Capítulo 10

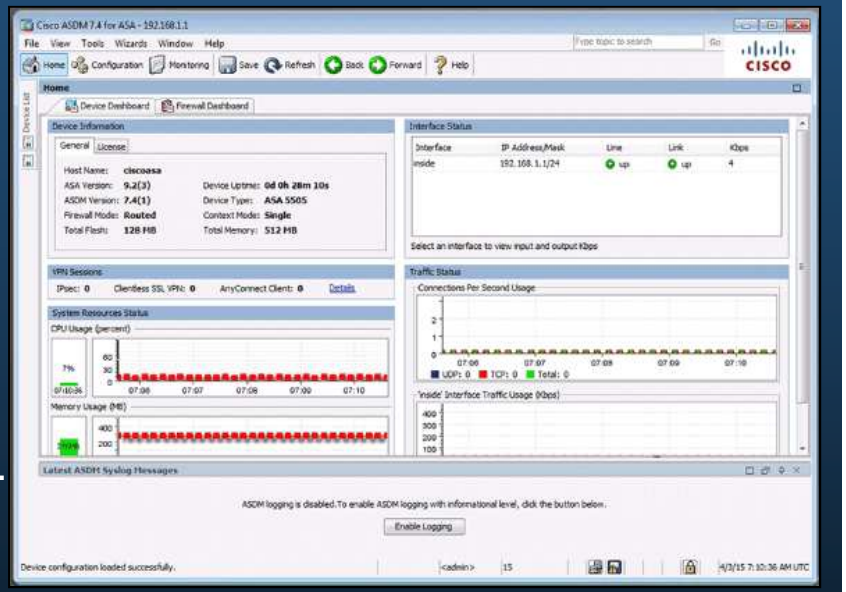
Dispositivo Avanzado de Seguridad Adaptable de Cisco

https://static-course-assets.s3.amazonaws.com/CCNAS2/en/index.html#10.1.1.1

10.1 ASDM.

No disponible en PacketTracer

- Introducción a ASDM.
  - Administrador de Dispositivo de Seguridad ASA.
    - GUI Java intuitiva que simplifica las tareas de administración de un ASA.
      - Configuración.
      - Monitoreo.
      - Resolución de problemas.
    - Elimina la necesidad de conocimientos avanzados en el uso de la CLI.
    - Utiliza SSL para comunicarse con el ASA.
    - Asistentes de configuración agilizan el proceso.



- Método preferido para configurar, administrar, y monitorear un ASA.

10.1 ASDM.

- Preparaciones para ASDM.
  - Configuraciones mínimas.
    - Configurar interface de administración (diferente en cada modelo)
      - En ASA 5505:
        - Interface VLAN Local Interna (p' admin): Asignar IP y nivel de seguridad
        - Ethernet 0/1, Por default pertenece a VLAN 1; Habilitar.
        - Habilitar Servidor Web; deshabilitado por defecto.
        - Permitir acceso al Servidor Web ASA; denegado por defecto.

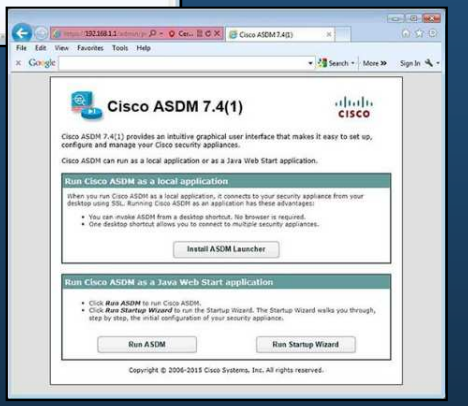
```
ciscoasa# conf t
ciscoasa(config)# interface vlan 1
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
ciscoasa(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
ciscoasa(config-if)# exit
ciscoasa(config)#
ciscoasa(config)# interface Ethernet0/1
ciscoasa(config-if)# no shut
ciscoasa(config-if)# exit
ciscoasa(config)#
ciscoasa(config)# http server enable
ciscoasa(config)# http 192.168.1.3 255.255.255.255 inside
ciscoasa(config)#
```

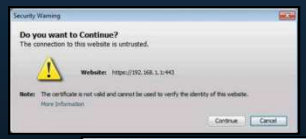
Habilita servidor http
Para deshabilitar:
`ASA(config)# clear configure http`

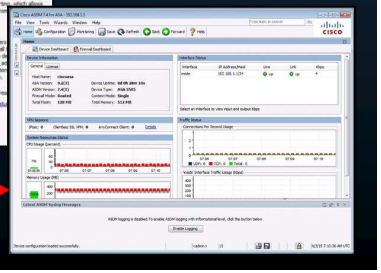
Permite acceso solo a 192.168.1.3

10.1 ASDM.

- Iniciar ASDM.
  - Aceptar certificado SSL (autofirmado) del servidor web ASA.
    - Abrir https://IP de la SVI del ASA en servidor WEB y aceptar certificado.
  - Ofrece dos opciones para lanzar ASDM:
    - Correr como aplicación local: Instala aplicación al equipo de escritorio (multiples ASAs).
    - Correr como aplicación Java WebStart: Ejecuta mediante conexión con el navegador web (No se instala / un solo ASA).
      - Correr asistente de configuración: Ejecuta asistente mediante web, para configuración paso a paso.
    - Correr mediante navegador genera advertencias de seguridad, que hay que aceptar.
  - ASMD solicita credenciales de usuario (dejar en blanco).
  - Elegir una opción en ventana de Inicio para SmartCall:
  - Despliega ventana de Inicio ASDM:



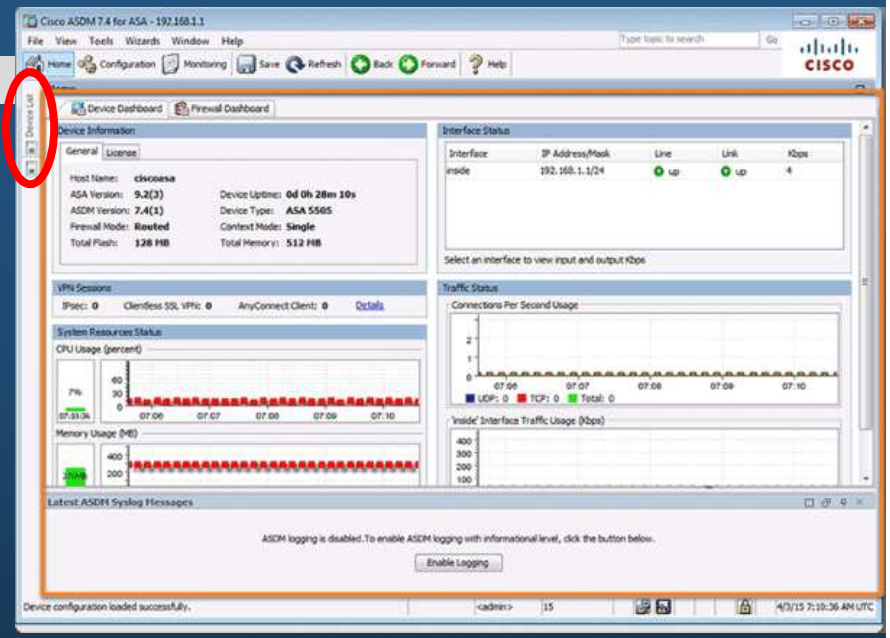


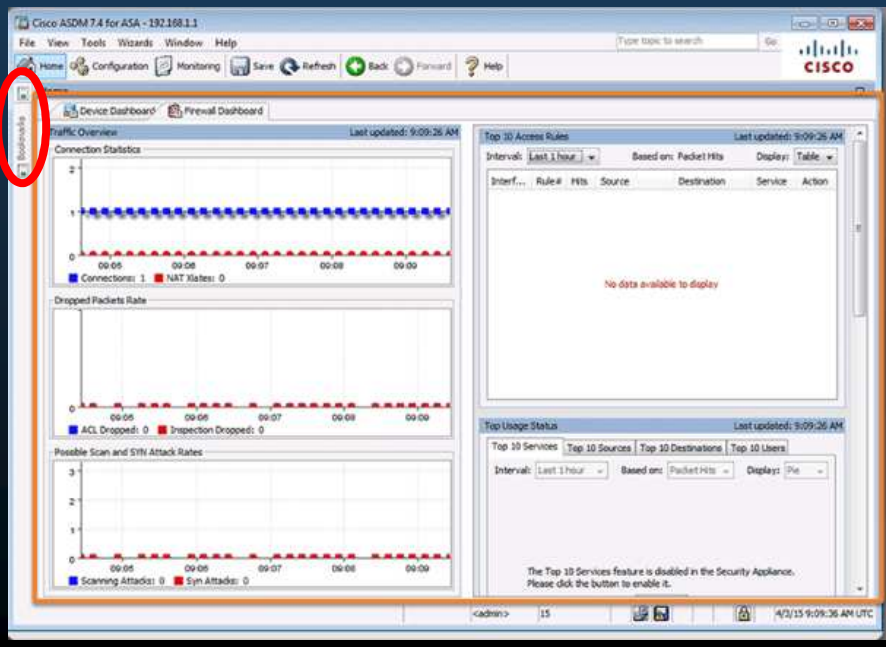


Envío de datos de uso a Cisco - Do not Enable

10.1 ASDM.

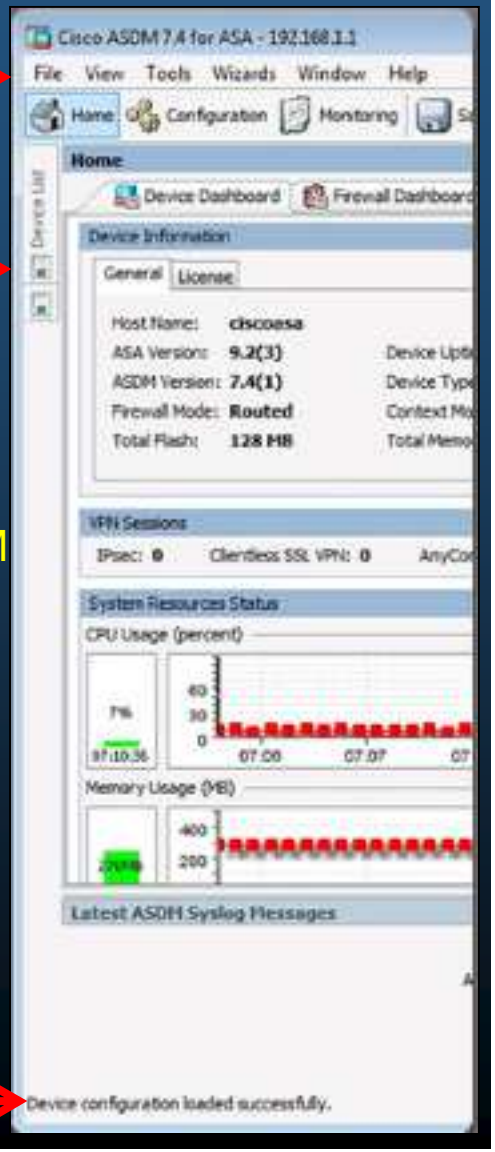
- Cuadros de Mando ASDM.
  - Pestaña Dispositivo (Inicio).
    - Estado ASA (actualiza cada 10s).
    - Interfaces
    - Versión de Sistema Operativo.
    - Licencia
    - Desempeño
  - Pestaña Firewall.
    - Estadísticas de Conexiones.
    - Paquetes Perdidos.
    - Escaneos.
    - Deteción de Ataques SYN
  - Prevención de Intrusiones.
    - Requiere Modulo IPS.
  - Contenido de Seguridad.
    - Requiere Módulo CSC-SSM.





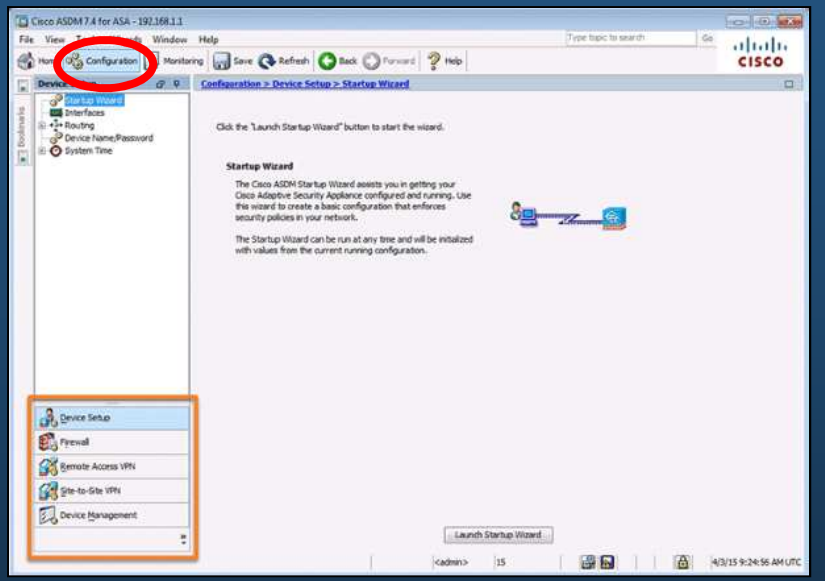
10.1 ASDM.

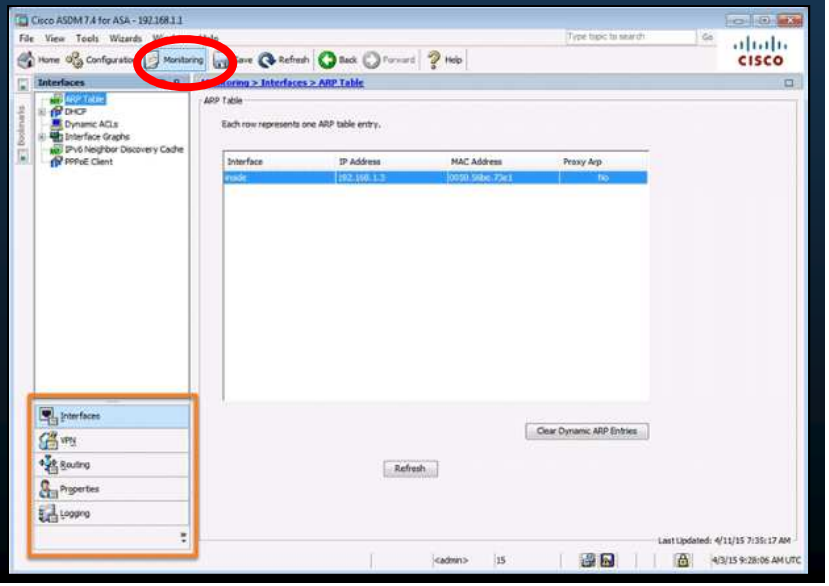
- Elementos ASDM.
  - Barra de Menú.
    - Acceso Rápido a Archivos, Herramientas, Asistentes, …
  - Barra de Herramientas.
    - Inicio, Configuración, Monitoreo, Guardar, Refrescar, Navegar entre Vistas, etc…
  - Botón Lista de Dispositivos.
    - Abre página con lista de otros dispositivos.
    - Permite cambiar a otro dispositivo con misma versión ASDM
  - Barra de Estado.
    - Despliega
      - Hora.
      - Estado de Conexión.
      - Usuario.
      - Estado de Memoria y Configuración.
      - Estado SSL.
      - …



10.1 ASDM.

- Vistas ASDM.
  - Configuración.
    - Configuración de Dispositivo.
    - Firewall
    - VPN de Acceso Remoto
    - VPN Sitio-a-Sitio
    - Administración de Dispositivo
  - Monitoreo.
    - Interfaces.
    - VPN.
    - Enrutamiento.
    - Propiedades.
    - Registros.
  - Video demostración de configuración.





10.1 ASDM.

- Asistentes ASDM.
  - Varios asistentes disponibles:
    - Configuración Inicial.
    - VPN.
    - Alta disponibilidad y escalabilidad.
    - Comunicación unificada.
    - Certificados de Identidad
    - Captura de Paquetes.

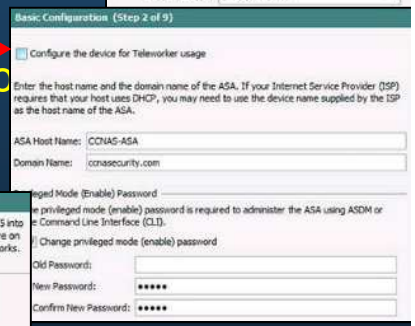
10.1 ASDM.

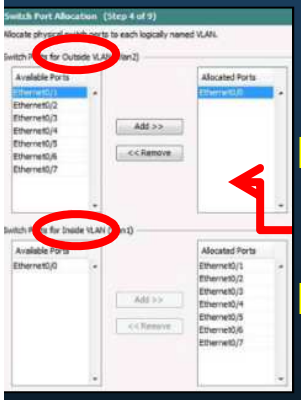
- Asistente de Configuración Inicial.
  - Wizards > Startup Wizard ó
  - Configuration > Device Setup > Startup Wizard > Launch Startup Wizard.
    - Paso 1. Punto Inicial.
      - Modificar Configuración Existente / Resetear a estado de fábrica.
    - Paso 2. Configuración Básica.
      - Nombre de Host; Nombre de Dominio, Contraseña de Modo Privilegiado; Configurar un trabajador a distancia.

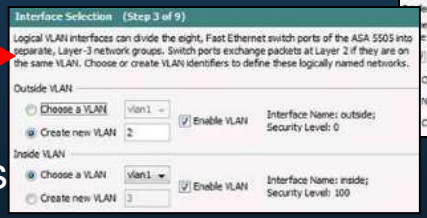
Paso 3. Selección de Interfaces.
- Elegir o Crear SVIs (ASA 5505).

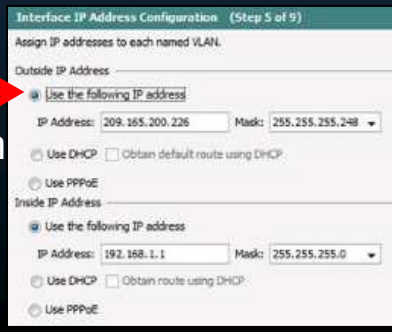
Paso 4. Asignación de Puertos Switcheados
- Mapeo de Puertos Capa 2 a VLANs.

    - Paso 5. Configuración IP de Interfaces.
      - Identificar red interna / externa; IPs para SVIs; Si se obtienen por DHCP ó PPPoE.



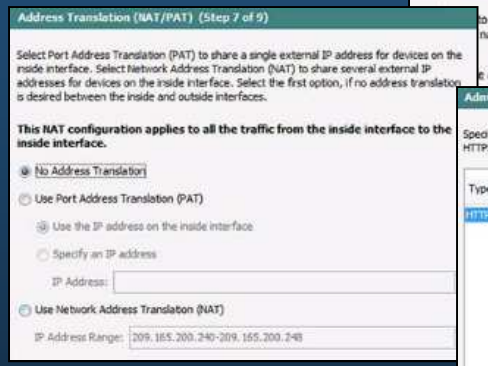


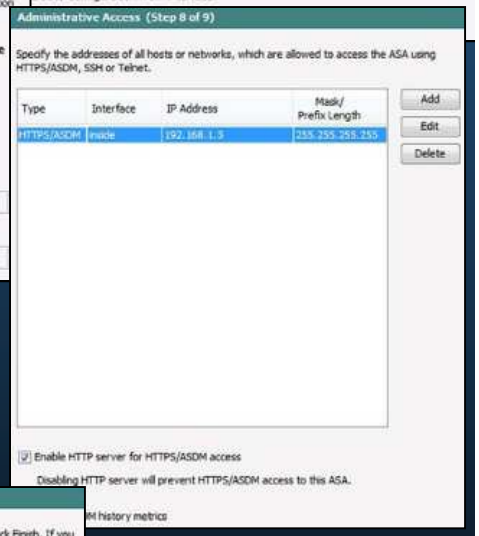




10.1 ASDM.

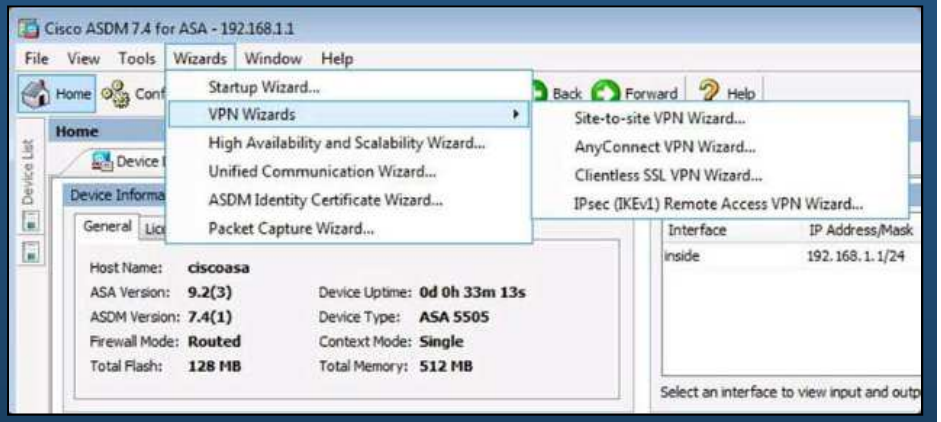
- Asistente de Configuración Inicial (Cont.).
  - Paso 6. Opciones DHCP.
    - Habilitar DHCP para red Interna. Y administrar sus opciones.
  - Paso 7. NAT / PAT.
    - Habilita NAT / PAT. Y administra sus opciones.
  - Paso 8. Acceso Adminitrativo.
    - Especifica Hosts que podrán acceder al ASA por: HTTPS/ASDM; SSH; Telnet.
  - Paso 9. Resumen.
    - Permite revisar la configuración propuesta.
    - Back para hacer cambios.
    - Finish para establecer configuración.





10.1 ASDM.

- Asistentes VPN.
  - Wizards > VPN Wizards.
    - Sitio-a-Sitio.
    - AnyConnect.
    - VPN Sin Clientes.
    - IPSec (IKEv1) Acceso Remoto.

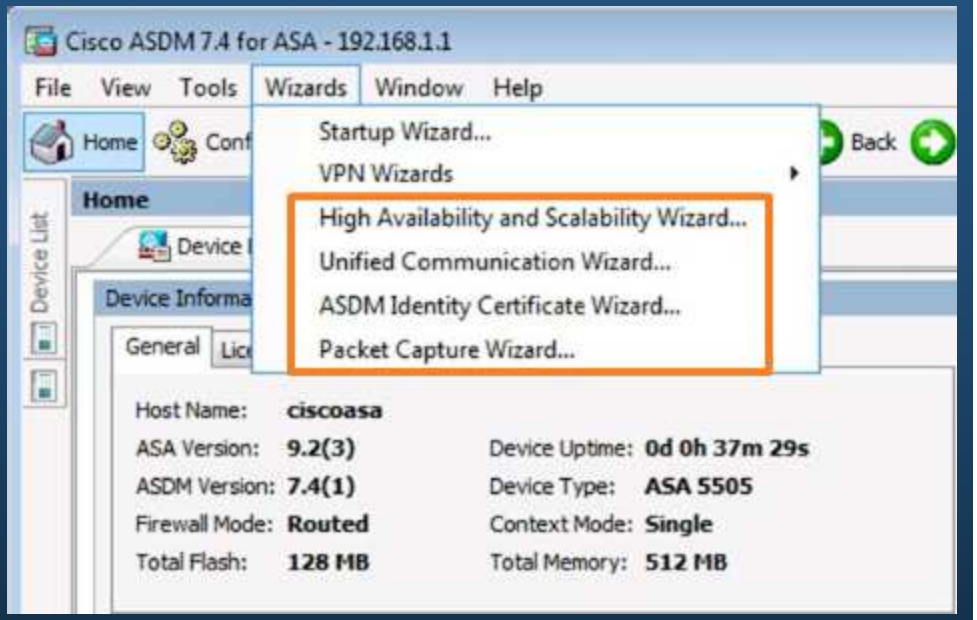


- Complementar configuración con Asistente ASDM.
  - Configurations > Remote-Access VPN > Introduction.

- Tras una configuración inicial, puede usarse ASDM, para realizar una configuración avanzada.

10.1 ASDM.

- Otros Asistentes.
  - Alta Disponibilidad y Escalabilidad.
    - Configura Cluster VPN con balanceo de carga.
    - Requiere dos ASAs que establezcan sesión a la misma red para el balanceo de carga.
    - No disponible en 5505 Base.



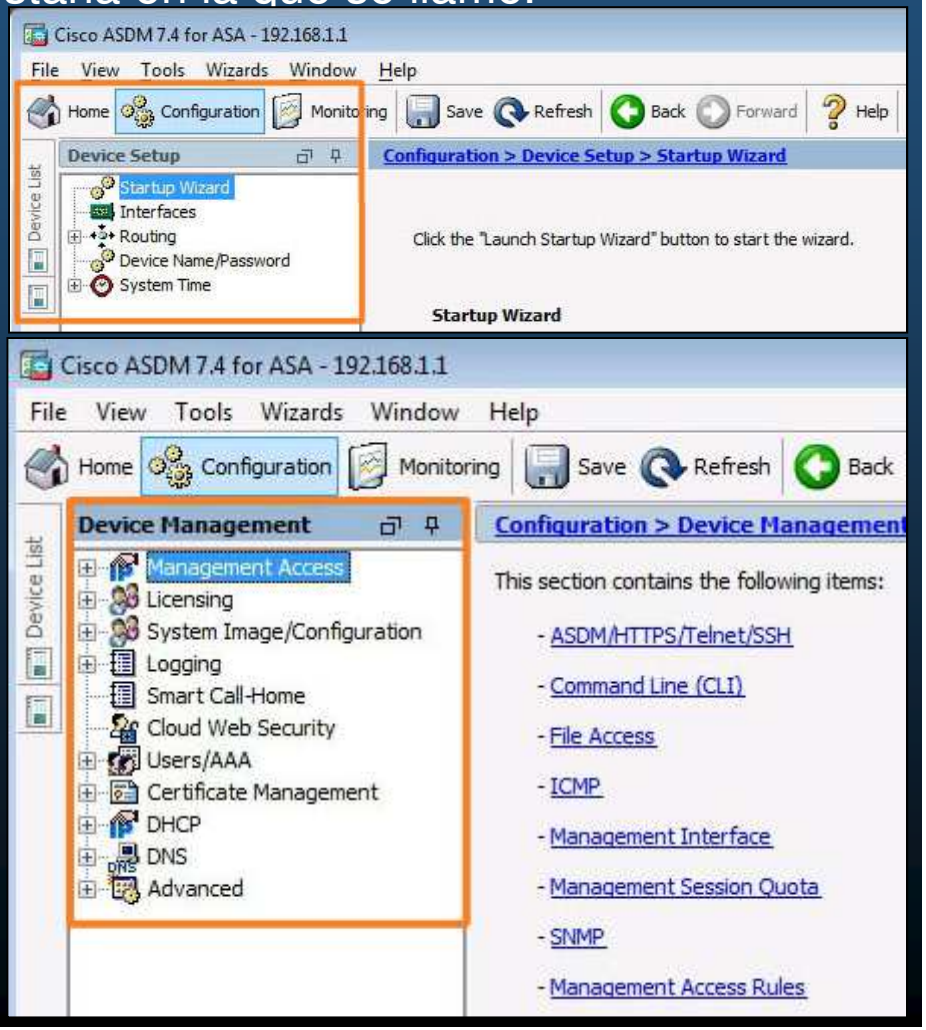
  - Comunicación Unificada.
    - Proxy Cisco. ACLs; NAT/PAT; Certificados Auto-firmados; Proxy TSL; Inspección de Aplicaciones.

