CloudPassage

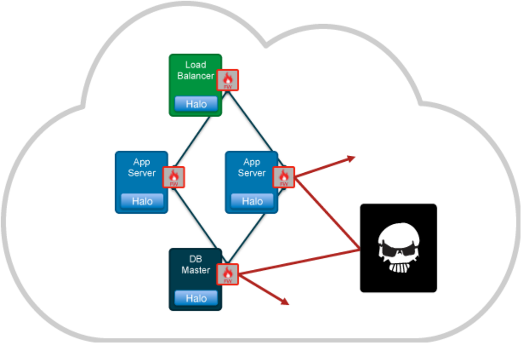
Workload Firewall Management

Setup Guide

Contents:

About Halo Workload Firewalls

CloudPassage Halo automatically deploys, updates, and monitors host-based Windows or Linux firewalls for your cloud server hosts. Host-based firewalls can provide more protection for your cloud servers or workloads than traditional perimeter firewalls, because they can be tailored to the exact purpose of each type of workload 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 workload firewalls also deploy themselves automatically and elastically, as your cloud-server population dynamically grows and shrinks. No hosts 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 workloads in the cloud, firewall implementation can involve tedious tracking of lists of host addresses. But with Halo these workloads 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 the Halo multi-factor network authentication feature, 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.

Implementing Halo Workload Firewalls

Start your Halo workload 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.

1. Create a Firewall Policy.

   To create a complete Firewall Policy, you must:

   a. Define firewall-related components. For information, see Define Firewall-Related Components, below.

   b. Create inbound rules. For information, see Create Inbound Rules, below.

   c. Create outbound rules. For information, see Create Outbound Rules, below.

2. Assign the Firewall Policy to a server group.

   For information, in the *Halo Operations Guide* see Assign Policies to a Group.

3. Set up firewall events and alerts.

   For information about configuring firewall events and alerts, see Setting Up Firewall Events and Alerts, below.

4. Address Firewall issues and events.

   To view information about unauthorized modifications to any of your servers' local firewalls, view firewall issues or events.

   - To view firewall issues, start with the Issues view on the Environment screen. In the *Halo Operations Guide*, see Viewing Issues.

     Click a firewall issue's name to view the Issue Details Sidebar. For information see View Firewall Issue Details, below.

- To view firewall events, start with the Security Events History page. In the *Halo Operations Guide*, see View the Security Events History.

  Search for a firewall event and view its details. For information see View Firewall Events, below.

For general information about Halo events and alerts, In the *Halo Operations Guide* see Setting Up Logging and Alerting.

Creating Firewall Policies

A firewall policy is a set of rules applied to a server that 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 Appendix: Example Firewall for Multi-Server 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.

Define Firewall-Related Components

This section gives additional information or instructions that helps 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).

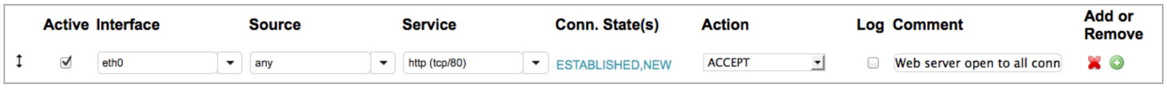
  Note that in order to REJECT a packet, a RELATED entry must exist in the iptables firewall for the ICMP response. In this case also, the Halo Firewall does this for you automatically; you do not need to worry about creating any outbound rules allowing ICMP when you select one or more services to REJECT.

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

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:



	Active	Interface	Source	Service	Conn. State(s)	Action	Log	Comment	Add or Remove
↕	☑	eth0	any	http (tcp/80)	ESTABLISHED,NEW	ACCEPT	☐	Web server open to all conn	✖ ⊕

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.

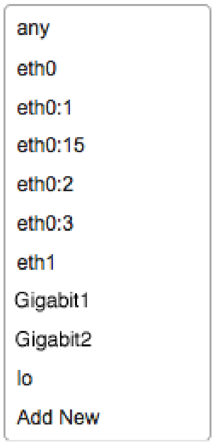
Automatic corollary rules do not appear on the Halo portal page that you use to create and edit firewall policies, but you can see them if you export a firewall policy.

