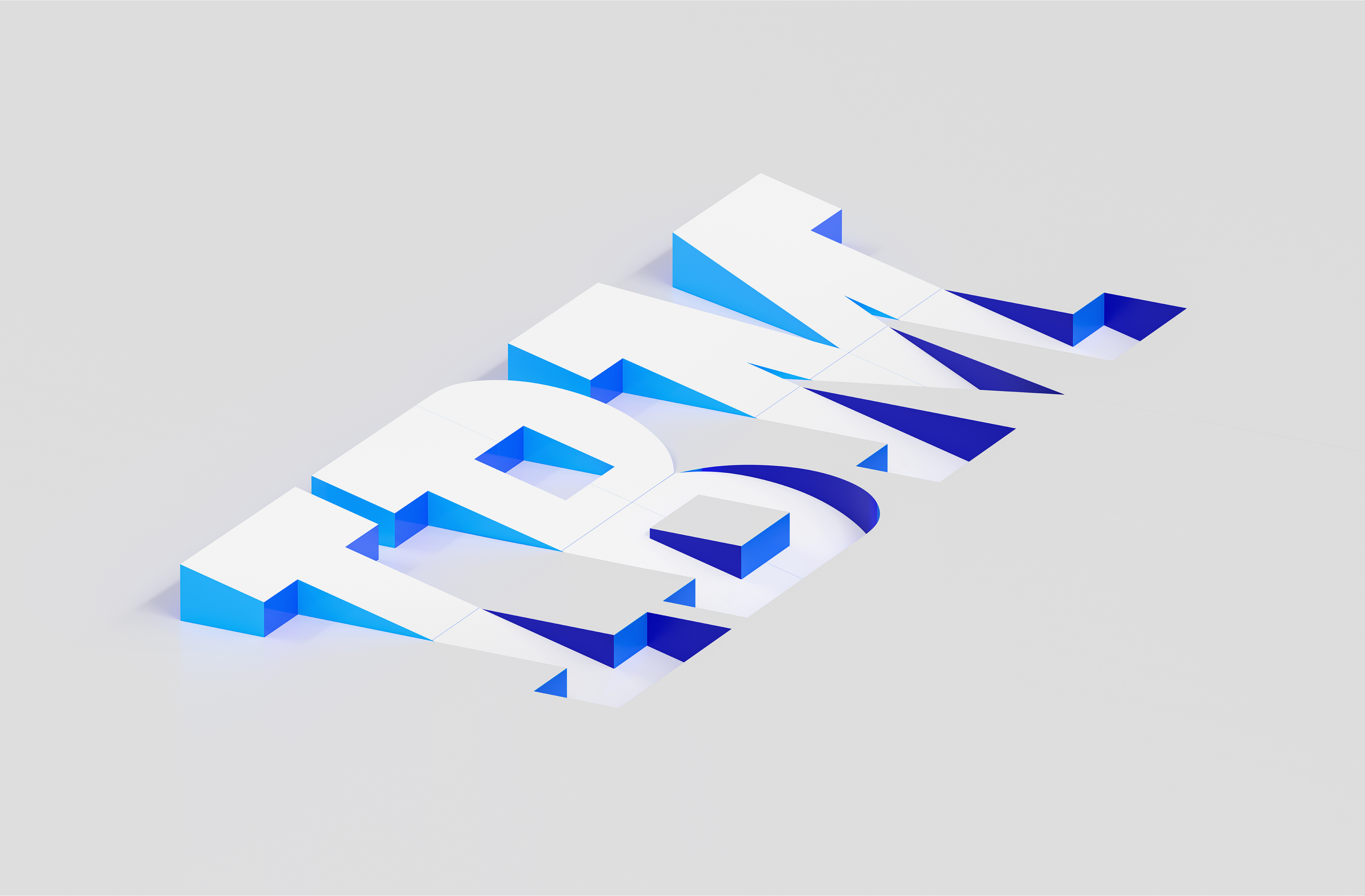
IBM Cloud

Hardware Firewall

Product guide



Edition notices

This PDF was created on 2024-10-15 as a supplement to *Hardware Firewall* in the IBM Cloud docs. It might not be a complete set of information or the latest version. For the latest information, see the IBM Cloud documentation at https://cloud.ibm.com/docs/hardware-firewall-shared.

Getting started with Hardware Firewall

The Hardware Firewall provides customers with an essential layer of security that is provisioned on demand without service interruptions. It prevents unwanted traffic from hitting your servers, reducing your attack surface, and allowing your server resources to be dedicated for their intended use.

To add a firewall to a server, perform the following procedure:

1. From your browser, open the IBM Cloud catalog and log in to your account.
2. Select the Menu icon ☰ from the upper left, then click **Classic Infrastructure**.
3. Select **Devices > Device List** and click the server that you want protected.
4. In the **Device Details** page, in the **Configuration** tab, scroll to the end of the page to the **Addons** section and click the **Order Hardware Firewall** link.
5. In the **Order Hardware Firewall** dialog, choose from the options presented (if applicable) and press **Continue** to complete the ordering process. The firewall speed defaults to the speed of the public network interface of your server.

About Hardware Firewall

A Hardware Firewall is a network device that is connected upstream from a server. The firewall blocks unwanted traffic from a server before the traffic ever reaches the server. The main advantage to having a Hardware Firewall is that a server handles only 'good' traffic and no resources are wasted dealing with the 'bad' traffic.

The Hardware Firewall uses a multi-tenant enterprise platform to protect an individual server. It can be purchased with the server or added on later. It delivers virtualized network security through its Virtual Domain (VDOM) technology, providing virtualized security domains that are separately provisioned and managed.

Because multiple customers are associated with the hardware, if the firewall fails or is overwhelmed by an attack, every customer that shares a Hardware Firewall instance might be impacted.

Up to 79 firewall rules can be configured for the primary and statically routed IP addresses assigned to the server. Reports for Firewalls are available based on the activity of a single IP for a selected date range. Customers can manage the firewall through two ways: the IBM Cloud console (the firewall tab under the protected server details page) and SLDN APIs.

Since monthly server bandwidth is recorded at the server switch port, traffic that is blocked by the Hardware Firewall is not counted against your monthly allotments, eliminating the need to pay for unwanted traffic.

Overview and features

Intended Use: Single-Server Primary Public IP Protection

User Interface: Integrated into IBM Cloud console and APIs

Features: Stateful Packet Inspection, Ingress Firewall Rules, IPv4, IPv6, Basic Logging

Server Network Interface Speeds:* 100 Mbps, 200 Mbps, 1000 Mbps, and 2000 Mbps

It is required that the throughput of a Hardware Firewall instance match the uplink speed of the server the firewall is being added to.

Exploring firewalls

IBM Cloud® offers several firewalls to choose from. The following table compares the firewall solutions to help you choose the one that's right for you. To learn more about the individual offering, click its name in the table.

⚠ **Important:** These offerings are not managed services. When using them, you should understand the shared responsibilities between the client (or their managed services provider) and IBM. For more information, refer to Roles and responsibilities for IBM Cloud gateways and firewalls .

	Security Groups **(VSI only)**	IBM Cloud Juniper vSRX Standard	Virtual Router Appliance	FortiGate Security Appliance 10 Gbps	Hardware Firewall	Cloud Internet Services	Virtual FortiGate Security Appliance
Stateful Packet Inspection	□	□	□	□	□	IP firewall only	□
Public Network Protection	□	□	□	□	□	□	□
Private Network Protection	□	□	□	□			□
Ingress Rules	□	□	□	□	□	IP Firewall only	□
Egress Rules	□	□	□	□			□
Single Tenant Appliance		□	□	□	□		□
VLAN Protection		□	□	□	□		□
Multi-VLAN Support		□	□	□			□
NAT Support		□	□	□			□
SSL/IPsec VPN Termination		□	□	□	□		□
Open VPN Termination			□			Only with single port on TCP/UDP	□
HA Option	N/A	□	□	□	Using range and load balancers	□	□
Manage from API & Portal	Yes	Appliance GUI	Appliance GUI	Appliance GUI	Yes	Cloud console	Appliance GUI

10 Gbps Support	N/A	□	□			□	□
NGFW Add-ons (IPS, AV, WF)		□		□		TLS encryption, IP Firewall rules, and Proxy Protocol v1	□
Remote Access VPN		□					□

Table 1: A comparison of IBM's firewall offerings

Roles and responsibilities for IBM Cloud gateways and firewalls

Overview of shared responsibilities

IBM Cloud provides several Gateway Appliances and firewall offerings. These offerings are not managed services. As a result, it's important when using these services that you understand the shared responsibilities between the client (or their managed services provider) and IBM. The following sections detail these responsibilities using the following guidelines.

Responsible (R)

Has the duty and the obligation to do the work. Also, has a duty to exercise independent judgement to raise appropriate issues.

Accountable (A)

Has the authority to decide, and is the recipient of, any consequences (there can only be one "A" per process step).

Consulted (C)

Must be given the opportunity to influence plans and decisions prior to finalization by the "Responsible" party.