Fuera del alcance del capítulo

  - Certificados de Identidad.
    - Requiere certificado de confianza. No Autofirmado.
  - Captura de Paquetes.
    - Útil para resolución de errores.
    - Puede usar ACLs para límitar tráfico capturado; origen y destino; interfaces; sentido; etc…

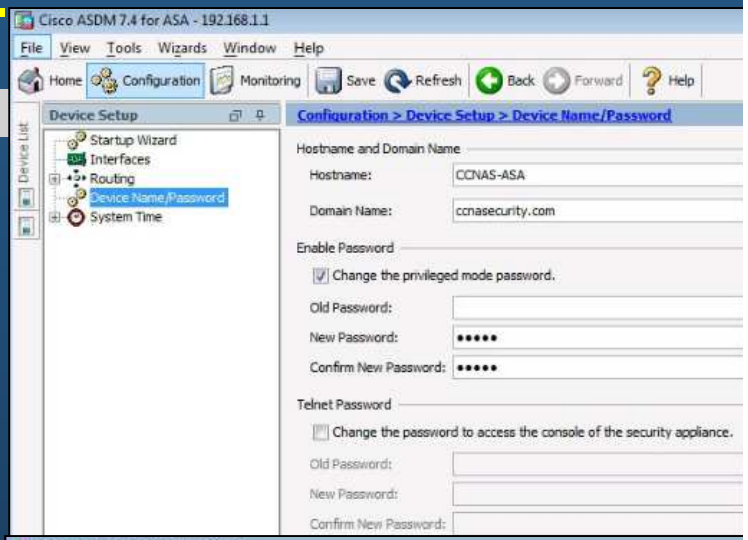
10.1 ASDM.

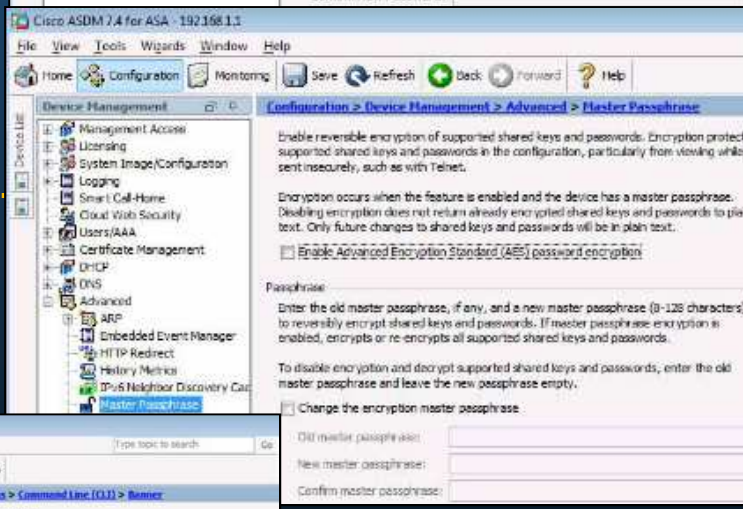
- Configuraciones en ASDM.
  - Vista Configuración depende de la Pestaña en la que se llame.
    - Configuración de Dispositivo:
      - Nombre de Host; Contraseñas; Fecha/Hora; Interfaces; Enrutamiento
    - Administración:
      - Acceso Administrativo
      - Usuarios y AAA
      - DHCP
      - Notificaciones Legales
      - Frase de Paso
      - …



10.1 ASDM.

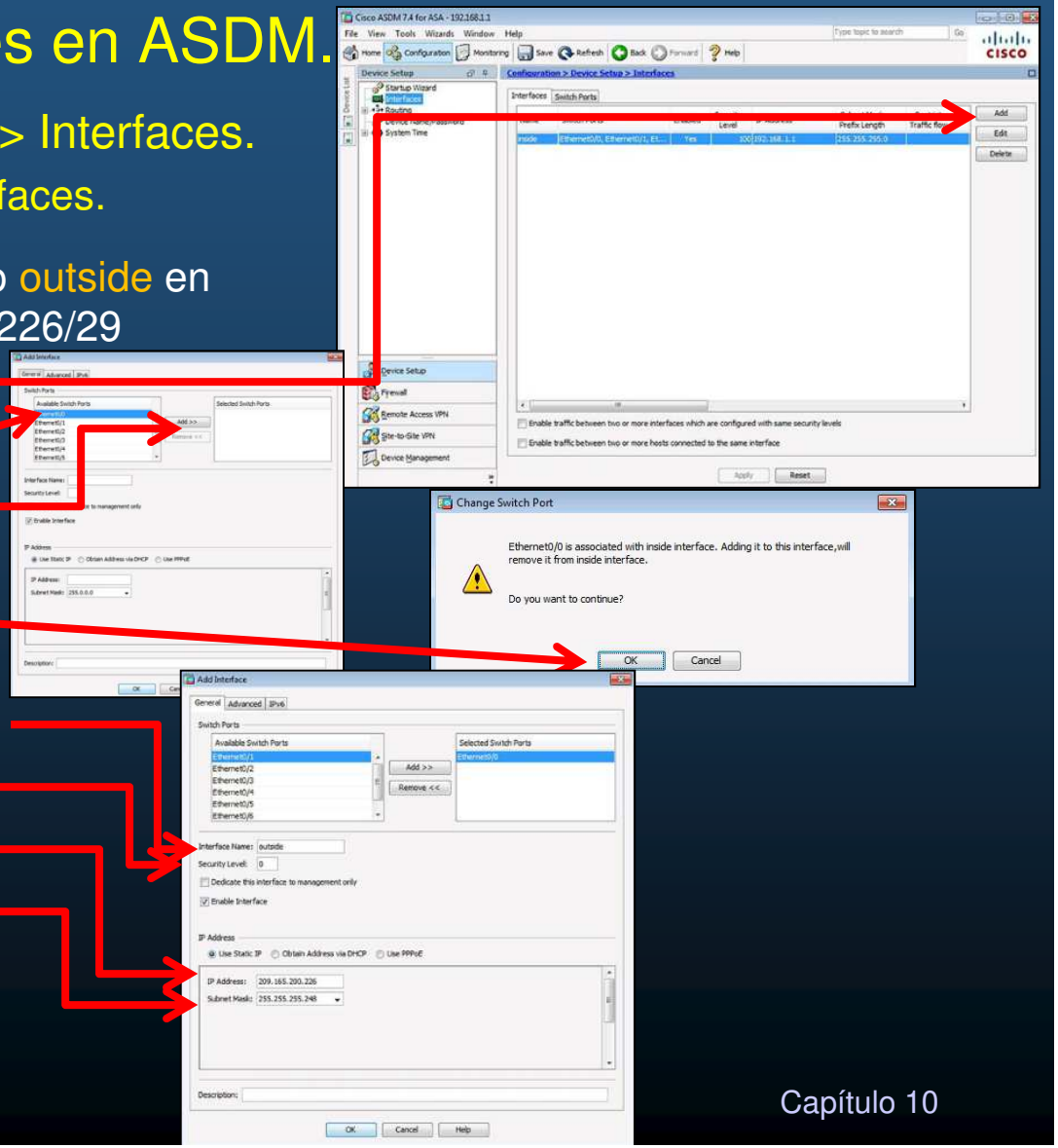
- Configuraciones Básicas en ASDM.
  - Configuration > Device Setup > Device Name/Password.
    - `hostname`,
    - `domain name`,
    - `enable password`.
  - Configuration > Device Management > Advanced > Master Passphrase.
    - `PassPhase` (Cifrado AES)
    - Re-cifra llaves compartidas en ASA.
  - Configuration > Device Management > Management Access > Command Line (CLI) > Banner.
    - Varios Banners





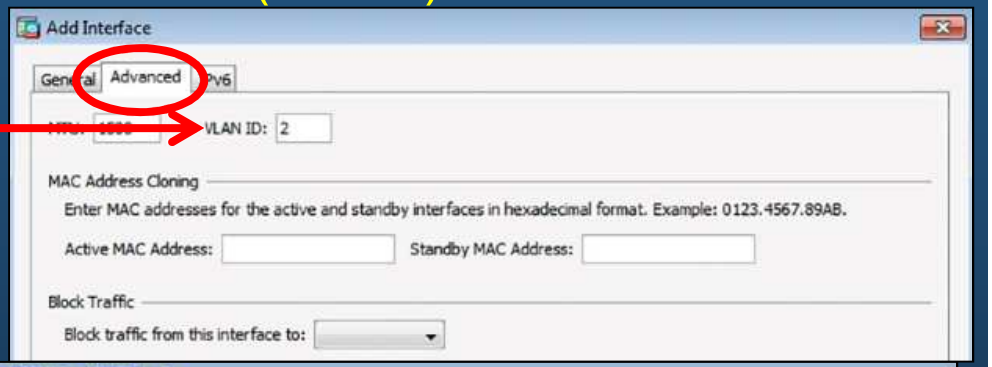
10.1 ASDM.

- Configuración de Interfaces en ASDM.
  - Configuration > Device Setup > Interfaces.
    - Crear; Editar o Eliminar Interfaces.
    - Vgr; Configurar Eth 0/0 como outside en VLAN2 con IP: 209.165.200.226/29
      - Boton “Add”
        - Elegir Eth 0/0
        - Añadir con Add >>
        - Click en OK a la confirmación
        - Entrar nombre de interface
        - Nivel de seguridad
        - Dirección IP
        - Mascara de Red

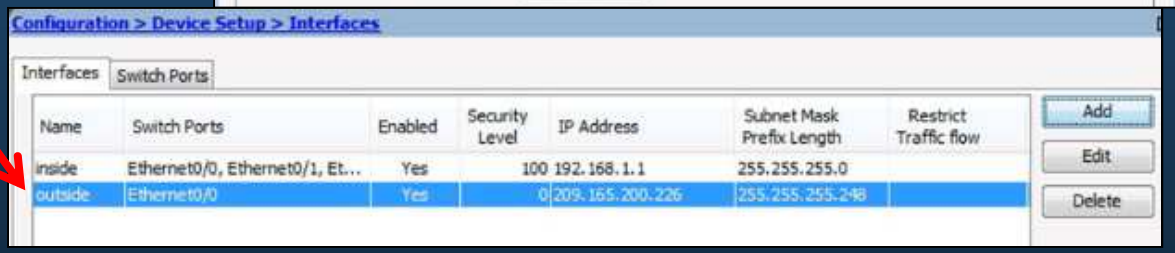


10.1 ASDM.

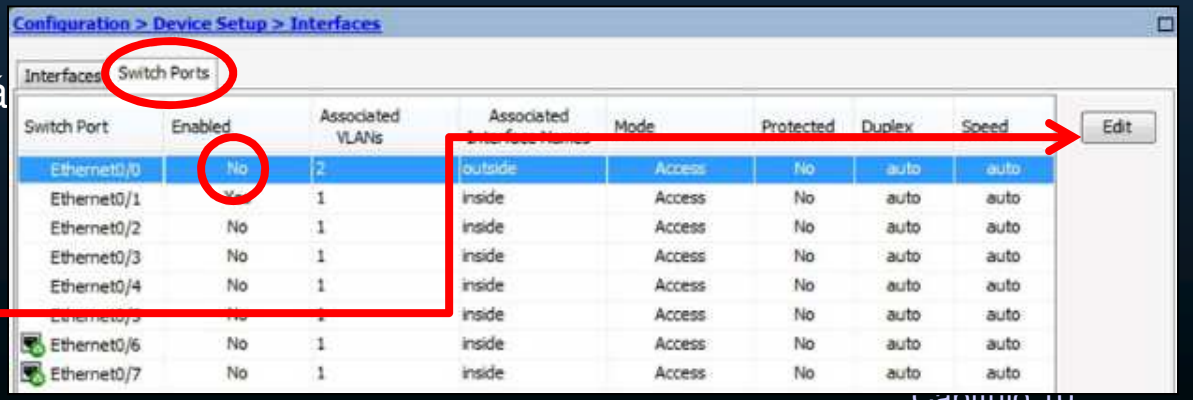
- Configuración de Interfaces en ASDM (Cont.).
  - Elegir Pestaña “Advanced”
    - Indicar VLAN 2
    - Click en OK



  - ASDM muestra configuración actualizada:

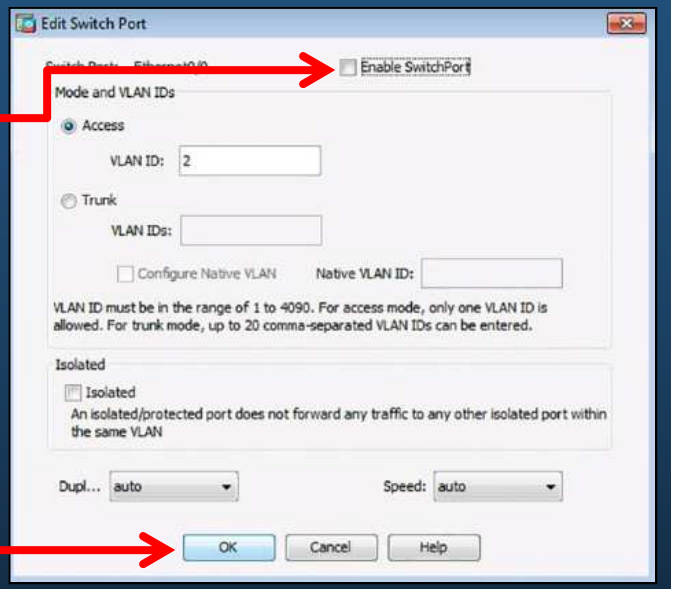


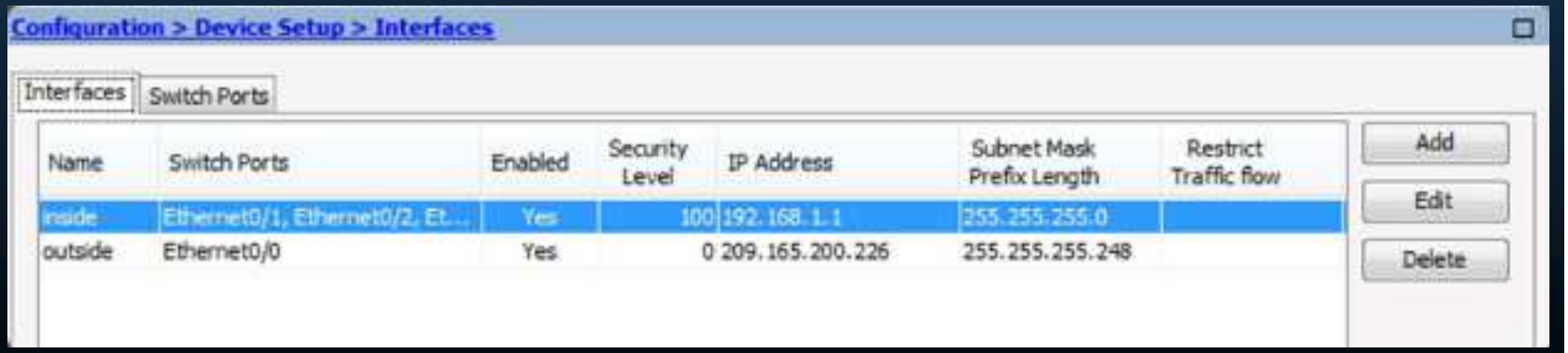
  - La Pestaña Switchport muestra varias configuraciones para puertos.
    - Eth 0/0 no está habilitada.
    - Click en Edit



10.1 ASDM.

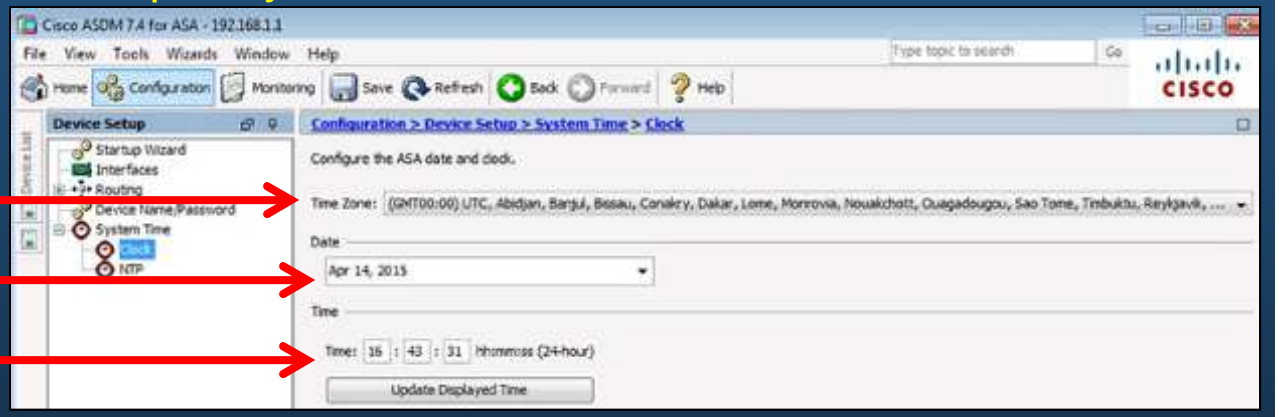
- Configuración de Interfaces en ASDM (Cont 2.).
  - Click en “Enable SwitchPort”
  - Click en OK
  - Aplicar la Configuración.
  - ASDM muestra configuración actualizada:



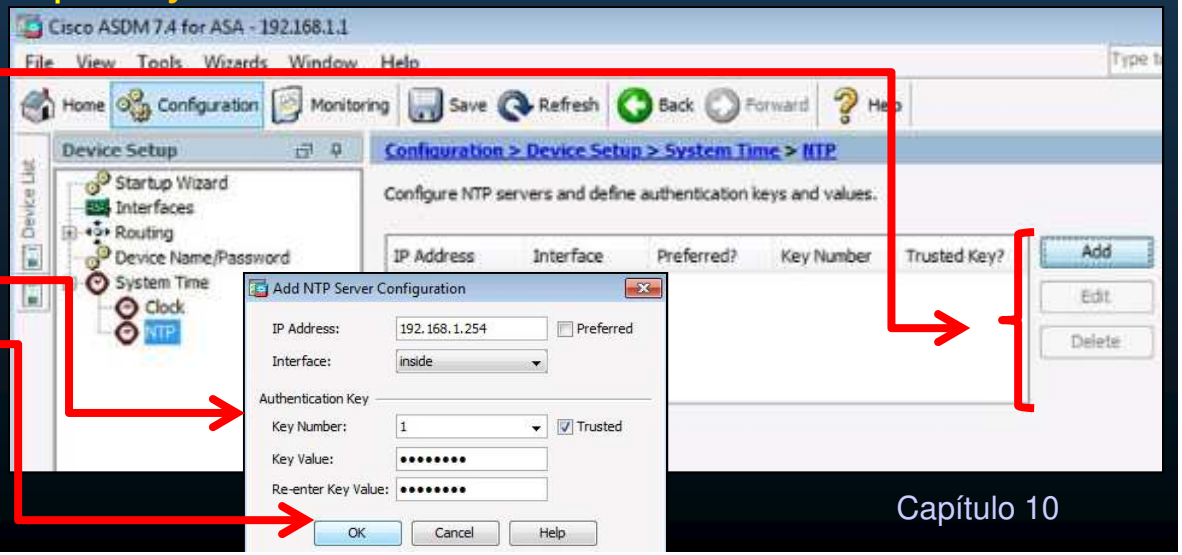


10.1 ASDM.

- Configurar Fecha / Hora en ASDM.
  - Configuration > Device Setup > System Time > Clock.
    - Zona Horaria.
    - Fecha.
    - Hora.

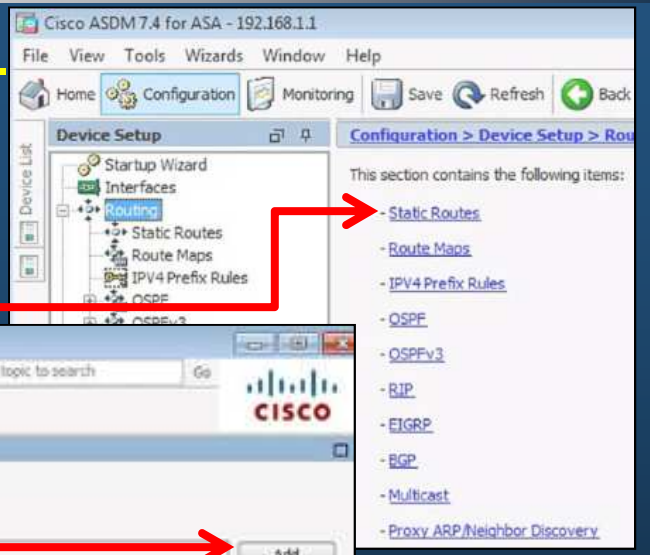


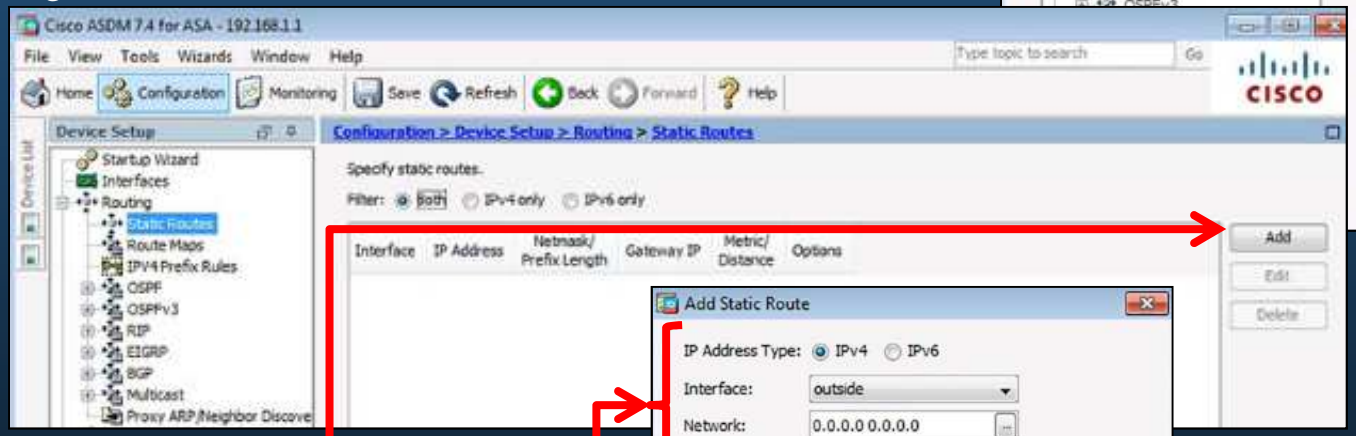
  - Configuration > Device Setup > System Time > NTP.
    - Añadir; Editar; Eliminar.
    - Add
      - Entrar parámetros de Servidor NTP.
      - Ok
    - Actualizará la vista de servidores NTP.

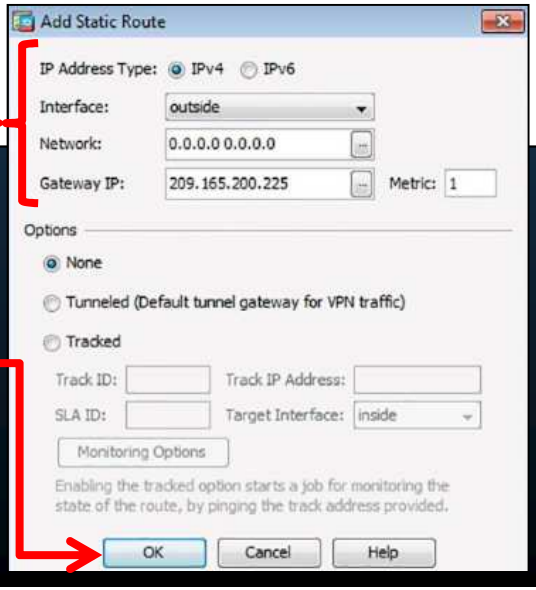


10.1 ASDM.

- Configuración de Enrutamiento en ASDM.
  - Configuration > Device Setup > Routing.
    - Habilitar enrutamiento estático y dinámico IPv4/6
    - Vgr; > Static Routes.



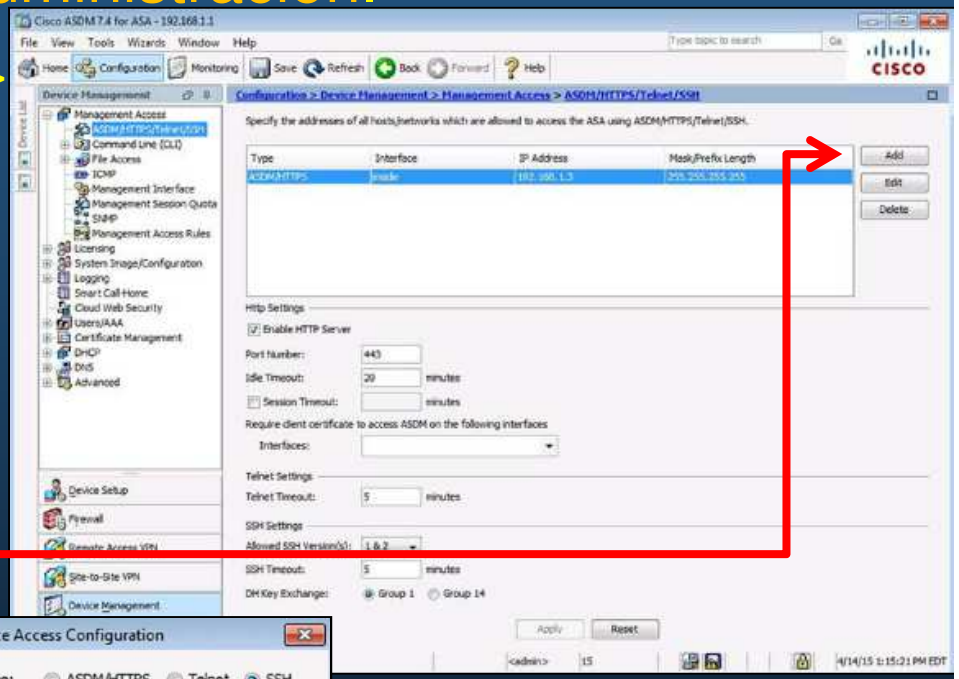


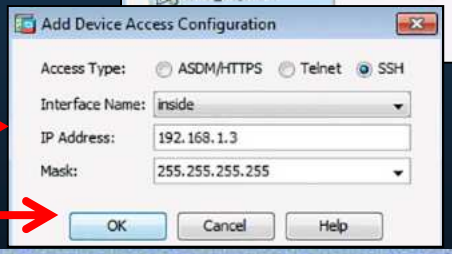


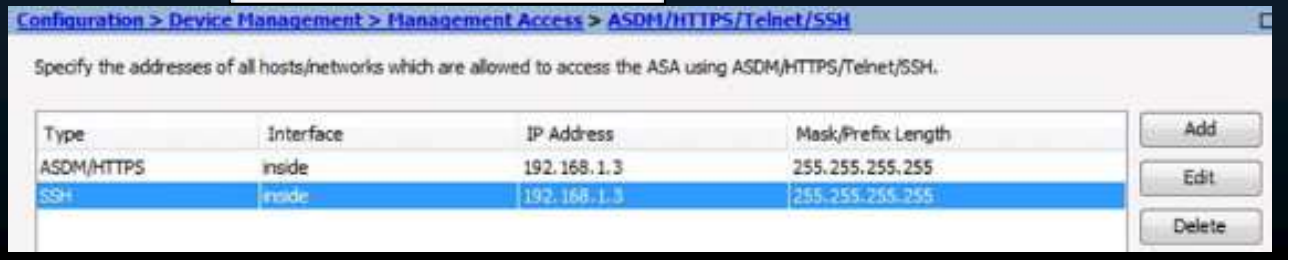
    - Add
      - Establecer parámetros de la ruta.
      - Click en Ok
    - Mostrará vista actualizada.
    - Click en Apply.

