



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

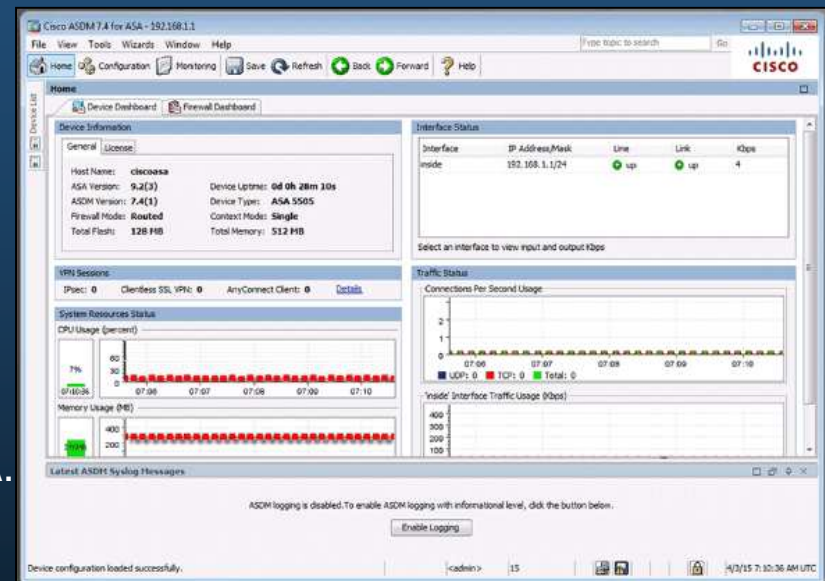
- **Introducción a ASDM.**

- **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 (múltiples 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.

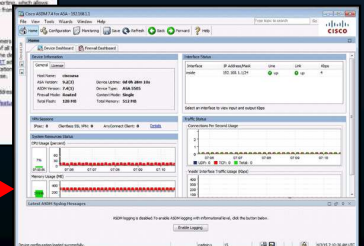
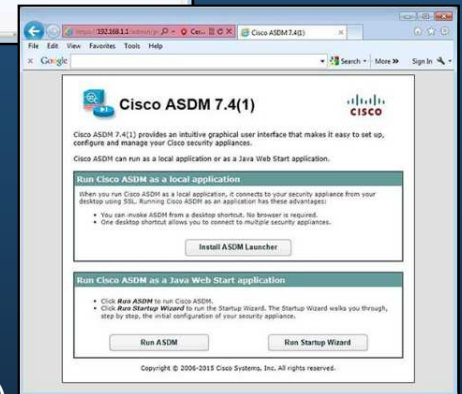
- Correr mediante navegador genera advertencias de seguridad, que hay que aceptar.

- **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

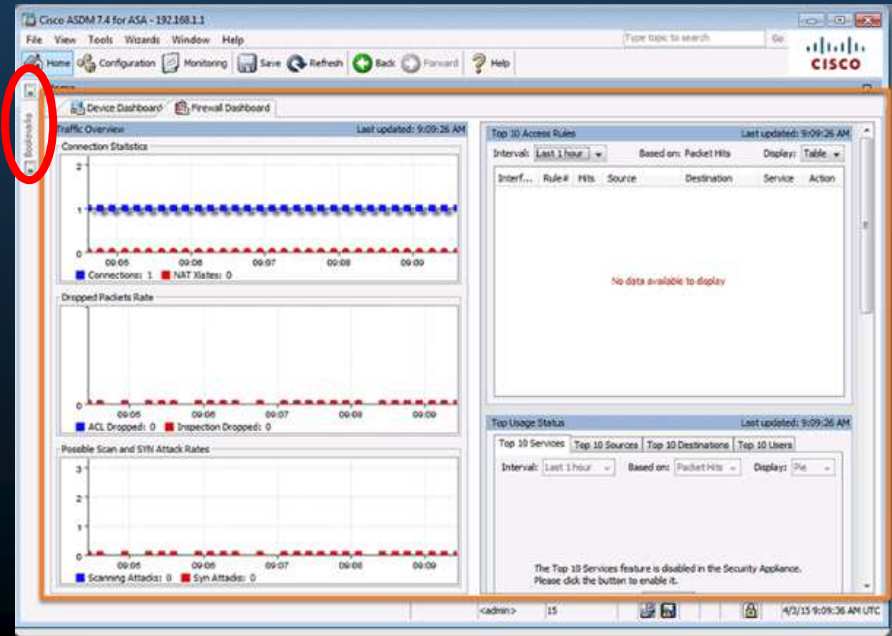
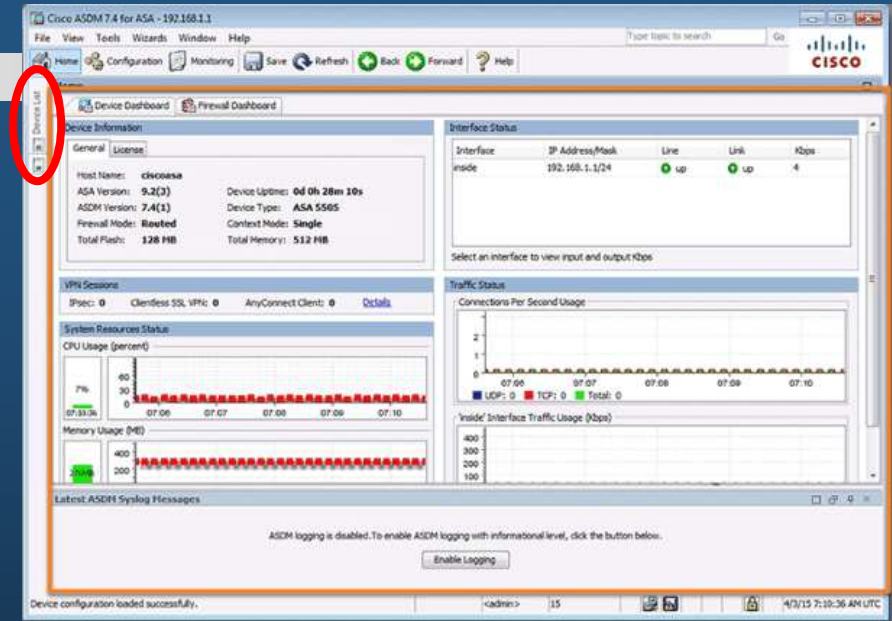
- Do not Enable



10.1 ASDM.

- Cuadros de Mando ASDM.

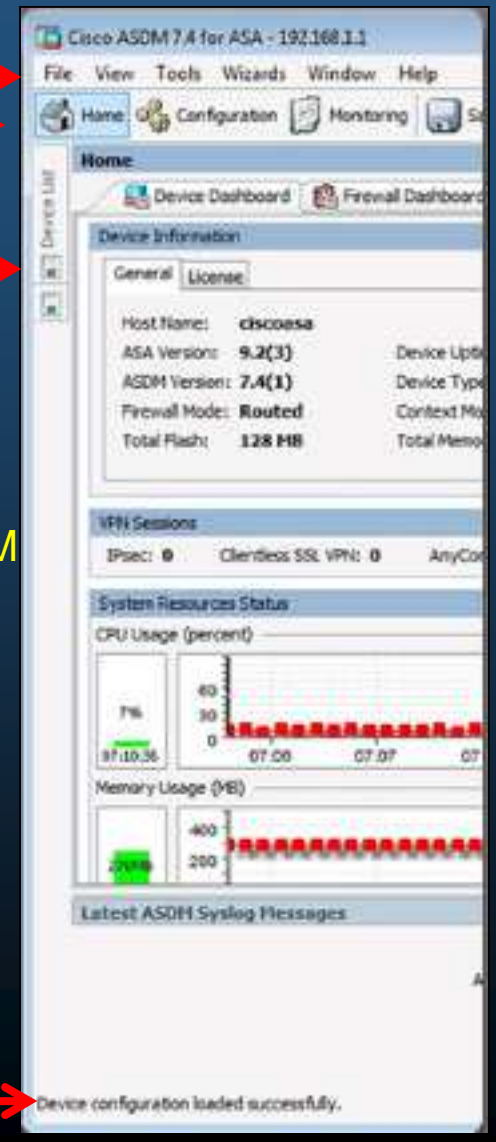
- Pestaña Dispositivo (Inicio).
 - Estado ASA (actualiza cada 10s).
 - Interfaces
 - Versión de Sistema Operativo.
 - Licencia
 - Desempeño
- Pestaña Firewall.
 - Estadísticas de Conexiones.
 - Paquetes Perdidos.
 - Escaneos.
 - Detección de Ataques SYN
- Prevención de Intrusiones.
 - Requiere Modulo 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.**

