Security Zones

What are Security Zones?

A Security Zone is a list of Gateways, Computers, or IP addresses that are defined and grouped together. This group now becomes a zone on the Gateway Network, which can have additional policies and restrictions placed on it. While Users and Roles restrict access to specific functions within the Gateway like making certain controls read-only for certain users and read/write for others, Security Zones provide this functionality to the Gateway Network, limiting locations instead of people to be read-only for specific actions. This allows for greater control over the type of information that is passing over the network, improving security and helping to keep different areas of the business separate, while still allowing them to interconnect.

On this page

...

- What are Security Zones?
  - Using Security Zones
- Defining a Security Zone
  - Identifiers
  - Qualifiers
- Service Security

Security Zones and Service Security

Watch the Video

Using Security Zones

Sometimes, in addition to knowing who the user is, it is important to know where they are sending a command from. An operator may have permissions to turn on a machine from an HMI, but if the operator were to login to a project on a different Gateway in the network that had remote access to those Tags, it might not be a good idea to let the operator write to those Tags. From the remote location , the operator can't see if the physical machine is clear to run.

This is where Security Zones come in. While Security Zones themselves don't define the security, they instead define an area of the Gateway Network, breaking up Gateways and network locations into manageable zones that can then have a security policy set on them. Once there are zones defined, a security policy can be assigned to each zone, and a priority of zones can be set in the event that more than one zone applies in a given situation.

> When using zone-based security in a project, the project stores the name of the security zone as a string. This means that if you were to modify the name of the zone in the gateway, the zone-based security in your project will not update to reflect the new name, and instead will try searching for a zone with the original name. Be very careful when modifying the names of security zones.

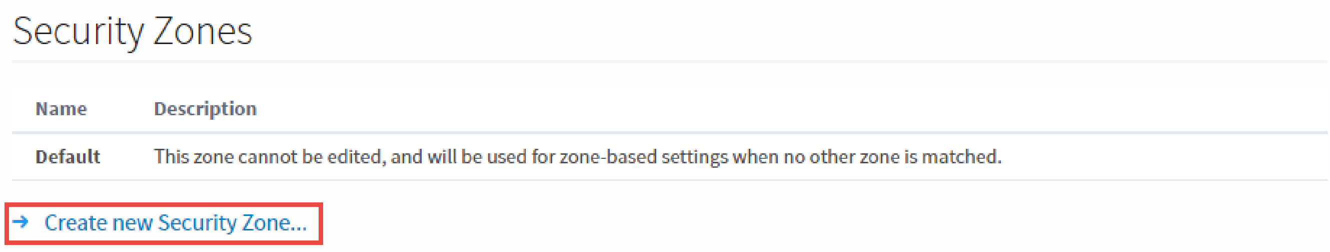
Defining a Security Zone

When setting up a new Security Zone, it might be a good idea to setup a Gateway Network first if you haven't already. While Security Zones can be defined and used without a connected Gateway, they work best when used in conjunction with other Gateways on a Gateway Network, so it is a good idea to setup a Gateway Network first.

Security Zones are defined in the **Configure** section of the Gateway webpage by going to **Security > Security Zones**.

> There is a special zone called Default. It is always present and can't be modified, and will be used if an incoming connection does not match any of the other defined zones.

Selecting the **Create new Security Zone** link brings up a new page where the Security Zone can be defined.

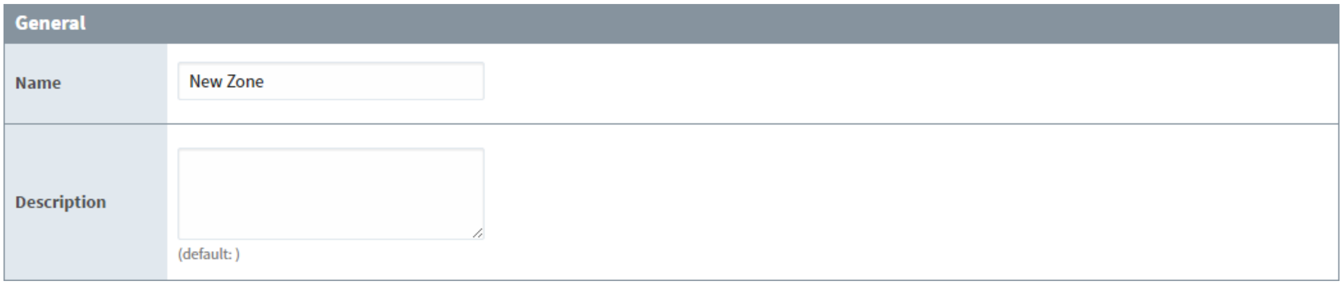


Security Zones

Name	Description
Default	This zone cannot be edited, and will be used for zone-based settings when no other zone is matched.

