AWS Security Group Guidance for Practitioners

Working with Existing Security Groups

The AWS Governance and Information Security teams have created standard security groups that address requirements for access to the AWS infrastructure and the University's most commonly used web applications. The following security groups have been created to address requirements for access to the infrastructure and the most commonly used web applications. When planning to create a new security group, check to see if one of the existing standard security groups will meet your needs. Many times practitioners start crafting new security groups not realizing that an existing security group already meets their communication requirements

Before creating new security groups, it is important for the practitioner to have a clear understanding of the AWS infrastructure design , otherwise the infrastructure itself and other systems can be put at risk. Always have a copy of the most up-to-date production architectural diagram as a reference when working with security groups.

Security Group Naming Convention

Security group names must follow the AWS Governance naming standard. all security group **names** must start with "**sgp**", for security group policy, followed by the two letter acronym for the **vpc** in which a security group will be used; next is the **access level**, the **source** and finally, the **services** provided. The name components must always be in this order (see below)

sgprefix + vpc + access level + source + services

Keep on reading for some good examples.

Changes to Standard Security Groups

Cloud deployment trends indicate that smaller security perimeters and the use of security groups at a container level will further reduce potential attacks. You will be notified and this documentation will reflect any change to the AWS security infrastructure.

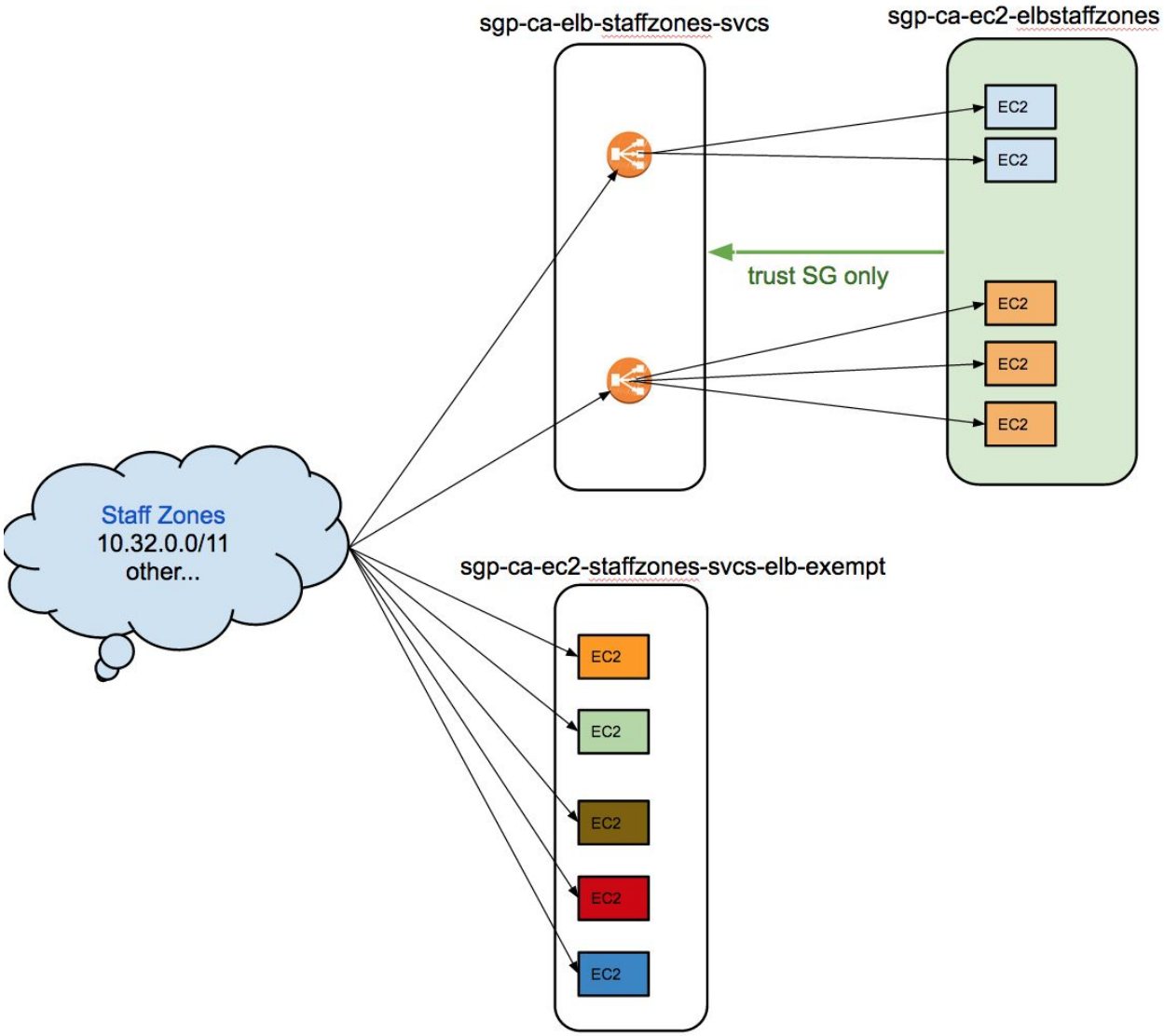
The following security groups can serve as guidance for practitioners when working with existing security groups. They can also serve as a reference when trying to create new security groups. Please note that these have been organized by VPC in the production DCND account and do not reflect all VPCs in this account.