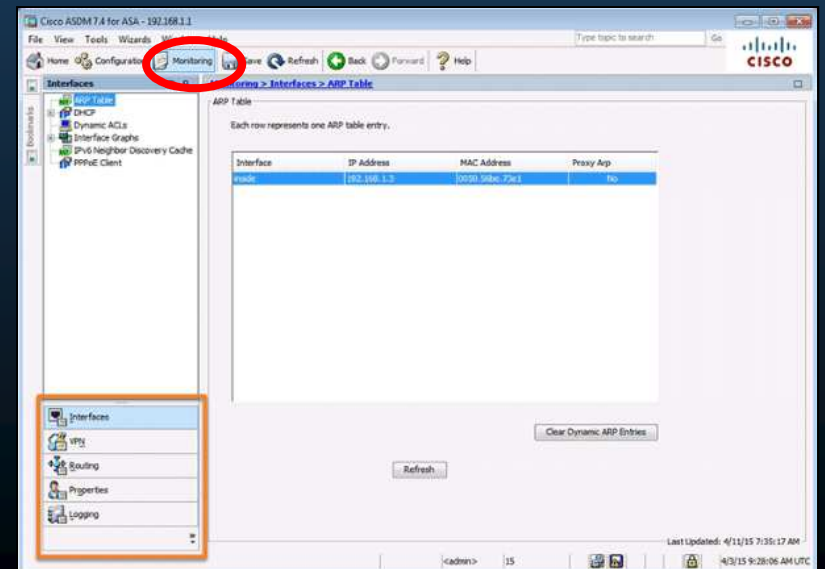
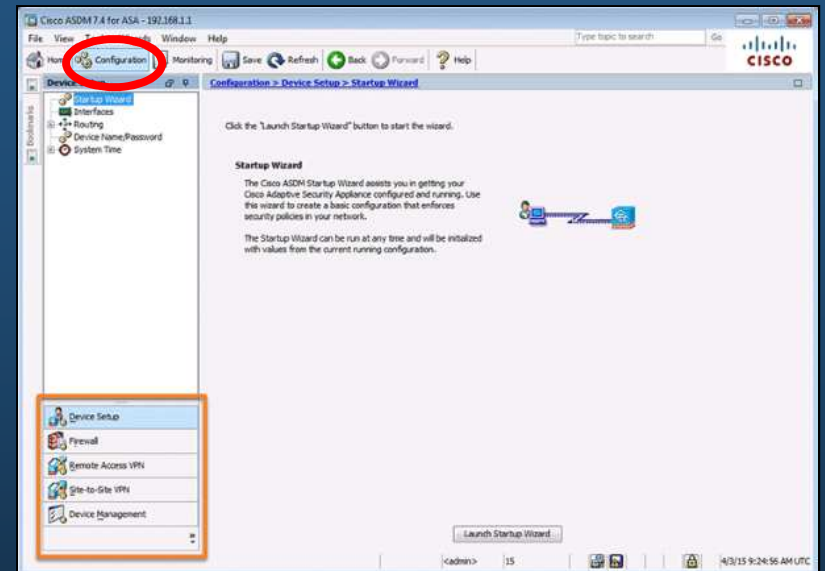
- **Configuración.**

- 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.

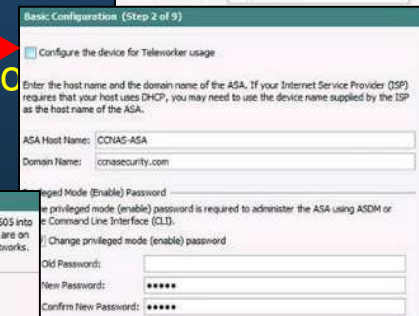
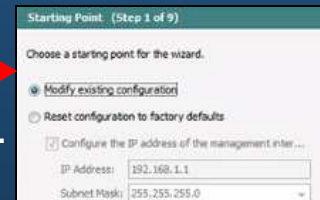
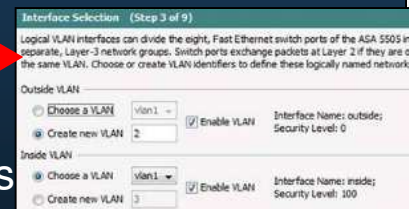
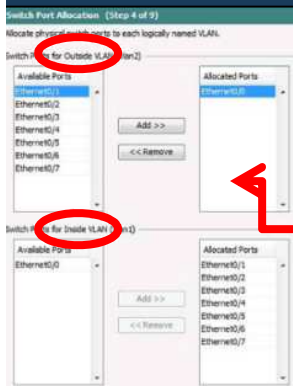
- Paso 1. Punto Inicial.
 - Modificar Configuración Existente / Resetear a estado de fábrica.

- 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 Administrativo.
 - 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.

DHCP Server (Step 6 of 9)

The ASA can act as a DHCP server and provide IP addresses to the hosts on your inside network. To configure a DHCP server on an interface other than the inside interface, go to Configuration > Device Management > DHCP > DHCP Server in the main ASDM window.

Enable DHCP server on the inside interface

DHCP Address Pool

Starting IP Address: 192.168.1.10 Ending IP Address: 192.168.1.41

DHCP Parameters

DNS Server 1: DNS Server 2:

WINS Server 1: WINS Server 2:

Lease Length: 1800 sec Ping Timeout: ms

Domain Name: cconasecurity.com

Address Translation (NAT/PAT) (Step 7 of 9)

Select Port Address Translation (PAT) to share a single external IP address for devices on the inside interface. Select Network Address Translation (NAT) to share several external IP addresses for devices on the inside interface. Select the first option, if no address translation is desired between the inside and outside interfaces.

This NAT configuration applies to all the traffic from the inside interface to the inside interface.

No Address Translation

Use Port Address Translation (PAT)

Use the IP address on the inside interface

Specify an IP address

IP Address:

Use Network Address Translation (NAT)

IP Address Range: 209.165.200.240-209.165.200.248

Auto-configuration causes the DHCP server to automatically configure DNS, WINS name. The values in the fields above take precedence over the auto-configured values.

Auto-configuration from interface:

Administrative Access (Step 8 of 9)

Specify the addresses of all hosts or networks, which are allowed to access the ASA using HTTPS/ASDM, SSH or Telnet.

Type	Interface	IP Address	Mask/Prefix Length	
HTTPS/ASDM	inside	192.168.1.3	255.255.255.255	<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>

Enable HTTP server for HTTPS/ASDM access

Disabling HTTP server will prevent HTTPS/ASDM access to this ASA.

Startup Wizard Summary (Step 9 of 9)

You have completed the Startup Wizard. To send your changes to the ASA, click Finish. If you want to modify any of the data, click Back.

Configuration Summary:

Host Name: CCNAS-ASA
Domain Name: cconasecurity.com

Switch Port Allocation:

Outside Interface (vlan 2): Switch Ports - Ethernet0/0,
Inside Interface (vlan 1): Switch Ports - Ethernet0/1, Ethernet0/2, Ethernet0/4, Ethernet0/5

Outside Interface (vlan 2):
outside, 209.165.200.226
Inside Interface (vlan 1):
inside, 192.168.1.1

DHCP Server is enabled on Inside interface. Pool : 192.168.1.10 - 192.168.1.41
No address translation is performed.

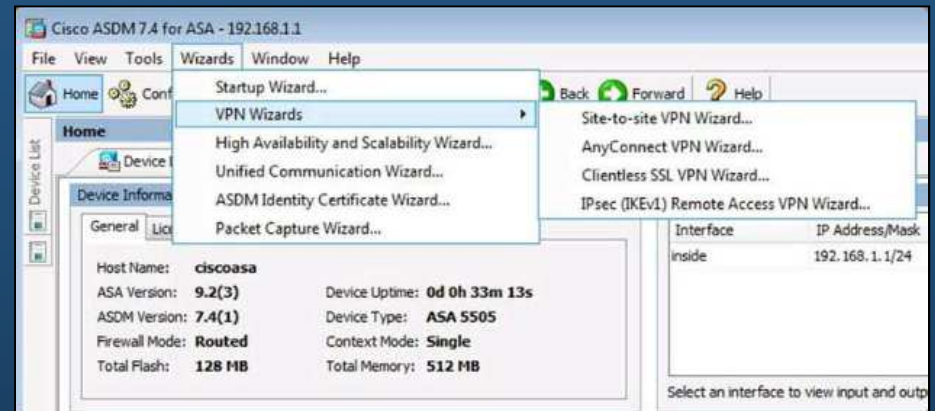
Administrative access to the device:
HTTPS/ASDM access for 192.168.1.3 through inside

History metrics

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.

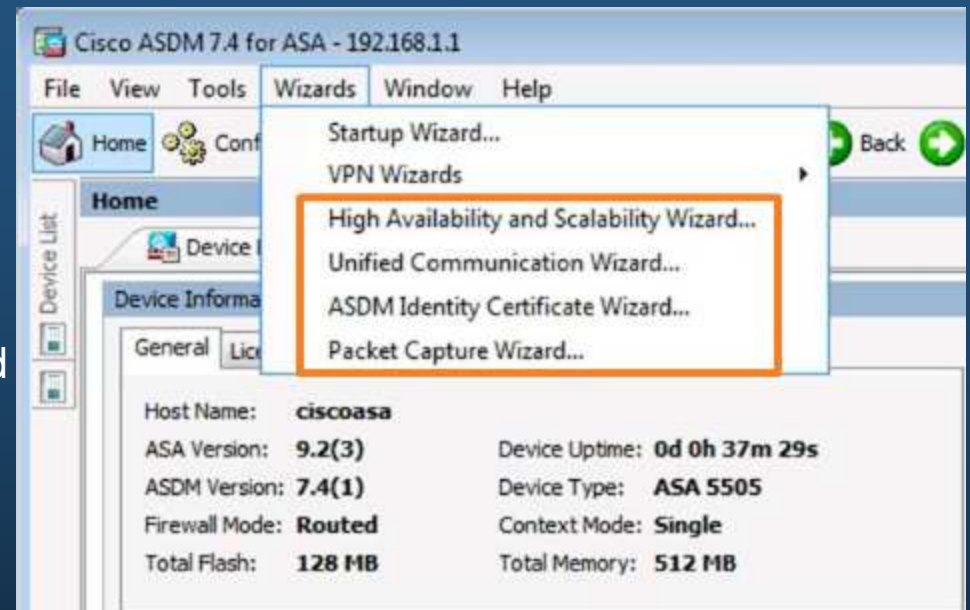


- **Tras una configuración inicial, puede usarse ASDM, para realizar una configuración avanzada.**

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 limitar tráfico capturado; origen y destino; interfaces;