→ Create new Security Zone...

Besides the name and description, there are two major sections here: Identifiers and Qualifiers. These are two forms of checks that need to happen before an incoming connection gets placed in a Security Zone.



General	
Name	New Zone
Description	(default:)

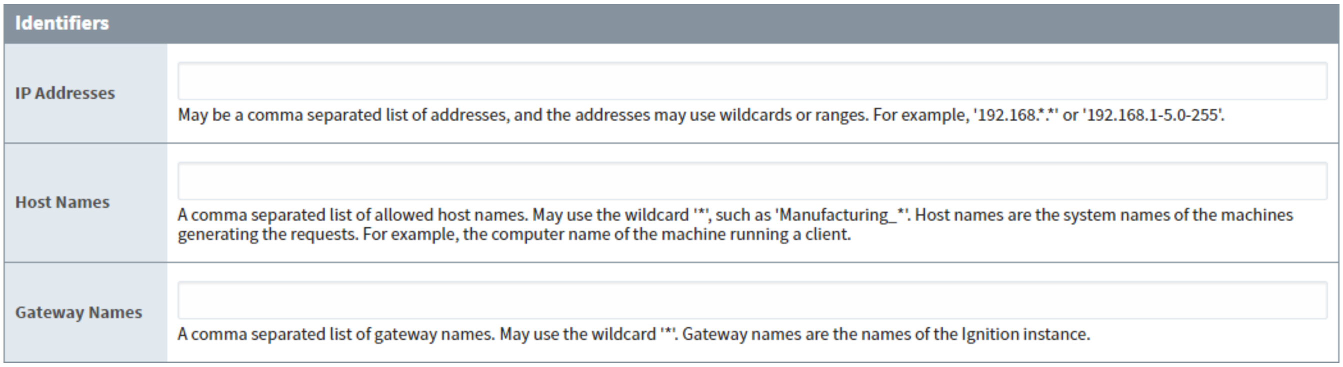
Identifiers

The identifiers are how incoming connections are distinguished between different zones. While there are a few different ways to define the incoming connection, it only needs to match one of them to match this zone.

- **IP Addresses** - This defines an IP address that the connection is coming from. This can be a list of IP addresses by using commas to separate them. It can also make use of the (*) wildcard like '192.168.100.*', or use a range such as '100.100.1-100.0-255'. With IP addresses, virtually all connections can be listed. Use 127.0.0.1 for the local connection.
- **Host Names** - The host name refers to the system name of the machine generating the request such as Joe_Workstation. This can be a list of names separated by commas, and it can also use the (*) wildcard like '*_Workstation'.
- **Gateway Names** - The Gateway name is the name of the Ignition instance. This is set in the **Configure** section by going to **System > Gateway Settings**, and changing the System Name. This can be a comma separated list and can use the wildcard such as '* Ignition Gateway'.

Many incoming connections can be defined using any of the three identifiers, or even multiple at once. As mentioned before, an incoming connection only needs to match one of the identifiers for it to be accepted.

> When identifying a Gateway through a proxy Gateway, the IP Address should be using the ip of the proxy, but the Gateway Name should use the name of the Gateway we are trying to identify.



Identifiers	
IP Addresses	May be a comma separated list of addresses, and the addresses may use wildcards or ranges. For example, '192.168.*.*' or '192.168.1-5.0-255'.
Host Names	A comma separated list of allowed host names. May use the wildcard '*', such as 'Manufacturing_*'. Host names are the system names of the machines generating the requests. For example, the computer name of the machine running a client.
Gateway Names	A comma separated list of gateway names. May use the wildcard '*'. Gateway names are the names of the Ignition instance.

Qualifiers

After first being identified as part of a particular Security Zone, the connection then must check the Qualifiers. With the Qualifiers, the incoming connection needs to fit in with all of the properties before it is fully placed into the Security Zone.