Shared Services	
sgp-ss-elb-public-web	Ingress web related access coming from 0.0.0.0 to elastic load balancers in Shared Services public
sgp-ss-ec2-elbpublic-web	Ingress trust access from sgp-ss-elb-public-web security group
sgp-ss-ec2-public-web-elb-exempt	Ingress public web access for webapps that are not fronted by an elastic load balancer
sgp-ss-private-allvpcs-dbsvcs	Ingress database services access allowed from all internal vpc subnets
sgp-ss-vpc-dcinternal-any	Ingress open access coming from all internal data center related networks
sgp-ss-vpc-ssjumpbox-engr	Ingress sysdadmin open access coming from Shared Services Private jumpbox group to Shared Services vpc
Consolidated Applications	
sgp-ca-elb-staffzones-svcs	security group for ingress trust access from campus staff zones only
sgp-ca-ec2-elbstaffzones	ec2 security group fronted by elb sg servicing staff zones only
sgp-ca-ec2-staffzones-svcs-elb-exempt	Ingress staff zones access for applications that are not fronted by an elastic load balancer
sgp-ca-elb-campus-web	Ingress web access coming from campus to elastic load balancers in CA campus
sgp-ca-ec2-elbcampus-web	Ingress trust access from elbcampus security group
sgp-ca-ec2-campus-web-elb-exempt	Ingress campus web access for webapps that are not fronted by an elastic load balancer
sgp-ca-elb-world-web	Ingress web access coming from 0.0.0.0 to elastic load balancers in CA world
sgp-ca-ec2-elbworld-web	Ingress trust access from elbworld security group
sgp-ca-ec2-world-web-elb-exempt	Ingress world web access for web applications that are not fronted by an elastic load balancer

sgp-ca-private-cavpc-dbsvcs	Ingress database access coming from CA vpc subnets to CA private database related subnets
sgp-ca-private-nat-egress	From systems in Consolidated Applications requiring egress access through a nat system
sgp-ca-vpc-ssjumpbox-engr	Ingress sysdadmin open access coming from Shared Services Private jumpbox group to Consolidated Application subnets

