From CCNA Security book videos - Keith Barker

Basic Firewall, NAT in CCP

- First time you open --->"Select/Manage Community
    - name new Community, add IP user/pass, check 'connect securely', add port info with box
    - discovery reports
- Select community from pull-down
- Configuration groups: interface mgmt, router, security, UC
- Choose interface mgmt, subgrp interface and connections
    - click edit gives
    - Association - access and inspect rules attached for in/out, zone, VPN policy
    - NAT - choose NAT config (pulldown)
    - General - modify int desc, checkbox dis/enable sec properties (like proxy-ARP, IP redirects)
    - Application Service- in/out QoS templates (or none); netflow in/out enable, NBAR on/off

In example we need to give G2/0 an outside IP addy for outside interface. We can't in CCP

- Create connection doesn't support WAN connection, so go to IOS
- in example - int g 2/0; no shutdown; description WAN OUT; ip address dhcp (gets ISP dhcp addy)
- Back in CCP, hit reload button, and discovery happens again like on startup

NAT in CCP

- Open router config group (too many items to list here) go to NAT
- Create NAT and Edit NAT panels. Create has basic, advanced choices, and "launch selected task"
- Basic for LAN PCs, Advanced for DMZ items.
    Basic brings up wizard, specify ISP (out) interface, then IP range in list to provide NAT for
    When done, presents preview of commands before applying, with cancel button
- Edit panel lets you quickly access specified NAT interface to change; also address pool
    - edit also allows setting times when NAT applies (8AM to 5PM) if desired

IOS sh ip nat translations to verify, telnet through and run "who" to see logins.

- NAT Simplification was v8.3 (Auto NAT or Object-based NAT- removed global, static, nat-control, alias commands; Added or changed Config>Firewall>Objects>Network Objects Group and Config>Firewall>NAT Rules Advanced version called TwiceNAT
The old kind are referred to as global NAT and policy NAT

--- Newer uses objects: can only do one subnet, as an object, at a time

```
object network INSIDE_NETWORK
>subnet 10.0.0.0 255.255.255.0
> nat (inside, outside) dynamic interface
> exit
```

These look like they are part of one thing but they are NAT and object
sh run nat
sh run object

New, Static:
object network R1_LOOPBACK0
nat (inside,outside) static 20.0.0.11
host 1.1.1.1

```
ASA3# show nat detail
Auto NAT Policies (Section 2)
1 (inside) to (outside) source static R1_LOOPBACK0 20.0.0.11
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 1.1.1.1/32, Translated: 20.0.0.11/32
2 (inside) to (outside) source dynamic INSIDE_NETWORK interface
    translate_hits = 1, untranslate_hits = 0
    Source - Origin: 10.0.0.0/24, Translated: 20.0.0.254/24
```

old static:
static (inside,outside) 20.0.0.12 1.1.1.1 netmask 255.255.255.255

Application> Options>Preview Commands before applying - to copy and apply in IOS if preferred

Object Groups for ACLs
In CCP go to Configure>Router>ACL>Object Groups to see items Network and Service Object Groups
List with options create, edit, delete
Create: Name, Desc, Type (IP addy/hostname, network, range of IPs, existing OBJ group)
- Put in appropriate info and click "add" to put in side list of Group Members
- Click ok, get preview to copy-paste; click 'deliver' to enable
- Contents:

```
object-group network SERVERS_TO_DENY
 host 2.2.2.2
 host 3.3.3.3
 exit
```

- it isn't used yet, but we can now call it from an ACL
Configure>Router>ACL> ACL Editor and ACL Summary items, next to Object Groups (above), NAT Rules, and IPSEC rlues
In ACL Editor
- options Name, type (basic or ext) desc, rule list (add/edit/del), int and inbound/outbound
- Add Ext Rule options: deny/Permit; source/ dest;
    - Source/dest types: a network, a host/ip, any ip, network object group
    - Wildcard mask (if applicable)
    - Protocol and service: UDP, TCP, IP, ICM, or Service Object Group
    - (separately) IP Protocol
    - option to log matches or not
- Click ok, get preview to copy-paste; click 'deliver' to enable

```
ip access-list extended OUR_ACL
 remark CCP_ACL Category=1
 deny ip 10.0.0.0 0.0.0.255 object-group SERVERS_TO_DENY log
 permit ip any any
 exit
interface GigabitEthernet1/0
 ip access-group OUR_ACL in
 exit
```

```
access-list 100 permit ip host 255.255.255.255 any
access-list 100 permit ip 127.0.0.0 0.255.255.255 any

class-map type inspect match-all CMAP_Bogus_Source
 match access-group 100

class-map type inspect match-any CMAP_Common_Protocols
 match protocol tcp
 match protocol udp
 match protocol icmp

policy-map type inspect PMAP_for_ZBF
  class type inspect  CMAP_Bogus_Source
    drop log
  class type inspect CMAP_Common_Protocols
    inspect

zone security in-zone
zone security out-zone

zone-pair security in-to-out source in-zone destination out-zone
 service-policy type inspect PMAP_for_ZBF

interface GigabitEthernet1/0
 zone-member security in-zone

interface GigabitEthernet2/0
 zone-member security out-zone
```

- make an ACL to define traffic addresses
- make a class-map to match protocol (tcp l udp l icmp) or access-group of ACL - to ID matching stuff
- make policy map inspect and specify log, drop, pass, inspect
- inspect necessary in both map steps, and again in service policy (zone-pair) for stateful
- declare zones with zone security ZONE_NAME (all you are doing is naming and declaring)
- zone-pair security source INNAME destination OUTNAME and specify service-policy POLICY_MAP
- interface BLAH apply ZONE_NAME

Overview- here is some matching traffic, identify it with this class(ification) map name, now do this stuff with THIS policy-map. Thiszone and thatzone exist and we are going to pair them with that policy-map with THIS interface taking the name thiszone and THAT interface taking the name thatzone.

Back to the original example, (we were in Configure>Router>ACL>)
Go to Configure>Security>Firewall>Firewall
- we get options of create basic or advanced, and again the basic option is not for DMZ configs
- there is also a Edit panel. A link on the create screen is there for the "classic" firewall, which is Context–Based Access Control (CBAC)
- When you view the edit window, columns under "Traffic Classification" are the Class Map portion
- The column Action is the policy map, and the column Rule Option extends that (usually logging)

Under Configure>Security>Firewall>Firewall Components are Zones, and Zone Pairs, to edit those.
Configure>Security>C3PL> has the items Class Maps and Policy Maps, containing those areas.

"ASAs use security levels- not Zone Based Firewalls" (??)
Security levels have a **default flow of traffic** from a high security level interface (i.e inside, 100) to a lower (like 50). It is only because of the stateful tables that the opposite direction is allowed (after an inside connection initiates a session like that).
The basic is just to make sure you have a name and security level.
You can use CCP, but ASAs have ASA Security Device Manager (ASDM) and in enterprises, it's common to use the CSM (Cisco Security Manager). ASDM is built into the device and you can connect up to 5 devices with it and switch between them with SSL.

The ASA Family
There are also devices in the ASA family that go into a switch like the 6500
The smaller model number represents smaller capacity for throughput
--- Firewall Services Module (FWSM) - Blade firewalls that fit into compatible switches
--- 5505
- entry level, small not big enough to rack-mount
- built-in 8port switch (2 PoE)
- Default all ports VLAN1
- uses SVI between two VLANS
- only model to have a built-in switch like this
- only single slot for compatible module

--- 5510
- 4 builtin routable interfaces + a management ethernet port that can alternately be a 5th
- single slot for compatible module like IPS

--- 5520 5540 5550 - like the 5510 with more capacity
--- 5585
- high perf, high capacity,
- more addon slots
- take up more rack space

ASA Features and Services:
Packet filtering with ACLs
Stateful filtering
Application inspection/ awareness
NAT, DHCP, Routing, VPN, Layer 2 and 3
Object groups
Botnet traffic filtering - works with Cisco's online Botnet Traffic Filter DB to identify traffic signatures
HA
AAA support

Note on packet filtering:
Often, inbound means uphill -from low level to high level
Reply traffic is stateful in nature, so the stateful part of the firewall the DB) handles that.
However- it often means inbound as "coming into AN interface"

Inbound to an interface - Traffic going into an interface - Ingress traffic (from interface perspective).

Inbound from a high-level perspective of the firewall as a whole device, is traffic that is being routed by the ASA from a lower-security interface to a higher-security interface, such as from the outside to the DMZ, from the outside to the inside, from the DMZ to the inside.
This is from a high-level perspective of the firewall as a whole device.

Outbound to an interface - exiting an interface - egress traffic (from an interface perspective).

Outbound from a high-level perspective of the firewall as a whole device - traffic that is being routed by the ASA from a high-security interface to a lower-security interface, such as inside to DMZ, inside to outside, or DMZ to outside.

When you have a DMZ, webservers, etc., traffic control needs to be more granular. This is where Service Policies (using class and policy maps) have to be applied

Layer 3 and 4 class maps can identify traffic using several different methods, including the following:
- Referring to an access list
- Looking at DSCP and/or IP Precedence fields of the packet
- TCP or UDP ports

- IP Precedence
- Real-time Transport Protocol (RTP) port numbers
- VPN tunnel groups

The policy maps use the services of the class maps to identify traffic, and then specify the actions to take on each class of traffic, which may include the following:
- Reroute the traffic to a hardware module such as the IPS inside the ASA
- Perform stateful filtering or application layer inspection/filtering)
- Give priority treatment to the forwarding of that traffic
- Rate-limit or police that traffic
- Perform advanced handling of the traffic

Recall that any given interface can have only one policy applied to it. You can also apply a policy globally, which means that all interfaces implement that policy. It is possible that an interface has a manually configured policy and an inherited global policy, at which point both policies are implemented (so long as no conflict of policy exists between the two).

Possible Sensor Responses to Detected Attacks

Deny attacker inline
- denies packets from the source IP address of the attacker for a configurable duration of time, after which the deny action can be dynamically removed.

Deny connection inline
- terminates the packet that triggered the action, and future packets on the same TCP flow. The attacker could open up a new TCP session (using different port numbers), which could still be permitted through the inline IPS.

Deny packet inline
- Deny packet terminates the packet that triggered the alert.

Log attacker packets
- This action begins to log future packets based on the attacker's source IP address. This is done usually for a short duration, such as 30 seconds, after the initial alert. Log files are stored in a format that is readable by most protocol analyzers

Log victim packets
- This logging action begins to log all IP packets that have a destination IP address of the victim (the destination address from the packet or packets that triggered the alert).

Log pair packets
- This logging action begins to log IP packets if the source and destination addresses indicate that the packets from the source IP address that triggered the alert and the destination address match the destination address of the packet that triggered the alert. In essence, it is future packets between the attacker and the victim (the attacked device address).

Produce alert
- An alert is the basic mechanism that is used by the IDS/IPS to identify that an event has occurred, such as a signature match indicating malicious traffic. This is the default behavior for most of the signatures.

Produce verbose alert
- Produce verbose alert has the same behavior as produce alert, with the added bonus that it includes a copy of the entire packet that triggered the alert. If both produce alert and produce verbose alert are enabled, it will still only generate a single alert and will include a copy of the triggering packet.

Request block connection
- Some sensor devices can ask for help to block the attacker's traffic at some point in the network. The device that connects to implement the blocking is called a blocking device, and could be an IOS router, a switch that supports VLAN access control lists (VACL), or an Adaptive Security Appliance (ASA) Firewall. This action causes the sensor to request a blocking device to block based on the source IP address of the attacker, the destination IP address of the victim, and the ports involved in the packet that triggered the alert. The difference between this option and the one that follows is that request blocked connection gives an opportunity for the attacker to send traffic on different ports or different destination IPs and still allows connectivity for new sessions.

Request block host
- This causes the sensor to requests its blocking devices (see the preceding paragraph) to implement blocks based on the source IP address of the attacker regardless of the ports in use or destination IP addresses for future packets.

Request SNMP trap
- This generates an Simple Network Management Protocol (SNMP) trap message that is sent to the configured management address for SNMP.

Reset TCP connection
- This causes a sensor to send a proxy TCP reset to the attacker, with the intention of fooling the attacker into believing it is the victim sending the TCP reset. This action has an effect only on TCP-based traffic.

Risk Rating (RR) Calculation

Due to the abundance of signatures available, Risk Rating (maximum 100) is a solution for how to allow IPS sensors to determine the significance of risk a signature indicates to a particular resource, to take appropriate countermeasures. SFR, ASR, and TVR are the 3 primary influencers to how this value is calculated.

Target value rating (TVR) - The value that you as an administrator have assigned to specific destination IP addresses or subnets where the critical servers/devices live.

Signature fidelity rating (SFR) - The accuracy of the signature as determined by the

person who
created that signature.

Attack severity rating (ASR) - How critical the attack is as determined by the person who created that signature.

Attack relevancy (AR) - This is a minor contributor to the risk rating. A signature match that is destined to a host where the attack is relevant, such as a Windows server-based attack, which is going to the destination address of a known Windows server, is considered a relevant attack, and the risk rating increases slightly as a result.

Global correlation - If the sensor is participating in global correlation and receives information about specific source addresses that are being used to implement large-scale attacks, attacks coming from the source IP addresses are also given a slightly increased risk rating value.

IPS/IDS Evasion Techniques, and Countermeasures

- Traffic fragmentation

The attacker splits malicious traffic into multiple parts with the intent that any detection system will not see the attack for what it really is.

- Solution: Complete session reassembly so that the IPS/IDS can see the big picture.

- Traffic substitution and insertion

The attacker substitutes characters in the data using different formats that have the same final meaning. An example is Unicode strings, which an end station could interpret but perhaps a lesser IPS/IDS might not.

- Solution: Data normalization and de-obfuscation techniques. Cisco's implementation is looking for Unicode, case sensitivity, substitution of spaces with tabs, and other similar anti-evasion techniques.

- Protocol-level misinterpretation

An attacker may attempt to cause a sensor to misinterpret the end-to-end meaning of a network protocol and so perhaps not catch an attack in progress.

- Solution: IP Time-To-Live (TTL) analysis, TCP checksum validation.

- Timing attacks

By sending packets at a rate low enough so as to not trigger a signature (for example, a flood signature that triggers at 1000 packets per second, and the attacker sending packets at 900 packets per second).

- Solution: Configurable intervals and use of third-party correlation.

- Encryption and tunneling

Encrypted payloads are called encrypted for a reason. If an IPS/IDS sees only encrypted traffic, the attacker can build a Secure Sockets Layer (SSL) or IPsec session between himself and the victim and could then send private data over that virtual private network (VPN).

- Solution: If traffic is encrypted and passing through the sensor as encrypted data, the

encrypted payload cannot be inspected. For generic routing encapsulation (GRE) tunnels, there is support for inspection if the data is not encrypted.

- Resource exhaustion

If thousands of alerts are being generated by distractor attacks, an attacker may just be trying to disguise the single attack that they are trying to accomplish. The resource exhaustion could be overwhelming the sensor and overwhelming the administration team who has to view the events.

- Solution: Dynamic and configurable event summarization. Here is an example: 20,000 devices are all under the control of the attacker. All those devices begin to send the same attack. The sensor summarizes those by showing a few of the attacks as alerts, and then summaries at regular intervals that indicate the attack is still in play and how many thousands of times it occurred over the last interval. This is much better than trying to wade through thousands of individual alerts.

sh run int
sh int ip br ??
sh ip - can be run instead of sh ip int br on ASA
no security-level
nameif inside l outside
- to automatically set security levels, but be sure to check just-in-case - esp with DMZ
same-security-traffic permit inter-interface
- allows traffic from one security level to pass to another area of the same security level without problems
- inter-interface is different interfaces with same sec level
- intra-interface between peers connected to same interface (hairpinning - in the interface and back out the same link. Sounds like split horizon a little for traffic flow)

No nameif, no security level ASA won't pass traffic

Bad firewall implementation
- too promiscuous
- redundancies
- incorrectly planned or implemented
- orphaned rules (ref subnets never seen, other similar clutter)
- shadowed rules (bad ordering makes the rule useless)

Firewall rules
- service
- address
- direction
- user (AAA)
- behavior (spam filter in email)

Generally,

- Be specific as possible avoiding using "any" and "all"
- Remember least privilege - especially internally
    - "do these workstations really need these ports open?" Restrict- then open!

Recall- Gateway in firewall terminology is "proxy"
Application Layer gateways are considered to work with Layer 3 and higher (not 4)

McGahan INE ASA Firewall

- mentions 5515-X, mentions the Cisco ASA All-in-one NGFW IPS and VPN services 3rd edition book, Cisco 365 Live videos and the ASA documentation. Cisco Live looks like a must-use resource.
Support>Configuration>Firewalls>ASA
ASA roadmap, version changes/ feature by release, configuration guides for CLI examples

- Before 9.0, if you wanted to run virtual firewalls, you ended up disabling IPSEC features. Multiple Context Mode Features, Site-to-site VPN in multiple context mode, fixed this. Also fix to allow EIGRP and OSPFv2 (not v3 or RIP, multicast routing)

Reminder: HA refers to status like active active, active standby, etc

Class HW topology based on INE's CCIE Sec v4:
ASA 5510 with ASA 8.2
ASA 5515-X with ASA 8.6 and 9.3
Various routers and switches (config unimportant- just "endpoints")

USE Cisco ASA - All-in-one Next-generation Firewall, IPS and VPN Services - 3rd Edition.pdf
And the configuration guide located here:
Cisco>Support>Configure>
Navigate to Products>Security>Firewalls>ASA>Cisco ASA 5500-X Series>ASA 5515-X
https://www.cisco.com/c/en/us/support/security/asa-5515-x-adaptive-security-appliance/model.html
Features differ little from this, newer may have more throughput, etc.
Ciscolive.com

In ACLs and OSPF, wildcards are NOT used as in regular IOS - use actual subnet mask

Video 2 - ASA Initialization and Routed Firewall
- Routed firewall is default Firewall Mode

Initial logging into the ASA:

(prior to beginning, he had executed a "write erase" to wipe the old config)
Like IOS routers and switches, you are asked to go through an autoconfigure Q/A, which you can and just cancel saving the configuration. Here is what it will ask:
Firewall mode [Routed]:
-- can be routed (IP routing) or transparent (Layer2 bridging)
-- Routed- we are doing Layer 3 IP routing
-- Transparent- Layer2 bridging - will affect the design of the IP subnetting and the routing of the devices on the inside and outside of the network

Asks to set enable password, set clock, enter management IP address, it's mask, hostname, domain name, and IP address of host running Device Manager
-- will make a security rule to be managed from the web interface on this device (IP)
-- without it you can always console port in, but SSH, telnet, ASDM you won't
---- This line in the running config will look like this:

```
!
interface management0/0
 nameif management
 security-level 0
 ip address 1.2.3.4 255.255.255.0
!
```

The rule for the ASDM access looks like this:
http 1.2.3.254 255.255.255.255 management"
(basically, protocol http allow 1.2.3.254 on interface 'management')

Use this configuration and write to flash?
-- do you want to save this stuff??

You get your user prompt ASA3> and can then go "enable" and config t
ASA IOS differences: you can run verification commands in global config without the "do" keyword, like in "do show run"

THE ALL KEYWORD
"All" is a new keyword that will in "show run all" (e.g.) show a bunch of stuff not normally revealed
show run all class-map, **show run all policy-map**, show run all group-policy (!) show run all tunnel-group
It can also show other default values set for stuff that you won't normally see.
Default options not in the saved configuration (because they are DEFAULTS- not needed there)

Says that we will later be modifying firewall policy rules in the **modular policy framework**
"All" keyword also possibly needed to see VPN terminations
The all keyword also allows you to see options you can set without going to the command reference!

"clear configure"
- a good way of putting the no item before something to negate all configurations of that item.
It's basically so you don't have to issue the "no" item over and over again for similarly grouped/named items
"clear config all" will basically delete the box's configuration - **no warning or confirmation!!**
clear configure access-list x or policy-map y is useful

In ASA, use sh ip instead of sh ip int brief:

```
ASA3(config-if)# int g0/1
ASA3(config-if)# ip address 10.0.0.254 255.255.255.0
ASA3(config-if)# no shut
ASA3(config-if)# int g0/2
ASA3(config-if)# ip address 20.0.0.254 255.255.255.0
ASA3(config-if)# no shut
ASA3(config-if)# end
ASA3#
ASA3# show ip int brief
          ^
ERROR: % Invalid input detected at '^' marker.
ASA3# show ip
System IP Addresses:
Interface                Name                IP address      Subnet mask     Method

GigabitEthernet0/1       inside              10.0.0.254      255.255.255.0   manual
GigabitEthernet0/2       outside             20.0.0.254      255.255.255.0   manual
```

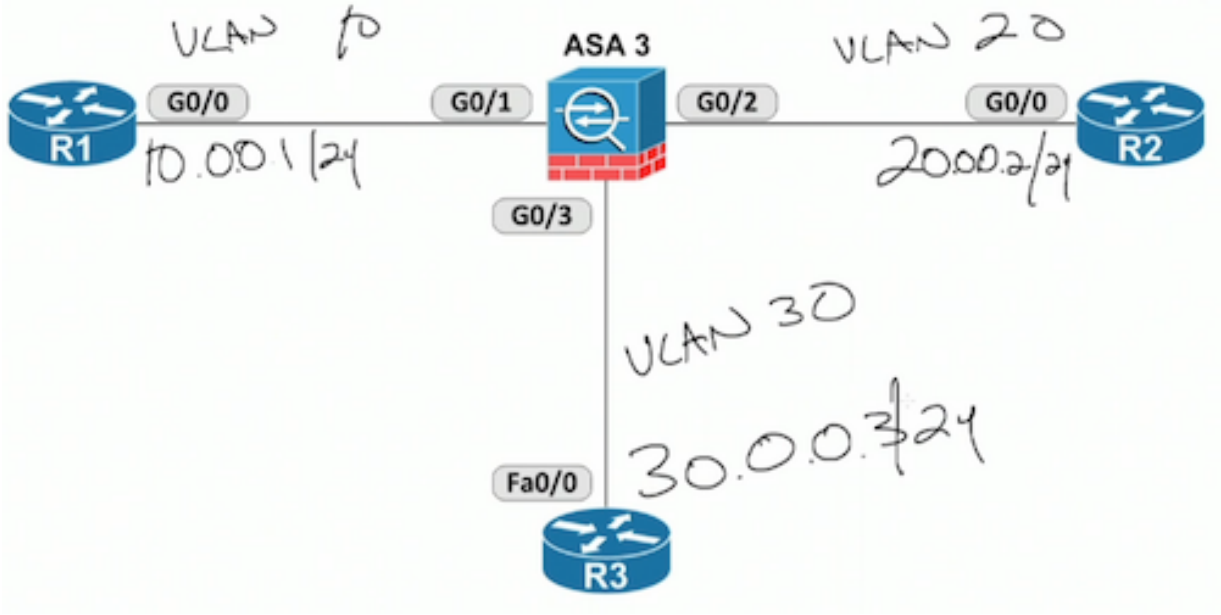
Doesn't show security levels- use sh nameif:

```
ASA3# show nameif
Interface                Name                    Security
GigabitEthernet0/1       inside                  100
GigabitEthernet0/2       outside                   0
```

Without a nameif and security-level set, ASA will NOT forward traffic over the interface!!
(applies in both routed and transparent modes)

Stateful allowances or disallows are governed by security level

BELOW R1 is INSIDE, R2 is OUTSIDE (internet)



In screenshots, R1 is inside (sec level 100) and r2 is outside
- any other name but "inside" is automatically assigned a security level of 0
- inside is the ONLY hardcoded default name-value for security levels!
- DHCP and DNS are default "inspect" - you don't have to tell the stateful database about them yourself
Default application inspections: eg. DNS and FTP.
Some flows inspected just based on the layer 4 info, some deeper at the application-level
Example given is that a huge string in a DNS query would be dropped

- Screenshot (different one) shows global_policy policy-map and service-policy. These are the defaults aside from TCP and UDP- which are declared in "class class-default"
- do show all class-map and do show all policy-map

ICMP is not inspected on the stateful firewall by default, so inside router won't be able to ping outside router. (or inner to outer router) You can either tell it to inspect that traffic, or configure with ACLs

---

Same mechanism as QoS on IOS/Catalyst IOS (Catalyst IOS??)
1 Which class does the traffic match? (ftp? http?)
2 Which policy does has a class matching this traffic?
3 Apply that policy with a service policy

(config)# sh run policy-map
policy-map **global_policy**
class inspection_default
inspect dns preset_dns_map

```
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
!
service-policy global_policy global
    <---global keyword means apply global_policy each direction (i/out or out/in)
!
```

Notice TCP and UDP are in a different policy-map class named "class_default" (like "inspection_default" above)

Here is a default policy for DNS:

```
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no message-length maximum server
  dns-guard
  protocol-enforcement
  nat-rewrite
  no id-randomization
  no id-mismatch
  no tsig enforced
```

This detours into what zone-based firewall means
- 0 totally untrusted to 100 totally trusted
- solicited replies from outside (0) are allowed but unsolicited (not in a active session) denied
- The nameif "inside" is the only name that means anything (100)
- Any other name gets a default security level of 0
- higher to lower and back in is allowed
- low to high with no session gets blocked
- in otherwards, traffic whose state was initiated from a high security level is allowed to go on.

- if you have two interfaces with the same security level (even 100) traffic between them is going to be DENIED by default

-You have to add a manual exception or change the default behavior
Command: "no same-security-traffic permit inter-interface"

"communication between interfaces with the same security-level"

Note: "intra-interface" on the other hand is completely different: hairpinning - will be denied:

"communication between peers connected to the same interface"

Sometimes becomes **an issue with VPNs** since you really DO need traffic going in and out the same interface

---

Example of limited visibility:

Configuring the default route on both R1 and R2 to those subnet's ASA interface IPs:

R2(config)# ip route 0.0.0.0 0.0.0.0 20.0.0.254
(and)
R1(config)# ip route 0.0.0.0 0.0.0.0 10.0.0.254

Now,
- Outside traffic can ping the outside gateway
- Yet routed traffic, (pinging the other router) will NOT work
- Same happens on Inside to outside!
- Because ICMP is not inspected by the stateful firewall by default

Solution: tell stateful firewall to inspect it or do manual ACLs

[WRONG- Manual ACL exceptions will disable useful stateful firewall stuff!]

Defeats the purpose of using stateful firewall to begin with
ACL exception is needed if there are items where the firewall can't inspect certain things

(port forwarded from the "outside-to-inside")
But is there an inspection engine for that protocol? Maybe we can enable it.
Notice above that **class inspection_default** did not inspect ICMP

(also recall that by default only UDP and TCP are inspected)

----------*Example solution: edit policy map global_policy*

(config)# policy-map global_policy
(config-pmap)# class inspection_default
(config-pmap-c)# inspect icmp
(config-pmap-c)# ^x and config t
-- so that affects traffic through.
So with the traffic rule we applied, the traffic is inspected and the traffic is handed to the stateful firewall according to security-levels - one ping is let out, one reply allowed in and the connection is torn down, deleted from the stateful DB. This disallows ping attacks -one ping was allowed out creating a stateful connection, and the returning one was allowed, tearing down the connection

[says in deep packet inspection, we can do inspect http, then specify another poilcy map to determine the traffic we want to filter]

[[This will affect traffic directed to the firewall itself (and unrelated to policy map):
(config)# icmp {deny | permit | unreachable} any any { inside | outside }
-- "unreachable" has other options
sh run icmp
clear configure icmp
-- the same as no icmp deny inside, no icmp deny outside
]]

So traffic sessions (states in the flow table) initiated from a high sec area can go out to low, but the answer coming from the outside won't be let in to answer unless that traffic is first being inspected (such as here in a policy map, etc). Security levels are totally separate
High to low, and only low to high if matching entry in the flow table

Here he demonstrated sending a ping out - 'ping 20.0.0.2 repeat 10000', switched to the ASA really
quick to **run 'show local-host all' to see the stats**

Sidebar on logging this to see what is happening:
logging console 7
logging on
Syslog level 7 too noisy!!!!

no ip domain-lookup --turn off host lookup

Using an ACL to define and allow non-standard traffic flow:
traceroute - udp out get icmp error replies (unreachable or time exceeded).
No state in stateDB makes it fail - the outbound traffic does not match the inbound traffic

so the firewall denies it.

