05- Cisco ASA Firewall

Ahmed Sultan
Senior Technical Instructor
ahmedsultan.me/about

Introduction

- Stateful Firewall systems are a mainstream defense method that can provide a set of effective methods to reduce risk to exposed services and business processes using network segmentation and perimeter filtering.
- Cisco Adaptive Security Appliance (ASA) is a stateful firewall with Application Inspection and Control (AIC) capabilities with a rich set of additional integrated software features that make it a very popular choice of a firewall in many networks.
- As the core functionality, the Cisco ASA appliance provides the administrator with a set of access control methods that can tightly control access between security zones in networks.

Cisco ASA Deployment Types

- The Cisco ASA appliance supports two firewall modes; *routed* and *transparent*, in which it operates and behaves slightly different.
- When you start the Cisco ASA appliance for the first time, the default mode is ***routed mode*** and allows the Cisco ASA appliance to participate in the network as a Layer 3 device.

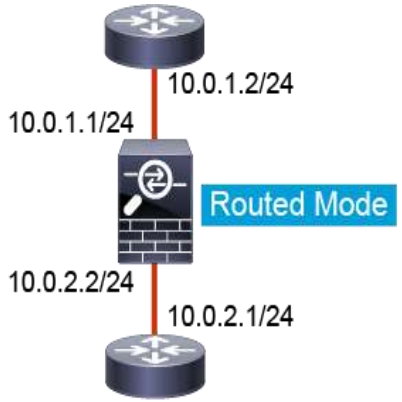


Figure 1

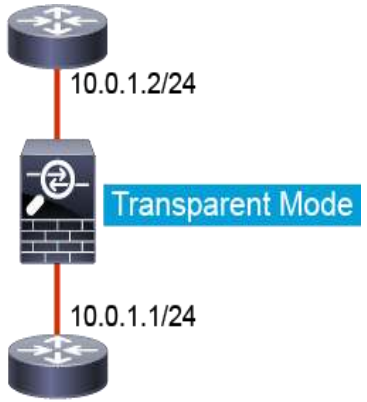
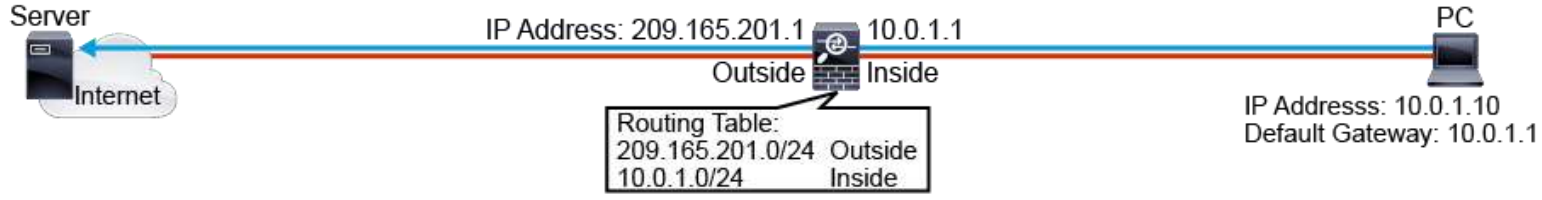


Figure 2

Cisco ASA Deployment Types (cont.)

Routed Firewall Outbound Data Flow

- When the Cisco ASA appliance runs in routed firewall mode, it operates like a Layer 3 device on the network.
- When the security appliance receives traffic on an interface, the security appliance forwards it based on the destination IP addresses of the packets.
- This means that the Cisco ASA appliance checks the routing table first to determine the exit interface, and optionally if configured, the security appliance performs NAT on the same packets. Once this process is finished, the packets are sent to the destination.



Cisco ASA Deployment Types (cont.)

Cisco ASA Appliance Multiple Context Mode

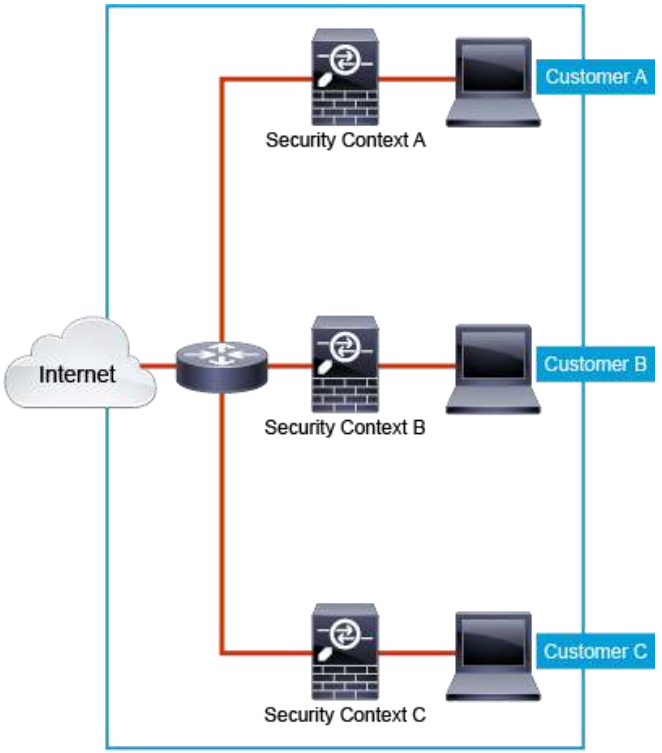
- When you must implement different security policies for traffic from different customers or departments, you can use the virtualization feature supported on the Cisco ASA appliance.
- In each security context, you can configure most of the features that are available on the security appliances configured in single mode.

