Introduction to Security Groups

Description

This article provides an overview of Security Groups, an optional feature in Private Cloud and Hosted Private Cloud data center locations.

- Introduction to Security Groups
- Availability of Security Groups
- Understanding Security Group Types and Behavior
- Security Group Maximums
- VLAN Security Group "How To" Articles
- Server Security Group "How To" Articles
- Security Groups and Usage Reporting

Introduction to Security Groups

Normally, IP traffic on a given VLAN ("intra-VLAN") is unrestricted -- any IP address on a VLAN can communicate with any other IP address on the same VLAN. Such traffic is not governed by Firewall Rules because the firewall functionality only manages IP traffic between VLANs ("inter-VLAN") or between a VLAN and the Public Internet or CPNC connection(s). Firewall rules do not police intra-VLAN traffic between addresses on the same VLAN.

Security Groups allow users to isolate Cloud Server NICs on the same VLAN from each other, preventing them from communicating. It essentially provides the equivalent of a "deny all traffic" rule between NICs in different Security Groups. With this functionality, users can create "groups" of NIC IP addresses that can communicate with each other but cannot communicate with other NIC IP addresses on the same VLAN.

In many cases, setting up multiple VLANs and isolating traffic by placing the NICs on separate VLANs is easier and provides more flexibility than isolation through Security Groups. As long as the IP traffic you wish to govern is between separate VLANs instead of within the same VLAN, you can use the **IP Address List** function (see Introduction to Firewall IP Address and Port Lists) to accomplish the same type of traffic restrictions. Such an implementation also provides additional flexibility since you can specify specific traffic ports or protocols for which you do want to allow traffic. However, if such a configuration is not an option, **Security Groups** provide an alternative.

For example, imagine a scenario where a user is running applications related to two separate companies - ACME Inc. and Widget Inc. The application for each company is run on a separate set of Cloud Servers, but these dedicated servers also need to communicate to a centralized billing engine. For security reasons, the user wants to isolate each company's dedicated Cloud Servers from each other while still allowing access to the centralized billing engine. Using Security Groups, they can achieve these goals as follows:

- *Create a Security Group called "ACME" and put the NICs/Servers associated with the ACME Inc. into that group*
- *Create a Security Group called "Widget" and put the NICs/Servers associated with the Widget Inc. into that group*
- *Leave the NICs associated with the centralized billing engine out of any Security Group, allowing them to communicate with NICs/Servers in both security groups*
    - *NOTE: If the centralized billing engine is placed on a different VLAN, communication will be governed by the firewall rather than its security group membership.*

Use of Security Groups incurs usage under the **Security Group Hours** element as described in the "Security Groups and Usage Reporting" section below.

Availability of Security Groups

Security Groups is an optional feature available in some MCP 2.0 locations. You can identify whether or not a given location is enabled for the feature by checking its capabilities and seeing if "VLAN/Server Security Groups" is enabled. For more information, see How do I Identify Hardware Specifications and Capabilities Available in a Data Center Location

In data center locations where this feature is enabled, Security Groups are available on both Advanced and Enterprise Network Domains.

Understanding Security Group Types and Behavior

There are two different types of Security Groups:

1. **VLAN Security Groups** allow you to isolate different Cloud Server NICs on a single VLAN from each other
2. **Server Security Groups** allow you to isolate all NICs on different Cloud Servers from each other on all VLANs

Normally, IP traffic on a given VLAN ("intra-VLAN") is unrestricted -- any IP address on a VLAN can communicate with any other IP address on the same VLAN. Security Groups modify this behavior to impose an "all or nothing" set of rules around traffic within a VLAN. The rules can be summarized as follows:

1. NICs on the same VLAN that are not in a Security Group at all can communicate with any NIC on the VLAN. They are not isolated from any other NIC.
2. NICs on the same VLAN that are in **different** VLAN Security Groups or in **different** Server Security Groups cannot communicate with each other. This implies:
    a. NICs in the same VLAN Security Group or Server Security Groups can communicate with each other
    b. NICs on the same VLAN where one Cloud Server is in a VLAN Security Group and another is in a Server Security Group can also communicate with each other. The Security Group feature only prevents communication between NICs in different Security Groups of the same type.
3. All of the above functions apply on to traffic in the same VLAN. Traffic between VLANs is always controlled by the firewall.