10.1 ASDM.

- Configuración de Acceso de Administración.
  - Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH.
    - Identificar Hosts para acceso al ASA.
    - Vgr; Habilitar 192.168.1.3 para acceso por SSH.
      - Add
        - Introducir datos del host.
        - Click en Ok.
      - Tras mostrar cambios.
      - Aplicar

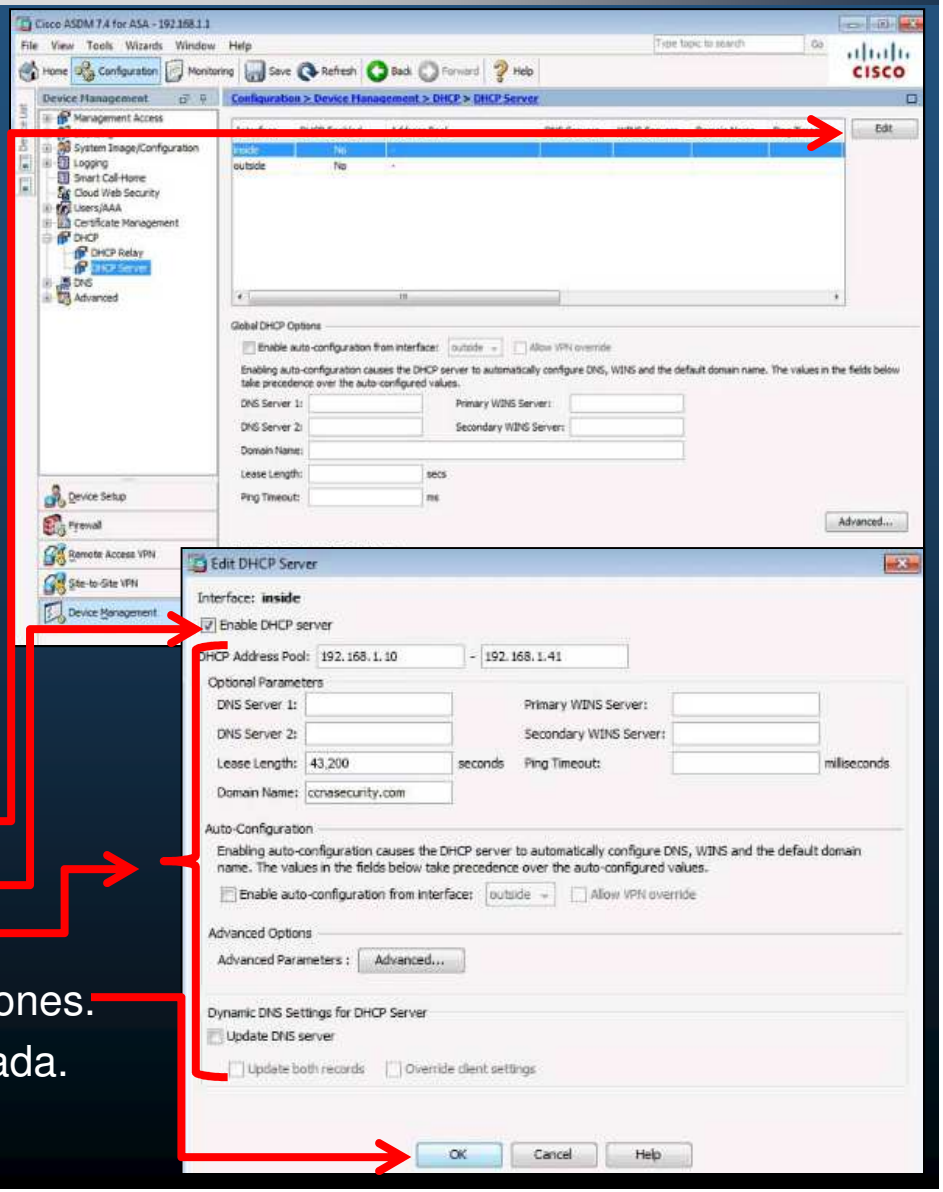






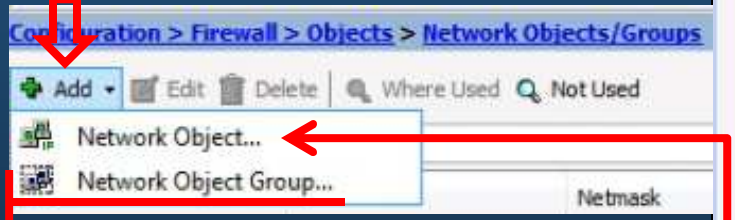
10.1 ASDM.

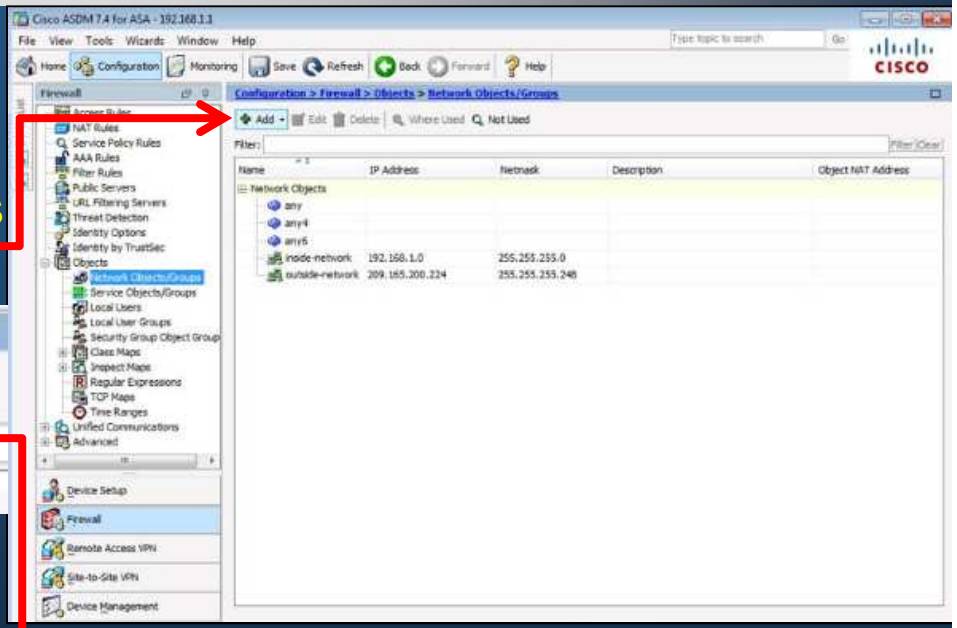
- Configurar Servicios DHCP en ASDM.
  - Configuration > Device Management > DHCP > DHCP Server.
    - Editar configuración DHCP para inside / outside.
    - Vgr; Servidor DHCP para inside Pool de 192.168.1.10 – 41 por 12 horas.
      - Elegir inside.
      - Edit.
        - Habilitar DHCP.
        - Entrar configuraciones.
        - Ok para aceptar configuraciones.
      - Mostrará configuración actualizada.
      - Aplicar.

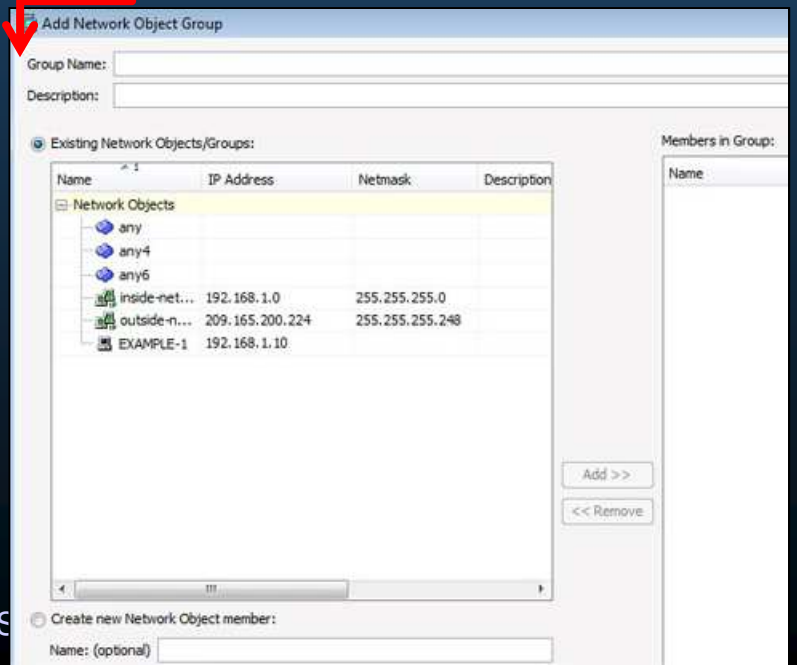


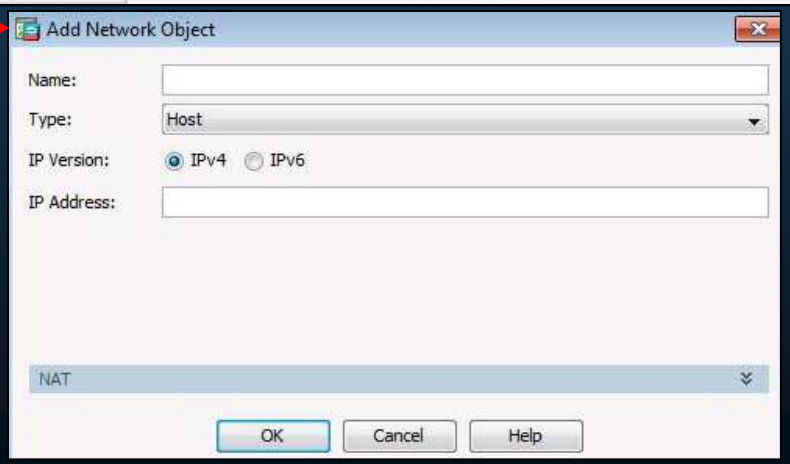
10.1 ASDM.

- Objetos Network en ASDM.
  - Configuration > Firewall > Objects > Network Objects/Groups
    - Add / Edit / Delete



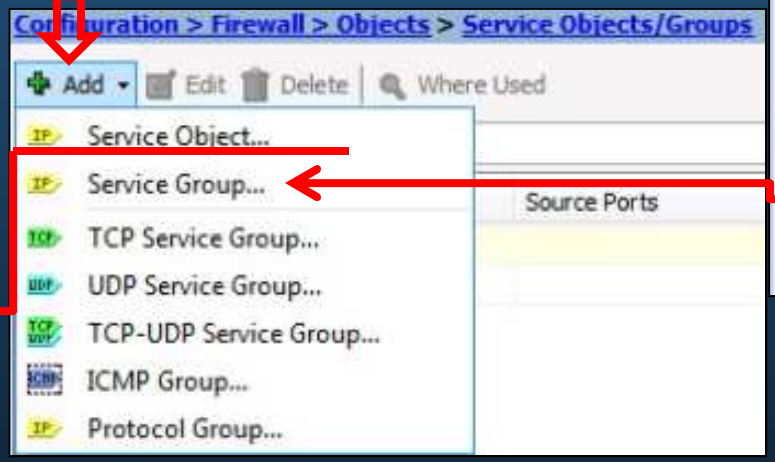


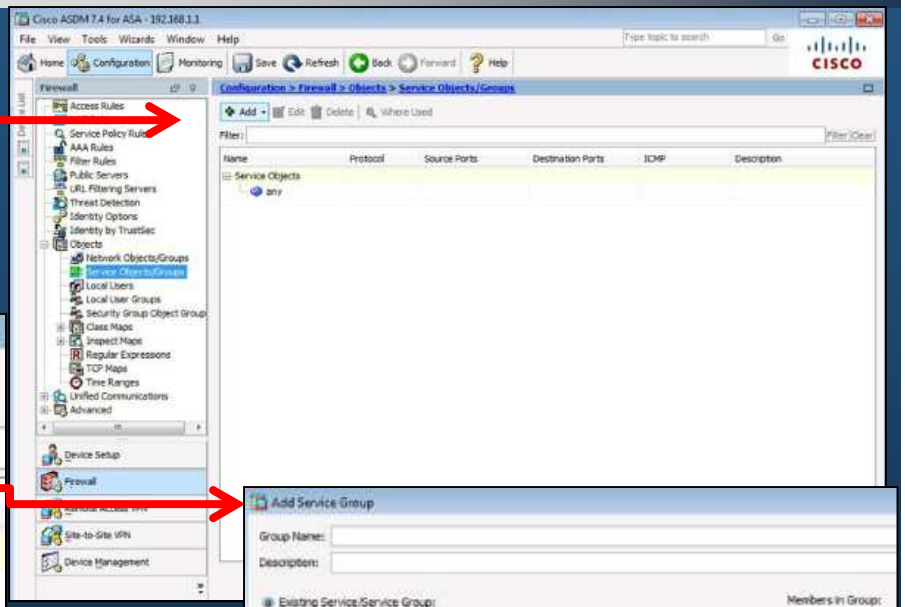


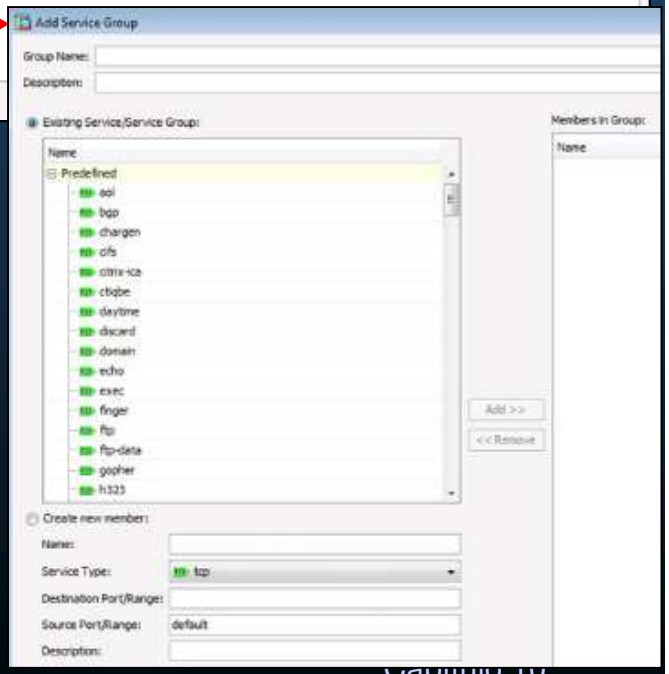


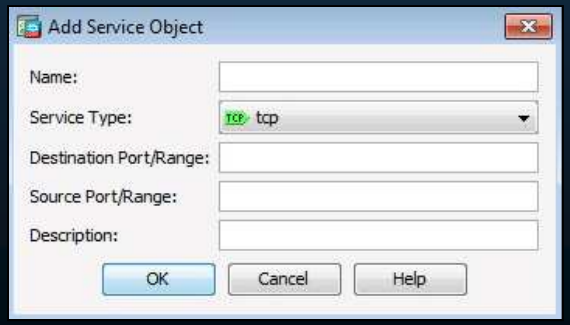
10.1 ASDM.

- Objetos Service en ASDM.
  - Configuration > Firewall > Objects > Service Objects/Groups.
    - Add / Edit / Delete



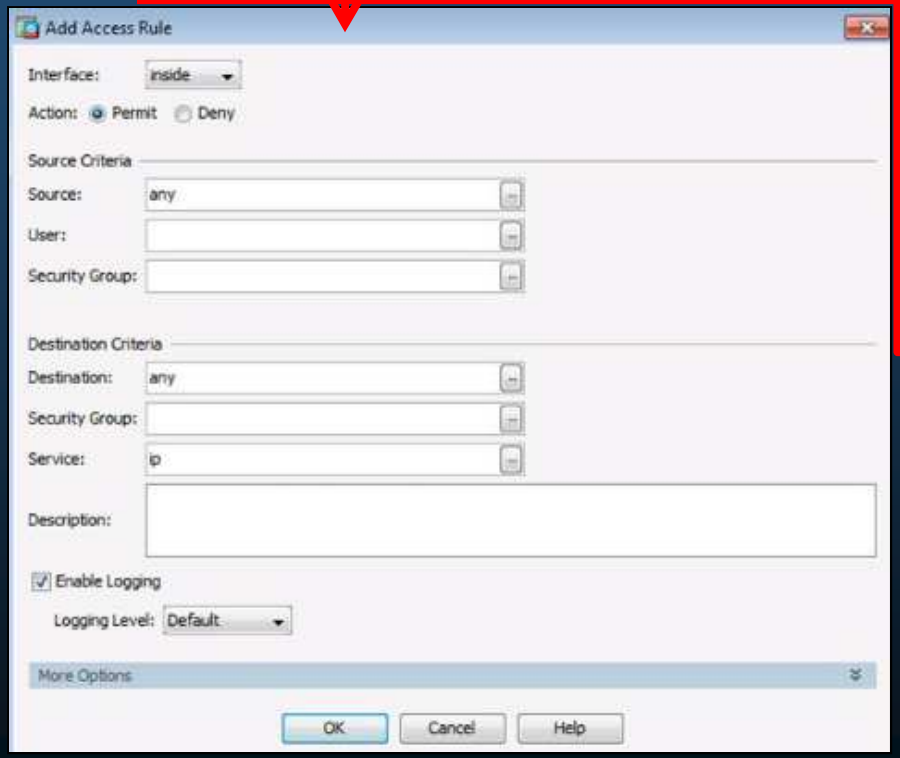


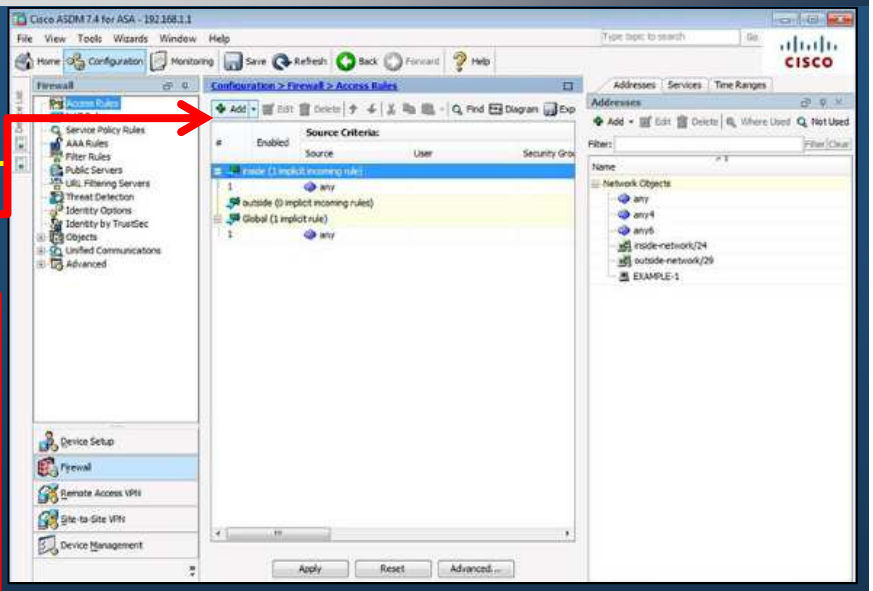


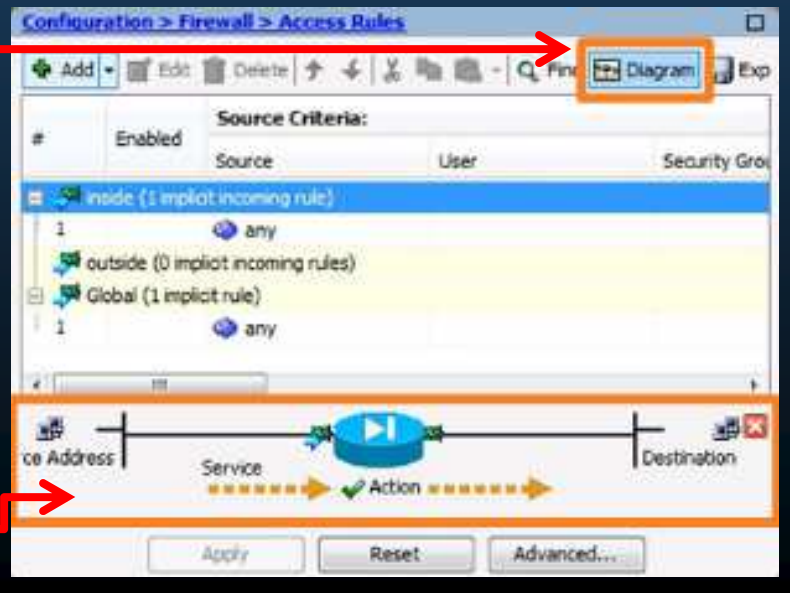


10.1 ASDM.

- ACLs en ASDM.
  - Configuration > Firewall > Access Rules.
    - Ver / Añadir / Editar / Eliminar /… / Diagramar reglas.



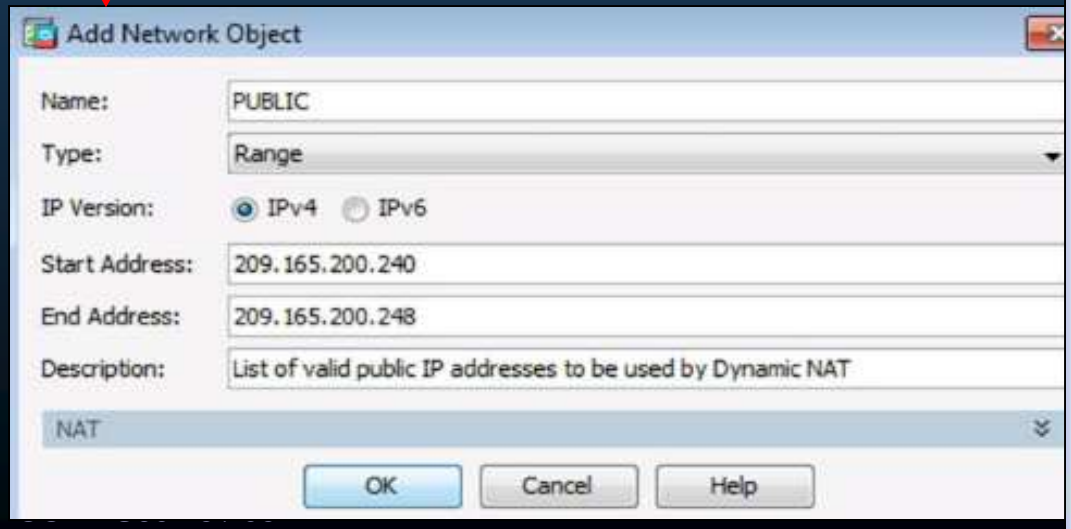


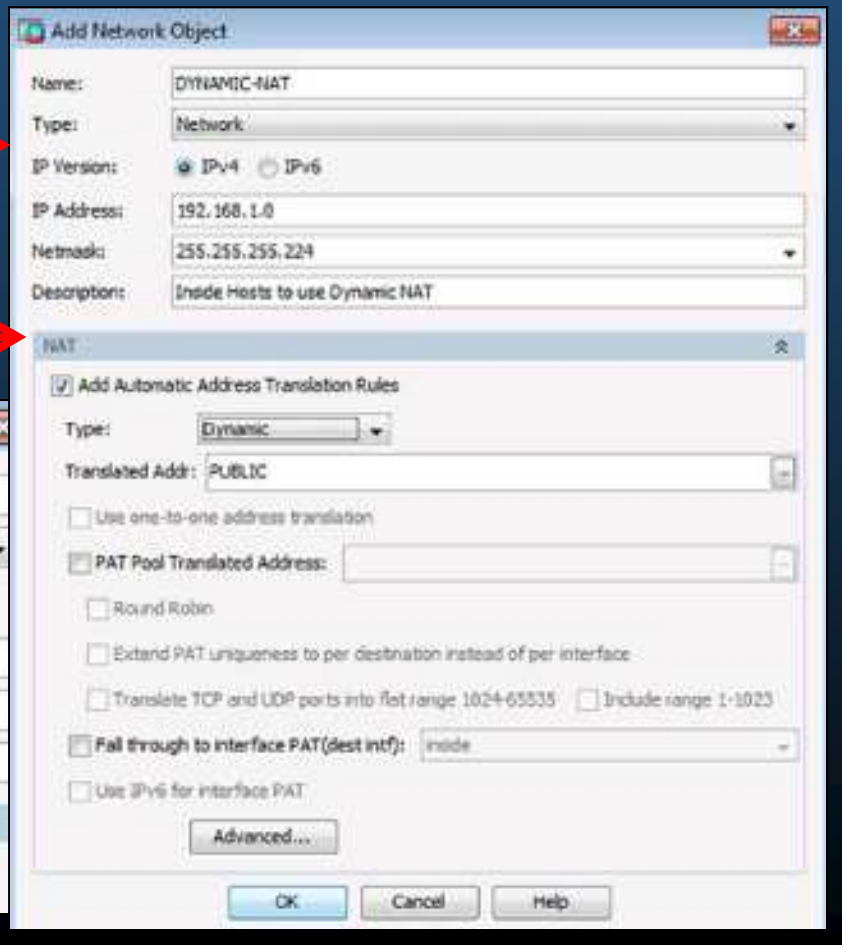


  - Diagrama muestra ayuda visual para entender y diagnosticar problemas.