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:

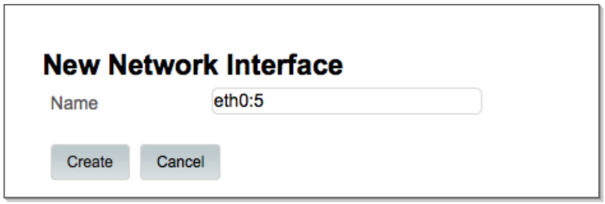


any
eth0
eth0:1
eth0:15
eth0:2
eth0:3
eth1
Gigabit1
Gigabit2
lo
Add New

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

Name: eth0:5

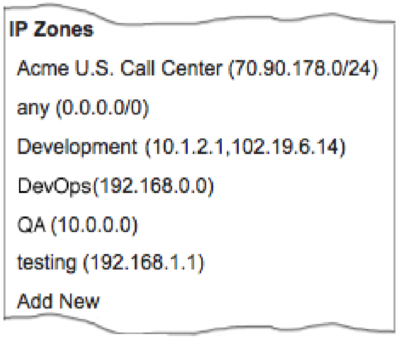
2. Enter the name of your custom interface device and click Create.

The interface will now appear in the Network Interfaces list and in the Interface drop-down list when you create a Linux firewall rule.

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 other installations, your suppliers and partners, and so on. Here is an example set of IP zones in a Source or Destination list:



IP Zones

Acme U.S. Call Center (70.90.178.0/24)

any (0.0.0.0/0)

Development (10.1.2.1,102.19.6.14)

DevOps(192.168.0.0)

QA (10.0.0.0)

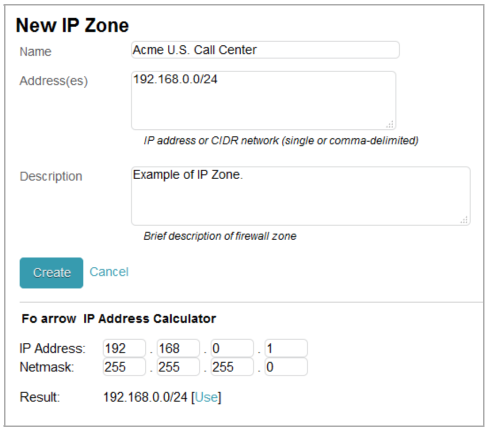
testing (192.168.1.1)

Add New

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

   Name: Acme U.S. Call Center

   Address(es): 192.168.0.0/24

   IP address or CIDR network (single or comma-delimited)

   Description: Example of IP Zone.

   Brief description of firewall zone

   Create Cancel

   Fo arrow IP Address Calculator

   IP Address: 192 . 168 . 0 . 1

   Netmask: 255 . 255 . 255 . 0

   Result: 192.168.0.0/24 [Use]

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

   Use the New IP Zone page's IP Address Calculator to calculate the new zone's IP Address and Netmask.

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

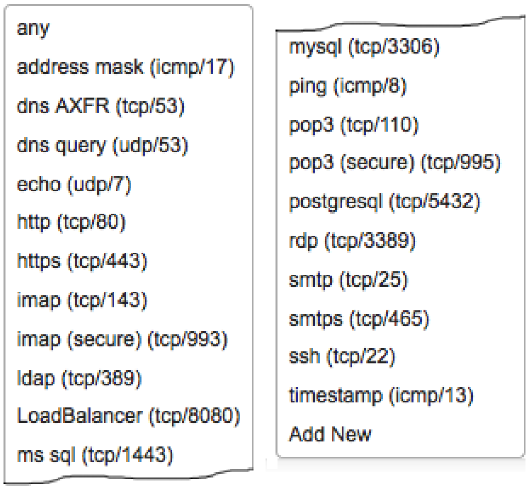
The IP zone will now appear in the IP Zones list and in the Source and Destination drop-down lists in a firewall rule.

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:

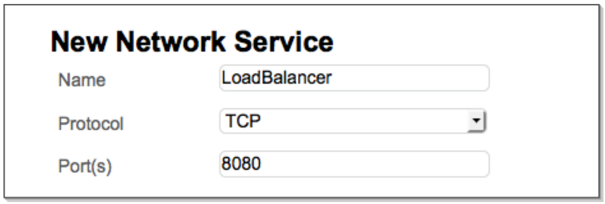


any
address mask (icmp/17)
dns AXFR (tcp/53)
dns query (udp/53)
echo (udp/7)
http (tcp/80)
https (tcp/443)
imap (tcp/143)
imap (secure) (tcp/993)
ldap (tcp/389)
LoadBalancer (tcp/8080)
ms sql (tcp/1443)
mysql (tcp/3306)
ping (icmp/8)
pop3 (tcp/110)
pop3 (secure) (tcp/995)
postgresql (tcp/5432)
rdp (tcp/3389)
smtp (tcp/25)
smtps (tcp/465)
ssh (tcp/22)
timestamp (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.)

   New Network Service

   Name: LoadBalancer
   Protocol: TCP
   Port(s): 8080

   Here, the service named "LoadBalancer" has been defined as the TCP protocol over port 8080.

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.