Informed (I)

Is informed of progress, key decisions, and deliverables by the "Responsible" party.

Order (O)

Has the ability to place an order.

Monitoring

The client (or their managed services provider) is responsible for monitoring the performance, connectivity, and hardware of their devices. IBM Cloud does not monitor individual customer devices, their configurations, or network status or assignments. Should issues arise, you can open a support ticket to schedule hardware replacement.

Activity	Client	IBM
Supervision and technical monitoring of devices (gateways, firewalls, bare metal / virtual servers)	R, A	C, I
Supervision and technical monitoring of hardware infrastructure outside of the direct customer environment	C, I	R, A
Customer hardware and component monitoring	R, A	C, I

MRO (Maintenance, repair, and operations)

The client (or their managed services provider) is responsible for ongoing maintenance and operation of their devices. The client team provides all relevant details regarding initial troubleshooting that has been completed and may request additional assistance using a support ticket, live chat, or phone call to IBM Cloud technical support.

Activity	Client	IBM
General maintenance of devices in customer infrastructure	R, A	C, I
Disaster recovery and high availability testing	R, A	C, I
Regularly scheduled device backups	R, A	C, I
Initial operating system set up and configuration (pre-provision and handoff to client)	C, I	R, A
Hardware maintenance and replacement	C, I, O	R, A
Break/fix support	C, I	R, A

Administration (ongoing device management)

The client (or their managed services provider) is responsible for the ongoing administration of their environment, devices, user accounts, and so on. IBM Cloud technical support is available to provide guidance, answer questions, and escalation to internal teams or vendors for complex issues that require additional assistance. IBM Cloud technical support does not perform migrations. Our technical staff is always available for assistance should an issue occur during a migration event/window, however we will not be able to join the entirety of a scheduled migration event call.

Activity	Client	IBM
Configuration and management of services (post-provision)	R, A	C, I
Configuration and management of firewalls, gateway devices, and underlying hosts (where applicable, post-provision)	R, A	C, I
Planning and preparation for change requests on firewall and gateway devices (configuration changes, operating system or firmware updates)	R, A	C, I
Perform change requests on firewall and gateway devices (configuration changes, operating system or firmware updates)	R, A	C, I
Manage IP address assignments (post provision)	R, A, O	C, I
Manage VLAN associations (post provision)	R, A, O	C, I
Configuration and management of IPSEC/GRE tunnels to remote client environment	R, A	C, I
Migrations - planning, preparation, implementation - moving from one solution to another	R, A	C, I

LCM (Life Cycle Management)

When a device or operating system reaches its End of Support (EOS) or End of Life (EOL), IBM Cloud no longer can provide support for it. Once the device has been upgraded to a supported firmware or operating system, support can resume on the device.

Activity	Client	IBM
Upgrade an operating system that has reached EOS/EOL	R, A, O	C, I
Upgrade the hardware of a device	R, A, O	C, I
Support of devices after EOS/EOL	R, A	

Additional notes and scope of support

For Consulting (C) and Informing (I), IBM Cloud technical support occurs through support tickets, live chats, or phone calls. It is expected that the client (or their managed services provider) provide technical resources with a strong understanding of the environment to aid with troubleshooting issues. IBM Cloud technical support is available to augment the client's own technical team and provide guidance and support as needed, bringing in any relevant internal team or vendor for additional assistance if warranted. Any break/fix support provided by IBM Cloud technical support (beyond restoring a device to its original working configuration) is done on a "best effort" basis.

Release notes for IBM Cloud Hardware Firewall

Find out about new and updated features in IBM Cloud Hardware Firewall.

8 December 2021

Managing permissions

Account administrators can now assign permissions to allow users to view and manage various parts of a hardware firewall. The following permissions can now be assigned:

- **Manage firewalls** - Allows you to view your list of firewalls. It also allows you to view and manage the details of a specific firewall.
- **Manage firewall rules** - Allows you to manage the rules of a specific hardware firewall.
- **Cancel services** - Allows you to cancel a firewall.

For more information, refer to Managing permissions.

Configuring the Hardware Firewall

Configuring your Hardware Firewall is as simple as creating a set of rules to allow access to certain IP addresses or ports from specific internet addresses while denying traffic from other sources.

Adding a firewall to a server

To add a firewall to a server, follow the steps in Getting Started. If you receive an error, see the Known Limitations and Getting help and support.

Editing rules

When a firewall is first added to a server, a set of rules is initially put in place that allows all traffic to reach the server. The rules can then be edited to control the traffic that reaches the server.

Make sure the "status" indicates that the firewall is "Processing All Rules." Users can choose to bypass the rules if implemented rules have an unintended impact on their environment by clicking **Bypass Rules** in the **Actions** menu.

1. From your browser, open the IBM Cloud catalog and log in to your account.
2. Select the Menu icon ☰ from the upper left, then click **Classic Infrastructure**.
3. Select **Devices > Device List** and click the firewall-protected device that you want to configure.
4. In the **Add-ons** section, click **Firewall details**. It will redirect you to the firewall page.
5. The Firewall Details page shows the current rules in effect for IPv4 and IPv6 addresses. If no rules are implemented, a yellow status icon shows with a "Bypassing all rules" message next to the device name.

   Rules are displayed in the order in which they are processed, with lower numbered rules having precedence over higher number rules. For example, if rule one allows a packet through, the packet ignores rules two and beyond.

   The fields are:

   Priority - This field contains the rule number. Lower numbered rules have precedence over higher numbered rules.

   Action - This select list is used to 'permit' or 'deny' traffic that matches this rule.

   Source - This field can be either 'any' or a specific IP address or the network address for a specific subnet.

   Destination - This field selects the destination IP (see Known Limitations if any issues arise).

   CIDR - This field indicates the standard CIDR notation for the selected source/destination.

   Port Range - These two fields indicate the range of ports (between 1 and 65535) that the rule applies to.

   Protocol - This field selects the protocol that the rule applies to (TCP/GRE/ICMP/UDP/PPTP/AH/ESP).

   Notes: Freeform field to enter any note about this rule.

6. Click the **Actions** menu icon at the end of the row of the firewall rule to edit or delete the rule. Click **Add rule** at the upper right of the table to add a rule. The rules are automatically validated as you enter them.
7. Click the **Save** or **Add** buttons to save the rule and apply to the firewall. The rule addition or update takes effect within two minutes.

Note: The **Delete** action is disabled if the firewall includes only one rule.

Common ports

Protocol	Port
FTP	21
SSH	22
Telnet	23

SMTP	25
DNS	53
HTTP	80
POP3	110
IMAP	143
HTTPS	443
MSSQL	1433
MySQL	3306
Remote Desktop	3389
PostgreSQL	5432
VNC web	5800
VNC Client	5900
Urchin	9999 or 10000

Common ports

Viewing your various firewalls

You can identify the Hardware Firewalls in use on an account and their associated VLANs, and identify unprotected VLANs and plan the deployment of a firewall solution.

Firewall overview by VLAN

To get an overview of firewalls on your system and initiate basic management:

1. From your browser, open the IBM Cloud catalog and log in to your account.
2. Select the Menu icon ☰ from the upper left, then click **Classic Infrastructure**.
3. Select **Network > IP Management > VLANs** .

☑ **Tip:** To view only public VLANS, click the **Filter** menu and enter `fcr` for **Primary Router**.

Each row represents a VLAN in your infrastructure. IBM© Cloud populates the **VLAN NUMBER** and **PRIMARY ROUTER** information automatically indicating the true VLAN number and the router that it is configured on. Use the **NAME** field to define a recognizable name.

The **GATEWAY/FIREWALL** column contains details about which hardware firewall protection is in place, for example:

Individually Protected Servers indicates that one or more servers is using a Hardware Firewall and that there is not a FortiGate Security Appliance, or Network Gateway in place. You cannot place VLAN firewalls and network gateways on a VLAN with individually protected servers.

Firewall-vlanXXXX.networklayer indicates that there is a FortiGate Security Appliance in place. Only one VLAN firewall or Network Gateway can be associated with a VLAN, but a server can be protected on the public VLAN by a VLAN firewall and associated on the private network with a Network Gateway.

GatewayName indicates that the VLAN is associated with that Network Gateway.

Individually protected servers view

On the VLANs screen, identify a row with **Individually Protected Servers** in the **Gateway/Firewall** column and click the associated VLAN number link. The details for the VLAN including the associated devices are displayed.

From here, you can click each device and review whether a firewall is in place for that particular Server.

After you click a device, scroll to the end of the Configuration tab. You see **Firewall** in the Addons section with **Installed** or **Not installed** for the status. **Not Installed** indicates that a firewall isn't in place for this device. **Installed** indicates that a firewall is in place and you have a **Firewall details** button. It will redirect you to the "Firewall Details" page where you can manage the firewall configuration.

Dedicated firewall view

On the VLANs screen, identify a row with **Firewall-vlanXXXX.networklayer.com** in the **Gateway/Firewall** column and click that firewall. You are presented with a FortiGate Security Appliance. The device details include the associated Router, VLAN, and IPv4/IPv6 Subnets, the devices associated with that VLAN, and the controls for routing traffic through or around the firewall.

