Automating Server Firewalls
With CloudPassage Halo

Contents:

About Halo Server Firewalls
Implementing Firewall Policies
  Create and Assign a Firewall Policy
  Specify Firewall-Related Components
Managing Server Firewalls
  View Your Firewall Dashboard
  View a Server's Firewall Status and Summary
  Update Firewall Policies
  Set Up Firewall Events and Alerts
Troubleshooting Firewalls
Example Firewalls: Multi-Server Web Application
  Web Server Firewall Policy
  Load Balancer Firewall Policy
  Database Server Firewall Policy

About Halo Server Firewalls

How Halo Server Firewalls Work
CloudPassage Halo automatically deploys, updates, and monitors host-based Windows or Linux firewalls for your cloud servers. Host-based firewalls can provide more protection for your cloud servers than traditional perimeter firewalls, because they can be tailored to the exact purpose of each type of server that you use. With Halo, you can design policies to facilitate inter-communication among the different categories of servers in your cloud, while simultaneously preventing malicious agents from gaining access.
Halo host firewalls also deploy themselves automatically and elastically, as your cloud-server population dynamically grows and shrinks. No servers are left uncovered and vulnerable to attack.

Halo firewall policies are also intelligent; they allow you to specify more than just IP addresses and ranges when defining the allowable sources or destinations of connections. For example:

- Because cloud providers typically assign arbitrary IP addresses to individual servers in the cloud, firewall implementation can involve tedious tracking of lists of server addresses. But with Halo these servers are in named server groups, so you can define high-level firewall policy rules using those group names as connection sources or destinations. Halo then uses those rules to create individual host-based firewall rules, taking care of tracking the IP addresses for you.

- To support CloudPassage GhostPorts multi-factor authentication, Halo allows you to create firewall policy rules that specify usernames as sources of inbound connections. When such a user authenticates, Halo temporarily updates the appropriate firewall rule, using that user’s IP address as the connection source and allowing access.

### Setting Up Your Halo Firewalls

You start your Halo server firewall deployment with a firewall policy—a template listing connection rules for inbound and outbound communication for a given kind of server. You create those rules in the Halo Portal using a convenient form, and then save them as a policy.

You then assign the firewall policy to a group of like-purpose servers, such as a web server group, or a database server group.

After that, Halo takes over—it installs individual firewalls based on your policy on all of the servers in the policy’s server group. Furthermore, Halo automatically updates all servers with any updates or changes you later make to that policy, or any changes to any of the servers’ IP addresses. Halo also automatically deploys new firewalls to any servers that are added to the group in the future, such as through cloning or re-activation.

Once your initial firewall setup is complete, you can track the state of all your server firewalls at once from the Halo Portal. Update your firewall policies anytime, and Halo will deploy the updates. Set up alerts so that you are notified if any firewall is tampered with.
Implementing Firewall Policies

The Halo Portal makes the process of creating and deploying firewalls as simple as possible. First, you optionally define some related components such as IP zones. Then you create a firewall policy that applies to a group of similar servers. Finally, you assign the policy to that server group.

Halo then takes care of the rest, automatically assigning a firewall based on that policy to each server in the group, patching in all the correct IP addresses, updating all the servers if you ever change the policy, and adding the firewall to any new servers that join the group, either by manual addition or by cloning/cloudbursting.

Create and Assign a Firewall Policy

Now use the Halo Portal to create a firewall policy and assign it to a server group. Once the policy is active and any server comes online through cloning or re-activation of a server in this group, that new server automatically receives the latest appropriate firewall from Halo.

1. Go to the Add New Firewall Policy page.

   In the Halo Portal, go to Policies > Firewall Policies and click Add New Windows Firewall Policy or Add New Linux Firewall Policy.

   a. Give the policy a descriptive name and optionally add an additional description.

   b. Windows only: Specify your logging preferences. (For Linux, you will specify a preference with each rule.)

2. Create firewall rules and save the policy.

   A firewall policy is just a set of rules that, when applied to a server, control which inbound and outbound connections will be permitted. To create the policy, you set up those rules. For examples of rules you might create, see Example: Firewall Policies for a Web Application.
Note: When you create an inbound or outbound rule that permits a connection, Halo automatically takes care of creating the corollary rule that allows return communication. You do not need to add the corollary rule in the policy. For details, see Implicitly Create Automatic Corollary Rules.