It may be easier to understand this behavior with examples:

VLAN Security Group Example

VLAN Security Groups are designed for scenarios where users want to isolate traffic on a single VLAN or a subset of VLANs. For example, let's have a Scenario Where

1. Server 1 has three NIC's: one on VLAN A, one on VLAN B, and one on VLAN C
2. Server 2 has three NIC's: one on VLAN A, one on VLAN B, and one on VLAN D

- With **VLAN Security Groups,** the security group can only be created at the VLAN level.
- So if user creates two **VLAN Security Groups** on VLAN A and places the VLAN A NIC on Server 1 and VLAN A NIC on Server 2 in different VLAN Security Groups:
    - Both of their NIC's on VLAN A CANNOT communicate with the other.
    - Both of their NIC's on VLAN B CAN communicate with each other because the VLAN A Security Group applies only to VLAN A
        - If the user desires to isolate traffic on VLAN B, then separate VLAN Security Groups would need to be created on VLAN B to isolate this traffic. Alternately, Server Security Groups could be used as described in the next example.
    - All other communication between NICs is between different VLANs and therefore is governed by the Firewall Rules. Their Server Security Group membership is irrelevant.

Server Security Group Example

Server Security Groups are designed for scenarios where users want to isolate traffic on all VLANs. For example, let's use the same scenario as above where:

1. Server 1 has three NIC's: one on VLAN A, one on VLAN B, and one on VLAN C
2. Server 2 has three NIC's: one on VLAN A, one on VLAN B, and one on VLAN D

- Sever Security Groups are created at the Network Domain level and apply to all VLANs.
- If Server 1 and Server 2 are in different Server Security Groups:
    - Both of their NIC's on VLAN A CANNOT communicate with the other.
    - Both of their NIC's on VLAN B CANNOT communicate with each other
    - All other communication between NICs is between different VLANs and therefore is governed by the Firewall Rules. Their Server Security Group membership is irrelevant.

Key points to remember when using Security Groups:

1. Servers can either have NICs that are members of VLAN Security Groups or the servers can be a member of a Server Security Group. You cannot mix the two Security Group types within the same server - *i.e. if the Server is a member of a Server Security Group, none of it's NICs can be part of a VLAN Security Group*.
2. The different Security Group types are not isolated from each other - *i.e. If Server A is a member of a VLAN Security group on VLAN A and Server B is a member of a Server Security Group and has a NIC on VLAN A, these NIC's can communicate with each other on VLAN A.*
3. The traffic restrictions on IP traffic between NICs or Servers in different Security Groups of the same type are absolute - *i.e.. If traffic is prohibited between NICs on the same VLAN because the NICs are in different VLAN groups, then all traffic on all ports/protocols is blocked within that VLAN. Conversely, traffic between NICs not in the same VLAN Security Groups is completely unrestricted.*
4. NICs can only be a member of a single Security Group and no "nesting" of Security Groups is allowed.
5. Remember, these rules only apply to traffic between NICs located on the same VLAN. If the NICs are on different VLANs, then traffic is governed by the firewall rules and Security Group membership is ignored.
    - This means if one NIC is a member of Security Group A on VLAN A and another NIC is a member of Security Group B on VLAN B, traffic between the NICs in Security Group A and Security Group B is governed entirely by the firewall rules. The fact that each NIC is in a different VLAN Security Group is irrelevant because the Security Groups are on different VLANs.