10.1 ASDM.

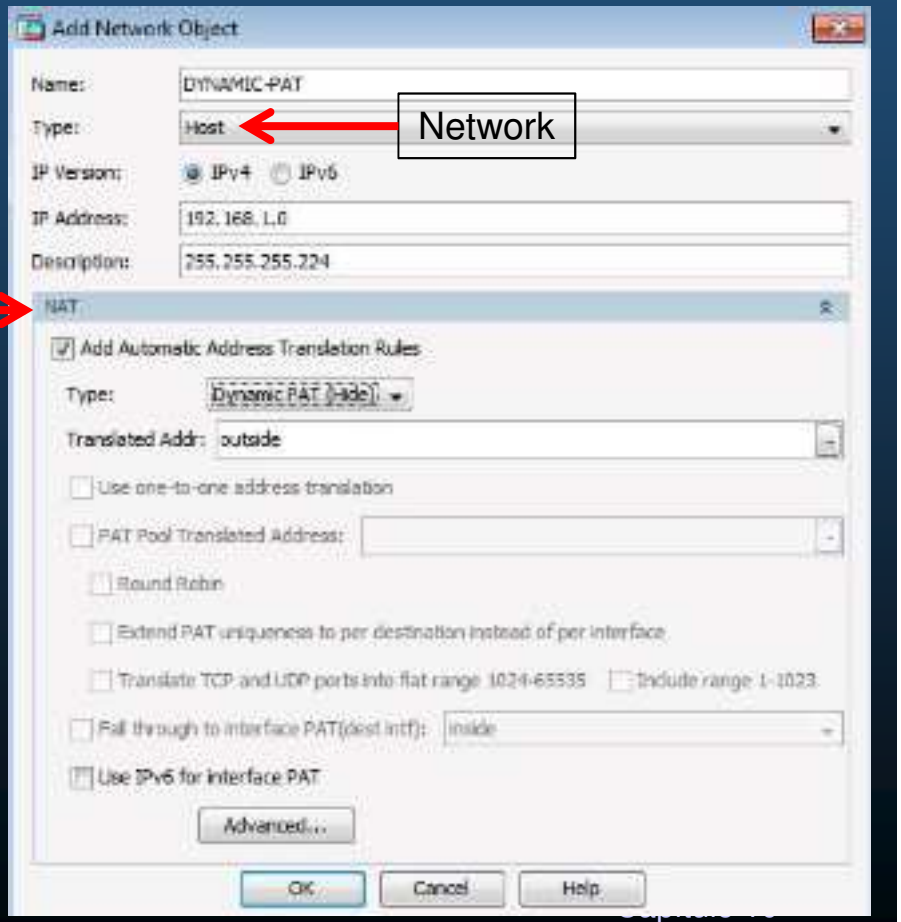
- NAT Dinámico en ASDM.
  - Dos Objetos Network.
    - Configurations > Firewall > Objects > Network Objects/Groups > Add > Network Object.
    - Objeto 1: Identifica el rango público.
    - Objeto 2: Identifica las direcciones internas y el método de traducción. (Click en NAT)





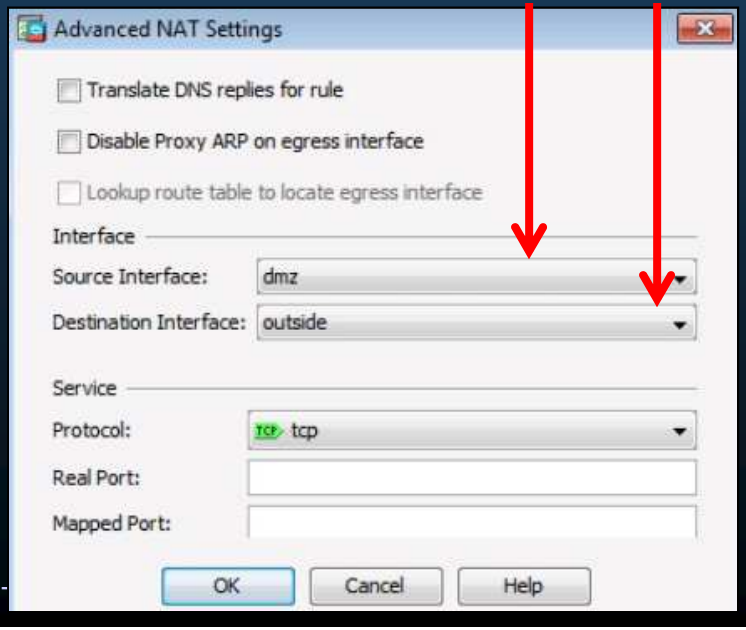
10.1 ASDM.

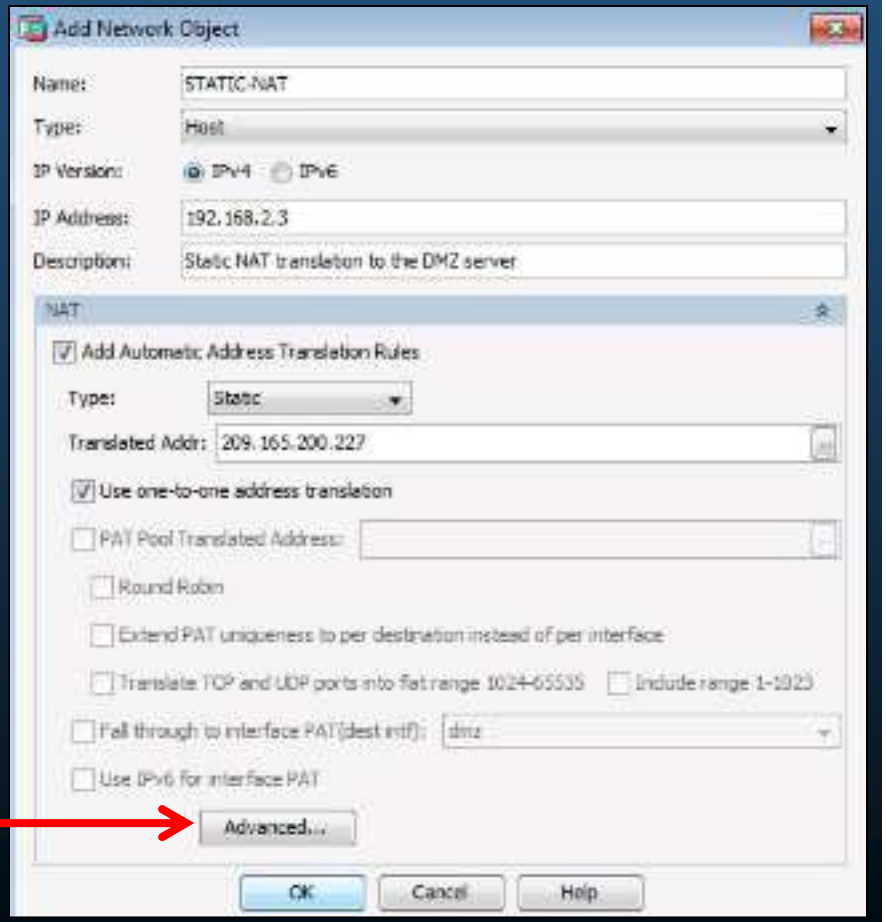
- PAT Dinámico en ASDM.
  - Objeto de Red que asocia direcciones internas a la interface externa.
    - Configurations > Firewall > Objects > Network Objects/Groups > Add > Network Object
    - Al Igual que para NAT Dinámico, la sección NAT se despliega haciendo click.
    - Al igual que en cualquier otra configuración, es imperativo dar click en OK para guardar los cambios.



10.1 ASDM.

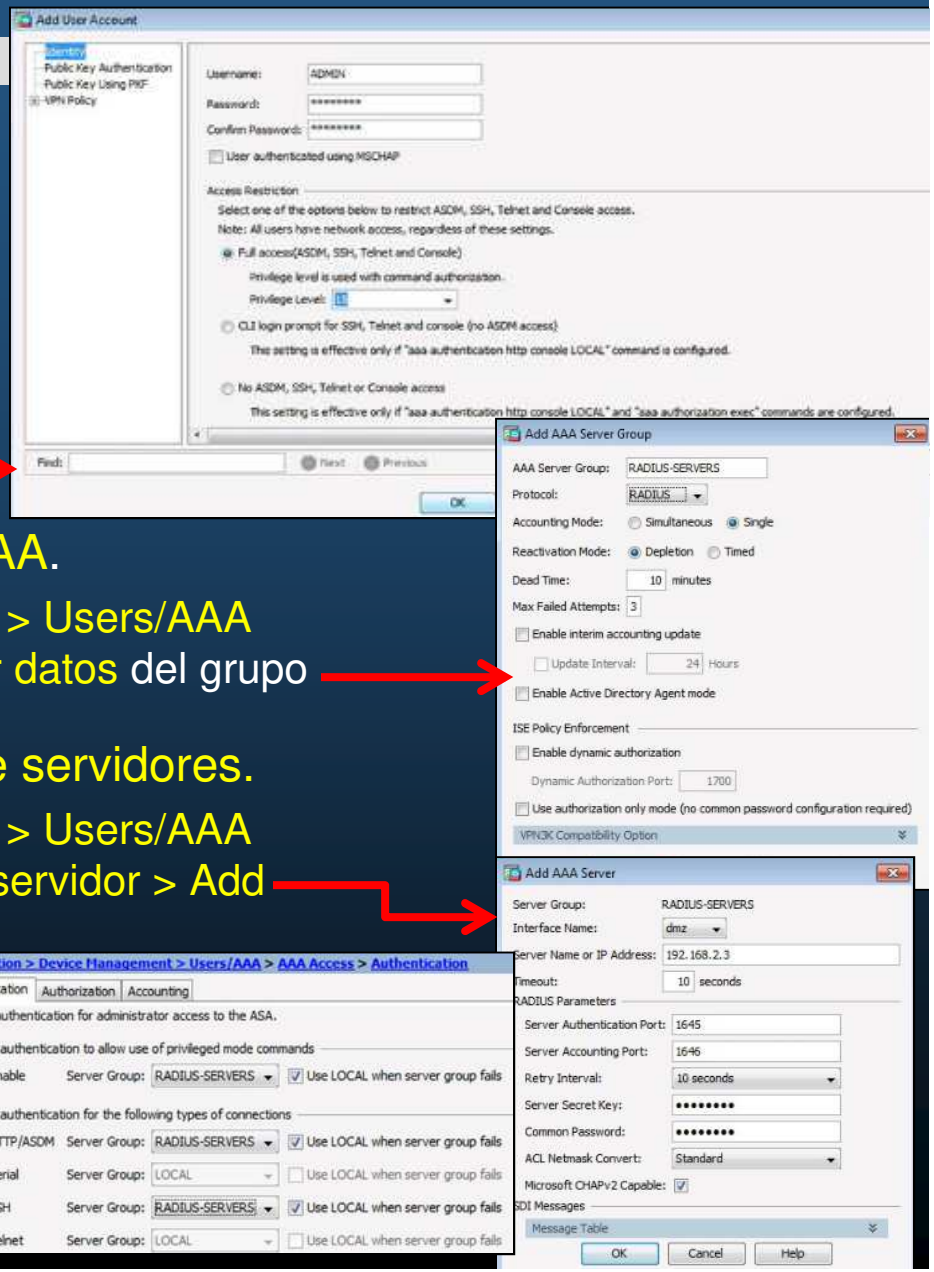
- NAT Estático en ASDM.
  - Objeto Network que asocia una dirección interna a una dirección externa.
    - Configurations > Firewall > Objects > Network Objects/Groups > Add > Network Object.
    - Llenar Información y Click en Advanced.
    - Identificar Interfaces Origen y Destino.





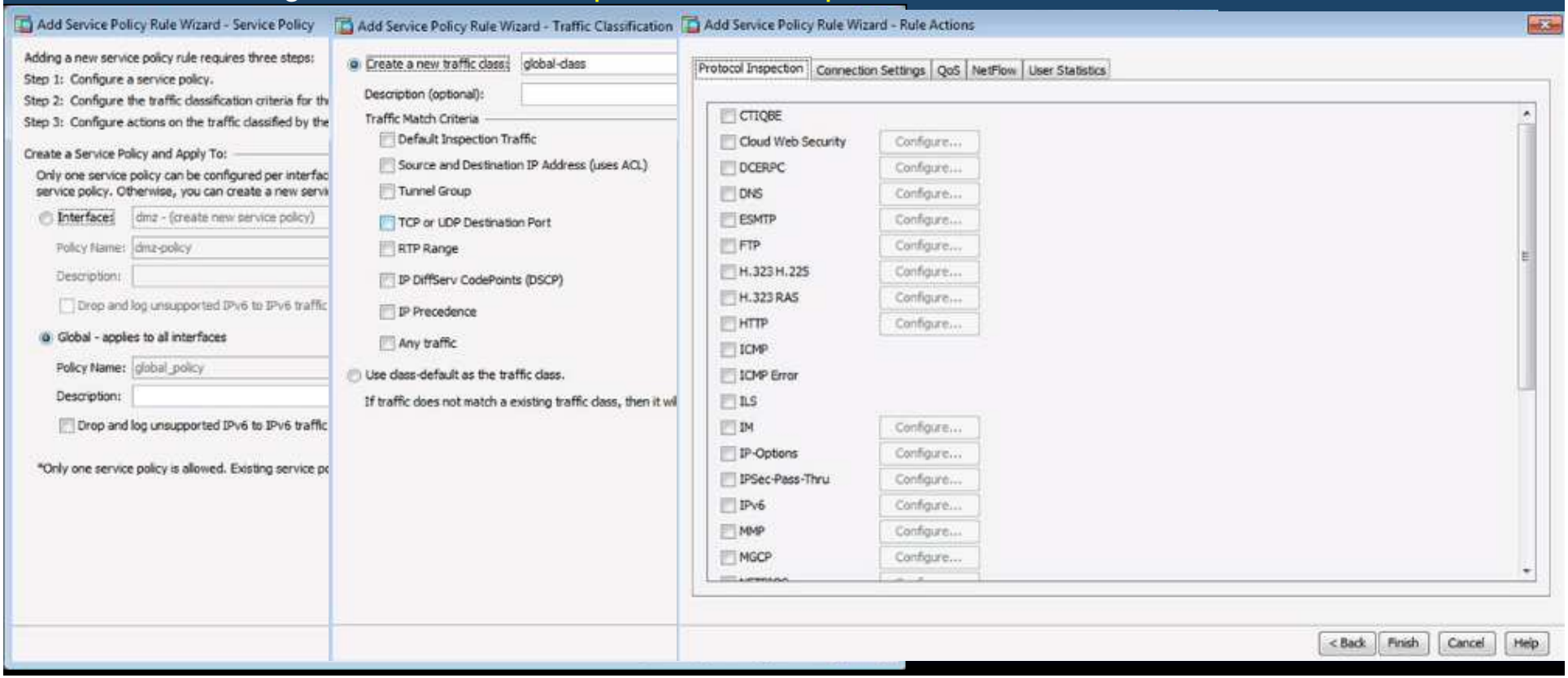
10.1 ASDM.

- Configurar AAA en ASDM.
  - Paso 1. Configurar cuentas de usuarios locales.
    - Configuration > Device Management > Users/AAA > User Accounts > Add
    - > Entrar datos para crear usuario.
  - Paso 2. Crear grupo de servidores AAA.
    - Configuration > Device Management > Users/AAA > AAA Server Groups > Add > Entrar datos del grupo
  - Paso 3. Añadir servidores al grupo de servidores.
    - Configuration > Device Management > Users/AAA > AAA Server Groups > seleccionar servidor > Add > Completar datos
  - Paso 4. Configurar autenticación AAA.
    - Configuration > Device Management > Users/AAA > AAA Access



10.1 ASDM.

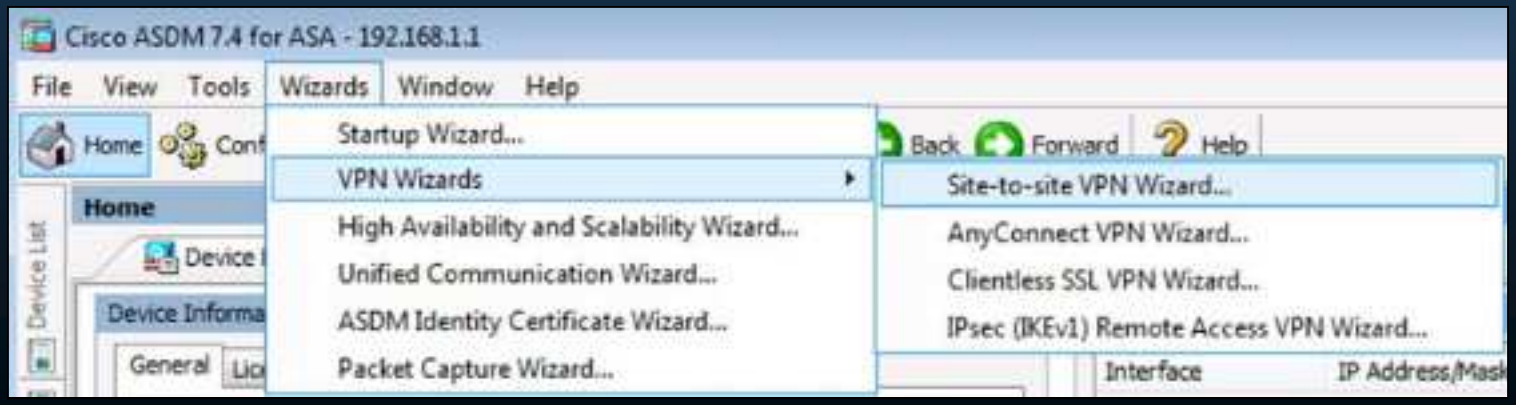
- Configurar Servidor de Políticas con ASDM.
  - Abrir Asistente: Configuration > Firewall > Service Policy Rules > Add.
    - Página 1: Indicar a donde se aplicarán las políticas.
    - Página 2: Identificar el tráfico a coincidir.
    - Página 3: Identificar específicos de la política.



10.2 Configuración VPN en ASA.

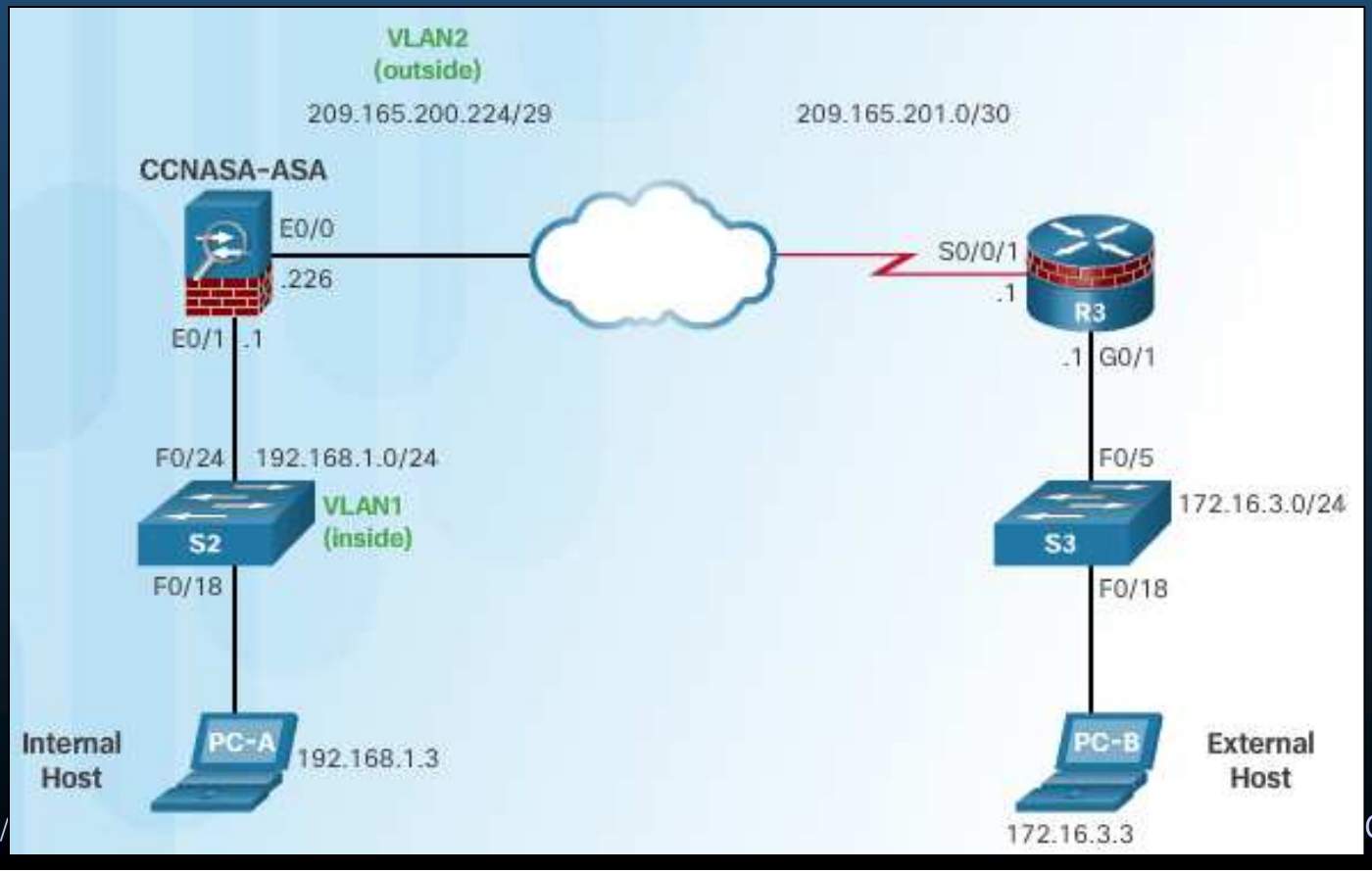
- Soporte para VPNs Sitio a Sitio en ASA.
  - VPNs Sitio a Sitio: Conexión LAN a LAN segura.
  - VPNs de Acceso Remoto: Conexión Usuario a LAN segura.

  - ASDM ofrece 4 asistentes para VPNs
    - Asistente para VPN Sitio a Sitio.
    - Asistente para VPN AnyConnect.
    - Asistente para VPN SSL Sin Cliente.
    - Asistente para VPN de Acceso Remoto IPSec (IKEv1)



10.2 Configuración VPN en ASA.

- VPN Sitio-a-Sitio en ASA con ASDM.
  - Ejemplo Didáctico: VPN sitio a sitio entre ASA y Router ISR (R3).
    - ISR inside: 172.16.3.0/24 / outside: 209.165.201.0/30
    - ASA inside (SL 100): 192.168.1.0/24 / outside (SL 0):209.165.200.224/29 + PAT.



10.2 Configuración VPN en ASA.

- Configuración del Router ISR para VPN Sitio a Sitio.

```
R3(config)# interface GigabitEthernet0/1
R3(config-if)# description R3 LAN
R3(config-if)# ip address 172.16.3.1 255.255.255.0
R3(config-if)# exit
R3(config)#
R3(config)# interface Serial0/0/1
R3(config-if)# description WAN Connected to the Internet
R3(config-if)# ip address 209.165.201.1 255.255.255.252
R3(config-if)# exit
R3(config)#
R3(config)# ip route 0.0.0.0 0.0.0.0 S0/0/1
```

0. Configuración Básica

```
R3(config)# crypto isakmp policy 10
R3(config-isakmp)# encryption 3des
R3(config-isakmp)# hash sha
R3(config-isakmp)# group 2
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)#
R3(config-isakmp)# crypto isakmp key SECRET-KEY address 209.165.200.226
```

1. Política ISAKMP para IKEv1 Cifrado 3DES; Hashing SHA; DH grupo 2 (1024 bits), Autenticación de llave pre-compartida "SECRET-KEY" con el par: 209.165.200.226

```
R3(config)# crypto ipsec transform-set ESP-TUNNEL esp-3des esp-sha-hmac
R3(cfg-crypto-trans)# mode tunnel
R3(cfg-crypto-trans)# exit
R3(config)#
R3(config)# ip access-list extended VPN-ACL
R3(config-ext-nacl)# remark VPN ACL defining interesting traffic
R3(config-ext-nacl)# permit ip 172.16.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R3(config-ext-nacl)# exit
R3(config)#
```

2. Política IPSec para IKE Fase 2

3. ACL para tráfico Interesante: de R3 interna a ASA interna

```
R3(config)# crypto map S2S-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R3(config-crypto-map)# set peer 209.165.200.226
R3(config-crypto-map)# set transform-set ESP-TUNNEL
R3(config-crypto-map)# match address VPN-ACL
R3(config-crypto-map)# exit
R3(config)#
R3(config)# interface Serial0/0/1
R3(config-if)# crypto map S2S-MAP
R3(config-if)#
```

4. Configura mapa criptográfico para la política IPSec y Define tráfico interesante (ACL).

5. Aplica Criptomapa a la interface de salida.

10.2 Configuración VPN en ASA.

- Configuración de VPN Sitio-a-Sitio en ASA con ASDM.

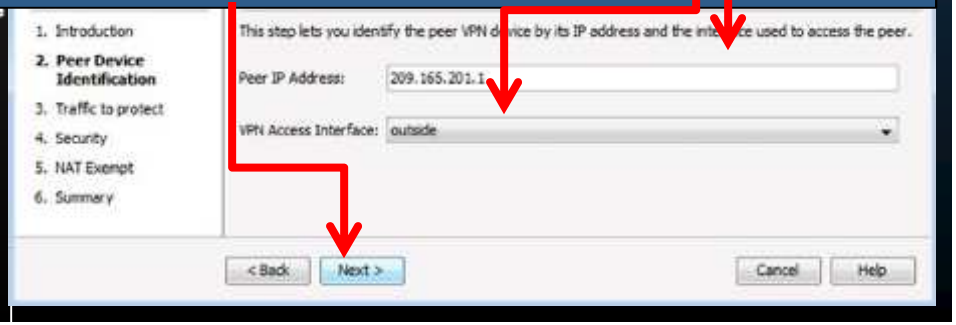
0. Configuración Básica

```
CNAS-ASA(config)# enable password class
CCNAS-ASA(config)#
CCNAS-ASA(config)# interface vlan 1
CCNAS-ASA(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
CCNAS-ASA(config-if)# ip address 192.168.1.1 255.255.255.0
CCNAS-ASA(config-if)#
CCNAS-ASA(config-if)# interface e0/1
CCNAS-ASA(config-if)# switchport access vlan 1
CCNAS-ASA(config-if)# no shut
CCNAS-ASA(config-if)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# interface vlan 2
CCNAS-ASA(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.
CCNAS-ASA(config-if)# ip address 209.165.200.226 255.255.255.224
CCNAS-ASA(config-if)#
CCNAS-ASA(config-if)# interface e0/0
CCNAS-ASA(config-if)# switchport access vlan 2
CCNAS-ASA(config-if)# no shut
CCNAS-ASA(config-if)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# route outside 0.0.0.0 0.0.0.0 209.165.200.225
CCNAS-ASA(config)#
CCNAS-ASA(config)# object network INSIDE-NET
CCNAS-ASA(config-network-object)# subnet 192.168.1.0 255.255.255.0
CCNAS-ASA(config-network-object)# nat (inside,outside) dynamic interface
CCNAS-ASA(config-network-object)#
CCNAS-ASA(config-network-object)# policy-map global_policy
CCNAS-ASA(config-pmap)# class inspection_default
CCNAS-ASA(config-pmap-c)# inspect icmp
CCNAS-ASA(config-pmap-c)# exit
CCNAS-ASA(config-pmap)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# http server enable
CCNAS-ASA(config)# http 192.168.1.0 255.255.255.0 inside
CCNAS-ASA(config)#
```

1. Wizards > VPN Wizards > Site-to-Site VPN Wizard

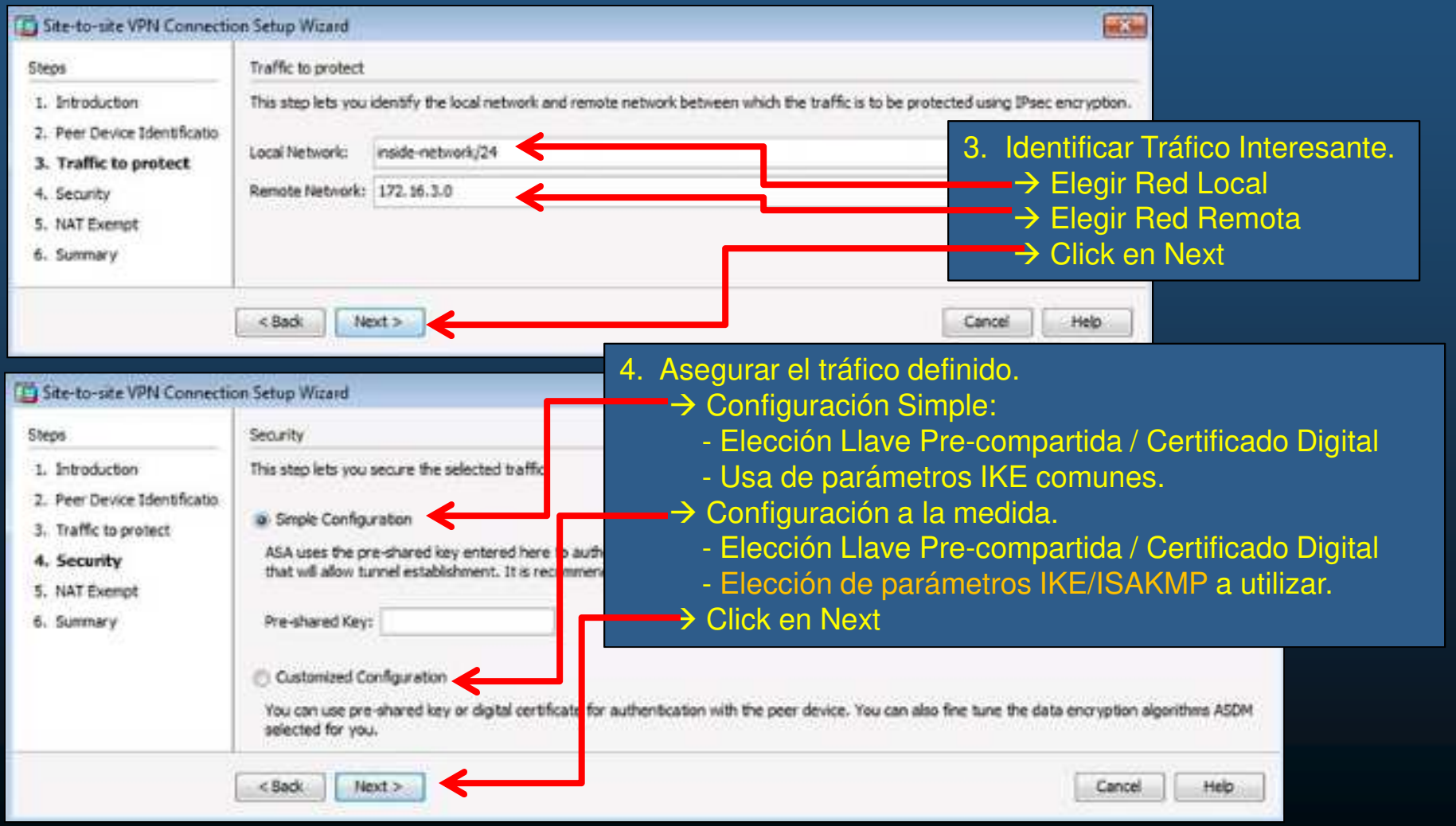
   → Click en Next

2. Identificar el dispositivo par.
   → Ingresar IP alcanzable del dispositivo par.
   → Identificar interfaces para acceder al par. (para aplicar el criptomapa)
   → Clic en Next.