You'll see from the instruction below that Windows firewall rules differ somewhat from Linux rules. Follow the instructions below that apply to your servers' operating system.

Create inbound rules:
Each inbound rule describes the specifics of one kind of connection from the outside into the server. To create a new rule, click Add New or the Add Rule icon ( ) beside any existing inbound rule.

For each that rule you add or edit, specify the following attributes:

- **Active.** Leave the checkbox selected to keep the rule in effect. (Or clear it to temporarily disable the rule.)

- **Interface (Linux only).** For a Linux policy, specify the hardware or software interface (for example, eth0) through which a connection will be established. For more explanation about interfaces, see Add a Network Interface.

- **Source.** Select the IP zone, server group, or GhostPorts user that is the source of the connection attempt. For more explanation about IP zones, see Add an IP Zone. For instructions on creating a firewall rule for GhostPorts users, see Administering GhostPorts in the GhostPorts guide.

- **Service.** Select the name and port number (for example, https (tcp/443)) of the service that is establishing a connection. For more explanation, see Add a Network Service.

- **Connection State (Linux only).** For a Linux policy, specify the state of the connection that this rule applies to: NEW, ESTABLISHED, or RELATED. Halo firewall policies for Linux are stateful, meaning that you can create different rules for different times during a connection. See Specify Connection States for more information.

- **Action.** This is the core of the rule—the action the firewall should take when the above attributes apply to an inbound connection. In Linux, the possibilities are ACCEPT, DROP, or REJECT; in Windows, only ACCEPT or DROP are supported.

Note: DROP means that the connection request is simply ignored; REJECT means that an ICMP "unreachable" error message is sent to the requestor.

- **Log (Linux only).** Select this checkbox to create a log entry each time this rule is invoked.

Note: On Linux you specify logging per rule. On Windows you specify logging of all accepted connections and/or all dropped connections.

Windows firewall rule:

[Table of Windows firewall rule]

Linux firewall rule:

[Table of Linux firewall rule]

End this section of the policy with a default rule, to apply to any inbound connection attempt that is not described by any of the other inbound rules. Normally, it is a rule that drops (denies) all other inbound connections. You can construct the rule yourself, or you can click the Make this change or Add This Rule link...
on the form to have Halo insert it for you.

**Create outbound rules:**

Each outbound rule describes the specifics of one kind of connection attempt from this server to an outside entity. To create a new rule, click **Add New** or the Add Rule icon (/button) beside any existing outbound rule.

Create outbound rules the same way you created inbound rules. The attributes for outbound rules are identical to those for inbound, except that there is an outbound **Destination** attribute in place of the inbound **Source** attribute.

End this section of the policy with a default rule, to apply to any outbound connection attempt that is not described by any of the other inbound rules. Normally, it is a rule that drops (denies) all other outbound connections. You can construct the rule yourself, or you can click the **Make this change** or **Add This Rule** link on the form to have Halo insert it for you.

*Note:* For evaluation or proof-of-concept installations of Halo firewalls, you may wish to leave all outbound communication unrestricted to avoid cutting off any necessary server access.

**Rearrange or de-activate rules:**

To refine your firewall policy, you can manipulate the rules in these ways:

- Use the up-down drag-and-drop arrows to change the ordering of the rules. In use, the firewall's inbound or outbound rules are tested in order from the top, and testing stops as soon as one rule's criteria are met. Make sure the ordering of the rules gives you the results you want, and make sure your default-drop rule is the last one in the list.

- Use the **Active** checkbox to de-activate or re-activate individual rules for testing purposes or to respond to changes in your cloud environment.

When you have finished creating and arranging your inbound and outbound rules, click **Apply** to save the policy.

**Export the policy:**

After creating your policy, you can at any time export it in text format to verify that its rules are as you expect them to be. Note that the export version of a firewall policy includes the hidden Daemon-specific rules and automatic corollary rules that Halo creates, which do not appear when you edit the policy in the Halo Portal. For explanation and examples, see [Seeing the whole firewall](#).