FortiGate Security Appliance devices have the management IP, username, and password. Management is completed through the management GUI or SSH-based console.

Network gateway view

On the VLANs screen, identify a row with the **Gateway/Firewall** column with a Network Gateway device name and click that network gateway. You are then taken to the interface that displays associated front end (FCR) and backend (BCR) VLANs and Network Gateway management options.

Bypassing the Hardware Firewall rules

You can bypass the rules of your Hardware Firewall by following the instructions here.

1. From your browser, open the IBM Cloud catalog and log in to your account.
2. Select the Menu icon ☰ from the upper left, then click **Classic Infrastructure**.
3. Select **Devices > Device List** and click the firewall-protected device that you want to bypass.
4. In the **Firewall** tab, click the **Actions** menu and choose **Bypass Rules**. Click **Yes** to confirm the action. Bypassing the rules takes approximately two minutes to take effect. While in bypass mode, the "Status" is "Bypassing All Rules".

Enabling the rules again

To enable the rules again, follow the preceding instructions to reach the Firewall tab of the device, and click the **Actions** menu and choose **Process Rules**. The "Status" changes back to "Processing All Rules" within two minutes.

Canceling a Hardware Firewall

Your Hardware Firewall can be cancelled at any time, by following the instructions here.

1. From your browser, open the IBM Cloud catalog and log in to your account.
2. Select the Menu icon ☰ from the upper left, then click **Classic Infrastructure**.
3. Select **Devices > Device List** and click the firewall-protected device that you want to cancel.
4. In the **Add-ons** section, click **Firewall details**. It redirects you to the Firewall Details page.
5. In the Firewall Details page, click the **Actions** menu and choose **Cancel firewall**. In the next dialog, choose whether you want to cancel immediately or at the next billing cycle.

All devices on the VLAN are left without front-end firewall protections. This service is provided month to month and billing will be discontinued for the next month upon cancellation.

Viewing log reports for Hardware Firewall

Logs for your Hardware Firewall are available on a per-IP basis by navigating to the protected device, on the Firewall Details page, and clicking **Actions > Firewall Logs**.

Logs are presented in .CSV format and contain the following items:

Event Type: The action taken by the firewall (Deny)

Protocol: The protocol used for communication (TCP/PING/UDP/IRD/etc)

Source IP Address: IP where the packet originated

Source Port: The port where the packet originated

Destination IP: Intended target for the packet

Destination Port: Intended port for the packet

Creation Date: Date and time of action (24-hour format)

Managing permissions

To view and manage your hardware firewalls, you need the correct permissions. After your account administrator grants your user account permissions and access, you can view your hardware firewall details by using the IBM Cloud® console, or by using the SoftLayer API. The information or actions that you see depend on your permissions.

The following permissions are required for viewing and managing various parts of your hardware firewalls:

- **Manage firewalls** - Allows you to view your list of firewalls. It also allows you to view and manage the details of a specific firewall.
- **View hardware details** - Allows you to view your list of hardware firewalls on bare metal servers. It also allows you to view and manage the details of a specific hardware firewall on a bare metal server.
- **View virtual server details** - Allows you to view your list of firewalls on virtual servers. It also allows you to view and manage the details of a specific hardware firewall on a virtual server.
- **Manage firewall rules** - Allows you to manage the rules of a specific hardware firewall.
- **Cancel services** - Allows you to cancel a firewall.

Adding permissions for your users

If you are the account administrator and you want to grant a user permission to view and manage gateway appliance details, complete the following steps.

1. Log in to the Access (IAM) page in the IBM Cloud® console.
2. Select **View: My classic infrastructure users** .
3. Select a user, click the **Classic infrastructure** tab, then click the **Permissions** tab.
4. Expand the **Devices** category and select **Manage firewalls**.
5. Expand the **Devices** category and select **View hardware details** .
6. Expand the **Devices** category and select **View virtual server details** .
7. Expand the **Devices** category and select **Manage firewall rules**.
8. Expand the **Account** category and select **Cancel services**.
9. Click **Apply**.

Next steps

User permissions are updated immediately after the changes are submitted. If permissions are granted, the user can view or interact with the selected features. If permissions are removed, the user can no longer view or interact with the selected features. Permissions can be updated again at any time.

IBM Cloud IP ranges

A frequently asked question is, "What IP ranges do I allow through the firewall?" The following tables contain the full range of IP addresses to use with these IBM firewalls and appliances.

- IBM Cloud Juniper vSRX Standard
- IBM Virtual Router Appliance
- Fortinet vFSA
- Fortinet Fortigate Security Appliance 10 Gbps
- IBM Security Groups
- Hardware Firewall

⚠ **Important:** To identify potential conflicts between IP ranges in your on-premises environment and IP ranges used in IBM Cloud, you can search in the IP Ranges Calculator tool. By using the tool, you can download the listed IP ranges in JSON format. Disclaimer: This community tool is updated based on support availability.

Front-end (public) network

Ports to allow:

- All TCP/UDP ports
- ICMP – ping (for support troubleshooting and monitoring)

Data center	City	IP range
ams03	Amsterdam	159.8.198.0/23
che01	Chennai	169.38.118.0/23
dal08	Dallas	192.255.18.0/24
dal09	Dallas	198.23.118.0/23
dal10	Dallas	169.46.118.0/23
dal12	Dallas	169.47.118.0/23
dal13	Dallas	169.48.118.0/24
fra02	Frankfurt	159.122.118.0/23
fra04	Frankfurt	161.156.118.0/24
fra05	Frankfurt	149.81.118.0/23
lon02	London	5.10.118.0/23
lon04	London	158.175.127.0/24
lon05	London	141.125.118.0/23
lon06	London	158.176.118.0/23
mad02	Madrid	13.120.118.0/24
mad04	Madrid	13.121.118.0/24

mad05	Madrid	13.122.118.0/24
mil01	Milan	159.122.138.0/23
mon01	Montreal	169.54.118.0/23
osa21	Osaka	163.68.118.0/24
osa22	Osaka	163.69.118.0/24
osa23	Osaka	163.73.118.0/24
par01	Paris	159.8.118.0/23
sao01	São Paulo	169.57.138.0/23
sjc01	San Jose	50.23.118.0/23
sjc03	San Jose	169.45.118.0/23
sjc04	San Jose	169.62.118.0/24
sng01	Jurong East	174.133.118.0/23
syd01	Sydney	168.1.18.0/23
syd04	Sydney	130.198.118.0/23
syd05	Sydney	135.90.118.0/23
tok02	Tokyo	161.202.118.0/23
tok04	Tokyo	128.168.118.0/23
tok05	Tokyo	165.192.118.0/23
tor01	Toronto	158.85.118.0/23
tor04	Toronto	163.74.118.0/23
tor05	Toronto	163.75.118.0/23
wdc01	Washington D.C.	208.43.118.0/23
wdc03	Washington D.C.	192.255.38.0/24
wdc04	Washington D.C.	169.55.118.0/23
wdc06	Washington D.C.	169.60.118.0/23
wdc07	Washington D.C.	169.61.118.0/23

Table 1: Front-end (public) network

Load balancer IPs

Data center	City	IP range

ams03	Amsterdam	159.8.197.0/24
che01	Chennai	169.38.117.0/24
dal05	Dallas	50.23.203.0/24 108.168.157.0/24 173.192.117.0/24 192.155.205.0/24
dal09	Dallas	169.46.187.0/24 198.23.117.0/24
dal10	Dallas	169.46.117.0/24
dal12	Dallas	169.47.117.0/24
dal13	Dallas	169.48.117.0/24
fra02	Frankfurt	159.122.117.0/24
fra04	Frankfurt	161.156.117.0/24
fra05	Frankfurt	149.81.117.0/24
lon02	London	5.10.117.0/24
lon04	London	158.175.117.0/24
lon05	London	141.125.117.0/24
lon06	London	158.176.117.0/24
mil01	Milan	159.122.137.0/24
mon01	Montreal	169.54.117.0/24
par01	Paris	159.8.117.0/24
sao01	São Paulo	169.57.137.0/24
sjc01	San Jose	50.23.117.0/24
sjc03	San Jose	169.45.117.0/24
sng01	Jurong East	174.133.117.0/24
syd01	Sydney	168.1.17.0/24
syd04	Sydney	130.198.117.0/24
syd05	Sydney	135.90.117.0/24
tok02	Tokyo	161.202.117.0/24
tok04	Tokyo	128.168.117.0/24
tok05	Tokyo	165.192.117.0/24

tor01	Toronto	158.85.117.0/24
wdc01	Washington D.C.	50.22.248.0/25 169.54.27.0/24 198.11.250.0/24 208.43.117.0/24
wdc04	Washington D.C.	169.55.117.0/24
wdc06	Washington D.C.	169.60.117.0/24
wdc07	Washington D.C.	169.61.117.0/24

Table 2: Load balancer IPs

Back-end (private) network

IP block: Your private IP block for server-to-server communications (`10.X.X.X/X`)

Ports to allow:

- All TCP/UDP ports
- ICMP – ping (for support troubleshooting and monitoring)

Customer private network space

City	Data center	Pod	IP range
Amsterdam	ams03	BCR01	10.1.243.0/24 10.3.48.0/24 10.3.139.0/24 10.136.0.0/15
	ams03	BCR02	10.175.0.0/16 10.214.0.0/16
Chennai	che01	BCR01	10.3.58.0/24 10.162.0.0/15 10.200.27.0/24
Dallas	dal05	BCR01	10.0.40.0/22 10.1.151.0/24 10.3.60.0/24 10.40.0.0/14 10.251.0.0/23 10.251.64.0/23
	dal05	BCR03	10.80.0.0/14 10.251.4.0/23 10.251.68.0/23
	dal05	BCR04	10.84.0.0/16 10.86.0.0/16 10.251.70.0/23
	dal09	BRC01	10.2.123.0/24 10.2.244.0/24 10.3.16.0/24 10.120.0.0/15
	dal09	BCR02	10.142.0.0/15

	dal09	BCR03	10.98.0.0/15 10.152.0.0/15
	dal09	BCR04	10.154.0.0/15
	dal09	BCR05	10.172.0.0/16
	dal09	BCR06	10.173.0.0/16
	dal10	BCR01	10.0.192.0/26 10.3.62.0/24 10.3.247.0/24 10.176.0.0/15 10.200.91.0/24
	dal10	BCR02	10.0.192.64/26 10.171.0.0/16
	dal10	BCR03	10.93.0.0/16
	dal10	BCR04	10.5.0.0/16 10.23.0.0/16 10.38.0.0/16 10.94.0.0/15 10.221.0.0/16
	dal12	BCR01	10.3.2.0/24 10.184.0.0/15 10.200.123.0/24 10.241.0.0/16
	dal12	BCR02	10.48.0.0/16 10.74.0.0/16
	dal13	BCR01	10.3.3.0/24 10.186.0.0/15 10.200.139.0/24 10.208.0.0/16
	dal13	BCR02	10.36.0.0/16 10.73.0.0/16 10.209.0.0/16 10.220.0.0/16
	dal13	BCR03	10.37.0.0/16
Frankfurt	fra02	BCR01	10.2.240.0/24 10.3.38.0/24 10.3.91.0/24 10.134.0.0/15 10.201.155.0/24
	fra02	BCR02	10.85.0.0/16 10.194.0.0/16
	fra02	BCR03	10.20.0.0/16 10.215.0.0/16

	fra04	BCR01	10.3.13.0/24 10.21.0.0/16 10.75.0.0/16 10.201.123.0/24 10.240.0.0/16
	fra05	BCR01	10.3.15.0/24 10.13.0.0/16 10.123.0.0/16 10.201.139.0/24
	fra05	BCR02	10.174.0.0/16
London	lon02	BCR01	10.1.219.0/24 10.3.40.8/29 10.3.40.16/28 10.3.40.32/27 10.3.40.64/26 10.3.40.128/25 10.112.0.0/15 10.201.107.0/24
	lon02	BCR02	10.164.0.0/15
	lon04	BCR01	10.3.7.0/24 10.45.0.0/16 10.201.43.0/24 10.222.0.0/16
	lon05	BCR01	10.3.21.0/24 10.196.0.0/15 10.201.59.0/24
	lon06	BCR01	10.3.11.0/24 10.72.0.0/16 10.201.75.0/24 10.242.0.0/16
Madrid	mad02	10.3.45.0/24 10.118.0.0/18	
	mad04	10.3.43.0/24 10.118.64.0/18 10.201.253.0/24	
	mad05	10.3.41.0/24 10.118.128.0/18 10.201.254.0/24	
Milan	mil01	BCR01	10.1.241.0/24 10.3.50.8/29 10.3.50.16/28 10.3.50.32/27 10.3.50.64/26 10.3.50.128/25 10.3.155.0/24 10.144.0.0/15

Montreal	mon01	BCR01	10.3.46.8/29 10.3.46.16/28 10.3.46.32/27 10.3.46.64/26 10.3.46.128/25 10.3.123.0/24 10.140.0.0/15
Osaka	osa21	BCR01	10.3.59.0/24 10.8.0.0/16 10.201.246.0/24
	osa22	BCR01	10.3.57.0/24 10.9.0.0/16 10.201.247.0/24
	osa23	BCR01	10.3.55.0/24 10.10.0.0/16 10.201.248.0/24
Paris	par01	BCR01	10.2.155.0/24 10.2.243.0/24 10.3.26.8/29 10.3.26.16/28 10.3.26.32/27 10.3.26.64/26 10.3.26.128/25 10.126.0.0/15
	par04	BCR01	10.3.27.0/24 10.217.0.0/16
	par05	BCR01	10.3.25.0/24 10.218.0.0/16
	par06	BCR01	10.3.24.0/24 10.219.0.0/16
São Paulo	sao01	BCR01	10.3.54.0/29 10.3.54.8/29 10.3.54.16/28 10.3.54.32/27 10.3.54.64/26 10.3.54.128/25 10.150.0.0/15 10.200.11.0/24
	sao04	BCR01	10.3.49.0/24 10.14.0.0/16 10.201.251.0/24
	sao05	BCR01	10.3.47.0/24 10.15.0.0/16 10.201.252.0/24
San Jose	sjc01	BCR01	10.1.203.0/24 10.3.14.0/24 10.52.0.0/14 10.251.6.0/23 10.251.72.0/23
	sjc01	BCR03	10.122.0.0/16

	sjc03	BCR01	10.3.56.0/24 10.3.187.0/24 10.160.0.0/15
	sjc03	BCR02	10.168.0.0/15
	sjc04	BCR01	10.3.9.0/24 10.87.0.0/16 10.201.91.0/24
Jurong East	sng01	BCR01	10.2.43.0/24 10.3.20.0/24 10.64.0.0/16 10.66.0.0/15 10.251.12.0/23 10.251.86.0/23
	sng01	BCR02	10.116.0.0/15
Sydney	syd01	BCR01	10.3.44.0/24 10.3.107.0/24 10.138.0.0/15 10.202.43.0/24
	syd01	BCR02	10.210.0.0/16
	syd04	BCR01	10.3.6.0/24 10.63.0.0/16 10.201.27.0/24
	syd05	BCR01	10.3.23.0/24 10.195.0.0/16 10.207.27.0/24
Tokyo	tok02	BCR01	10.2.241.0/24 10.3.30.0/24 10.3.75.0/24 10.3.242.0/24 10.129.0.0/16 10.132.0.0/15 10.201.171.0/24
	tok02	BCR02	10.212.0.0/16 10.44.0.0/16
	tok04	BCR01	10.3.17.0/24 10.192.0.0/16 10.201.187.0/24
	tok05	BCR01	10.3.19.0/24 10.193.0.0/16 10.201.203.0/24
	tor01	BCR01	10.2.59.0/24 10.3.42.0/24 10.114.0.0/15 10.202.107.0/24
	tor01	BCR02	10.166.0.0/15

	tor04	BCR01	10.1.2.0/24 10.3.53.0/24 10.11.0.0/16
	tor05	BCR01	10.1.6.0/24 10.3.51.0/24 10.243.0.0/16
Washington D.C.	wdc01	BCR05	10.108.0.0/15
	wdc01	BCR06	10.124.0.0/15
	wdc04	BCR01	10.3.10.0/29 10.3.52.0/24 10.3.171.0/24 10.3.240.0/24 10.148.0.0/15
	wdc04	BCR02	10.0.192.128/26 10.170.0.0/16
	wdc04	BCR03	10.183.0.0/16 10.216.0.0/16
	wdc04	BCR04	10.65.0.0/16 10.201.11.0/24 10.211.0.0/16
	wdc04	BCR05	10.213.0.0/16
	wdc06	BCR01	10.3.4.0/24 10.188.0.0/15 10.200.171.0/24
	wdc07	BCR01	10.3.5.0/24 10.39.0.0/16 10.190.0.0/15 10.200.187.0/24

Table 3: Customer private network space

Service network (on back-end/private network)

CHANGE LOG

To provision and reload classic Virtual Servers and classic Bare Metal Servers, the following private service networks must be allowed through your gateway appliances and firewalls.

⚠ **Important:** Be sure to configure rules and verify routes for the service networks listed in the table below for "All", dal10, wdc04, and the location of your server.

Additionally, complete the following steps:

- Allow and route the following service networks to the BCR on your gateway appliance or firewall for all Bare Metal and Virtual Server provisions and reloads: 10.0.64.0/19, 10.200.80.0/20, 161.26.13.0/24, 161.26.96.0/22, 166.9.12.0/23, 166.9.48.0/24, 166.9.50.0/24, 166.9.228.0/24, 166.9.250.192/27, 10.3.160.0/20, 10.201.0.0/20, 161.26.92.0/22, 161.26.132.0/22, 166.9.20.0/23, 166.9.231.0/24.
- For RHEL servers, ensure the entire 161.26.0.0/16 is allowed and routed properly to the BCR. Add any additional datacenter service networks that are mentioned in the RHEL section near the bottom of the page.
- Allow traffic between the service networks and your server in both directions.
- By default, all classic servers and classic gateway and firewall devices are configured with a static route for the `10.0.0.0/8`, `161.26.0.0/16` and `166.8.0.0/14` networks to the Back-end Customer Router (BCR). If you configure overlapping routes with those subnets, validate that you have also configured PBR or a similar service. Otherwise, consider using different IP space that doesn't overlap with our service networks for your VPNs or

tunnels. Failing to do so can result in the failure to provision your Virtual Servers and Bare Metal Servers.