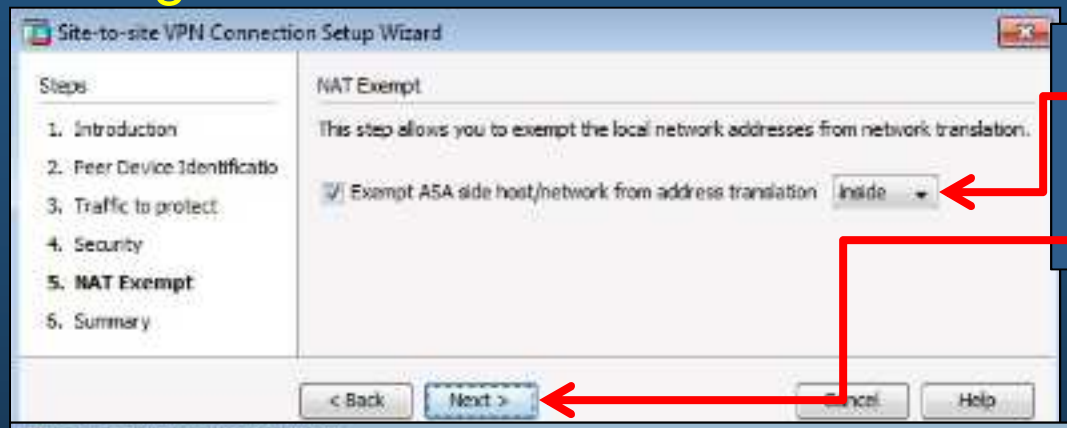
10.2 Configuración VPN en ASA.

- Configuración de VPN Sitio-a-Sitio en ASA con ASDM (Cont.).

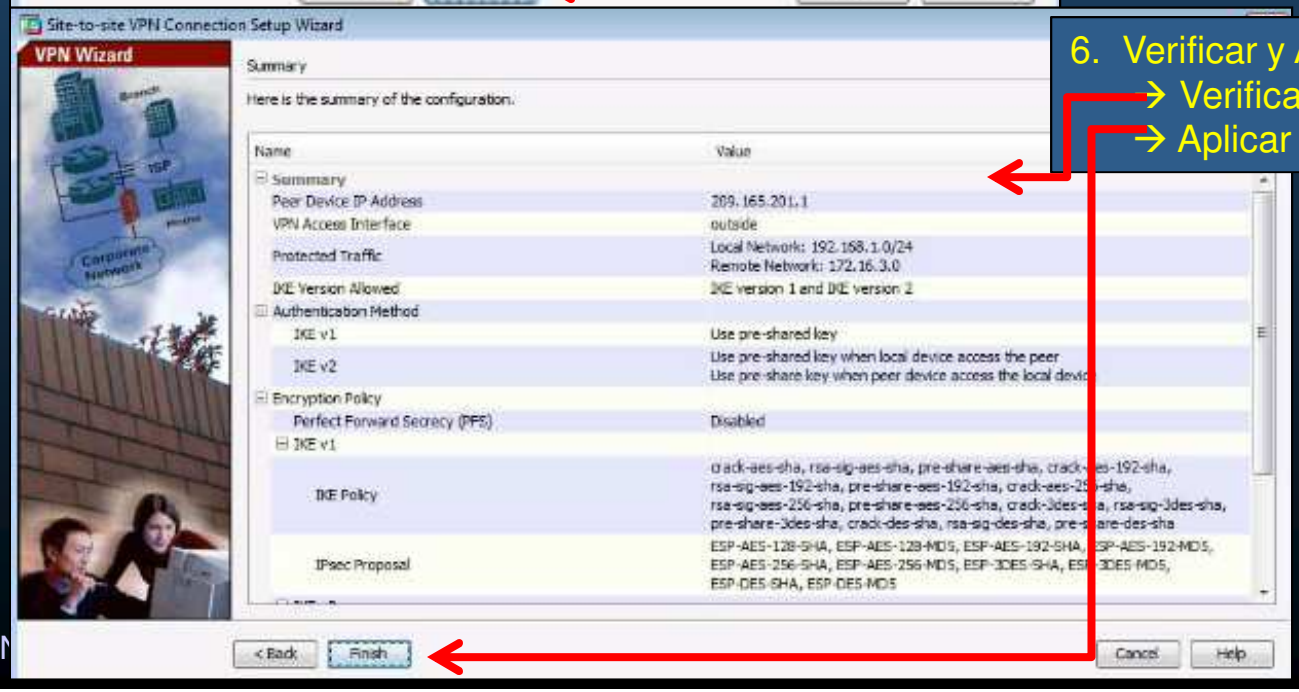


10.2 Configuración VPN en ASA.

- Configuración de VPN Sitio-a-Sitio en ASA con ASDM (Cont.).



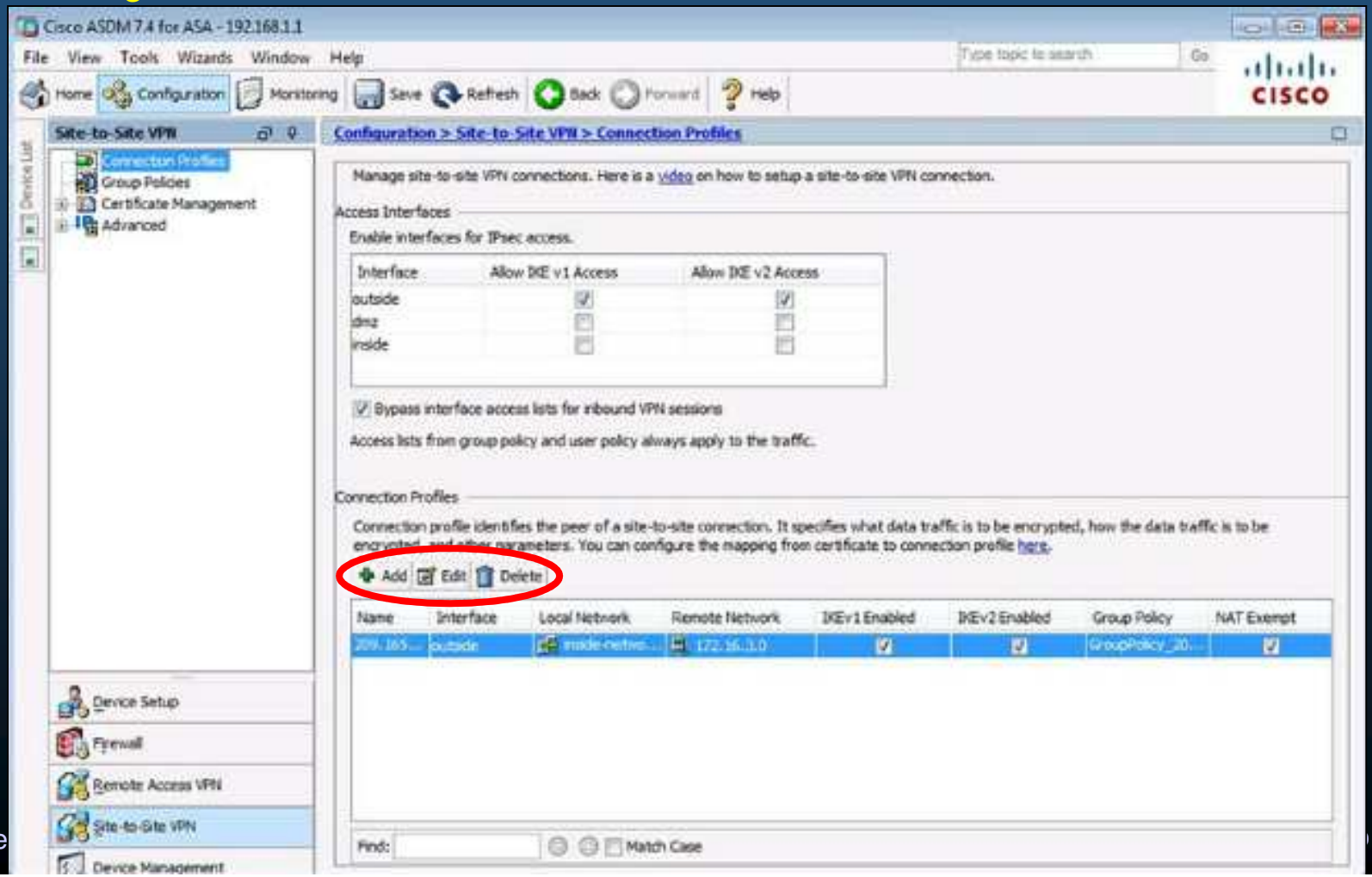
5. Identificar si NAT debe ser dispensado.
   → Elegir Si hosts internos serán accesibles con sus Ips reales.
   → Típicamente seleccionado
   → Click en Next



6. Verificar y Aplicar configuración.
   → Verificar Resumen.
   → Aplicar configuración con Finish.

10.2 Configuración VPN en ASA.

- Verificación de VPNs Sitio-a-Sitio mediante ASDM.
  - Configuration > Site-to-Site VPN > Connection Profiles.



10.2 Configuración VPN en ASA.

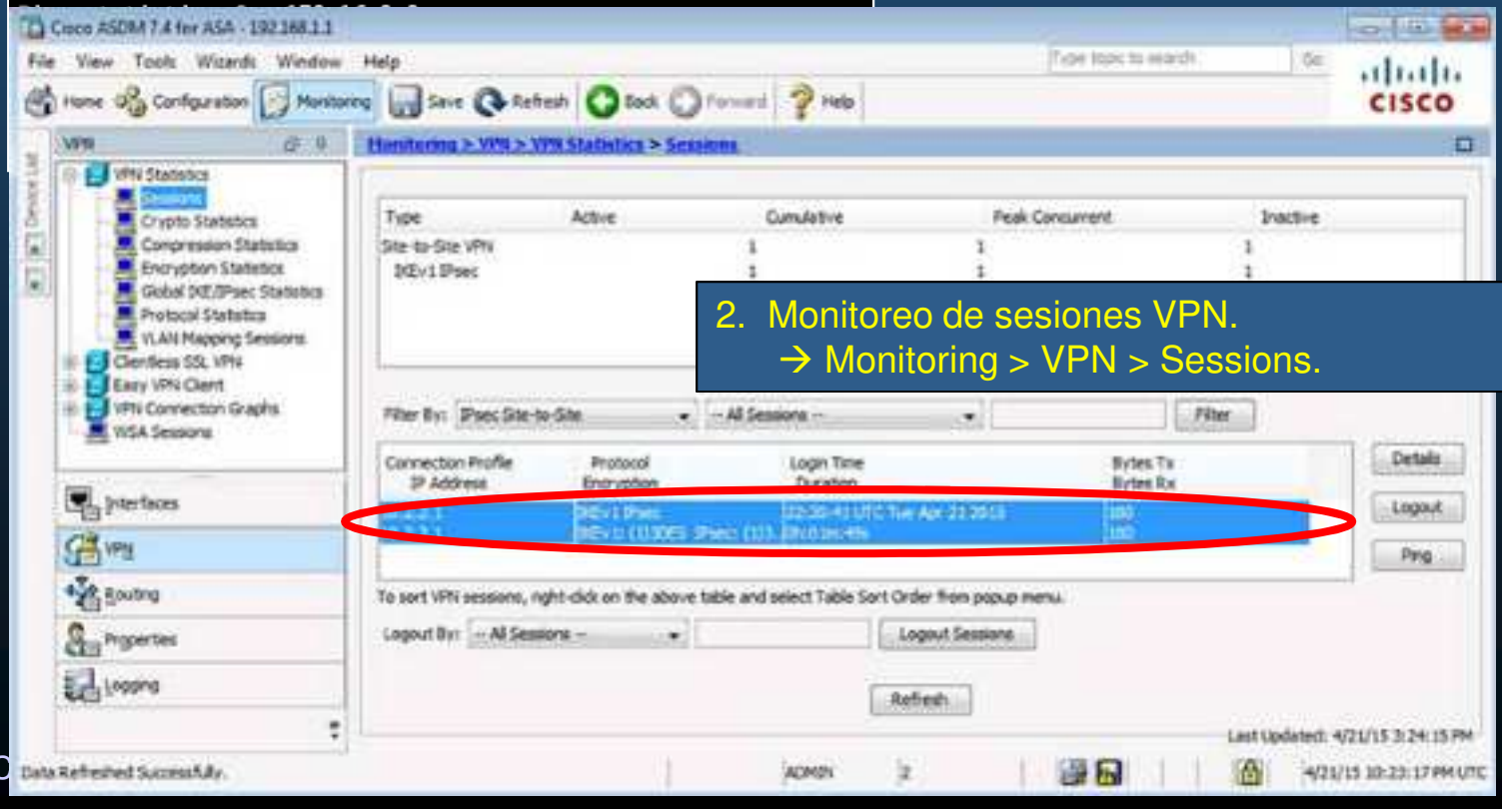
- Prueba de VPNs Sitio-a-Sitio mediante ASDM.