Create Inbound Rules

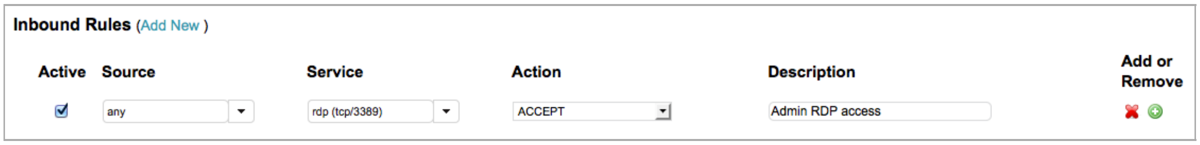
Each inbound rule describes the specifics of one kind of connection from the outside into the server. To create a new rule, click Add New or the Add Rule icon (⊕) beside any existing inbound rule.

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

Rule Attribute	Description
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 the Multi-Factor Network Authentication Setup Guide.

Service	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.
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)*	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.
Log prefix *(Linux only)*	Optionally enter a text string that will uniquely identify matches to this rule in the firewall logs. One use case for this feature is to allow Log-Based Intrusion Detection to easily identify important firewall events when it scans the firewall log. The string may be up to 29 characters long, and it may contain spaces or special characters. For more information, see the *Log-Based Intrusion Detection Setup Guide*.
Description or Comment	Optionally enter a description for this rule. A comment or description can be useful for explaining the purpose of the rule, especially to security auditors. *Note*: For Linux firewalls, the set of acceptable characters for the Comment field includes letters, numbers, and spaces, plus comma, #, @, :, /, and single and double quotes. Windows firewalls accept only letters, numbers, spaces, periods, and underscores in the Description field.

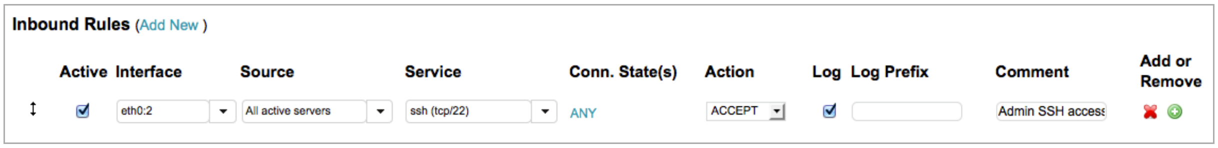
Windows Firewall Rule



Inbound Rules (Add New)

Active	Source	Service	Action	Description	Add or Remove
☑	any	rdp (tcp/3389)	ACCEPT	Admin RDP access	✖ ⊕

Linux Firewall Rule



Inbound Rules (Add New)

	Active	Interface	Source	Service	Conn. State(s)	Action	Log	Log Prefix	Comment	Add or Remove
↕	☑	eth0:2	All active servers	ssh (tcp/22)	ANY	ACCEPT	☑		Admin SSH access	✖ ⊕

End firewall policies with a default rule to apply to any inbound connection attempt that is not described by any of the other inbound rules. Normally, this 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 (⊕) 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 deactivate rules

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

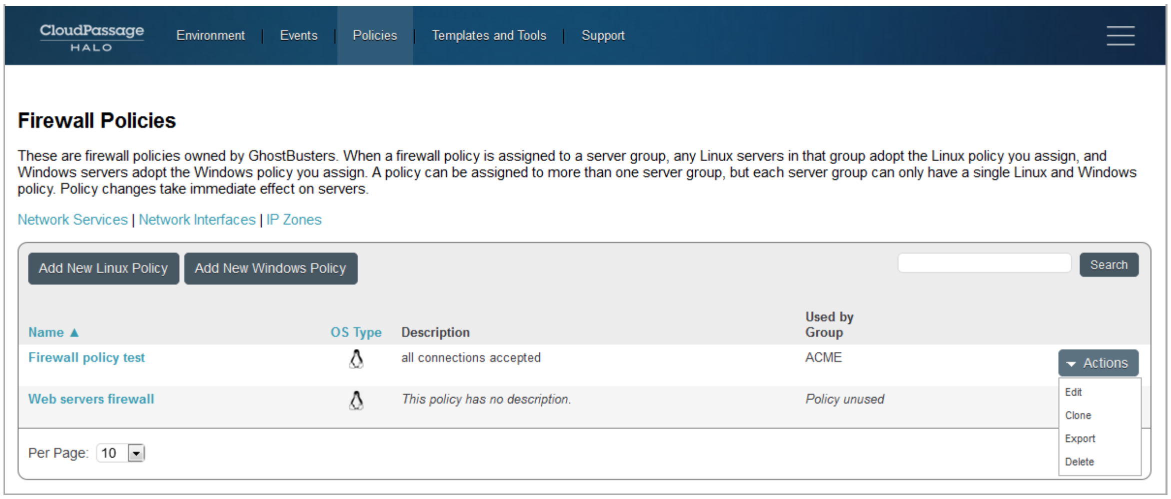
- Use the up-down drag-and-drop arrows to change the ordering of the rules. In use, the firewall's inbound or outbound rules are tested in order from the top, and testing stops as soon as one rule's criteria are met. Make sure the ordering of the rules gives you the results you want, and make sure your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

Managing Firewall Policies

As your security requirements grow and change, you will also want to use Halo's policy management options to manage the policies that are or are not included in the list of active policies.