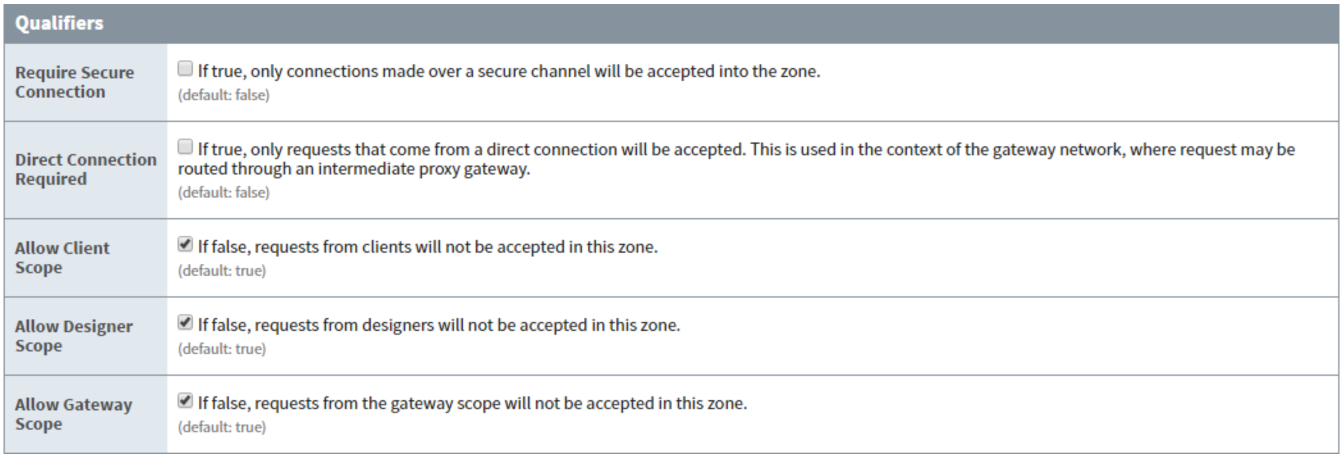
- **Require Secure Connection** - If this is true, only connections that are made over a secure channel will be accepted.

  > A Security Zone is only able to check connections made to the gateway the zone is defined on. This means that connections through a proxy Gateway may not be secure.

- **Direct Connection Required** - If this is true, only connections that come from a direct connection will be accepted. The Gateway Network allows you to connect three Gateways in a 1-2-3 configuration, where Gateway 1 can see Gateway 3 through the proxy Gateway 2.
- **Allow Client Scope** - If this is false, Clients will not be placed in the zone.
- **Allow Designer Scope** - If this is false, Designers will not be placed in the zone.
- **Allow Gateway Scope** - If this is false, any Gateway scoped requests will not be placed in the zone.

As mentioned above, a connection must pass all of the qualifier checks before being accepted into a Security Zone. So if Require Secure Connection was checked, and Allow Client Scope was not, any requests coming from Clients would be rejected even if they are secure, and the same goes for any non-secure connections coming from sources other than a Client.

Requests can be a part of more than one zone, depending on how the zones are setup. This can be useful for making a whole section of IP addresses read only, but a specific Gateway in that IP address range may be listed specifically in another zone, which can be given read/write access. Any connection which does not fall into one of the zones will be placed in the Default zone.



Qualifiers	
Require Secure Connection	□ If true, only connections made over a secure channel will be accepted into the zone. (default: false)
Direct Connection Required	□ If true, only requests that come from a direct connection will be accepted. This is used in the context of the gateway network, where request may be routed through an intermediate proxy gateway. (default: false)
Allow Client Scope	☑ If false, requests from clients will not be accepted in this zone. (default: true)
Allow Designer Scope	☑ If false, requests from designers will not be accepted in this zone. (default: true)
Allow Gateway Scope	☑ If false, requests from the gateway scope will not be accepted in this zone. (default: true)

Service Security

After creating some Security Zones, a Security Policy can then be defined for each zone. This can be found by going to the **Configure** section and navigating to **Security > Service Security**. At first, none of the zones will have a policy defined, and the Default zone will be at the top. Editing any of them will bring up the Security Policy definition page for that zone. The Security Policy has four sections: Alarm Notification, Alarm Status, History Provider Access, and Tag Access. They work together to define how the local Gateway gives access to incoming Gateway connections. All four sections also have the ability to completely block access to specific services with the Service Access setting in each section. Setting that to deny will deny the zone access to that particular information, regardless of what the rest of the options are set to.