### 3 Assign the firewall policy to your server group.

Return to the Halo Dashboard and, in the list of server groups, locate the name of the server group you want to assign this firewall policy to. Click the group's name, then click **Edit Details** beneath the name.

The Edit Group Details dialog opens. In the **Firewall Policies** area, open either the **Windows policy** or **Linux Policy** drop-down menu and select the name of the policy that you just created. Then click **Save**.
Your firewall policy is deployed automatically to the servers in your server group and it will immediately start protecting them. If you make changes to the policy in the future, those changes will be transmitted automatically to those same servers plus any clones dynamically generated from them.

*Note:* If at this point you find that your firewalls are not functioning as expected, you may need to add, edit, or remove some firewall rules. See [Troubleshooting Firewalls](#) for suggestions.

---

### Specify Firewall-Related Components

This section gives additional information or instructions that may help you specify certain firewall rules, attributes, and values.

---

### Specify Connection States

*(Linux only)*

On Linux platforms, Halo firewall policies generate iptable firewalls that are *stateful*—they support three types of connection states, called NEW, ESTABLISHED, and RELATED in the Halo Portal.

- From the standpoint of the firewall, a NEW connection is the first packet sent to the server.
- After the first packet has been received by the firewall, the connection is said to be ESTABLISHED.

To enable a connection to a server on most ports, use the connection states NEW and ESTABLISHED in your firewall rules. The Halo Firewall product will automatically create the [corollary outbound rule](#) with a connection state of ESTABLISHED only.

- The RELATED state is used for protocols like FTP that use one port for control and another port for data. If you want to enable external devices to be able to FTP files from a server, or use any other protocol that has a control port and a data port, create an inbound rule with the connection state of ANY (which is the same as NEW plus ESTABLISHED plus RELATED).

Note that in order to REJECT a packet, a RELATED entry must exist in the iptables firewall for the ICMP response. In this case also, the Halo Firewall does this for you automatically; you do not need to worry about creating any outbound rules allowing ICMP when you select one or more services to REJECT.

For more on connection states in iptables, see [http://www.faqs.org/docs/iptables/userlandstates.html](http://www.faqs.org/docs/iptables/userlandstates.html)

---

### Implicitly Create Automatic Corollary Rules

When you create an inbound rule in the Halo Firewall, the corollary outbound rule to allow return communication is automatically created—as also occurs with the common enterprise firewall offerings from Checkpoint, Juniper, Cisco, and so on.

For example, suppose you create the following inbound firewall rule for a Linux firewall:
It enables inbound NEW and ESTABLISHED communications of TCP to port 80. Halo will automatically create the outbound corollary rule, which enables outbound ESTABLISHED communications through the same hardware interface of TCP on port 80 to any destination. Note that the corollary rule will not permit NEW traffic to exit the server. This is an example of what makes the firewall stateful.

Automatic corollary rules do not appear on the Halo Portal page that you use to create and edit firewall policies, but you can see them if you export a firewall policy.

*Note:* Halo also creates automatic corollary rules for Windows firewalls, although those rules are not stateful, because Windows firewalls do not distinguish between NEW and ESTABLISHED connections.

## Add a Network Interface

*(Linux only)*

Network Interfaces are the physical or virtual hardware interfaces used by a Linux server. In a Linux firewall policy rule, you specify which interface the rule applies to by selecting it from the **Interface** drop-down list. Typical device names are `eth0` and `eth1`.

Halo provides a list of common interface device names, and you can add custom names to the list as needed. Here is an example **Interface** list:

```
any
eth0
eth0:1
eth0:15
eth0:2
eth0:3
eth1
Gigabit1
Gigabit2
lo
```

If you have implemented custom network interface devices on your servers, you can add their names to Halo so that they can be used in firewall rules.

1. In the Halo Portal, go to **Policies > Firewall Policies** and click **Network Interfaces**. Then click **Add Network interface**.
   