This section describes Halo's policy actions. To perform most of the following actions, you choose an active policy, policy template, or retired policy from a list and click its Action button. Then you select an action from the drop-down list.



Firewall Policies

These are firewall policies owned by GhostBusters. When a firewall policy is assigned to a server group, any Linux servers in that group adopt the Linux policy you assign, and Windows servers adopt the Windows policy you assign. A policy can be assigned to more than one server group, but each server group can only have a single Linux and Windows policy. Policy changes take immediate effect on servers.

Name ▲	OS Type	Description	Used by Group
Firewall policy test	🐧	all connections accepted	ACME
Web servers firewall	🐧	*This policy has no description.*	*Policy unused*

Policy Manipulation Actions:

Export a Policy

To export a policy from Halo, select "Export" from the Actions dropdown list.

Halo saves the policy's settings as a JSON-formatted file. You can securely archive the policy file, share the policy with other Halo users, or re-import it at a later time.

Delete a Policy

To delete a policy, select "Delete" from the Actions dropdown list, then in the confirmation dialog click OK.

Halo permanently removes the policy. It no longer appears in the Active Policies page and cannot be retrieved.

Note: The only way you can recover a deleted policy is to have exported it first, so that you can re-import the exported file.

Policy Creation and Editing Actions:

Clone a Policy or Template

To clone a policy or policy template, select "Clone" from the Actions dropdown list..

Halo creates a copy of the policy, adds the word *Copy* to the policy's name, and places it in the Active Policies list. You often can use the cloned template as-is, or you may wish to use it as the starting point for a custom policy. In that case, create a unique name and description for the new policy, then customize its rules.

Note that Halo will not permit you to save a cloned policy if it does not have a unique name.

Create a New Policy

To create a new policy, click the Add New Policy button above the policy list.

On the new Policy page, Create a unique name and description for the policy. Initially, the policy is empty; add rules as desired.

Halo will not permit you to save a new policy until you assign the policy a unique name.

Edit a Policy

To edit an active policy, select "Edit" from the Actions dropdown list..

The Edit Policy page opens, on which you can change the policy's name, description, and rules. When you save it, the updated policy appears on the Active policies page.

Setting Up Firewall Events and Alerts

Configure Halo to send you or other users an email alert notification whenever any of your protected servers' firewalls are modified outside of Halo.

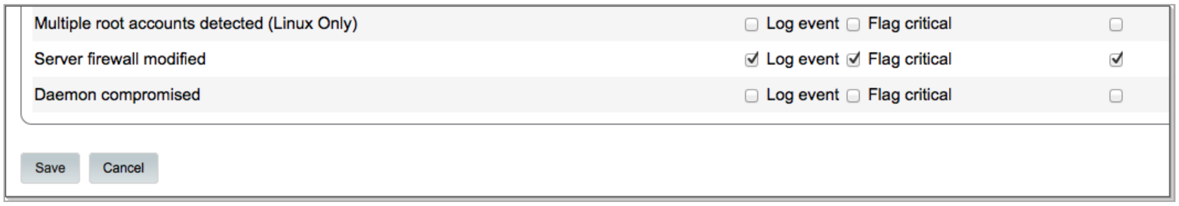
1. Create and assign an alert profile.

   Configure Halo to send you or other users an email alert notification whenever any of your protected servers' firewalls are modified outside of Halo.

   For information, in the *Halo Operations Guide*, see Working With Alerts.

2. Create and assign a special-events policy.

   For firewall alerting, select the Server firewall modified event, then configure it as Critical and to Generate an alert.



Multiple root accounts detected (Linux Only)	□ Log event □ Flag critical	□
Server firewall modified	☑ Log event ☑ Flag critical	☑
Daemon compromised	□ Log event □ Flag critical	□

   For information about special events policies, in the *Halo Operations Guide*, see Create a Special Events Policy.