It also is nonstandard in that the port and destination are not complimentary
(the outbound traffic profile does not match the return traffic)
[in tcp 3-way handshake, client sends http request to port 80 from a random client port, and server synacks on that same random port from it's port 80. This complimentary response is what stateful firewalls typically expect as "standard"]
This is where we need to do the application-level inspection

The list in the global_policy policy-map, class inspection_default are non-standard profiles (ftp inits on port 21 works on tcp 20) that the ASA comes with (defaults)

So this traceroute issue is an opportunity to make an access list-
Looking at the logs- our UDP is going out fine ("Built outbound UDP connection...")
Corresponding ICMP traffic needs to be allowed, since it is currently blocked ("Deny inbound icmp src outside...")
The exception would be on the outside interface inbound, where we see it blocked

access-list OUTSIDE_IN permit ip any any
access-group OUTSIDE_IN in interface outside (in for direction)
- with this ACL example, I don't like it since it is using ANY- it isn't precise enough, but it is simply showing how to allow traffic to cross from the outside low-security level (0) to the high (100) security level interface.
- So then ASA lets it work.
ASA does not show up since it doesn't send it's address or reply with an ICMP unreachable- to not give away information on the filtering policy on the firewall. (On IOS if you drop a packet based on an ACL, it will say ICMP administratively prohibited)

- Side note: in ASA there are not standard and extended ACLs- there are just ACLs. Also- ASA doesn't use wildcard masks- it uses subnet masks (so you can't just copy standard IOS ACLs and paste them in.

----------Q/A section notables Video 2

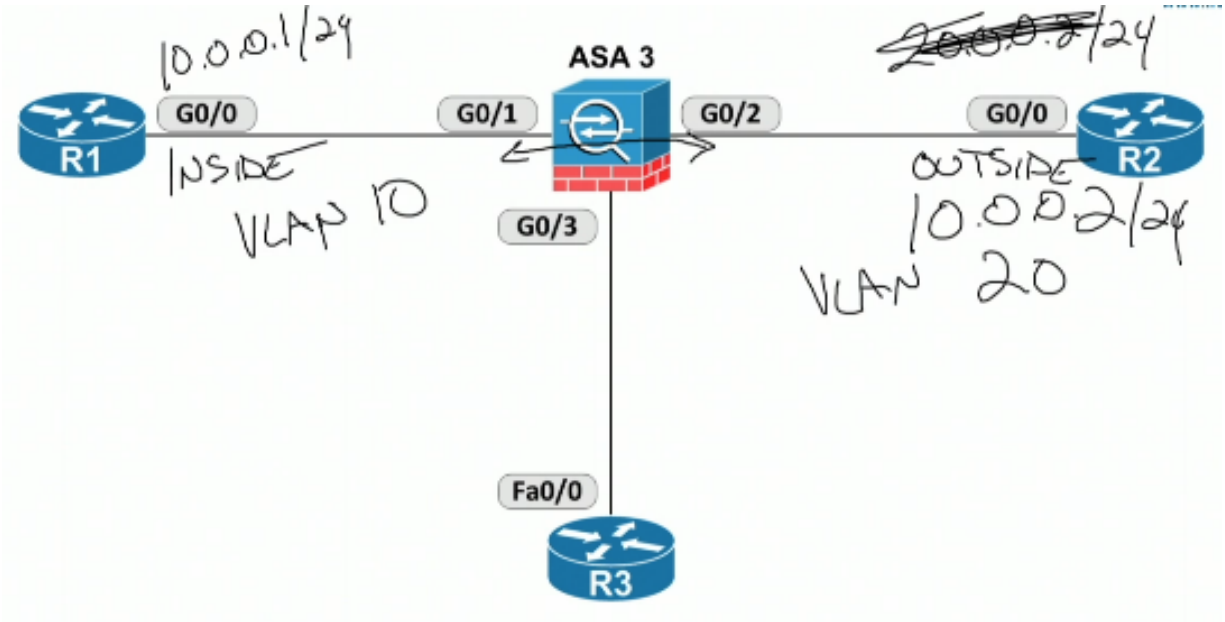
Using Packet tracer:
packet-tracer input { inside | outside } { icmp | rawip | tcp | udp } { source ipaddr | <username> | <fqdn> } { dest ipaddr | <username> | <fqdn> }
packet-tracer input inside icmp 10.0.0.1 ?
<0-255> Enter ICMP type
packet-tracer input inside icmp 10.0.0.1 8 ? - type 8 is ping
<0-255> Enter ICMP code
packet-tracer input inside icmp 10.0.0.1 8 0 ? -code 0 is echo
(enter ICMP identifier, destination ip4 addy or fqdn)
packet-tracer input inside icmp 10.0.0.1 8 0 20.0.0.2

You can also try "packet-tracer input outside icmp 20.0.0.2 8 0 10.0.0.1 detail"
When it checks it goes through different phases:
Phase 1 is the routing table (before I even inspect this can I even forward it?)
- This won't happen in transparent mode since that's bridging, not routing
Phase 2 is access-list...
If we remove the ACL, it says "implicit deny" - there is not rule permitting and it is outside to inside traffic
So packet tracer can show when a trace packet is denied in the inspection chain it is dropped
Question:
show connections" the same as "show localhost all"?
yes, but more info;
show xlate only for NAT translated- is from PIX days; it used to be you needed a NAT rule for everything (translation or not) pre v6.0.4

Transparent Firewall -video 3

Use filtering without redesigning IPv4 or IPv6 networking
- in routed mode, if you had a webserver behind the 10.0.0.1 network, you would have to use routing protocols or use the ASA as a default gateway.
- Advantage to transparent especially with virtual firewalls with security context is that it can be split into multiple firewalls in different portions of the network based on the (layer 2) VLAN configuration. "The devices on the inside of the interface and outside of the interface would be in the same subnet, so the applications, etc, wouldn't need a default gateway defined as in routed mode.

So using the same diagram previously, lets say R1 and R2 are in 10.0.0.x as below, and we have one in VLAN10 and the other in VLAN20
We also need to make sure it is not bridging those VLANs through other connected ports
These will also still be labeled inside and outside (since we need nameifs all the time anyway)



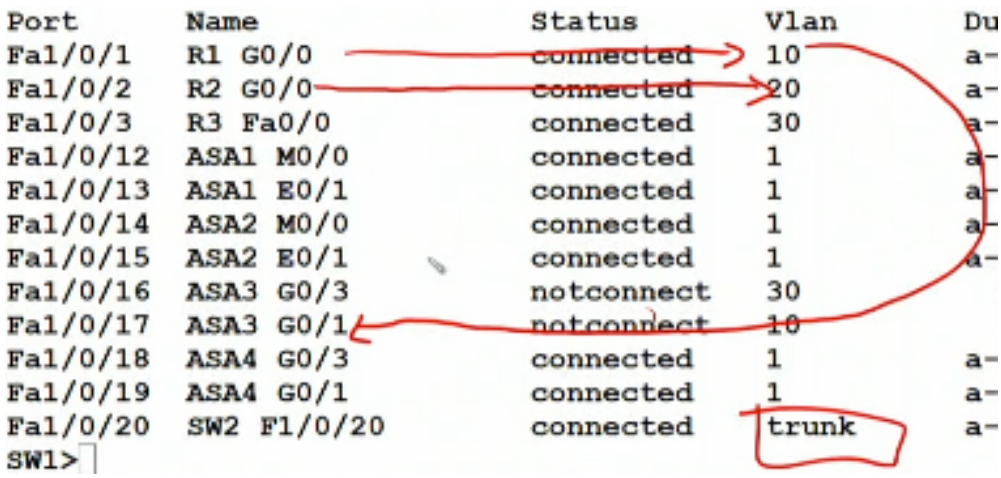
#show firewall
  Firewall mode: Router
- Running "firewall transparent" will delete the routing config, and <u>will not warn/ ask for confirmation!!</u>
- THIS INCLUDES IP ADDYS and NAMEIFs and SECURITY LEVELS! ALL GONE

Here is what is shown on the switch for the topology after clearing the configuration on the ASA3:

```
SW1>show int status | exclude disabled

Port      Name               Status       Vlan       Duplex  Speed Type
Fa1/0/1   R1 G0/0            connected    10         a-full  a-100 10/100BaseTX
Fa1/0/2   R2 G0/0            connected    20         a-full  a-100 10/100BaseTX
Fa1/0/3   R3 Fa0/0           connected    30         a-full  a-100 10/100BaseTX
Fa1/0/12  ASA1 M0/0          connected    1          a-full  a-100 10/100BaseTX
Fa1/0/13  ASA1 E0/1          connected    1          a-full  a-100 10/100BaseTX
Fa1/0/14  ASA2 M0/0          connected    1          a-full  a-100 10/100BaseTX
Fa1/0/15  ASA2 E0/1          connected    1          a-full  a-100 10/100BaseTX
Fa1/0/16  ASA3 G0/3          notconnect   30           auto   auto 10/100BaseTX
Fa1/0/17  ASA3 G0/1          notconnect   10           auto   auto 10/100BaseTX
Fa1/0/18  ASA4 G0/3          connected    1          a-full  a-100 10/100BaseTX
Fa1/0/19  ASA4 G0/1          connected    1          a-full  a-100 10/100BaseTX
Fa1/0/20  SW2 F1/0/20        connected    trunk      a-full  a-100 10/100BaseTX
```

This shows us (at the top) R1 is connected in VLAN10 which then connects to ASA3's G0/1 (4th from the bottom of list)
R2 on VLAN20 is going across a trunk to another interface on ASA3.

Note illustrated better below, and notice this is the output on SW1



```
Port      Name               Status       Vlan       Du
Fa1/0/1   R1 G0/0            connected    10         a-
Fa1/0/2   R2 G0/0            connected    20         a-
Fa1/0/3   R3 Fa0/0           connected    30         a-
Fa1/0/12  ASA1 M0/0          connected    1          a-
Fa1/0/13  ASA1 E0/1          connected    1          a-
Fa1/0/14  ASA2 M0/0          connected    1          a-
Fa1/0/15  ASA2 E0/1          connected    1          a-
Fa1/0/16  ASA3 G0/3          notconnect   30
Fa1/0/17  ASA3 G0/1          notconnect   10
Fa1/0/18  ASA4 G0/3          connected    1          a-
Fa1/0/19  ASA4 G0/1          connected    1          a-
Fa1/0/20  SW2 F1/0/20        connected    trunk      a-
SW1>
```

[Checking out the Cisco website in the same spot as before for ASA configs, 5515-X configuration guides for v9.3, Firewall CLI or General Operations CLI Config Guides. In Gen Ops, go to "interfaces" section, and "transparent mode interfaces"

As of ASA 9, virtual firewalls (aka "security context") no longer restricted whole-device of running in either transparent mode or router mode- they can run both at the same time now if needed

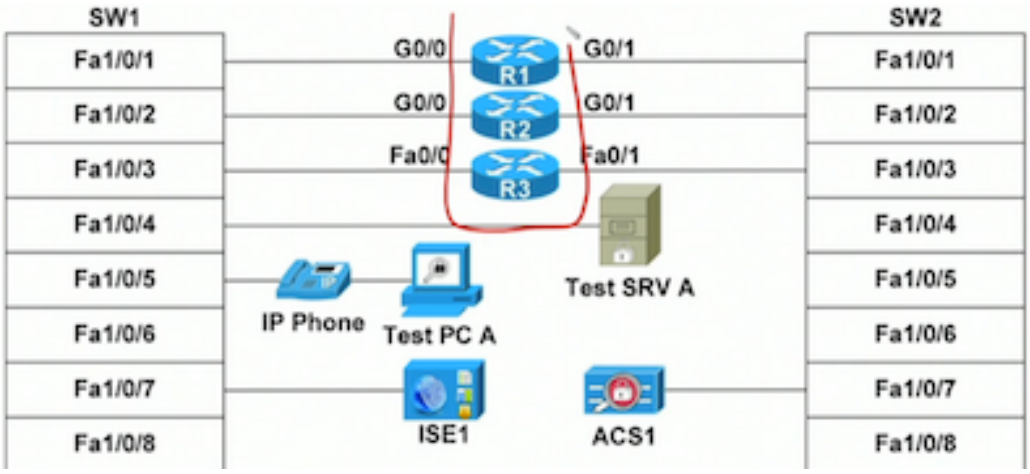
Two bridge groups of three interfaces each, plus a management-only interface: This looks like it is from the Cisco documentation:

```
interface gigabitethernet 0/0
nameif inside1
security-level 100
bridge-group 1
no shutdown
interface gigabitethernet 0/1
nameif outside1
security-level 0
bridge-group 1
no shutdown
interface gigabitethernet 0/2
nameif dmz1
security-level 50
bridge-group 1
no shutdown
interface bvi 1
ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2

interface gigabitethernet 1/0
```

```
nameif inside2
security-level 100
bridge-group 2
no shutdown
interface gigabitethernet 1/1
nameif outside2
security-level 0
bridge-group 2
no shutdown
interface gigabitethernet 1/2
nameif dmz2
security-level 50
bridge-group 2
no shutdown
interface bvi 2
ip address 10.3.5.8 255.255.255.0 standby 10.3.5.9

interface management 0/0
nameif mgmt
security-level 100
ip address 10.2.1.1 255.255.255.0 standby 10.2.1.2
no shutdown
```

```
ASA3(config)# int bvi1
ASA3(config-if)# ip address 10.0.0.254 255.255.255.0
ASA3(config-if)# int g0/1
ASA3(config-if)# bridge-group 1
ASA3(config-if)# nameif inside
ASA3(config-if)# no shut

ASA3(config-if)# int g0/2
ASA3(config-if)# bridge-group 1
ASA3(config-if)# nameif outside
ASA3(config-if)# no shut
ASA3(config-if)# end

ASA3(config)# sh ip
Management System IP Address:
        ip address 10.0.0.254 255.255.255.0
Management Current IP Address:
        ip address 10.0.0.254 255.255.255.0
 --- Management IP is the bvi1 address
 --- recall that inside (g0/1) is pointing to R1@10.0.0.1 and outside (g0/2) is
R2@10.0.0.2
 --- also recall those are VLAN 10 and VLAN 20, and that this bridge-group is bridging
```

the two
 --- from the ASA we can ping both routers fine
 --- think about spanning tree (considering there is a switch in the middle, we are told it will look a little strange):
ASA3(config-if)#
ASA3(config-if)#
ASA3(config-if)#
ASA3(config-if)#



Over on the switch:

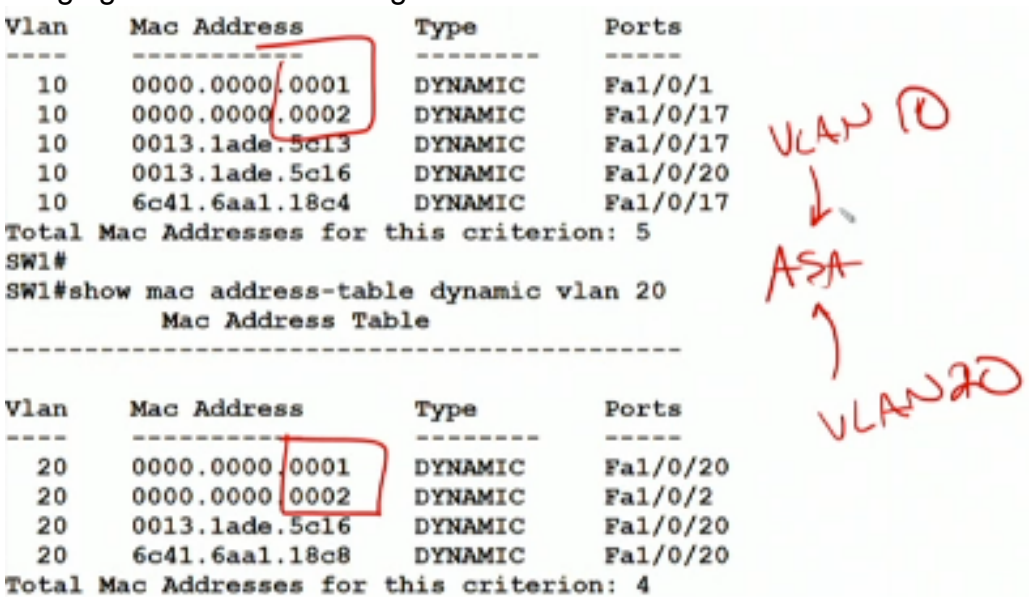
```
SW1#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    32778
              Address     0013.1ade.5c00
              Cost        19
              Port        22 (FastEthernet1/0/20)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32778  (priority 32768 sys-id-ext 10)
              Address     001d.4507.d400
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------
Fa1/0/1             Desg FWD 19        128.3    P2p Edge
Fa1/0/17            Desg FWD 19        128.19   P2p
Fa1/0/20            Root FWD 19        128.22   P2p
SW1#show spanning-tree vlan 20

VLAN0020
  Spanning tree enabled protocol ieee
  Root ID     Priority    32778
              Address     0013.1ade.5c00
              Cost        57
              Port        22 (FastEthernet1/0/20)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32788  (priority 32768 sys-id-ext 20)
              Address     001d.4507.d400
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------
Fa1/0/2             Desg FWD 19        128.4    P2p Edge
Fa1/0/20            Root FWD 19        128.22   P2p
```

Observe that both are using the same root bridge.
The traffic needs to be forced to bridge on the ASA or the traffic is not going to be inspected
This is where spanning tree gets to be super important
We have a trunk link between the two switches, that are on the inside and outside of the interface
Normally what we would want to do is remove VLANS 10 and 20 from the trunk in order to force the
traffic to be bridged through the ASA

R1(config)# int g0/0 <---- same int with 10.0.0.1
R1(config-if)#mac-address 0000.0000.0001

R2(config)# int g0/0 <---- same int with 10.0.0.2
R2(config-if)#mac-address 0000.0000.0002

Now those mac addresses show up in both VLANs, and the ASA is in the middle bridging VLAN 10 and 20 together



Try not to trunk VLAN10 and 20 on other links outside the ports that are going to the ASA

So all traffic is going through the transparent firewall and the transparent firewall is bridging those interfaces

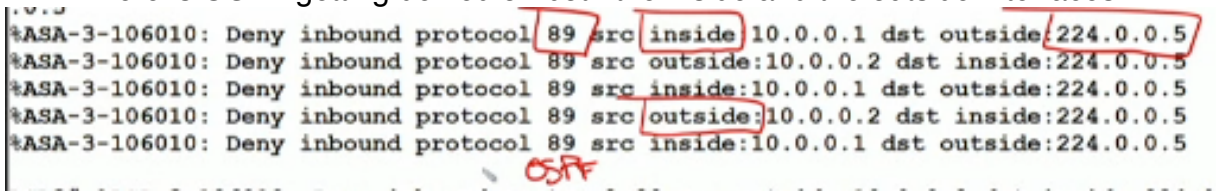
With a routed firewall, traffic to come back through from the outside, we need either a manual entry in the inspection table (rule 1) or an entry in an ACL (rule 2).

With the transparent firewall, there are also some other issues- things being blocked from being sent from inside to outside (!), such as routing protocols (other kinds of control plane traffic). Here is OSPF and MPLS trying to work:

r2(config)# int g0/0
r2(config-if)# ip ospf area 0 <---note the different syntax here- placing on an interface like IPv6 on regular IOS

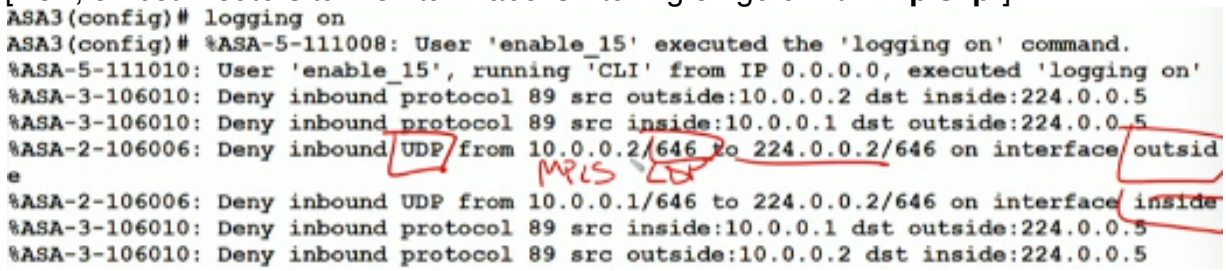
Do this on both routers and on the ASA turn on **logging console 7**

Here is OSPF getting denied on both the inside and the outside interfaces



Notice also this is multicast traffic (224.0.0.5) Says most unicast is ok

[Now, on both routers turn on turn label switching on g0/0 with "**mpls ip**"]



MPLS Layer Distribution Protocol (LDP) runs on UDP port 646, TCP 646 also needs to be open - UDP seems to be going to the outside direction while TCP is coming to the inside)

access-list INSIDE_IN permit ip any any
access-list OUTSIDE_IN permit ospf any any
access-list OUTSIDE_IN permit udp any any eq 646
access-list OUTSIDE_IN permit tcp any any eq 646
(he says you need an implicit deny somewhere but doesn't show it video3 @ 20:52
access-group INSIDE_IN in interface inside
access-group OUTSIDE_IN in interface outside

INSIDE_IN is fine, but on the OUTSIDE_IN you would still need them to end on an implicit deny - you need it to check to see if there was a flow/session that was previously created - if not, we have two exceptions for MPLS and OSPF and anything else is going to be denied without an entry in the table

Routed firewall, you'd just need an outbound in exception, but with a transparent firewall you also need inbound in and outbound in exceptions - multicast routing protocols and other multicast in the data and control plane are not going to be able to be inspected by default, and these sort of provisions have to be made for transparent routing (allowing out as well as in)

sh run l in bridge (include bridge)
show conn
show conn detail
show local-host all

Below is from:
http://www.cisco.com/c/en/us/td/docs/security/asa/asa93/configuration/general/asa-general-cli/intro-fw.html

Allowing Layer 3 Traffic

Unicast IPv4 and IPv6 traffic is allowed through the transparent firewall automatically from a higher security interface to a lower security interface, without an ACL.
Note: Broadcast and multicast traffic can be passed using access rules. See the firewall configuration guide for more information.

ARPs are allowed through the transparent firewall in both directions without an ACL. ARP traffic can be controlled by ARP inspection. (**You need to use a transparent**

firewall for ARP inspection)

For Layer 3 traffic travelling from a low to a high security interface, an extended ACL is required on the low security interface. See the firewall configuration guide for more information.

Allowed MAC Addresses

The following destination MAC addresses are allowed through the transparent firewall. Any MAC address not on this list is dropped.

TRUE broadcast destination MAC address equal to FFFF.FFFF.FFFF
IPv4 multicast MAC addresses from 0100.5E00.0000 to 0100.5EFE.FFFF
IPv6 multicast MAC addresses from 3333.0000.0000 to 3333.FFFF.FFFF
BPDU multicast address equal to 0100.0CCC.CCCD
AppleTalk multicast MAC addresses from 0900.0700.0000 to 0900.07FF.FFFF

Passing Traffic Not Allowed in Routed Mode

In routed mode, some types of traffic cannot pass through the ASA even if you allow it in an ACL. The transparent firewall, however, can allow almost any traffic through using either an extended ACL (for IP traffic) or an EtherType ACL (for non-IP traffic).
Non-IP traffic (for example AppleTalk, IPX, BPDUs, and MPLS) can be configured to go through using an EtherType ACL.

Note: The transparent mode ASA does not pass CDP packets packets, or any packets that do not have a valid EtherType greater than or equal to 0x600. An exception is made for BPDUs and IS-IS, which are supported.

So you can set up transparent firewalls for any bridge group to include interfaces you need them for (not just physical!), AND can 802.1q trunk in vlans to implement SVIs - subinterfaces (logical organizations), etc to do the same! You have multiple bvis, different bridge groups with different purposes, getting nameifs, security levels, etc. segmenting and tying off specific VLANs with individual settings (ACLs) from one spot!