Cisco ASA Deployment Types (cont.)

Cisco ASA Appliance Multiple Context Mode (cont.)

- The Cisco ASA appliance can operate in two modes, ***single context mode*** which is used by default or ***multiple-context mode***.

- Each security context on the Cisco ASA appliance has its own configuration that identifies the security policy, interfaces, and almost all options that you can configure on a single mode firewall.



Cisco ASA Deployment Types (cont.)

Cisco ASA Appliance Multiple Context Mode (cont.)

Cisco ASA Appliance Context Configuration Files

- In multiple-context mode the Cisco ASA appliance offers multiple separate virtual firewalls. This mode creates three different types of configuration files rather than just one like in single mode:

1. The System Configuration
2. The Admin Context Configuration
3. The Context Configurations for each separate security context

Cisco ASA Deployment Types (cont.)

Cisco ASA Appliance Multiple Context Mode (cont.)

Cisco ASA Appliance Context Configuration Files (cont.)

- The system configuration identifies basic settings for the security appliance, including a list of contexts and the physical settings of its interfaces.
- The system configuration is the startup configuration for a Cisco ASA appliance running in multiple-mode.
- The system configuration does not include network interfaces or IP network settings for the system context itself.

Cisco ASA Deployment Types (cont.)

Cisco ASA Appliance Multiple Context Mode (cont.)

Cisco ASA Appliance Context Configuration Files (cont.)

- When you convert the Cisco ASA appliance from single context mode to multiple context mode, the appliance immediately creates one security context named “admin” that has the administrative role.
- Users who are logged into the admin context are able to change to the system configuration and create new contexts.
- The running configuration of the single mode security appliance is transferred to the admin context. It means that if the single mode security appliance was already configured with management access, the admin context will also be configured with the same management access features.

Cisco ASA Interface Security Levels

- To make the Cisco ASA interfaces operational, you must configure at least the basic interface configuration parameters.
- This includes IP address, interface name, and security levels.
- The security level is very important parameter on the Cisco ASA appliance, because it designates whether an interface is trusted (more protected) or untrusted (less protected) compared to other interface.
- An interface is considered trusted or more protected in relation to another interface if its security level is higher than the security level of the other interface.

Cisco ASA Interface Security Levels (cont.)

- Security levels are numbers that range from 0 (lowest) to 100 (highest).
- On the Cisco ASA appliance, the default access control is based on interface security levels, each interface must have a security level from 0 to 100 configured.

- When you set the name *"Inside"* to an interface,

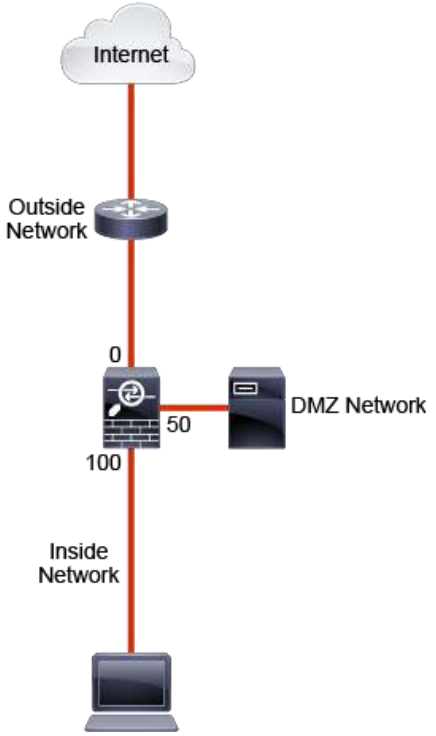
the security level automatically sets to **100** by default

and makes the interface as trusted it can be.