Ports to allow:

- All TCP/UDP ports (for access from your local workstation)
- ICMP – ping (for support troubleshooting and monitoring)

Data center	City	IP range
All	•	10.0.64.0/19
ams03	Amsterdam	10.3.128.0/20 161.26.28.0/22
che01	Chennai	10.200.16.0/20 161.26.32.0/22 166.9.60.0/24
dal05	Dallas	10.1.128.0/19 [1] 161.26.12.0/24
dal08	Dallas	100.100.0.0/20
dal09	Dallas	10.2.112.0/20 10.3.192.0/24 161.26.4.0/22
dal10	Dallas	10.200.80.0/20 161.26.13.0/24 161.26.96.0/22 166.9.12.0/23 166.9.48.0/24 166.9.50.0/24 166.9.228.0/24 166.9.250.192/27
dal12	Dallas	10.200.112.0/20 161.26.108.0/22 166.9.14.0/23 166.9.51.0/24 166.9.229.0/24 166.9.250.224/27
dal13	Dallas	10.200.128.0/20 161.26.112.0/22 166.9.16.0/23 166.9.58.0/24 166.9.230.0/24 166.9.251.0/27
fra02	Frankfurt	10.3.80.0/20 161.26.36.0/22 166.9.28.0/23
fra04	Frankfurt	10.201.112.0/20 161.26.144.0/22 166.9.30.0/23
fra05	Frankfurt	10.201.128.0/20 161.26.148.0/22 166.0.32.0/23

lon02	London	10.1.208.0/20 161.26.8.0/22
lon04	London	10.201.32.0/20 161.26.128.0/22 166.9.36.0/23
lon05	London	10.201.48.0/20 161.26.140.0/22 166.9.34.0/23
lon06	London	10.201.64.0/20 161.26.160.0/22 166.9.38.0/23
mad02	Madrid	10.203.96.0/20 161.26.212.0/22
mad04	Madrid	10.203.112.0/20 161.26.216.0/22
mad05	Madrid	10.203.128.0/20 161.26.220.0/22
mil01	Milan	10.3.144.0/20 161.26.52.0/22
mon01	Montreal	10.3.112.0/20 161.26.56.0/22
osa21	Osaka	10.202.112.0/20 161.26.184.0/22 166.9.70.0/24
osa22	Osaka	10.202.144.0/20 161.26.188.0/22 166.9.71.0/24
osa23	Osaka	10.202.160.0/20 161.26.192.0/22 166.9.72.0/24
par01	Paris	10.2.144.0/20 161.26.60.0/22 166.9.79.0/24 166.9.245.128/27
sao01	São Paulo	10.200.0.0/20 161.26.64.0/22 166.9.82.0/24
sao04	São Paulo	10.202.208.0/20 161.26.204.0/22 166.9.83.0/24
sao05	São Paulo	10.202.240.0/20 161.26.208.0/22 166.9.84.0/24
sjc01	San Jose	10.1.192.0/20 10.200.32.0/20

sjc03	San Jose	10.3.176.0/20 161.26.72.0/22
sjc04	San Jose	10.201.80.0/20 161.26.136.0/22
sng01	Jurong East	10.2.32.0/20 10.200.144.0/20 161.26.76.0/22
syd01	Sydney	10.3.96.0/20 10.202.32.0/20 161.26.80.0/22 161.26.168.0/22 166.9.52.0/23
syd04	Sydney	10.201.16.0/20 161.26.124.0/22 166.9.54.0/23
syd05	Sydney	10.202.16.0/20 161.26.164.0/22 166.9.56.0/23
tok02	Tokyo	10.3.64.0/20 10.201.160.0/20 161.26.84.0/22 166.9.40.0/23
tok04	Tokyo	10.201.176.0/20 161.26.152.0/22 166.9.42.0/23
tok05	Tokyo	10.201.192.0/20 161.26.156.0/22 166.9.44.0/23
tor01	Toronto	10.2.48.0/20 10.202.96.0/20 161.26.88.0/22 166.9.76.0/24
tor04	Toronto	10.202.176.0/20 161.26.196.0/22 166.9.77.0/24
tor05	Toronto	10.202.192.0/20 161.26.200.0/22 166.9.78.0/24
wdc01	Washington D.C.	10.1.96.0/19 161.26.16.0/22
wdc04	Washington D.C.	10.3.160.0/20 10.201.0.0/20 161.26.92.0/22 161.26.132.0/22 166.9.20.0/23 166.9.231.0/24

wdc06	Washington D.C.	10.200.160.0/20 161.26.120.0/22 166.9.22.0/23 166.9.232.0/24 166.9.251.64/27
wdc07	Washington D.C.	10.200.176.0/20 161.26.132.0/22 166.9.24.0/23 166.9.233.0/24 166.9.251.96/27

Table 4: Service network

Service by data center

Deprecated: As of 8 June 2020, all instances of the AdvMon (Nimsoft) by Data Center service are deprecated and are no longer supported. For more information, see FAQs.

Data center	IP range
Required Flows: • Outbound TCP 8086 and TCP 8087 from your private VLANs to IP ranges documented in dal09 and dal10 only. • Outbound TCP 2546 from your private VLANs to IP ranges documented for each DC where you need to access your vault.	
ams03	10.3.134.0/24
che01	10.200.22.0/24
dal08	100.100.6.0/24
dal09	10.2.118.0/24
dal09	10.2.126.0/24
dal10	10.200.86.0/24
dal12	10.200.118.0/24
dal13	10.200.134.0/24
fra02	10.3.86.0/24 10.201.150.0/24
fra04	10.201.118.0/24
fra05	10.201.134.0/24
lon02	10.1.214.0/24 10.201.102.0/24
lon04	10.201.38.0/24
lon05	10.201.54.0/24

lon06	10.201.70.0/24
mil01	10.3.150.0/24
mon01	10.3.118.0/24
osa21	10.202.118.0/24
osa22	10.202.150.0/24
osa23	10.202.166.0/24
par01	10.2.150.0/24
sao01	10.200.6.0/24
sjc01	10.1.198.0/24 10.200.38.0/24
sjc03	10.3.182.0/24
sjc04	10.201.86.0/24
sng01	10.2.38.0/24 10.200.150.0/24
syd01	10.3.102.0/24
syd04	10.201.22.0/24
tok02	10.201.166.0/24
tok04	10.201.182.0/24
tok05	10.201.198.0/24
tor01	10.2.54.0/24
wdc01	10.1.114.0/24
wdc03	100.100.38.0/24
wdc04	10.3.166.0/24 10.201.6.0/24
wdc06	10.200.166.0/24
wdc07	10.200.182.0/24

eVault by Data Center

Data center	IP range

Required Flows: File Storage for Classic: • TCP & UDP 111 (sunrpc) • TCP & UDP 2049 (nfs) • TCP & UDP 111(portmapper) • TCP & UDP 635 (nfsd) • TCP & UDP 4045-4048 • UDP 4049	**Required Flows**: Block Storage for Classic: • TCP & UDP 3260 (iscsi)
ams03	10.3.142.0/24 161.26.30.0/24
che01	10.200.30.0/24 161.26.34.0/24
dal05	10.1.154.0/24 10.2.110.0/24
dal08	100.100.14.0/24
dal09	10.2.125.0/24 10.2.126.0/24
dal10	10.200.94.0/24 10.202.239.0/24 161.26.13.0/24 161.26.98.0/24 161.26.99.0/24
dal12	10.200.126.0/24 161.26.110.0/24 161.26.111.0/24
dal13	10.200.142.0/24 10.200.142.0/24 10.200.143.128/25 161.26.114.0/24 161.26.115.0/24
dal14	10.203.157.0/24 161.26.226.0/24
fra02	10.3.94.0/24 10.201.154.0/24 161.26.38.0/24 161.26.39.0/24
fra04	10.201.110.0/24 161.26.146.0/24
fra05	10.201.142.0/24 161.26.150.0/24
lon02	10.1.222.0/24 10.201.110.0/24 161.26.10.0/24
lon04	10.201.46.0/24 161.26.130.0/24