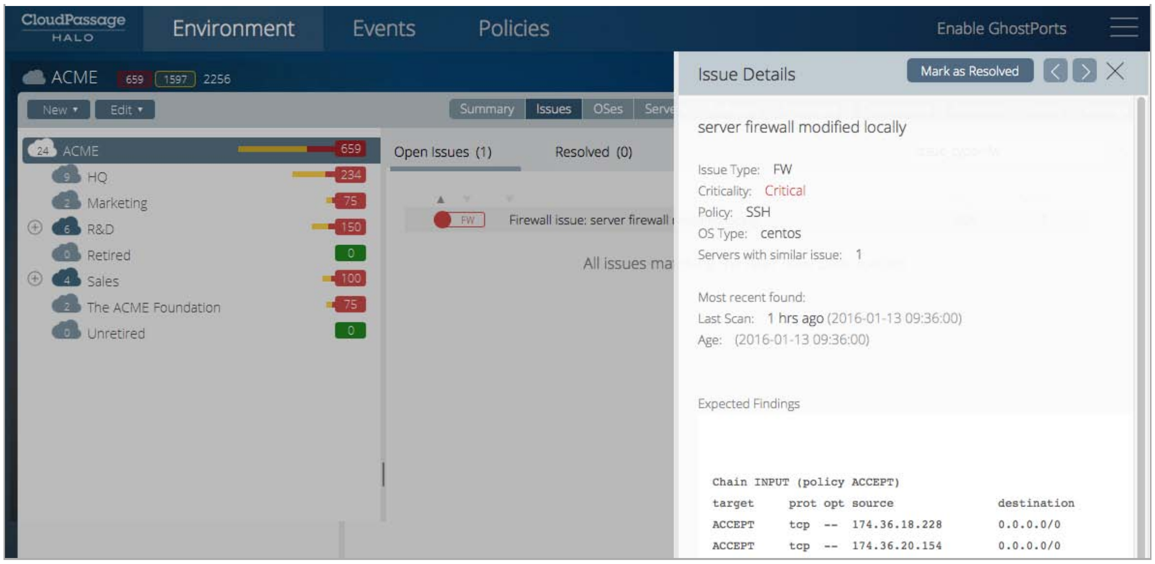
For information about responding to firewall events, see Addressing Firewall Issues and Events, below.

Addressing Firewall Issues and Events

To accurately assess the level of risk associated with a given firewall event, you need to examine the event's details.

View Firewall Issue Details

In the list of issues, click a firewall issue's description to view the Issue Details sidebar.



server firewall modified locally

Issue Type: FW
Criticality: Critical
Policy: SSH
OS Type: centos
Servers with similar issue: 1

Most recent found:
Last Scan: 1 hrs ago (2016-01-13 09:36:00)
Age: (2016-01-13 09:36:00)

Expected Findings

```
Chain INPUT (policy ACCEPT)
target     prot opt source              destination
ACCEPT     tcp  --  174.36.18.228       0.0.0.0/0
ACCEPT     tcp  --  174.36.20.154       0.0.0.0/0
```

In the firewall issues sidebar, scroll down to view the following sections:

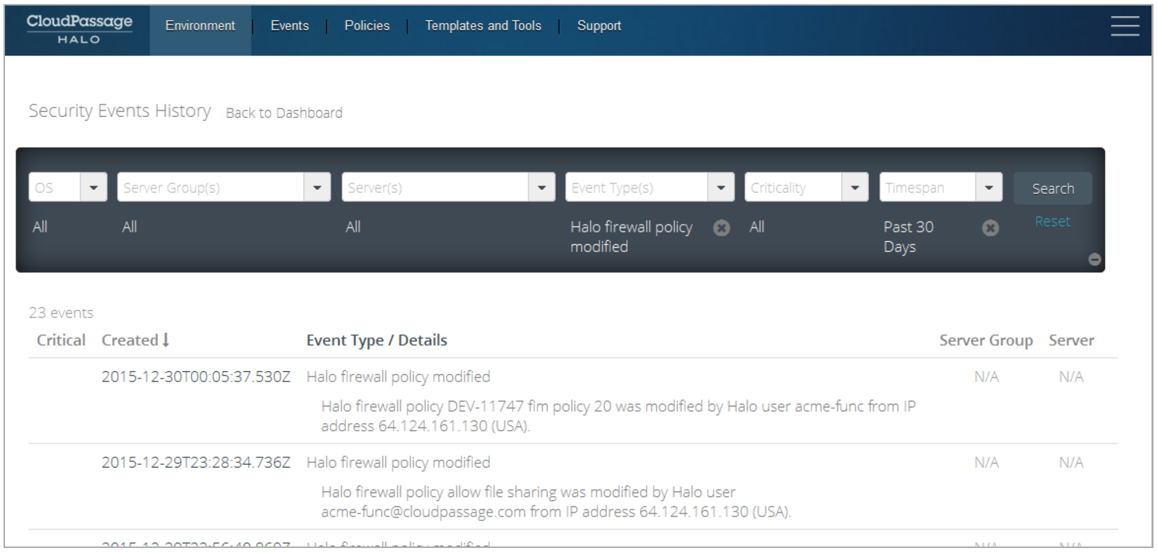
- The Expected Findings section lists the rules specified by the firewall policy.
- The Actual Findings section lists any discrepancies between the firewall rules specified by the policy versus the configuration of the firewall at the time the scan was performed.