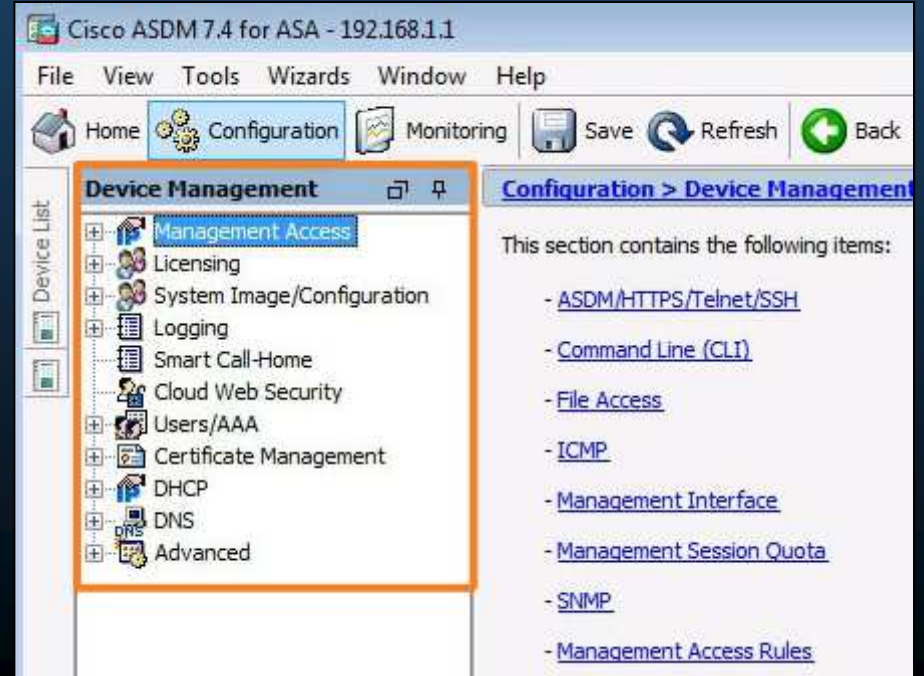
10.1 ASDM.

- 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.

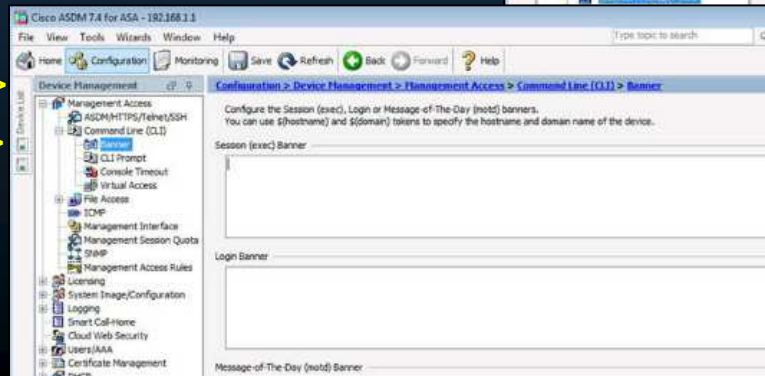
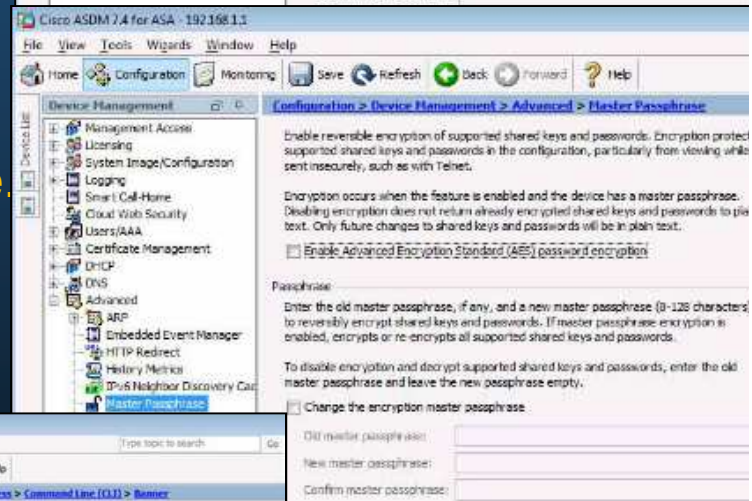
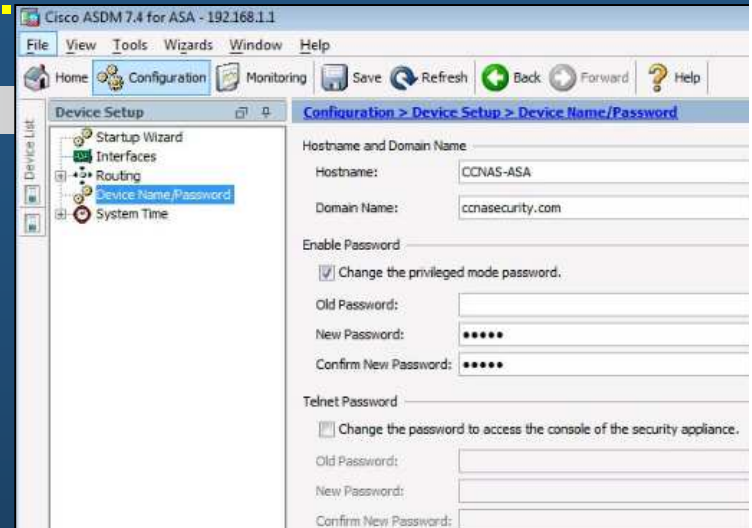
- hostname,
- domain name,
- enable password.

- 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



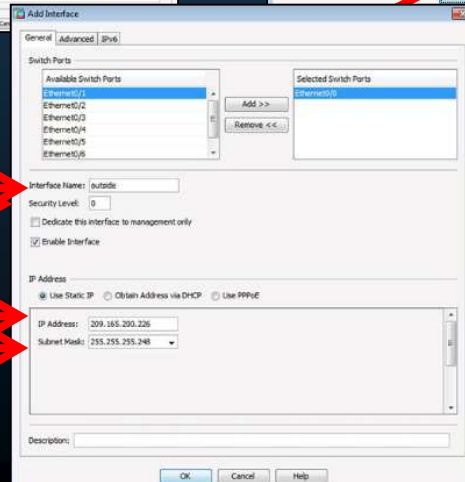
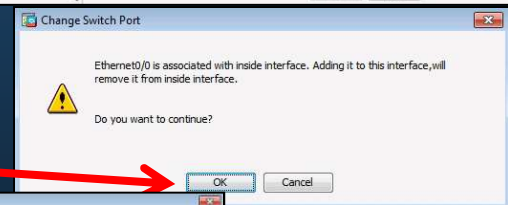
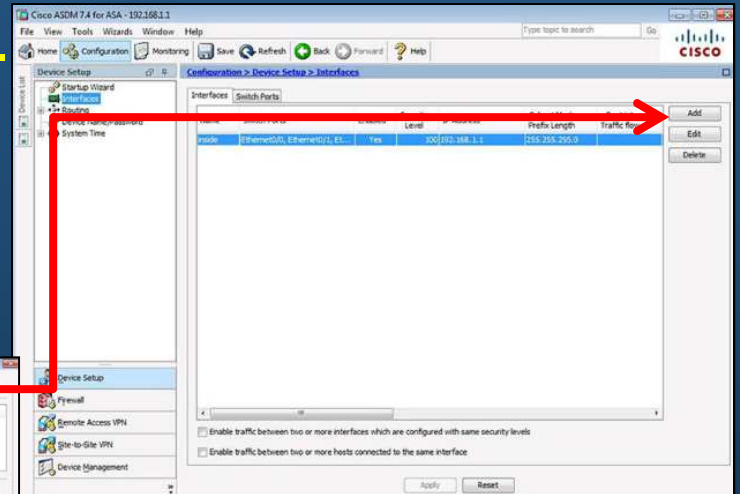
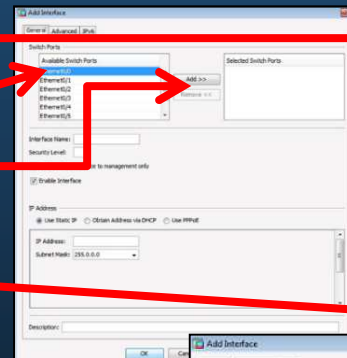
10.1 ASDM.

• 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"

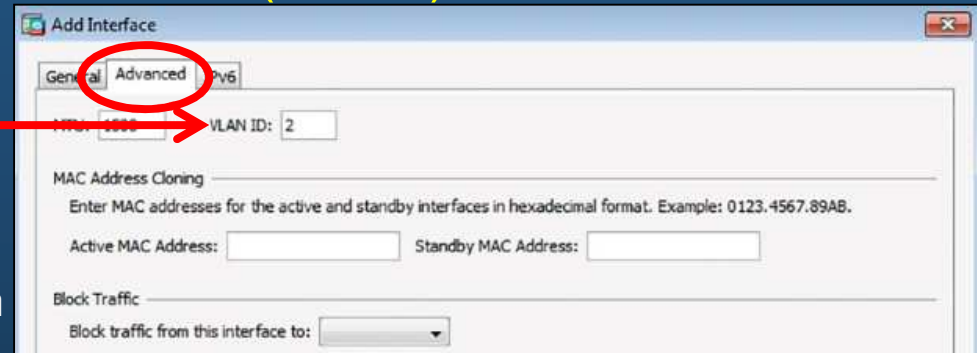
- Elegir Eth 0/0
- Añadir con Add >>
- Click en OK a la confirmación
- Entrar nombre de interface
- Nivel de seguridad
- Dirección IP
- Mascara de Red



10.1 ASDM.

• Configuración de Interfaces en ASDM (Cont.).

- Elegir Pestaña “Advanced”
 - Indicar VLAN 2
 - Click en OK



- ASDM muestra configuración actualizada:

Name	Switch Ports	Enabled	Security Level	IP Address	Subnet Mask Prefix Length	Restrict Traffic flow
inside	Ethernet0/0, Ethernet0/1, Et...	Yes	100	192.168.1.1	255.255.255.0	
outside	Ethernet0/0	Yes	0	209.165.200.226	255.255.255.248	

- La Pestaña Switchport muestra varias configuraciones para puertos.