- When you set the name to *"Outside"*

the security level automatically sets to **0** by default

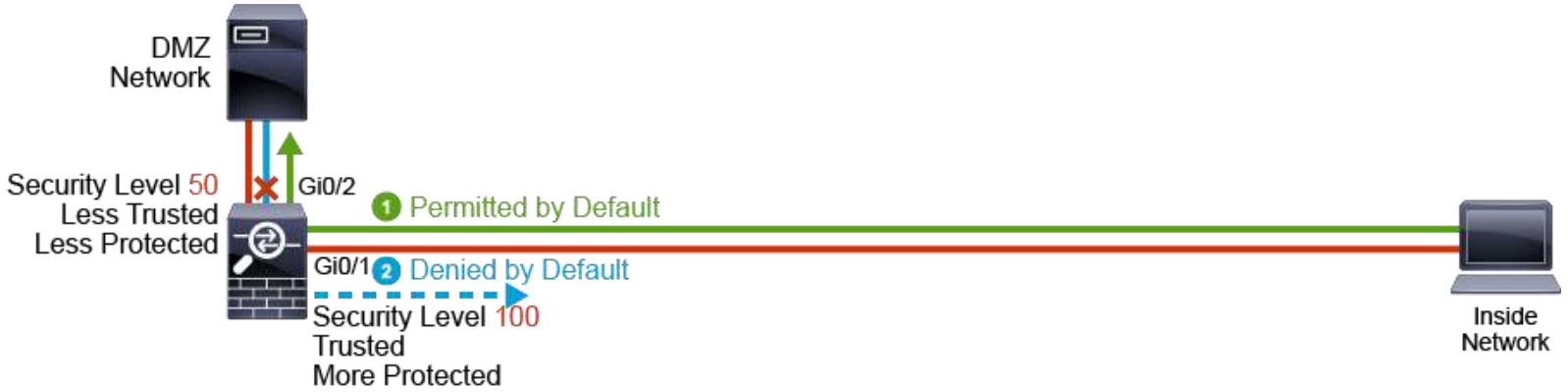
and the interface is less trusted.



Cisco ASA Interface Security Levels (cont.)

Default Security Policy

- Security levels define the level of trustworthiness of an interface. The higher the level, the more trusted the interface is. Traffic flows are defined as inbound or outbound based on the security levels of the incoming and outgoing interfaces of the Cisco ASA appliance:
- **Inbound traffic** travels from a less trusted interface to a more trusted interface.
- **Outbound traffic** travels from a more trusted interface to a less trusted interface.



Cisco ASA Interface Security Levels (cont.)

Default Security Policy (cont.)

- **The primary rule of the Cisco ASA appliance for security levels is that outbound traffic is *allowed by default*.**
  - This means that there is an *implicit permit* for connections initiated from a more trusted interface to a less trusted interface (outbound traffic).

- **The secondary rule of the Cisco ASA appliance for security levels is that inbound traffic is *denied by default*.**
  - This means that there is an *implicit deny* action for connections from a less trusted interface to a more trusted interface (inbound traffic) by default.

Cisco ASA Interface Security Levels (cont.)

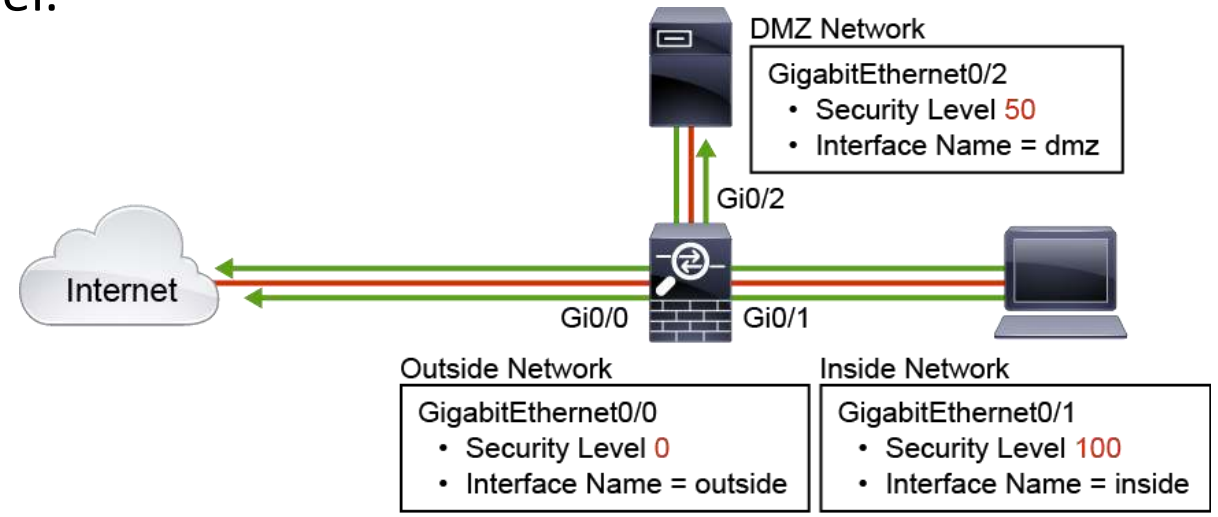
Default Security Policy (cont.)

