $static::msgid \
   deny \
   [IP::protocol] \
   $src \
   $srcp \
   $dst \
   $dstp \
   [virtual name] \
   $src \
   $dst \
   -"
   if { $static::dbg } { log local0. $msg }
   foreach hsp $static::hsl_dst {
      set hsl [HSL::open -proto UDP -pool $hsp]
      HSL::send $hsl $msg
      unset hsl
   }
   reject
}
```

This rule continues on the following page

```
when SERVER_CONNECTED {
   set msg "[clock format [clock seconds] -format "%Y-%m-%d %H:%M:%S" ] \
   $static::hostname \
   $static::module \
   $vdg \
   $static::msgid \
   allow \
   [IP::protocol] \
   $src \
   $srcp \
   $dst \
   $dstp \
   [virtual name] \
   [IP::local_addr] \
   [IP::remote_addr] \
   -"
   if { $static::dbg } { log local0. $msg }
   foreach hsp $static::hsl_dst {
      set hsl [HSL::open -proto UDP -pool $hsp]
      HSL::send $hsl $msg
      unset hsl
   }
   unset -nocomplain src dst srcp dstp msg vdg
}
```

5. Click the **Finished** button. If you are using the iRule for a Forwarding or Performance Layer 4 virtual server, continue with *Attaching the iRule to virtual servers on page 13*.
6. If you are using the iRule with a virtual server type of something other than Forwarding or Performance Layer 4, use the following guidance to create another version of the iRule.
7. Click **Create** to start a new iRule.
8. In the **Name** box, give the iRule a unique name. We recommend a name with TCP or UDP in it, as appropriate.
9. In the **Definition** section, copy and paste the iRule above.
10. You must change the switch statement in the iRule, depending on which protocol you are using (TCP or UDP).

    Locate lines 13 to 26:

```
switch [IP::protocol] {
      6 {
         set srcp [TCP::remote_port]
         set dstp [TCP::local_port]
      }
      17 {
         set srcp [UDP::remote_port]
         set dstp [UDP::local_port]
      }
      default {
         set srcp 0
         set dstp 0
      }
   }
```

11. Depending on which protocol you are using, replace lines 13-26 with the following lines:

    a. **TCP**:

```
switch [IP::protocol] {
   6 {
      set srcp [TCP::remote_port]
      set dstp [TCP::local_port]
   }
   default {
      set srcp 0
      set dstp 0
   }
}
```

    b. **UDP**:

```
switch [IP::protocol] {
   17 {
      set srcp [UDP::remote_port]
      set dstp [UDP::local_port]
   }
   default {
      set srcp 0
      set dstp 0
   }
}
```

12. Click **Finished**.
13. See *Attaching the iRule to virtual servers on page 13*.

This completes the configuration.

Appendix B: Using third-party SIEM and Management applications

This appendix contains information on configuring the BIG-IP system with Splunk and FireMon. All of the procedures in this section are optional.

No matter which application you are using, you need to create a BIG-IP pool for the logging servers as described in the preceding section.

Using Splunk

Splunk collects and harness machine data. Splunk has the flexibility to do any type of real-time and historical analysis, and the power to deliver custom dashboards and views to anyone in your organization. By monitoring and analyzing everything from customer clickstreams and transactions to network activity to call records, Splunk turns your machine data into valuable insights. For more information on Splunk, see *http://www.splunk.com/*.

Installing the Splunk application for F5 Networks

The first task is to download and install the Splunk application for F5 Networks.

To download and install the Splunk application for F5

1. From the Splunk web interface home page, on the Menu bar, select **App**, and then click **Find more apps**.
2. In the search box, type **F5 Networks**.
3. Find **Splunk for F5 Networks**, and then click the **Install free** button.

Important → *Make sure you install **Splunk for F5 Networks**, and not one of the other Splunk for F5 options.*

Once the Application is installed, it appears in the App menu as **Splunk for F5 Networks**.

Adding a data input to Splunk

The data input is a configuration setting that configures Splunk to listen for log messages on UDP or TCP and a specific protocol port number. Use the following procedure to configure a data input to listen for the data center firewall log messages.

To add a data input

1. From the Splunk web interface home page, click **Manager** on the upper right corner of the screen.
2. In the Data section, click **Data inputs**.
3. Click the **Add new** link in the row for the protocol (TCP or UDP) you specified when configuring the F5 Data Center Firewall:

Figure 2: *Add new link*

4. In the Source section, in the **UDP port** or **TCP port** box, type **514**.
5. In the Source type section, from the **Set sourcetype** list, select **From list**.
6. From the **Select source type from list** options, select **syslog**.
7. Click **Save**.

Accessing the Splunk for F5 Networks Application

To start using the Splunk for F5 Networks application, from the App menu on the upper right, select **Splunk for F5 Networks**. The Menu bar on the summary page is the location to make selections for navigating within the Splunk Application.