- Eth 0/0 no está habilitada.

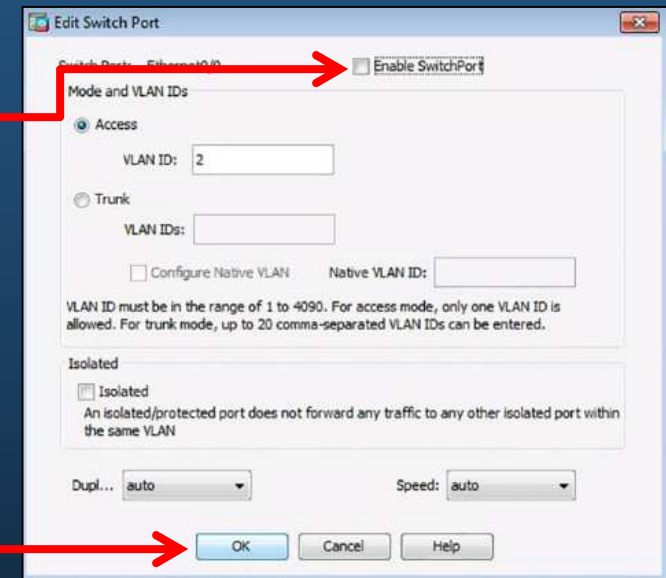
Switch Port	Enabled	Associated VLANs	Associated Interface Names	Mode	Protected	Duplex	Speed
Ethernet0/0	No	2	outside	Access	No	auto	auto
Ethernet0/1	Yes	1	inside	Access	No	auto	auto
Ethernet0/2	No	1	inside	Access	No	auto	auto
Ethernet0/3	No	1	inside	Access	No	auto	auto
Ethernet0/4	No	1	inside	Access	No	auto	auto
Ethernet0/5	No	1	inside	Access	No	auto	auto
Ethernet0/6	No	1	inside	Access	No	auto	auto
Ethernet0/7	No	1	inside	Access	No	auto	auto

- 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:



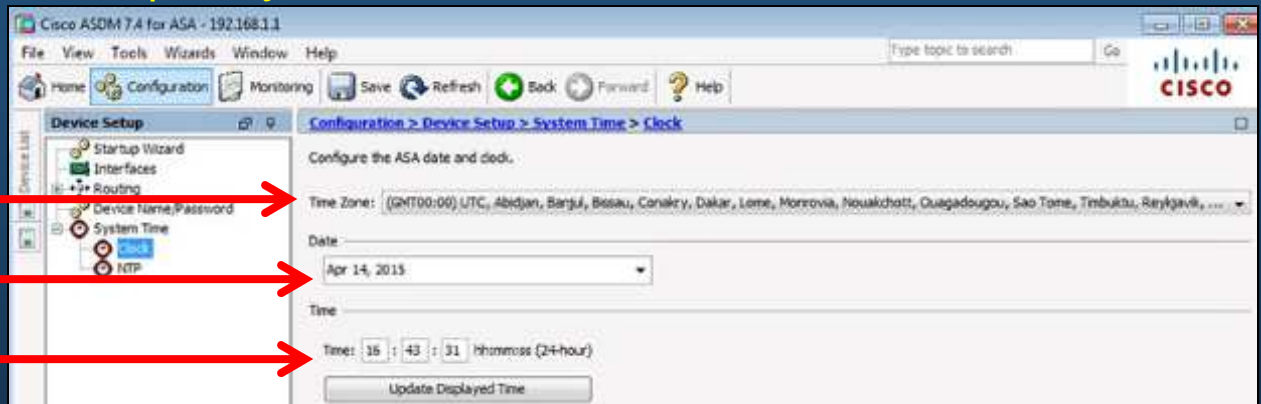
Name	Switch Ports	Enabled	Security Level	IP Address	Subnet Mask Prefix Length	Restrict Traffic flow
inside	Ethernet0/1, Ethernet0/2, Et...	Yes	100	192.168.1.1	255.255.255.0	
outside	Ethernet0/0	Yes	0	209.165.200.226	255.255.255.248	

10.1 ASDM.

- Configurar Fecha / Hora en ASDM.

- Configuration > Device Setup > System Time > Clock.

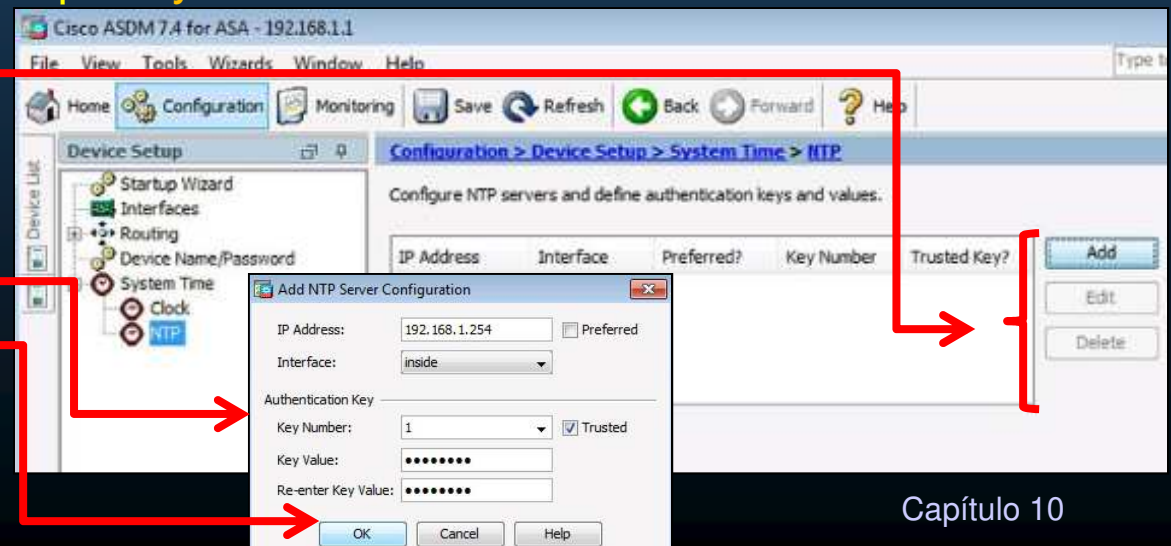
- Zona Horaria.
- Fecha.
- Hora.



- Configuration > Device Setup > System Time > NTP.

- Añadir; Editar; Eliminar.

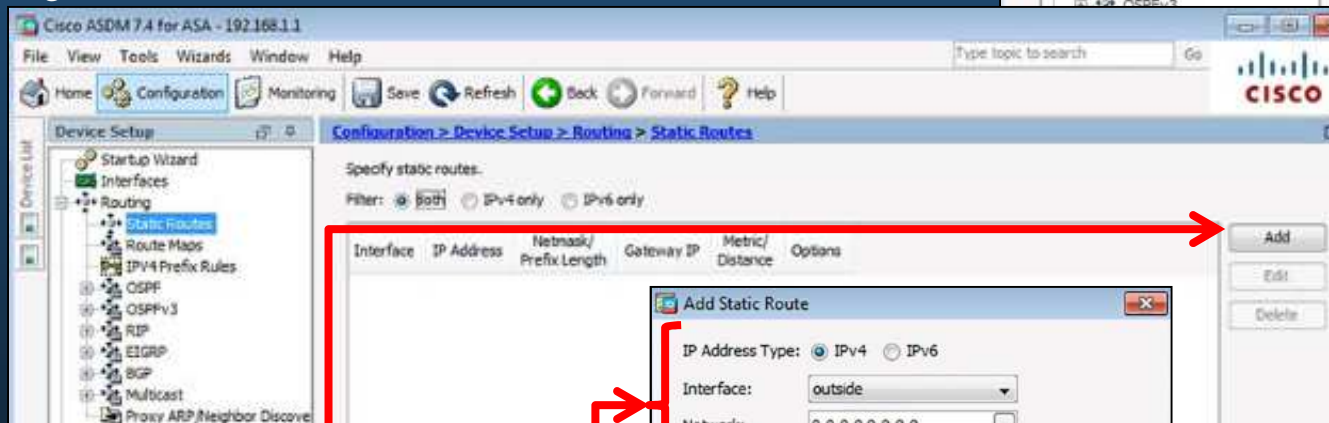
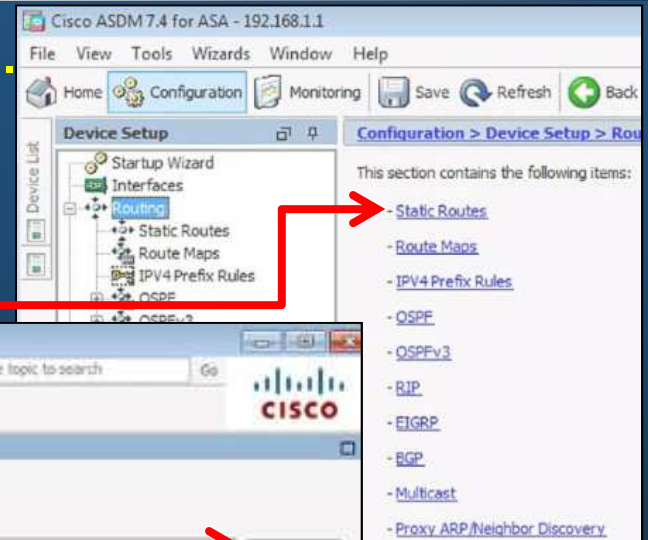
- Add
 - Entrar parámetros de Servidor NTP.
- Ok
- Actualizará la vista de servidores NTP.