lon05	10.201.62.0/24 161.26.162.0/24
lon06	10.201.78.0/24 161.26.142.0/24
mad02	10.203.109.0/24 161.26.214.0/24
mad04	10.203.125.0/24 161.26.218.0/24
mad05	10.203.141.0/24 161.26.222.0/24
mil01	10.3.158.0/24 161.26.54.0/24
mon01	10.3.126.0/24 161.26.58.0/24
osa21	10.202.126.0/24 161.26.186.0/24
osa22	10.202.158.0/24 161.26.190.0/24
osa23	10.202.174.0/24 161.26.194.0/24
par01	10.2.158.0/24 10.2.159.0/24 161.26.62.0/24
par04	10.202.94.0/24 161.26.174.0/24
par05	10.202.78.0/24 161.26.178.0/24
par06	10.202.62.0/24 161.26.182.0/24
sao01	10.200.14.0/24 10.200.15.0/25 10.203.78.0/24 161.26.66.0/24 161.26.67.0/24
sao04	10.202.221.0/24 161.26.206.0/24
sao05	10.202.253.0/24 161.26.210.0/24
sjc01	10.1.206.0/24
sjc03	10.3.190.0/24 161.26.74.0/24

sjc04	10.201.94.0/24 161.26.138.0/24
sng01	10.2.46.0/24 10.200.158.0/24 161.26.78.0/24
syd01	10.3.110.0/24 10.202.46.0/24 161.26.170.0/24 161.26.82.0/24
syd04	10.201.30.0/24 130.198.64.0/18 161.26.126.0/24
syd05	10.202.30.0/24 161.26.166.0/24
tok02	10.3.78.0/24 10.3.79.0/24 10.201.174.0/24 161.26.86.0/24 161.26.87.0/24
tok04	10.201.190.0/24 161.26.154.0/24
tok05	10.201.206.0/24 161.26.158.0/24
tor01	10.2.62.0/24 10.202.110.0/24 161.26.90.0/24 161.26.91.0/24
tor04	10.202.189.0/24 161.26.198.0/24
tor05	10.202.205.0/24 161.26.202.0/24
wdc01	10.1.122.0/24 10.1.104.0/24
wdc03	100.100.46.0/24
wdc04	10.201.10.0/24 10.201.14.0/24 10.3.174.0/24 10.3.175.0/25 161.26.134.0/24 161.26.94.0/24
wdc06	10.200.174.0/24 161.26.118.0/24
wdc07	10.200.90.0/24 161.26.122.0/24

File and Block by Data Center

Data center	IP range

Required Flows:

- Inbound: TCP and UDP, 48000.
- Outbound: TCP and UDP, 48000-48020.

ams03	10.3.131.0/24
che01	10.200.19.0/24
dal05	10.1.143.0/24 10.1.139.0/24
dal08	100.100.3.0/24
dal09	10.2.115.0/24
dal10	10.200.83.0/24
dal12	10.200.115.0/24
dal13	10.200.131.0/24
fra02	10.3.83.0/24 10.201.147.0/24
fra04	10.201.115.0/24
fra05	10.201.131.0/24
lon02	10.1.211.0/24 10.201.99.0/24
lon04	10.201.35.0/24
lon05	10.201.51.0/24
lon06	10.201.67.0/24
mil01	10.3.147.0/24
mon01	10.3.115.0/24
par01	10.2.147.0/24
sao01	10.200.3.0/24
sjc01	10.1.195.0/24
sjc03	10.3.179.0/24
sjc04	10.201.83.0/24
sng01	10.2.35.0/24
syd01	10.3.99.0/24

syd04	10.201.19.0/24
tok02	10.3.67.0/24 10.201.163.0/24
tok04	10.201.179.0/24
tok05	10.201.195.0/24
tor01	10.2.51.0/24
wdc01	10.1.111.0/24
wdc03	100.100.35.0/24
wdc04	10.3.163.0/24
wdc04	10.201.3.0/24
wdc06	10.200.163.0/24
wdc07	10.200.179.0/24

AdvMon (Nimsoft) by Data Center

Data center	IP range
Required Flows: Outbound: TCP 80, 443. [2]	
ams03	10.3.130.0/24
che01	10.200.18.0/24
dal05	10.1.142.0/24 10.1.138.0/24
dal08	100.100.2.0/24
dal09	10.2.114.0/24
dal10	10.200.82.0/24
dal12	10.200.114.0/24
dal13	10.200.130.0/24
fra02	10.3.82.0/24 10.201.146.0/24
fra04	10.201.114.0/24
fra05	10.201.130.0/24
lon02	10.1.210.0/24 10.201.98.0/24
lon04	10.201.34.0/24

lon05	10.201.50.0/24
lon06	10.201.66.0/24
mil01	10.3.146.0/24
mon01	10.3.114.0/24
osa21	10.202.114.0/24
osa22	10.202.146.0/24
osa23	10.202.162.0/24
par01	10.2.146.0/24
sao01	10.200.2.0/24
sjc01	10.1.194.0/24 10.200.34.0/24
sjc03	10.3.178.0/24
sjc04	10.201.82.0/24
sng01	10.2.34.0/24 10.200.146.0/24
syd01	10.3.98.0/24
syd04	10.201.18.0/24
tok02	10.3.66.0/24 10.201.162.0/24
tok04	10.201.178.0/24
tok05	10.201.194.0/24
tor01	10.2.50.0/24
wdc01	10.1.110.0/24 10.1.106.0/24
wdc03	100.100.34.0/24
wdc04	10.3.162.0/24
wdc04	10.201.2.0/24
wdc06	10.200.162.0/24
wdc07	10.200.178.0/24

ICOS by Data Center

Change log for service network IP ranges (26 October 2022)

Removed

- All address 166.8.0.0/14
- ams01 address 10.2.64.0/20
- ams01 address 10.2.66.0/24
- ams01 address 10.2.67.0/24
- ams01 address 10.2.70.0/24
- ams01 address 10.2.78.0/24
- ams01 address 10.200.48.0/20
- ams01 address 10.200.50.0/24
- ams01 address 10.200.54.0/24
- ams01 address 10.200.62.0/24
- dal01 address 10.0.90.0/24
- dal05 address 10.1.143/139.0/24
- dal05 address 10.1.159.0/24
- dal06 address 10.2.128.0/20
- dal06 address 10.2.130.0/24
- dal06 address 10.2.131.0/24
- dal06 address 10.2.142.0/24
- dal06 address 10.2.134.0/24
- dal07 address 10.1.176.0/20
- fra02AZ address 10.201.158.0/24
- hkg02 address 161.26.40.0/22
- hkg02 address 10.2.162.0/24
- hkg02 address 10.2.163.0/24
- hkg02 address 10.2.166.0/24
- hkg02 address 10.2.174.0/24
- hou02 address 10.1.174.0/24
- lon02AZ address 10.201.110.0/24
- mel01 address 10.2.94.0/24
- mel01 address 161.26.46.0/24
- mex01 address 10.2.176.0/20
- mex01 address 10.2.178.0/24
- mex01 address 10.2.179.0/24
- mex01 address 10.2.182.0/24
- mex01 address 10.2.190.0/24
- mex01 address 161.26.48.0/22
- mex01 address 161.26.50.0/24
- osl01 address 10.200.110.0/24
- osl01 address 161.26.106.0/24
- seo01 address 10.200.64.0/20
- seo01 address 10.200.66.0/24
- seo01 address 10.200.67.0/24
- seo01 address 10.200.78.0/24
- seo01 address 10.200.86.0/24
- seo01 address 161.26.100.0/22
- seo01 address 161.26.102.0/24
- seo01 address 166.9.46.0/23
- sjc01 address 10.200.46.0/24
- tok02AZ address 10.201.174.0/24
- wdc01 address 10.1.127.0/24
- wdc03 address 100.100.32.0/20

Added

- ams03 address 161.26.28.0/22
- ams03 address 161.26.30.0/24
- che01 address 161.26.32.0/22
- che01 address 161.26.34.0/24
- che01 address 166.9.60.0/24
- dal05 address 10.1.139.0/24
- dal05 address 10.1.143.0/24
- dal05 address 10.2.110.0/24
- dal05 address 161.26.12.0/24
- dal09 address 10.2.126.0/24
- dal09 address 161.26.4.0/22
- dal10 address 10.202.239.0/24
- dal10 address 161.26.13.0/24
- dal10 address 161.26.96.0/22
- dal10 address 161.26.98.0/24
- dal10 address 161.26.99.0/24
- dal10 address 166.9.12.0/23
- dal10 address 166.9.48.0/24
- dal10 address 166.9.50.0/24
- dal10 address 166.9.228.0/24
- dal10 address 166.9.250.192/27
- dal12 address 161.26.108.0/22
- dal12 address 161.26.110.0/24
- dal12 address 161.26.111.0/24
- dal12 address 166.9.14.0/23
- dal12 address 166.9.51.0/24
- dal12 address 166.9.229.0/24
- dal12 address 166.9.250.224/27
- dal13 address 161.26.112.0/22
- dal13 address 166.9.16.0/23
- dal13 address 166.9.58.0/24
- dal13 address 166.9.230.0/24
- dal13 address 166.9.251.0/27
- dal13 address 10.200.142.0/24
- dal13 address 10.200.143.128/25
- dal13 address 161.26.114.0/24
- dal13 address 161.26.115.0/24
- fra02 address 10.201.154.0/24
- fra02 address 161.26.36.0/22
- fra02 address 161.26.38.0/24
- fra02 address 161.26.39.0/24
- fra02 address 166.9.28.0/23
- fra04 address 161.26.144.0/22
- fra04 address 161.26.146.0/24
- fra04 address 166.9.30.0/23
- fra05 address 161.26.148.0/22
- fra05 address 161.26.150.0/24
- fra05 address 166.0.32.0/23
- lon02 address 161.26.8.0/22
- lon02 address 161.26.10.0/24