- Therefore, external hosts connecting on a lower security interface (for example, hosts from the internet) are not allowed to initiate connections to hosts connected on a higher security interface (hosts in the private part of the network).
- However, this default behavior can be ***overridden*** by applying an ACL to an interface that explicitly permits inbound traffic originated from the less trusted interface.

Cisco ASA Interface Security Levels (cont.)

Use Case for Security Levels

- One of the easiest ways to permit or deny communication between different zones on the Cisco ASA appliance is to configure interfaces with different security levels.
- If you want to permit traffic only from the inside network to the DMZ or the outside , while denying traffic in the opposite direction, all you have to do is to configure the inside interface with higher security level.



Cisco ASA Interface Security Levels (cont.)

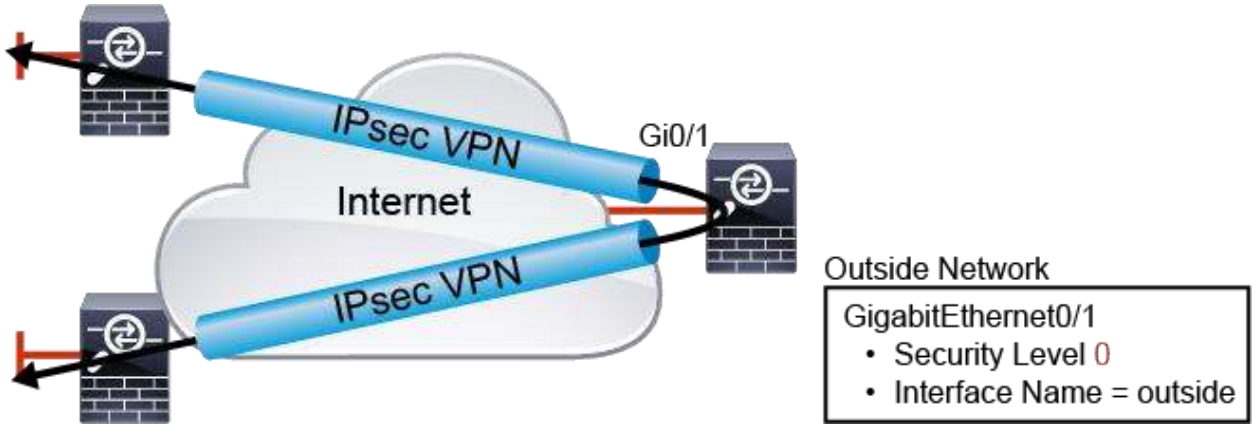
Inter-Interface Communication

- On the Cisco ASA appliance, traffic is not allowed between two interfaces with the same security level by default, even if an ACL with permit statements is applied.
- You can override this default behavior by enabling same-security-level inter-interface communication on the Cisco ASA appliance.

Cisco ASA Interface Security Levels (cont.)

Intra-Interface Communication

- Like the default behavior of the Cisco ASA appliance for limiting inter-interface communication, the same rule applies for intra-interface communication, meaning packets cannot enter and exit the same interface on the Cisco ASA appliance by default.

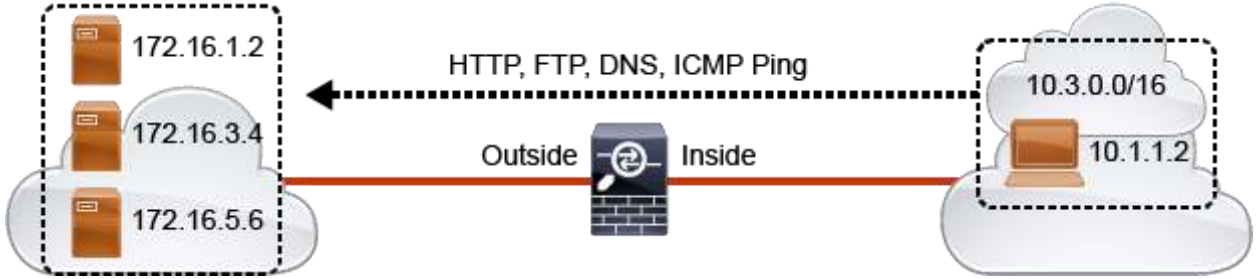


Cisco ASA Objects and Object Groups

- Objects and object groups are reusable components that can be used in many different Cisco ASA configurations, such as access rules or NAT configurations.
- A network object can represent a host, a network, a range of IP addresses, or a fully qualified domain name (FQDN)
- Using object/object groups instead of raw data (IP address, network, and so on) in the configurations, simplifies the overall approach of using the Cisco ASA appliance and making the management of the configurations a lot easier and flexible.

Cisco ASA Objects and Object Groups (cont.)