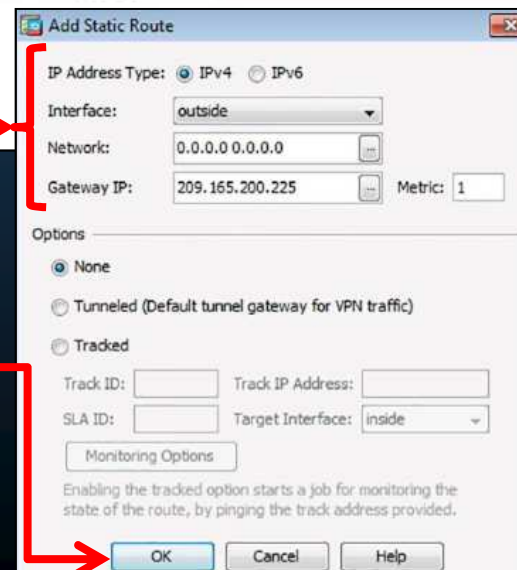
10.1 ASDM.

- 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.

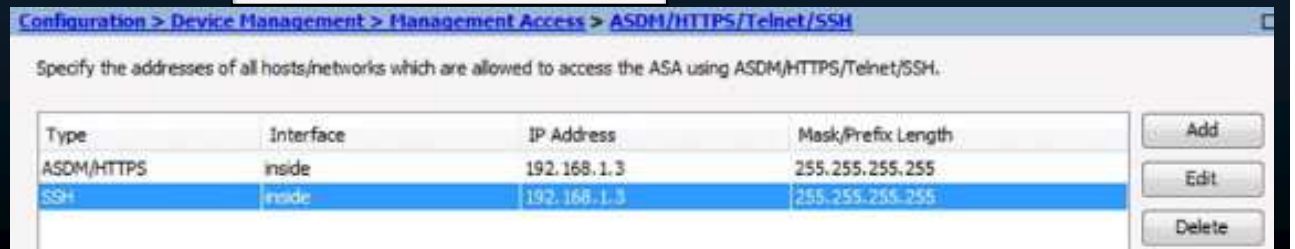
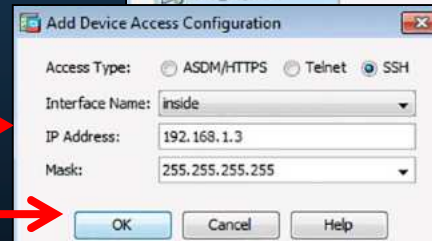
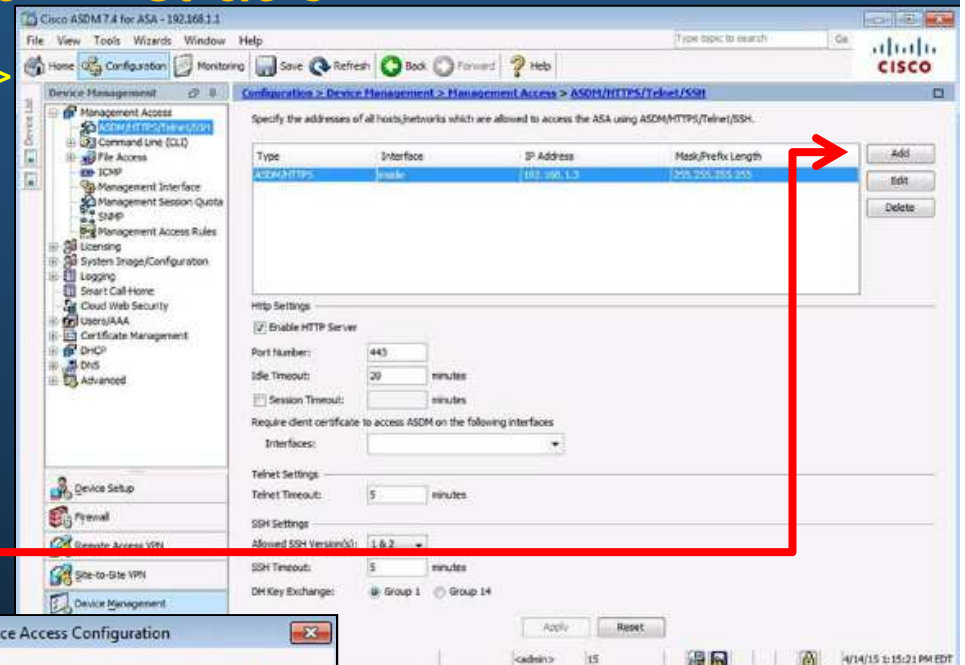
- Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH.

- Identificar Hosts para acceso al ASA.
- Vgr; Habilitar 192.168.1.3 para acceso por SSH.

- Add

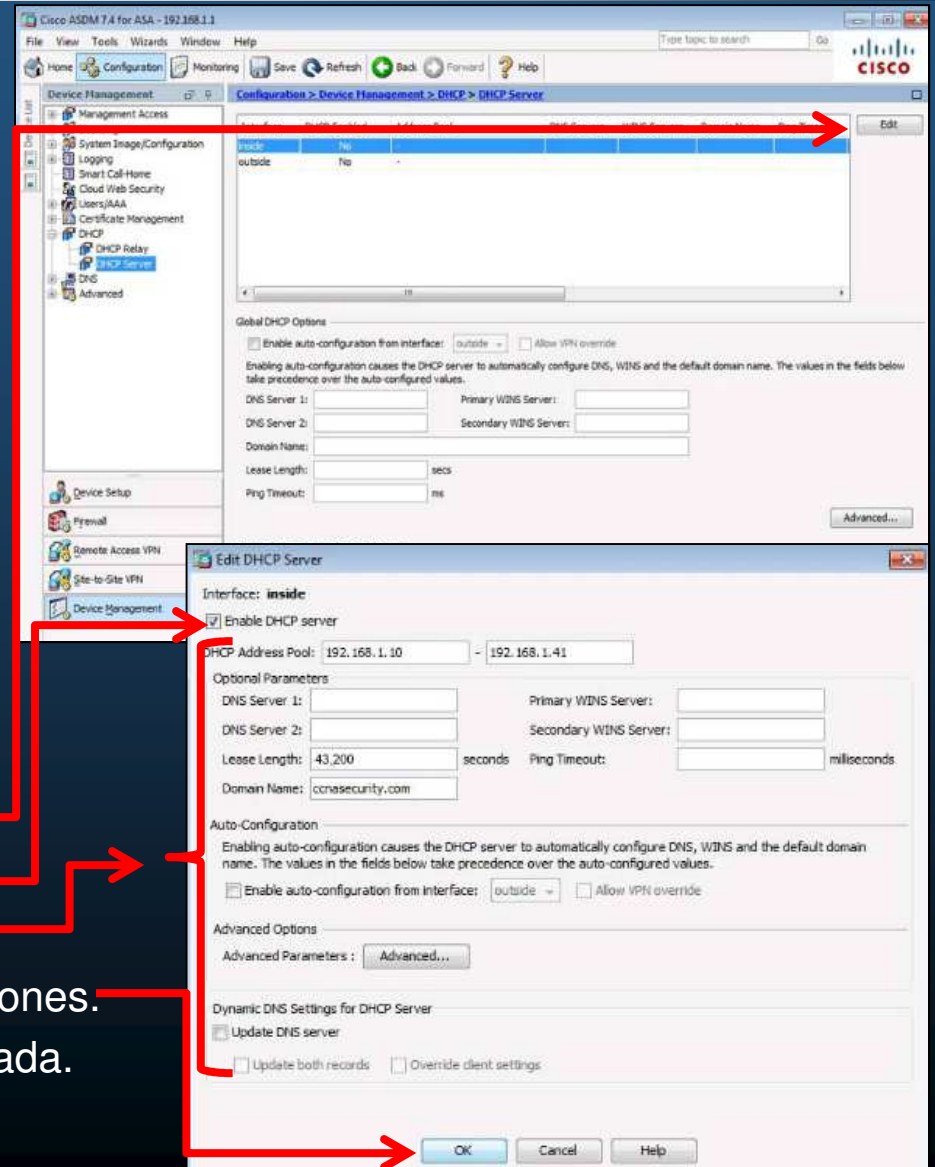
- Introducir datos del host.
- Click en Ok.

