## Cisco ASA protects an internal network from external threats sourced an untrusted interface

**Cisco ASA Family**

* Support NAT, DHCP configuration (server or client)
* Supports most of interior gateway routing protocols (RIP, OSPF, EIGRP), static routing
* Used for remote access VPN and site to site VPN tunnels
* Support IPsec, SSL VPN and full AnyConnect SSL VPN tunnels
* Provides a basic botnet traffic filtering feature

**Cisco ASA FirePOWER Module**

* All Cisco ASA models except the ASA 5506-X, 5508-X and 5516-X can be managed by Firepower Management Center (FMC)
* Required additional licenses
* FirePOWER Services running on the cisco ASA 5506-X, 5508-X and 5516-X can be managed using Adaptive Security Device manager ASDM and licenses can be installed using ASDM

**Cisco ASA deployment types**

**Routed mode Transparent mode**

* **Routed firewalls** do not provide a way to filter packets that traverse from one host to another in the same LAN segment. It is required a new network segment to be created when they are inserted into a network. Layer 3 firewall, where forwarding of traffic is based on IP addresses
* **Transparent firewalls** have been developed to provide LAN-based protection (we can place a transparent firewall between the LAN and the next-hop Layer 3 device without having to readdress the network devices. Forwarding of traffic is based on mac addresses



**Routed firewall outbound data flow**

* When cisco ASA receives the packet, it verifies if the packet belongs to the existing session in the state table
* The cisco ASA appliance checks the routing table to determine the egress interface to forward the packet and checks the configured security policy to determine if the packet should be allowed.
* (optional ) Cisco ASA performs NAT if it is configured
* The packet is sent out through the outside interface

**Transparent firewall guidelines**

* Enabling transparent firewall mode (routed mode is enabled by default)
* One bridge group (logical group pf interfaces) must be configured and all data interfaces must belong to a group
* Each bridge group include a bridge virtual interface to which you assign an IP address on the network
* Only interfaces that are associated with BVI groups can pass traffic
* Support for up to 250 bridge groups, and maximum of 64 interfaces per bridge group
* Bridge groups are also supported in routed firewall mode
* Feature that are not supported in bridge groups in transparent mode available in routed mode: DHCP relay, Dynamic Domain Name System (DDNS), Dynamic routing protocols, DHCPv6 etc

**Steps:**

* Cisco ASA appliance adds the source mac address of the internal user to the mac address table when packet is received on an interface
* Cisco ASA checks the configured security policy (such as ACL, AAA) to determine if the packet should be allowed.
* Cisco ASA appliance performs stateful packet inspection and records this session in its state table
* If the destination mac address is in the mac address table, the ASA forward the packet out of an appropriate interface otherwise the ASA discovers the MAC address. To discovers, Cisco ASA does not flood the original packet because it is a security appliance:
  + It is uses ARP or ICMP to learn the specific MAC address

**Security contexts**

* Enable a physical firewall to be partitioned into multiple standalone virtual firewalls
* Example of Useful of security context in network deployment: when a service provider wants to provide firewall services to customers, when you want to segregate student network from faculty network for improved security while using security appliance, when you administer a large enterprise with different departmental groups, and each department wants to implement its own security policies. etc.
* We have two modes: single context mode (by default) and multiple context mode
* Security context resource management is recommended
* Sharing interfaces between contexts
* Several features are not supported when using security contexts

**Contexts configuration files**

In multiple context mode, ASA has these configuration files:

* each context has its own configuration file. It is stored on the local disk partition or in a TFTP, FTP or HTTP/HTTPS server
* system configuration that identifies basic settings for the security appliance, including a list of contexts, physical settings of its interface. It is a startup configuration for a cisco ASA appliance and it is residing in the flash memory partition of cisco ASA
* admin context configuration: it is created when you convert the cisco ASA appliance from single context to multiple contexts. User who are logged into admin context are able to change the system configuration and create new contexts.