Objects and Object Groups Deployment



Action	Source Address	Destination Address	Service
PERMIT	10.3.0.0/16	172.16.1.2	HTTP
PERMIT	10.3.0.0/16	172.16.1.2	FTP
…	…		

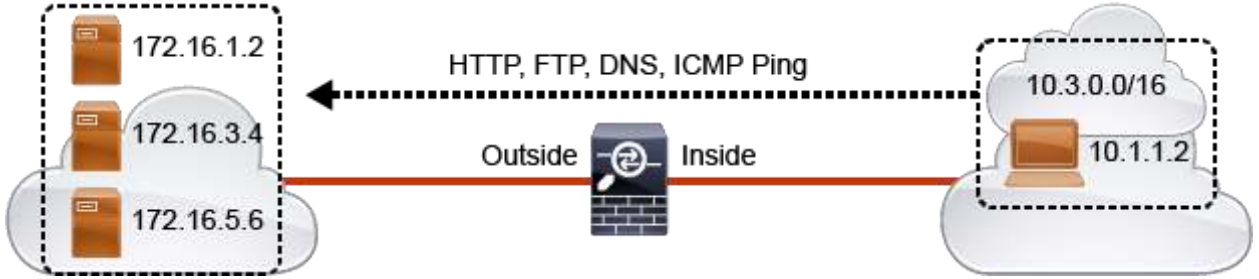
Cisco ASA Objects and Object Groups (cont.)

Objects and Object Groups Deployment (cont.)

- The easiest solution is to create *two network object groups* ,one for the internal sources (the single host and the network) and other for external servers, as well as *one service object group* for the services.
- For example, you can define a network object group named *"Inside_sources"* that will group the host with the 10.1.1.2 IP address and the 10.3.0.0/16 network from the inside.
- Furthermore, additional network object group named *"Outside_servers"* can represent the three external servers, 172.16.1.2, 172.16.3.4, and 172.16.5.6, on the outside.
- Lastly, you can define a service object group for the required services named *"In_to_out_services"* containing TTP, FTP, DNS, and ICMP pings.

Cisco ASA Objects and Object Groups (cont.)

Objects and Object Groups Deployment (cont.)



Action	Source Address	Destination Address	Service
PERMIT	Inside_sources	Outside_servers	In_to_out_services

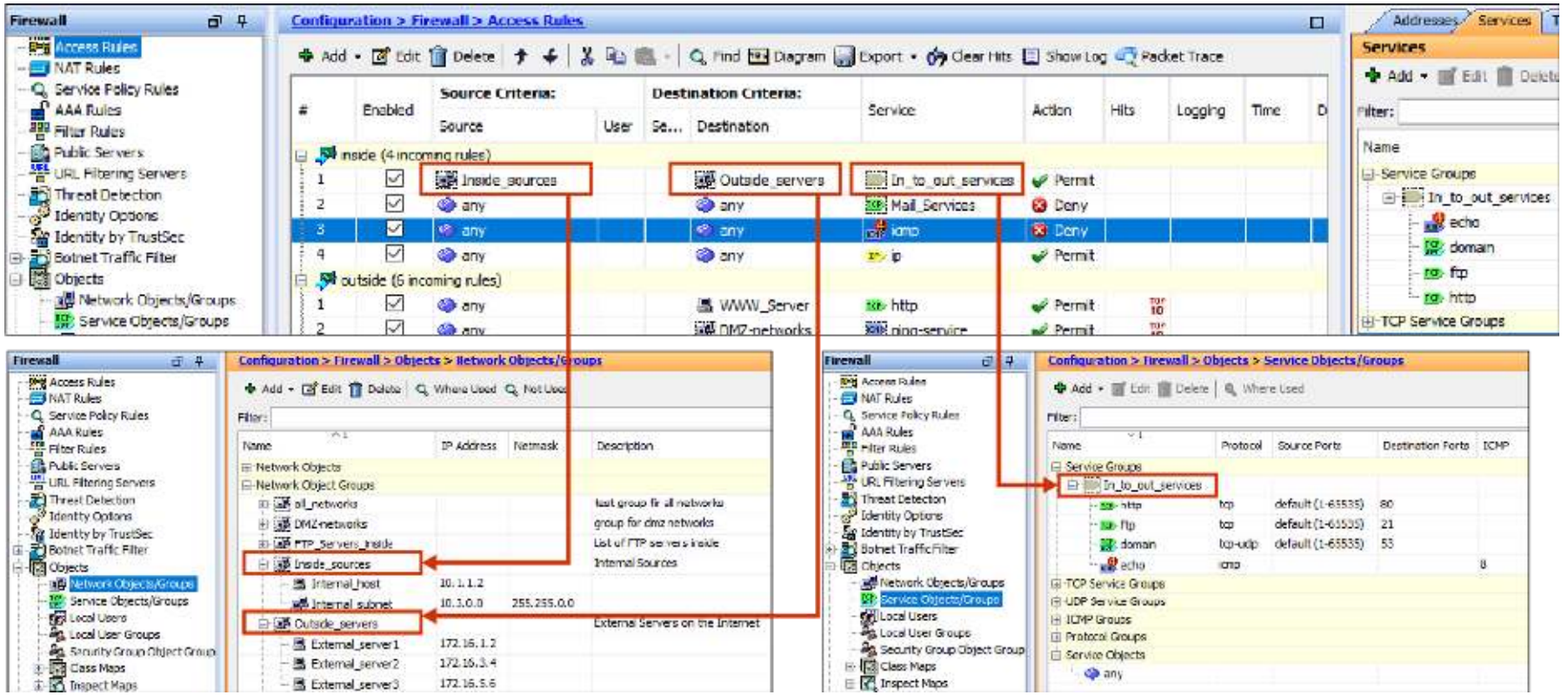
Cisco ASA Objects and Object Groups (cont.)