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\NetAcad> ping 172.16.3.3

Pinging 172.16.3.3 with 32 bytes of data:
Request timed out.
Reply from 172.16.3.3: bytes=32 time=64ms TTL=127
Reply from 172.16.3.3: bytes=32 time=63ms TTL=127
Reply from 172.16.3.3: bytes=32 time=71ms TTL=127
```

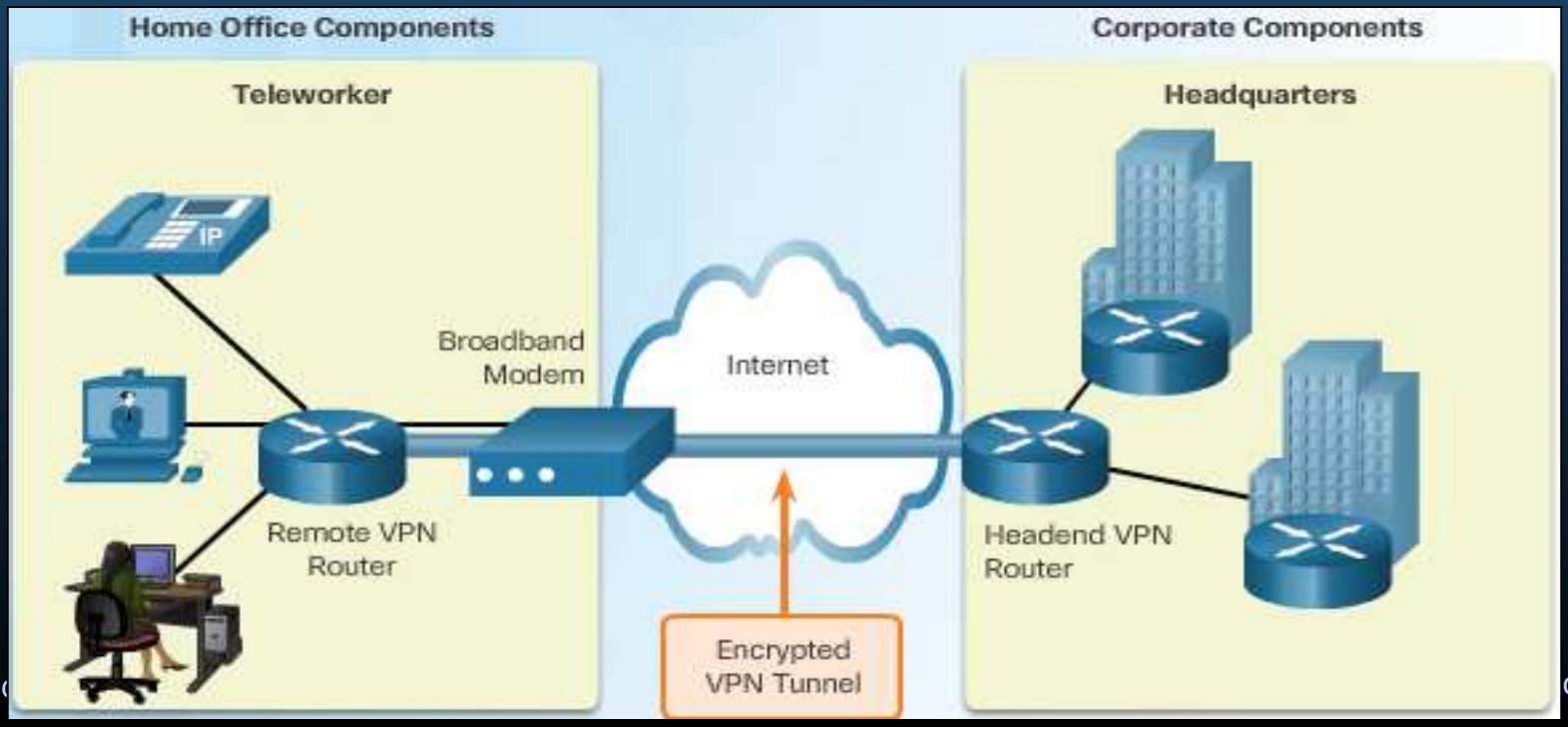
1. Verificar conectividad capa 3.
   → El primer ping puede fallar por el tiempo que tarda en establecerse el tunel.
   → Que un ping conteste no implica que exista un tunel.



2. Monitoreo de sesiones VPN.
   → Monitoring > VPN > Sessions.

10.2 Configuración VPN en ASA.

- Opciones para VPNs de Acceso Remoto en ASA.
  - Teletrabajo = Flexibilidad de horario y localidad.
    - Ahorra costos a las empresas → Lo ofrecen de manera voluntaria.
  - VPNs habilitan conexiones seguras de trabajadores a sitios corporativos.
    - Extienden la red corporativa e incrementan productividad, reduciendo costos de trasnporte (Trabajadores llevan la oficina consigo).



10.2 Configuración VPN en ASA.

- IPSec vs SSL.

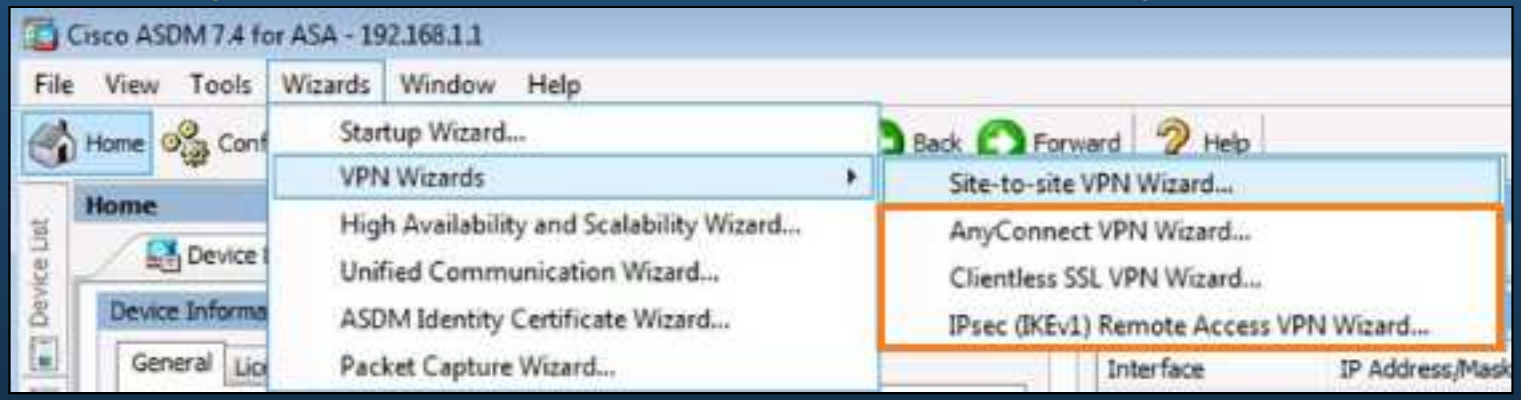
No son excluyentes sino complementarias.

  - Principales tecnologías para VPNs de acceso remoto.
    - IPSec. Solución convencional para accesos remotos por teletrabajadores.
    - SSL. Diseñada (1990s) para habilitar comunicaciones http seguras.
      - 1. El cliente y servidor negocian autenticación, cifrado y llaves.
      - 2. Servidor envía certificado al cliente.
      - 3. Cliente envía certificado al servidor. Establecen sesión y llaves de cifrado.
      - 4. Transferencia de datos con llaves de sesión.

	IPSec	SSL
Aplicaciones Soportadas	**Extensas**. Cualquier aplicación IP.	**Limitadas**. Solo aplicaciones web.
Seguridad de Autenticación	**Fuerte**. Autenticación de dos vías con llaves compartidas o certificados.	**Moderada**. Autenticación de una o dos vías.
Seguridad de Cifrado	**Fuerte**. Longitudes de llave de 56 a 256 bits	Moderado a Fuerte. Longitudes de llave de 40 a 256 bits
Complejidad de Conexión	**Media**. Requiere cliente VPN pre-instalado en el host.	**Baja**. Solo requiere un navegador web.
Opciones de Conexión	**Limitadas**. Solo dispositivos específicos, con configuraciones específicas..	**Extensas**. Cualquier dispositivo con un navegador web.

10.2 Configuración VPN en ASA.

- VPNs SSL mediante ASA
  - Soportadas por ISR y ASA (ASA puede soportar hasta 10,000 conexiones).
    - Tres tipos de soluciones, cada una con un asistente disponible:

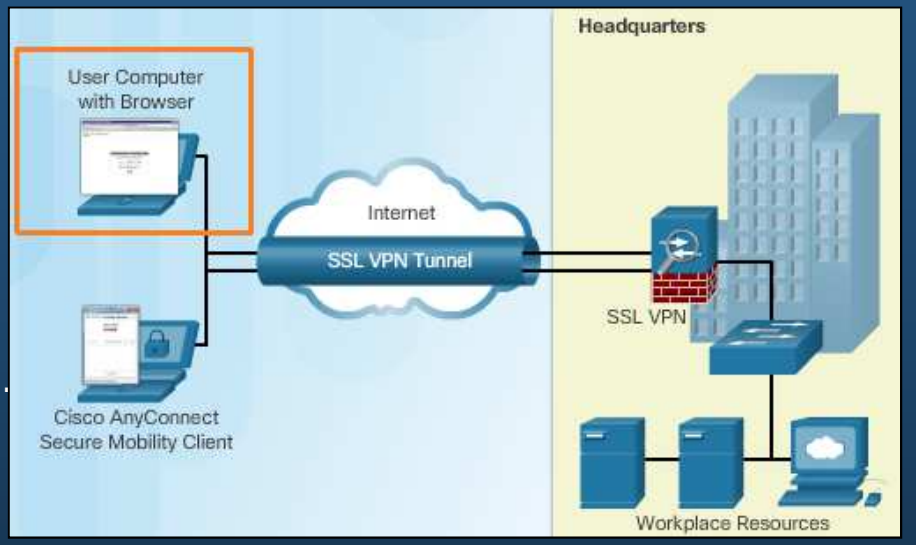


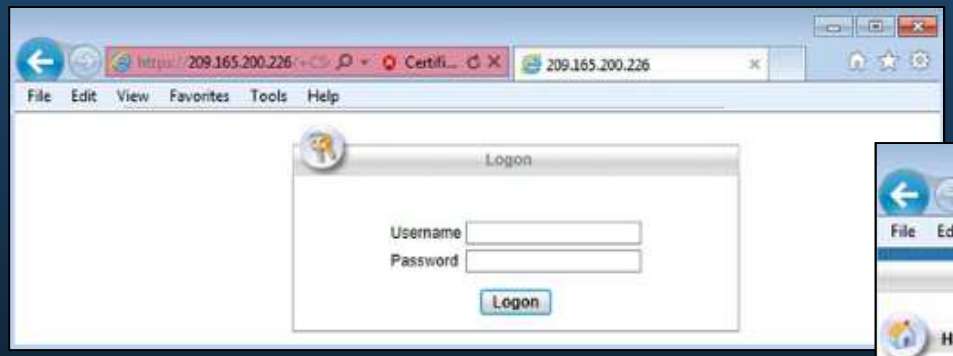
    - Soporte IKEv1 para clientes VPN antiguos
      - Un solo tipo de autenticación/encriptación por política.
      - Cisco VPN Client.
    - Soporte IKEv2 para clientes VPN Nuevos.
      - Múltiples tipos de autenticación/encriptación por política.
      - Cisco Anyconnect Secure Mobility Client

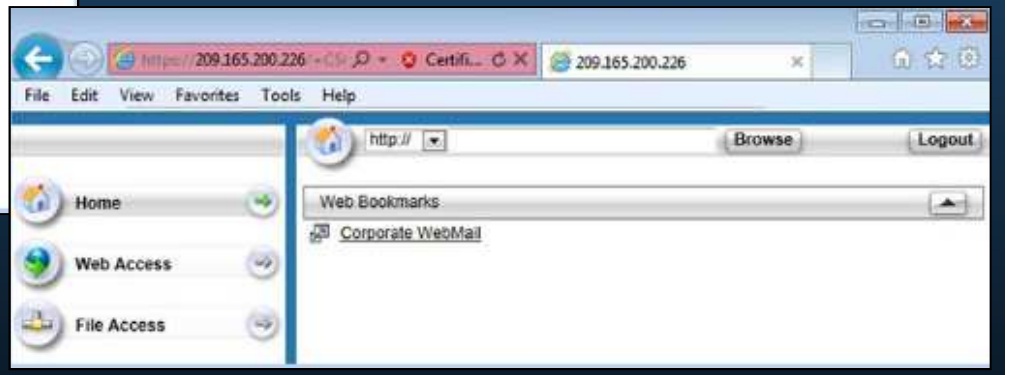
El capítulo se centra en VPNs de Acceso remoto SSL Basadas en Clientes y Sin Clientes

10.2 Configuración VPN en ASA.

- Solución VPN SSL sin Clientes.
  - Busca flexibilidad de proporcionar accesos a recursos corporativos a dispositivos no administrados por la corporación.
    - Un navegador web, establece el túnel.



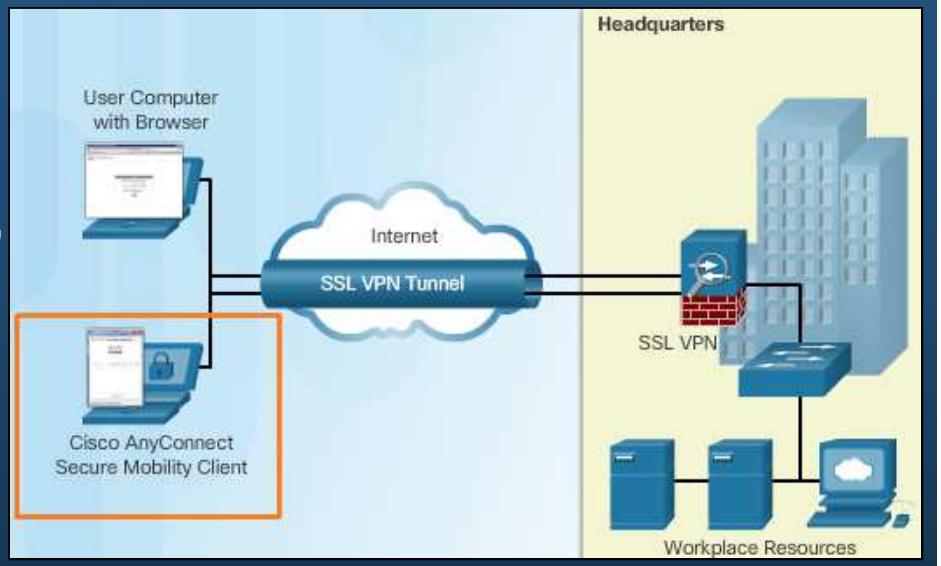




  - Tras autenticarse, los usuarios acceden a recursos internos de la corporación mediante web.
- ASA funge como servidor proxy a los recursos de red y genera el portal web.
- Clientes requieren navegador web con capacidades SSL.
- Fácil de implementar vs Acceso limitado a recursos y Riesgos de Seguridad.

10.2 Configuración VPN en ASA.

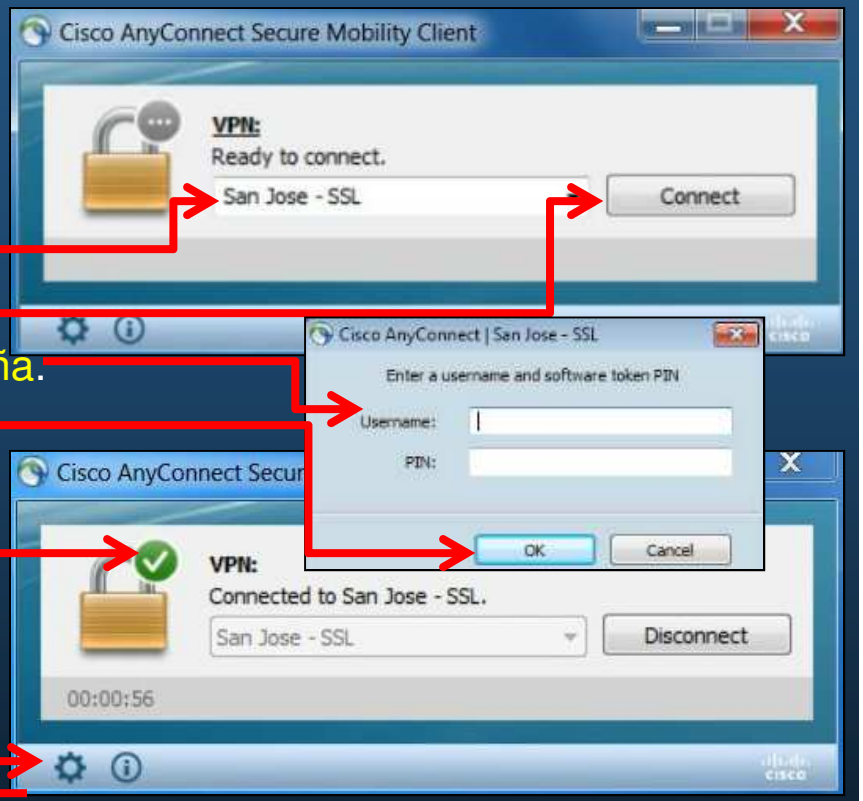
- Solución VPN SSL Basada en Cliente.
  - Proporciona a usuarios autenticados, acceso IP completo a la red corporativa y sus servicios.

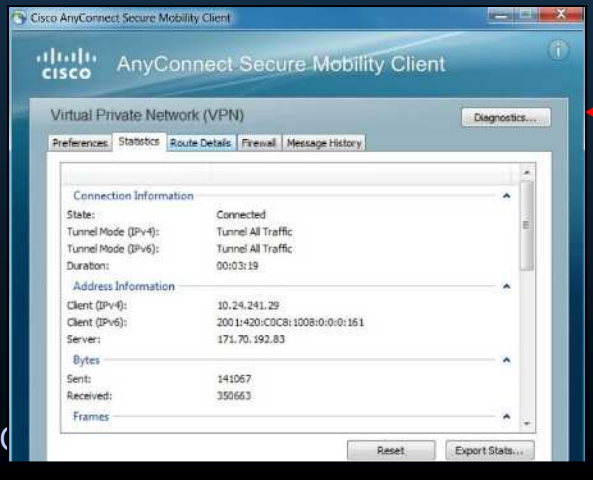


    - Requiere aplicación cliente (Cisco Anyconnect Secure Mobility Client).
      - Puede descargarse Clientless y autoconfigurarse tras instalarse (Windows/Mac/Linux).
      - Instalarlo requiere permisos administrativos.
      - Evaluar el host tras instalarse y antes de autoconfigurarse.
      - Requiere mantenimiento.
      - Dificulta la implementación (No es transparente para el usuario final).
    - Soporta mayor cantidad de aplicaciones.

10.2 Configuración VPN en ASA.

- Cisco AnyConnect Security Client.
  - Pre-Instalado, establece la conexión VPN fácilmente al iniciarlo.
    - Indicar VPN pre-configurada a utilizar:
    - Click en Connect.
    - Ingresar Nombre de Usuario y Contraseña.