- lon02 address 10.201.110.0/24
- lon04 address 161.26.128.0/22
- lon04 address 161.26.130.0/24
- lon04 address 166.9.36.0/23
- lon05 address 161.26.140.0/22
- lon05 address 161.26.162.0/24
- lon05 address 166.9.34.0/23
- lon06 address 161.26.142.0/24
- lon06 address 161.26.160.0/22
- lon06 address 166.9.38.0/23
- mil01 address 161.26.52.0/22
- mil01 address 161.26.54.0/24
- mon01 address 161.26.56.0/22
- mon01 address 161.26.58.0/24
- osa21 address 161.26.184.0/22
- osa21 address 161.26.186.0/24
- osa21 address 166.9.70.0/24
- osa22 address 161.26.188.0/22
- osa22 address 161.26.190.0/24
- osa22 address 166.9.71.0/24
- osa23 address 161.26.192.0/22
- osa23 address 161.26.194.0/24
- osa23 address 166.9.72.0/24
- par01 address 10.2.159.0/24
- par01 address 161.26.62.0/24
- par01 address 161.26.60.0/22
- par01 address 166.9.79.0/24
- par01 address 166.9.245.128/27
- par04 address 10.202.94.0/24
- par04 address 161.26.174.0/24
- par05 address 10.202.78.0/24
- par05 address 161.26.178.0/24
- par06 address 10.202.62.0/24
- par06 address 161.26.182.0/24
- sao01 address 10.200.15.0/25
- sao01 address 10.203.78.0/24
- sao01 address 161.26.64.0/22
- sao01 address 161.26.66.0/24
- sao01 address 161.26.67.0/24
- sao01 address 166.9.82.0/24
- sao04 address 10.202.221.0/24
- sao04 address 161.26.204.0/22
- sao04 address 161.26.206.0/24
- sao04 address 166.9.83.0/24
- sao05 address 10.202.253.0/24
- sao05 address 161.26.208.0/22
- sao05 address 161.26.210.0/24
- sao05 address 166.9.84.0/24
- sjc01 address 10.200.32.0/20
- sjc03 address 161.26.72.0/22
- sjc03 address 161.26.74.0/24

- sjc04 address 161.26.136.0/22
- sjc04 address 161.26.138.0/24
- sng01 address 10.200.144.0/20
- sng01 address 161.26.76.0/22
- sng01 address 161.26.78.0/24
- syd01 address 10.202.46.0/24
- syd01 address 161.26.80.0/22
- syd01 address 161.26.82.0/24
- syd01 address 161.26.168.0/22
- syd01 address 161.26.170.0/24
- syd01 address 166.9.52.0/23
- syd04 address 130.198.64.0/18
- syd04 address 161.26.124.0/22
- syd04 address 161.26.126.0/24
- syd04 address 166.9.54.0/23
- syd05 address 10.202.30.0/24
- syd05 address 161.26.164.0/22
- syd05 address 161.26.166.0/24
- syd05 address 166.9.56.0/23
- tok02 address 10.201.174.0/24
- tok02 address 10.3.79.0/24
- tok02 address 161.26.84.0/22
- tok02 address 161.26.86.0/24
- tok02 address 161.26.87.0/24
- tok02 address 166.9.40.0/23
- tok04 address 161.26.152.0/22
- tok04 address 161.26.154.0/24
- tok04 address 166.9.42.0/23
- tok05 address 161.26.156.0/22
- tok05 address 161.26.158.0/24
- tok05 address 166.9.44.0/23
- tor01 address 10.202.96.0/20
- tor01 address 10.202.110.0/24
- tor01 address 161.26.88.0/22
- tor01 address 161.26.90.0/24
- tor01 address 161.26.91.0/24
- tor01 address 166.9.76.0/24
- tor04 address 10.202.189.0/24
- tor04 address 161.26.196.0/22
- tor04 address 161.26.198.0/24
- tor04 address 166.9.77.0/24
- tor05 address 10.202.205.0/24
- tor05 address 161.26.200.0/22
- tor05 address 161.26.202.0/24
- tor05 address 166.9.78.0/24
- wdc01 address 161.26.16.0/22
- wdc04 address 10.201.10.0/24
- wdc04 address 10.3.175.0/25
- wdc04 address 161.26.92.0/22
- wdc04 address 161.26.94.0/24
- wdc04 address 161.26.132.0/22

- wdc04 address 161.26.134.0/24
- wdc04 address 166.9.20.0/23
- wdc04 address 166.9.231.0/24
- wdc06 address 161.26.118.0/24
- wdc06 address 161.26.120.0/22
- wdc06 address 166.9.22.0/23
- wdc06 address 166.9.232.0/24
- wdc06 address 166.9.251.64/27
- wdc07 address 161.26.122.0/24
- wdc07 address 161.26.132.0/22
- wdc07 address 166.9.24.0/23
- wdc07 address 166.9.233.0/24
- wdc07 address 166.9.251.96/27

SSL VPN network (on back-end/private network)

ICMP – ping (for support troubleshooting)

All TCP/UDP ports (for access from your local workstation)

SSL VPN data centers

Data center	City	IP range	Endpoint
ams03	Amsterdam	10.3.220.0/24	vpn.ams03.softlayer.com
che01	Chennai	10.200.232.0/24	vpn.che01.softlayer.com
dal08	Dallas	100.101.128.0/24	vpn.dal08.usgov.softlayer.com
dal10	Dallas	10.200.228.0/24	vpn.dal.softlayer.com
dal12	Dallas	10.200.216.0/22	vpn.dal.softlayer.com
dal13	Dallas	10.200.212.0/22	vpn.dal.softlayer.com
fra02	Frankfurt	10.2.236.0/24	vpn.fra.softlayer.com
fra04	Frankfurt	10.3.196.0/24	vpn.fra.softlayer.com
lon04	London	10.200.196.0/24	vpn.lon.softlayer.com
lon06	London	10.3.200.0/24	vpn.lon.softlayer.com
mad02	Madrid	10.1.56.0/24	vpn.mad.softlayer.com
mad04	Madrid	10.1.60.0/24	vpn.mad.softlayer.com
mil01	Milan	10.3.216.0/24	vpn.mil01.softlayer.com
mon01	Montreal	10.3.224.0/24	vpn.mon01.softlayer.com
osa22	Osaka	10.202.132.0/24	vpn.osa.softlayer.com
osa23	Osaka	10.202.136.0/24	vpn.osa.softalyer.com

par01	Paris	10.3.236.0/24	vpn.par01.softlayer.com
par04	Paris	10.201.236.0/24	vpn.par.softlayer.com
par06	Paris	10.201.220.0/24	vpn.par.softlayer.com
sao04	São Paulo	10.202.8.0/24	vpn.sao.softlayer.com
sao05	São Paulo	10.202.12.0/24	vpn.sao.softlayer.com
sjc03	San Jose	10.3.204.0/24	vpn.sjc.softlayer.com
sjc04	San Jose	10.200.192.0/24	vpn.sjc.softlayer.com
sng01	Jurong East	10.2.192.0/23	vpn.sng01.softlayer.com
syd01	Sydney	10.3.228.0/24	vpn.syd.softlayer.com
syd04	Sydney	10.200.200.0/24	vpn.syd.softlayer.com
tok04	Tokyo	10.201.228.0/24	vpn.tok.softlayer.com
tok05	Tokyo	10.201.224.0/24	vpn.tok.softlayer.com
tor04	Toronto	10.1.0.0/24	vpn.tor.softlayer.com
tor05	Toronto	10.1.4.0/24	vpn.tor.softlayer.com
wdc03	Washington D.C.	100.101.132.0/24	vpn.wdc03.usgov.softlayer.com
wdc04	Washington D.C.	10.3.212.0/24	vpn.wdc.softlayer.com
wdc07	Washington D.C.	10.200.204.0/24	vpn.wdc.softlayer.com

Table 9: SSL VPN data centers

Legacy networks

IP range
12.96.160.0/24
66.98.240.192/26
67.18.139.0/24
67.19.0.0/24
70.84.160.0/24
70.85.125.0/24
75.125.126.8
209.85.4.0/26
216.12.193.9

216.40.193.0/24
216.234.234.0/24

Table 11: Legacy networks

Red Hat Enterprise Linux server requirements

If your server uses a Red Hat Enterprise Linux (RHEL) license provided by IBM Cloud infrastructure, provisioning is dependent on completing the following actions:

- Complete the SSL VPN requirements listed in Service network (on back-end/private network).
- Open the RHEL endpoint rhha01.updates.us-south.iaas.service.networklayer.com. This requires adding the IP 161.26.112.28 to the firewall rules. Since DNS round robin is involved, this endpoint is not a single endpoint and could be moved as needed.
- Allow access to the service network as follows. Otherwise, updates and licensing do not function properly.