**Packets classification into contexts**

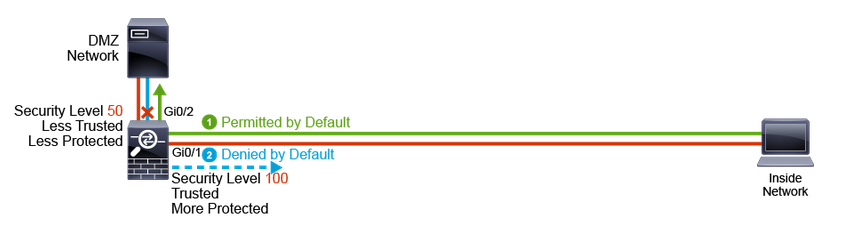
* Cisco ASA determine in which security context packets should be processed when they are received on an interface allocated to multiple contexts by using packet-classifying criteria to identify the correct security context before forwarding packets
* Three classifier criteria can be used: unique interface (if only one context use the interface), unique mac addresses, NAT configuration
* Unique mac address: if multiple contexts share an interface, the classifier uses the packet destination mac address and compare it to the interface mac address of each context sharing the interface. You should assign a different mac address in each context to the same shared interface (by default it is the same mac address)
* Mac addresses is the easiest and the most commonly used method
* (+++ When we you share one or more interfaces between security contexts, to classify the packet Cisco ASA can use either a destination IP address or a unique MAC address. When the interface uses the same Mac address across virtual firewalls, the classifier uses the packet’s destination ip address to identify which security context should receive packets in a shared environment. It uses the NAT table of each security context to learn about the subnets located behind each security context. Firewall cannot classify traffic based on the routing table because multiple mode allows for overlapping networks, routing table might be the same for two contexts)

**Cisco ASA Interface Security Levels**

* Each interface must have a name to designate its role on network and security level (can be between 0 and 100)
* Security level reflect the level of trust of this interface (The higher the security level, the more protected the interface)
* Most secure network label: inside network;
* least secure network: outside network
* For semi trusted networks you can define terms as demilitarized zones (DMZ) or any logical interface name
* Safest network is placed behind the interface with a security level of 100, least protected network 0.
* A DMZ interface should be assigned a security level between 0 and 100

**Default security Policy:**

* Inbound traffic is denied by default
* Outbound traffic is allowed and inspected by default (returning traffic is allowed because of stateful packet inspection)



**Use case of security levels**

* Traffic from the inside network to the DMZ or outside network is allowed by default
* Traffic from DMZ to the outside network is allowed by default

**Inter-Interface security communication**

* Cisco ASA security appliance supports 101 (0- 100) security levels
* You can assign the same security level to different interfaces
* Traffic between interfaces with same security level is not allowed by default. To do this we must enable inter-interface communication

**Intra-Interface communication**

* In hub-and-spoke VPN topologies, traffic needs to enter and leave the cisco ASA appliance through the same interface
* Traffic entering and leaving the same ASA interface is not allowed by default. To do this we must enable intra-interface communication

**Cisco ASA Objects and Object Groups**

* Objects represent network or service entities
* Network object: can be represent a host, a network, a range of IP addresses, FQDN
* Service objects: protocol and ports (source/destination, single/range)
* Object group allows to arbitrarily group hosts, resources, or services that share a same policy
* Network object group: group of one or more network objects
* Service object group: group of one or more service objects
* For example, if we have servers that are going to have similar rules, we can place them inside of an object group. If we create some more servers in the future and add them in the object group, any ACL, NAT policies, anything I’ve built their references to the object group is now going to inherit that new server.
* Advantage: easy update in the future, flexible and easy management of the configuration