   *(Or, select "Add New" at the bottom of the **Interface** drop-down list in a firewall rule.)*

   ![New Network Interface](image)

2. Enter the name of your custom interface device and click **Create**.

The interface will now appear in the Network Interfaces list and in the **Interface** drop-down list when you create a
Add an IP Zone

**IP Zones** are arbitrary sets of IP addresses or CIDR blocks that specify the possible sources or destinations of a communication. In a firewall policy rule, you select an IP zone name from the **Source** or **Destination** drop-down list rather than entering individual IP addresses or ranges.

Halo provides only one default IP zone—"any (0.0.0.0/0)". It is up to you to define meaningful zones based on the IP addresses of your cloud servers, your other installations, your suppliers and partners, and so on. Here is an example set of IP zones in a **Source** or **Destination** list:

![Image of IP Zones]

You will likely want to define several IP zones for your firewall policies, to describe various parts of your corporate network. You may not need to define IP zones for the addresses of your Halo-protected servers, because you will be able to refer to them by server-group name in your firewall policies. However, if for example you need to specify only the internal IP addresses for a group of servers, you might want to create an IP zone for that purpose.

1. In the Halo Portal, go to **Policies > Firewall Policies** and click **IP Zones**. Then click **Add IP Zone**.
   
   (Or, select "Add New" at the bottom of the **Source** or **Destination** drop-down list in a firewall rule.)

![New IP Zone]

   *Here, the CIDR block defining all of the IP addresses in the U.S. call center is given a name.*

2. Enter a name for the zone, then enter one or more IP addresses or CIDR blocks, separated by commas. Then click **Create**.

   The IP zone will now appear in the IP Zones list and in the **Source** and **Destination** drop-down lists in a firewall rule.

**Note:** CloudPassage recommends that you include no more than 300 IP addresses and CIDR blocks in a single IP zone. If you need to specify a larger number, you can allocate them among multiple IP zones, and assign the zones individually to multiple, otherwise identical firewall rules.

Add a Network Service

**Network Services** are named IP application protocol/port number pairs (for example, "ldap(tcp/389)") that you specify in firewall policy rules by selecting them from the **Service** drop-down list.

Halo provides a list of the most common Linux and Windows services, and you can define custom services as well.
Here is the default **Services** list:

- any
- address mask (icmp/17)
- dns AXFR (tcp/53)
- dns query (udp/53)
- echo (udp/7)
- http (tcp/80)
- https (tcp/443)
- imap (tcp/143)
- imap (secure) (tcp/993)
- ldap (tcp/389)
- LoadBalancer (tcp/8080)
- mysql (tcp/3306)
- ping (icmp/8)
- pop3 (tcp/110)
- pop3 (secure) (tcp/995)
- postgresql (tcp/5432)
- rdp (tcp/3389)
- smtp (tcp/25)
- smtps (tcp/465)
- ssh (tcp/22)
- timeslamp (icmp/13)
- Add New

You may not have to add any new network services to Halo, but it is simple to do so if you need to.

1. In the Halo Portal, go to **Policies > Firewall Policies** and click **Network Services**. Then click **Add Network Service**.
   (Or, select "Add New" at the bottom of the **Service** drop-down list in a firewall rule.)

2. Enter a name for the service, specify a protocol, and specify a port. Then click **Create**.

   The network service will now appear in the Network Services list and in the **Service** drop-down list in a firewall rule.

---

**Managing Server Firewalls**

Once you have completed one or more firewall policies and assigned them to server groups, you can use the Halo Portal to manage them.

- You can verify that every protected server in your cloud has a functioning firewall that is appropriate for its server group. You can view detailed firewall status for any server. You can also perform server administration—adding or deleting servers, moving them among server groups and so on. (Server administration is documented in the *Halo Operations Guide*.)

- You can create new firewall policies and delete unwanted ones. You can also modify a policy, which will automatically update the firewalls on all servers in the groups that the policy is assigned to.

- You can also set up an alerting capability that will notify you whenever an unauthorized change is made to a firewall on any of your protected servers.
View Your Firewall Dashboard

To view the high-level firewall status of all your servers at a glance, go to **Servers > Firewall Management** in the Halo Portal (or click the CloudPassage icon at the page top). The Firewall Management page of the Halo Dashboard appears.

From the server group list, select one of your groups or select **All Servers**. View the list of servers, optionally changing the sorting of the list by clicking a column heading.