Objects and Object Groups Deployment (cont.)

- Once the network and service object groups are defined on the Cisco ASA appliance, you can start using them in the ACL configuration.
- Instead of using 24 individual access rules, you can now define just a single access rule to accomplish the same goal.
- You can use the network object group "Inside_sources" as a source, the network object group "Outside_servers" as a destination and the service object group "In_to_out_services" as a service.
- This downsizes the configuration of the ACLs, and makes them more readable and scalable for future use.

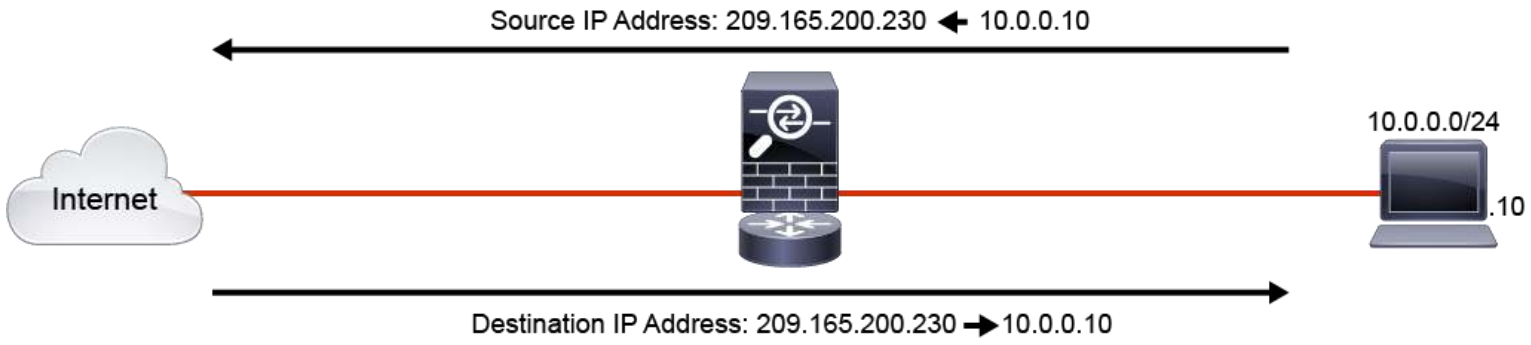
Cisco ASA Objects and Object Groups (cont.)

Objects and Object Groups Deployment (cont.)



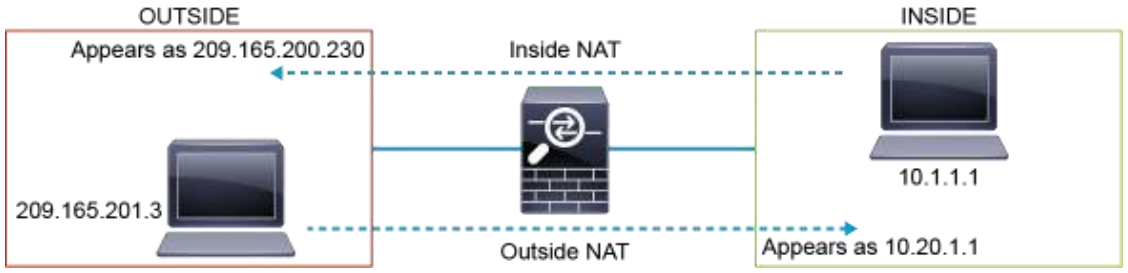
Network Address Translation

- The NAT technology was developed primarily to overcome IPv4 addressing problems that occurred with the expansion of the Internet.
- NAT is required to translate private (local) IPv4 addresses into public (global) routable IPv4 addresses.



Network Address Translation (cont.)