**Objects and objects group deployment**

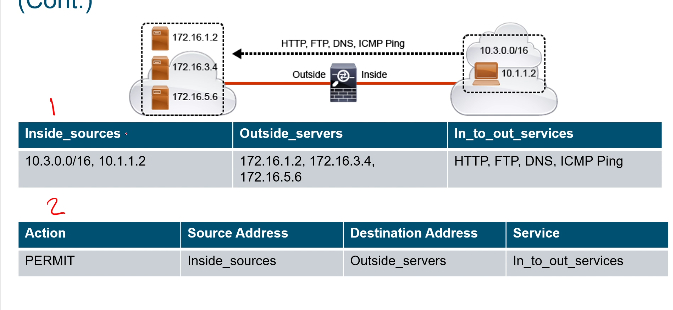
Task to define objects/objects group

* Create individual network objects (host, ip address range, FQDN) or service objects (protocols and ports) and assign them a name
* Create network object groups by defining members in network objects, all sharing common actions
* Create service object groups
* We can edit objects/object group when they are used in access rules or NAT configurations
* Active objects/object group cannot be deleted when used in configurations

**Use case for Objects/object group in Access Rules**

When we have large number of access rules, the configuration is unmanageable and difficult for using. So we must optimize the access rules by using objects/object group

Ex (Au lieu de configurer 24 access rules on a un seule regle)



* Configuration of the objects/object groups and the access rules can be done by using cisco ASDM or the cli.
* Cisco ADSM is a recommended option, because of simplicity and manageability

We can use objects/objects groups in NAT Rules configuration and the configuration can be done by using the cisco ASDM

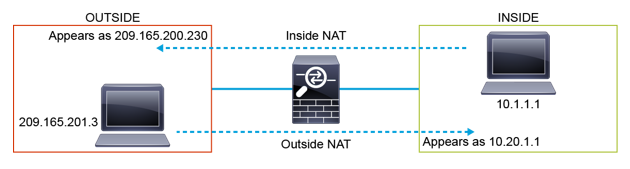
**Network Address Translation**

* Mitigate global IPV4 address depletion
* Preserves internal addressing
* Hides internal network topology
* Cisco ASA appliance performs inside NAT and also perform outside NAT

**Cisco NAT Translations and terms**

**Inside NAT:** translate the private (local) addresses of hosts in the inside NAT domain into public (global) addresses

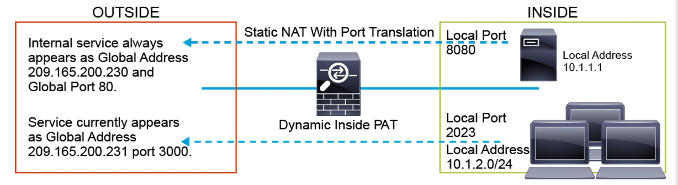
**Outside NAT**: Translate external addresses of hosts in the outside NAT domain to internal addresses



We have inside local address, inside global address, outside local address (IP address of an outside host as it appears to the inside network), outside global address (IP address that is assigned to a host on the outside network)

**NAT deployment modes**

* **Static NAT**: translate a real IP address to a mapped IP address
* **Dynamic NAT**: translate a real IP address to a mapped IP address from a group of mapped IP addresses
* **Dynamic** PAT translate multiple real IP addresses to a few or even a single mapped IP address (many to one) by using different ports. (NAT overload)
* **Static PAT** translate one real IP address and real service port to a mapped IP address and mapped service port



**Cisco ASA NAT**

Two types of NAT

**Network object (Auto) NAT** (recommended for most uses cases)

* You define NAT as a parameter for network object
* Two rules might be used, one for the source IP address, and one for the destination IP address
* Automatically ordered in the NAT table
* Simplest NAT configuration, support static NAT, Dynamic NAT, PAT

**Manual NAT:**

* You identify a network object or network object group for both the real and translated addresses. The network object or group is a parameter of the NAT
* A single rule translates both the source and destination
* Manually ordered in the NAT table
* It is only used for: policy-based NAT, where different translations are needed for the same hosts going to different destinations, when inside and outside NAT is needed