It is important to realize that if you have a single Gateway, limiting access of certain clients to certain Tags is still done in the individual Tags.

- **Alarm Notification** - The Accessible Pipeline Filter setting is a list of Pipelines in the current Gateway that other connections can use for alarm notification. Note that this setting is an inclusionary list not an exclusionary list, meaning that if there are no pipelines listed there, then all of them will be available. The list is a comma separated list, and it can make use of the (*) wildcard.
- **Alarm Status** - The Allow Acknowledge setting will allow the Gateways that fall within the zone to acknowledge alarms on the local Gateway.

  This feature is new in Ignition version **7.9.7**
  Click here to check out the other new features

  The Allow Shelving setting will allow the Gateways that fall within the zone to Shelve alarms on the local Gateway. IE: Other Gateways can shelve alarms on this Gateway. For this Gateway to shelve alarms on others, this must be set on the remote Gateway.

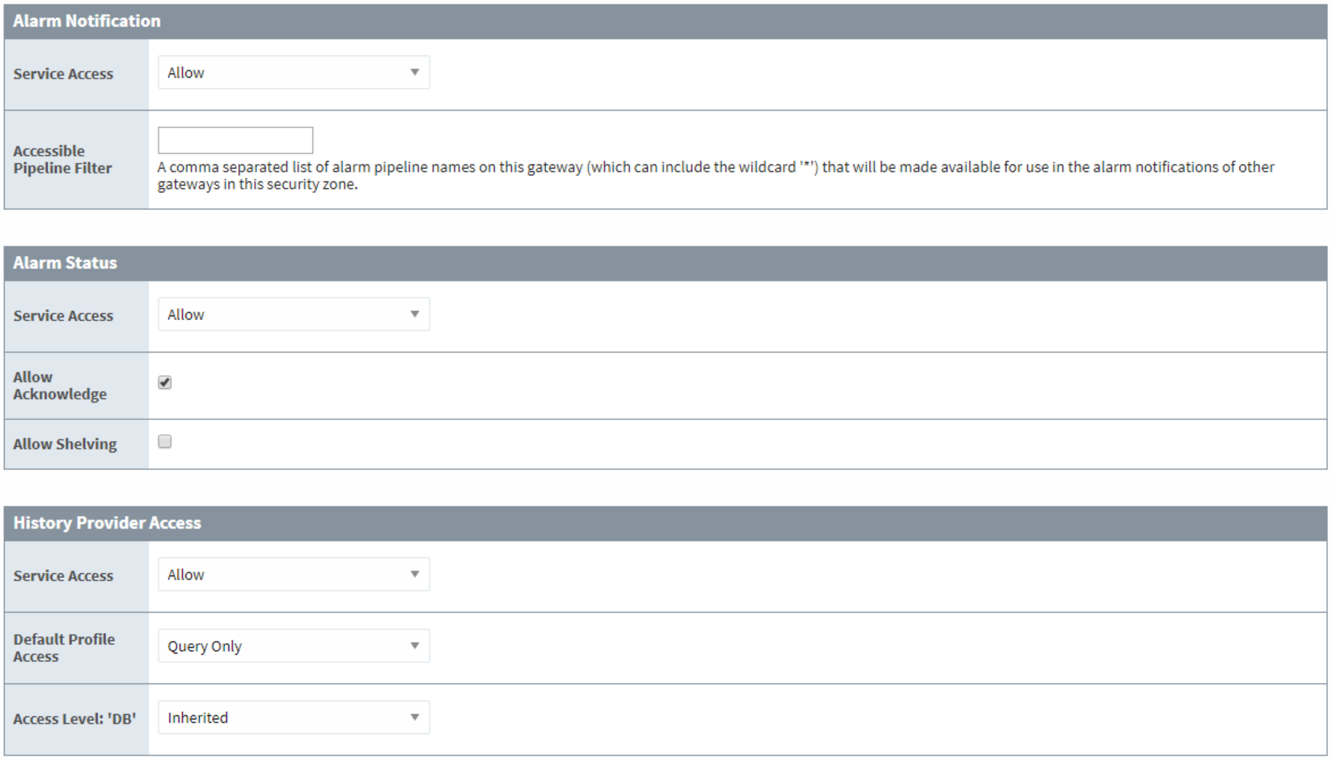
- **History Provider Access** - The History Provider Access has two different settings. First, it has a Default Access Profile. This is the default access rights for Tag History. Second, there will be a setting for each History Provider setup on the local Gateway. In the picture below, there is an "Access Level: 'New Connection" that can be set that corresponds to the History Provider that was created when a database was connected. It can be set to Query and Storage, which will allow connections in the current zone to both run queries and store Tag History against the Tag History provider, Query Only, which will only allow the zone to query out history data, but not store it, and No Access, which will completely block access to that History Provider. The final setting is Inherited, which will inherit the Default Profile Access rights. Any new history providers will automatically get added to the security policy set at inherited so it may be beneficial to set the Default Profile Access to be either Read Only or No Access so that a recently added history provider does not accidentally get storage rights when it should not.