The Summary page includes four sections. The top section shows the Indexed data information and reports the total number of events that are indexed, and the date for the earliest and most recent events. The next section lists the available log source protocols and counts. The example shown below is reporting more than 13 million logs have been indexed via UDP on port 514.

The last two sections contain a listing of the identified source types with counts. It also reports a list of all the log source hosts with event counts.

Two dashboards and reports are installed and available in the Applications tab. The report is a collection of database queries and charts pertaining to the most recent 30 minutes of traffic. This report can be scheduled to automatically run. The dashboards are based on BIG-IP LTM logs and the Data Center Firewall iRule logged data, as well as the standard administrative logging of BIG-IP messages. The former is used for the Firewall details. And the latter is used for the LTM Pool details.

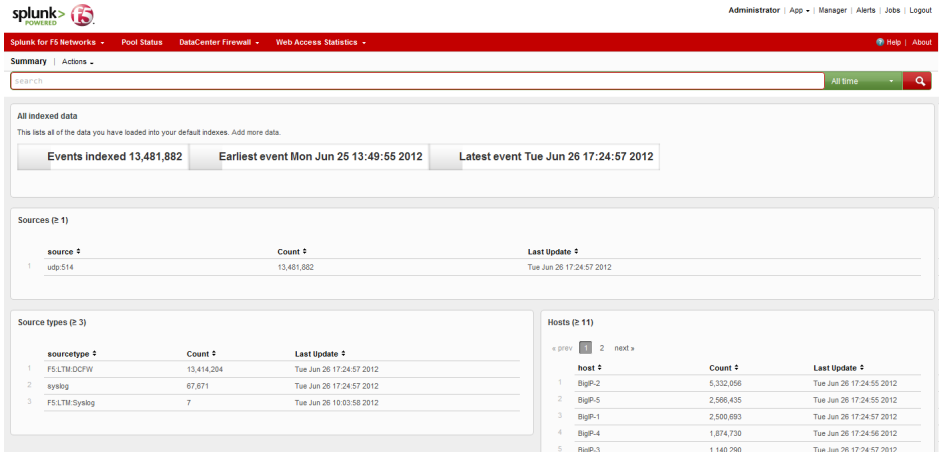


Figure 3: *Summary page of Splunk for F5 Networks*

Data Center Firewall menu

From the Data Center Firewall menu at the top of the page, you can choose to launch the dashboards or the Data Center Firewall 30 minute report.

Firewall Activity page

In this section, we describe the contents of the Data Center Firewall activity report. From the **Data Center Firewall** menu, click **Last 30 minutes**. This report has nine sections. Eight are charted data, and the last section is a listing of log events.

- *Allow vs Deny*
  The Allow vs Deny charts plot the log activity over time. This indicates which devices are most active and the distribution of allowed requests versus denied requests.
- *Top 10 rules*

The Top 10 Source Groups chart will report the DCFW Source group activity. These are the names of the data groups that contain the allowed address lists.

- *Top 10 allowed by source IP*
  This chart shows the top 10 source IP addresses that were allowed access.
- *Top 10 denied by source IP*
  This chart shows the top 10 source IP addresses that were denied access.
- *Allowed by Device ID*
  This chart enumerates all the allowed log messages and sorts them by the device ID. The Device ID is the individual LTM that is receiving the connections requests and in turn sending the log data to Splunk. This value is defined within the iRule variable definitions
- *Allowed by Virtual Server*
  This chart enumerates all the allowed connection log events and catalogs them by the Virtual Server Name. If all Virtual Server names are unique within the deployment then this chart will report each individually. Virtual servers that are named the same will have those stats accumulated and reported as a single element.
- *Denied by Device ID*
  This chart enumerates all the denied log messages and sorts them by the device ID.
- *Denied by Virtual Server*
  This chart enumerates all the denied connection log events and catalogs them by the Virtual Server Name. If all Virtual Server names are unique within the deployment then this chart will report each individually. Virtual servers that are named the same will have those stats accumulated and reported as a single element.
- *F5 LTM Data Center Firewall events*
  The final section is a listing of the DCFW log events in a table. These events can be clicked on and drilled into so custom searches can be performed.