- Tras mostrar cambios.
- Aplicar



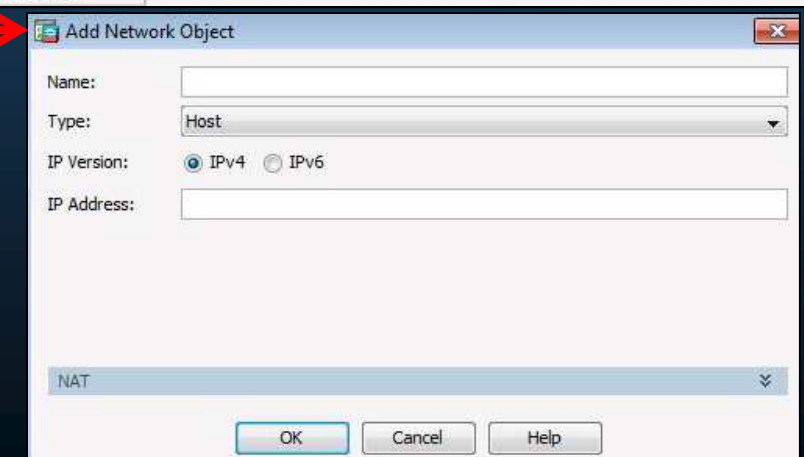
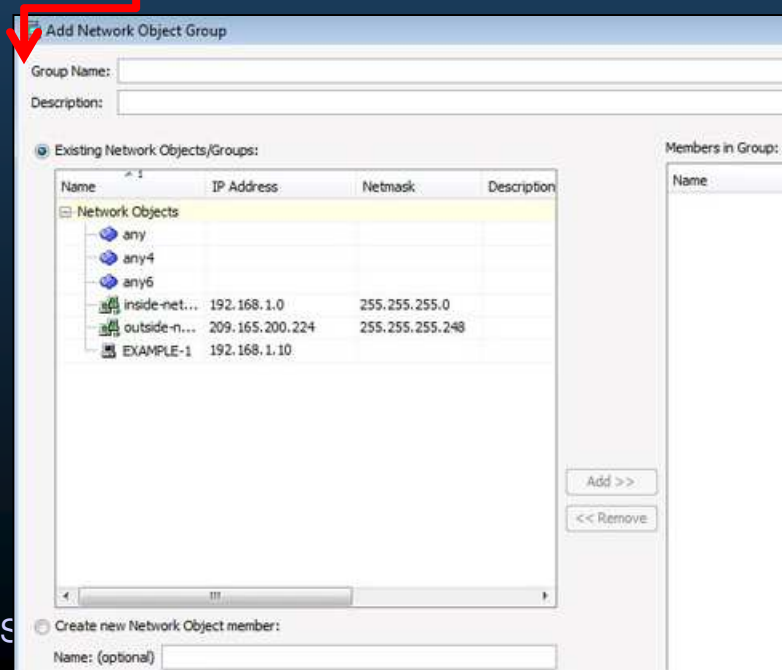
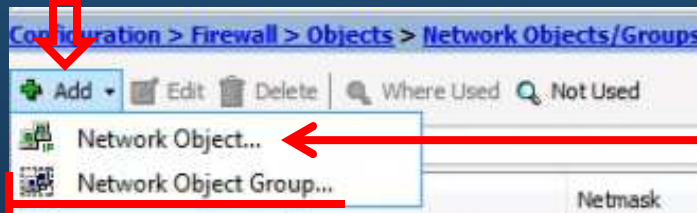
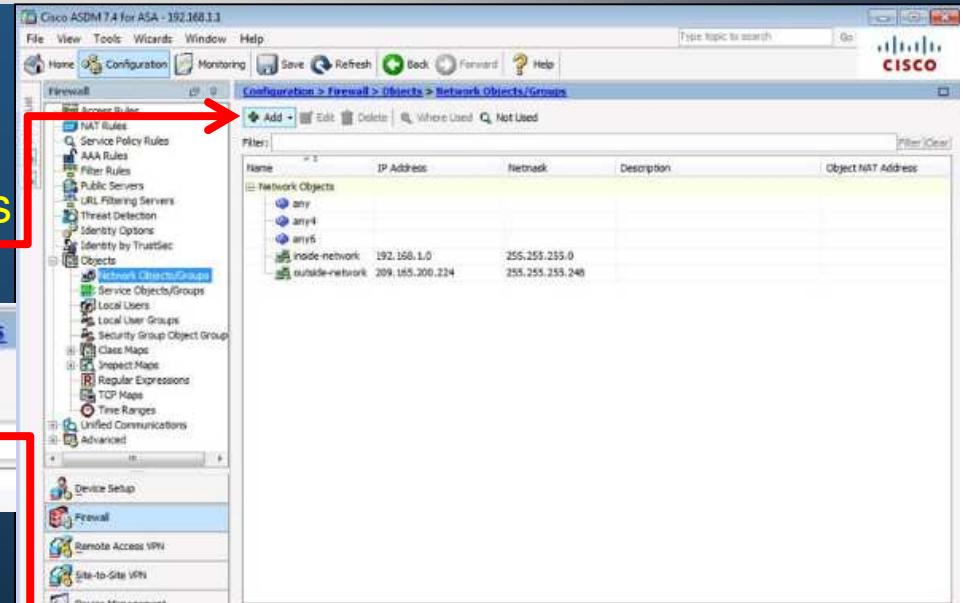
10.1 ASDM.

- 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

The screenshot illustrates the configuration path in Cisco ASDM 7.4 for ASA - 192.168.1.1. The main window shows the 'Configuration > Firewall > Objects > Service Objects/Groups' path. A red arrow points to the 'Add' button, which opens a dropdown menu with options: 'Service Object...', 'Service Group...', 'TCP Service Group...', 'UDP Service Group...', 'TCP-UDP Service Group...', 'ICMP Group...', and 'Protocol Group...'. A red arrow points from 'Service Group...' to the 'Add Service Group' dialog box. Another red arrow points from the 'Add Service Group' dialog box to the 'Add Service Object' dialog box. The 'Add Service Group' dialog box shows a list of predefined service groups: aol, bgp, chargen, cifs, citrix-ica, ctpbe, daytime, discard, domain, echo, exec, finger, ftp, ftp-data, gopher, h323. The 'Add Service Object' dialog box shows fields for Name, Service Type (tcp), Destination Port/Range, Source Port/Range, and Description.

10.1 ASDM.

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

Add Access Rule

Interface:

Action: Permit Deny

Source Criteria

Source:

User:

Security Group:

Destination Criteria

Destination:

Security Group:

Service:

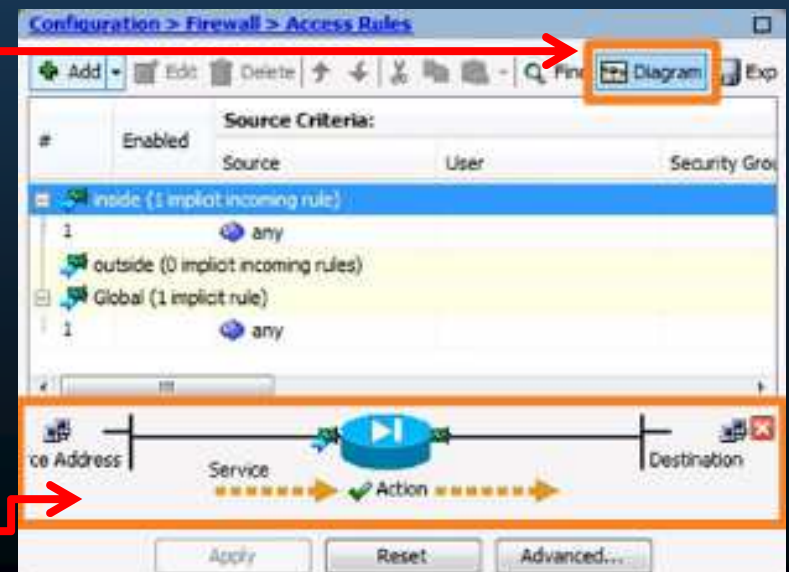
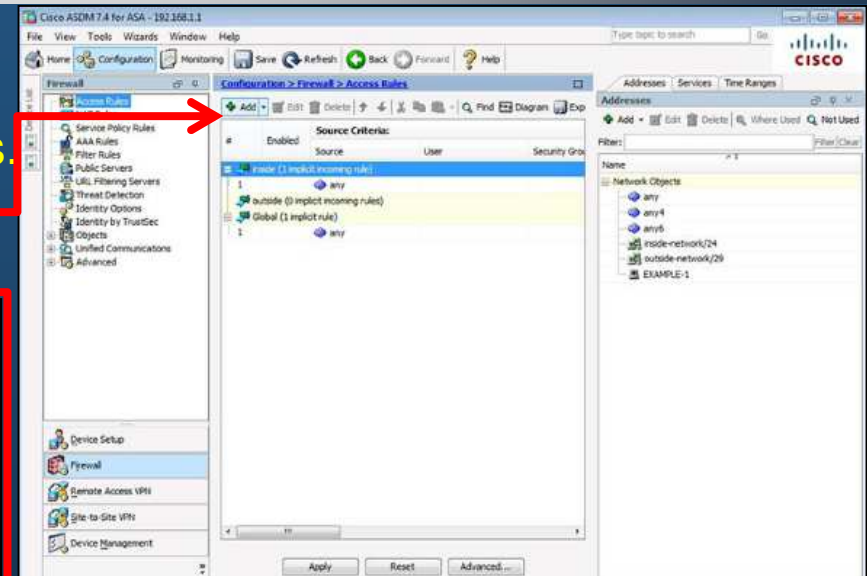
Description:

Enable Logging

Logging Level:

More Options

OK Cancel Help



- 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)

The screenshot shows the 'Add Network Object' dialog box in ASDM. The 'Name' field is 'DYNAMIC-NAT', 'Type' is 'Network', 'IP Version' is 'IPv4', 'IP Address' is '192.168.1.0', 'Netmask' is '255.255.255.224', and 'Description' is 'Inside Hosts to use Dynamic NAT'. Below this, the 'NAT' section is expanded, showing 'Add Automatic Address Translation Rules' checked, 'Type' set to 'Dynamic', and 'Translated Addr' set to 'PUBLIC'. Other options like 'Use one-to-one address translation', 'PAT Pool Translated Address', 'Round Robin', 'Extend PAT uniqueness to per destination instead of per interface', 'Translate TCP and UDP ports into flat range 1024-65535', 'Include range 1-1023', 'Fall through to interface PAT (dest intf): inside', and 'Use IPv6 for interface PAT' are unchecked. An 'Advanced...' button is visible at the bottom of the NAT section.

The screenshot shows the 'Add Network Object' dialog box in ASDM. The 'Name' field is 'PUBLIC', 'Type' is 'Range', 'IP Version' is 'IPv4', 'Start Address' is '209.165.200.240', 'End Address' is '209.165.200.248', and 'Description' is 'List of valid public IP addresses to be used by Dynamic NAT'. A 'NAT' dropdown menu is visible at the bottom of the dialog box.

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.