It is mentioned transparent mode can also do ARP inspection for protection there as well
(look for "ARP Inspection" at the same URL mentioned above) - routed can't

He also mentions to check the section "Reference" of this general Ops CLI book for a adresses protocols and ports section to save

int g0/0.10
vlan10
nameif branch1
security-level = 75

FILL THIS IN:
Transparent firewalls can do this, and routed mode can't:

Routed mode can do this, but bridging ones cant:

Virtual Firewall/ Security Context (Multiple Context Mode) - video 4

"Allows us to take on physical device
Virtualize it with the physical interfaces or virtual subinterfaces
So that we have multiple sections (i.e) for administration if we are offering managed services
(say one department has a firewall they manage, and another department has a different firewall they manage independently)
Or can be used for things like VPN termination vs regular firewall filtering"
(multiple firewalls) can be used for separation of policy, multi-tenancy, or firewall as a service to customer

Before we had 2 interfaces inside and out, routed mode (routing traffic at layer 3), and transparent mode (defined by bridging traffic at layer 2), in single mode before.
Looking at it now in multiple contexts; in this, R1 will be context1, and R3 will be context2, R2 outside

---
The mode command says single mode is "mode without security contexts"
After doing the mode change below, the previous mode/ context is saved in Flash

```
ASA3# show mode
  Security context mode: single
ASA3#  show firewall
  Firewall mode: Transparent
ASA3#  config t
ASA3(config)# mode multiple
        --- this will restart the box after confirmation
```

"sh run" to see the different contexts have been created
There is an admin-context admin defined; the primary admin account; for when you need superuser-like remote access through ssh/ASDM/etc. For when you don't want to go through the console, but you want to manage the contexts for the various firewalls administered by different "customer" admins

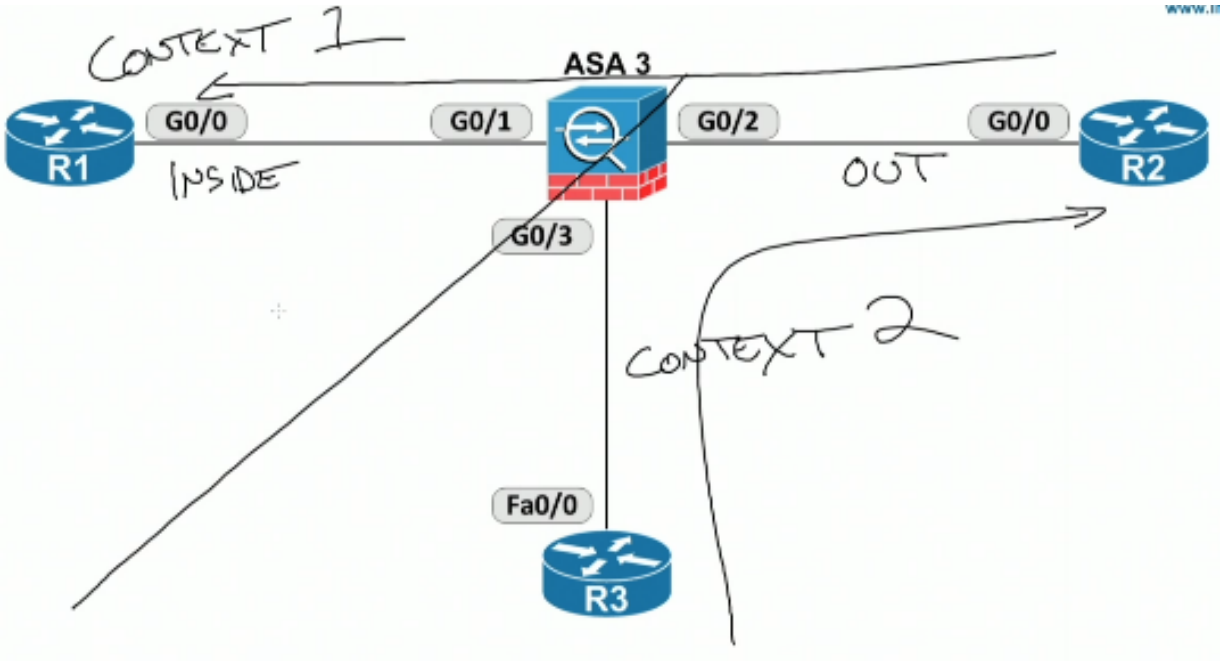
admin-context admin
context admin
  allocate-interface GigabitEthernet0/1
  allocate-interface GigabitEthernet0/2 <--- could be a logical subinterface assigned to a VLAN
  config-url disk0:/admin.cfg <---where config will be stored

Define some contexts:
ASA3(config)# no firewall transparent <-----did this first in demo to dump any previous contexts applied
ASA3(config)# admin-context admin
ASA3(config)# context admin
ASA3(config-ctx)# config-url disk0:/admin.cfg
<----- you have to define admin context with config location set before it will let you make other contexts

---

With interfaces in ASA contexts, Nexus virtual device contexts are similar, or VRF virtual routing/forwarding instances, which traffic from one context can't talk to another one unless it goes to an external device and comes back in.
For this simple example we are segregating the two routers - contexts by their physical interfaces.
We are also going to configure these interfaces (the ones in both contexts) with 2 different IP addresses in the same subnet (just to prove they can be in the same subnet)

Below, R3 (context2) is segregated and cant talk to R1 (context1) without going out and coming back in from another device:




```
ASA3(config)# context CONTEXT1
ASA3(config-ctx)# ?
  Context configuration commands:
    allocate-interface Allocate interface to context
    allocate-ips       Allocate IPS virtual sensor to context
    config-url         Configure URL for a context configuration
    description        Provide a description of the context
    exit               Exit from context configuration mode
    help               Interactive help for context subcommands
    join-failover-group Join a context to a failover group
    member             Configure class membership for a context
    no                 Negate a command
ASA3(config-ctx)# allocate-interface g0/1    <----to R1
ASA3(config-ctx)# allocate-interface g0/2    <----to R2
ASA3(config-ctx)# config-url disk0:/CONTEXT1.cfg

ASA3(config)# context CONTEXT2
ASA3(config-ctx)# allocate-interface g0/2    <----to R2
ASA3(config-ctx)# allocate-interface g0/3    <----to R3
ASA3(config-ctx)# config-url disk0:/CONTEXT2.cfg
ASA3(config-ctx)# end
```

---------- Break for discussion:

In routed mode, the shared g0/2 would have a different IP address in each context, but still wouldn't be able to route between the contexts without going out to another device unless you forced a config that is not default or in "best practices"

Multiple context items:
Separation between the admin and user context
User context is where the actual data traffic is going to flow (where R1's and R3's port are assigned: 2 different user contexts)
System and admin contexts for managing the box
Some commands aren't available in the system context since they are appropriate for the user context, such as "show ip" because user contexts are where IP addresses are configured- not the system context.
The line is sort of drawn such as what is an attribute of the physical box, and what is an attribute of the virtual firewall.
IP addressing is now part of the virtual firewall, not the physical box. Shutdown/ no shutdown (see below) has to be done in system context, since it is a attribute of the physical box.

The changeto command lets you move around like that: "changeto context" or "changeto system"

Prompt changes:
ASA3# show ip
        ERROR: % Unrecognized command
ASA3# changeto CONTEXT1
ASA3/CONTEXT1# show ip <--- now show ip will work
ASA3/CONTEXT1(config)# show interface <--- this will only shows this context's stuff

---------- **Below continuing configuration:**

[Again, the interfaces below could be virtual/logical subinterfaces, where you have a trunk bringing in different VLANs, and those VLANs are then assigned to the subinterfaces, which are in turn placed into different contexts for filtering, etc]

[Below, no shut needs to be applied to the physical interface, but this is not something in the user context- we have to jump back into the system context to change that physical property of the interface, which the system context provides to it's user contexts]

ASA3(config)# changeto context CONTEXT1
ASA3/CONTEXT1(config)# int g0/1
ASA3/CONTEXT1(config-if)# nameif inside
ASA3/CONTEXT1(config-if)# ip address 10.0.0.254 255.255.255.0
ASA3/CONTEXT1(config-if)# int g0/2
ASA3/CONTEXT1(config-if)# nameif outside
ASA3/CONTEXT1(config-if)# ip address 20.0.0.**101** 255.255.255.0
-----> ping doesn't work - the interface is shut down, needs no shut.
ASA3/CONTEXT1(config)#changeto system
ASA3(config)# config t
ASA3(config)# int g0/1 <----also do this for g0/2
ASA3(config-if)# no shut
ASA3(config)# changeto context CONTEXT1

ASA3/CONTEXT1# config t
ASA3/CONTEXT1(config)#

R1- 10.0.0.0/24, R2- 20.0.0.0/24, R3- 30.0.0.0/24
We are going to do the same thing with CONTEXT2, but G0/3 is going to be inside, g0/2 outside
The network number for g0/2 in CONTEXT2 is **20.0.0.102** 255.255.255.0

---------- Break for discussion:

How does ASA know which context a traffic reply from outside is for when interface has 2 or more contexts?
Given this scenario, G0/2 has an different IP address in each context, for a different IP in each context*
If a client on R1 requests a webpage from a host on the outside (sending a syn out R2 to the internet)
How does the ASA know whether the synack reply from the webserver is for R1(context1) or R3 (context2)?
The ASA has a MAC address on the outside with a physical address on layer 2, but it needs to rebuild the layer 2 frame to go to either R1 or R3.
[The documentation (CLI book 1, HA and Scalability, Multiple Context Mode, How the ASA Classifies Packets), says to use either unique MAC addresses, unique interfaces, or make allowances in NAT config]
Solution that works here is for each logical interface (one in each context) to be given a unique MAC address to distinguish the two. The NAT solution does not allow overlapping IP addressing in participating contexts such as this.

* it is also mentioned that the two contexts could have the same subnet (overlapping addressing, same IP) as on
a VRF on a router or a vPC on Nexus

ASA3/CONTEXT1#change system <---"change" works for changeto (sometimes)
ASA3# config t
ASA3(config)#mac-address auto <--- tells the ASA to "auto-generate MAC address for context interface".

After doing this, here is R2 pinging the addresses specified inside each context for G0/2 (101 and 102).
Notice the arp table shows unique MAC addresses for both:

```
R2#ping 20.0.0.101
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.0.0.101, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
R2#ping 20.0.0.102
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.0.0.102, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
R2#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  20.0.0.2                -   0000.0000.0002  ARPA   GigabitEthernet0/0
Internet  20.0.0.101             0   1200.0200.0300  ARPA   GigabitEthernet0/0
Internet  20.0.0.102             0   1200.0200.0400  ARPA   GigabitEthernet0/0
```

Limitations on 8.6 multiple context mode

1. You can't run dynamic routing
ASA3/CONTEXT1(config)# router ?
ERROR: % Unrecognized command
You can do static though.
Make inside routers use ASA interface IP matching context the default route
Make outside routers use ASA interface IP matching each context:
R2# ip route 10.0.0.0 255.255.255.0 20.0.0.101
R2# ip route 30.0.0.0 255.255.255.0 20.0.0.102
2. Limited crypto- no crypto config - limited enough to not support VPN termination
3. Can't switch between firewall mode (bridging) or routed mode inside a context.

Multicontext and user databases for AAA. Set up in either the admin context (admin privilege!) or specific to a user context.

Allowing telnet access:
ASA3/CONTEXT1# config t
ASA3/CONTEXT1(config)# username john password cisco
ASA3/CONTEXT1(config)# telnet ?
-- prompts for ip4, ip6 address or hostname (0 for any)
ASA3/CONTEXT1(config)# telnet 0 ?
-- prompts for IP netmask
ASA3/CONTEXT1(config)# telnet 0 0 ?
-- prompts for interface
ASA3/CONTEXT1(config)# telnet 0 0 inside <--- turns on the telnet server

```
ASA3/CONTEXT2(config)# aaa ?

configure mode commands/options:
  accounting      Configure user accounting parameters
  authentication  Configure user authentication parameters
  authorization   Configure user authorization parameters
  local           AAA Local method options
  mac-exempt      Configure MAC Exempt parameters
  proxy-limit     Configure number of concurrent proxy connections allowed per
                  user
ASA3/CONTEXT2(config)# aaa authentication ?

configure mode commands/options:
  enable              Enable
  exclude             Exclude the service, local and foreign network which
                      needs to be authenticated, authorized, and accounted
  http                HTTP
  include             Include the service, local and foreign network which
                      needs to be authenticated, authorized, and accounted
  listener            Configure an HTTP or HTTPS authentication listener
  match               Specify this keyword to configure an ACL to match
  secure-http-client  Specify this keyword to ensure HTTP client authentication
                      is secured (over SSL)
  serial              Serial
  ssh                 SSH
  telnet              Telnet
ASA3/CONTEXT2(config)# aaa authentication telnet ?

configure mode commands/options:
  console  Specify this keyword to identify a server group for administrative
           authentication
ASA3/CONTEXT2(config)# aaa authentication telnet con
ASA3/CONTEXT2(config)# aaa authentication telnet console ?

configure mode commands/options:
  LOCAL  Predefined server tag for AAA protocol 'local'
  WORD   Name of RADIUS or TACACS+ aaa-server group for administrative
         authentication
ASA3/CONTEXT2(config)# aaa authentication telnet console LOCAL
```

Since this user is set up through this specific context, it would not be able to use the changeto command. An admin telnet AAA configuration would have to be configured in order to administer the box rather than a specific context

We need different isolated AAA databases for each context and the admin mode Using the same TACACS+ or RADIUS servers to do authentication on multiple contexts violates the idea of having the contexts completely segregated!

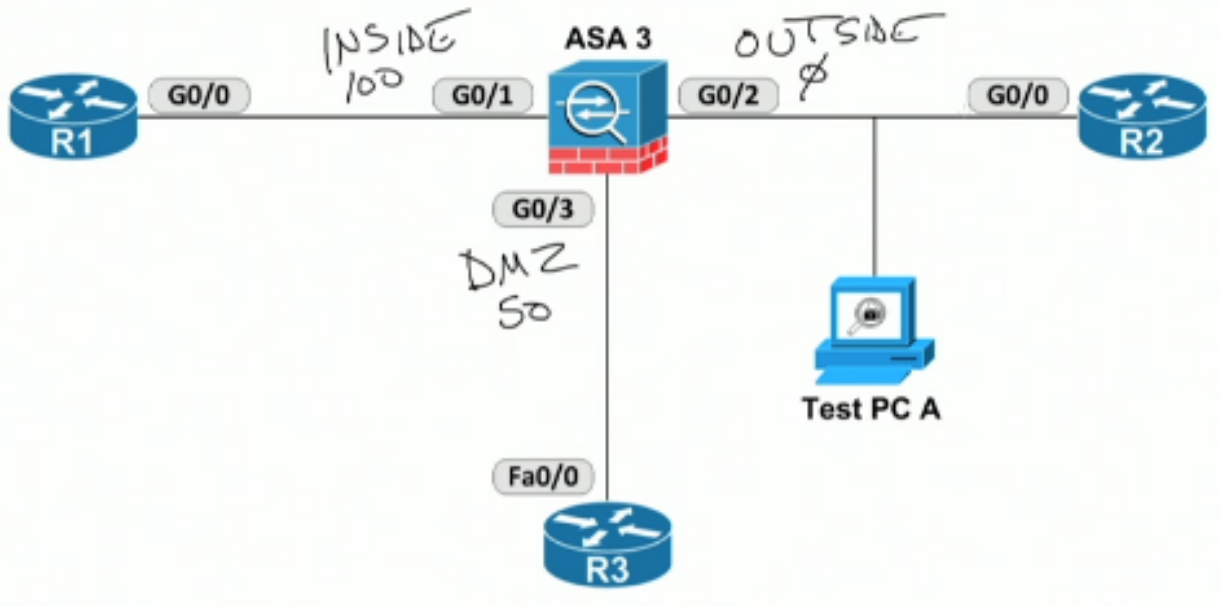
<u>One solution here is to isolate the admin context to the unused G0/0 on the ASA, as the only allocated interface:</u>

changeto system
context admin
allocate interface g0/0
int g0/0
noshut
changeto admin
int g0/0

ip address 192.168.0.254 255.255.255.0
nameif inside
no shut
username john password cisco
telnet 0 0 inside
-- at this point go over to the switch where the ASA is plugged up as fa1/0/16 give it 192.168.0.1 no switchport, no shut. Telnet over and we can get in as admin, change contexts as desired.

End of section discussion: Prompt
Prompt command to change prompt. Default is "prompt hostname context" (see **sh run | include prompt**) but you can also use domain, hostname, priority or state (for "traffic passing state")
"hostname context state" is good for failover so you can see if you are primary or secondary- or the active or standby device
(because you want to make changes on the active one so it replicates to standby) This puts it right in the prompt so you don't have to check

Setup for ASDM presentation



In this topology, Test PC A is for running ASDM and testing IPSEC Remote Access VPN client, and SSL VPN (AnyConnect client) in the next sections. This is now going to be using ASA 9.3, routing on routers is OSPF area 0 with loopback on each (naturally)

Review: traffic flows from higher level zone to lower freely, then on responce (from lower trusted to higher level)checks if there is a state table entry - checks connection table, if

no matching entry it looks for an ACL entry/exception - if it can't apply it drops the traffic the packets are dropped.
In this case this will be sending traffic to the control/management plane directly, so the configuration is going to be controlled different than making exceptions to the normal filtering engine.
By default everything is denied on the control plane

ASA3(config)# http server enable <--- turn on web service
ASA3(config)# http 10.0.0.1 255.255.255.255 inside <---which connection is allowed
<---- at this point there are other http options with the http command- including authentication-certificate
<---- of note with certs is ASA defaults to a self-signed cert, so when logging in, you may get a cert error

```
ASA3(config)# http ?

configure mode commands/options:
  Hostname or A.B.C.D          The IP address of the host and/or network
                               authorized to access the HTTP server
  X:X:X:X::X/<0-128>           IPv6 address/prefix authorized to access the HTTP
                               server
  authentication-certificate   Request a certificate from the HTTPS client when
                               a management connection is being established
  redirect                     Redirect HTTP connections to the security gateway
                               to use HTTPS
  server                       Enable the http server required to run Device
                               Manager
```

http 0 0 outside <---allow http from any source, any mask through interface "outside"
dir disk0: <--- find asdm image first
asdm image disk0:asdm-731-101.bin
<--- 731 IS actually 9.3 (even though in the dir listing there is another file that says 9.3- it isn't the one.) Check CLI docs
<--- the ASDM version here is 7.x.x which is why the numbering change is present

On PC A, browser to 20.0.0.254, install launcher
Enter username password, run ASDM-IDM launcher

Presentation skips most of the Wizard, says we will come back to it and address version differences
Quick look at routing - got OSPF up,
Verified routing table updates going to routers which of course doesn't guarantee routED traffic
which depends on stateful firewall, security levels, ACL exceptions

Logging control, you can set up filtering based on message type- for example
%ASA-7-710005: UDP request discarded from 10.0.0.200/64281 to

inside:10.0.0.254/53
This line as an example, you could enable or disable seeing this with it's identifying number (710005)
(Logging>Syslog Setup)
These numbers aren't found easily in the docs, so the quickest way is sometimes to find them in the logs already collected.

Site to Site IPSEC VPN - Video 6

R2 IOS to ASA tunnel to route traffic from R2 over the VPN to R1 to get access to the resources behind R1
OSPF is set up, we are bypassing the inspection engine

On interfaces, by default, all traffic is going to be denied when it comes from an outside interface in (due to the
By default, VPNs are allowed unless we specify that VPN connections are subject to ACL filtering, because they are treated like an internal interface. Traffic is allowed in the VPN tunnel to the inside or to the DMZ - it's basically not going to have to go through the inspection engine in order to get through to it's destination
First, we have to define tunnel group. It is either LAN-to-LAN (site to site- what is the dest endpoint?) or Remote Access tunnel.

3 default tunnel-groups:
DefaultL2LGroup (LAN-to-LAN/Site-to-Site) gets IP address
DefaultRAGroup (IPSEC RA) gets VPN tunnel-group address
DefaultWEBVPNGroup (SSL VPN)

```
ASA3# show run all tunnel-group
tunnel-group DefaultL2LGroup type ipsec-121
tunnel-group DefaultL2LGroup general-attributes
 no accounting-server-group
 default-group-policy DfltGrpPolicy       <-------------------group policy refers to
tunnel-group DefaultL2LGroup ipsec-attributes
 no ikev1 pre-shared-key    <-----------------------------------password
 peer-id-validate req
 no chain
 no ikev1 trust-point    <-----------------------------------cert authority
 isakmp keepalive threshold 10 retry 2
 noikev1 remote-authentication
 no ikev1 local-authentication

tunnel-group DefaultRAGroup type remote-access
tunnel-group  general-attributes
```

```
 no address-pool
 no ipv6-address-pool
 authentication-server-group LOCAL
 secondary-authentication-server-group none
 no accounting-server-group
 default-group-policy DfltGrpPolicy
 no dhcp-server
 no strip-realm
 no nat-assigned-to-public-ip
 no scep-enrollment enable
 no password-management
 no override-account-disable
etc etc - DefaultRAGroup webvpn-attributes, ipsec-attributes, etc...

tunnel-group DefaultWEBVPNGroup ppp-attributes
 no authentication pap
 authentication chap
 authentication ms-chap-v1
 no authentication ms-chap-v2
 no authentication eap-proxy
```

GrpPolicy - things like what traffic allowed, wins and dns server, whether the user gets a banner, message- tons of stuff
Too much to put here
L2L gets IP address
RA gets VPN group address
These tunnel groups in turn get/call a group policy attached - the one DfltGrpPolicy
If you don't change anything, all of the groups and policy will be defaults provided

In IOS, for IPSec we set up
Phase 1) define ISAKMP/IKEv1/ rarely except newer stuff uses IKEv2 (AnyConnect uses suite B encryption)
 - set encryption, authent, hashing, and DH Group - all make up what is referred to formally as the IKE policy
Phase 2)
 - who (IP, tunnel group - "peer") What (ACL allowed traffic) How (IPSEC transform set attributes)

```
R2#show run | section isakmp
crypto isakmp policy 1
 encr aes 256
 authentication pre-share
 group 2
crypto isakmp key cisco address 20.0.0.254
crypto map MAP1 10 ipsec-isakmp
 set peer 20.0.0.254
 set transform-set ESP-AES-256-MD5
 match address CRYPTO
```

Default ISAKMP AES 256, PSK, DH Group 2, SHA 128
crypto isakmp key CISCO address 20.0.0.254
 -pass is CISCO, address is that IP
Here it uses an ACL for crypto map called MAP1, saying:
permit ip host 2.2.2.2 10.0.0.0 0.0.0.255
2.2.2.2 is R2's loopback, 10.0.0.0/24 is the inside network
(source, dest) Common mistake is if tunnels ACLs don't match up the tunnel will be rejected
What traffic is allowed is the "match address CRYPTO" line (CRYPTO is an ACL)

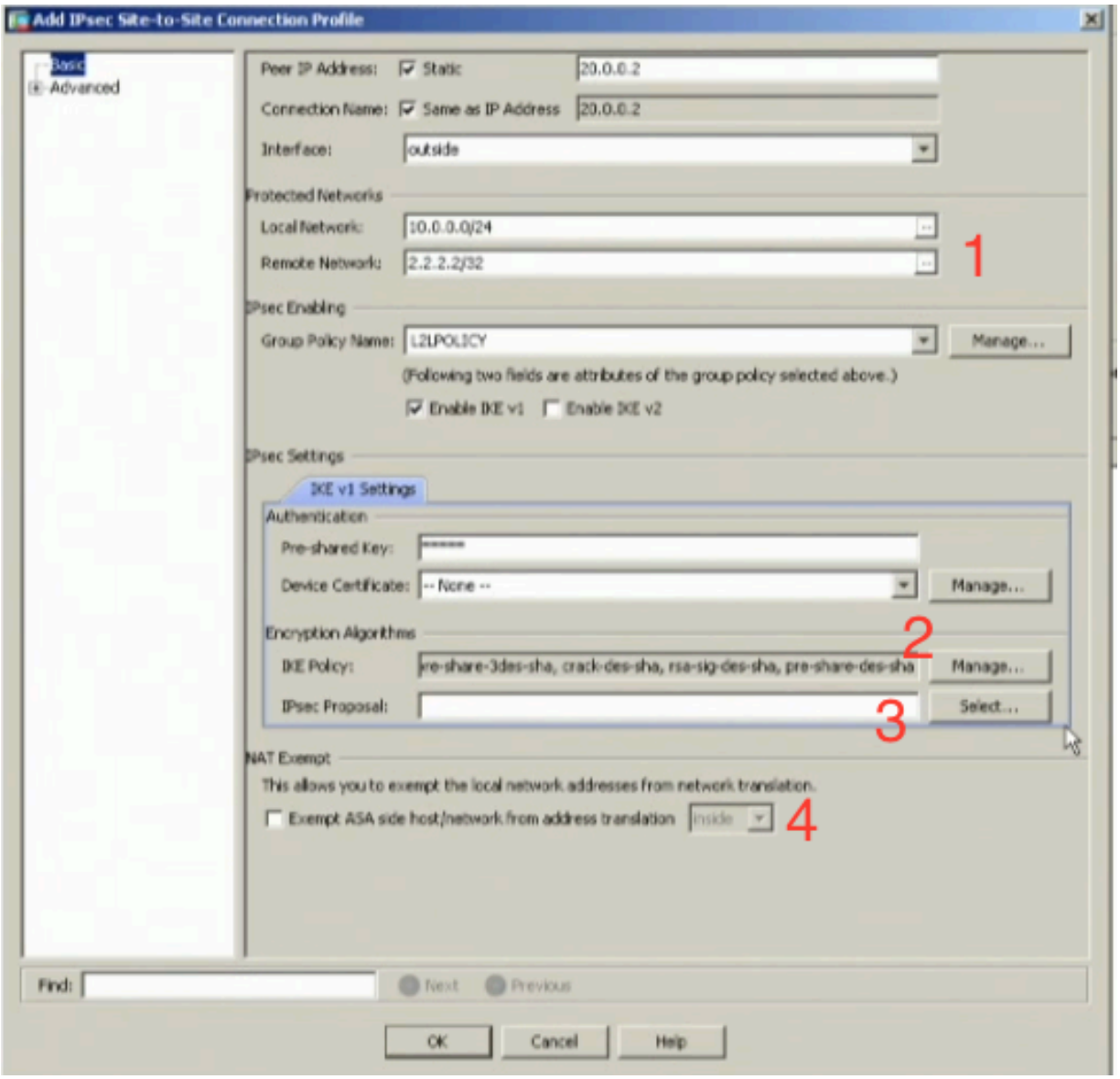
sh run | s isakmp
sh run | section crypto
sh run | s access-list
show crypto isakmp policy
show crypto ipsec transform-set
crypto map of course is just your phase 2 transform set

```
R2#show crypto ipsec transform-set
Transform set default: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },

Transform set ESP-AES-256-MD5: { esp-256-aes esp-md5-hmac  }
   will negotiate = { Tunnel,  },
```

Everything on the router has to be matched in ASA!

PSK or certs? IKEv2 has 'flexible authentication' where one end can use PSK and other a cert. IKEv1 has to match

That was on R2's IOS Config. Here is the ASDM setup:
In ASDM click "Configuration" on top" and choose "Site-to-Site VPN" on the bottom left
A tunnel-group is called a "connection profile" in ASDM (click "Add" to make one)



1 - match what is in R2's IOS sh run | section access-list

L2L policy was created to simply uncheck ikev2 box without modifying defaults

IKE setup preshared key is just CISCO

2 - sh run | section crypto and the info for "crypto isakmp policy 1" (and sha-128) Also in "sh crypto isakmp policy"

This field will have every possible option to match the other side (pre-populated- leave as-is)

3 - IPSec proposal is phase2- match what is in R2's IOS sh crypto ipsec transform-set, be sure to select the one that says 'tunnel mode'

4 - NAT Exempt (exempt local network from translation)

Normally needed when ASA is edge device doing translation and termination at the same time

Order of operations issue- If the traffic gets NAT'd going out, and then ends up getting NAT'd before entering the tunnel, it might not be encrypted (or worse). This should be reviewed in the NAT section. IPSEC tunnels and NAT need careful

consideration when run together
Box doesn't need checking for this in this example.
Click 'ok' and be sure to check box afterward enabling IKEv1 on the interface

[[If you have a NAT rule that says all traffic from the inside of my network going out to the internet needs to have my outside address
Then, if you are trying to do a VPN tunnel to the outside, when traffic from inside goes out, it will get translated to the outside address before it goes in the VPN tunnel, and the traffic would not be encrypted]]

So on the ASA at the command line, **sh run crypto** will have a long, long list such as below to match what is on the other side
If there is no match to the other side, a tunnel isn't going to happen.

```
crypto ikev1 policy 10
 authentication crack
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 30
 authentication pre-share
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
```

There is also a line "crypto ikev1 enable outside" which is matches to the checkbox in the ASDM

```
ASA3# sh run tunnel-group
tunnel-group 20.0.0.2 type ipsec-l2l
tunnel-group 20.0.0.2 general-attributes
 default-group-policy L2LPOLICY
tunnel-group 20.0.0.2 ipsec-attributes
 ikev1 pre-shared-key *****
```

Usually an ASA would have several tunnel groups but this is the only one this one is listening for
If the IP address doesn't match the UDP port 500 IKE for this IP address, the tunnel isn't happening.
(Unless there is an ACL exception, to let the traffic inbound to another device or something)

it is IKE v1 that only goes up to DH Group 4 or 5 - IKEv2 goes up to the higher (more acceptable numbers) If you have have a VPN and only have IKE1, forget it- Use SSL VPN instead.