**NAT table:**

* Cisco ASA uses Nat table to build NAT configuration entries when packets from the inside NAR domain are destined to outside NAT domain
* Nat table has three sections:
  + **Manual NAT (first section**): default location for manual NAT statement
  + **Auto NAT (second section):** default location for auto NAT statement
  + **Manual NAT after auto NAT** (third section): manual NAT entries that are specified with the after-auto keyword

**ACCESS Rules in ASA**

* ACL: collection of security rules or policies that allows or denies packets after looking at the packet headers and other attributes
* ACLs include a five-tuple: source and destination IP address (or subnet), Source and destination port, protocol
* Cisco ASA supports four different types of ACL: **standard, extended, EtherType, Webtype ACLs**
* **Standard ACL:** 
  + are used to identify packets based on their destination IP addresses (only used if the cisco is running in routed mode, by acting as an extra layer 3 hop in the network)
* **Extended:**
  + classify packets based on the following attributes: source and destination IP address, Source and/or destination TCP and UDP ports, protocol layer 3 protocols, user identity attributes such as Active Directory (AD) username or group membership.
  + These ACLs can be set up on the cisco ASA in both routed mode and transparent firewall mode.
  + Can be used for QoS packet classification, interface packet filtering, packet identification for NAT and VPN encryption…
* **EtherType ACLs:**
* are used to filter IP and non-IP-based traffic by checking the Ethernet type code field in the layer 2 header.
* Can be configured only if the cisco ASA is running in transparent mode
* **WebType ACL:**
* Allows admin to restrict traffic coming through the SSL VPN tunnels)

**Time based ACLs**

* Use to prevent users from accessing the network services when the traffic arrives outside the preconfigured time intervals
* Cisco ASA relies on the system’s clock when evaluating time-based ACLs
* Time restrictions types:
  + **Absolute**: with this we can specify the start time and the end time. The consultant cannot pass traffic through the security appliance
  + **Periodic**: it is used when for example an enterprise wants to allow user access during the normal business hours on the weekdays and wants to deny access over the weekends. (we can configure a day of th week such as Monday, specify the keyword weekdays)

**Interface Access Rules Structure:**

* The rule that matches first is selected
* Traffic is denied by implicit deny-all rule
* Cisco ASA interface access rules use subnet masks instead of wildcard masks

**Interface Access Rules Behavior**

* All outbound connection for hosts on that interface are permitted
* All inbound connection for hosts on that interface are denied
* We need to specially allow connectivity between interfaces with the same security levels, in and out the same interface

**Interface access rules direction**

* **Inbound:** When you configure access rules and apply them in inbound direction on the interfaces, they apply to traffic that enters an interface.
* **Outbound:** When you configure access rules and apply them in outbound direction on the interfaces, they apply to traffic that exits an interface.
* **Global:** The global access rules, if configured, apply to all inbound traffic that does not match any interface access rules.
* A common strategy for using ACLs on the Cisco ASA appliance is to apply the access rules to the interfaces only in inbound direction

**Interface ACL recommendations**

* It is recommended that you apply ACLs to all Cisco ASA interface and implement a least-privilege policy, if possible
* The simplest and often most effective strategy is to apply inbound to all appliance interface
* Use objects/objects groups to minimize the number of access rules in the ACLs
* Use descriptive naming for ACLs and possibly include comments for the access rules
* Remove unneeded access rules
* Use deny-all clause at the end of every ACL

**Global ACL**

* Global ACL was designed to simplify management of the access policy configurations and applies to all interfaces on the security appliance
* Global ACL filter traffic only in inbound direction
* Interface access rules are always matched before the global access rules

ASA uses the following order to match rules when only interface access rules are configured:

* Interfaces access rules
* Default implicit deny-all interface access rule

ASA uses the following order to match rules when both interface access rules and global Acl are configured:

* Interfaces access rules
* Bridge virtual interface access rule for bridge group member interfaces
* Global acl rules if no match is found against the interface acl
* Default implicit deny-all global access rule

**Global ACL benefits**: flexibility, easier management in configuration

**Global ACL limitation**: just apply only to inbound traffic

**Cisco ASA High Availability**

**Cisco ASA EtherChannel**

* Provide fault tolerance and increases bandwidth for a single network, load balancing,
* It is a logical interface consisting of bundle of individual interfaces
* Support for up to 48 EtherChannel, maximum of 16 actives interfaces per EtherChannel
* Interfaces in an EtherChannel: same type, speed and duplex
* Supports LACP or static configuration (on)

**Cisco ASA Appliance Redundant Interface**

* Logical redundant interface consists of a pair of physical interfaces an active and standby interface (when the active member fails, the standby becomes actives)
* Both member interfaces have to be of the same physical type
* Name, security level and ip addresses are configured on the redundant interface
* Security appliance must be connected to a switch when using redundant interfaces

**Cisco ASA Active/Standby Failover**

* Two ASA can be paired into an active/standby failover to provide redundancy (one is primary (active), the other is a secondary (standby))
* If the active ASA fails, the standby ASA immediately takes its place, becoming the new active unit in the pair
* The primary and secondary cisco ASA devices are interconnected using a dedicated **LAN failover interface.** Over this interface the two units replicate their configuration and mutually monitor the health of each other by exchanging hello packets
* The active cisco ASA appliance provides the management interface and management ip addresses, and automatically replicates all configurations changes to the standby cisco ASA appliance

**Types of failover**

**Stateless failover**

* Only provides hardware redundancy
* If the active cisco ASA appliance fails, all information on tracked connections is lost. Client applications must start a new connection to restart communication through the newly active cisco ASA (previous active appliance did not pass state information to the standby appliance)

**Stateful failover**

* The stateful failover feature extends the stateless failover functionality by continuously passing state information from the active to the standby unit.
* If a failover occurs, all relevant state information is already available on the newly active unit.
* you must designate a stateful link interface over which the two ASA devices will exchange state information
* **Stateful failover interface**: The stateful failover interface passes per-connection stateful information to the standby unit.

**Cisco ASA Active/Active Failover**

* The two ASA in active/active failover can both process traffic and serve as a backup for a peer unit at the same time.
* Active/active failover requires the use of security contexts and therefore is available only on security appliances running in multiple context mode.

**ASA cluster**

* groups multiple Cisco ASA devices together to operate as a single logical firewall.
* A cluster provides all the convenience of a single ASA (management, integration into a network) while achieving the increased throughput and redundancy of multiple Cisco ASA devices.
* One member of the cluster is **the control unit** and all other are **data units (slave)**
* Instead of configuring and managing every Cisco ASA appliance in the cluster separately, all configuration is done on the control (master) unit only.
* The **cluster control link (CCL)** is used for all cluster control plane traffic.
* Members communicate over the ccl

**ASA Cluster data interface modes**

**Layer 2 mode (spanned EtherChannel mode)**

* All of data interfaces on the ASA devices act as a single logical port-channel interface (one IP and mac address in the cluster)
* This mode uses cluster LACP to support the spanned EtherChannel on the ASA devices
* This mode uses ECLB as the external stateless load-balancing method. If one link in the etherchannel fails, then traffic is automatically rebalanced between the remaining links

Layer 3 mode (a lire)

* Each ASA data interface has its own IP and mac address in the cluster
* Slower convergence

**Cisco ASA cluster role ( a relire pour plus de details)**

**Cluster members roles:**

* **Owner:** state connection is centralized in owner
* **Director**: the connection state is backup in the director to provide fault tolerance
* **Backup director**
* **Forwarder**: unit that forwards connection traffic to the owner, over the CCL, when it receives a packet that it does not own.
* Devices that receive the first packets becomes the owner of connection
* Roles are established on a per-connection basis