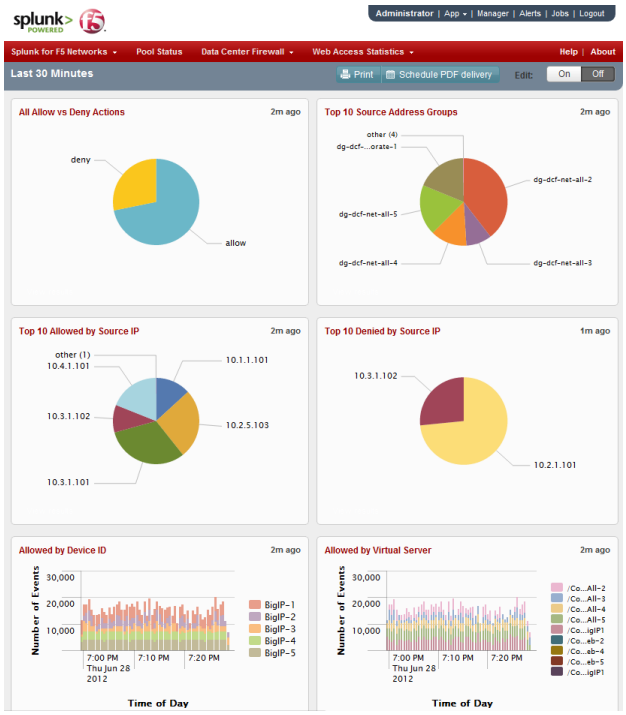


Figure 4: *Last 30 minutes page (truncated)*

The Firewall Traffic dashboard

In this section, we describe the contents of the Data Center Firewall Traffic Summary. From the **Data Center Firewall** menu, click **Firewall Traffic** to launch the Firewall traffic dashboard. This dashboard is an accumulation of event statistics based on the logs sent by the Data Center Firewall iRule.

- *Summary*
  The top section is a summary of the dashboard contents. From the list, you can select a specific time frame, create a custom time frame, or view real time reports.
- *Filters*
  The next section is a set of four data fields. These fields allow you to tailor which statistics are reported. For example, you can specify a BIG-IP virtual server to narrow the report to just that object. By default all fields are reported without filters.
- *Session Statistics*
  The session stats section reports the accumulated numbers of unique Source IPs, Destination IPs, and Devices.
- *Traffic by Device over time*
  The traffic by device over time section reports by LTM device the total number of events being received. This is the combination of both allowed and denied events. It's a rough measurement of how active each device is.
- *Traffic by Action over time*
  The traffic by action reports the accumulated allowed vs denied events across the entire deployment.
- *Action Breakdown*
  Action breakdown is similar to the Traffic action graph. The user sees a pie chart depicting the ratio of allowed vs denied events. The user can click on the denied or allow pie slices and build a custom report.
- *Allowed by Source*
  This section shows the top source IPs that have been allowed. This, and the following sections, allows the user to see the top number of source or destination IPs that are either being allowed access or denied access and which ports they are attempting to access.
- *Allowed by Destination*
  This section shows the top destination IPs that have been allowed.
- *Denied by Source*
  This section shows the top source IPs that have been denied.
- *Denied by Destination*
  This section shows the top destination IPs that have been denied.

The Data Center Firewall Rules Dashboard

In this section, we describe the contents of the Data Center Firewall Rules Summary. From the **Data Center Firewall** menu, click **Firewall Rules** to launch the Firewall traffic dashboard. This dashboard is an accumulation of event statistics based on the logs sent by the Data Center Firewall iRule.

- *Summary*
  The top section is a summary of the dashboard contents. From the list, you can select a specific time frame, create a custom time frame, or view real time reports.
- *Filters*
  The next section is a set of four data fields. These fields allow you to tailor which statistics are reported. For example, you can specify a Action or RuleID to narrow the report. By

default all fields are reported without filters.

- *Session Statistics*
  The session stats section reports the accumulated numbers of unique Source IPs, Destination IPs, and Devices.
- *Firewall Activity Over Time*
  This section charts in a stacked bar chart the active Source Address groups (Rules) as well as the Virtual Servers activity. These charts are an indication of the load of traffic being serviced by all of the LTMs in the network.
- *Top Virtual Server*
  Reports that top 10 virtual servers and the number of events each server is reporting.
- *Top Source Address Group*
  This chart is an indication of the distribution of traffic being reported on a per source address group basis. It also shows which address groups are more or less used.
- *Top Firewall Comment*
  This section is based on the Source Address group comment. If comment reporting is enabled in the iRule / iApp settings, this chart reports on each unique comment and accumulates the values over time. For best performance the reporting of Comment fields is disabled by default.
- *Action by Virtual Server*
  This reports the number of events each Virtual Server has reported for both the allowed and denied actions.