For any server in the list, note its firewall status (active or not), and the name of the firewall policy (if any) that is assigned to that server's server group. Click the name of a firewall policy to view its details on the Edit Firewall page.

You also can perform several server actions from the **Actions** drop-down list. For details about those actions and about Daemon status, see the **Halo Operations Guide**.

View a Server's Firewall Status and Summary

For additional firewall information for a server, click the server's name in the table on the Firewall Management page of the Dashboard. The Server Firewall details page for that server appears.

The page includes information about when the firewall was installed and when it was last checked to verify that it had not been altered outside of Halo.

If you click the name of the server in the "breadcrumb" hierarchy at the top of the page (in the screen image above, it is **App-Dev**), the Server Summary page for that server appears.
The Firewall Management section of the Server Summary page includes the same information as the Server Firewall Details page—firewall status, time since installation, time since last check, and firewall policy name.

At the top of the Server Summary page, you can click the **View additional server details** link to see more server summary information. The firewall-related information on the Additional Server Details page includes firewall presence, status, and policy name.

The Server Summary page and Additional Server Details page are described more fully in the *Halo Operations Guide*.

### Update Firewall Policies

Making changes to your firewall policies is simple, and updating all of your servers' firewalls with those changes is completely automatic.

1. In the Halo Portal, go to **Policies > Firewall Policies** and click the name of the policy that you want to change. That policy's Edit Policy page appears.

2. Activate or de-activate rules, re-arrange rules, add or delete rules, or change rule attributes as you need to, just as described in *Create and Assign a Firewall Policy* and in *Troubleshooting Firewalls*. Change the logging settings for the policy (Windows) or for individual rules (Linux). You can even change the policy's name or description.

3. Add, clone, or delete entire policies, if you wish. If you attempt to delete a policy that is assigned to a server group, you must first accept a confirmation dialog stating that the group's servers will be left without an assigned firewall.

4. You can also change the server-group assignment of a firewall policy, if needed. (You accomplish that by editing the affected server group details, not by editing the firewall policy.)

Whatever changes you make, within a few minutes of when you save them Halo will transmit the updates to all servers in all affected server groups. Also, any server that comes online subsequently in any of those groups will receive the group's latest updated firewall.

### Set Up Firewall Events and Alerts

You can configure Halo to send you or other users an email alert notification whenever any of your protected servers' firewalls are modified outside of Halo. By enabling this feature, you can have immediate knowledge of any potentially
malicious alterations to your server firewalls.

1. Create and assign an alert profile

Halo uses alert profiles assigned to a server group to determine who should receive alerts from that group. You create profiles in the Portal and then you assign them to groups.

Note: You do not have to perform this step if you are a Halo registered user and you want alerts to go only to you. Halo automatically creates a default alert profile for every registered user and assigns it by default to every server group. Complete this step if you want to send alerts to a different email address or to multiple users.

1. In the Halo Portal, go to Policies > Alert Profiles and click Add New Alert Profile.

2. Enter a name and optional description for the profile, specify "Instant" or some other value for the frequency, and then select one or more of your company's Halo users to receive alerts. Also specify whether each user should receive all alerts or just a subset based on event criticality. Then click Save.

3. Now assign the profile to a server group: on the Halo Dashboard page, click the name of the server group you want to assign the profile to, then click Edit Details below the name. On the Edit Group Details page, select the name of your alert profile from the Alert Profiles drop-down list. Then click Save.

Your designated users will receive an email when a security event that fits your settings occurs.

2. Create and assign a special-events policy

1. In the Halo Portal, go to Policies > Special Events Policies and click Add New Special Events Policy.

2. Enter a name and optional description for the policy. Then select, from the available set of security events, the specific events that you want this policy to monitor. For firewall alerting, select the Server firewall modified event and flag it as Critical and Generate an alert.

3. Click Save to save the policy. Then assign it to your server group: go the Portal Dashboard page, click Edit Details for your server group, and select your policy from the Special Events Policy drop-down list. Then click Save.

Security-event logging and alerting for firewall modifications are now set up for your server group.