It is NOT out of the question to go in and remove transform sets that you won't be using or don't want to support
These are simply all provided to us to make everything as plug-n-play as possible

In fact removing those you know clients won't need will make the list of available policies to check for a match smaller and quicker
(Site-to-site you will know what the other side has)

In testing- pings, traceroutes originating from the ASA will have the ip address of the outgoing interface on the ASA even if you tell it differently. You should run those services from the routers instead. This makes sense if you look at the tunnel's ACL which states that the start of the tunnel is the interface on the inside of the firewall (10.0.0.0/24). Consider the visibility- the firewall is outside the tunnel so the firewall's interfaces and presence isn't even seen by the endpoints

Same in IOS and ASA:
show crypto isakmp -- phase 1
show crypto isakmp sa --phase 2
show crypto ipsec sa

----------R2# show crypto isakmp sa
- Status- active. GOOD
- if you see state of QM_IDLE it's ok- that is quick mode - has passed to Phase 2.
- MM_ACTIVE is main mode (we'll see in ASA below), also ok

```
R2#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
20.0.0.254      20.0.0.2        QM_IDLE           1017 ACTIVE

IPv6 Crypto ISAKMP SA
```

R2# show crypto ipsec sa
- more info - SPI security parameter index - sort of a sequence id

----------show crypto isakmp sa FROM R2 (IOS):
current peer is the ASA's address .254
tunnel is sourced from 20.0.0.2
Local ident are the tunnel's endpoints
pkts encaps/decaps are our traffic count
SPI - Security Parameter Index: sequence number for the tunnel inbound and outbound, with it is tunnel crypto and hashing info
Sequence # inside the actual data packets

```
interface: GigabitEthernet0/0
    Crypto map tag: MAP1, local addr 20.0.0.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (2.2.2.2/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (10.0.0.0/255.255.255.0/0/0)
   current_peer 20.0.0.254 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 18, #pkts encrypt: 18, #pkts digest: 18
    #pkts decaps: 16, #pkts decrypt: 16, #pkts verify: 16
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 20.0.0.2, remote crypto endpt.: 20.0.0.254
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
     current outbound spi: 0xBD743E0E(3178511886)
     PFS (Y/N): N, DH group: none
     inbound esp sas:
      spi: 0xDF5CB0FC(3747393788)
        transform: esp-256-aes esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 2005, flow_id: Onboard VPN:5, sibling_flags 80000040, crypto map: MAP
1
        sa timing: remaining key lifetime (k/sec): (4262900/3441)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xBD743E0E(3178511886)
        transform: esp-256-aes esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 2006, flow_id: Onboard VPN:6, sibling_flags 80000040, crypto map: MAP
```

On the ASA side: See ASA-Logs-LONG-Site-to-SiteVPN.png
This is just regular logging- not debug see the file above for annotations in actual log

Packets received on 20.0.0.254:500 from 20.0.0.2:500
  -IKE udp port from R2 and ASA exterior port

IKE SA Proposal #1 Transform #1 acceptable .. matches policy entry 13
  - it matches internal settings for #13 in our listfor phase 1

Connection landed on tunnel group 20.0.0.2
---
retrieved default group policy L2LPOLICY (remember? filters, dns server, ip addresses, all that)
PHASE 1 completed

IPSec SA Proposal #1, Transform #1 acceptable
--- ESP Phase 2 transform set, tunnel parameters etc stuff accepted
IKE: requesting SPI!

Security negotiation complete for LAN-toLAN
...
Built inbound ICMP
Teardown ICMP
Sending keep-alives.....

To see if tunnel is up on ASA outside of that log:

----------show crypto isakmp

```
ASA3# show crypto isakmp

IKEv1 SAs:

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 20.0.0.2
    Type    : L2L             Role    : responder
    Rekey   : no              State   : MM_ACTIVE

There are no IKEv2 SAs

Global IKEv1 Statistics
  Active Tunnels:              1
  Previous Tunnels:           20
  In Octets:               63813
  In Packets:                569
  In Drop Packets:            17
  In Notifys:                459
  In P2 Exchanges:            19
  In P2 Exchange Invalids:     0
  In P2 Exchange Rejects:     14
  In P2 Sa Delete Requests:    4
  Out Octets:              60100
```

Shows phase 1, shows IKEv1 or v2, responder means the other side negotiated it, MM_active is "main mode" - IOS side should say QM_idle or QM-idle

----------show crypto ipsec sa

```
ASA3# show crypto ipsec sa
interface: outside
    Crypto map tag: outside_map0, seq num: 1, local addr: 20.0.0.254

      access-list outside_cryptomap extended permit ip 10.0.0.0 255.255.255.0 host 2.2
.2.2
      local ident (addr/mask/prot/port): (10.0.0.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (2.2.2.2/255.255.255.255/0/0)
      current_peer: 20.0.0.2


      #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
      #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 20.0.0.254/0, remote crypto endpt.: 20.0.0.2/0
      path mtu 1500, ipsec overhead 74(44), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: DF5CB0FC
      current inbound spi : BD743E0E
<--- More --->
```

```
  inbound esp sas:
    spi: 0xBD743E0E (3178511886)
       transform: esp-aes-256 esp-md5-hmac no compression
       in use settings ={L2L, Tunnel, IKEv1, }
       slot: 0, conn_id: 118784, crypto-map: outside_map0
       sa timing: remaining key lifetime (kB/sec): (4373999/3049)
       IV size: 16 bytes
       replay detection support: Y
       Anti replay bitmap:
        0x00000000 0x0000001F
  outbound esp sas:
    spi: 0xDF5CB0FC (3747393788)
       transform: esp-aes-256 esp-md5-hmac no compression
       in use settings ={L2L, Tunnel, IKEv1, }
       slot: 0, conn_id: 118784, crypto-map: outside_map0
       sa timing: remaining key lifetime (kB/sec): (4373999/3047)
       IV size: 16 bytes
```

Actual tunnel, network to network, tunnel endpoint,
10.0.0.0/24, 2.2.2.2/32, current peer 20.0.0.0.2
We have packet stats, make sure the SPI numbers match, if not it is a "code bug" of some kind (his words)
[compare SPIs between ASA and other device]
SPI (Security Parameter Index) is a counter but also serves a purpose to identify to the application layer which tunnel customer traffic is for when multiple tunnels go to the same destination.
Each ACL for a tunnel would have a separate SPI created for it

sh local-host all or sh connection detail gives us more:

```
  Conn:
    OSPF dmz 30.0.0.3 NP Identity Ifc  224.0.0.5, idle 0:00:00, bytes 27288, flags
Interface outside: 4 active, 4 maximum active, 0 denied
local host: <20.0.0.2>,
    TCP flow count/limit = 0/unlimited
    TCP embryonic count to host = 0
    TCP intercept watermark = unlimited
    UDP flow count/limit = 1/unlimited

  Conn:
    ESP outside 20.0.0.2 NP Identity Ifc  20.0.0.254, idle 0:00:05, bytes 2632, flags

    UDP outside  20.0.0.2:500 NP Identity Ifc  20.0.0.254:500, idle 0:00:25, bytes 136
52, flags -
    OSPF outside 20.0.0.2 NP Identity Ifc  224.0.0.5, idle 0:00:08, bytes 27420, flags

    ESP outside 20.0.0.2 NP Identity Ifc  20.0.0.254, idle 0:00:05, bytes 2540, flags

local host: <2.2.2.2>,
    TCP flow count/limit = 1/unlimited
    TCP embryonic count to host = 0
    TCP intercept watermark = unlimited
    UDP flow count/limit = 0/unlimited

  Conn:
    TCP outside  2.2.2.2:58037 inside  10.0.0.1:23, idle 0:00:05, bytes 109, flags UIO
B
local host: <224.0.0.5>,
    TCP flow count/limit = 0/unlimited
    TCP embryonic count to host = 0
    TCP intercept watermark = unlimited
    UDP flow count/limit = 0/unlimited

  Conn:
    OSPF outside 224.0.0.5 NP Identity Ifc  20.0.0.254, idle 0:00:06, bytes 27756, fla
gs
local host: <20.0.0.200>,
```

We still se traffic subject to inspection
ESP for the tunnel, and UDP 500 for the IKE negotiation
The telnet connection is described below, which demonstrates we have decryption then inspection

The telnet connection brings up an interesting point:
As traffic is received from the tunnel it is going to be treated as if it comes from the most-trusted interface
Outside in should work:
R2# ping 10.0.0.1 source 2.2.2.2 (works)
R2# telnet 10.0.0.1 /source-interface lo0 (works) - this is the telnet connection in the above sh local-host all output above

From the inside back outbound, devices that are not matched in the "proxy ACL" or "proxy identities" defined by the access list:

```
ASA3# sh access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list outside_cryptomap; 1 elements; name hash: 0x39bea18f
access-list outside_cryptomap line 1 extended permit ip 10.0.0.0 255.255.255.0 host 2.
2.2.2 (hitcnt=1) 0x887725aa
access-list outside_cryptomap_1; 1 elements; name hash: 0x759febfa
access-list outside_cryptomap_1 line 1 extended permit ip 10.0.0.0 255.255.255.0 host
10.20.30.40 (hitcnt=0) 0x9f900274
```

Unless traffic matches this line specifically, it isn't going to be allowed to come into the tunnel:

"access-list outside_cryptomap line 1 extended permit ip 10.0.0.0 255.255.255.0 host 2.2.2.2 (hitcnt=1) 0x887725aa"

We can telnet to R1, but only when it is sourced from the loopback interface

R2# telnet 10.0.0.1 (wont work)

It won't work because it is coming from a different IP that doesn't match the proxy identities, and it isn't allowed inbound on the tunnel

Described as part of the Phase 2 negotiation, that if the ACLs did not match between the endpoints, the tunnel would not set up.

The error would be reported as related to the negotiation of the tunnel, and no SPI

debug crypto isakmp
debug crypto ipsec
show cypto ipsec sa l spi

After making changes:
clear crypto sa
clear crypto isakmp

Did a test- reversed the IP addresses of source and destination in the ACL of R2, ran those clear crypto commands and looked at the debug messages after ping or telnetting - result is, IKE Phase 1 actually works, it is in Phase 2 of the negotiation parameter check that it messes up and gets refused.

ASA debug message is unclear! "Received non-routine notify message: No proposal chosen"

The responder (R2) will be more specific with something about ACLs not matching up

IPSEC IP 50 ethertype

In IOS IKEv2 is called FlexVPN

SSL VPN for clients - don't need client SW - can use web browser

ASA-sh-run-crypto-transforms-list.png

Order of ops: tunnel group specifies ip addresses, PSK, calls group policy, looks for matching IKE policy (v1 or v2) with DH, hash, enc, then crypto map for transform set

IOS automatically will set up the tunnel, whereas ASA needs "crypto ikev1 enable outside" in the running config to turn it on

Traffic coming in from the tunnel will be treated as if "higher than sec level 100" (?direct quote)
Meaning by default it skips over ACL checks on the interface. Turn that off with the command
"no sysopt connection permit-vpn"
This of course is referring to traffic coming into the tunnel- not the tunnel itself.

Question: How do you ask a customer what the SPI is on their end??

Question- how to change the implicit permit rules with security levels?
If you wanted to prevent inside(100) from sending traffic to DMZ(50) you would need an ACL

```
ASA3(config)# access-LIST INSIDE_IN deny ip 10.0.0.0 255.255.255.0 30.0.0.0 25$
ASA3(config)# ACCESS-LIST INSIDE_IN permit ip any any
ASA3(config)# access-group INSIDE_IN in interface inside
ASA3(config)# end
```

You could also make the DMZ and INSIDE have the same security level (won't pass traffic)
If you wanted to check with packet-tracer
packet-tracer input inside icmp 10.0.0.1 8 0 30.0.0.3

On sec levels - recall the command same-security-traffic permit inter-interface to override the sec level thing

IPSec Remote Access VPN - Video 7

Thought of as for legacy VPN client users rather than those with AnyConnect
IPSec or SSL?
IPSec - Client could be a router using EasyVPN remote feature or endpoint running EasyVPN client
SSL VPN- Just for remote access - not LAN-to-LAN connections - don't need client - can use web browser

vpnsetup command
 --- lays out steps, commands for each you need to use (is a guide) 11:30 in video 7
ASA3(config)# vpnsetup ?
    ipsec-remote-access Display IPSec Remote Access Configuration Commands
    l2tp-remote-access   Display L2TP/IPSec Configuration Commands
    site-to-site   Display IPSec Site-to-Site Configuration Commands
    ssl-remote-access   Display SSL Remote Access Configuration Commands

ciscoasa(config)# vpnsetup ipsec-remote-access steps
  Steps to configure a remote access IKE/IPSec connection with examples:

1. Configure Interfaces
>>THESE ALSO NEED SECURITY LEVELS!
interface GigabitEthernet0/0
ip address 10.10.4.200 255.255.255.0
nameif outside
no shutdown

interface GigabitEthernet0/1
ip address 192.168.0.20 255.255.255.0
nameif inside
no shutdown

2. Configure ISAKMP policy (Phase 1)
>>THIS ALSO NEEDS DH GROUP?
crypto isakmp policy 65535
authentication pre-share <----- in IPSEC RA, tunnel group name is username and tunnel group holds PSK (see below)
encryption aes
hash sha

3. Setup an address pool
ip local pool client-pool 192.168.1.1-192.168.1.254

4. Configure authentication method -------(tunnel-group step5 is group authentication - this is user auth, and assumes you employ a Radius server)
aaa-server MyRadius protocol radius
aaa-server MyRadius host 192.168.0.254
key $ecretK3y

5. Define tunnel group "WHO?"
-------(with group username and group password in ipsec client, the username is the tunnel-group name "client" , and the password the PSK)
tunnel-group client type remote-access
tunnel-group client general-attributes
address-pool client-pool
-------(here is where the address is obtained- the rest from group policy. Here it is DefltGroupPolicy, but in Split Tunnel this will change)
authentication-server-group MyRadius
tunnel-group client ipsec-attributes
pre-shared-key VpnUs3rsP@ss

6. Setup ipsec parameters - transfor set (Phase 2) "HOW"
crypto ipsec transform-set myset esp-aes esp-sha-hmac

7. Setup dynamic crypto map
crypto dynamic-map dynmap 1 set transform-set myset

crypto dynamic-map dynmap 1 set reverse-route

8. Create crypto map entry and associate dynamic map with it
crypto map mymap 65535 ipsec-isakmp dynamic dynmap
--->dynamic since we don't know the ip address of the client like in site-to-site
9. Attach crypto map to interface
crypto map mymap interface outside

10. Enable isakmp on interface
crypto isakmp enable outside

==========

ASDM>Configuration>Remote Access VPN>
(3 options)
Clientless SSL VPN (web browser)
SSL or IPSec(IKEv2) VPN RA (with Cisco AnyConnect client)
IPSec(IKEv1) VPN RA using Cisco VPN client <----------This is the one we are looking at

----Like a LAN-to-LAN tunnel using ESP for encapsulation but is dynamically negotiated
---- On the router side configured with either a dynamic crypto map or a dynamic virtual tunnel interface (DVTI)
---- ASA doesn't use DVTI - uses a dynamic cryptomap to listen for inbound connections

[ASDM Assistant sidebar is basically a webpage in the side frame with hyperlinks leading to the config pages]
1. Address assignment policy - whether to use DHCP or not, local pool;
2. Click on address pools on sidebar to get address pools panel and create a pool (start, end, mask, name)
Example put in 192.168.0.0/24
3. Create IPSec connection profile (tunnel-group). Here you also specify PSK or a TACACS+ or RADIUS auth
a) Instead of the router address like in site-to-site, this will be based on a user group (username)
(the username is going to specify it's own specific tunnel identity - you could make tunnel-groups like engineering or accounting and then tweak it so a username lands in those tunnel groups, and/or uses a specific group policy, but that isn't covered here)
b) we need to create a non-CLI user:

```
ASA3(config)# username rauser password cisco
ASA3(config)# username rauser ?
configure mode commands/options:
  attributes  Enter the attributes sub-command mode for the specified user
  nopassword  Indicates that this user has no password
  password    The password for this user
ASA3(config)# username rauser attributes
ASA3(config-username)#
```

Attributes list has service-type and one of it's options is remote-access (which has no CLI access period.)

ASA3 (config-username)# service-type remote-access

4. Server Group should be "local" and Address assignment should have the DHCP pool name from step 2
5. Policy, a new policy named IPSEC_Policy, leave all settings as-is (default)
6. Finally it asks if you want L2TP or IPSec, choose IPSec.

Click save/ok, and don't forget to hit enable interface before going back to CLI.

Note on settings in CLI- anything not specified will be inherited from the default group policy

[next to the interfaces in the GUI is a checkbox that says "bypass interface access lists for inbound connections" if unchecked the ASA would execute the ""no sysopt connection permit-vpn"" mentioned previously, and they would be able to connect but not have data flows allowed unless added to further access list design. (in other words, just leave it checked)]

After setting up the ASDM group info:

sh run crypto has a dynamic map which specifies transform-sets, which is in turn called from a static cryptomap

```
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev1 transform-set ESP-AES-128
-SHA ESP-AES-128-MD5 ESP-AES-192-SHA ESP-AES-192-MD5 ESP-AES-256-SHA ESP-AES-256-MD5 E
SP-3DES-SHA ESP-3DES-MD5 ESP-DES-SHA ESP-DES-MD5
crypto map outside_map0 1 match address outside_cryptomap
crypto map outside_map0 1 set peer 20.0.0.2
crypto map outside_map0 1 set ikev1 transform-set ESP-AES-256-MD5
crypto map outside_map0 2 match address outside_cryptomap_1
crypto map outside_map0 2 set peer 1.2.3.4
crypto map outside_map0 2 set ikev1 transform-set ESP-AES-128-SHA ESP-AES-128-MD5 ESP-
AES-192-SHA ESP-AES-192-MD5 ESP-AES-256-SHA ESP-AES-256-MD5 ESP-3DES-SHA ESP-3DES-MD5
ESP-DES-SHA ESP-DES-MD5
crypto map outside_map0 2 set ikev2 ipsec-proposal AES256 AES192 AES 3DES DES
crypto map outside_map0 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTO_MAP
crypto map outside_map0 interface outside
crypto ca trustpool policy
crypto ikev2 policy 100
```

IPSec RA

This gets the number 65535 to ensure remote access gets picked last. If you later intend site-to-site, and it picks remote access as a fit when it needs something else, it will close the cryptomap giving you the wrong one, so put remote access at the bottom of the list of them.

sh run tunnel-group

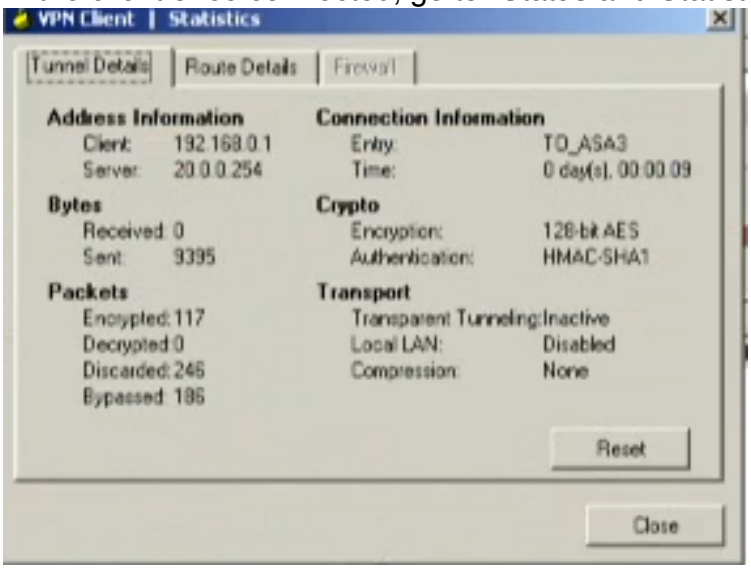
```
tunnel-group RAGROUP1 type remote-access
tunnel-group RAGROUP1 general-attributes
 address-pool IPSEC_RA_POOL
 default-group-policy IPSEC_RA_POLICY
tunnel-group RAGROUP1 ipsec-attributes
 ikev1 pre-shared-key *****
```

sh run group-policy

```
group-policy IPSEC_RA_POLICY internal
group-policy IPSEC_RA_POLICY attributes
 vpn-tunnel-protocol ikev1
```

If this said SSL, that would be WebVPN/SSLClient

On the IPSec RA client, if no box comes up with username and password when hitting 'connect' it probably means something is wrong with the Phase 1 negotiation. If it works we know Phase 1 is fine.
In the client once connected, go to "Status and Statistics" and it brings this up:



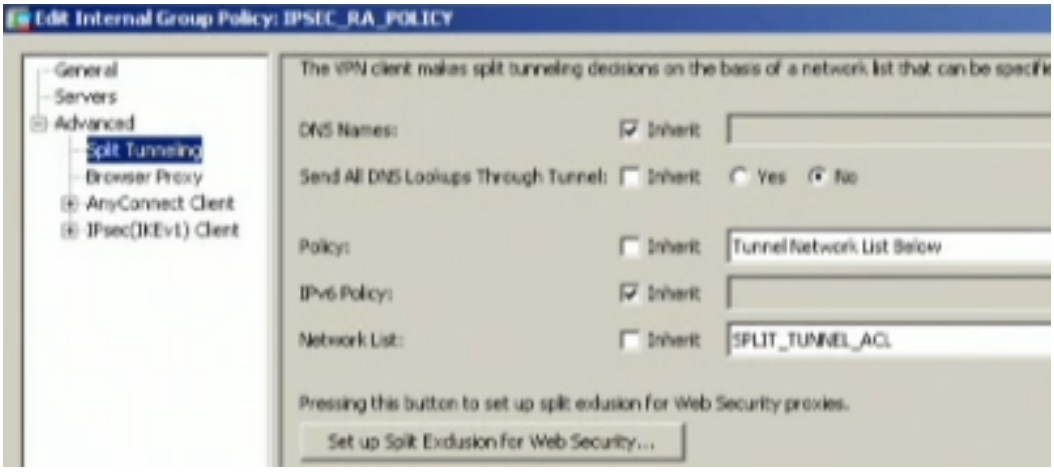
Crypto reflects the transport set.
Says transport is transparent tunnelling is inactive.
Recall that IPSEC ESP is IP 50 ethertype.
NAT problems - generally stateful firewalls can't inspect ESP, and NAT can't do a port translation - THUS it ends up being problematic unless transparent tunnelling is allowed.
In the running config, **crypto isakmp nat-traversal** is supposed to offer transparent to client if they are behind NAT
SSL doesnt have this issue since it is using TCP/IP traffic (ports) but ESP tunnel does need NAT traversal

Also in settings is crypto isakmp nat-traversal> no nat-assigned-to-public-ip
All these sort of issues are generally addressed in group policies/ connection profiles

In the stats window, if you click on the panel "route details" it shows what traffic is allowed over the tunnel (ACL/proxy identities) and 0.0.0.0 0.0.0.0 means any, and indicates that there is no split tunnelling- everything is going through the tunnel and nothing in plaintext except the ISAKMP negotiation and the ESP packets of encapsulated tunnel traffic

ESP vs ESP encapsed in UDP?

Transparent good for when you need to internal traffic to go over the VPN but internet traffic should go out plain text
This is controlled under Group Policy-
In ASDM, see Configuration>Remote Access VPN> Network (Client) Access> IPsec(IKEv1) Connection Profiles click "edit" on desired profile, and then double-click the tunnel group, click manage under "Group Policy", select the group policy to edit, and open advanced options... this is where split tunnels is. (Split meaning there is unencrypted session info in transport outside the ESP tunnel) From here- select "allow traffic from the list below", and make new ACL for allowed traffic, which is applied to the policy



sh access-list

```
access-list SPLIT_TUNNEL_ACL; 1 elements; name hash: 0x22dc5344
access-list SPLIT_TUNNEL_ACL line 1 standard permit 10.0.0.0 255.255.255.0 (hitcnt=0)
```

sh run | group-policy

```
group-policy GroupPolicy1 attributes
 vpn-tunnel-protocol ikev1 ikev2
group-policy IPSEC_RA_POLICY internal
group-policy IPSEC_RA_POLICY attributes
 vpn-tunnel-protocol ikev1
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value SPLIT_TUNNEL_ACL
```

Routing and other issues

Did the address pool we set up get put in the routing table?? Nope!
With tunneling you might run into routing problems since the firewall, VPN, routing table,

and NAT are all separate things. You could put a static route in the routing table... You could add a static entry on R1 to send over to the ASA - ip route 192.168.0.0 255.255.255.0 10.0.0.254

In sh route we see:
In the example OSPF is running - the ASA is advertising a static route inserted when remote access connected- specific IP/32 to the outside interface - (RRI Reverse Route Injection) - inserted by the VPN server to accommodate the client it allocated the address for.

----->Here is another way that it more stable:

```
ASA3(config)# route ?
configure mode commands/options:
Current available interface(s):
  Null0    Null interface
  dmz      Name of interface GigabitEthernet0/3
  inside   Name of interface GigabitEthernet0/1
  outside  Name of interface GigabitEthernet0/2
ASA3(config)# route null0 ?
configure mode commands/options:
  Hostname or A.B.C.D  The foreign network for this route, 0 means default
ASA3(config)# route null0 192.168.0.0 255.255.255.0
ASA3(config)# route-map STATIC_TO_OSPF
ASA3(config-route-map)# match ?
route-map mode commands/options:
  as-path      Match BGP AS path list
  community    Match BGP community list
  interface    Match first hop interface of route
  ip           IP specific information
  ipv6         IPv6 specific information
  metric       Match metric of route
  policy-list  Match IP policy list
  route-type   Match route-type of route
  tag          Match tag of route
ASA3(config-route-map)# match ip ?
route-map mode commands/options:
  address       Match address of route or match packet
  next-hop      Match next-hop address of route
  route-source  Match advertising source address of route
ASA3(config-route-map)# match ip address ?
route-map mode commands/options:
  WORD          IP access-list name
  prefix-list  Match entries of prefix-lists
ASA3(config-route-map)# match ip address prefix-list ?
route-map mode commands/options:
  WORD  IP prefix-list name
ASA3(config-route-map)# match ip address prefix-list IPSEC_RA_POOL
ERROR: Prefix list IPSEC_RA_POOL does not exist
ASA3(config-route-map)# exit
ASA3(config)# ip pre
ASA3(config)# ip pre?
ERROR: % Unrecognized command
ASA3(config)# ip pref
```

```
ASA3(config)# ip pref?
ERROR: % Unrecognized command
ASA3(config)# prefix-list ?
configure mode commands/options:
  WORD             Name of a prefix list
  sequence-number  Include/exclude sequence numbers in NVGEN
ASA3(config)# prefix-list IPSEC_RA_POOL ?
configure mode commands/options:
  deny         Specify packets to reject
  description  Prefix-list specific description
  permit       Specify packets to forward
  seq          sequence number of an entry
ASA3(config)# prefix-list IPSEC_RA_POOL permit 192.168.0.0/24
ASA3(config)# route-map STATIC_TO_OSPF
ASA3(config-route-map)# match ip address prefix-list IPSEC_RA_POOL
```

```
ASA3(config)# router ospf 1
ASA3(config-router)# redistribute ?
router mode commands/options:
  bgp        Border Gateway Protocol (BGP)
  connected  Connected
  eigrp      Enhanced Interior Gateway Routing Protocol (EIGRP)
  ospf       Open Shortest Path First (OSPF)
  rip        Routing Information Protocol (RIP)
  static     Static routes
ASA3(config-router)# redistribute static ?
router mode commands/options:
  metric       Metric for redistributed routes
  metric-type  Set OSPF exterior metric type for redistributed routes
  route-map    Route map reference
  subnets      Consider subnets for redistribution into OSPF
  tag          Set tag for routes redistributed into OSPF
  <cr>
ASA3(config-router)# redistribute static route-map ?
router mode commands/options:
  WORD  Pointer to route-map entries
ASA3(config-router)# redistribute static route-map STATIC_TO_OSPF
% Only classful networks will be redistributed
ASA3(config-router)# redistribute static route-map STATIC_TO_OSPF subnets
ASA3(config-router)# end
ASA3# show ospf database

            OSPF Router with ID (30.0.0.254) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
3.3.3.3         3.3.3.3         531         0x8000000e 0x5658 2
10.0.0.1        10.0.0.1        721         0x8000000e 0x5e86 2
10.0.0.2        10.0.0.2        258         0x80000031 0xd665 3
30.0.0.254      30.0.0.254      6           0x80000006 0xac8e 3

                Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
10.0.0.1        10.0.0.1        721         0x80000005 0x38bf
20.0.0.2        10.0.0.2        509         0x80000005 0xaf3b
30.0.0.3        3.3.3.3         784         0x80000005 0x3ba4

                Type-5 AS External Link States

Link ID         ADV Router      Age         Seq#       Checksum Tag
```

```
192.168.0.0     30.0.0.254      5           0x80000001 0x2dec 0
ASA3#
```

-- now has OSPF AS external route Type-5

This is more stable than adding a static /32 because every time a new tunnel connects it doesn't have to reconverge routes, etc.