- *Action by Source Address Group*
  This lists the top Source address group reporting the allowed vs denied connection requests.

Pool status dashboard

In this section, we describe the contents of the Pool status dashboard, which is a collection of report data pertaining to LTM Pool status.

- *Summary*
  The top section is a summary of the dashboard contents. From the list, you can select a specific time frame, create a custom time frame, or view real time reports.
- *Session Statistics*
  This section reports the number of members that are down, number of affected pools, and the maximum downtime counter.
- *Member Up Events*
  This section is the listing of Pool Member up events. This also lists the downtime for that member, which pool they belong to, the node name of the pool member and the current status column. The Downtime column reports how long that member was down prior to returning to an active up state.
- *Members Down by Pool*
  This chart reports the number of members that are down per pool. In the example on the following page, there are 4 pools being reports with members down counts ranging from 1 to 5 down members.
- *Member Down Events*
  This section is similar to Member Up Events. However, it is reporting the member events for nodes that reported down and how long they had been up prior to changing to a down state.

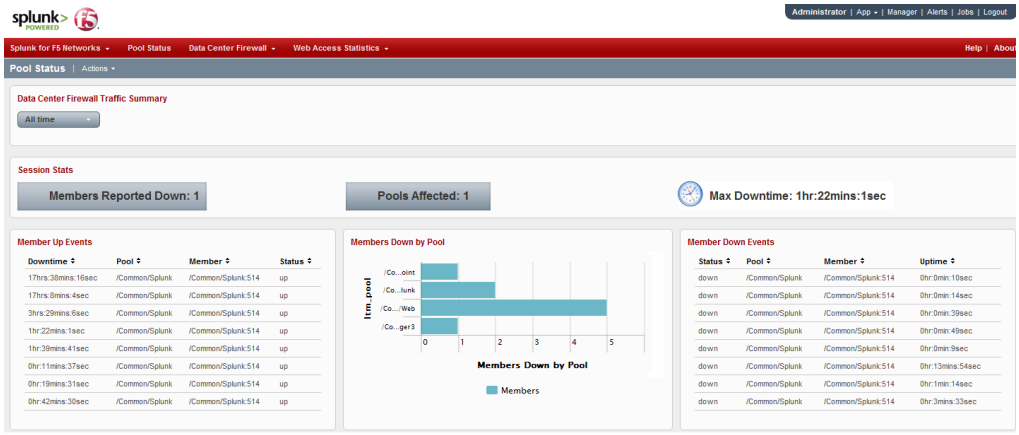


Figure 5: *Pool Status summary*

Scheduling PDF reporting

Splunk is capable of scheduling reports to be performed on schedule. The dashboards have an Action menu pull down is how to access the scheduler. This is an add-on application that can be installed the same way the Splunk for F5 Networks was installed. This is a Linux only supported application.

For more information on scheduling PDF delivery refer to the Splunk documentation.

Using FireMon

FireMon Security Manager provides policy and configuration management, enforcement and auditing of network devices such as firewalls, routers, switches and load balancers, while monitoring for and alerting on configuration changes. Security Manager also assesses current configuration settings and audits these against best practices and compliance standards – and provides extensive options for remediating configuration issues. For more information on FireMon, see *http://www.firemon.com/*.

Prerequisites

- Before configuring FireMon to monitor the BIG-IP LTM instances, make sure the FireMon server is defined in the High Speed Logging configuration for the iApp / iRule as described earlier in this document.
- The Remote log server must be configured to send administrative syslog messages to the FireMon server.

Configuring FireMon with the F5 Datacenter Firewall iRule

FireMon is distributed as a virtual machine or as an appliance. Management access to the FireMon server is accomplished via a client side application.

Configuring FireMon for the BIG-IP LTM

The first task is to configure FireMon for the BIG-IP LTM device.

To configure FireMon for the BIG-IP system

1. Launch the application and enter a valid user name, password, and host IP address or name.
2. From the **Tasks** box, click **Create a new Device**.
3. From the By Vendor menu, expand **F5 Networks** and select **BIG-IP**. The Device-specific menu items open.
4. In the General section, type the appropriate information from your BIG-IP system in the **IP Address** and **DNS name** boxes. You can optionally provide a description.
5. In the Credentials section, in the **User name** and **Password** boxes, type the BIG-IP system credentials.
6. Click **OK**.

Configuration details

There is a second tab for configuration details. This is for configuration monitoring, and is enabled by default. This feature instructs FireMon to periodically pole the device for its device configuration details. If a device configuration changes, FireMon alerts the administrator changes have been made since the last poling period.