3. Respond to a "firewall changed" alert.

If a modification to one of your protected servers' firewalls occurs, you can find out about it in either of these ways:

- Go to your email inbox. A notification from CloudPassage should be there, describing the firewall-change event.
- In the Halo Portal, go to Servers > Security Events History, set the Event type filter to "Server firewall modified", and click Filter. A description of the event should appear on the page.

For more information about security events, alerts, special-events policies, and the Security Events History page, see the "Issues and Events" section of the Halo Operations Guide.
Troubleshooting Firewalls

In a firewall, individual rules can be complex, their execution can be dependent on their relationship with other rules in the firewall, and the result of their execution can sometimes be the opposite of their intended purpose.

You may notice symptoms such as complete blocking of inward or outward communication, or unwanted blocking or acceptance of communication with a given source or service. To correct the problem, examine your firewall policy on the Edit Policy page in the Portal. It is most often a situation in which the logic of rule execution doesn't exactly match the logic of your conceptual design for the firewall.

If you have noticed any of the following problems, try its suggested remediation technique:

- **All outward communication blocked**. If you had wanted to allow all outward communication and so created no outbound rules at all in your policy, you may still have inadvertently created the outbound default-block rule recommended on the Edit Firewall Policy page. That would effectively block all outward connections.
  
  **Remediation:** Remove the default outbound rule (Linux) or select "Allow outbound traffic not specified above" (Windows).

- **All inward communication blocked**. If you had wanted to allow all inward communication and so created no inbound rules at all in your policy, you may still have inadvertently created the inbound default-block rule recommended on the Edit Firewall Policy page. That would effectively block all inward connections.
  
  **Remediation:** Remove the default inbound rule (Linux) or select "Allow inbound traffic not specified above" (Windows).

- **Cannot access DNS server**. If you are running a DNS server in the cloud, there needs to be an outbound rule accepting UDP traffic to port 53 on the DNS server.
  
  **Remediation:** Add the needed outbound rule to your firewall policy.

- **Cannot auto-update system software**. If the servers in the group need be able to initiate system software updates, there needs to be an outbound rule accepting HTTP/HTTPS traffic to the proper IP address for obtaining those updates.
  
  **Remediation:** Add the needed outbound rule to your firewall policy.

- **GhostPorts-enabled admin cannot log into server**. In order for a GhostPorts-enabled user to access a server after authenticating into GhostPorts, there must be a firewall rule in a server group that gives that user access, the server that the user is accessing must be in that group, there must be no higher-priority rules that prohibit access to the port or server the user needs, the user must log in from the computer on which the user authenticated to GhostPorts, and it must happen within 4 hours of authenticating.
  
  **Remediation:** Ensure that all of the above conditions are met.

- **GhostPorts-enabled admin can log into server at any time from anywhere**. If a server administrator can access a GhostPorts-protected server without authenticating to GhostPorts, or from any machine, or at any time, the firewall rule establishing GhostPorts protection is either missing, or of lower priority than a rule that permits access from anywhere, or applies to a different server group, or has an error such as specifying the wrong protocol and port.
  
  **Remediation:** Add the rule, correct any errors in it, make sure it is not overruled by another rule, make sure it is assigned to the correct server group.
This section describes a simplified set of firewall policies for an enterprise web application. The application is implemented using a typical 3-tier architecture: a set of load balancers distributes incoming Internet connections among a bank of web servers, and the web servers read and write to a set of database servers. All servers in the cloud are running CloudPassage Halo.

As shown in the above diagram, the servers are organized into 3 server groups: "Load Balancers", "Web Servers", and "Database Servers". The basic connections between the servers are shown in the diagram, as well as the connections with the Internet, the server administrator, and a database analyst. Note these details about this example setup:

- Connections to the Halo grid (from the Halo Daemon running on each server) are indicated but not explicitly drawn and labeled, because you do not need to specify them when you create a policy.

- The server admin and the data analyst are both shown as GhostPorts users, meaning that there must be GhostPorts rules for them in the appropriate firewall policies.

- For simplicity, the diagram and the example firewall policies shown here omit other common kinds of connections that would need firewall rules, such as outbound HTTP connections from servers for downloading automatic software updates.