The null interface (similar to a loopback in that it is virtual) the /24 is going to be there provisioning it.

This placeholder is also called a "holddown route"

Old way way just to point the route to the outside interface

This null0 technique is fairly new in version 9 and comes with BGP support - in Remote Triggered Black Hole Filtering with Unicast Reverse Path Forwarding (uRPF) - a way to drop traffic in a more scalable way

---

BGP support in Remote Triggered Black Hole Filtering with Unicast Reverse Path Forwarding (uRPF)

Remote Triggered Black Hole (RTBH) filtering is a popular and
effective technique for the mitigation of denial-of-service attacks.

https://tools.ietf.org/html/rfc5635

```
   A common DoS attack directed against a customer of a service
provider
   involves generating a greater volume of attack traffic
destined for
   the target than will fit down the links from the service
provider(s)
   to the victim (customer).  This traffic "starves out"
legitimate
   traffic and often results in collateral damage or negative
effects to
   other customers or the network infrastructure as well.
Rather than
   having all destinations on their network be affected by the
attack,
   the customer may ask their service provider to filter traffic
   destined to the target destination IP address(es), or the
service
   provider may determine that this is necessary themselves, in
order to
   preserve network availability.
destination-based RTBH
   filtering injects a discard route into the forwarding table
for the
   target prefix.  All packets towards that destination, attack
traffic
   AND legitimate traffic, are then dropped by the participating
```

routers,thereby taking the target completely offline. The benefit is
that collateral damage to other systems or network availability at
the customer location or in the ISP network is limited, but the
negative impact to the target itself is arguably increased
By coupling unicast Reverse Path Forwarding (uRPF) [RFC3704]
techniques with RTBH filtering, BGP can be used to distribute discard
routes that are based not on destination or target addresses, but on
source addresses of unwanted traffic. Note that this will drop all
traffic to/from the address, and not just the traffic to the victim

So you make tunnel-groups with different policies
First- ike determines matching crypto policy, then tunnel group is determined (initial username and password), So a group log-in is given to accounting, a different one to engineering, two tunnels with different policies, filters, attributes... They log in with the group credentials, then username.
group policies called by tunnel group with vpn filters, split tunnelling, ip address pools, etc...
sh run all tunnel-group
sh run all group-policy
Anything not specified in any of these policies, etc, gets inherited from the defaults and you can find it there.

no logging on
undebug all

Securing the data Plane and Secure Connectivity config guides:
http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/config_library/15-mt/secdata-15-mt-library.html
http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/config_library/15-mt/secon-15-mt-library.html
EasyVPN remote is the client built into routers (and supports using dynamic addressing)

Putting the client config on a router is something like this:

```
R2(config)#crypto ipsec client ezvpn easy_vpn_remote
R2(config-crypto-ezvpn)# peer 20.0.0.254
R2(config-crypto-ezvpn)# group RAGROUP1 key cisco
R2(config-crypto-ezvpn)# mode client
R2(config)#int g0/0
R2(config-if)#ip address
R2(config-if)#ip address 20.0.0.222 255.255.255.0
R2(config-if)#crypto ipsec client ezvpn easy_vpn_remote
R2#crypto ipsec client ezvpn connect
```
(This failed in the demo unceremoniously but it was obvious from debug messages the other config was interfering)

http://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/vpn/asa_91_vpn_config/vpn_groups.html
http://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/vpn/asa_91_vpn_config/vpn_groups.html#73582

username <user> attributes subcommands
Show up when viewing "sh run username" in a list under username <user> attributes
With remote access, one of the endpoints is unknown/ dynamic, compared to site-to-site where we define both

The username attributes command enters username attributes mode, in which you can configure any of the following attributes:

group-lock
  Names an existing tunnel group with which the user is required to connect.

password-storage
  Enables or disables storage of the login password on the client system.

service-type [remote-access | admin | nas-prompt]
  Restricts console login and enables login for users who are assigned the appropriate level. **The remote-access option specifies basic AAA services for remote access**. The admin option specifies AAA services, login console privileges, EXEC mode privileges, the enable privilege, and CLI privileges. The nas-prompt option specifies AAA services, login console privileges, EXEC mode privileges, but no enable privileges.

ssh authentication { pkf [nointeractive] | publickey key [hashed]}
  Enables public key authentication on a per-user basis. The value of the key argument

can refer to the following:

When the key argument is supplied and the hashed tag is not specified, the value of the key must be a base64 encoded public key that is generated by SSH key generation software that can generate SSH-RSA raw keys (that is, with no certificates). After you submit the base64 encoded public key, that key is then hashed via SHA-256 and the corresponding 32-byte hash is used for all further comparisons.

When the key argument is supplied and the hashed tag is specified, the value of the key must have been previously hashed with SHA-256 and be 32 bytes long, with each byte separated by a colon (for parsing purposes).

The pkf option enables you to authenticate using 4096-bit RSA keys as an SSH public key file (PKF). This option is not restricted to 4096-bit RSA keys, but can be used for any size less than or equal to 4096-bit RSA keys.

The nointeractive option suppresses all prompts when importing an SSH public key formatted key. This noninteractive data entry mode is only intended for ASDM use.

The key field and the hashed keyword are only available with the publickey option, and the nointeractive keyword is only available with the pkf option.

When you save the configuration, the hashed key value is saved to the configuration and used when the ASA is rebooted.

Note You can use the PKF option when failover is enabled, but the PKF data is not automatically replicated to the standby system. You must enter the write standby command to synchronize the PKF setting to the standby system in the failover pair.

vpn-access-hours
Specifies the name of a configured time-range policy.

vpn-filter
Specifies the name of a user-specific ACL.

vpn-framed-ip-address
Specifies the IP address and the netmask to be assigned to the client.

vpn-group-policy
Specifies the name of a group policy from which to inherit attributes.

vpn-idle-timeout [alert-interval]
Specifies the idle timeout period in minutes, or none to disable it. Optionally specifies a pre-timeout alert interval.

vpn-session-timeout [alert-interval]
Specifies the maximum user connection time in minutes, or none for unlimited time. Optionally specifies a pre-timeout alert interval.

vpn-simultaneous-logins
Specifies the maximum number of simultaneous logins allowed.

vpn-tunnel-protocol

Specifies permitted tunneling protocols.

webvpn
Enters username webvpn configuration mode, in which you configure WebVPN attributes.
==========

From QA - Easy VPN Client is built into the router
IPSEC usually over ESP or ESP encapsulated inside of UDP if needed

SSLVPN - Video 8

2 types of connecting- clientless with web browser or Anyconnect/ secure mobility client
DefaultWEBVPNGroup, with DfltGrpPolicy and vpn-filter

After Configure>Remote Access>SSL or IPsec(IKEv2) VPN RA (including AnyConnect client)
Again, ASDM assistant sidebar has hyperlink instructions, address assignment policy first, configure address pool (using 192.168 already configured), AnyConnect VPN profile.
Checkbox: enable AnyConnect VPN
Asks if you want to designate an image? This is for offering a client to download (client for Windows)
Allow access on interface checkbox
Bypass interface ACLs for AnyConnect connections (so we don't have to sysopt command or ACLs)
Allow user to select connection profile on login page - leaving this blank to see how it messes up on login (see below)
Create connection profile- name SSL_VPN_GROUP alias is SSL_ALIAS, Local auth, pool is the same (192.168) New policy SSLVPN_POLICY as before keep defaults, we just need one named new.
Checkbox enable SSL VPN protocol (yes) Asks for DNS, WINS, etc servers (left blank)
Gives option to offer IKEv2 unchecked.

Instead of ipsec-attributes, this will use webvpn-attributes
Instead of show crypto isakmp or ipsec (crypto is not for any SSL)
show vpn-sessiondb ---sessiondb also shows stats on all types of VPN though
show vpn-sessiondb anyconnect

show webvpn
debug vpn-sessiondb
debug webvpn

```
ASA3# sh run webvpn
webvpn
 enable outside
 anyconnect image disk0:/anyconnect-win-3.0.11042-k9.pkg 1
 anyconnect enable
 error-recovery disable
```

-- Listening on the outside for 443
-- Offers client.

Connect to 20.0.0.254, it asks you to log in, a username (RAUSER)

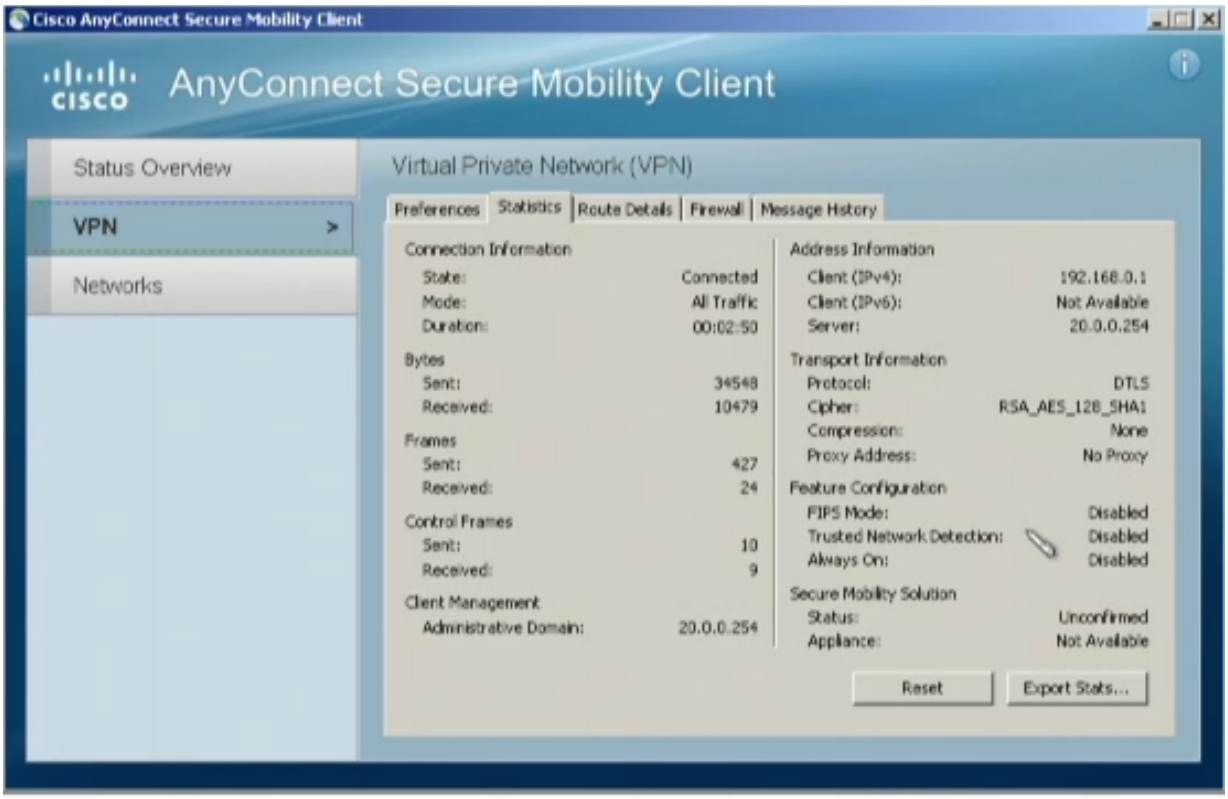
```
%ASA-7-734003: DAP: User rauser, Addr 20.0.0.200: Session Attribute aaa.cisco.tunnelgr
oup = DefaultWEBVPNGroup
%ASA-6-734001: DAP: User rauser, Addr 20.0.0.200, Connection AnyConnect: The following
 DAP records were selected for this connection: DfltAccessPolicy
 SESS_Mgmt_FreeSessionFileLineFunc: unable to delete session from tree!
%ASA-6-725007: SSL session with client outside:20.0.0.200/1447 terminated.
%ASA-6-302014: Teardown TCP connection 1930 for outside:20.0.0.200/1447 to identity:20
.0.0.254/443 duration 0:00:00 bytes 1103 TCP Reset-I
```

DfltAccessPolicy is called from DfltGroupPolicy and DefaultWEBVPNGroup

Common error on ASA VPN server- when user goes to log in, if somehow they aren't logging into the correct group, auth could be denied, or attributes like IP address pool, filters, etc could be incorrect.
If there are problems always make sure the user is being assigned to the correct tunnel group to begin with

Returning to checkbox "Allow user to select connection profile on login page"
If this isn't checked and the user is not queried, everyone is just going to fall back to the default WEBVPN group
You can edit the defaults, but that's never a good idea!
There is AnyConnect Profile Editor program that spits out XML to upload to the ASA...
BUT,
ASDM is actually better than CLI for editing this stuff- you can just edit profiles directly
Best option - in ASDM AnyConnect Client Profile under Remote Access VPN
Set up an alias that has a URL matching a specific tunnel group

Ultimately, just check the damn box allowing them to choose the profile we made! (SSL_ALIAS)
- client gets pulldown menu labelled "group"



==========

DTLS- Datagram Transport Layer Security

(Wikipedia) - "provides security for datagram-based applications by allowing them to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery. Is based on the stream-oriented Transport Layer Security (TLS) protocol and is intended to provide similar security guarantees. The DTLS protocol datagram preserves the semantics of the underlying transport — the application does not suffer from the delays associated with stream protocols, but has to deal with packet reordering, loss of datagram and data larger than the size of a datagram network packet."

"Applications

Cisco AnyConnect VPN Client uses TLS and DTLS,[16] as does the AnyConnect-compatible open-source OpenConnect client

Cisco InterCloud Fabric uses DTLS to form a tunnel between private and public/provider compute environments[17]

F5 Networks Edge VPN Client uses TLS and DTLS[18]

Citrix Systems NetScaler uses DTLS to secure UDP[19]

Web browsers: Google Chrome, Opera and Firefox support DTLS-SRTP[20] for WebRTC

Vulnerabilities

In February 2013 two researchers from Royal Holloway, University of London discovered an attack[21] which allowed them to recover plaintext from a DTLS

connection using the OpenSSL implementation of DTLS when Cipher Block Chaining mode encryption was used."
==========

Split tunnelling very similar to IPSec VPN

```
ASA3# sh run group-policy
group-policy SSLVPN_POLICY internal
group-policy SSLVPN_POLICY attributes
 wins-server none
 dns-server none
 vpn-tunnel-protocol ssl-client
 default-domain none
```

```
ASA3(config)# group-policy SSLVPN_POLICY attributes
ASA3(config-group-policy)#  split-tunnel-policy ?
group-policy mode commands/options:
  excludespecified  Exclude only networks specified by
                    split-tunnel-network-list
  tunnelall         Tunnel everything
  tunnelspecified   Tunnel only networks specified by split-tunnel-network-list
ASA3(config-group-policy)#  split-tunnel-policy tunnelspecified
ASA3(config-group-policy)# split-tunnel-?
group-policy mode commands/options:
  split-tunnel-all-dns    split-tunnel-network-list    split-tunnel-policy
ASA3(config-group-policy)# split-tunnel-network-list ?
group-policy mode commands/options:
  none   Specify that no access-list will be used for split tunnel
         configuration
  value  Specify a standard or extended type access-list for split tunnel
         configuration
ASA3(config-group-policy)# split-tunnel-network-list value ?
group-policy mode commands/options:
  WORD  Name of a standard or extended type access-list for split tunnel
        configuration
ASA3(config-group-policy)# sh run | in access-list
access-list outside_cryptomap extended permit ip 10.0.0.0 255.255.255.0 host 2.2.2.2
access-list outside_cryptomap extended permit ip 10.0.0.0 255.255.255.0 host 22.22.22.
22
access-list outside_cryptomap_1 extended permit ip 10.0.0.0 255.255.255.0 host 10.20.3
0.40
access-list INSIDE_IN extended deny ip 10.0.0.0 255.255.255.0 30.0.0.0 255.255.255.0
access-list INSIDE_IN extended permit ip any any
access-list SPLIT_TUNNEL_ACL standard permit 10.0.0.0 255.255.255.0
threat-detection statistics access-list
ASA3(config-group-policy)# split-tunnel-network-list value SPLIT_TUNNEL_ACL
```

(disconnect client and re-connect)
So what this does is allow the tunnel to be straight to 10.0.0.0 /24 inside, but other subnets be from the outside interface of the firewall in cleartext traffic. (ping to 1.1.1.1 won't work as plaintext traffic filtered at firewall)
You could get even more granular inside the tunnel restricting to certain servers with an extended ACL or two.
This is how you sandbox access between the tunnels :)
You can also grab these to use (just like we did with the split tunnel ACL) with other things like AAA RADIUS and TACACS configs
You dont have to memorize a bunch of junk because "sh run all tunnel-group" and "sh run all group-policy" show you all of the configurations in the defaults.

Split DNS: when you have it set up that local domain stuff does lookups on local servers, but other domains are looked up using public DNS

A clientless setup can offer bookmarks for Sharepoint, etc for the user to click on
you would delete the anyconnect reference in the profile and go to the settings in ASA to add options for those links.

NAT on ASAs
http://www.cisco.com/c/en/us/support/security/asa-5515-x-adaptive-security-appliance/model.html#ConfigurationGuides
This is the link he showed, which did not have links to the stuff below we need (the page changed since the video was made)
Here is what you need:
Configuring NAT Chapter parts from Cisco ASA 5500 Series Configuration Guide using the CLI, 8.4 and 8.6
http://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/nat_overview.html

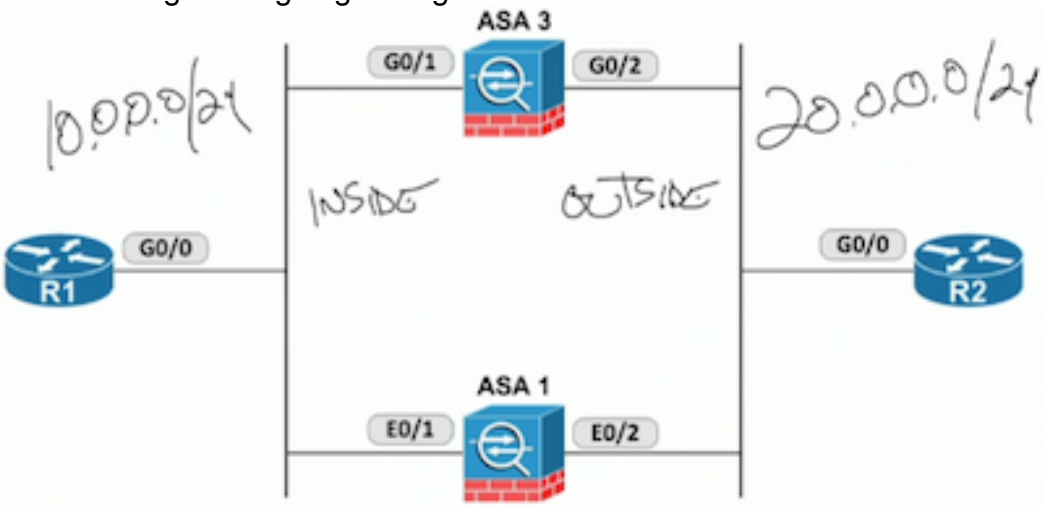
For older NAT this is referred to:
Cisco ASA 5500 Series Configuration Guide using the CLI, 8.2
http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config.html
Configuring NAT
- Information About NAT
- Configuring NAT Control
- Configuring Dynamic NAT and PAT
- Configuring Static NAT
- Configuring Static PAT
- Bypassing NAT

I downloaded the PDF of the whole book, since these are now all separate HTML files/pdfs. The URL gets you to all of links in the TOC

Newer: Auto NAT aka Object based NAT aka Static NAT - Advanced version is Twice NAT This will be on ASA3 runninv9.3
Legacy versions was Global NAT AKA Policy NAT - This will be on ASA1 running v8.2

Static NAT is now object-based NAT
Static is always one-to one including port translation types - internal server address to external IP address
Twice NAT is going to be the modern equivalent of Policy NAT

Bypassing NAT important with Remote Access and Site to Site VPN - we DON'T want our tunneling traffic going through NAT!



R1 10.0.0.0 /24 Inside - (G0/1 and E0/1) - loopback 11.11.11.11
R2 20.0.0.0 /24 outside - (G0/2 and E0/2) - loopback 2.2.2.2
ASA 3 - G0/x - v9.x - x.x.x.254 - for newer (8.3+, but generally 8.6 and above)
ASA 1 - E0/x - v8.2 825-k8 - x.x.x.253 - for legacy
Both running OSPF
To direct traffic to the proper ASA, set ospf cost 1000 on ASA3 for ASA1 work. Shut down those interfaces if you need to quickly cancel that routing detour.

```
ASA1# show ip
System IP Addresses:
Interface                  Name                IP address      Subnet mask     Method

Ethernet0/1                inside              10.0.0.253      255.255.255.0   manual
Ethernet0/2                outside             20.0.0.253      255.255.255.0   manual
Current IP Addresses:
Interface                  Name                IP address      Subnet mask     Method

Ethernet0/1                inside              10.0.0.253      255.255.255.0   manual
Ethernet0/2                outside             20.0.0.253      255.255.255.0   manual
```

R1's routing table:

```
      1.0.0.0/32 is subnetted, 1 subnets
C        1.1.1.1 is directly connected, Loopback0
      2.0.0.0/32 is subnetted, 1 subnets
O        2.2.2.2 [110/12] via 10.0.0.254, 00:27:01, GigabitEthernet0/0
                 [110/12] via 10.0.0.253, 00:01:20, GigabitEthernet0/0
      3.0.0.0/32 is subnetted, 1 subnets
O        3.3.3.3 [110/12] via 10.0.0.254, 00:27:01, GigabitEthernet0/0
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.0.0.0/24 is directly connected, GigabitEthernet0/0
L        10.0.0.1/32 is directly connected, GigabitEthernet0/0
      11.0.0.0/32 is subnetted, 1 subnets
C        11.11.11.11 is directly connected, Loopback11
      20.0.0.0/24 is subnetted, 1 subnets
O        20.0.0.0 [110/11] via 10.0.0.254, 00:27:01, GigabitEthernet0/0
                  [110/11] via 10.0.0.253, 00:01:20, GigabitEthernet0/0
      22.0.0.0/32 is subnetted, 1 subnets
```

We want to make ASA3 (254) less preferred as an exit point, so traffic will go to ASA1 (253):

```
ASA3(config)# int g0/1
ASA3(config-if)# ospf cost 1000
ASA3(config-if)# int g0/2
ASA3(config-if)# ospf cost 1000
ASA3(config-if)# end
```

Shut down those interfaces if you need to quickly cancel that routing detour.

show xlate options

```
ASA1# show xlate ?

  count      Show translation count
  debug      Enter this keyword for debug information
  detail     Enter this keyword for detailed information
  global     Enter this keyword to specify global ip range
  gport      Enter this keyword to specify global port(s)
  interface  Enter this keyword to specify an interface
  local      Enter this keyword to specify local ip range
  lport      Enter this keyword to specify local port(s)
  state      Enter this keyword to specify state
  |          Output modifiers
```

Many to one PAT
- nat, global, and static commands
- tie nat rule to global rule (and numbers
- says the order below changes if static or not
 nat (source_int, destination_int) destination source
 nat (low, high) high low --- in terms of security-level-areas
- show xlate will show how the translation will actually happen
- [[in the newer version "show xlate" is replaced with "show nat," "show nat detail"]]
- [[packet- tracer more effective]]

OLD METHOD OF PAT (ASA1, v8.2)

NAT, the inside network, rule 1, any IP, any mask

```
ASA1(config)# nat (inside) ?
configure mode commands/options:
  <0-2147483647>  The <nat_id> of this group of hosts/networks. This <nat_id>
                  will be referenced by the global command to associate a
                  global pool with the local IP address. <nat_id> '0' is used
                  to indicate no address translation for local IP. The limit is
                  65535 with access-lists
ASA1(config)# nat (inside) 1 ?
configure mode commands/options:
  Hostname or A.B.C.D  The hosts/networks in this <nat_id> group, '0' indicates
                       all networks or the default <nat_id> group
  access-list          Specify access-list name after this keyword
ASA1(config)# nat (inside) 1 0 0
```

Pair it to the outside translation with a global rule:

```
ASA1(config)# global (?
configure mode commands/options:
Current available interface(s):
  inside   Name of interface Ethernet0/1
  outside  Name of interface Ethernet0/2
ASA1(config)# global (outside) ?
configure mode commands/options:
  <0-2147483647>  The id of the NAT group that will draw from these global
                  addresses
ASA1(config)# global (outside) 1 ?
configure mode commands/options:
  WORD       Enter IP address or a range of IP addresses <start_ip>[-<end_ip>]
  interface  Specifies PAT using the IP address at the interface
ASA1(config)# global (outside) 1 interface
INFO: outside interface address added to PAT pool
```

This is NAT overload aka PAT (many to one), and it says above how to do many-to-many standard NAT

Here is a show xlate after sending a telnet from R1 to 2.2.2.2 (which showed NAT'd as 20.0.0.253)

```
ASA1# show xlate
1 in use, 3 most used
PAT Global 20.0.0.253(27955) Local 10.0.0.1(47962)
```

```
ASA1# show xlate detail
1 in use, 3 most used
Flags: D - DNS, d - dump, I - identity, i - dynamic, n - no random,
       r - portmap, s - static
TCP PAT from inside:10.0.0.1/47962 to outside:20.0.0.253/27955 flags ri
```

Key with old method is it is based on the NAT rule (1)

IF this traffic was inspected to begin with, the inspection engine should be able to refer to this NAT rule for the session/port information and let the reply through.
Since we are going from high to low security level areas and getting a reply from low, it should be inspected, but in some cases you might need an ACL to make an exception

NEW METHOD OF PAT (ASA3, v8.6+) using Auto/ Object NAT

Step 1. Create an object for the source address that we want to do translation from (inside network)
- can only match one subnet, one host or range of addresses at a time
- multiple subnets or individual specific addresses need to be separate objects!

```
ASA3(config)# object ?
configure mode commands/options:
  network  Specifies a host, subnet or range IP addresses
  service  Specifies a protocol/port
ASA3(config)# object network ?
configure mode commands/options:
  WORD < 65 char  Specifies object ID (1-64 characters)
ASA3(config)# object network INSIDE_NETWORK
ASA3(config-network-object)# ?
  description  Specify description text
  fqdn         Enter this keyword to specify an FQDN
  help         Help for network object configuration commands
  host         Enter this keyword to specify a single host object
  nat          Enable NAT on a singleton object
  no           Remove an object or description from object
  range        Enter this keyword to specify a range
  subnet       Enter this keyword to specify a subnet
ASA3(config-network-object)# subnet ?
network-object mode commands/options:
  A.B.C.D             Enter an IPV4 network address
  X:X:X:X::X/<0-128>  Enter an IPv6 prefix
ASA3(config-network-object)# subnet 10.0.0.0 ?
network-object mode commands/options:
  A.B.C.D  Enter an IPv4 network mask
ASA3(config-network-object)# subnet 10.0.0.0 255.255.255.0
ASA3(config-network-object)# ?
  description  Specify description text
  fqdn         Enter this keyword to specify an FQDN
  help         Help for network object configuration commands
  host         Enter this keyword to specify a single host object
```

```
  nat           Enable NAT on a singleton object
  no            Remove an object or description from object
  range         Enter this keyword to specify a range
  subnet        Enter this keyword to specify a subnet
ASA3(config-network-object)# nat ?
  dynamic  Specify NAT type as dynamic
  static   Specify NAT type as static
configure mode commands/options:
  (               Open parenthesis for (<internal_if_name>,<external_if_name>)
                  pair where <internal_if_name> is the Internal or prenat
                  interface and <external_if_name> is the External or postnat
                  interface
  <1-2147483647>  Position of NAT rule within before auto section
  after-auto      Insert NAT rule after auto section
  source          Source NAT parameters
ASA3(config-network-object)# nat (
configure mode commands/options:
Current available interface(s):
  any      Global address space
  dmz      Name of interface GigabitEthernet0/3
  inside   Name of interface GigabitEthernet0/1
  outside  Name of interface GigabitEthernet0/2
ASA3(config-network-object)# nat (inside,outside) ?
  dynamic  Specify NAT type as dynamic
  static   Specify NAT type as static
configure mode commands/options:
  <1-2147483647>  Position of NAT rule within before auto section
  after-auto      Insert NAT rule after auto section
  source          Source NAT parameters
ASA3(config-network-object)# nat (inside,outside) dynamic ?
network-object mode commands/options:
  A.B.C.D    Mapped IP address
  WORD       Mapped network object/object-group name
  interface  Use interface address as mapped IP
  pat-pool   Specify object or object-group name for mapped source pat pool
ASA3(config-network-object)# nat (inside,outside) dynamic interface
```

In the config, the NAT and the object reside separately as shown here:

```
ASA3# sh run nat
!
object network INSIDE_NETWORK
 nat (inside,outside) dynamic interface
ASA3# show run object
object network INSIDE_NETWORK
 subnet 10.0.0.0 255.255.255.0
```

This subnet *object*, and *dynamic interface* out meaning PAT (in context)
Anything from this subnet will be overloaded to the address of this interface

```
ASA3# show nat
Auto NAT Policies (Section 2)
1 (inside) to (outside) source dynamic INSIDE_NETWORK interface
    translate_hits = 1, untranslate_hits = 0
```

==========

Auto because it automatically figures out what order the translation should occur from the most detailed to the least detailed, so a more specific translation for a specific port, that would be done before a translation to an interface.