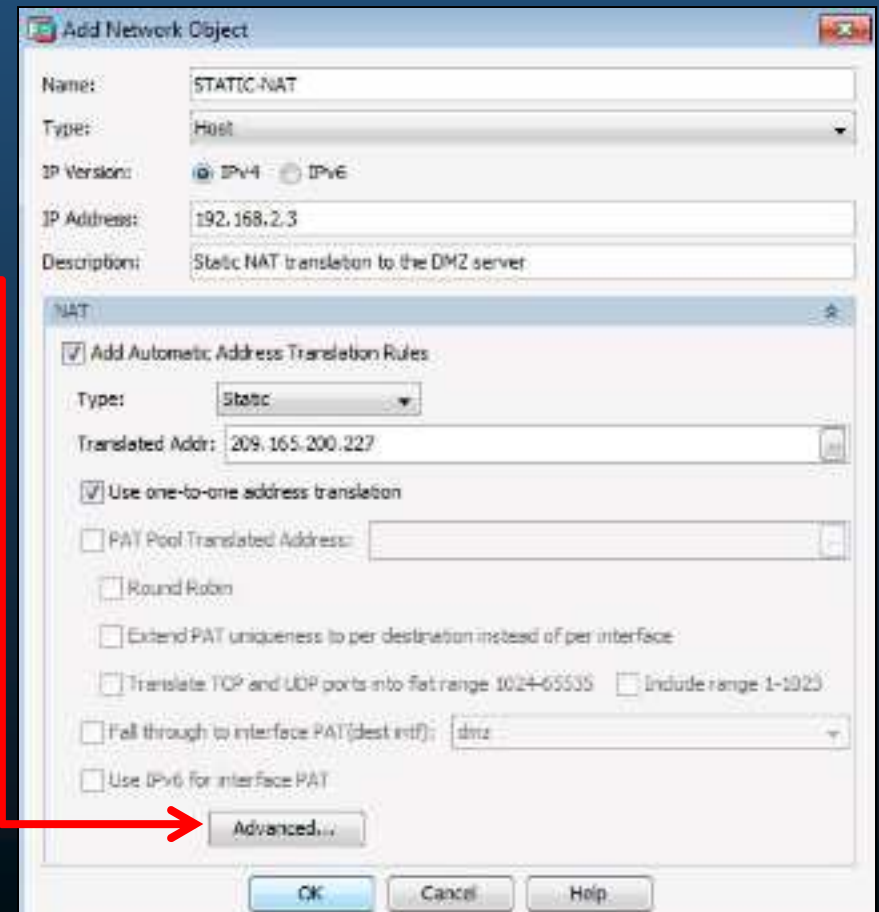
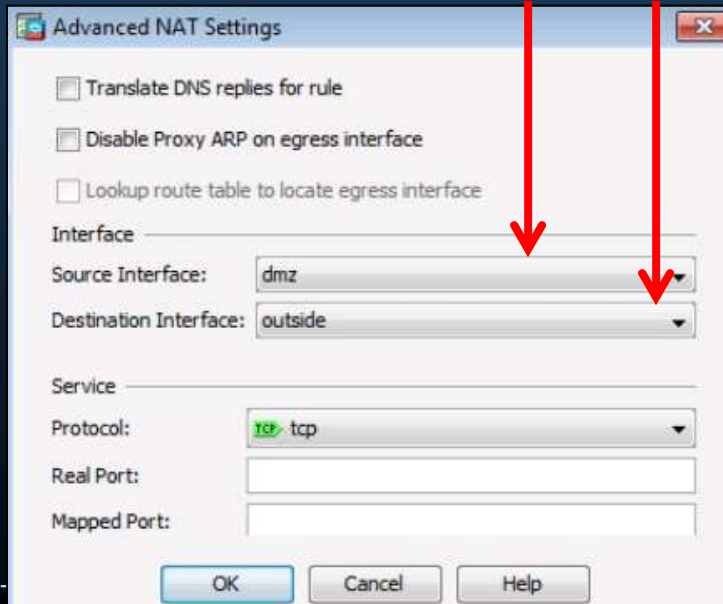
The screenshot shows the 'Add Network Object' dialog box in ASDM. The 'Name' field is 'DYNAMIC-PAT', 'Type' is 'Host', 'IP Version' is 'IPv4', 'IP Address' is '192.168.1.0', and 'Description' is '255.255.255.224'. The 'NAT' section is expanded, showing 'Add Automatic Address Translation Rules' checked, 'Type' set to 'Dynamic PAT (hide)', and 'Translated Addr' set to 'outside'. There are 'OK', 'Cancel', and 'Help' buttons at the bottom.

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.

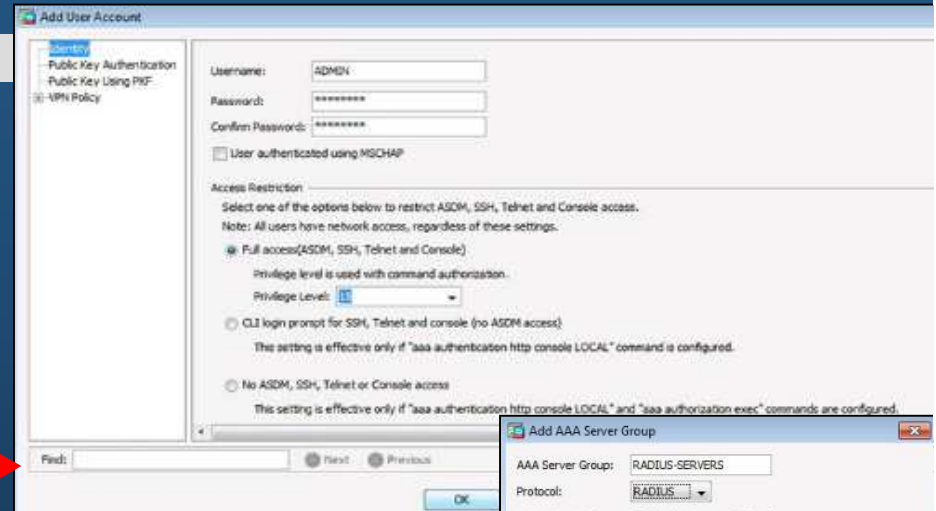


10.1 ASDM.

- **Configurar AAA en ASDM.**

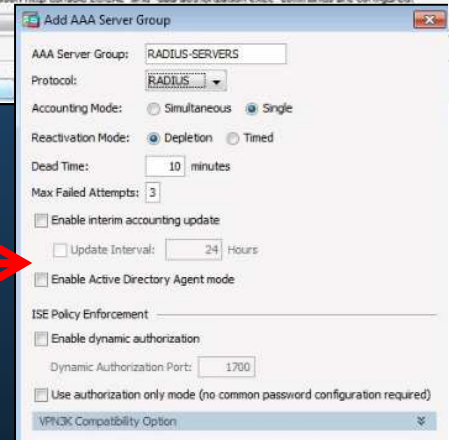
- **Paso 1. Configurar cuentas de usuarios locales.**

- Configuration > Device Management > Users/AAA > User Accounts > Add
- > Entrar datos para crear usuario. →



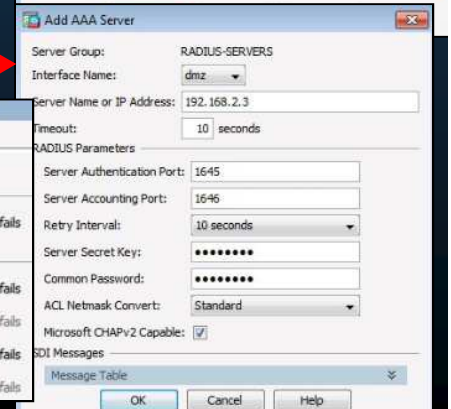
- **Paso 2. Crear grupo de servidores AAA.**

- 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.**

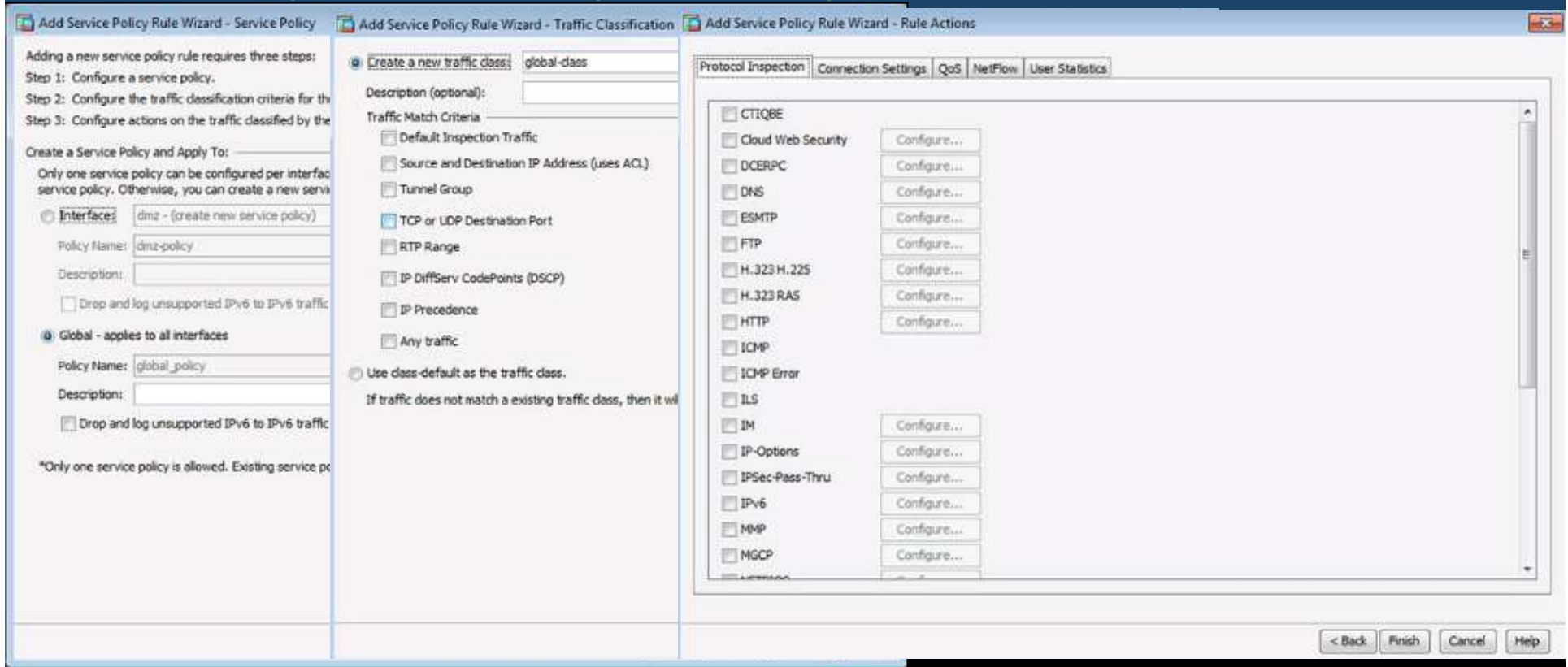
- Configuration > Device Management > Users/AAA > AAA Access →