  See Act on Firewall Issues, below.

View Firewall Events

If you have not already done so, you must first configure Firewall events. For information see Setting Up Firewall Events and Alerts, above.

To view firewall-modified events, in the Event Types list choose "Halo firewall policy modified" then click Search.



OS	Server Group(s)	Server(s)	Event Type(s)	Criticality	Timespan
All	All	All	Halo firewall policy modified	All	Past 30 Days

23 events

Critical	Created ↓	Event Type / Details	Server Group	Server
	2015-12-30T00:05:37.530Z	Halo firewall policy modified Halo firewall policy DEV-11747 fim policy 20 was modified by Halo user acme-func from IP address 64.124.161.130 (USA).	N/A	N/A
	2015-12-29T23:28:34.736Z	Halo firewall policy modified Halo firewall policy allow file sharing was modified by Halo user acme-func@cloudpassage.com from IP address 64.124.161.130 (USA).	N/A	N/A
	2015-12-29T23:56:49.969Z	Halo firewall policy modified	N/A	N/A

By default, Halo lists the log-based intrusion detection events captured in the past 24 hours. For information about Events History options, in the *Halo Operations Guide*, see View the Security Events History.

For each displayed event, the page indicates the event's criticality, lists its date-time of occurrence, which firewall policy was modified, and the affected server and server group.

To respond to a firewall issue, see Act On Firewall Issues, below.

Act on Firewall Issues

An event type of "Server firewall modified" indicates that an individual server's firewall has been changed outside of Halo. If you approve of the change, either re-assign the firewall policy to the server group to restore the proper firewall, or modify the group's firewall policy to make it consistent with the server's new state. If the change was not approved or known of by anyone in your organization, start an investigation.

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 examine your firewall policy by selecting it from the Firewall Policies page. 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.

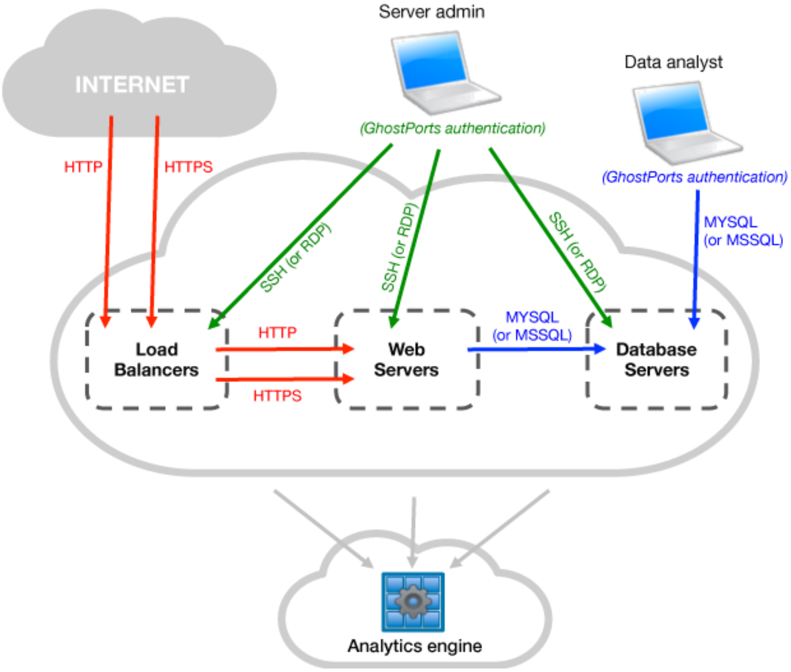
If you have noticed any of the following problems, try its suggested remediation technique:

Problem	Possible solution
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	To enable a GhostPorts-enabled user to access a server after authenticating into GhostPorts, requires that: • A firewall rule in a server group gives that user access • The server that the user is accessing must be in that group and • there must be no higher-priority rules that prohibit access to the port or server the user needs.