- The diagram and the example policies shown here do not include the automatic corollary rules that Halo creates. You do not have to specify corollary rules in your policies.

*Note:* These example firewalls do not include any outbound default-drop rules. For the purposes of Halo evaluation, it is safest to leave all outbound communication unrestricted to avoid cutting off any necessary server access. However, we do recommend that your production firewalls include default-drop outbound rules.

### Web Server Firewall Policy

These are the inbound and outbound firewall rules for the example "Web Servers" server group. Note that automatic
corollary rules and rules required for Daemon communication are in the policy but do not appear in the Portal UI because you do not have to create them. You can export the policy to view all of the rules in text format.

**Policy Rules**

<table>
<thead>
<tr>
<th>Interface (Linux only)</th>
<th>Source</th>
<th>Service</th>
<th>Conn. State(s) (Linux only)</th>
<th>Action</th>
<th>Log? (Linux only)</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth0</td>
<td>Load Balancers</td>
<td>http (tcp/80)</td>
<td>ESTABLISHED, NEW</td>
<td>ACCEPT</td>
<td>No</td>
</tr>
<tr>
<td>eth0</td>
<td>Load Balancers</td>
<td>https (tcp/443)</td>
<td>ESTABLISHED, NEW</td>
<td>ACCEPT</td>
<td>No</td>
</tr>
<tr>
<td>eth0</td>
<td>Derek Wong [GhostPorts user]</td>
<td>ssh (tcp/22)</td>
<td>ESTABLISHED, NEW</td>
<td>ACCEPT</td>
<td>Yes</td>
</tr>
<tr>
<td>any</td>
<td>any</td>
<td>any</td>
<td>ANY</td>
<td>Linux: REJECT Windows: DROP</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Outbound Rules**

<table>
<thead>
<tr>
<th>Interface (Linux only)</th>
<th>Destination</th>
<th>Service</th>
<th>Conn. State(s) (Linux only)</th>
<th>Action</th>
<th>Log? (Linux only)</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth0</td>
<td>Database Servers</td>
<td>mysql (tcp/3306)</td>
<td>ESTABLISHED, NEW</td>
<td>ACCEPT</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mssql (tcp/1433)</td>
<td>ESTABLISHED, NEW</td>
<td>ACCEPT</td>
<td>No</td>
</tr>
</tbody>
</table>

**Notes**

In summary, firewalls generated from this policy will do the following:

- Allow inbound connections on ports 80 and 443 from any of the load balancers (plus the return of packets to them, because of automatic corollary rules).
- Allow inbound SSH or RDP connections (and return packets) for a specific server administrator, if the admin has authenticated to GhostPorts.
- Reject all other inbound traffic with an ICMP response and with logging (on Linux), to respond to and record direct attempts to connect to their external IP addresses.
- Allow outbound packets to the group of database servers listening on port 3306 (and the return of packets from them).

**Web Servers Firewall rules on Edit Policy Page (Windows)**

**Load Balancers Firewall Policy**
These are the inbound and outbound firewall rules for the example "Load Balancers" server group. Note that automatic corollary rules and rules required for Daemon communication are in the policy but do not appear in the Portal UI because you do not have to create them. You can export the policy to view all of the rules in text format.

### Policy Rules

#### Inbound Rules

<table>
<thead>
<tr>
<th>Interface (Linux only)</th>
<th>Source</th>
<th>Service</th>
<th>Conn. State(s) (Linux only)</th>
<th>Action</th>
<th>Log? (Linux only)</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth0</td>
<td>any (0.0.0.0/0)</td>
<td>http (tcp/80)</td>
<td>ESTABLISHED, NEW</td>
<td>ACCEPT</td>
<td>No</td>
</tr>
<tr>
<td>eth0</td>
<td>any (0.0.0.0/0)</td>
<td>https (tcp/443)</td>
<td>ESTABLISHED, NEW</td>
<td>ACCEPT</td>
<td>No</td>
</tr>
<tr>
<td>eth0</td>
<td>Derek Wong</td>
<td>Linux: ssh (tcp/22)</td>
<td>ESTABLISHED, NEW</td>
<td>ACCEPT</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>[GhostPorts user]</td>
<td>Windows: RDP (tcp/3389)</td>
<td>ESTABLISHED, NEW</td>
<td>ACCEPT</td>
<td></td>
</tr>
<tr>
<td>any</td>
<td>any</td>
<td>any</td>
<td>ANY</td>
<td>DROP</td>
<td>No</td>
</tr>
</tbody>
</table>