The new BIG-IP system device displays in the Devices pane. Expand the menu tree if necessary and then click the new device to see the properties.

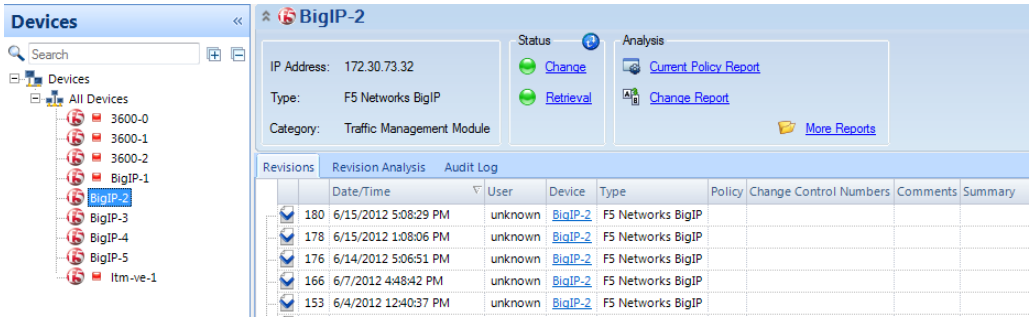


Figure 6: *FireMon showing the new BIG-IP device*

Figure 6 shows that the device is actively being poled for changes and a listing of when the changes have been detected.

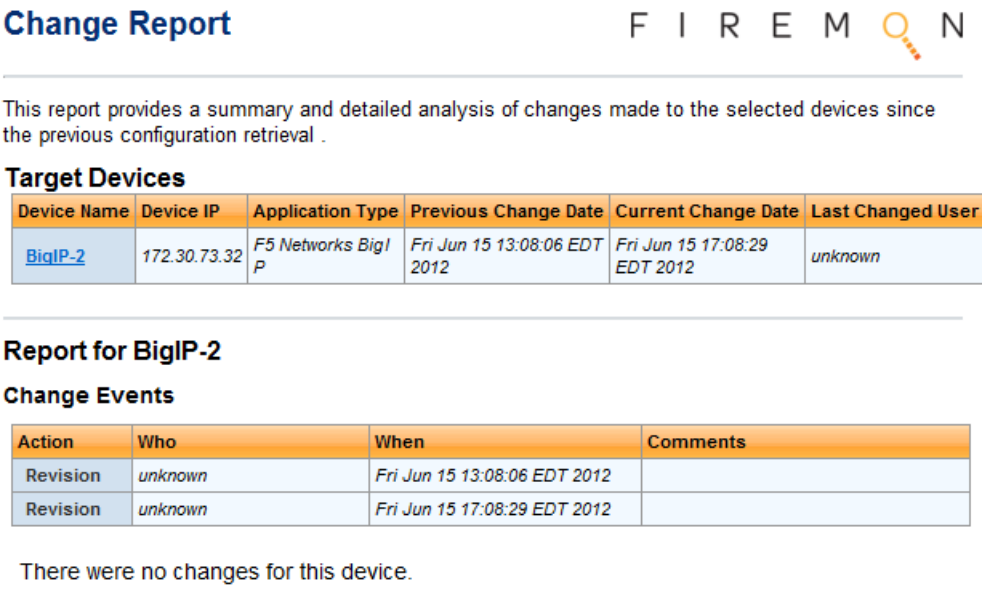
FireMon reports

FireMon has a rich set of prebuilt reports. These reports include Usage, Compliance, Analysis, change control, and change reporting. They are accessed using the Reports menu tab on the left pane.

To run a report

1. From the Reports pane, expand **Reports** and then click **Change Report**.
2. Click **Run Report**.
3. From the Target list, select the appropriate BIG-IP device.
4. Click **Finished**.

The report runs and a Change Report opens, similar to the following.



Change Report

FIREMON

This report provides a summary and detailed analysis of changes made to the selected devices since the previous configuration retrieval .

Target Devices

Device Name	Device IP	Application Type	Previous Change Date	Current Change Date	Last Changed User
BigIP-2	172.30.73.32	F5 Networks BigIP	Fri Jun 15 13:08:06 EDT 2012	Fri Jun 15 17:08:29 EDT 2012	unknown

Report for BigIP-2

Change Events

Action	Who	When	Comments
Revision	unknown	Fri Jun 15 13:08:06 EDT 2012	
Revision	unknown	Fri Jun 15 17:08:29 EDT 2012	

There were no changes for this device.

Figure 7: *FireMon change report*

You can repeat this process for other reports of interest.

Document Revision History

Version	Description	Date
1.0	New guide	06/13/2012

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com