Security Group Maximums

- Security Group names must be at least 1-24 characters in length and cannot contain spaces
- Security Group names must be unique to a given Organization ID and Location
- Each VLAN is limited to a total of 300 Security Groups
- Each data center location is limited to a total of 9,000 Security Groups

VLAN Security Group "How To" Articles

- How to View and Manage VLAN Security Groups on a Network Domain
- How to Add or Remove a Cloud Server NIC to / from a VLAN Security Group
- How to Delete a VLAN Security Group

Server Security Group "How To" Articles

- How to View, Create, and Manage Server Security Groups on a Network Domain
- How to Add or Remove a Cloud Server to / from a Server Security Group
- How to Delete a Server Security Group

Security Groups and Usage Reporting

Security Groups usage is reported under the usage element **Security Group Hours** and appears on the Summary Usage Report described at How to Create a Summary Usage Report.

A report showing how Security Group Hours are calculated is available as described at: How to Create a Security Group Usage Report

Security Group Hours start accruing starting from the time that either:

- A Cloud Server is added to a **Server Security Group**, or
- The first Server NIC is added to a **VLAN Security Group**

Security Group Hours will continue to accrue until either the Cloud Server is removed from a Security Group or all Server NICs on a given Cloud Server are removed from Security Groups.

When the first NIC on a Server is added to a **VLAN Security Group**, **Security Group Hours** will start accruing. **Security Group Hours** will appear on the Security Group Usage Report as being associated with this NIC. If another NIC on the same server is added to another VLAN Security Group, no additional usage will be incurred. In other words, **Security Group Hours** are only incurred once per Server, regardless of how many NICs (must be >1) on that Server are members of a Security Groups.

There is a scenario where Users may see a change in which NIC is associated with their **VLAN Security Group**. Example: *A Server has 2 NICs, NIC A, and NIC B. NIC A is added to VLAN Security Group "Bob". NIC B is then added to VLAN Security Group "Elvis". On the **Security Groups Usage Report**, Users will see one line item with NIC A showing **Security Group Hours** starting from when NIC A was added to VLAN Security Group "Bob". There will be no entry in the report when NIC B is added to a VLAN Security Group "Elvis" because NIC A already has **Security Group Hours** associated with it. At a later date, the User decides to remove NIC A from Security Group "Bob". At that point, **Security Group Hours** will stop accruing for NIC A, but will start accruing for NIC B. Users will see two new lines on the Security Group Usage report, one that shows the number of hours in that day when NIC A had Security Group Usage, stopping when NIC A was removed from the Security Group, and another line that shows NIC B started accruing Security Groups Usage.*

The screenshot below illustrates this example:

Location	Server Name	Server Id	Start Time	End Time	Security Group Name	Security Group Type	Security Group Id	Security Group Hours
NA9	Server A	07daedca-102f-49ed-8d7a-610434ee8fe3	6/19/18 4:16	6/20/18 0:00	Bob	VLAN	07da5dca-102f-49ed-42dh-610434ee8fe3	19.8
NA9	Server A	07daedca-102f-49ed-8d7a-610434ee8fe3	6/20/18 0:00	6/21/18 0:00	Bob	VLAN	07da5dca-102f-49ed-42dh-610434ee8fe3	24
NA9	Server A	07daedca-102f-49ed-8d7a-610434ee8fe3	6/21/18 0:00	6/21/18 10:42	Bob	VLAN	07da5dca-102f-49ed-42dh-610434ee8fe3	10.7
NA9	Server A	07daedca-102f-49ed-8d7a-610434ee8fe3	6/21/18 10:42	6/22/18 0:00	Elvis	VLAN	52da5dca-203g-49ed-42dh-610434ee8ac2	13.4
NA12	Server B	0fb3ebb7-45eb-4783-bca6-814eb9b8ec76	6/22/18 3:42	6/23/18 0:00	Sales	SERVER	32ab5dca-102f-49ed-42dh-610434ee8fe5	20.3
NA12	Server B	0fb3ebb7-45eb-4783-bca6-814eb9b8ec76	6/23/18 0:00	6/24/18 0:00	Sales	SERVER	32ab5dca-102f-49ed-42dh-610434ee8fe5	24
NA12	Server B	0fb3ebb7-45eb-4783-bca6-814eb9b8ec76	6/24/18 0:00	6/24/18 12:00	Sales	SERVER	32ab5dca-102f-49ed-42dh-610434ee8fe5	12