	The user log in from the computer on which the user authenticated to GhostPorts - Log in must occur within 4 hours of authenticating *Remediation:* Ensure 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 in any of the following ways: - Without authenticating to GhostPorts - From any machine - At any time THEN the firewall rule establishing GhostPorts protection contains one or more of the following: - Missing - Of lower priority than a rule that permits access from anywhere - Applies to a different server group - Specifies the wrong protocol or 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.

Appendix: Example Firewall for Multi-Server Web App

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 three 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 analytics engine (from the Halo agent 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 agent 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					
Interface ***(Linux only)***	Source	Service	Conn. State(s) ***(Linux only)***	Action	Log? ***(Linux only)***
eth0	Load Balancers	http (tcp/80)	ESTABLISHED, NEW	ACCEPT	No
eth0	Load Balancers	https (tcp/443)	ESTABLISHED, NEW	ACCEPT	No
eth0	Derek Wong *[GhostPorts user]*	***Linux:*** ssh (tcp/22) ***Windows:*** RDP (tcp/3389)	ESTABLISHED, NEW	ACCEPT	Yes
any	any	any	ANY	***Linux:*** REJECT ***Windows:*** DROP	Yes
Outbound Rules					
eth0	Database Servers	***Linux:*** mysql (tcp/3306) ***Windows:*** mssql (tcp/1433)	ESTABLISHED, NEW	ACCEPT	No

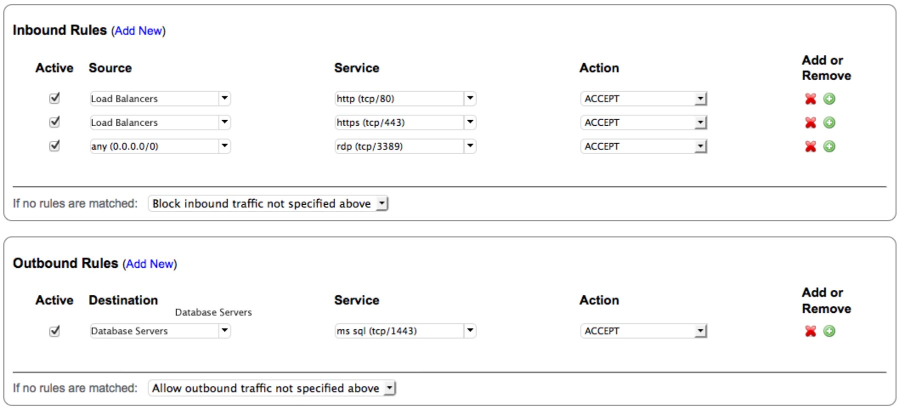
Notes

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)



Inbound Rules (Add New)

Active	Source	Service	Action	Add or Remove
☑	Load Balancers	http (tcp/80)	ACCEPT	✖ ⊕
☑	Load Balancers	https (tcp/443)	ACCEPT	✖ ⊕
☑	any (0.0.0.0/0)	rdp (tcp/3389)	ACCEPT	✖ ⊕

If no rules are matched: Block inbound traffic not specified above

Outbound Rules (Add New)

Active	Destination	Service	Action	Add or Remove
	Database Servers			
☑	Database Servers	ms sql (tcp/1443)	ACCEPT	✖ ⊕

If no rules are matched: Allow outbound traffic not specified above

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 agent 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

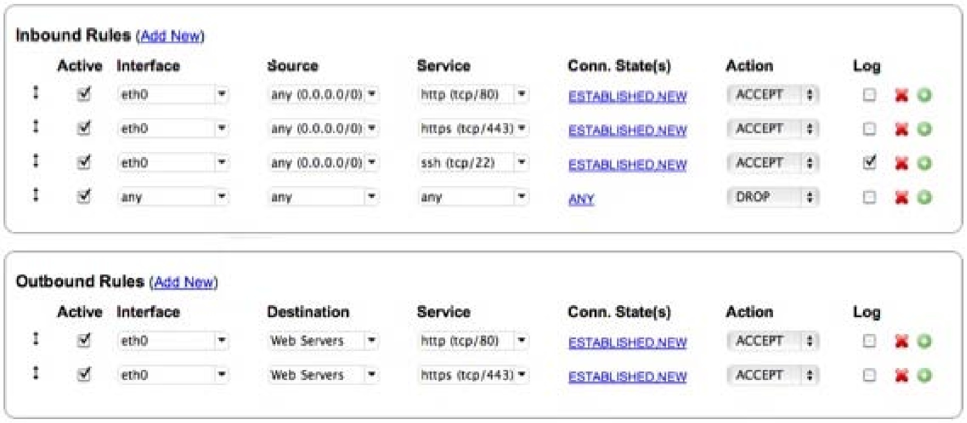
Inbound Rules					
Interface ***(Linux only)***	Source	Service	Conn. State(s) ***(Linux only)***	Action	Log? ***(Linux only)***
eth0	any (0.0.0.0/0)	http (tcp/80)	ESTABLISHED, NEW	ACCEPT	No
eth0	any (0.0.0.0/0)	https (tcp/443)	ESTABLISHED, NEW	ACCEPT	No
eth0	Derek Wong *[GhostPorts user]*	***Linux:*** ssh (tcp/22) ***Windows:*** RDP (tcp/3389)	ESTABLISHED, NEW	ACCEPT	Yes
any	any	any	ANY	DROP	No
Outbound Rules					
eth0	Web Servers	http (tcp/80)	ESTABLISHED, NEW	ACCEPT	No
eth0	Web Servers	https (tcp/443)	ESTABLISHED, NEW	ACCEPT	No