#### Outbound Rules

<table>
<thead>
<tr>
<th>Interface</th>
<th>Source</th>
<th>Service</th>
<th>Conn. State(s)</th>
<th>Action</th>
<th>Log?</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth0</td>
<td>Web Servers</td>
<td>http (tcp/80)</td>
<td>ESTABLISHED, NEW</td>
<td>ACCEPT</td>
<td>No</td>
</tr>
<tr>
<td>eth0</td>
<td>Web Servers</td>
<td>https (tcp/443)</td>
<td>ESTABLISHED, NEW</td>
<td>ACCEPT</td>
<td>No</td>
</tr>
</tbody>
</table>

#### Notes

In summary, firewalls generated from this policy will do the following:

- Allow inbound connections on ports 80 and 443 from anywhere on the Internet. (plus the return of packets to senders, because of automatic corollary rules).
- Allow inbound SSH or RDP connections (and allow return packets) for a specific server administrator, if the admin has authenticated to GhostPorts.
- Drop all other inbound traffic without an ICMP response and without logging (on Linux), because the load balancers face the Internet and are subject to frequent port scans.
- Allow outbound connections to the group of web servers listening on ports 80 and 443 (and the return of packets from them).

### Load Balancers Firewall rules on Edit Policy Page (Linux)

![Inbound Rules (Add New)](image)

![Outbound Rules (Add New)](image)
These are the inbound and outbound firewall rules for the example "Database Servers" server group. Note that automatic corollary rules and rules required for Daemon communication are in the policy but do not appear in the Portal UI because you do not have to create them. You can export the policy to view all of the rules in text format.

### Policy Rules

#### Inbound Rules

<table>
<thead>
<tr>
<th>Interface (Linux only)</th>
<th>Source</th>
<th>Service</th>
<th>Conn. State(s) (Linux only)</th>
<th>Action</th>
<th>Log? (Linux only)</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth0</td>
<td>Web Servers</td>
<td>Linux: mysql (tcp/3306) Windows: mssql (tcp/1433)</td>
<td>ESTABLISHED, NEW</td>
<td>ACCEPT</td>
<td>No</td>
</tr>
<tr>
<td>eth0</td>
<td>Erica Westford [GhostPorts user]</td>
<td>Linux: mysql (tcp/3306) Windows: mssql (tcp/1433)</td>
<td>ESTABLISHED, NEW</td>
<td>ACCEPT</td>
<td>Yes</td>
</tr>
<tr>
<td>eth0</td>
<td>Derek Wong [GhostPorts user]</td>
<td>Linux: ssh (tcp/22) Windows: RDP (tcp/3389)</td>
<td>ESTABLISHED, NEW</td>
<td>ACCEPT</td>
<td>Yes</td>
</tr>
<tr>
<td>any</td>
<td>any</td>
<td>any</td>
<td>ANY</td>
<td>Linux: REJECT Windows: DROP</td>
<td>Yes</td>
</tr>
</tbody>
</table>

#### Outbound Rules (None created)

### Notes

In summary, firewalls generated from this policy will do the following:

- Allow inbound connections on port 3306 from any of the web servers (plus the return of packets to them, because of automatic corollary rules).
- Allow inbound SSH or RDP connections (and the return of packets) for a specific server administrator, if the admin has authenticated to GhostPorts.
- Allow inbound MYSQL or MSSQL connections on port 3306 from a specific database analyst (plus the return of packets to them, because of automatic corollary rules), if the analyst has authenticated to GhostPorts.
- Reject all other inbound traffic with an ICMP response and with logging (on Linux), to respond to and record direct attempts to connect to their external IP addresses.)

### Database Servers Firewall rules on Edit Policy Page (Linux)

[Database Servers Firewall rules on Edit Policy Page (Linux)](https://example.com)