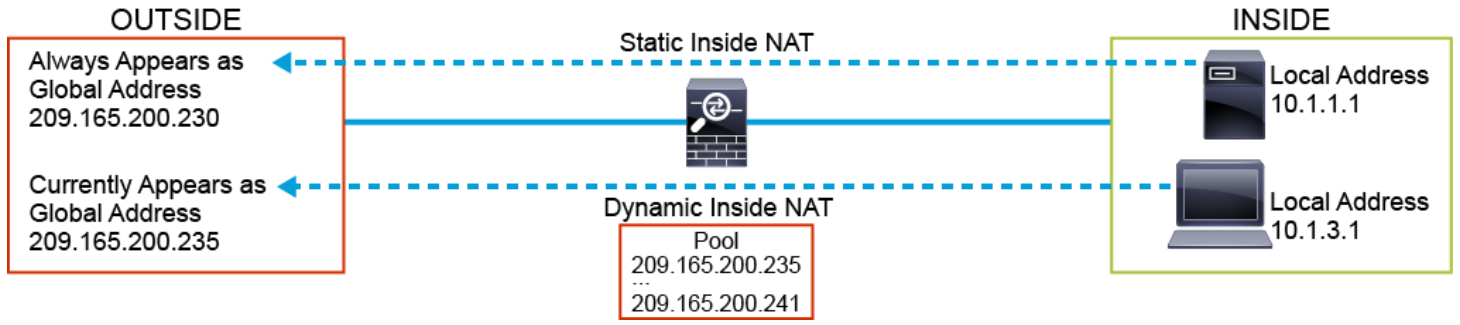
- The Cisco ASA appliance performs *inside NAT* process in which it translates the private (local) addresses of hosts in the inside NAT domain into public (global) addresses as the local hosts communicate with external hosts in the outside NAT domain.
- The Cisco ASA appliance can also perform *outside NAT* process in which it translates the external addresses of hosts in the outside NAT domain to internal addresses while the external hosts communicate with internal hosts in the inside NAT domain.



Network Address Translation (cont.)

NAT Deployment Modes

- **Static NAT** manually map a private to public IPv4 address in the NAT configuration of the Cisco ASA appliance.
- When the internal host sends traffic to the Internet, the source IP address of each packet will always automatically translate to the corresponding mapped public IP address available in the NAT table.



Network Address Translation (cont.)

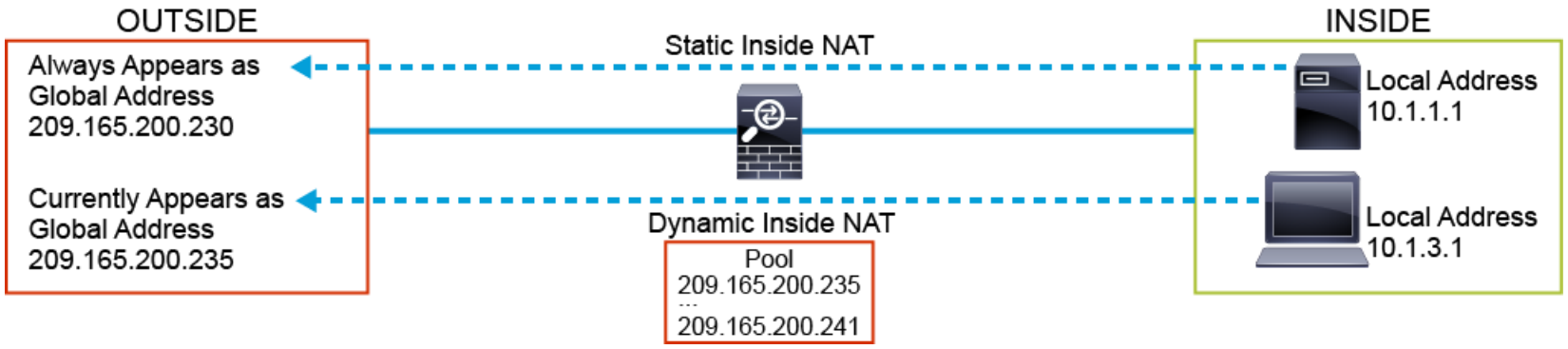
NAT Deployment Modes (cont.)

- **Static NAT** is a one-to-one translation for a host that never changes. When a local host in the inside NAT domain communicates with the outside NAT domain, by using a preconfigured rule, NAT always maps the private IP address of the host to the same public IP address. Static NAT is particularly useful when an internal device must always be accessible on the same public IP address from outside the network.

Network Address Translation (cont.)

NAT Deployment Modes (cont.)

- **Dynamic NAT** is similar to static NAT, because it still uses one-to-one mapping, but instead of statically configuring these mappings in the NAT configuration, the private IP address of the internal host automatically translates to the first available public IP address from a previously configured pool of registered IP addresses.



Network Address Translation (cont.)