  The Default Access Profile should not be set to Inherited. This also goes for the Default Provider Access Level in the Tag Access section.

- **Tag Access** - The Tag Access also has a few different settings. The Default Provider Access Level, which works the same as the History Provider Default Access Profile. It sets the default access rights for realtime providers. It will then have a setting for each provider configured in the local Gateway, as well as an additional one for system Tags. These can be set to **ReadWriteEdit**, which will allow connections in the current zone to read, write to, and edit the Tags in that provider, **ReadWrite**, which allows the zone to read and write to Tags, and **ReadOnly**, which only allows the zone to read the Tags. It also can be set to None, which will prevent the zone from interacting with the Tag Provider altogether, and Inherited, which will again inherit the access rights set in the Default Provider Access Level. Any new Tag Providers will automatically get added to the security policy with Inherited access rights.

This feature is new in Ignition version **7.9.1**
Click here to check out the other new features

The Trust Remote Roles setting will allow similarly named roles on other Gateways to access Tags with role specific security on them.



Alarm Notification

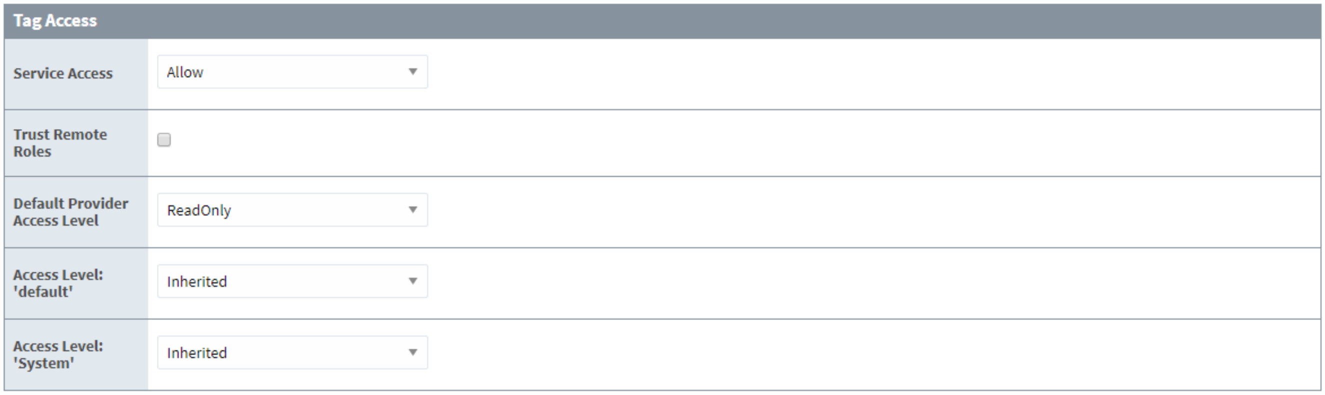
Service Access	Allow
Accessible Pipeline Filter	A comma separated list of alarm pipeline names on this gateway (which can include the wildcard '*') that will be made available for use in the alarm notifications of other gateways in this security zone.