==========

STATIC NAT (ASA3, v8.6+) using Auto/ Object NAT

Here is an example of a static NAT, and we also get to see Auto NAT in action at the end. We need R1's loopback (1.1.1.1) to send traffic leaving ASA3's exit interface masquerading as 20.0.0.11:

```
ASA3(config)# object ?
configure mode commands/options:
  network  Specifies a host, subnet or range IP addresses
  service  Specifies a protocol/port
ASA3(config)# object network ?
configure mode commands/options:
  WORD < 65 char  Specifies object ID (1-64 characters)
ASA3(config)# object network R1_LOOPBACK0
ASA3(config-network-object)# ?
  description  Specify description text
  fqdn         Enter this keyword to specify an FQDN
  help         Help for network object configuration commands
  host         Enter this keyword to specify a single host object
  nat          Enable NAT on a singleton object
  no           Remove an object or description from object
  range        Enter this keyword to specify a range
  subnet       Enter this keyword to specify a subnet
ASA3(config-network-object)# host 1.1.1.1
ASA3(config-network-object)# nat (inside,outside) static ?
network-object mode commands/options:
  A.B.C.D    Mapped IP address
  WORD       Mapped network object/object-group name
  interface  Use interface address as mapped IP
ASA3(config-network-object)# nat (inside,outside) static 20.0.0.11
ASA3(config-network-object)# end
```

We can see below the static NAT is more **specific**, so it gets priority from Auto NAT over the PAT overload
Even if the 1.1.1.1 address was different and fell into the 10.0.0.0/24 specified by PAT, static would take priority.

```
ASA3# show nat
Auto NAT Policies (Section 2)
1 (inside) to (outside) source static R1_LOOPBACK0 20.0.0.11
    translate_hits = 0, untranslate_hits = 0
2 (inside) to (outside) source dynamic INSIDE_NETWORK interface
    translate_hits = 1, untranslate_hits = 0
ASA3# show nat detail
Auto NAT Policies (Section 2)
1 (inside) to (outside) source static R1_LOOPBACK0 20.0.0.11
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 1.1.1.1/32, Translated: 20.0.0.11/32
2 (inside) to (outside) source dynamic INSIDE_NETWORK interface
    translate_hits = 1, untranslate_hits = 0
    Source - Origin: 10.0.0.0/24, Translated: 20.0.0.254/24
```

And that's why it's called Auto NAT.
Here is one thing- if you telnet 2.2.2.2 from R1, it will still come from the 20.0.0.254- because the source address is coming from the inside SUBNET of 10.0.0.0/24 - not specifically the loopback address (1.1.1.1). If we want it to actually come from the loopback interface, we have to tell it that with "telnet 2.2.2.2 /source-interface lo0"

Here is *sh run object* and *sh run nat* with both PAT and static NAT displayed:

```
ASA3# sh run object
object network INSIDE_NETWORK
 subnet 10.0.0.0 255.255.255.0
object network R1_LOOPBACK0
 host 1.1.1.1
ASA3# sh run nat
!
object network INSIDE_NETWORK
 nat (inside,outside) dynamic interface
object network R1_LOOPBACK0
 nat (inside,outside) static 20.0.0.11
```

Most common is not static from a range of addresses but for individual hosts (like a webserver) that have specific needs.

New: nat (inside,outside) static 20.0.0.11
 -- (for this object), nat (in_interface, out_interface) statically_change_src_to 20.0.0.11

OLD METHOD OF STATIC NAT (ASA1, v8.2)

Old: static (inside,outside) 20.0.0.12 1.1.1.1 netmask 255.255.255.255
 -- statically, with (in-int, out-int) use_this_masq_addr for_this_src_addr with this_mask

```
ASA1(config)# static ?
configure mode commands/options:
  (  Open parenthesis for (<internal_if_name>,<external_if_name>) pair where 55
     <internal_if_name> is the Internal or prenat interface and
     <external_if_name> is the External or postnat interface
ASA1(config)# static (inside,outside) ?
configure mode commands/options:
  Hostname or A.B.C.D  Global or mapped address
  interface            Global address overload from interface
  tcp                  TCP to be used as transport protocol
  udp                  UDP to be used as transport protocol
ASA1(config)# static (inside,outside) 20.0.0.12 ?
configure mode commands/options:
  Hostname or A.B.C.D  Real IP address of the host or hosts
  access-list          Configure access-list name after this keyword
ASA1(config)# static (inside,outside) 20.0.0.12 1.1.1.1 ?
configure mode commands/options:
  <0-65535>    The maximum number of simultaneous tcp connections the local IP
               hosts are to allow, default is 0 which means unlimited
               connections. Idle connections are closed after the time
               specified by the timeout conn command
  dns          Use the created xlate to rewrite DNS address record
  netmask      Configure Netmask to apply to IP addresses
  norandomseq  Disable TCP sequence number randomization
  tcp          Configure TCP specific parameters
  udp          Configure UDP specific parameters
  <cr>
ASA1(config)# static (inside,outside) 20.0.0.12 1.1.1.1 net
ASA1(config)# static (inside,outside) 20.0.0.12 1.1.1.1 netmask ?
configure mode commands/options:
  A.B.C.D  Netmask to apply to IP addresses
ASA1(config)# static (inside,outside) 20.0.0.12 1.1.1.1 netmask 255.255.255.255
```

```
ASA1# show xlate detail
1 in use, 3 most used
Flags: D - DNS, d - dump, I - identity, i - dynamic, n - no random,
       r - portmap, s - static
NAT from inside:1.1.1.1 to outside:20.0.0.12 flags s
```

Older NAT doesn't like conflicting rules... not so much a problem on newer NAT with auto-ordering

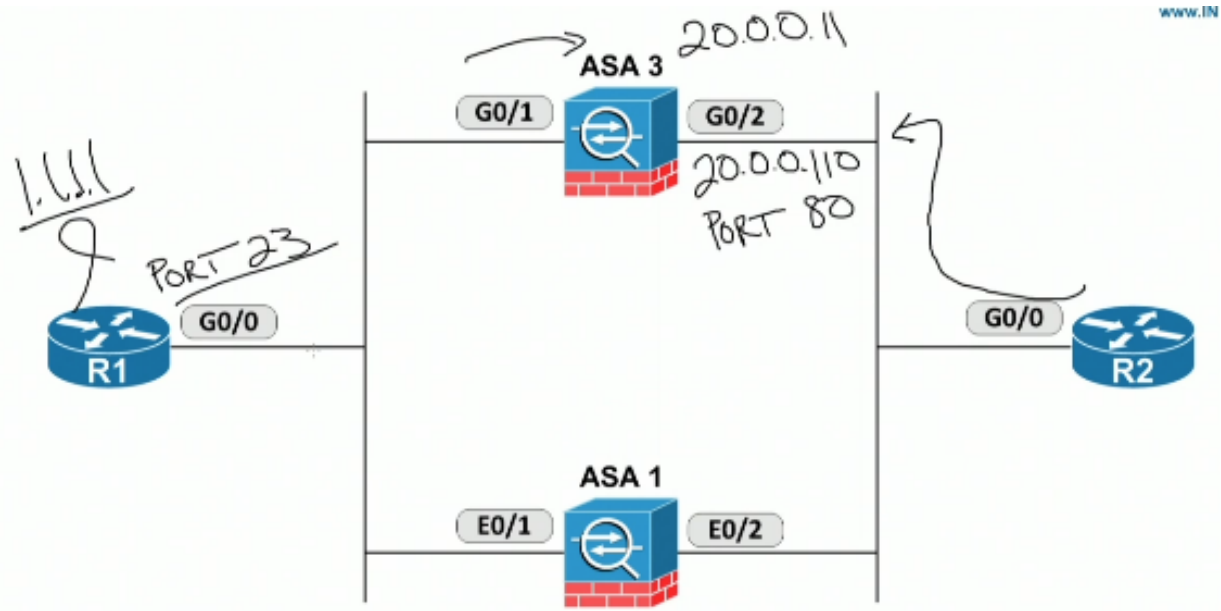
Doing port translation you still need an ACL
Older and newer types are going to be different in order of operations, and the method used in ACLs

How about this?? IMPORTANT POINT! (OLD NAT pre v8.6)
Already in ASA1:
ASA1# sh run static
static (inside,outside) 20.0.0.12 1.1.1.1 netmask 255.255.255.255
R1# telnet 2.2.2.2 /source-interface lo0
This is working fine, showing in "show users" as 20.0.0.12

We want to reverse this: We want someone on the outside to be able to hit the device on the inside, but specifically for that individual port. We need a static translation based on the port- not the IP.

Hypothetical:

Port 23 on loopback 11.11.11.11 is listening - The ASA is port translating to this on 20.0.0.110, port 80, outside to inside.



static (inside,outside) <-----technically in this case is from the outside-to-IN, but if we translate inside-to-out and it's static, it will be a reversible translation (you could move in either direction)

This is different from a dynamic translation that would have to be initiated from the source interface - this is why NAT is seen as a being a security-type feature that is normally doing inside to outside translation and you can't initiate traffic from the outside to begin with

```
ASA1(config)# static (inside,outside) ?
configure mode commands/options:
  Hostname or A.B.C.D  Global or mapped address
  interface            Global address overload from interface
  tcp                  TCP to be used as transport protocol
  udp                  UDP to be used as transport protocol
ASA1(config)# static (inside,outside) tcp ?
configure mode commands/options:
  Hostname or A.B.C.D  Global or mapped address
  interface            Global address overload from interface
ASA1(config)# static (inside,outside) tcp 20.0.0.120
ASA1(config)# static (inside,outside) tcp 20.0.0.120 80 11.11.11.11 23
```

Trying to get port 23 on loopback 11.11.11.11 listening to incoming port translation on 20.0.0.110, port 80, outside to inside

Put the above in and tried to tellnet from R2

```
R2#telnet 20.0.0.120 80
Trying 20.0.0.120, 80 ...
```

FAILED!!

Here is what we can see from ASA1

```
ASA1(config)# logging on
ASA1(config)# %ASA-5-111008: User 'enable_15' executed the 'logging on' command.
ASA1(config)# %ASA-2-106001: Inbound TCP connection denied from 20.0.0.2/29527 to 20.0
.0.120/80 flags SYN  on interface outside
%ASA-2-106001: Inbound TCP connection denied from 20.0.0.2/29527 to 20.0.0.120/80 flag
s SYN  on interface outside
ASA1(config)#
ASA1(config)# %ASA-2-106001: Inbound TCP connection denied from 20.0.0.2/29527 to 20.0
.0.120/80 flags SYN  on interface outside
%ASA-2-106001: Inbound TCP connection denied from 20.0.0.2/29527 to 20.0.0.120/80 flag
s SYN  on interface outside
```

Post-translation address 20.0.0.120/80- what we are listening for on the public interface
Translation did occur- we have a static port-mapping:

```
ASA1(config)# show xlate detail
2 in use, 3 most used
Flags: D - DNS, d - dump, I - identity, i - dynamic, n - no random,
       r - portmap, s - static
NAT from inside:1.1.1.1 to outside:20.0.0.12 flags s
TCP PAT from inside:11.11.11.11/23 to outside:20.0.0.120/80 flags sr
```

In order to allow the flow in, the access list would have to match the post-NAT address or the inside global
-- This won't translate to the new version good, but here is how you'd have to do it- manually.
ASA1(config)# access list OUTSIDE_IN permit tcp any host 20.0.0.120 eq 80
ASA1(config)# access list OUTSIDE_IN deny ip any any
-- Since access lists end in an implicit deny you don't need that last line, but it is easier to read
ASA1(config)# access-group OUTSIDE_IN in interface outside

[[access-group name in/out (for input/output traffic on) interface ifname/int]]

Often forgotten: you can use pipe to mean "or" as well:

```
ASA1# sh run | in static|access-list
access-list OUTSIDE_IN extended permit tcp any host 20.0.0.120 eq www
access-list OUTSIDE_IN extended deny ip any any
static (inside,outside) tcp 20.0.0.120 www 11.11.11.11 telnet netmask 255.255.255.255
static (inside,outside) 20.0.0.12 1.1.1.1 netmask 255.255.255.255
threat-detection statistics access-list
```

In this old way, the translated address is the one that needs to be called by the ACL (20.0.0.120)
In the new way, NAT translation is more decoupled from the ACL processing so it's

easier- the ACL will be working with to the real address on the inside- not the mapped addresses

Here is the newer way to do this:

```
ASA3(config)# object network R1_LOOPBACK_STATIC_PORT
ASA3(config-network-object)# host 1.1.1.1
ASA3(config-network-object)# nat
ASA3(config-network-object)# nat (inside,outside) ?
network-object mode commands/options:
  dynamic  Specify NAT type as dynamic
  static   Specify NAT type as static
configure mode commands/options:
  <1-2147483647>  Position of NAT rule within before auto section
  after-auto      Insert NAT rule after auto section
  source          Source NAT parameters
ASA3(config-network-object)# nat (inside,outside) static ?
network-object mode commands/options:
  A.B.C.D    Mapped IP address
  WORD       Mapped network object/object-group name
  interface  Use interface address as mapped IP
ASA3(config-network-object)# nat (inside,outside) static 20.0.0.110 ?
network-object mode commands/options:
  dns           Use the created xlate to rewrite DNS record
  no-proxy-arp  Disable proxy ARP on the egress interface
  route-lookup  Perform route lookup for this rule
  service       Define port mapping
  <cr>
ASA3(config-network-object)# nat (inside,outside) static 20.0.0.110 service ?
network-object mode commands/options:
  tcp  TCP to be used as transport protocol
  udp  UDP to be used as transport protocol
ASA3(config-network-object)# nat (inside,outside) static 20.0.0.110 service tcp 23 80
```

```
ASA3# sh run object
object network INSIDE_NETWORK
 subnet 10.0.0.0 255.255.255.0
object network R1_LOOPBACK0
 host 1.1.1.1
object network R1_LOOPBACK_STATIC_PORT
 host 1.1.1.1
ASA3# sh run nat
!
object network INSIDE_NETWORK
 nat (inside,outside) dynamic interface
object network R1_LOOPBACK0
 nat (inside,outside) static 20.0.0.11
object network R1_LOOPBACK_STATIC_PORT
 nat (inside,outside) static 20.0.0.110 service tcp telnet www
```

Note the two overlapping translations (different names)
Based on auto-NAT it should know which is the more-specific translation

```
ASA3# show nat detail

Auto NAT Policies (Section 2)
1 (inside) to (outside) source static R1_LOOPBACK0 20.0.0.11
    translate_hits = 1, untranslate_hits = 0
    Source - Origin: 1.1.1.1/32, Translated: 20.0.0.11/32
2 (inside) to (outside) source static R1_LOOPBACK_STATIC_PORT 20.0.0.110   service tcp
 telnet www
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 1.1.1.1/32, Translated: 20.0.0.110/32
    Service - Protocol: tcp Real: telnet Mapped: www
3 (inside) to (outside) source dynamic INSIDE_NETWORK interface
    translate_hits = 2, untranslate_hits = 0
    Source - Origin: 10.0.0.0/24, Translated: 20.0.0.254/24
```

-- What happens when the telnet connection is initiated?

```
%ASA-2-106001: Inbound TCP connection denied from 20.0.0.2/60612 to 1.1.1.1/23 flags S
YN  on interface outside
```

-- See 1.1.1.1:23 - It did the translation first, then at the filtering engine had blocked it.

-- This means the ACL has to deal with the real internal addresses- not the mapped external addresses

access-list OUTSIDE_IN permit tcp any host 1.1.1.1 eq 23
access-list OUTSIDE_IN deny ip any any
access-group OUTSIDE_IN in interface outside

-- This works, but try to telnet the other direction (R1, telnet 2.2.2.2 /source-interface lo0)
and check the "show users".
-- Auto NAT chose the other NAT mapping (that was static, more specific) and it shows connected to 20.0.0.11.

--- Run packet tracer:
packet-tracer input <int> < icmp | rawip | tcp | udp > < SOURCE ipv4 |ipv6 | fqdn | user > <port> < DEST ipv4 |ipv6 | fqdn | user > <port>

```
ASA3# packet-tracer input inside tcp 1.1.1.1 12345 2.2.2.2 80
Phase: 2
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in   2.2.2.2          255.255.255.255 outside

Phase: 3
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: NAT
Subtype:
Result: ALLOW
Config:
object network R1_LOOPBACK0
 nat (inside,outside) static 20.0.0.11
Additional Information:
Static translate 1.1.1.1/12345 to 20.0.0.11/12345

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 47, packet dispatched to next module

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

Here, Phase 2- routing lookup- passed; Phase 3- IP-options- passed; Phase 4- Object

NAT- translate to 20.0.0.11, source port stays the same; etc. Final action is to allow.

Flip around the previous query:
packet-tracer input outside tcp 2.2.2.2 12345 20.0.0.110 80
First it "untranslates" 20.0.0.110/80 to 1.1.1.1/23, THEN it gets filtered through the access-list

```
Subtype: static
Result: ALLOW
Config:
object network R1_LOOPBACK_STATIC_PORT
 nat (inside,outside) static 20.0.0.110 service tcp telnet www
Additional Information:
NAT divert to egress interface inside
Untranslate 20.0.0.110/80 to 1.1.1.1/23

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group OUTSIDE_IN in interface outside
access-list OUTSIDE_IN extended permit tcp any host 1.1.1.1 eq telnet
```

Inbound translation happens first, then ACL check.
In previous version the ACL came first so it had to match the global address - not the inside local

---

More Advanced Inspections - Policy NAT and Twice NAT

Policy NAT (old name/version) - translate based on specific source/ destination, ports, granular policy.
Twice NAT also means exempting a translation from a VPN-based config
---

Policy NAT example- static translation + an ACL
Listen for source 1.1.1.1 and dest 2.2.2.2, masquerade source as 20.0.0.222 on ASA1

Conditional translation based on more than the source or port number
It is source and destination together
Legacy Policy Nat combo of static translation and ACL, which makes an unnamed **POLICY**
1. How do we classify the traffic, ACL

access-list FROM_R1_TO_R2_LOOPBK permit ip host 1.1.1.1 host 2.2.2.2
static (inside, outside) 20.0.0.222 access-list FROM_R1_TO_R2_LOOPBK
  -- an existing rule overlapped, and we are in the old NAT that doesn't have AutoNAT functionality. "sh run static"
  -- run "no static (inside,outside) 20.0.0.12 1.1.1.1 netmask 255.255.255.255"
  -- killed the other rule, retry - still a conflict message!! Run "clear xlate" to flush.
  -- it could be it applied twice so say "no (your rule)" and apply again

So this worked-
If you "telnet 2.2.2.2 source-interface lo0" this NAT catches it, (check "show users" - 20.0.0.222)
From R1 regular interface it falls back to the dynamic translation set up earlier to overload the interface at 20.0.0.253

This also happens if the destination address is changed for the telnetting- because **it doesn't match the *full policy*** with both IP addresses. This is the old way, and why it is called **POLICY NAT**

Switching to ASA3 for Twice NAT

Twice NAT can be tricky but if you follow the order of operations in "show nat detail" output you can follow backwards to help figure out how to match things.

ASA3 has 3 policies showing up:

```
ASA3# show run object
object network INSIDE_NETWORK
 subnet 10.0.0.0 255.255.255.0
object network R1_LOOPBACK0
 host 1.1.1.1
object network R1_LOOPBACK_STATIC_PORT
 host 1.1.1.1
ASA3# show run nat
!
object network INSIDE_NETWORK
 nat (inside,outside) dynamic interface
object network R1_LOOPBACK0
 nat (inside,outside) static 20.0.0.11
object network R1_LOOPBACK_STATIC_PORT
 nat (inside,outside) static 20.0.0.110 service tcp telnet www
```

So first, order of matching would be the port-static, then the other static, finally falling back to the dynamic match
They are in reverse order as listed above in terms of which is most specific.

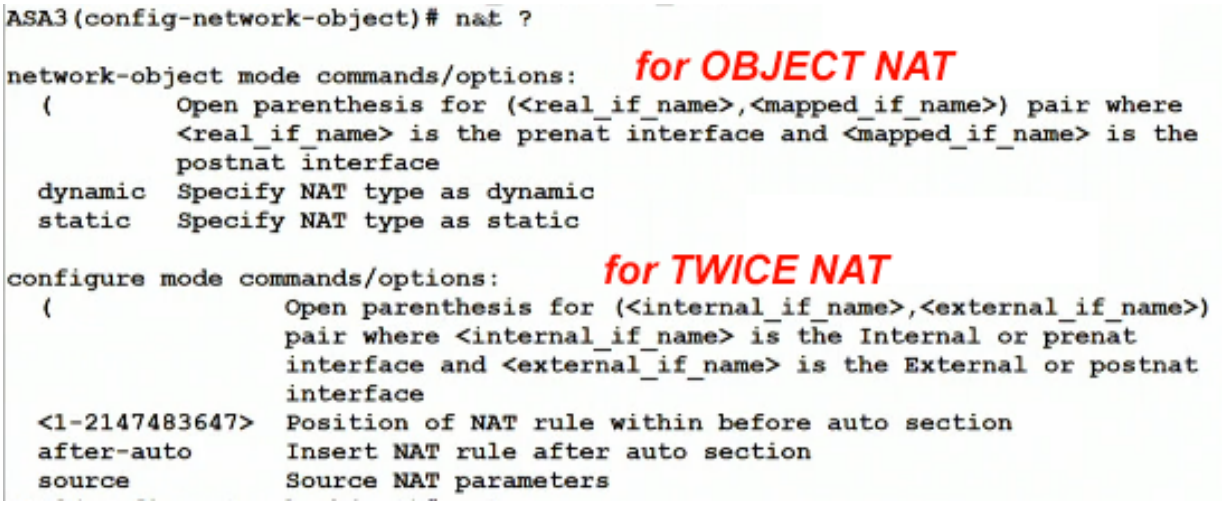
For the new one, three objects:

```
ASA3(config)# object network R1_LOOPBACK11
ASA3(config-network-object)# host 11.11.11.11
ASA3(config-network-object)# exit
ASA3(config)# object network R2_LOOPBACK0
ASA3(config-network-object)# host 2.2.2.2
ASA3(config)# object network R1_TRANSLATED_ADDRESS
ASA3(config-network-object)# host 20.0.0.111
```

Instead of referencing the NAT statement from inside of the object, we are referencing it globally

Here we get some help from ASA's context sensitive "?" display, giving us more options as appropriate
It is presenting us with both types of NAT, adding the global Twice NAT syntax.
If you were in routed mode it would show you those options as well.

Below, network-object config mode pertains to what we were just doing- defining objects (Object NAT, get it?)
Configure mode refers to the global config- for Twice NAT
If you are under router mode, and you have a command that overlaps over to global config, the "?" will give you both help options.



ASA3(config-network-object)# nat (inside,outside) source dynamic R1_LOOPBACK11 R1_TRANSLATED_ADDRESS destination static R2_LOOPBACK0 R2_LOOPBACK0**
This says, for inside and outside interfaces, if traffic is source R1_LOOPBACK11, change it to (mapped source) R1_TRANSLATED, but ONLY if the destination is R2_LOOPBACK0

-- In example R2_LOOPBACK0 was in as both the mapped (masq'd) destination and real destination address
-- **why it's there two times? double NAT - you can optionally specify the real

destination here if you want a double-nat translation; used **if you had overlapping addresses on both the inside and outside and you are trying to translate it both directions.** Typical usage is when you have two departments and/or networks merging together both using addresses in the 10.0.0.0/24 network and they need some sort of translation to talk together

```
ASA3# sh run nat
nat (inside,outside) source dynamic R1_LOOPBACK11 R1_TRANSLATED_ADDRESS destination st
atic R2_LOOPBACK0 R2_LOOPBACK0
!
object network INSIDE_NETWORK
 nat (inside,outside) dynamic interface
object network R1_LOOPBACK0
 nat (inside,outside) static 20.0.0.11
object network R1_LOOPBACK_STATIC_PORT
 nat (inside,outside) static 20.0.0.110 service tcp telnet www
ASA3# show nat detail
Manual NAT Policies (Section 1)
1 (inside) to (outside) source dynamic R1_LOOPBACK11 R1_TRANSLATED_ADDRESS   destinati
on static R2_LOOPBACK0 R2_LOOPBACK0
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 11.11.11.11/32, Translated: 20.0.0.111/32
    Destination - Origin: 2.2.2.2/32, Translated: 2.2.2.2/32

Auto NAT Policies (Section 2)
1 (inside) to (outside) source static R1_LOOPBACK0 20.0.0.11
    translate_hits = 3, untranslate_hits = 0
    Source - Origin: 1.1.1.1/32, Translated: 20.0.0.11/32
2 (inside) to (outside) source static R1_LOOPBACK_STATIC_PORT 20.0.0.110   service tcp
 telnet www
    translate_hits = 0, untranslate_hits = 5
    Source - Origin: 1.1.1.1/32, Translated: 20.0.0.110/32
    Service - Protocol: tcp Real: telnet Mapped: www
3 (inside) to (outside) source dynamic INSIDE_NETWORK interface
    translate_hits = 2, untranslate_hits = 0
    Source - Origin: 10.0.0.0/24, Translated: 20.0.0.254/24
```

- Our rule (our twice NAT) is under "Manual", separated from the Auto NAT policies
- In place of keyword "source" you can put in "after-auto" which directs it to be looked at after the Auto NAT/ Object NAT ones
- The previous version didn't have a way (like sh nat det) to check the order rules would take, and would simply tell you rules overlapped
- This is illustrated in show xlate:

```
ASA3# show xlate
3 in use, 3 most used
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice
NAT from inside:1.1.1.1 to outside:20.0.0.11
    flags s idle 0:05:14 timeout 0:00:00
TCP PAT from inside:1.1.1.1 23-23 to outside:20.0.0.110 80-80
    flags sr idle 0:12:29 timeout 0:00:00
TCP PAT from inside:10.0.0.1/54884 to outside:20.0.0.254/19779 flags ri idle 0:00:10 t
imeout 0:00:30
```

So in testing there is the "packet-tracer" command, telnetting with different "/ source-interface" and checking with "show users"

Excluding VPNs from NAT

- Given: IPSec Tunnel if traffic is from R2 2.2.2.2 to 10.0.0.0/24 through ASA3
- CRYPTO-MAP 1 and PROXY_ACL do this for us:

```
ASA3# show run crypto
crypto ipsec ikev1 transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
crypto map CRYPTO_MAP 1 match address PROXY_ACL
crypto map CRYPTO_MAP 1 set peer 20.0.0.2
crypto map CRYPTO_MAP 1 set ikev1 transform-set ESP-AES-256-MD5
crypto ikev1 enable outside
crypto ikev1 policy 10
 authentication pre-share
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 65535
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
ASA3# sh run access-list
access-list PROXY_ACL extended permit ip 10.0.0.0 255.255.255.0 host 2.2.2.2
access-list OUTSIDE_IN extended permit tcp any host 1.1.1.1 eq telnet
access-list OUTSIDE_IN extended deny ip any any
```

```
ASA3# sh run access-list
access-list PROXY_ACL extended permit ip 10.0.0.0 255.255.255.0 host 2.2.2.2
access-list OUTSIDE_IN extended permit tcp any host 1.1.1.1 eq telnet
access-list OUTSIDE_IN extended deny ip any any
```

- Tunnel destination of 20.0.0.2 for traffic matching PROXY_ACL (above - traffic from 10.0.0.0/24 to 2.2.2.2), and also allow telnet traffic from any host destined for 1.1.1.1
- "sh run tunnel-group" didn't come up with anything- we need a tunnel-group!