Server location	Allow private service network for this data center
Amsterdam (ams03)	fra02
Chennai (che01)	tok02
Dallas (dal05, dal09, dal10, dal12, dal13)	dal09
Frankfurt (fra02, fra04, fra05)	fra02
London (lon02, lon04, lon05, lon06)	lon02
Milan (mil01)	fra02
Montreal (mon01)	mon01
Paris (par01)	fra02
San Jose (sjc01, sjc03, sjc04)	dal09
Sao Paulo (sao01)	dal09
Singapore (sng01)	syd01
Sydney (syd01, syd04, syd05)	syd01
Tokyo (tok02, tok04, tok05)	tok02
Toronto (tor01)	mon01
Washington DC (wdc01, wdc04, wdc06, wdc07)	mon01
Any data center not listed	dal09

Table 12: Red Hat Enterprise Linux server requirements

⚠ **Important:** To resolve common provisioning issues, permit access to the entire service network by allowing the IP 161.26.0.0/16.

Windows VSI server requirements

If you have a firewall, you must allow your Windows VSI to access to WSUS server IP address ranges as follows; otherwise, updates and licensing do not function properly.

- wsustok0401.service.softlayer.com is 10.201.177.200
- wsustok0201.service.softlayer.com is 10.3.65.50
- wsustok0501.service.softlayer.com is 10.201.193.200

Data Center	City	BCR IP Range
tok04	Tokyo	10.3.17.0/24 10.192.0.0/16 10.201.187.0/24

Table 13: Windows VSI server requirements

For more information about locating your WSUS server in the Windows registry by using a registration key, see Configuring Automatic Updates by editing the registry or Configure Clients in a Non–Active Directory Environment .

1. The 10.1.129.0/24 subnet, within the 10.1.128.0/19 master subnet, is used for Global service virtual IPs, which are not located in dal05. ↩
2. **Note:** Directionality is from the customer compute perspective. Outbound means leaving your account towards the service. Inbound means service reaching out to compute. ↩

FAQs for Hardware Firewall

The following frequently asked questions can help you when you work with your Hardware Firewall.

What is a firewall?

A firewall is a network device that is connected upstream from a server. The firewall blocks unwanted traffic from a server before the server is reached.

Why use a firewall?

The primary advantage of having a firewall is that your server handles only “good” traffic. This means that your resource is solely being used for its intended purpose as opposed to handling unwanted traffic, too.

What firewall products does IBM offer?

You can find a detailed comparison of all firewall products that are offered in Exploring firewalls.

Is the Hardware Firewall compatible with IBM's load balancer products?

Yes. The Hardware Firewall is compatible with the cloud load-balancing service, local load balancer, and the Citrix Netscaler VPX and MPX.

Can portable IP’s be protected by the Hardware Firewall?

No. Portable IPs are not available for protection because they can be moved between servers. Exceptions are made on a case-by-case basis as there are numerous caveats and require more details about the customer's system design.

Can I have a Hardware Firewall and a Network Gateway associated with the same VLAN?

No, it is not possible to have a Hardware Firewall and a Network Gateway device that is assigned to the same VLAN. The expanded functions of the Network Gateway device provide firewall features for your network in place of a standard firewall.

Does public traffic pass through my load balancer or Hardware Firewall first?

Coming from the public internet in, the load-balancing products are first. The Hardware Firewall products are next, and the NetScaler products are last (along with the customers' servers).

Does a server's uplink port speed need to match the Hardware Firewall?

The Hardware Firewall does need to match the public uplink speed of the server. However, because it protects only the public side of the network, the public uplink speed is what must match the firewall selection. Customers can create a case to request a downgrade of only the public interfaces if wanted.

Does IBM Cloud charge for firewall bandwidth?

The Hardware Firewall and FortiGate Security Appliance (FSA) 1G are not metered for bandwidth. FSA 10G is charged for firewall bandwidth after 20 TB is used. Also, these products can reduce total bandwidth use by limiting the traffic that servers must respond to.

How do I upgrade the uplink of my Hardware Firewall?

The Hardware Firewall is locked to the public uplink port speed of a server. You can upgrade in place by cancelling the firewall, upgrading the port speed for the server, and ordering a new firewall. Alternatively, you can deploy a new server with the wanted uplinks and associated firewall.

Is High Availability possible with the Hardware Firewall?

No. The Hardware Firewall platform is enterprise-grade and highly durable, but true High Availability (redundant devices) is not an option for the Hardware Firewall. For HA, a Hardware Firewall (High Availability) or FortiGate Security Appliance (High Availability) is required. The Network Gateway product also has an HA option with firewall capabilities.

I am running a hypervisor on an IBM Cloud server. Will the Hardware Firewall protect the virtual machines that run on my hypervisor?

No. Portable IPs are used for the VMs in a hypervisor environment and portable IPs are not protected by the hardware firewall. A FortiGate Security Appliance is recommended.

What are the unavailable ports in my Windows Firewall?

IBM Cloud offers many different services that you can use with your server, including EVault, SNMP, and Nagios monitoring. These services require that our internal systems communicate with your server to some degree. The unavailable ports that you see in the Exceptions list are ports that are open on the internal network port only. They are still blocked on the public (internet) network connection. Because the internal network is a secured network, having these ports open is considered secure.

These ports generally cannot be modified; however, if you reset the firewall rules, it clears them from the Exceptions list. Beware that resetting the firewall rules might have an adverse effect, not only on these additional services, but also might cause other issues with your server (depending on its current configuration).

What Hardware Firewall options are available for 10 Gbps servers?

FSA 10G is the only option to support 10 Gbps servers for both public and private traffic. If 10 Gbps is only required on the private network (for database, backup, storage, and so on), then customers can request a downgrade of only their public uplinks and order any of the Hardware Firewall products.

What IP ranges do I allow through the firewall?

For the list of IP addresses and IP ranges to allow through the firewall, go here.

What VPN options are included with each firewall product?

Not all firewalls offer VPN and not all VPN options are the same. The general options for VPN are:

- Each customer receives unlimited SSL VPN connections to our private network. These connections can be established by clicking the VPN link while logged in to the IBM Cloud console.
- IBM Cloud also offers a basic multi-tenant IPsec VPN service.
- The FortiGate Security Appliance 1G provides SSL and IPsecVPN options with Public network access only (no access to the IBM Cloud Private network). FSA 10G provides SSL and IPsecVPN options with Public or Private network access.
- The Network Gateway provides SSL, IPsec, and OpenVPN capabilities on the public or private network
- The NetScaler products can provide SSL and IPsecVPN on the public or private network.
- Customers can also deploy a VPN solution on to a server within their IBM Cloud environment.

Which firewall products support public-to-private NAT, private VLAN segmentation, or both?

Fortigate Security Appliance 10G supports NAT and private VLAN segmentation. The other firewall offerings support only public traffic.

Known limitations with Hardware Firewall

Review limitations when you work with your Hardware Firewall.

A Hardware Firewall cannot be deployed to a server on a VLAN that meets any of the following criteria.

- Is associated with a Network Gateway, Hardware Firewall, or FortiGate Security Appliance.
- Contains 30 or more servers.
- Has a primary subnet that is larger than a /28.
- Contains a bare-metal server that hosts a gateway, such as a Juniper vSRX or VRA, as these servers are deployed on a transit VLAN.

In these instances, a new VLAN must be established for the Firewall or another product must be selected.

Further limitations for the Hardware Firewall include:

- Portable subnets are not protected
- Not available for 10 Gb servers
- Maximum of 79 firewall rules per Hardware Firewall
- Incompatible with Windows network load balancing due to the way ARP is processed
- The rule destination subnet is limited to the public IP of the protected server.
- The VLAN for the primary public IP that is protected by the hardware firewall cannot be associated or routed through another gateway, such as a Juniper vSRX or VRA.

Getting help and support for Hardware Firewall

If you experience an issue or have questions when you use Hardware Firewall, you can use the following resources before you open a support case.

- Review the FAQs.
- Review known limitations.
- Check the status of the IBM Cloud platform and resources by going to the Status page.

If you still can't resolve the problem, you can open a support case. For more information, see Creating support cases.

Providing support case details for Virtual Router Appliance

To ensure a timely resolution to your issue, include the following information in your support case for issues with your Hardware Firewall:

1. The public IP address of the server this issue affects.
2. To track down where an issue is happening across a network connection, we generally request the source IP address, destination IP address, the destination port and protocol, and the relevant output from network tools such as `ping`, `traceroute`, `mtr`, or `nmap` and `netcat`.
3. Hardware Firewalls can affect traffic on the same VLAN as other servers that do not have a Hardware Firewall applied. As a result, indicate whether the affected server has a Hardware Firewall that is applied, or if it is only on the same VLAN as another server with a Hardware Firewall applied.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
2024-10-15

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

IBM products are warranted according to the terms and conditions of the agreements under which they are provided.