Alarm Status

Service Access	Allow
Allow Acknowledge	☑
Allow Shelving	☐

History Provider Access

Service Access	Allow
Default Profile Access	Query Only
Access Level: 'DB'	Inherited



Tag Access

Service Access	Allow
Trust Remote Roles	☐
Default Provider Access Level	ReadOnly
Access Level: 'default'	Inherited
Access Level: 'System'	Inherited

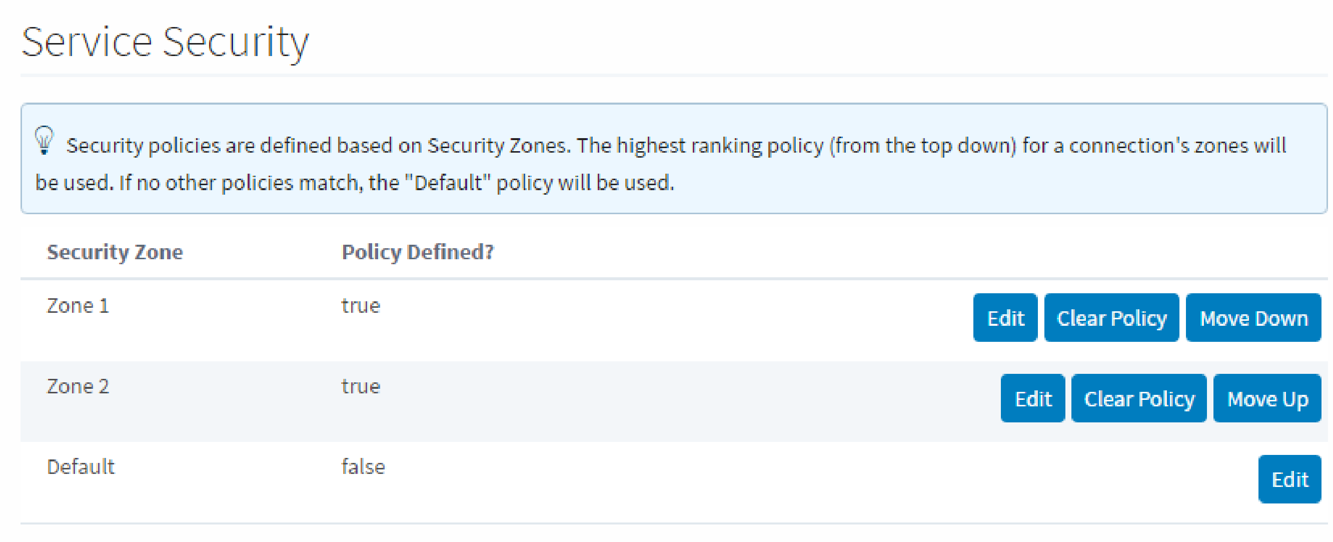
Default Security Zone

While the Default zone may not have a custom security policy defined, it does default to not include any notification pipelines, allow alarm acknowledgment, query only history access, and read only Tag access. This means that if a remote Tag Provider is setup on a remote Gateway, and the local Gateway has not changed the default security settings, the remote Gateway will have read only access to the

Tag History Provider. This can be changed by editing the Default zone's security policy to fit a different preference, or creating new Security Zones with custom security policies. Once a security policy has been defined on a zone, it will automatically jump to the top of the list. A new option will also become available that will clear the policy from the zone.

Setting Zone Priority

Once a security policy has been defined for two or more zones, a new option appears on the Service Security page to move the zones up and down the list. This allows a priority to be set on the Security Zones, since a connection can apply to multiple zones. For example, say Zone 2 dictates that all requests coming from a range of IP addresses have query only history access, and read write access to Tags. Zone 1 includes specific Gateways, one of which is also contained in Zone 2, that will have query and storage history access and read write edit access to Tags. When a request comes in from a connection, it first determines which Security Zones it belongs to. The request then starts at the top of the Service Security list and goes down until it finds the first zone that it is in, and uses the access rights of that zone. In our example, we want to make sure Zone 1 is above Zone 2, so that the Gateway that is in both Zone 1 and Zone 2 gets the full access rights afforded to it by the security policy of Zone 1 instead of getting the limited access rights from Zone 2.



Service Security

Security policies are defined based on Security Zones. The highest ranking policy (from the top down) for a connection's zones will be used. If no other policies match, the "Default" policy will be used.

Security Zone	Policy Defined?
Zone 1	true
Zone 2	true
Default	false

Related Topics ...

- Client Security
- Gateway Security