```
ASA3(config)# tunnel-group 20.0.0.2 type ?

configure mode commands/options:
  ipsec-l2l       IPSec Site to Site group
  ipsec-ra        IPSec Remote Access group (DEPRECATED)
  remote-access   Remote access (IPSec and WebVPN) group
  webvpn          WebVPN group (DEPRECATED)
ASA3(config)# tunnel-group 20.0.0.2 type ipsec-l2l
ASA3(config)# tunnel-group 20.0.0.2 ipsec
ASA3(config)# tunnel-group 20.0.0.2 ipsec-attributes
ASA3(config-tunnel-ipsec)# ?

tunnel-group configuration commands:
  chain              Enable sending certificate chain
  exit               Exit from tunnel-group IPSec attribute configuration mode
  help               Help for tunnel group configuration commands
  ikev1              Configure IKEv1
  ikev2              Configure IKEv2
  isakmp             Configure ISAKMP policy
  no                 Remove an attribute value pair
  peer-id-validate   Validate identity of the peer using the peer's certificate
ASA3(config-tunnel-ipsec)# ikev1 ?

tunnel-group-ipsec mode commands/options:
  pre-shared-key       Associate a pre-shared key with the connection policy
  trust-point          Select the trustpoint that identifies the cert to be
                       sent to the IKE peer
  user-authentication  Set the IKEv1 user authentication method
ASA3(config-tunnel-ipsec)# ikev1 pre
ASA3(config-tunnel-ipsec)# ikev1 pre-shared-key cisco
ASA3(config-tunnel-ipsec)# crypto map CRYPTO_MAP int outside
```

-- So that's in place, and double-checked tunnel on R2 as well:

```
R2#show run | s crypto|isakmp|access-list
crypto isakmp policy 1
 encr aes 256
 authentication pre-share
 group 2
crypto isakmp key cisco address 20.0.0.254
crypto ipsec transform-set ESP-AES-256-MD5 esp-aes 256 esp-md5-hmac
 mode tunnel
crypto map CRYPTO_MAP 10 ipsec-isakmp
 set peer 20.0.0.254
 set transform-set ESP-AES-256-MD5
 match address PROXY_ACL
ip access-list extended PROXY_ACL
 permit ip host 2.2.2.2 10.0.0.0 0.0.0.255
```

-- It is there, but it wasn't applied to g0/0 --> int g0/0; crypto map CRYPTO_MAP
-- R1 telnet 2.2.2.2, and R2's "show users" lists exterior int of ASA
-- But "show crypto isakmp sa" says there are no IKE SAs- the tunnel didn't form.
-- The reason: NAT rule was applied before crypto was processed, so it no longer matched the proxy ACL (the order of operations)

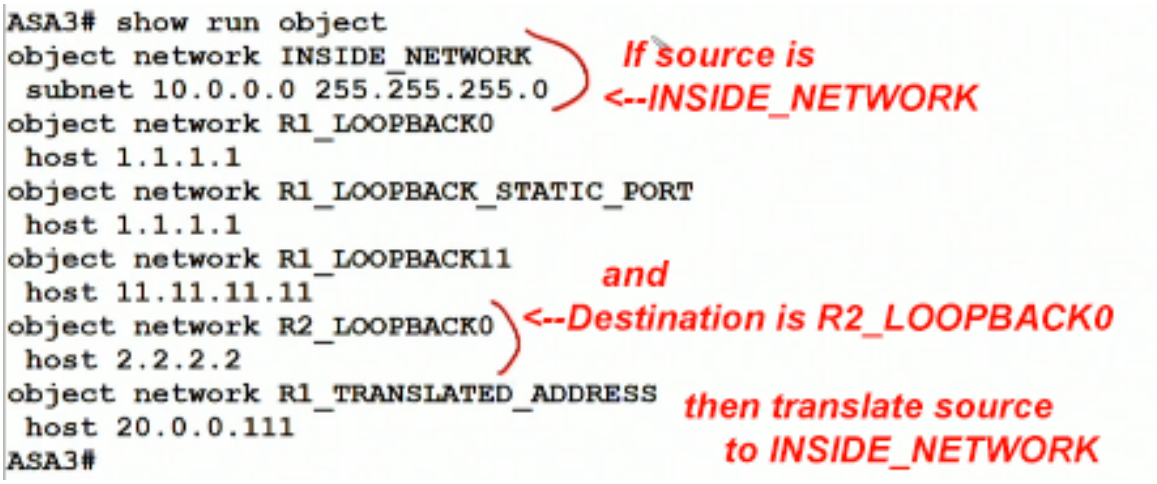
-- Solution: an "identity NAT" or NAT exemption

--- The old way - configure "NAT Zero"

```
ASA1(config)# nat (inside) 0 access-list NO_NAT
ERROR: Access-list "NO_NAT" does not exist
ASA1(config)# access-list NO_NAT permit ip 10.0.0.0 255.255.255.0 host 2.2.2.2
```

- Says if traffic comes in on the inside, matches the ACL, then the result "0" is that it's not translated.

--- The new way - there is no "NAT Zero" - **We use Twice NAT**
--- Says "if this traffic pattern is true, translate the source to the same source",
--- You are doing a translation, but you are doing the translation to the same address (it is almost just a redundancy)



nat (inside,outside) source static INSIDE_NETWORK INSIDE_NETWORK destination R2_LOOPBACK0 R2_LOOPBACK0
nat (inside,outside) source static <sourceIP> <translateToIP> destination <destIPReal> <DestIPmasqd>
-- manual NAT rule is processed first in the order of operations

```
ASA3# show nat detail
Manual NAT Policies (Section 1)
1 (inside) to (outside) source dynamic R1_LOOPBACK11 R1_TRANSLATED_ADDRESS   destinati
on static R2_LOOPBACK0 R2_LOOPBACK0
    translate_hits = 2, untranslate_hits = 0
    Source - Origin: 11.11.11.11/32, Translated: 20.0.0.111/32
    Destination - Origin: 2.2.2.2/32, Translated: 2.2.2.2/32
2 (inside) to (outside) source static INSIDE_NETWORK INSIDE_NETWORK   destination stat
ic R2_LOOPBACK0 R2_LOOPBACK0
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 10.0.0.0/24, Translated: 10.0.0.0/24
    Destination - Origin: 2.2.2.2/32, Translated: 2.2.2.2/32

Auto NAT Policies (Section 2)
1 (inside) to (outside) source static R1_LOOPBACK0 20.0.0.11
    translate_hits = 4, untranslate_hits = 0
    Source - Origin: 1.1.1.1/32, Translated: 20.0.0.11/32
2 (inside) to (outside) source static R1_LOOPBACK_STATIC_PORT 20.0.0.110   service tcp
 telnet www
    translate_hits = 0, untranslate_hits = 5
    Source - Origin: 1.1.1.1/32, Translated: 20.0.0.110/32
    Service - Protocol: tcp Real: telnet Mapped: www
3 (inside) to (outside) source dynamic INSIDE_NETWORK interface
    translate_hits = 4, untranslate_hits = 0
    Source - Origin: 10.0.0.0/24, Translated: 20.0.0.254/24
```

-- Preferred order: static twice NAT, then dynamic twice NAT, static object NAT, dynamic object NAT

-- Issuing "after-auto" in translation can re-order things, but generally you want those manual policies before the Auto NAT policies

-- Running "sh crypto isakmp sa" shows it active:

```
ASA3# show crypto isakmp sa

IKEv1 SAs:

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 20.0.0.2
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE

There are no IKEv2 SAs
```

-- Running "sh crypto ipsec sa" shows the IPsec stats:

```
access-list PROXY_ACL extended permit ip 10.0.0.0 255.255.255.0 host 2.2.2.2
local ident (addr/mask/prot/port): (10.0.0.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (2.2.2.2/255.255.255.255/0/0)
current_peer: 20.0.0.2

#pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
#pkts decaps: 8, #pkts decrypt: 8, #pkts verify: 8
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 10, #pkts comp failed: 0, #pkts decomp failed: 0
```

Typically you'd see this when you have either remote access or site-to-site VPNs, and

you are trying to do NAT translation toward the internet at the same time. You need to exempt the traffic in your local address space (RFC 1918) from NAT and use it only when going out to public space.

ASA3# packet-tracer input inside icmp 10.0.0.1 8 0 2.2.2.2
 -- 8 and 0 are ICMP types from 10.0.0.1 to 2.2.2.2

```
Result: ALLOW
Config:
Additional Information:
in   2.2.2.2          255.255.255.255 outside

Phase: 2
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 3
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
class-map inspection_default
 match default-inspection-traffic
policy-map global_policy
 class inspection_default
  inspect icmp
service-policy global_policy global
Additional Information:

Phase: 4
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:

Phase: 5
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside,outside) source static INSIDE_NETWORK INSIDE_NETWORK destination static R2
_LOOPBACK0 R2_LOOPBACK0
Additional Information:
Static translate 10.0.0.1/0 to 10.0.0.1/0

Phase: 6
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:
```

```
Phase: 7
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 9
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 73, packet dispatched to next module

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

Here is the final outputs for "sh run nat" and "sh run object":

```
ASA3# sh run object
object network INSIDE_NETWORK
 subnet 10.0.0.0 255.255.255.0
object network R1_LOOPBACK0
 host 1.1.1.1
object network R1_LOOPBACK_STATIC_PORT
 host 1.1.1.1
object network R1_LOOPBACK11
 host 11.11.11.11
object network R2_LOOPBACK0
 host 2.2.2.2
object network R1_TRANSLATED_ADDRESS
 host 20.0.0.111
ASA3# sh run nat
nat (inside,outside) source dynamic R1_LOOPBACK11 R1_TRANSLATED_ADDRESS destination st
atic R2_LOOPBACK0 R2_LOOPBACK0
nat (inside,outside) source static INSIDE_NETWORK INSIDE_NETWORK destination static R2
_LOOPBACK0 R2_LOOPBACK0
!
object network INSIDE_NETWORK
 nat (inside,outside) dynamic interface
object network R1_LOOPBACK0
 nat (inside,outside) static 20.0.0.11
object network R1_LOOPBACK_STATIC_PORT
 nat (inside,outside) static 20.0.0.110 service tcp telnet www
ASA3#
```

TWICE NAT

PAT

1:1

1:1 PAT

==========

I also found this:
http://www.cisco.com/c/en/us/td/docs/security/asa/asa83/configuration/guide/config/nat_objects.html

"twice NAT simply means that both the source and the destination IP addresses in the packet are translated"

"static(inside,outside) source static real_ip mapped_ip destination static mapped_ip real_ip".
So , SA=10.1.1.1 DA=172.16.1.1
After leaving the firewall
SA=Outside Interface DA=192.168.1.1

High Availability and Failover

See CLI Book1 ASA Gen Ops Config Guide

Failover is mainly used in older setups that can't do clustering

Can only be done with HW of the same model # and SW of the same version.

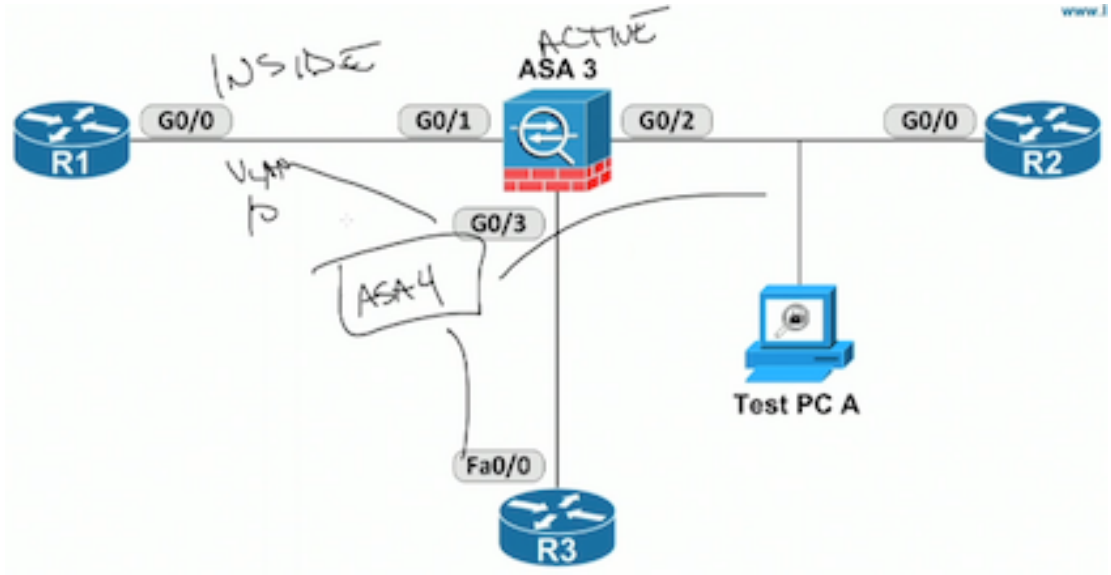
Failover vs Clustering =
Can we have more than 2 units in the HA cluster
or
Are we going to be forwarding actively on multiple units simultaneously?

Failover works in routed and transparent firewall
Failover types- active-active or active-standby
subtypes - stateless vs stateful failover
 - -stateful copies connection tables, NAT, IPSec SA info to standby to prevent sessions, VPN to disconnect
single context or multicontext mode

single context active standby
one unit forwarding the other monitoring primary box to see if it goes down and it needs to become primary
active active can have multiple boxes forwarding at the same but only on a per-context basis

Example- 2 virtual firewalls
- Context a and context b, with one of the firewalls in each group (one-for-one) - one context will be busier than the other so there is a loss of resources.
- X series ASAs support clustering mode
- Lower level models 2 virt FW's per cluster, higher level models 16 per cluster
Sort of how stackwise works with catalyst switching - multiple boxes in the data plane, but one in mgmt and control plane)

Active and standby need equal layer 2 connectivity

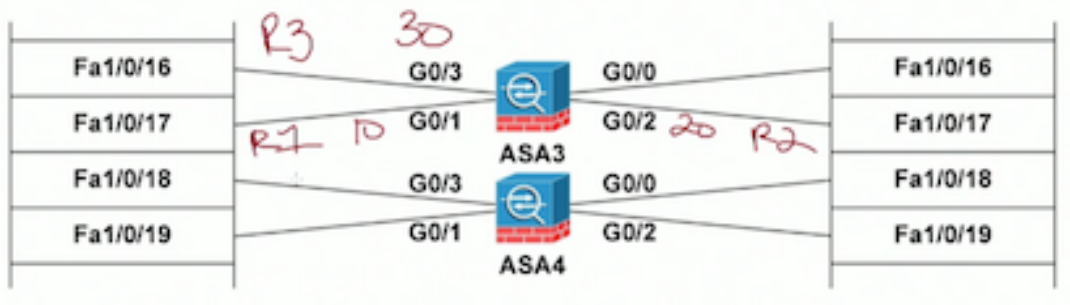


Hypothetical scenario: ASA 4 is standby for ASA3

- ASA3 G0/1 to R1 (inside int) goes down
- ASA4 monitors through the inside int - sees this and attempts to promote itself to primary
- if we fail to take into account that the R3 (DMZ) and R2(outside) need the same VLAN (or other L2) configuration
  - You could run into the standby device taking over but it isn't able to successfully forward traffic

So layer 2 needs to be EQUAL and solid! between the firewalls.

Here is a subset of the physical diagram, showing links to routers and their VLANs
Switch1 is on the left



Fa1/0/1	R1 G0/0	connected	10	a-full	a-100 10/100BaseTX
Fa1/0/2	R2 G0/0	connected	20	a-full	a-100 10/100BaseTX
Fa1/0/3	R3 Fa0/0	connected	30	a-full	a-100 10/100BaseTX
Fa1/0/4	Test SRV A	disabled	10	auto	auto 10/100BaseTX
Fa1/0/5	Test PC A	connected	20	a-full	a-100 10/100BaseTX
Fa1/0/6		disabled	1	auto	auto 10/100BaseTX
Fa1/0/7		disabled	1	auto	auto 10/100BaseTX
Fa1/0/8		disabled	1	auto	auto 10/100BaseTX
Fa1/0/9		disabled	1	auto	auto 10/100BaseTX
Fa1/0/10		disabled	1	auto	auto 10/100BaseTX
Fa1/0/11		disabled	1	auto	auto 10/100BaseTX
Fa1/0/12	ASA1 M0/0	connected	1	a-full	a-100 10/100BaseTX
Fa1/0/13	ASA1 E0/1	connected	10	a-full	a-100 10/100BaseTX
Fa1/0/14	ASA2 M0/0	connected	1	a-full	a-100 10/100BaseTX
Fa1/0/15	ASA2 E0/1	connected	1	a-full	a-100 10/100BaseTX
Fa1/0/16	ASA3 G0/3	connected	30	a-full	a-100 10/100BaseTX
Fa1/0/17	ASA3 G0/1	connected	10	a-full	a-100 10/100BaseTX
Fa1/0/18	ASA4 G0/3	connected	1	a-full	a-100 10/100BaseTX
Fa1/0/19	ASA4 G0/1	connected	1	a-full	a-100 10/100BaseTX
Fa1/0/20	SW2 F1/0/20	connected	trunk	a-full	a-100 10/100BaseTX
Fa1/0/21		disabled	1	auto	auto 10/100BaseTX
Fa1/0/22		disabled	1	auto	auto 10/100BaseTX

So Fa1/0/16 and 18 need to be identical, as do 17 and 19, in both capability and configuration!
There should be a management port/ VLAN for transferring data for stateful failover setups

Yep these need to be made identical. Also add VLAN 999 or something for the stateful failover data exchange

```
SW2#sh run | b 1/0/16
interface FastEthernet1/0/16
 description ASA3 G0/0
 no switchport
 ip address 192.168.0.1 255.255.255.0
!
interface FastEthernet1/0/17
 description ASA3 G0/2
 switchport access vlan 20
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet1/0/18
 description ASA4 G0/0
!
interface FastEthernet1/0/19
 description ASA4 G0/2
```

Always make sure you havea backup of the config before you go over the failover steps ESPECIALLY IN A PRODUCTION ENVIRONMENT!!
When setting up, you don't wan't a messed up configuration replicating the wrong way and clobbering everything!

Remember this?

```
ASA3# show firewall
Firewall mode: Router
ASA3# show mode
Security context mode: single
```

This means active-standby. Only in multiple context can we run active-active, and then it will be active for one group and standby for another group

Step 1: specify which is the primary:
ASA(config)# failover lan unit primary
Step 2: Define the failover link interface:
ASA(config)# failover lan interface folink gigabitethernet/0/0
Step 3: Assign the active and standby IP addresses to the failover link
ASA(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
again?
ASA(config)# failover lan interface folink gigabitethernet/0/0
int g0/0
no shut
ASA(config)# failover link folink gigabitethernet/0/0

```
ASA3# sh run failover
no failover
failover lan unit primary
failover lan interface folink GigabitEthernet0/0
failover link folink GigabitEthernet0/0
failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
```

Now, if you execute the failover command and the other device is not recognized as

available, it will promote itself to active and later write over the others configuration! (I don't see what the problem is if you execute the failover command on the box that is already set up as primary to begin with!)

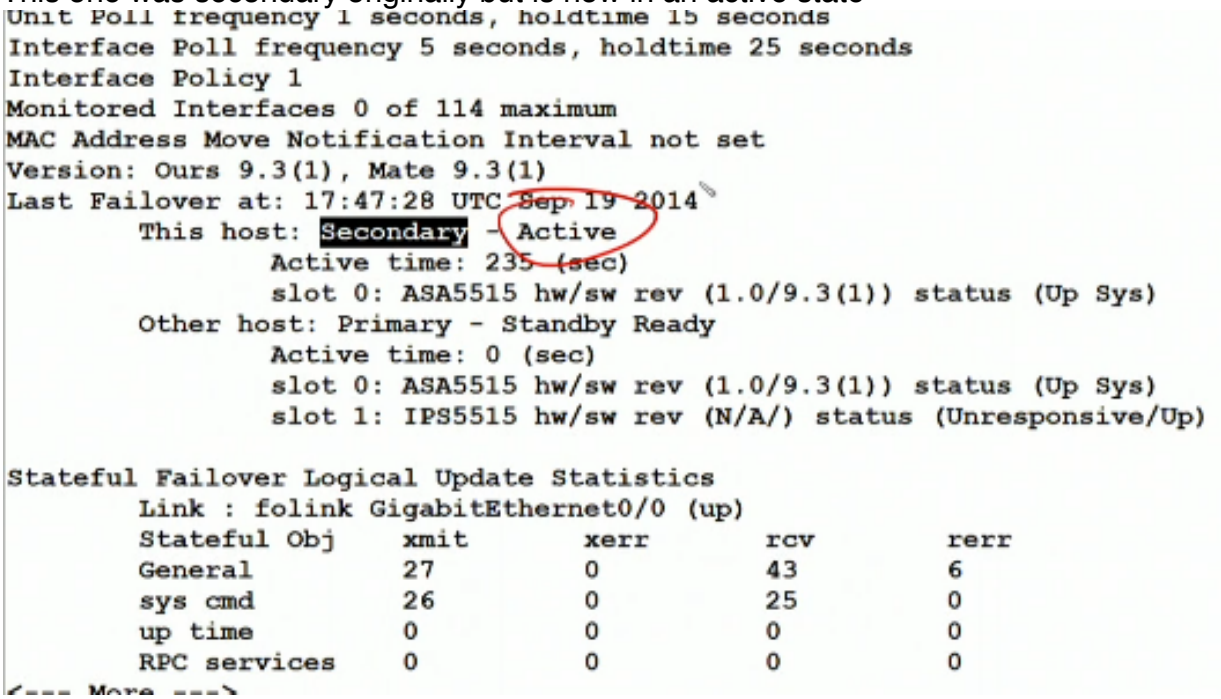
The other box gets the same stuff but you say secondary instead of primary

When you are done run "failover" on primary box, wait a sec and run "failover" on secondary

All of this is straight from this: http://www.cisco.com/c/en/us/td/docs/security/asa/asa93/configuration/general/asa-general-cli/ha-failover.html

show failover

This one was secondary originally but is now in an active state



```
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 0 of 114 maximum
MAC Address Move Notification Interval not set
Version: Ours 9.3(1), Mate 9.3(1)
Last Failover at: 17:47:28 UTC Sep 19 2014
        This host: Secondary - Active
                Active time: 235 (sec)
                slot 0: ASA5515 hw/sw rev (1.0/9.3(1)) status (Up Sys)
        Other host: Primary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5515 hw/sw rev (1.0/9.3(1)) status (Up Sys)
                slot 1: IPS5515 hw/sw rev (N/A/) status (Unresponsive/Up)

Stateful Failover Logical Update Statistics
        Link : folink GigabitEthernet0/0 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         27         0          43         6
        sys cmd         26         0          25         0
        up time         0          0          0          0
        RPC services    0          0          0          0
<--- More --->
```

```
VPN IKEv1 SA        0           0           2           0
VPN IKEv1 P2        0           0           2           0
VPN IKEv2 SA        0           0           0           0
VPN IKEv2 P2        0           0           0           0
VPN CTCP upd        0           0           0           0
VPN SDI upd         0           0           0           0
VPN DHCP upd        0           0           0           0
SIP Session         0           0           0           0
Route Session       0           0           13          0
Router ID           0           0           0           0
User-Identity       1           0           1           0
CTS SGTNAME         0           0           0           0
CTS PAC             0           0           0           0
TrustSec-SXP        0           0           0           0
IPv6 Route          0           0           0           0
STS Table           0           0           0           0

Logical Update Queue Information
                    Cur     Max     Total
Recv Q:             0       6       254
Xmit Q:             0       32      115
```

Checking status you can do the prompt command, and this should be inherited immediately in the other's config as well
(here shows as active or stby for standby -- always make changes on the active box or they will get clobbered))

```
ASA3(config)# prompt hostname cluster-unit ?

configure mode commands/options:
  context          Display the context in the session prompt (multimode only)
  domain           Display the domain in the session prompt
  management-mode  Display management mode
  priority         Display the priority in the session prompt
  state            Display the traffic passing state in the session prompt
  <cr>
ASA3(config)# prompt hostname cluster-unit con
ASA3(config)# prompt hostname cluster-unit context st
ASA3(config)# prompt hostname cluster-unit context state
ASA3/NoCluster/act(config)# end
```

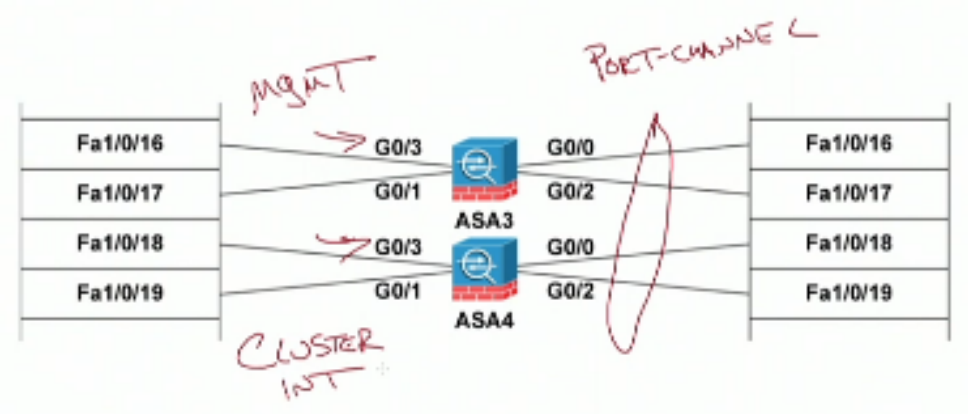
Monitoring individual interfaces
If you want the links to the devices (the R1 or R2) then make a standby address on the interface, so for R3
int g0/3
ip address 30.0.0.254 255.255.255.0 standby 30.0.0.250
This will put a line to the interface in **sh failover**

```
This host: Secondary - Active
        Active time: 580 (sec)
        slot 0: ASA5515 hw/sw rev (1.0/9.3(1)) status (Up Sys)
          Interface inside (10.0.0.254): Normal (Monitored)
          Interface outside (20.0.0.254): Normal (Monitored)
```

You can set failover tolerance: how many links go down before device is marked as "down"?