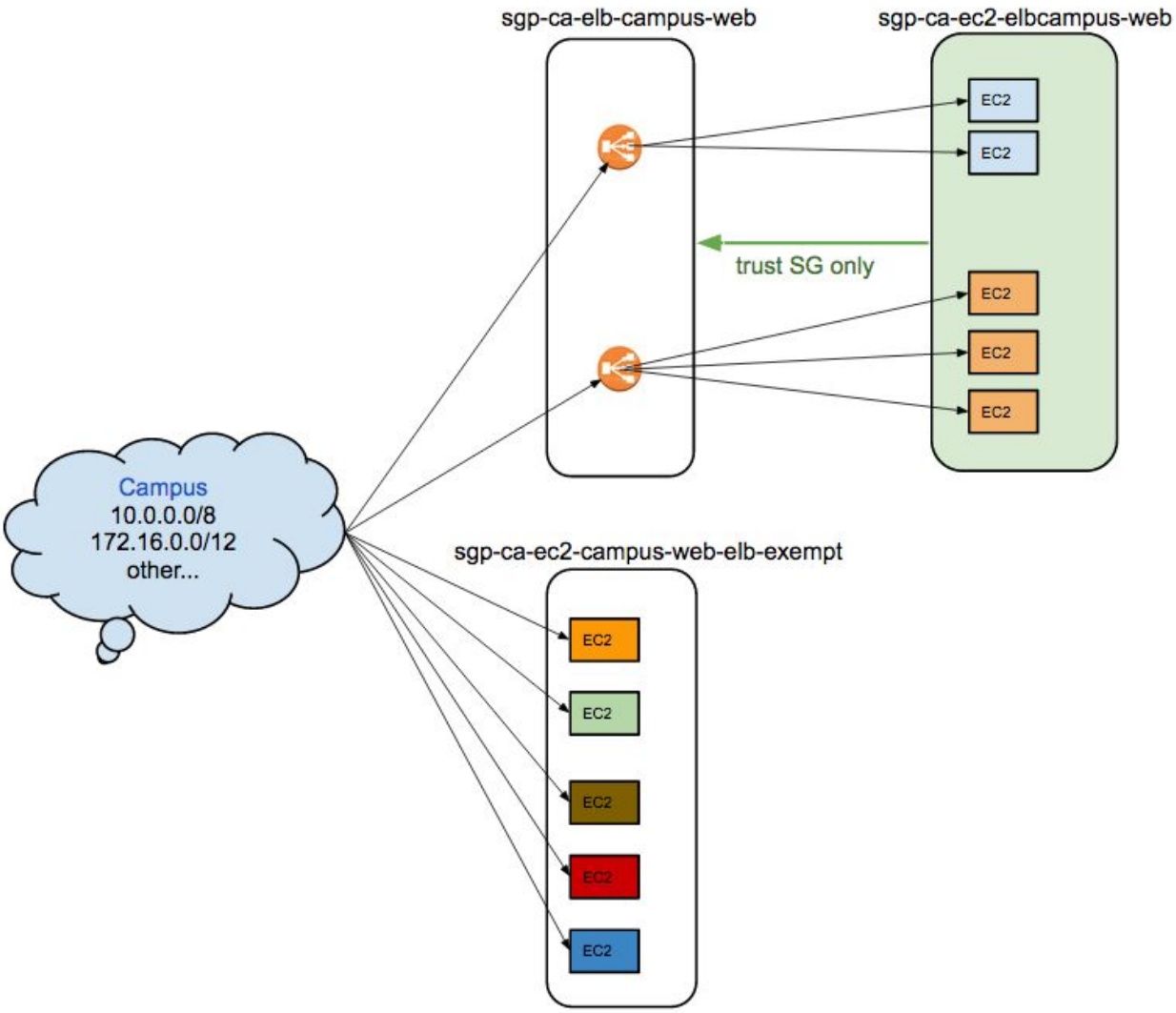
The following graphic illustrates an example and the relationship between the following three security groups:

sgp-ca-elb-staffzones-svcs,
sgp-ca-ec2-elbstaffzones,
sgp-ca-ec2-staffzones-svcs-elb-exempt



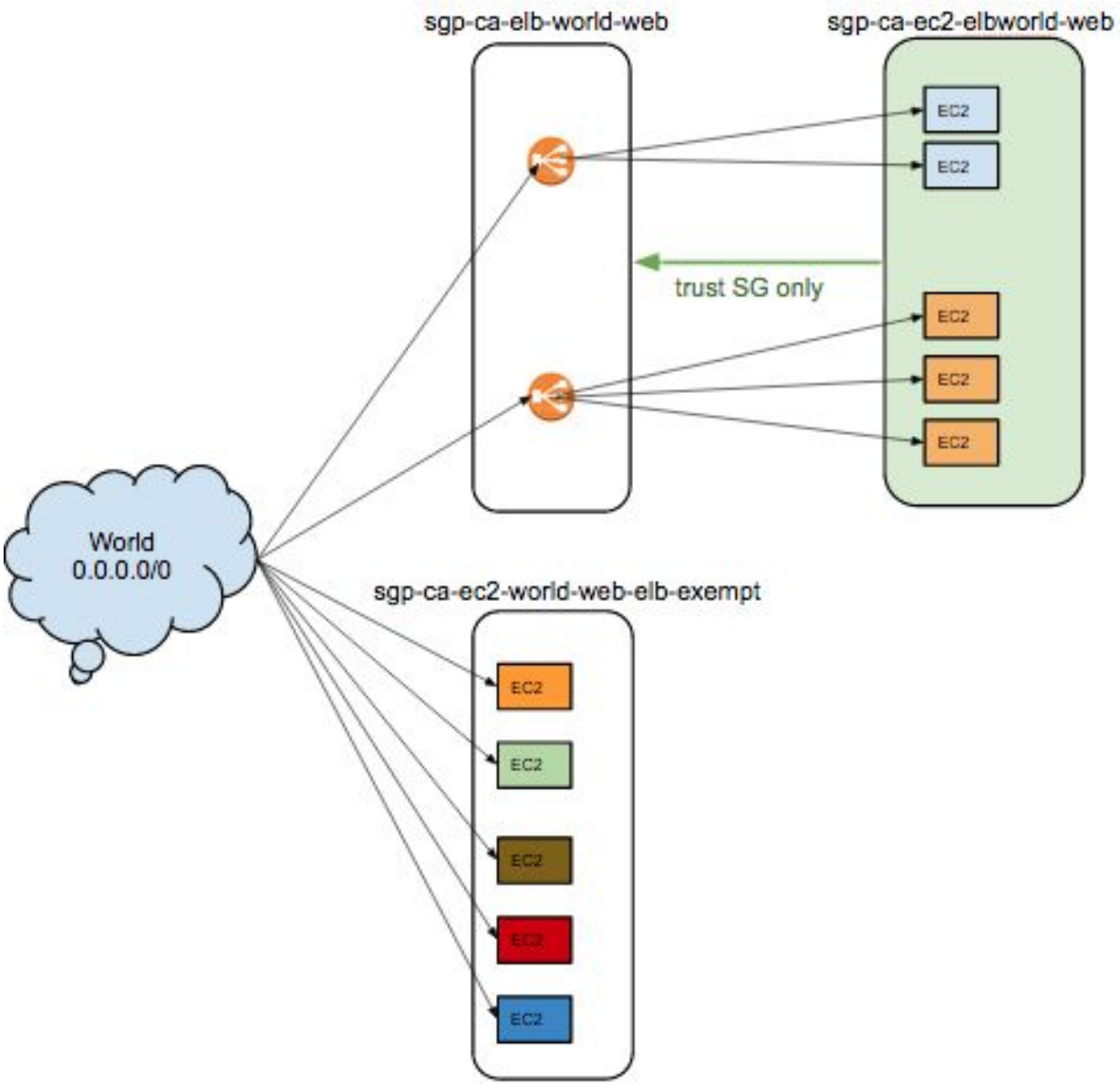
The following graphic illustrates an example and the relationship between the following three security groups:

sgp-ca-elb-campus-web,
sgp-ca-ec2-elbcampus-web,
sgp-ca-ec2-campus-web-elb-exempt



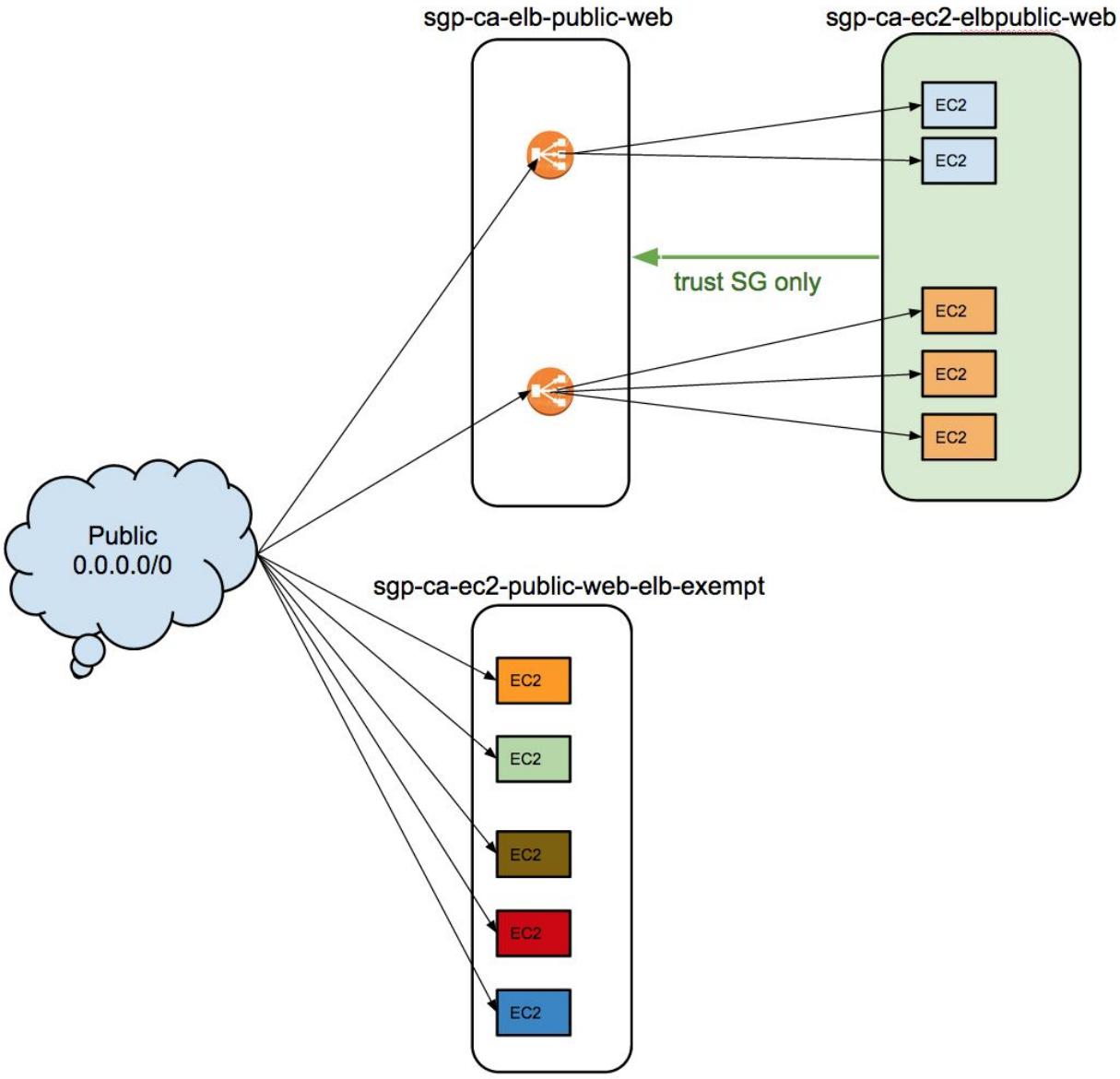
The following graphic illustrates an example and the relationship between the following security groups:

sgp-ca-elb-world-web,
sgp-ca-ec2-elbworld-web,
sgp-ca-ec2-world-web-elb-exempt



The following graphic illustrates an example and the relationship between the following three security groups:

sgp-ca-elb-public-web,
sgp-ca-ec2-elbpublic-web,
sgp-ca-ec2-public-web-elb-exempt



Security Group Rules

The best way to work with security groups is to understand which security group rules are already available to the practitioner. Security group rule inventories will be generated on a regular basis for the practitioner for guidance. Such rules will be presented to the practitioner in a human readable CSV format.

The following table is a simple illustration for rules contained security groups hosted in Shared Services Private. These are sorted by source CIDR notation. Please note that a value of “-1” represents “all”. For a reference of source networks other than 0.0.0.0/0 please refer to network documentation provided by the networking team.

SG-GroupName	Source	FromPort	ToPort	Protocol	Direction
sgp-ss-private-ssjumpbox-engr	x.x.0.0/19	3389	3389	tcp	INBOUND
sgp-ss-private-ssjumpbox-engr	x.x.0.0/19	22	22	tcp	INBOUND
sgp-ss-private-ssjumpbox-engr	x.x.0.0/19	80	80	tcp	INBOUND
sgp-ss-private-ssjumpbox-engr	x.x.0.0/19	1432	1435	tcp	INBOUND
sgp-ss-private-ssjumpbox-engr	x.x.0.0/19	443	443	tcp	INBOUND
sgp-ss-private-ssjumpbox-engr	x.x.0.0/19	1521	1522	tcp	INBOUND
sgp-ss-private-allvpcs-dbsvcs	x.x.224.0/20	1433	1435	tcp	INBOUND
sgp-ss-private-allvpcs-dbsvcs	x.x.224.0/20	1432	1434	udp	INBOUND
sgp-ss-private-allvpcs-dbsvcs	x.x.224.0/20	1521	1522	tcp	INBOUND
sgp-ss-private-allvpcs-dbsvcs	x.x.0.0/16	1433	1435	tcp	INBOUND
sgp-ss-private-allvpcs-dbsvcs	x.x.0.0/16	1432	1434	udp	INBOUND
sgp-ss-private-allvpcs-dbsvcs	x.x.0.0/16	1521	1522	tcp	INBOUND

Expectations before creating new or changing existing security groups

- Before doing any changes related to existing or new security groups, do a sanity check with any member of the Information Security team to analyse the potential risks

associated with increasing the attack surface. In most situations, security groups already exist to meet the application requirements.

- Only after that conversation takes place, a practitioner can continue to implement the planned security group changes.

- Submit and RFC describing your change. The assyst template for AWS security groups is: “**PD_FIREWALL_RULES_AWS**".

- Create an **"RFC" tag** in your security group or if you already have an rfc tag, append the rfc number to your existing tag. Any security group found without an RFC tag reference, will be considered unapproved by Information Security.

Please note that any changes to security groups are closely monitored by the Information Security team.