    - Click en OK
    - Si las credenciales son válidas mostrará indicador de conexión realizada.
    - Click en el boton de configuraciones, mostrará estadísticas de conexión.





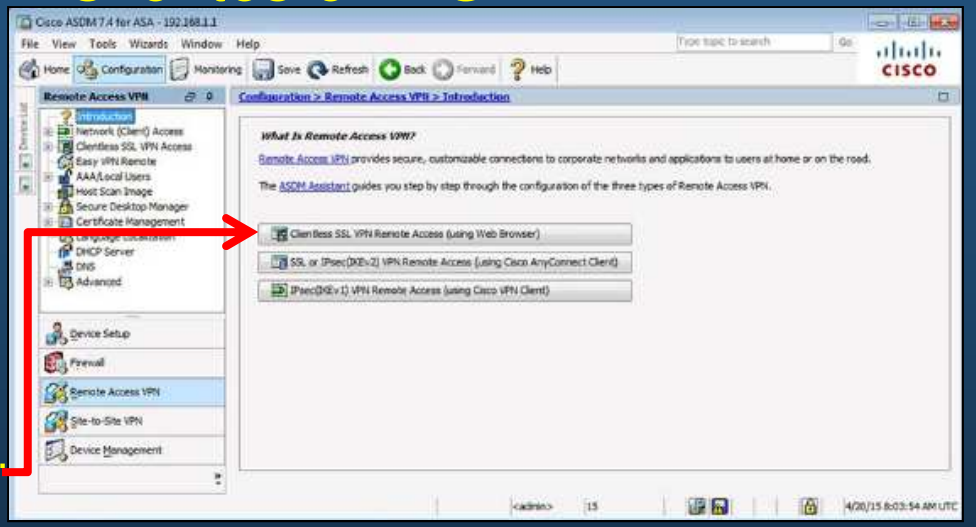
Puede configurarse Anyconnect para:
- Autoconectar a una VPN específica al iniciar equipo, y mantenerse activo hasta que éste se apague.
- Descargarse Clientless y autoconfigurarse tras instalarse (Windows/Mac/Linux)
- Evaluar el host tras instalarse y antes de autoconfigurarse (antivirus/antimalware/firewall instalados y operativos).

10.2 Configuración VPN en ASA.

- AnnyConnet para Equipos Mobiles.
  - Disponible para:
    - iOS (iPhone, iPad, y iPod Touch)
    - Android
    - BlackBerry
    - Windows Mobile
  - Solo disponible para determinados modelos.
  - Incluido como App nativa por algunas marcas.
  - Mas información:
    - http://www.cisco.com/c/en/us/products/security/anyconnect-secure-mobility-client/index.html

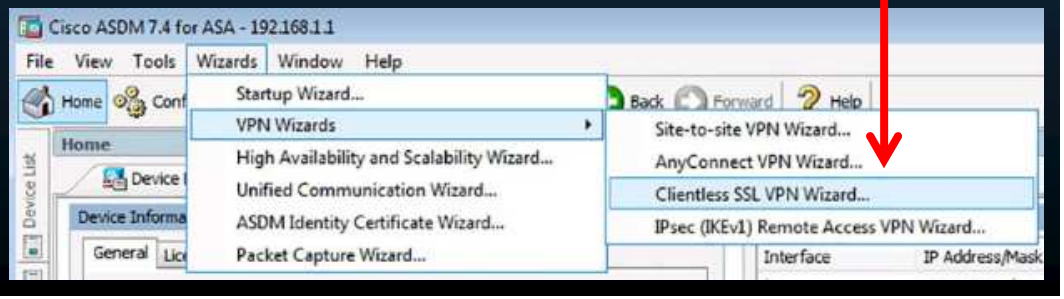
10.2 Configuración VPN en ASA.

- Configuración de VPN SSL Sin Clientes en ASA.
  - Dos Herramientas.
    - Asistente ASDM: Configuración de la VPN SSL.
      - Configurations > Remote Access VPN > Introduction > Clientless SSL VPN Remote Access (using Web Browser).



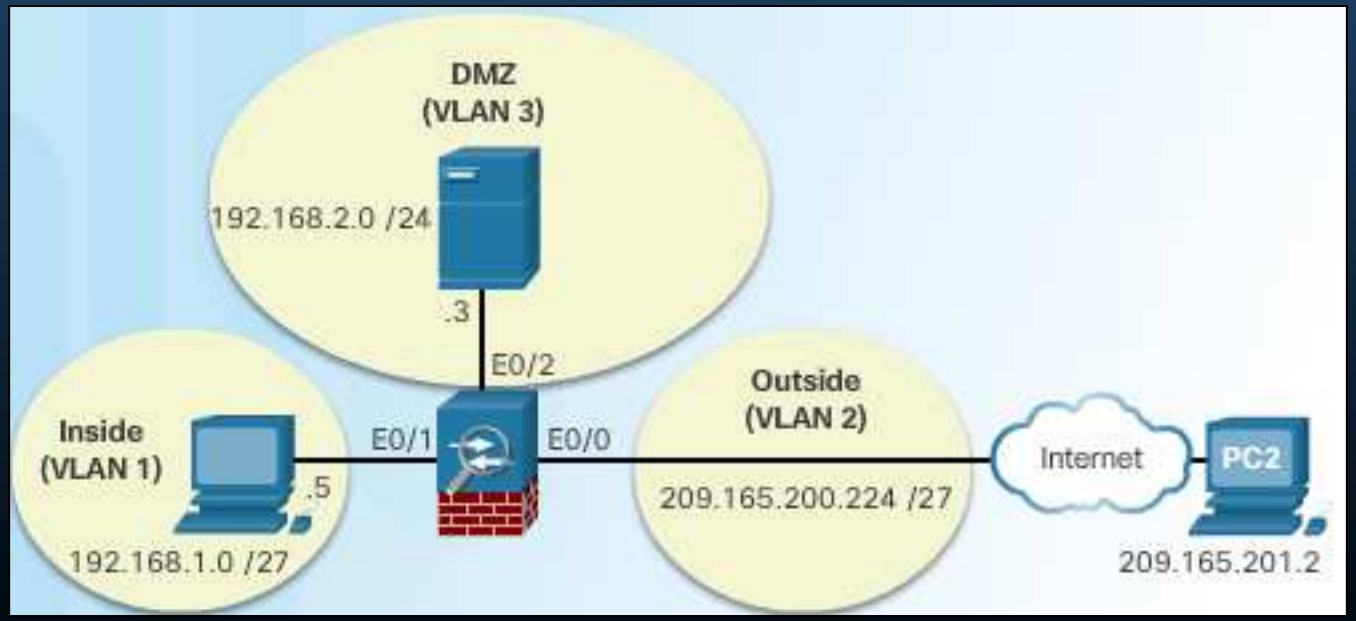
    - Asistente VPN: Simplifica la configuración de la VPN SSL.
      - Wizards > VPN Wizards > Clientless SSL VPN Wizard

  - El curso considera el uso del Asistente VPN.



10.2 Configuración VPN en ASA.

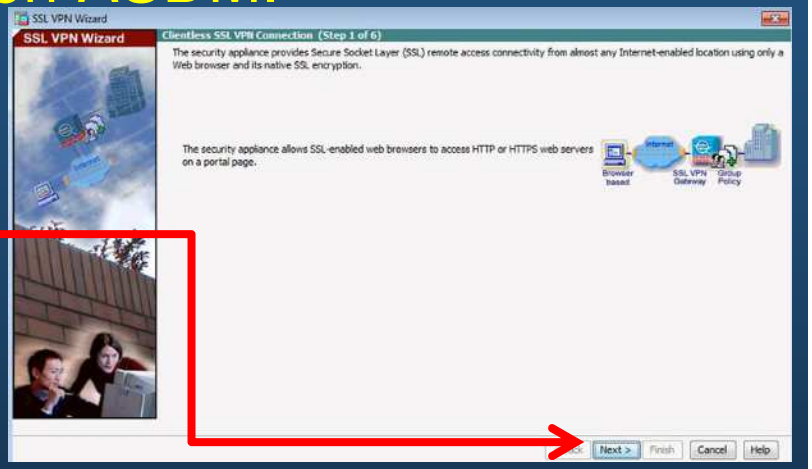
- Topología de Ejemplo para VPN Sin Clientes.
  - Una red interna con nivel de seguridad 100.
  - Una zona DMZ con nivel de seguridad 50.
    - Acceso a servidor mediante NAT estático.
  - Una red exterior con nivel de seguridad 0.
  - Un host externo que requiere acceso a aplicaciones específicas sin un túnel dedicado.

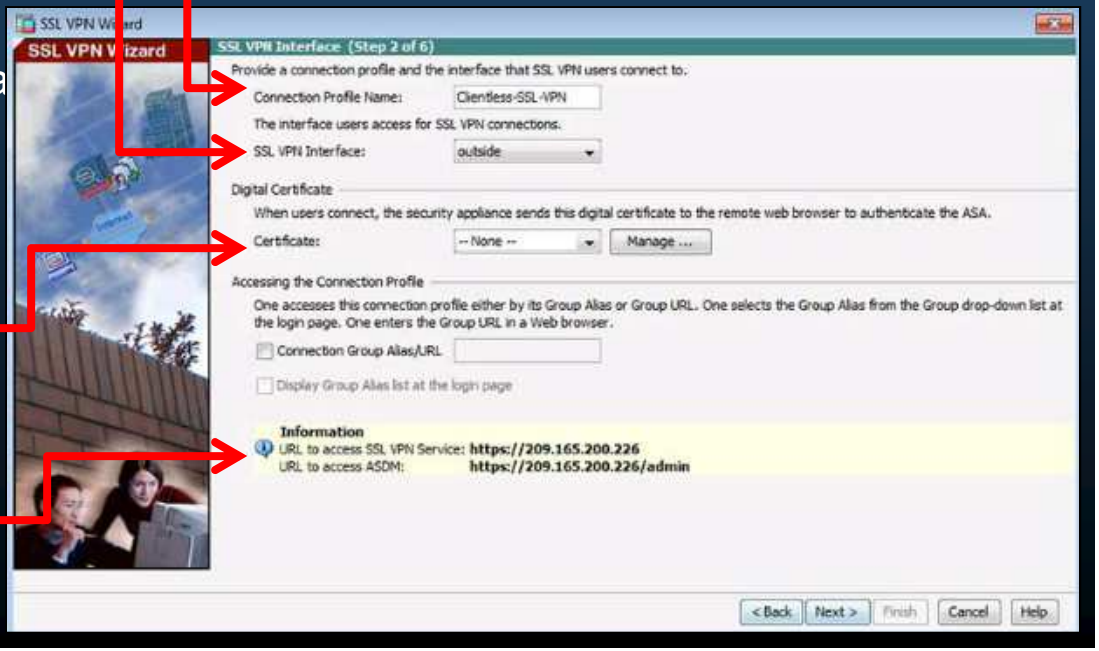


10.2 Configuración VPN en ASA.

- Creación de VPN SSL Sin Clientes en ASDM.
  - 1. Lanzar el asistente:
    - Wizards > VPN Wizards > Clientless SSL VPN Wizard > Next.
  - 2. Configurar Interface VPN Sin Clientes.
    - Entrar Nombre de Perfil.
    - Identificar interface outside.
    - Por defecto ASA usa certificado auto-firmado para autenticar.

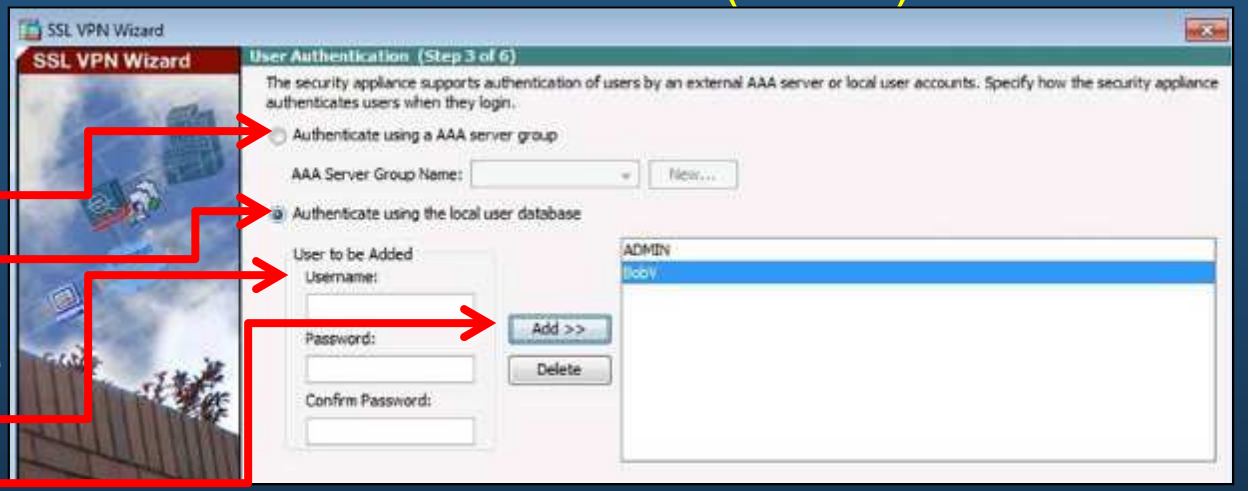
      Puede configurarse un certificado comprado a un tercero (VeriSign).
    - Proporcionará URLs para:
      - Login
      - Administrar.





10.2 Configuración VPN en ASA.

- Creación de VPN SSL Sin Clientes en ASDM (Cont.).
  - 3. Autenticación de Usuario.
    - Servidor AAA.
    - B.D. Local.
      - Ingresar credenciales de Usuario.
      - Añadir Usuario.

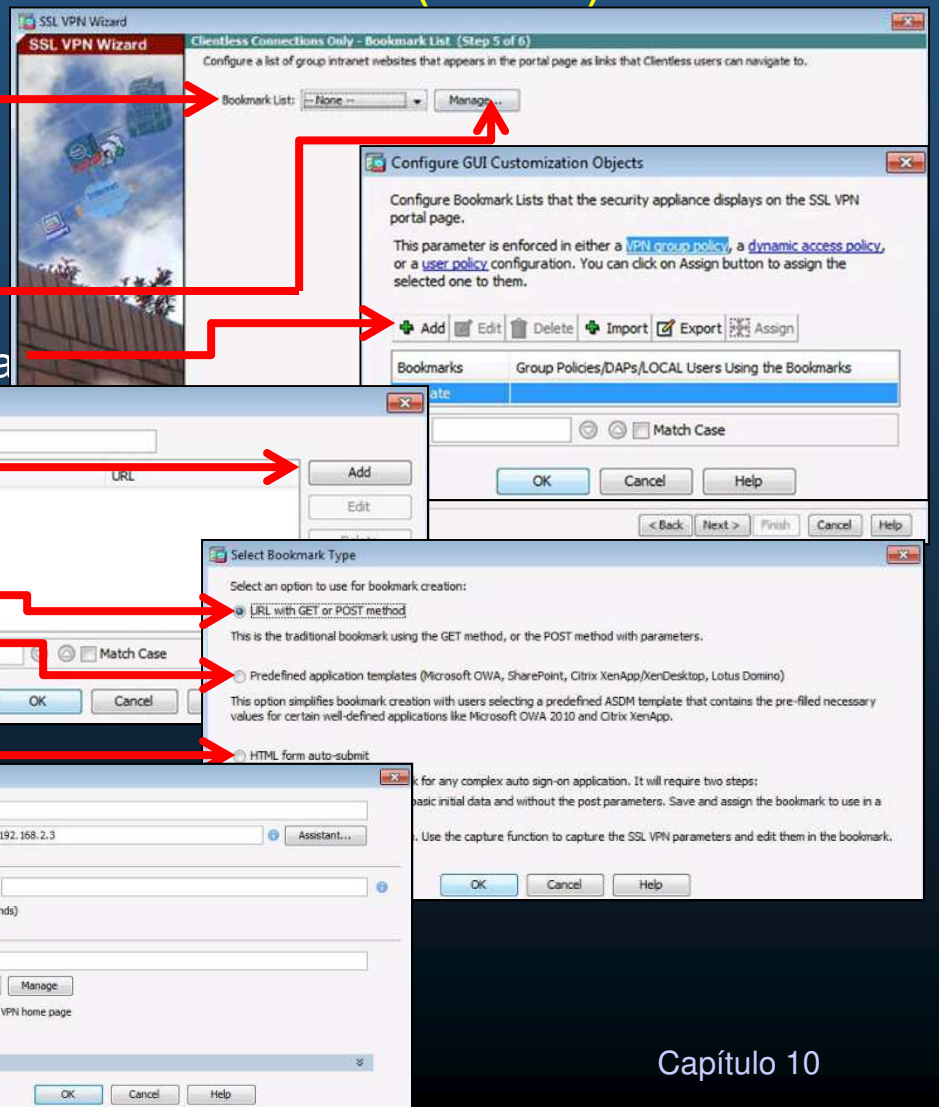


  - 4. Definir política de grupo.
    - Crear nueva política de grupo.
      - El nombre no debe tener espacios.
    - Modificar política de grupo existente.

Modificar configuraciónes de política de grupo creada: Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies

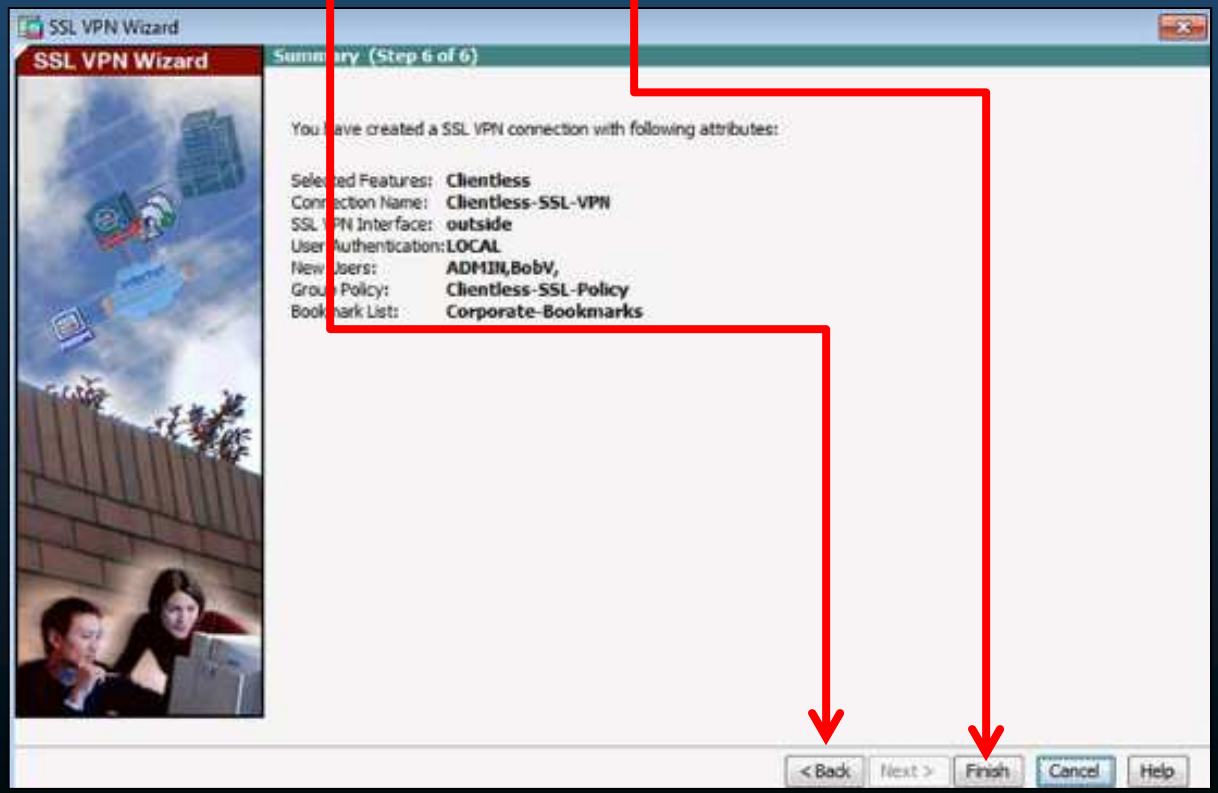
10.2 Configuración VPN en ASA.

- Creación de VPN SSL Sin Clientes en ASDM (Cont.).
  - 5. Configurar lista de marcadores para conexiones sin cliente.
    - Elegir uno existente.
    - Por default no hay marcadores Crear uno nuevo con Manage.
      - Add para añadir Marcador a lista
        - Add para crear marcador.
        - Tres tipos:
          + URL GET/POST
          - Apps predefinidas
          - HTML
        - OK
          - Entrar datos de marcador.
            - Nombre.
            - URL (http(s) / ftp + IP) .
          - OK, OK, OK.



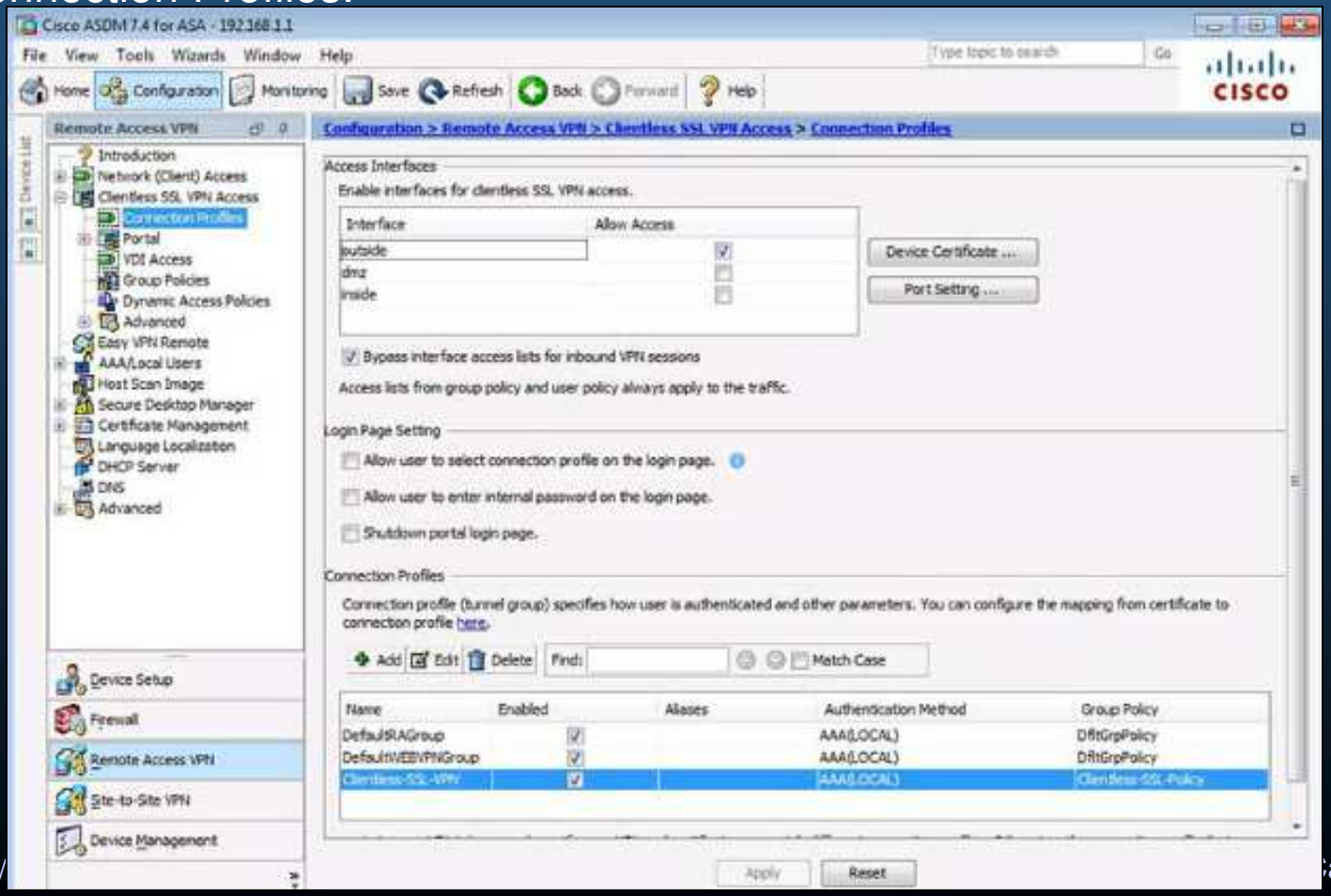
10.2 Configuración VPN en ASA.

- Creación de VPN SSL Sin Clientes en ASDM (Cont.).
  - 6. Verificar Resumen y Guardar Cambios
    - Back para modificar.
    - Finish para establecer marcadores.



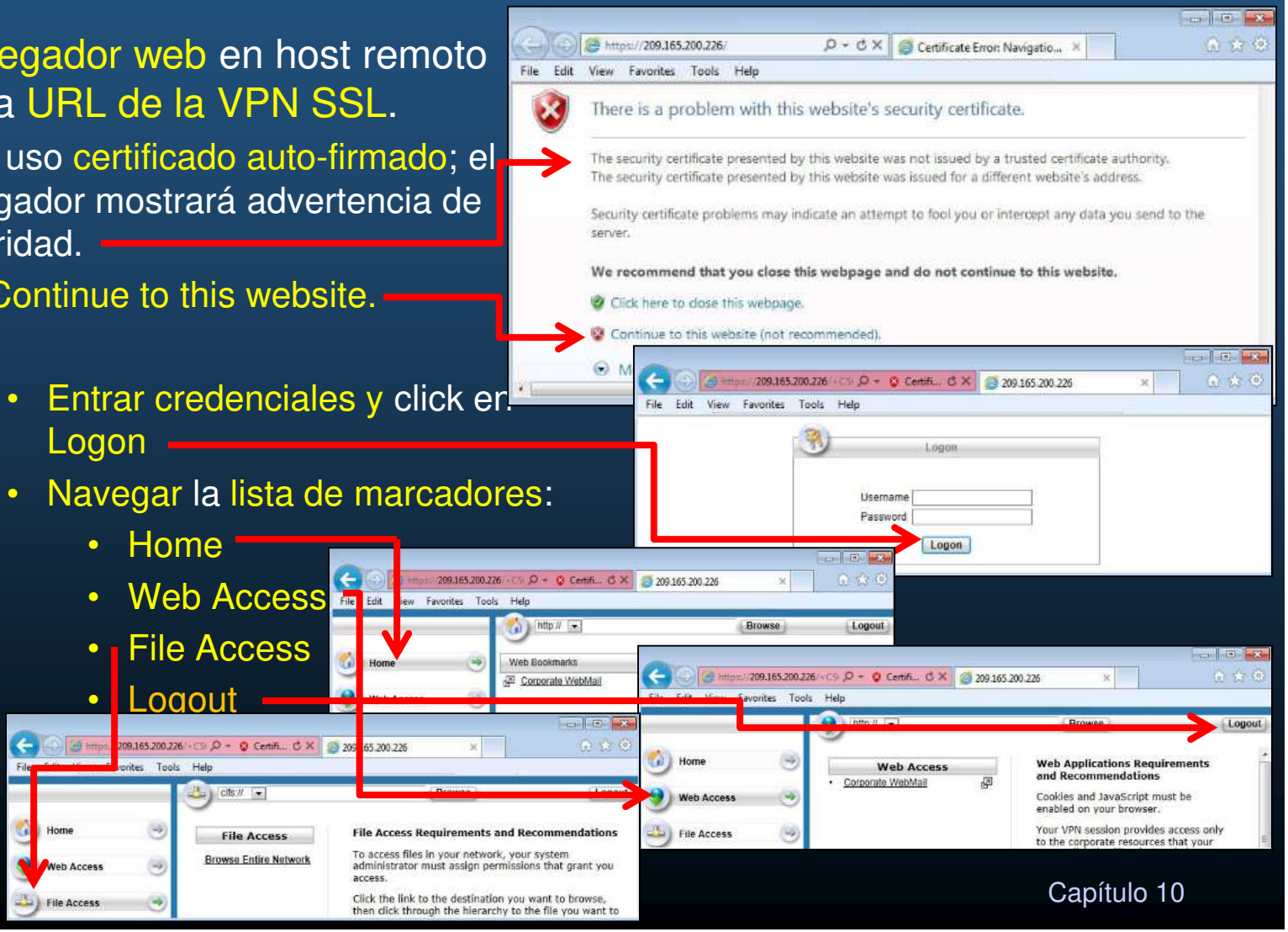
10.2 Configuración VPN en ASA.

- Verificar y Editar VPN SSL Sin Clientes.
  - Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles.



10.2 Configuración VPN en ASA.

- Prueba de VPN SSL Sin Clientes .
  - Abrir navegador web en host remoto y entrar la URL de la VPN SSL.
    - Si se uso certificado auto-firmado; el navegador mostrará advertencia de seguridad.
      - Continue to this website.
    - Entrar credenciales y click en Logon
    - Navegar la lista de marcadores:
      - Home
      - Web Access
      - File Access
      - Logout



10.2 Configuración VPN en ASA.

- Ver en CLI la Configuración Generada.
  - El Asistente genera las siguientes configuraciones:

```
webvpn
 enable outside

group-policy Clientless-SSL-Policy internal
group-policy Clientless-SSL-Policy attributes
 vpn-tunnel-protocol ssl-clientless
 webvpn
  url-list value Corporate-Bookmarks

username ADMIN password 3MBOT/Mpbpc4KbOv encrypted privilege 0
username ADMIN attributes
 vpn-group-policy Clientless-SSL-Policy
username BobV password AOv1eG/KWkzEwhtN encrypted privilege 0
username BobV attributes
 vpn-group-policy Clientless-SSL-Policy

tunnel-group Clientless-SSL-VPN type remote-access
tunnel-group Clientless-SSL-VPN general-attributes
 default-group-policy Clientless-SSL-Policy
```

WebVPN: Habilita la VPN SSL en la interface especificada.

Grupo de Políticas:
- Crea y Aplica grupo de políticas a la interface.
- Especifica SSL para usar en VPN sin Clientes.
- Configura el grupo de políticas para WebVPN.
- Identifica una lista de URLs para WebVPN.

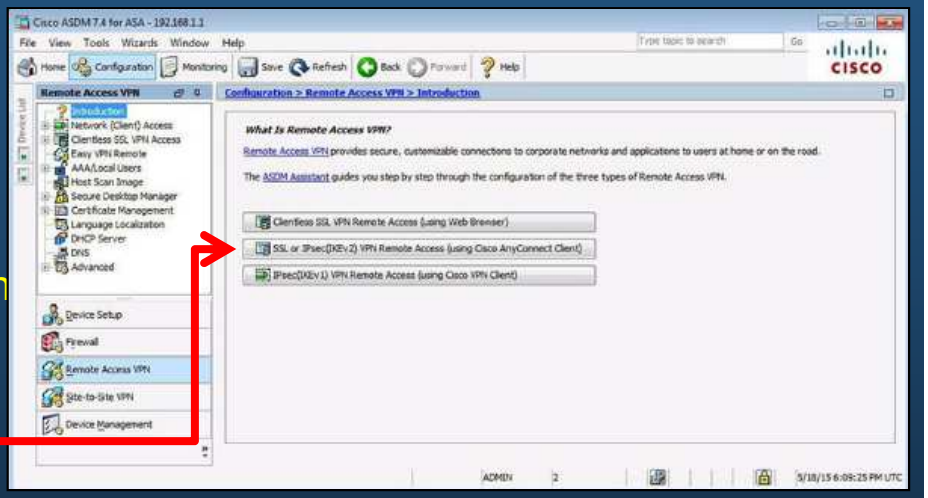
Usuario Remoto:
- Crear entrada en B.D. local para usuario.
- Configura usuario para heredar atributos del grupo de políticas especificado.

Grupo de Tunel:
- Los usuarios se conectan por IPSec o SSL.
- Especifica los atributos que el usuario hereda por defecto.

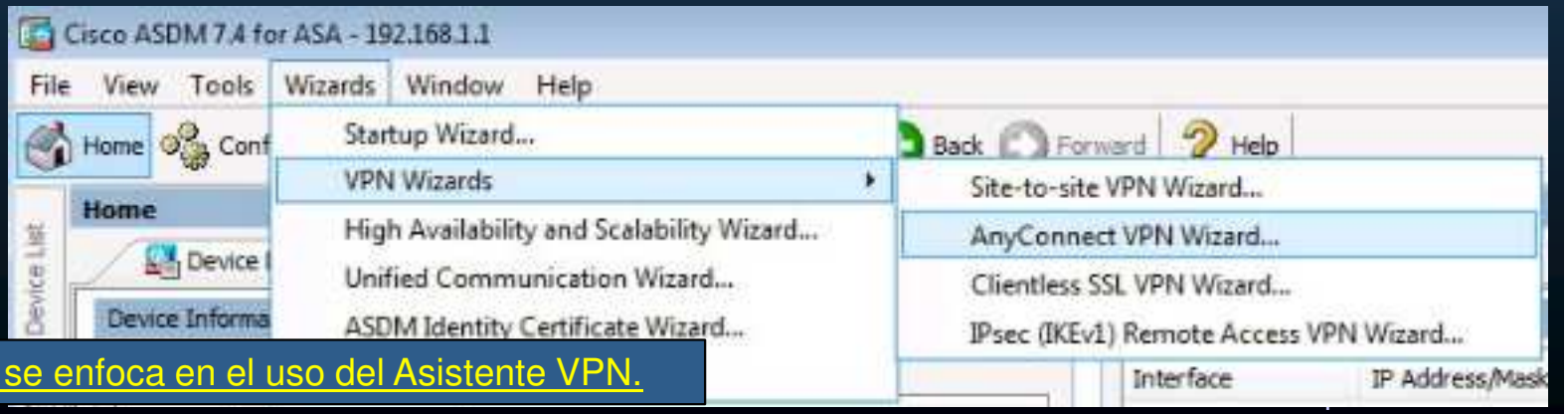
La descripción de estos comandos está fuera del alcance del curso.

10.2 Configuración VPN en ASA.

- Configuración de ASA para VPN SSL por AnyConnect.
  - Dos herramientas:
    - Asistente ASDM: guía de configuración de VPN por SSL.
      - Configurations > Remote-Access VPN > Introduction > SSL or IPsec(IKEv2) VPN Remote Access (using Cisco AnyConnect Client)



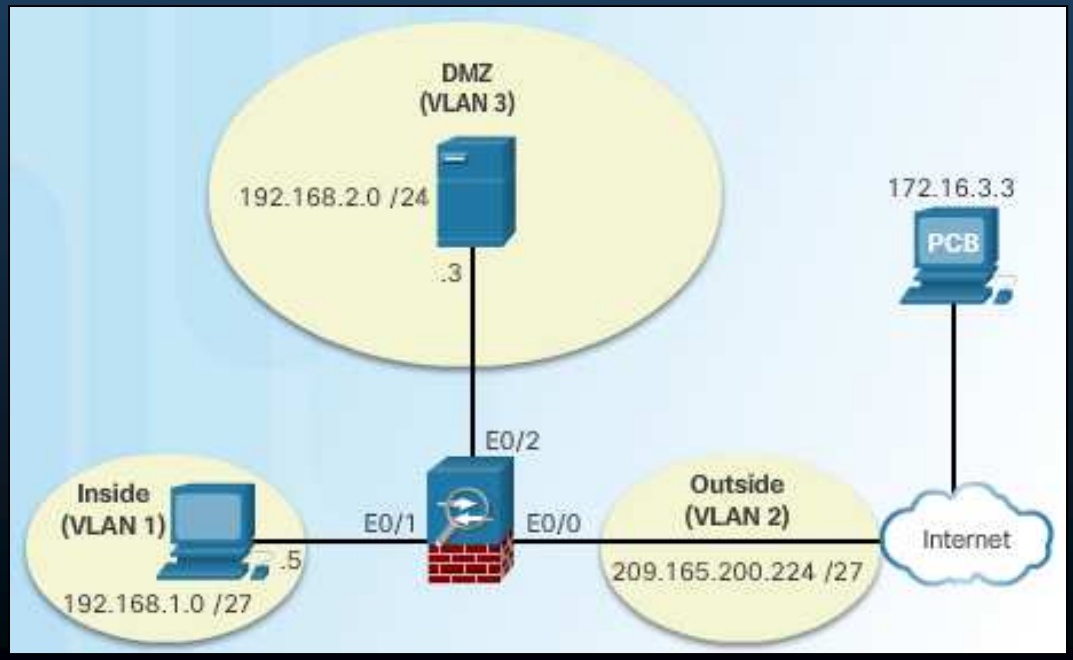
    - Asistente VPN: simplifica la configuración de VPN por SSL.
      - Wizards > VPN Wizards > AnyConnect VPN Wizard.



El presente curso se enfoca en el uso del Asistente VPN.

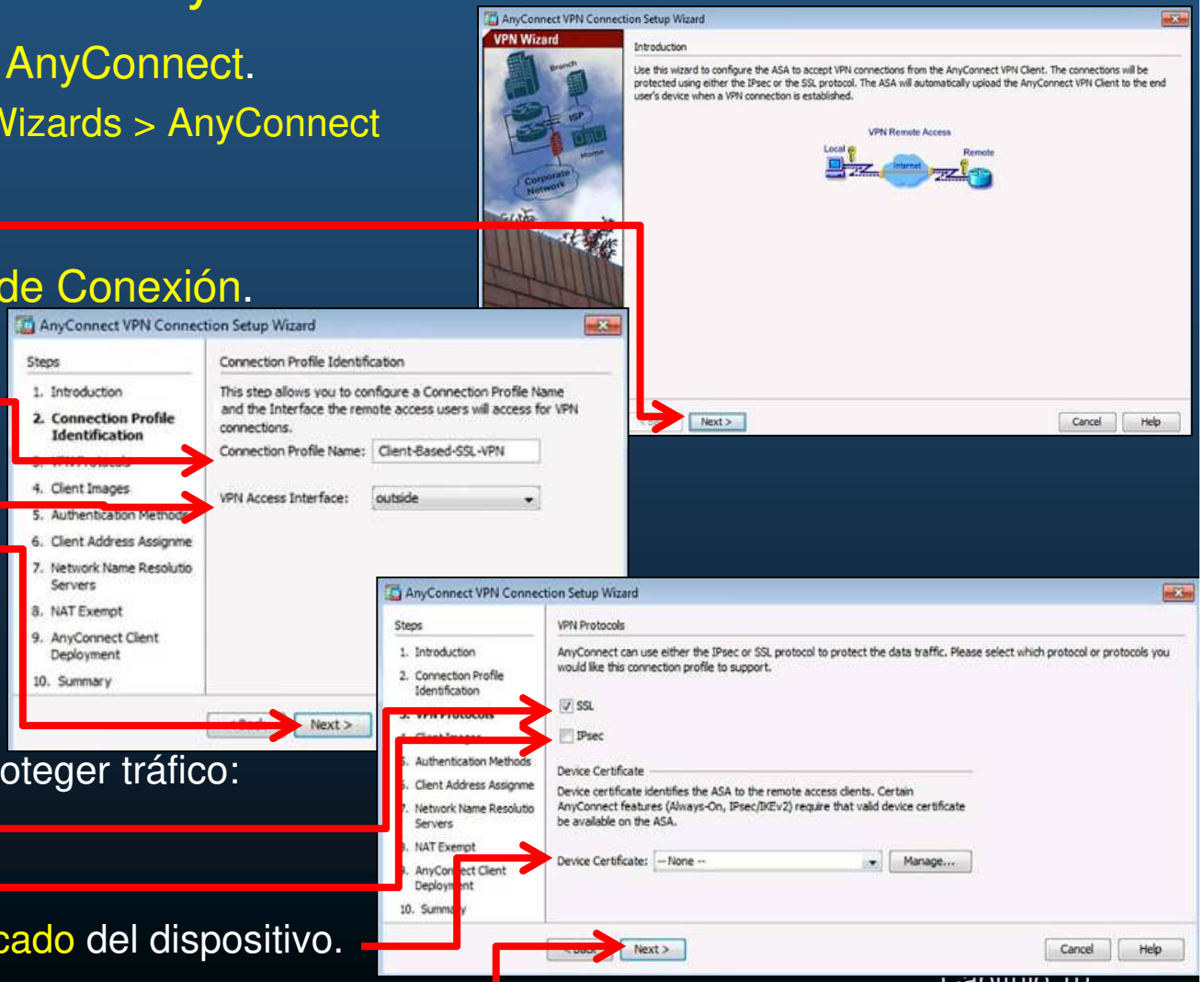
10.2 Configuración VPN en ASA.

- Topología de Ejemplo para VPN SSL AnyConnect.
  - Una red interna con nivel de seguridad 100.
  - Una zona DMZ con nivel de seguridad 50.
    - Acceso a servidor mediante NAT estático.
  - Una red exterior con nivel de seguridad 0.
  - Un host externo que requiere acceso a la red interna.
    - No cuenta con cliente VPN pre-instalado / Requiere descarga Sin cliente.



10.2 Configuración VPN en ASA.

- Creación de VPN SSL AnyConnect en ASDM
  - 1. Lanzar Asistente AnyConnect.
    - Wizards > VPN Wizards > AnyConnect VPN Wizard
    - Next
  - 2. Configurar Perfil de Conexión.
    - Entrar Nombre de Perfil.
    - Identificar interface outside.
    - Next.
  - 3. Protocolos VPN.
    - Seleccionar protocolo para proteger tráfico:
      - SSL.
      - IPSec.
    - Configurar certificado del dispositivo.
    - Next

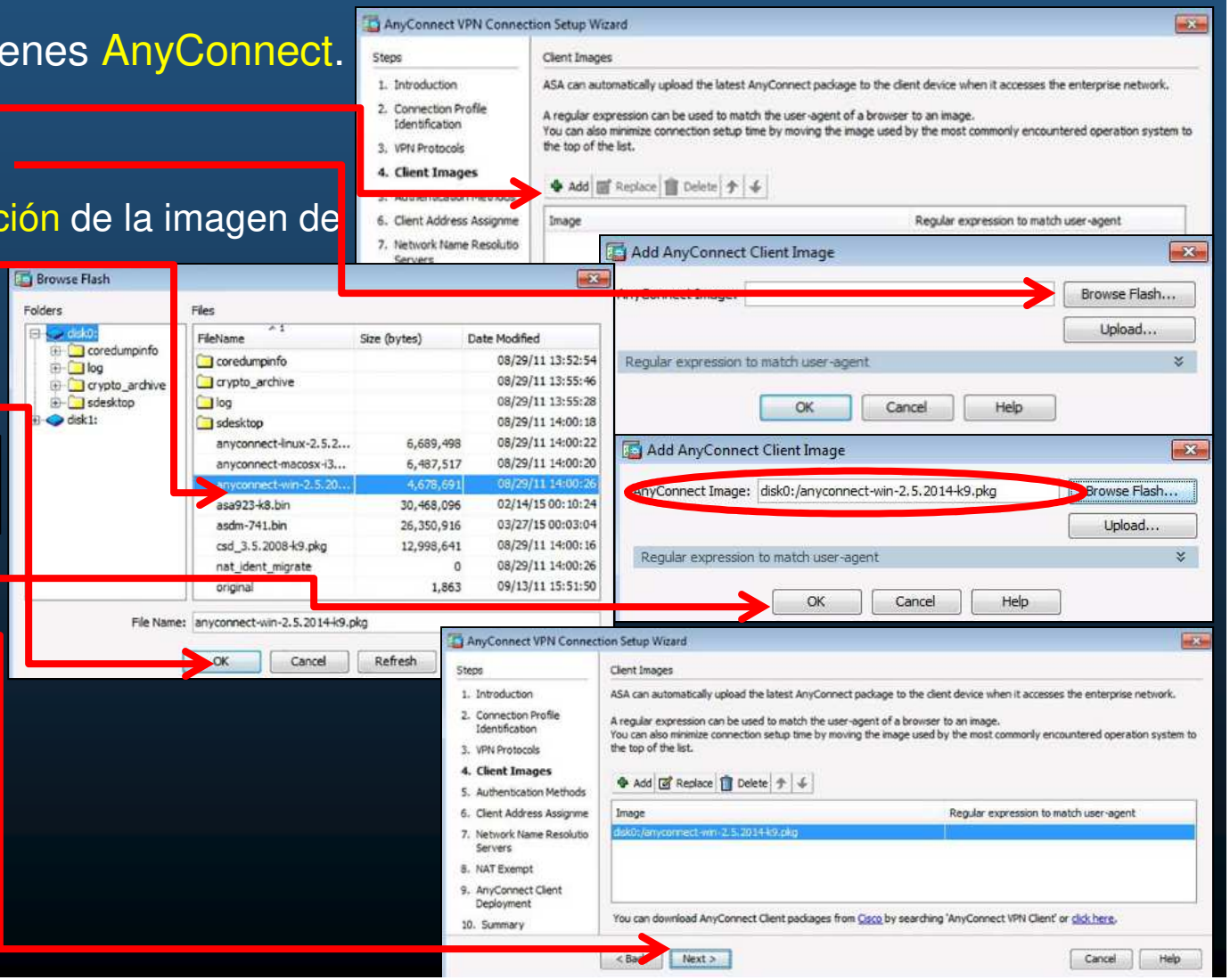


10.2 Configuración VPN en ASA.

- Creación de VPN SSL AnyConnect en ASDM (Cont).
  - 4. Agregar Imágenes AnyConnect.
    - Add.
    - Browse Files
    - Indicar ubicación de la imagen de AnyConnect. (para Win / Mac / Linux)
    - OK.

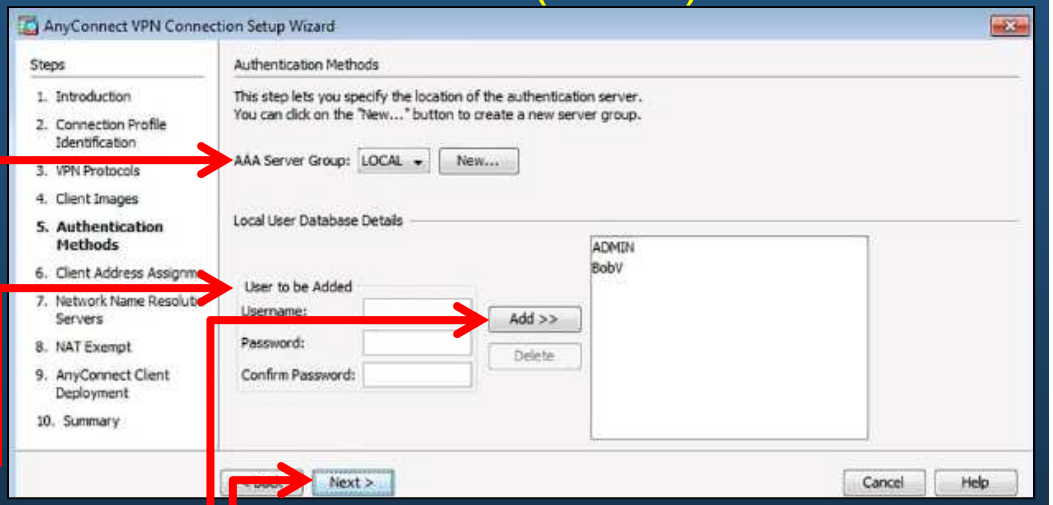
Windows 8.1 Requiere AnyConnect 4.1

    - OK.
    - Next.



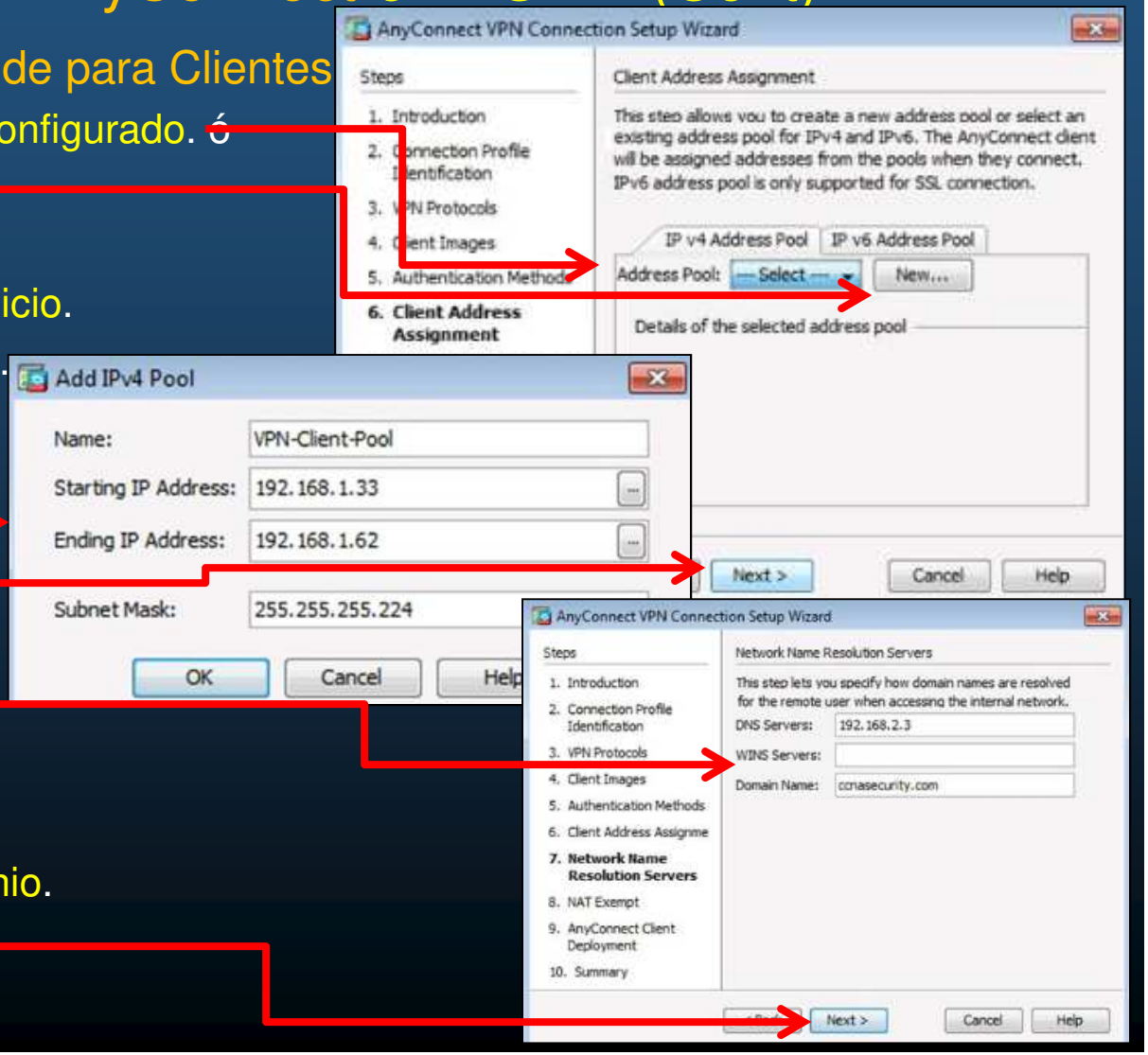
10.2 Configuración VPN en ASA.

- Creación de VPN SSL AnyConnect en ASDM (Cont).
  - 5. Configurar Métodos de Autenticación.
    - Definir grupo de servidores AAA.
      - LOCAL
      - New
        - Entrar credenciales de usuario.
        - Add >>
    - Next para continuar.



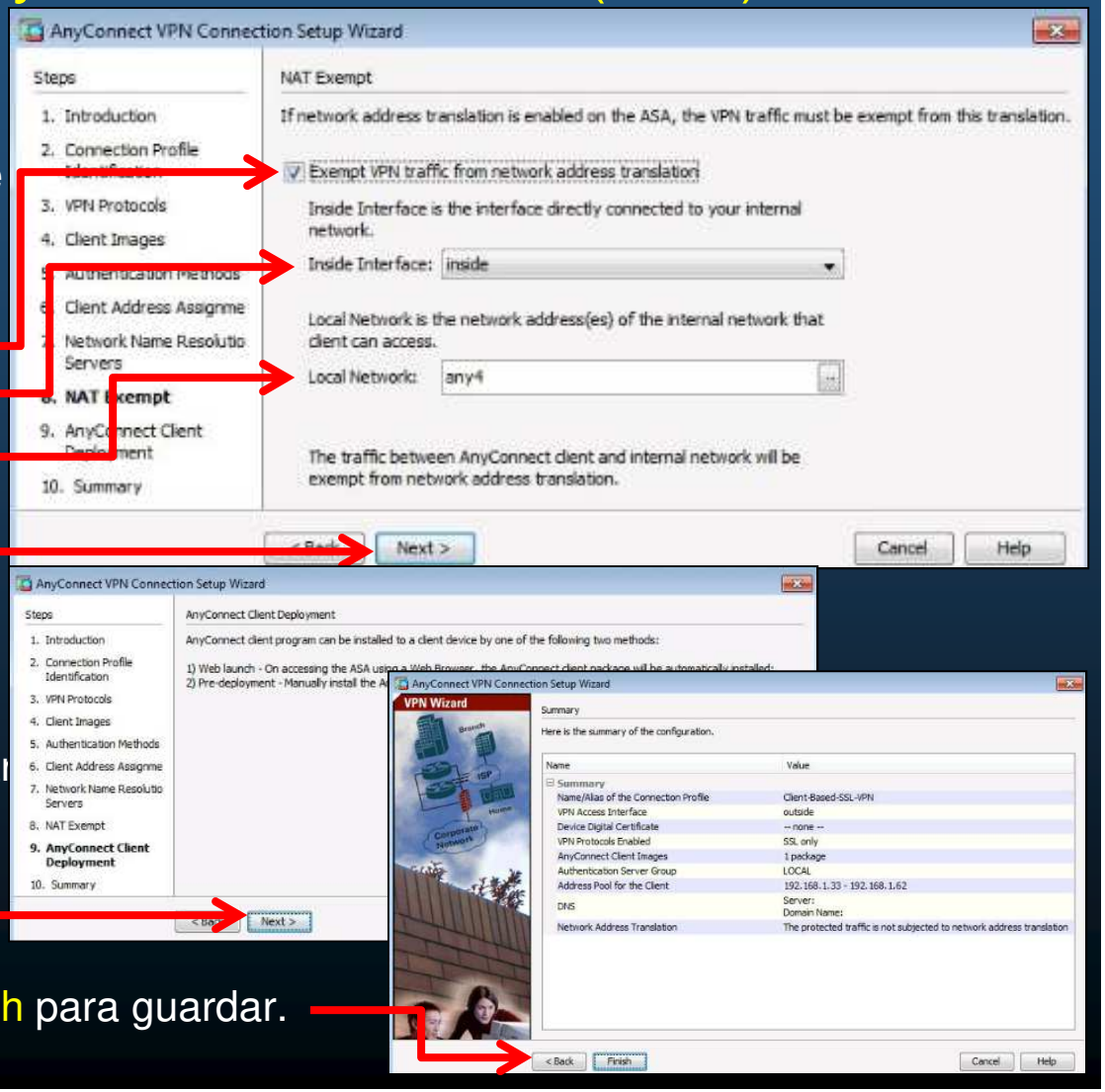
10.2 Configuración VPN en ASA.

- Creación de VPN SSL AnyConnect en ASDM (Cont).
  - 6. Crear Pool de IPs inside para Clientes
    - Seleccionar Pool preconfigurado. ó
    - New.
      - Dar Nombre.
      - Dirección IP de Inicio.
      - Dirección IP Final.
      - Mascara de Subred.
      - OK
    - Next.
  - 7. Especificar DNSs.
    - Entrar Datos de DNS.
      - Servidor DNS.
      - Servidor WINS.
      - Nombre de Dominio.
    - Next.



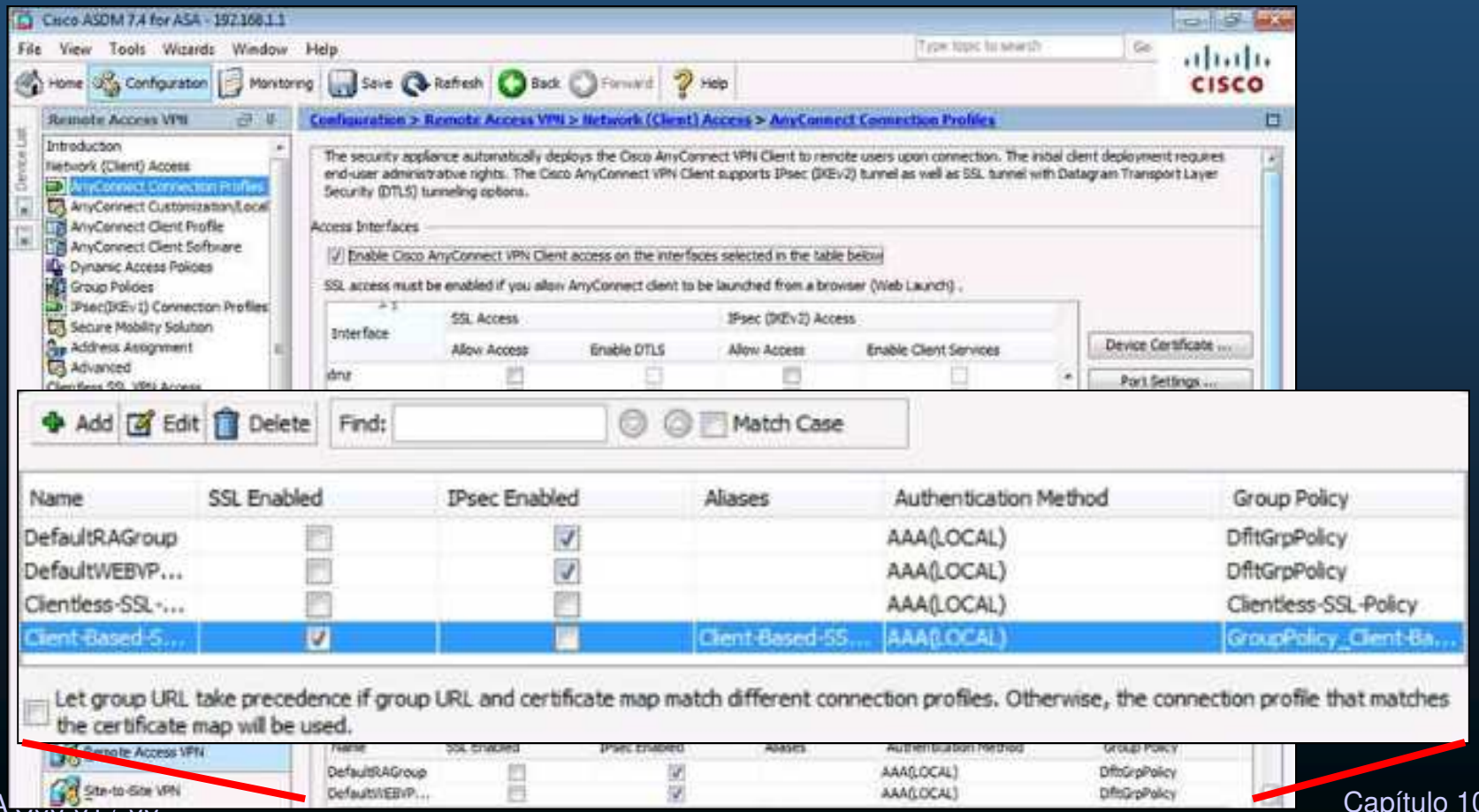
10.2 Configuración VPN en ASA.

- Creación de VPN SSL AnyConnect en ASDM (Cont).
  - 8. Excepción de NAT.
    - Los clientes del pool deberían estar excentos de NAT. Pues al encriptar ya conocen la IP interna.
    - Excempt VPN traffic…
    - Inside Interface.
    - Direcciones Accesibles.
    - Next.
  - 9. Implantación de Cliente AnyConnect.
    - Información para Descargar AnnyConnect en clientes.
    - Next.
  - 10. Verificar y Guardar.
    - Back si hay cambios / Finish para guardar.



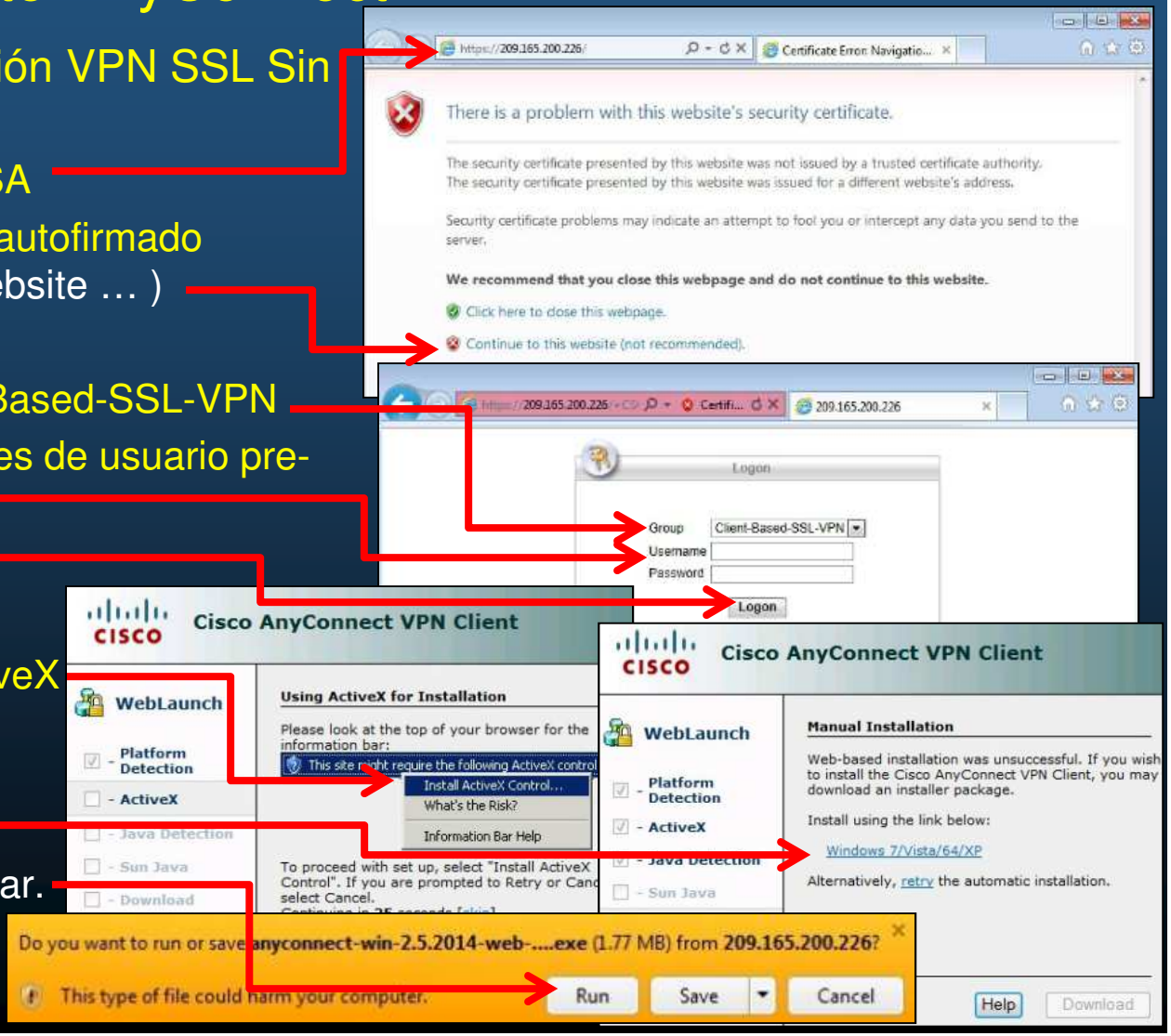
10.2 Configuración VPN en ASA.

- Verificar Conexión AnyConnect.
  - Configurations > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles.



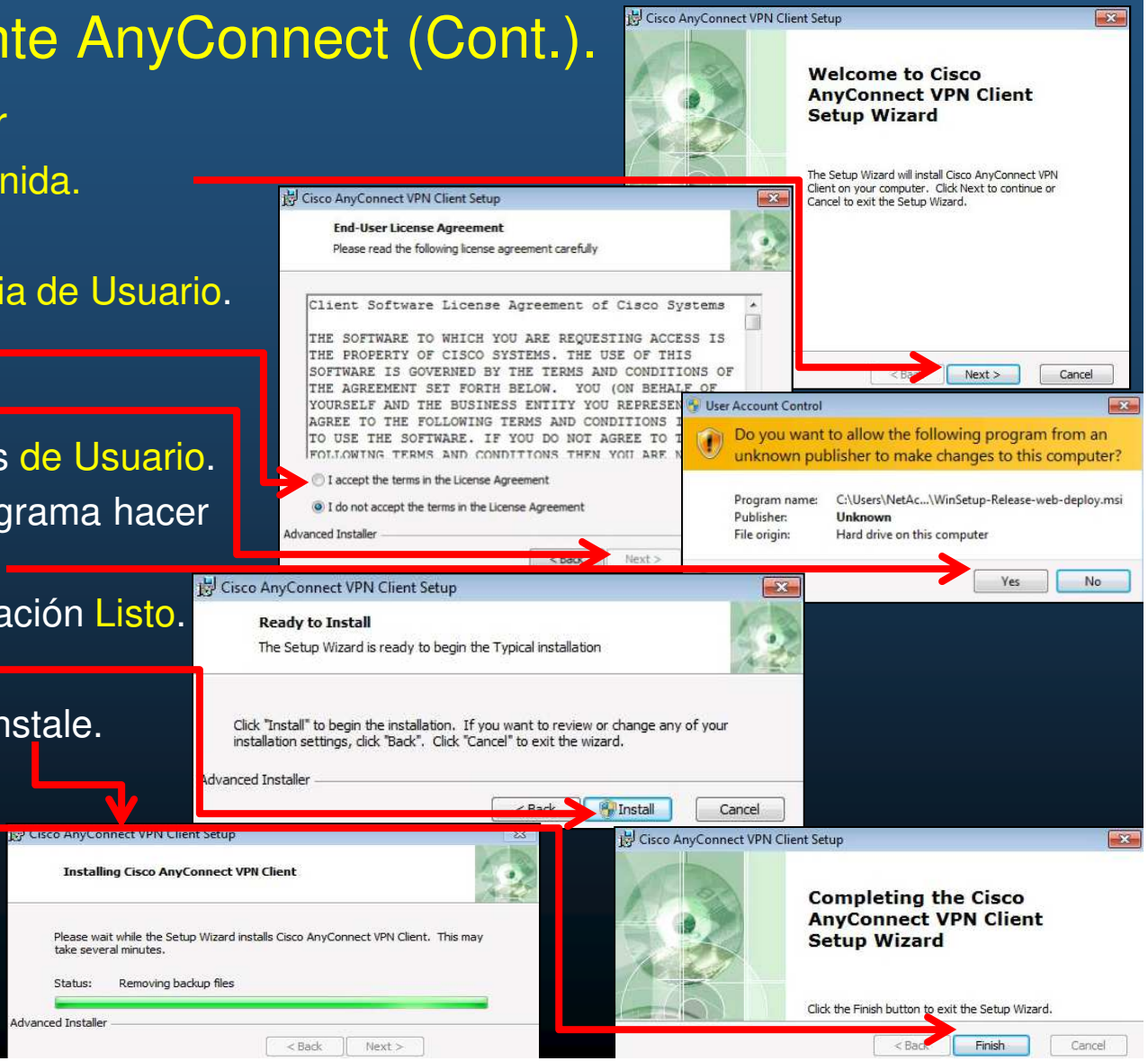
10.2 Configuración VPN en ASA.

- Instalación del Cliente AnyConnect.
  - Establecer una conexión VPN SSL Sin Cliente.
    - Entrar https://IP_ASA
    - Aceptar certificado autofirmado (Continue to this website …)
    - En el grupo Client-Based-SSL-VPN
    - Ingresar credenciales de usuario pre-registrado.
    - Logon.
    - Instalar control ActiveX para autoinstalar.
    - Ó Descargar Manualmente.
      - Run para instalar.



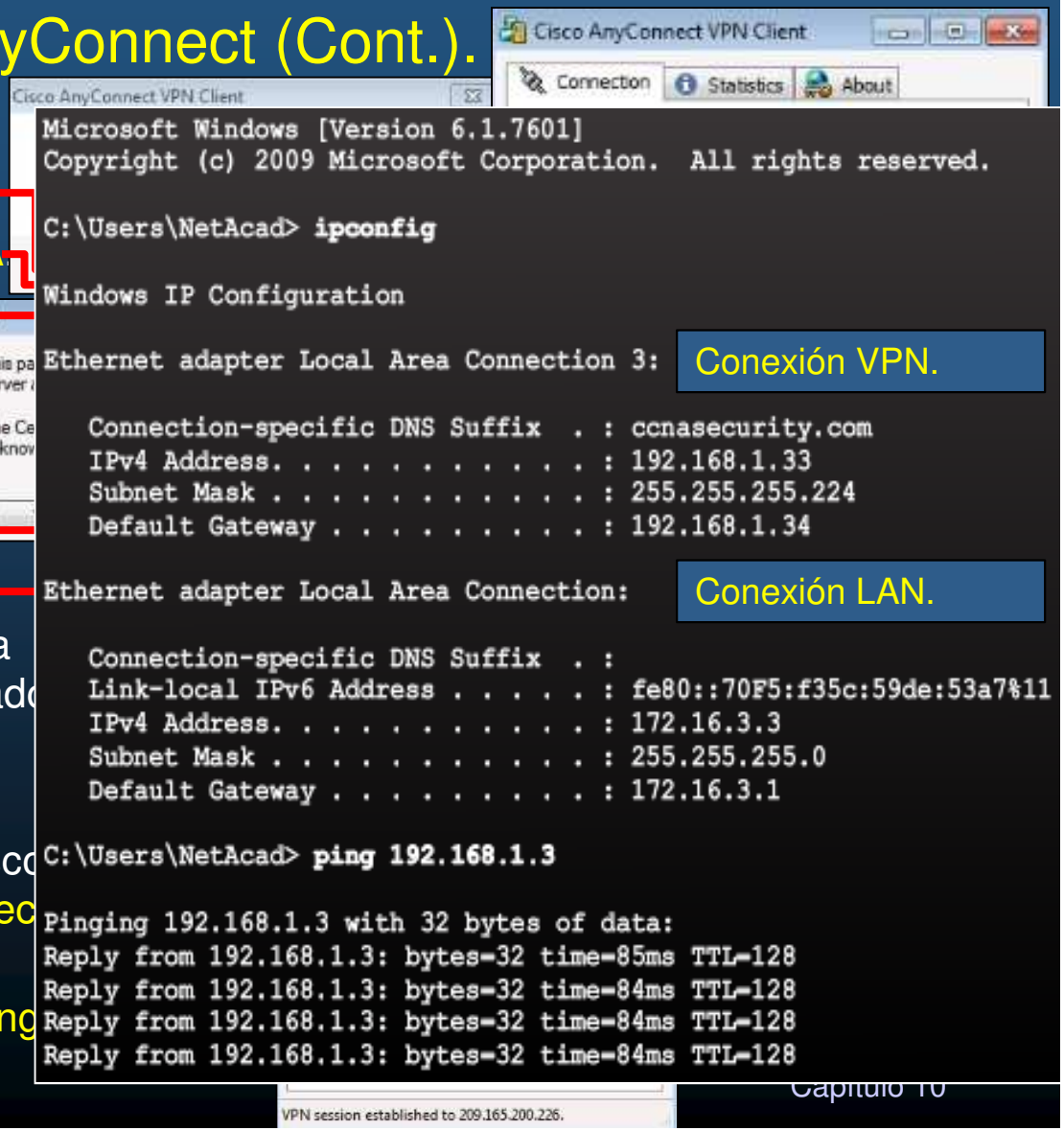
10.2 Configuración VPN en ASA.

- Instalación del Cliente AnyConnect (Cont.).
  - Tras Iniciar Instalador
    - Pantalla de Bienvenida.
      - Next.
    - Acuerdo de Licencia de Usuario.
      - I accept …
      - Next.
    - Control de Cuentas de Usuario.
      - Permitir al programa hacer cambios (Yes)
    - Asistente de Instalación Listo.
      - Instalar.
    - Esperar a que se instale.
    - Finalizar.



10.2 Configuración VPN en ASA.

- Instalación del Cliente AnyConnect (Cont.).
  - Iniciar Cisco AnyConnect.
    - Solicitud de gateway. Ok.
    - Ingresar IP Pública del ASA.
    - Select.
    - Aceptar certificado autofirmado. Yes.
    - Ingresar credenciales de usuario.
    - Connect.
    - **Nota**. Podría generarse otra solicitud de aceptar certificado autofirmado → Yes.
    - Verificar Información VPN.
      - Windows Sys Try > Cisco AnyConnect (Click Derec > Open AnyConnect.
    - Verificar IP con ipconfig / ping



10.2 Configuración VPN en ASA.

- Ver las Configuraciones Generadas en la CLI.

```
ip local pool VPN-Client-Pool 192.168.1.33-192.168.1.62 mask 255.255.255.224
object network NETWORK_OBJ_192.168.1.32_27
 subnet 192.168.1.32 255.255.255.224
nat (inside,outside) source static any any destination static NETWORK_OBJ_192.168.1.32_27
NETWORK_OBJ_192.168.1.32_27 no-proxy-arp route-lookup
!
webvpn
 enable outside
 anyconnect image disk0:/anyconnect-win-2.5.2014-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable

group-policy GroupPolicy_Client-Based-SSL-VPN internal
group-policy GroupPolicy_Client-Based-SSL-VPN attributes
 wins-server none
 dns-server value 192.168.2.3
 vpn-tunnel-protocol ssl-client
 default-domain value ccnasecurity.com

tunnel-group Client-Based-SSL-VPN type remote-access
tunnel-group Client-Based-SSL-VPN general-attributes
 address-pool VPN-Client-Pool
 default-group-policy GroupPolicy_Client-Based-SSL-VPN
tunnel-group Client-Based-SSL-VPN webvpn-attributes
 group-alias Client-Based-SSL-VPN enable
!
```

Configuración NAT.
- Pool de IPs locales.
- Objeto Network para traducir.
- Regla de traducción twice-NAT.

Configuración WEBVPN.
- Habilita VPN SSL en outside.
- Habilita AnyConnect para descarga y uso.
- Habilita tunnel-group-list.

Configuración de Políticas de Grupo
- Creación de Grupo de políticas con atributos generales.
- Configuración de DNS e información de dominio.
- Conexión de usuariuos por VPN SSL.

Configuración de Grupo de Tunel.
- Identifica atributos del grupo de tunel.
-Asocia pool local con pool de usuarios externos.
- Identifica grupo de políticas por defecto (parámetros).
- Establece configuraciones comunes para webvpn.

La descripción de estos comandos está fuera del alcance del curso.