HA CLUSTERING

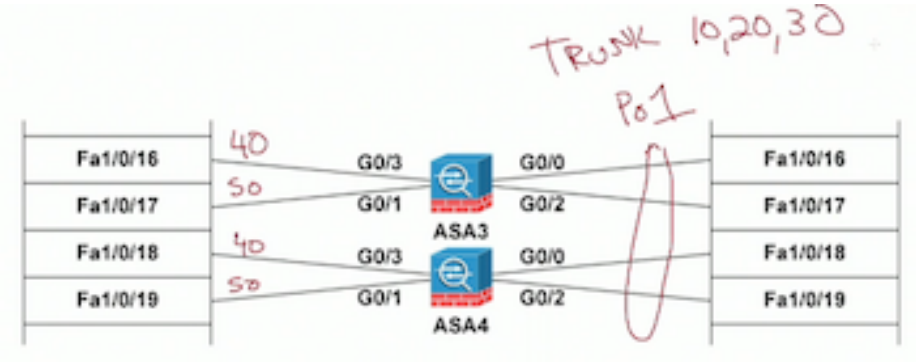
Different load balancing methods
- policy routing
- ECMP (every interface as native layer 3 routed interfaces (running a dynamic protocol)
Preferred:
- Spanned etherchannel
- single etherchannel that contains all of the interfaces in the data plane of the cluster
The switch won't know ASA3 and 4 are separate devices
- Management goes through other switch on 2 ints as does clustering ints to do control plane of cluster administrative duties



Says ideally a cluster int would be a port-channel but doesn't have to- not in example due to limited ints.
 ASA3 is going to be master, ASA4 slave
(clear config all on both and start fresh)

```
SW1(config)#vlan 40,50
SW1(config-vlan)#int range f1/0/16, f1/0/18
SW1(config-if-range)#sw
SW1(config-if-range)#switchport access vlan 40
SW1(config-if-range)#int range f1/0/17, f1/0/19
SW1(config-if-range)#switchport access vlan 50
SW1(config-if-range)#end
```

```
SW1#sh int status | in ASA3|ASA4
Fa1/0/16  ASA3 G0/3          notconnect   40           auto   auto 10/100BaseTX
Fa1/0/17  ASA3 G0/1          notconnect   50           auto   auto 10/100BaseTX
Fa1/0/18  ASA4 G0/3          notconnect   40           auto   auto 10/100BaseTX
Fa1/0/19  ASA4 G0/1          notconnect   50           auto   auto 10/100BaseTX
```



The portchannel could be made of separate physical interfaces if you want, but this is more portable/convenient/etc

```
SW2(config)#default int range f1/0/16 - 19
SW2(config)#int range f1/0/16 - 19
SW2(config-if-range)#shut
SW2(config-if-range)#channel-group 1 mode active
Creating a port-channel interface Port-channel 1
SW2(config-if-range)#switchport trunk encapsulation dot1q
SW2(config-if-range)#switchport mode trunk
SW2(config-if-range)#switchport trunk allowed vlan 10,20,30
SW2(config-if-range)#no shut
```

cluster interface-mode spanned - will show to other devices this is one device instead of several
On that line after, you can say check-details or force (to check config or just go with it)

Most configuration (such as on interfaces) will replicate over, but the cluster interface has to be set up individually on each box
int g0/0
channel-group 1 mode active <----this is going to be the cluster link for synchronizing data
no shut
int g0/2
channel-group 1 mode active
no shut
int po1
port-channel span-cluster ---- Cluster LACP protocol - so it can synchronize channels over cluster link

Need ip pool for giving IP addresses to secondaries

ip local pool CLUSTER_POOL 50.0.0.2-50.0.0.10 55585x allows 16- 5500x only2

int g0/3
management-only
security-level 100
ip address 50.0.0.1 255.255.255.0 cluster-pool CLUSTER_POOL

shut down this port on standby box too:
int g0/1
shut
exit

cluster-group CLUSTER1
cluster-interface g0/1 ip 40.0.0.1 255.255.255.0 priority 1 (since this is the primary lower is higher)
enable noconfirm <<--- how it starts up a box?
local-unit ASA3

```
ASA3# sh run cluster
cluster group CLUSTER1
 local-unit ASA3
 cluster-interface GigabitEthernet0/1 ip 40.0.0.1 255.255.255.0
 priority 1
 health-check holdtime 3
 clacp system-mac auto system-priority 1
 enable
```

place this on the secondary:

```
ciscoasa(config-if)# cluster group CLUSTER1
ciscoasa(cfg-cluster)#  local-unit ASA4
ciscoasa(cfg-cluster)#  cluster-interface GigabitEthernet0/1 ip 40.0.0.2 255.2$
INFO: Non-cluster interface config is cleared on GigabitEthernet0/1
ciscoasa(cfg-cluster)#  priority 2
ciscoasa(cfg-cluster)#  int g0/1
ciscoasa(config-if)# no shut
ciscoasa(config-if)# cluster group CLUSTER1
ciscoasa(cfg-cluster)# enable as-slave
```

Unlike failover, a slave in a cluster won't even allow making changes to it's config
Here, ended up restarting both boxes to get them to cooperate

```
ASA3# show cluster info
Cluster CLUSTER1: On
    Interface mode: spanned
    This is "ASA4" in state SLAVE
        ID        : 1
        Version   : 9.3(1)
        Serial No.: FCH1719J46Q
        CCL IP    : 40.0.0.2
        CCL MAC   : 6c41.6aa1.193c
        Last join : 18:29:32 UTC Sep 19 2014
        Last leave: N/A
Other members in the cluster:
    Unit "ASA3" in state MASTER
        ID        : 0
        Version   : 9.3(1)
        Serial No.: FCH1719J4A2
        CCL IP    : 40.0.0.1
        CCL MAC   : 6c41.6aa1.18c4
        Last join : 18:29:36 UTC Sep 19 2014
        Last leave: N/A
```

```
ASA3(config)# int po1.10
ASA3(config-subif)# vlan 10
ASA3(config-subif)# nameif inside
INFO: Security level for "inside" set to 100 by default.
ASA3(config-subif)# ip address 10.0.0.254 255.255.255.0
ASA3(config-subif)# int po1.20
ASA3(config-subif)# vlan 20
ASA3(config-subif)# ip address 20.0.0.254 255.255.255.0
ASA3(config-subif)# nameif outside
INFO: Security level for "outside" set to 0 by default.
ASA3(config-subif)# int po1.30
ASA3(config-subif)# vlan 30
ASA3(config-subif)# ip address 30.0.0.254 255.255.255.0
ASA3(config-subif)# nameif dmz
INFO: Security level for "dmz" set to 0 by default.
ASA3(config-subif)# security-level 50
ASA3(config-subif)# router ospf 1
ASA3(config-router)# network 10.0.0.254 255.255.255.255 area 0
ASA3(config-router)# network 20.0.0.254 255.255.255.255 area 0
ASA3(config-router)# network 30.0.0.254 255.255.255.255 area 0
```

Deep Packet Inspection:

Default policy:

```
ASA3# sh run policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect rsh
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect xdmcp
  inspect netbios
  inspect tftp
  inspect ip-options
```

sh run all class-map

```
 match response header content-type regex _default_msn-messenger
class-map type inspect http match-all _default_yahoo-messenger
 match request body regex _default_yahoo-messenger
class-map type inspect http match-all _default_windows-media-player-tunnel
 match request header user-agent regex _default_windows-media-player-tunnel
class-map type inspect http match-all _default_gnu-http-tunnel
 match request args regex _default_gnu-http-tunnel_arg
 match request uri regex _default_gnu-http-tunnel_uri
class-map type inspect http match-all _default_firethru-tunnel
 match request header host regex _default_firethru-tunnel_1
 match request uri regex _default_firethru-tunnel_2
class-map type inspect http match-all _default_aim-messenger
 match request header host regex _default_aim-messenger
class-map type inspect http match-all _default_http-tunnel
 match request uri regex _default_http-tunnel
class-map type inspect http match-all _default_kazaa
 match response header regex _default_x-kazaa-network count gt 0
class-map type inspect http match-all _default_shoutcast-tunneling-protocol
 match request header regex _default_icy-metadata regex _default_shoutcast-tunneling-p
rotocol
class-map class-default
 match any
```

sh run all policy-map

```
  message-length maximum client auto
  message-length maximum 512
  no message-length maximum server
  dns-guard
  protocol-enforcement
  nat-rewrite
  no id-randomization
  no id-mismatch
  no tsig enforced
policy-map type inspect rtsp _default_rtsp_map
 description Default RTSP policymap
 parameters
policy-map type inspect ipv6 _default_ipv6_map
 description Default IPV6 policy-map
 parameters
  verify-header type
  verify-header order
 match header routing-type range 0 255
  drop log
policy-map type inspect h323 _default_h323_map
 description Default H.323 policymap
 parameters
```

Making policy and class maps for http filtering:

```
ASA3(config)# policy-map type inspect ?
configure mode commands/options:
  dcerpc              Configure a policy-map of type DCERPC
  dns                 Configure a policy-map of type DNS
  esmtp               Configure a policy-map of type ESMTP
  ftp                 Configure a policy-map of type FTP
  gtp                 Configure a policy-map of type GTP
  h323                Configure a policy-map of type H.323
  http                Configure a policy-map of type HTTP
  im                  Configure a policy-map of type IM
  ip-options          Configure a policy-map of type IP-OPTIONS
  ipsec-pass-thru     Configure a policy-map of type IPSEC-PASS-THRU
  ipv6                Configure a policy-map of type IPv6
  mgcp                Configure a policy-map of type MGCP
  netbios             Configure a policy-map of type NETBIOS
  radius-accounting   Configure a policy-map of type Radius Accounting
  rtsp                Configure a policy-map of type RTSP
  scansafe            Configure a policy-map of type SCANSAFE
  sip                 Configure a policy-map of type SIP
  skinny              Configure a policy-map of type Skinny
ASA3(config)# policy-map type inspect http ?
configure mode commands/options:
  WORD < 129 char  policy-map name
ASA3(config)# policy-map type inspect http WEB_INSPECTION
ASA3(config-pmap)# ?
MPF policy-map configuration commands
  class         Policy criteria
  description   Specify policy-map description
  exit          Exit from MPF policy-map configuration mode
  help          Help for MPF policy-map configuration commands
  match         Specify policy criteria via inline match
```

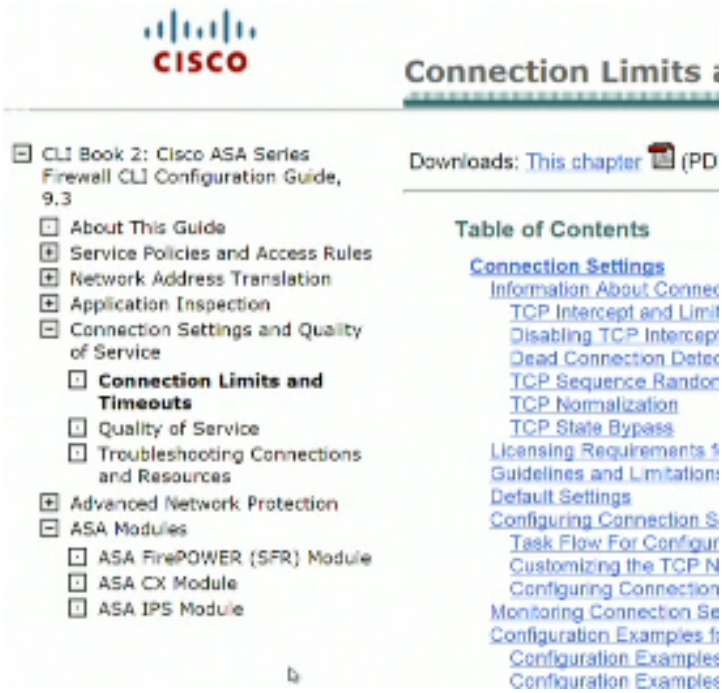
```
  no            Negate or set default values of a command
  parameters    Specify this keyword to enter policy parameters.
  rename        Rename this policy-map
  <cr>
ASA3(config-pmap)# class type ?
mpf-policy-map mode commands/options:
  <cr>
configure mode commands/options:
  inspect     Configure a class-map of type inspect
  management  Configure a class-map of type Management
  regex       Configure a class-map of type REGEX
ASA3(config-pmap)# class type inspect ?
configure mode commands/options:
  dns         Configure a class-map of type DNS
  ftp         Configure a class-map of type FTP
  h323        Configure a class-map of type H323
  http        Configure a class-map of type HTTP
  im          Configure a class-map of type IM
  rtsp        Configure a class-map of type RTSP
  scansafe    Configure a class-map of type SCANSAFE
  sip         Configure a class-map of type SIP
ASA3(config-pmap)# class type inspect http ?
configure mode commands/options:
  WORD < 129 char  class-map name
  match-all        Logical-AND all matching statements under this classmap
  match-any        Logical-OR all matching statements under this classmap
ASA3(config-pmap)# class type inspect http HTTP_CLASS
ASA3(config-cmap)# exit
ASA3(config)# class-map type inspect ?
configure mode commands/options:
  dns         Configure a class-map of type DNS
  ftp         Configure a class-map of type FTP
  h323        Configure a class-map of type H323
  http        Configure a class-map of type HTTP
  im          Configure a class-map of type IM
  rtsp        Configure a class-map of type RTSP
  scansafe    Configure a class-map of type SCANSAFE
  sip         Configure a class-map of type SIP
ASA3(config)# class-map type inspect http HTTP_CLASS
ASA3(config-cmap)# ?
MPF class-map configuration commands:
  description  Specify class-map description
  exit         Exit from MPF class-map configuration mode
  help         Help for MPF class-map configuration commands
  match        Configure classification criteria
  no           Negate or set default values of a command
  rename       Rename this class-map
ASA3(config-cmap)# match ?
mpf-class-map mode commands/options:
  not       Negate this match result
  req-resp  Apply match to request and response
  request   Apply match to request
  response  Apply match to response
ASA3(config-cmap)# match response ?
mpf-class-map mode commands/options:
  body         Apply the regular expression class-map to the message body
  header       Apply the regular expression class-map to the message header
  status-line  Apply the regular expression class-map to the status-line
ASA3(config-cmap)# match response hea
```

```
ASA3(config-cmap)# match response header ?
  age                 Age field
  allow               Allow field
  cache-control       Cache-Control field
  connection          Connection field
  content-Encoding    Content-Encoding field
  content-language    Content-Language field
  content-length      Content-Length field
  content-location    Content-Location field
  content-md5         Content-MD5 field
  content-range       Content-Range field
  content-type        Content-Type field
  count               Match maximum number of header fields
  date                Date field
  eTag                ETag field
  expires             Expires field
  last-modified       Last-Modified field
  length              Match total header length
  location            Location field
  non-ascii           Match non-ASCII characters in the header
  pragma              Pragma field
  proxy-authenticate  Proxy-Authenticate field
  regex               Match header name to a user-entered regex
  retry-after         Retry-After field
  server              Server field
  set-cookie          Set-Cookie field
  trailer             Trailer field
  transfer-encoding   Transfer-Encoding field
  upgrade             Upgrade field
  vary                vary
  via                 Via field
  warning             Warning field
  www-authenticate    www-authenticate
ASA3(config-cmap)# match req-resp
mpf-class-map mode commands/options:
  content-type  Match content-type in response to accept-types in request
ASA3(config-cmap)# match req-resp con
ASA3(config-cmap)# match req-resp content-type ?
mpf-class-map mode commands/options:
  mismatch  Specify that the content type in the response must match one of the
            mime-types in the  'accept' field of the request
ASA3(config-cmap)# match req
ASA3(config-cmap)# match req?
mpf-class-map mode commands/options:
  req-resp    request
ASA3(config-cmap)# match requ
ASA3(config-cmap)# match request ?
mpf-class-map mode commands/options:
  args    Apply the regular expression class-map to the arguments
  body    Apply the regular expression class-map to the message body
  header  Apply the regular expression class-map to the message header
  method  Apply the regular expression class-map to the method
  uri     Apply the regular expression class-map to the URI
ASA3(config-cmap)# match request method ?
  bdelete             Match on 'bdelete'
  bmove               Match on 'bmove'
  bpropfind           Match on 'bpropfind'
  bproppatch          Match on 'bproppatch'
  connect             Match on 'connect'
  copy                Match on 'copy'
```

```
  delete              Match on 'delete'
  edit                Match on 'edit'
  get                 Match on 'get'
  getattribute        Match on 'getattribute'
  getattributenames   Match on 'getattributenames'
  getproperties       Match on 'getproperties'
  head                Match on 'head'
  index               Match on 'index'
  lock                Match on 'lock'
  mkcol               Match on 'mkcol'
  mkdir               Match on 'mkdir'
  move                Match on 'move'
  notify              Match on 'notify'
  options             Match on 'options'
  poll                Match on 'poll'
  post                Match on 'post'
ASA3(config-cmap)# match request method post
```

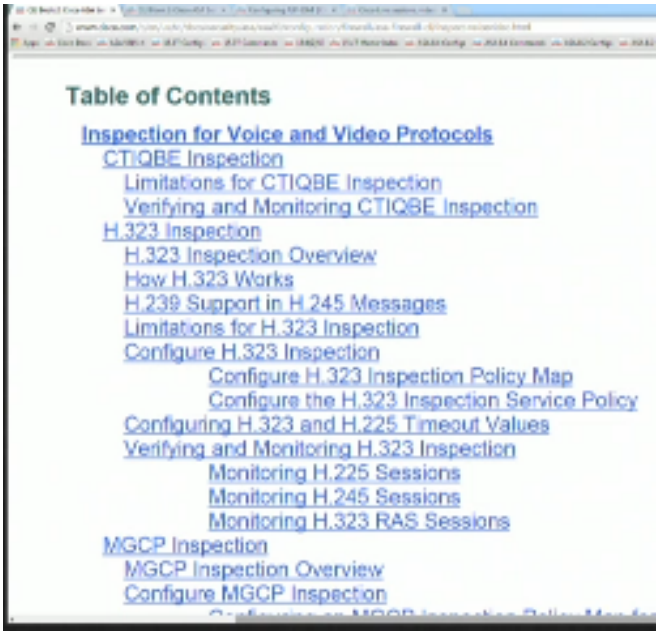
Book 2 ASA Firewall CLI Config Guide>Application Inspection>Getting Started Section on Connection Limits and Timeouts has methods of TCP normalization (protecting VS DoS attacks, half-open connections/ scanning)

```
ASA3(config)# tcp-map ABC
ASA3(config-tcp-map)# ?
TCP-map configuration commands:
  check-retransmission    Check retransmit data, disabled by default
  checksum-verification   Verify TCP checksum, disabled by default
  default                 Set a command to its defaults
  exceed-mss              Packet that exceed the Maximum Segment Size set by
                          peer, default is to allow packet
  invalid-ack             Packets with invalid ACK, default is to drop packet
  no                      Negate a command or set its defaults
  queue-limit             Maximum out-of-order packets queued for a connection,
                          default is 0 packets
  reserved-bits           Reserved bits in TCP header are set, default is to
                          allow packet
  seq-past-window         Packets that have past-window seq numbers, default is
                          to drop packet
  syn-data                TCP SYN packets that contain data, default is to
                          allow packet
  synack-data             TCP SYN-ACK packets that contain data, default is to
                          drop packet
  tcp-options             Options in TCP header
  ttl-evasion-protection  Protection against time to live (TTL) attacks,
                          enabled by default
  urgent-flag             Urgent flag and urgent offset set, default is to
                          clear flag and offset
  window-variation        Unexpected window size variation, default is to allow
                          connection
```



CX and FirePower modules need module or hard drive image. Web based GUI - content filtering
IPS module - IPS 4200 device in a module

FirePower obtained from SourceFire
Need subscription for updates
Cisco Live website - nextgen FW videos



With voice you also need to remember outbound and inbound - existing maps should do it

---

vpnsetup command
--- lays out steps, commands for each you need to use (is a guide) 11:30 in video 7

ASA3(config)# vpnsetup ?
  ipsec-remote-access Display IPSec Remote Access Configuration Commands
  l2tp-remote-access Display L2TP/IPSec Configuration Commands
  site-to-site Display IPSec Site-to-Site Configuration Commands
  ssl-remote-access Display SSL Remote Access Configuration Commands

ipsec-remote-access	IPSec site-to-site	ssl-remote access	
1. Configure Interfaces	1. Configure Interfaces	1. Configure Interfaces	
2. Configure ISAKMP policy	2. Configure ISAKMP policy	2. Enable WebVPN on the interface	
3. Setup an address pool	3. Configure transform-set	3. Configure default route	
4. Configure authentication method	4. Configure ACL	4. Configure AAA authentication and tunnel group	
5. Define tunnel group	5. Configure Tunnel group	5. If using LOCAL database, add users to the Database	
6. Setup ipsec parameters	6. Configure crypto map, attach to interface	6. Point the ASA to an AnyConnect image	
7. Setup dynamic crypto map	7. Enable isakmp on interface	7. enable AnyConnect	
8. Create crypto map entry and associate dynamic map		8. Add an address pool	
9. Attach crypto map to interface		9. Configure group policy	
10. Enable isakmp on interface			

ciscoasa(config)# vpnsetup ipsec-remote-access steps

Steps to configure a remote access IKE/IPSec connection with examples:

1. Configure Interfaces
interface GigabitEthernet0/0
ip address 10.10.4.200 255.255.255.0
nameif outside
no shutdown

interface GigabitEthernet0/1
ip address 192.168.0.20 255.255.255.0
nameif inside
no shutdown

2. Configure ISAKMP policy
crypto isakmp policy 65535
authentication pre-share
encryption aes
hash sha

3. Setup an address pool
ip local pool client-pool 192.168.1.1-192.168.1.254

4. Configure authentication method -------(tunnel-group step5 is group authentication - this is user auth, and assumes you employ a Radius server)

aaa-server MyRadius protocol radius
aaa-server MyRadius host 192.168.0.254
key $ecretK3y

5. Define tunnel group -------(with group username and group password in ipsec client, the username is the tunnel-group name "client" , and the password the PSK)
tunnel-group client type remote-access
tunnel-group client general-attributes
address-pool client-pool --------(here is where the address is obtained- the rest from group policy. Here it is DefltGroupPolicy, but in Split Tunnel this will change)
authentication-server-group MyRadius
tunnel-group client ipsec-attributes
pre-shared-key VpnUs3rsP@ss

6. Setup ipsec parameters
crypto ipsec transform-set myset esp-aes esp-sha-hmac

7. Setup dynamic crypto map
crypto dynamic-map dynmap 1 set transform-set myset
crypto dynamic-map dynmap 1 set reverse-route

8. Create crypto map entry and associate dynamic map with it
crypto map mymap 65535 ipsec-isakmp dynamic dynmap

9. Attach crypto map to interface
crypto map mymap interface outside

10. Enable isakmp on interface
crypto isakmp enable outside

ciscoasa(config)# vpnsetup l2tp-remote-access steps

Steps to configure a remote access L2TP/IPSec connection with examples:

1. Configure Interfaces
interface GigabitEthernet0/0
ip address 10.10.4.200 255.255.255.0
nameif outside
no shutdown

interface GigabitEthernet0/1
ip address 192.168.0.20 255.255.255.0
nameif inside
no shutdown

2. Configure ISAKMP policy
crypto isakmp policy 65535
authentication pre-share

encryption aes
hash sha

3. Setup an address pool
ip local pool client-pool 192.168.1.1-192.168.1.254

4. Configure authentication method
aaa-server MyRadius protocol radius
aaa-server MyRadius host 192.168.0.254
key $ecretK3y

5. Define tunnel group
tunnel-group client type remote-access
tunnel-group client general-attributes
address-pool client-pool
authentication-server-group MyRadius
tunnel-group client ipsec-attributes
pre-shared-key VpnUs3rsP@ss
tunnel-group DefaultRAGroup ppp-attributes
authentication pap

6. Setup ipsec parameters
crypto ipsec transform-set myset esp-aes esp-sha-hmac
crypto ipsec transform-set myset mode transport

7. Setup dynamic crypto map
crypto dynamic-map dynmap 1 set transform-set myset

8. Create crypto map entry and associate dynamic map with it
crypto map mymap 65535 ipsec-isakmp dynamic dynmap

9. Attach crypto map to interface
crypto map mymap interface outside

10. Enable isakmp on interface
crypto isakmp enable outside

ciscoasa(config)# vpnsetup site-to-site steps

Steps to configure a site-to-site IKE/IPSec connection with examples:

1. Configure Interfaces
interface GigabitEthernet0/0
ip address 10.10.4.200 255.255.255.0
nameif outside
no shutdown

interface GigabitEthernet0/1

ip address 192.168.0.20 255.255.255.0
nameif inside
no shutdown

2. Configure ISAKMP policy -------(usually IKEv1)
crypto isakmp policy 10
authentication pre-share
encryption aes
hash sha

3. Configure transform-set -------(how encrypt?)
crypto ipsec transform-set myset esp-aes esp-sha-hmac

4. Configure ACL -------(what traffic inside tunnel?)
access-list L2LAccessList extended permit ip 192.168.0.0 255.255.255.0 192.168.50.0 255.255.255.0

5. Configure Tunnel group -------(who is traffic going towards?)
tunnel-group 10.20.20.1 type ipsec-l2l
tunnel-group 10.20.20.1 ipsec-attributes
pre-shared-key P@rtn3rNetw0rk

6. Configure crypto map and attach to interface
crypto map mymap 10 match address L2LAccessList
crypto map mymap 10 set peer 10.10.4.108
crypto map mymap 10 set transform-set myset
crypto map mymap 10 set reverse-route
crypto map mymap interface outside

7. Enable isakmp on interface
crypto isakmp enable outside

ciscoasa(config)# vpnsetup ssl-remote access steps

Steps to configure a remote access SSL VPN remote access connection and AnyConnect with examples:

1. Configure and enable interface
interface GigabitEthernet0/0
ip address 10.10.4.200 255.255.255.0
nameif outside
no shutdown

interface GigabitEthernet0/1
ip address 192.168.0.20 255.255.255.0
nameif inside
no shutdown

2. Enable WebVPN on the interface
webvpn
enable outside

3. Configure default route
route outside 0.0.0.0 0.0.0.0 10.10.4.200

4. Configure AAA authentication and tunnel group
tunnel-group DefaultWEBVPNGroup type remote-access
tunnel-group DefaultWEBVPNGroup general-attributes
authentication-server-group LOCAL

5. If using LOCAL database, add users to the Database
username test password t3stP@ssw0rd
username test attributes
service-type remote-access

Proceed to configure AnyConnect VPN client:

6. Point the ASA to an AnyConnect image
webvpn
svc image anyconnect-win-2.1.0148-k9.pkg

7. enable AnyConnect
svc enable

8. Add an address pool to assign an ip address to the AnyConnect client
ip local pool client-pool 192.168.1.1-192.168.1.254 mask 255.255.255.0

9. Configure group policy
group-policy DfltGrpPolicy internal
group-policy DfltGrpPolicy attributes
vpn-tunnel-protocol svc webvpn