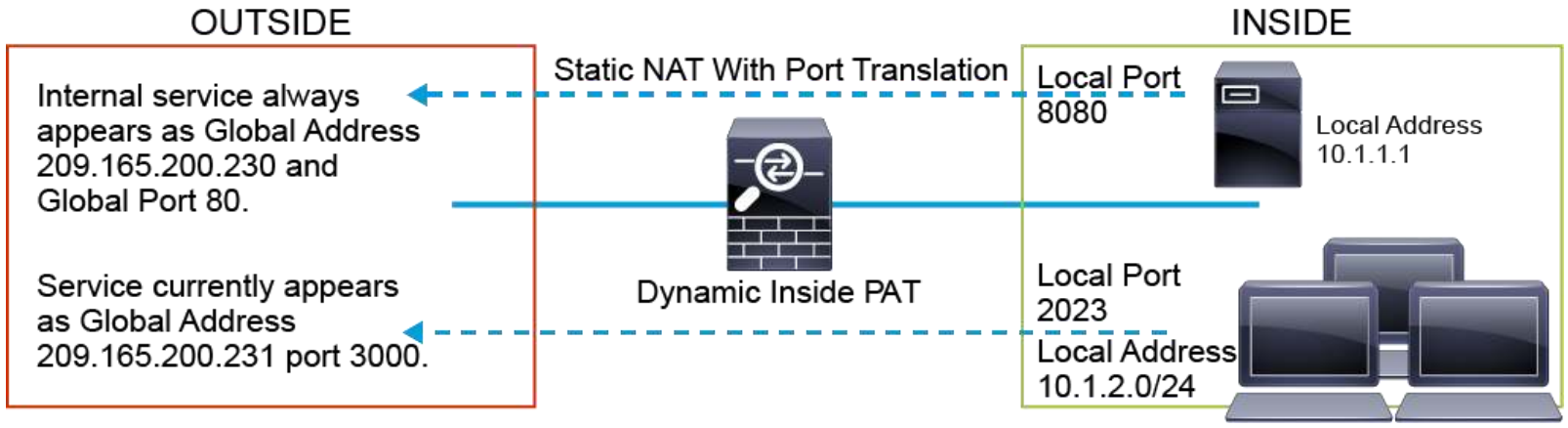
NAT Deployment Modes (cont.)

- **Dynamic NAT** maps a local IP address in the inside NAT domain to a global IP address that is temporarily borrowed from a pool of mapped IP addresses, when the internal host in the inside NAT domain communicates with the outside NAT domain.

Network Address Translation (cont.)

NAT Deployment Modes (cont.)

- **PAT** is sometimes referred to as "NAT overload" and translates individual connections, meaning it alters both the address and one of the host session ports.



Network Address Translation (cont.)

NAT Deployment Modes (cont.)

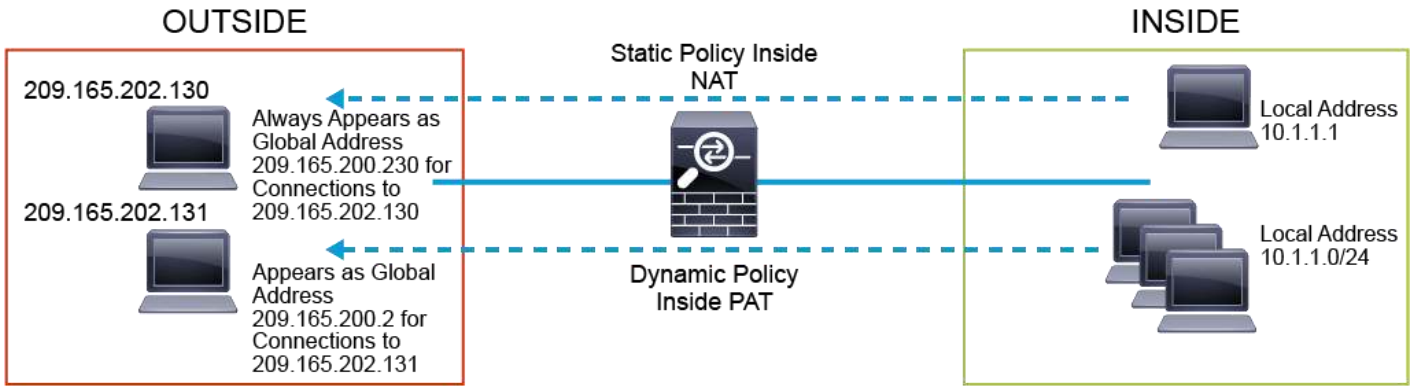
- **PAT** allows you to translate multiple internal addresses into a few external addresses, or even a single external address, essentially allowing the internal addresses to share one external address.
- This is achieved by using a different translation port for each translation occurring in the NAT table.

  - ***Dynamic PAT:*** Translates multiple real IP addresses to a few or even a single mapped IP address (many-to-one) by using different ports. Overloading is also known as PAT, and is a form of dynamic NAT.
  - ***Static PAT:*** Translates one real IP address and real service port to a mapped IP address and mapped service port.

Network Address Translation (cont.)

NAT Deployment Modes (cont.)

- **Policy NAT** allows a single private IP address of a local host might need to get translated to different public IP addresses, depending on the destination hosts or networks, to which it tries to establish a connection.



Configure Cisco ASA Access Control Policies and NAT

LAB