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)

	Active	Interface	Source	Service	Conn. State(s)	Action	Log	
↕	☑	eth0	any (0.0.0.0/0)	http (tcp/80)	ESTABLISHED,NEW	ACCEPT	□	✖ ⊕
↕	☑	eth0	any (0.0.0.0/0)	https (tcp/443)	ESTABLISHED,NEW	ACCEPT	□	✖ ⊕
↕	☑	eth0	any (0.0.0.0/0)	ssh (tcp/22)	ESTABLISHED,NEW	ACCEPT	☑	✖ ⊕
↕	☑	any	any	any	ANY	DROP	□	✖ ⊕

Outbound Rules (Add New)

	Active	Interface	Destination	Service	Conn. State(s)	Action	Log	
↕	☑	eth0	Web Servers	http (tcp/80)	ESTABLISHED,NEW	ACCEPT	□	✖ ⊕
↕	☑	eth0	Web Servers	https (tcp/443)	ESTABLISHED,NEW	ACCEPT	□	✖ ⊕

Database Server Firewall Policy

These are the inbound and outbound firewall rules for the example "Database Servers" server group. Note that automatic corollary rules and rules required for agent 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					
Interface ***(Linux only)***	Source	Service	Conn. State(s) ***(Linux only)***	Action	Log? ***(Linux only)***
eth0	Web Servers	***Linux:*** mysql (tcp/3306) ***Windows:*** mssql (tcp/1433)	ESTABLISHED, NEW	ACCEPT	No
eth0	Erica Westford *[GhostPorts user]*	***Linux:*** mysql (tcp/3306) ***Windows:*** mssql (tcp/1433)	ESTABLISHED, NEW	ACCEPT	Yes
eth0	Derek Wong *[GhostPorts user]*	*Linux:* ssh (tcp/22) ***Windows:*** RDP (tcp/3389)	ESTABLISHED, NEW	ACCEPT	Yes
any	any	any	ANY	***Linux:*** REJECT ***Windows:***DROP	Yes
Outbound Rules ***(None created)***					

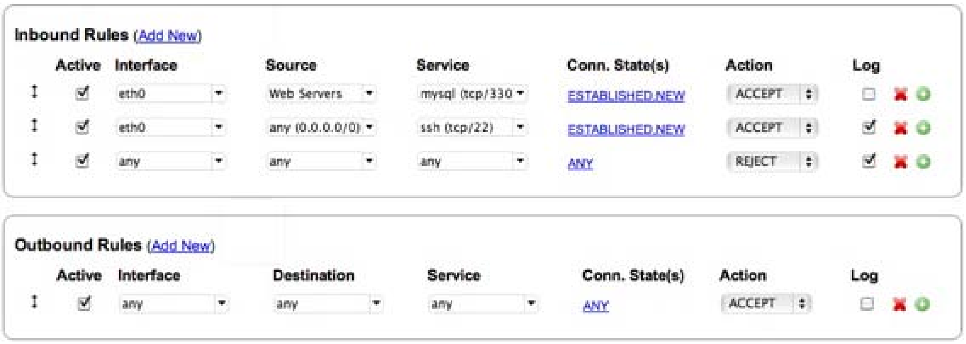
Notes

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)



Inbound Rules (Add New)

	Active	Interface	Source	Service	Conn. State(s)	Action	Log		
↕	☑	eth0	Web Servers	mysql (tcp/330	ESTABLISHED,NEW	ACCEPT	□	✖	⊕
↕	☑	eth0	any (0.0.0.0/0)	ssh (tcp/22)	ESTABLISHED,NEW	ACCEPT	☑	✖	⊕
↕	☑	any	any	any	ANY	REJECT	☑	✖	⊕

Outbound Rules (Add New)

	Active	Interface	Destination	Service	Conn. State(s)	Action	Log		
↕	☑	any	any	any	ANY	ACCEPT	□	✖	⊕