10.1 ASDM.

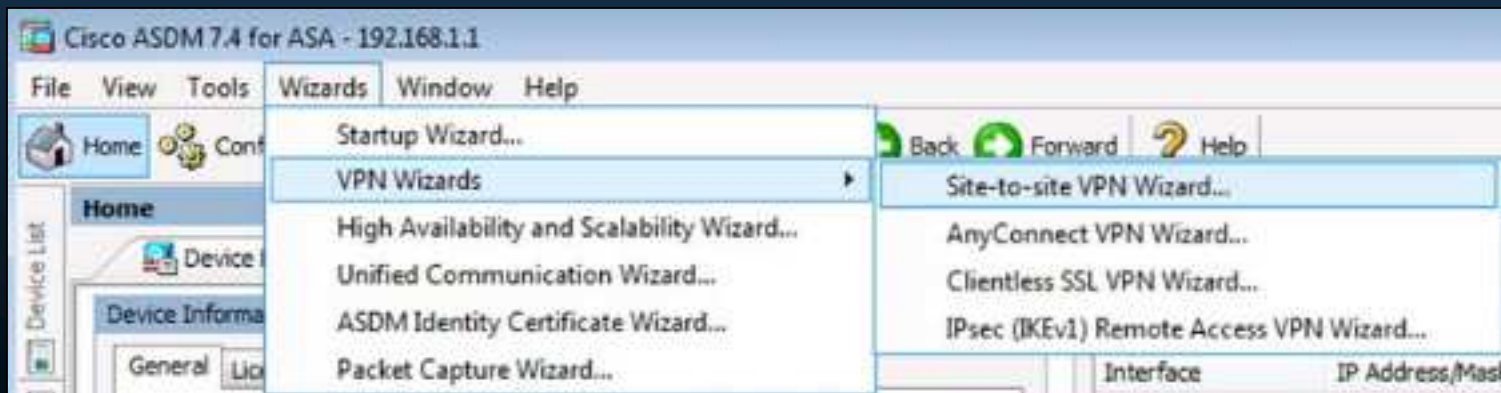
- **Configurar Servidor de Políticas con ASDM.**

- **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.



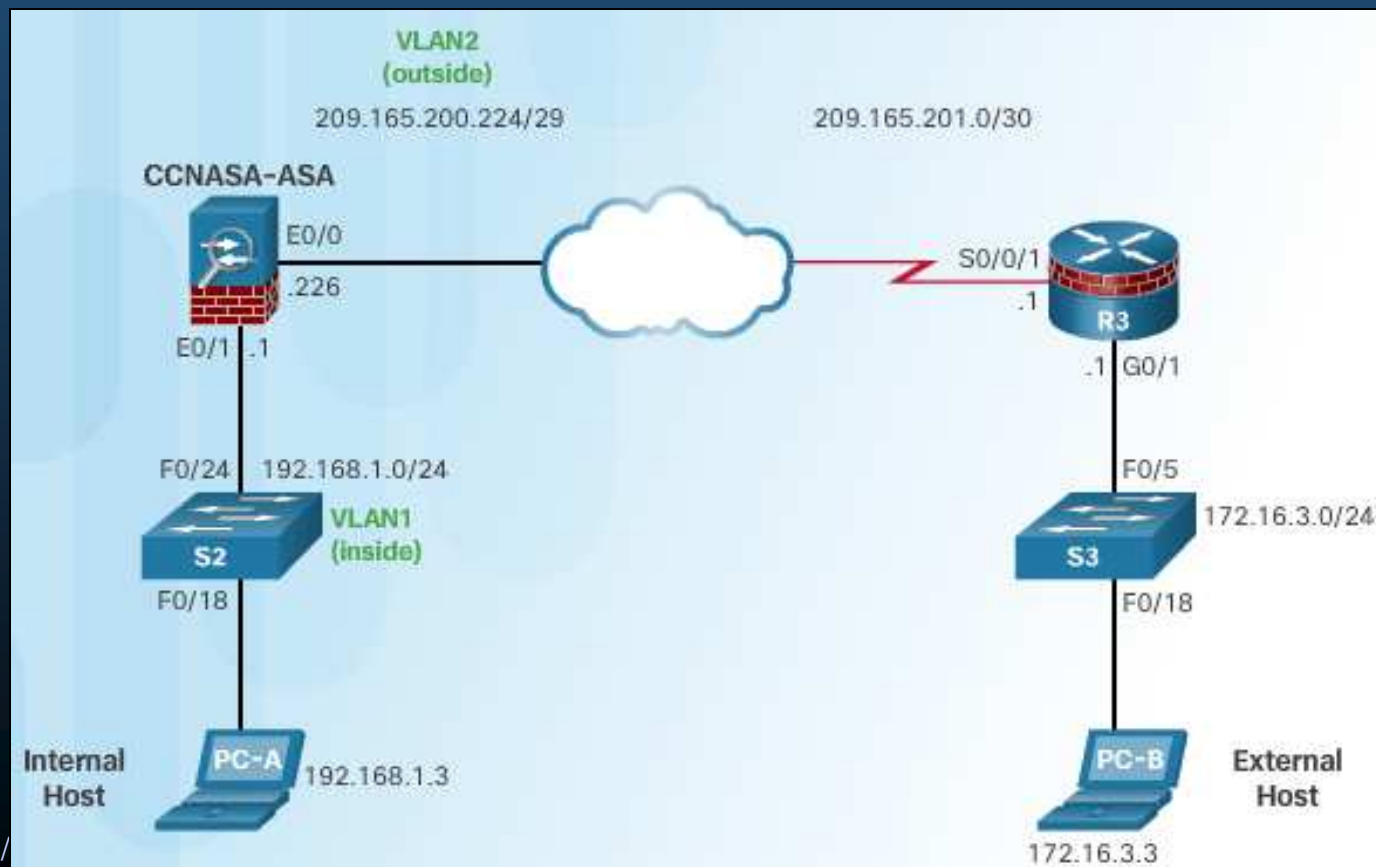
10.2 Configuración VPN en ASA.

- 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.

```
CCNAS-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)#
```

0. Configuración Básica

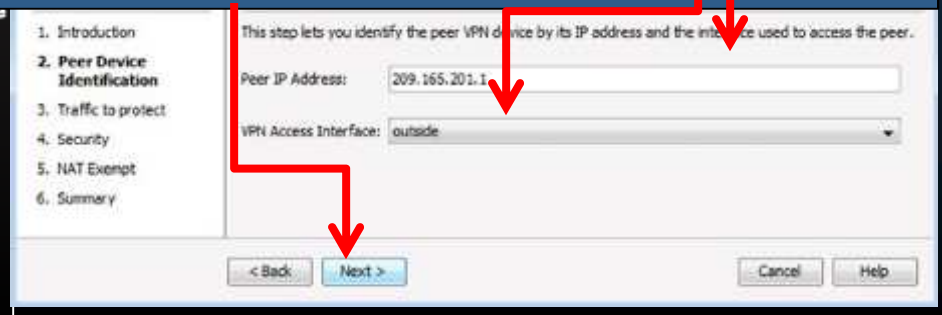


1. Wizards > VPN Wizards > Site-to-Site VPN Wizard

→ Click en Next

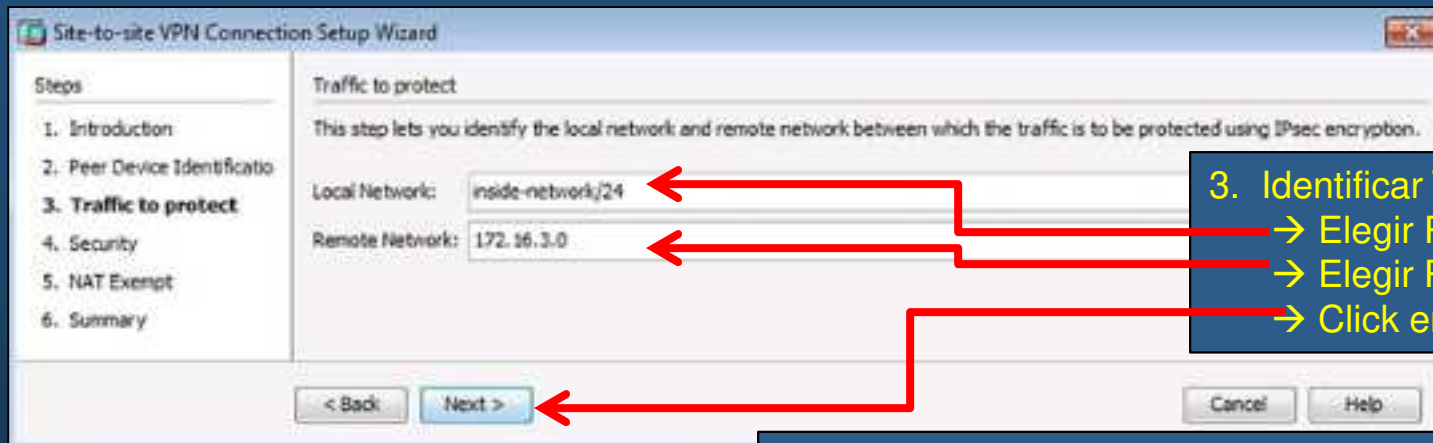
2. Identificar el dispositivo par.

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



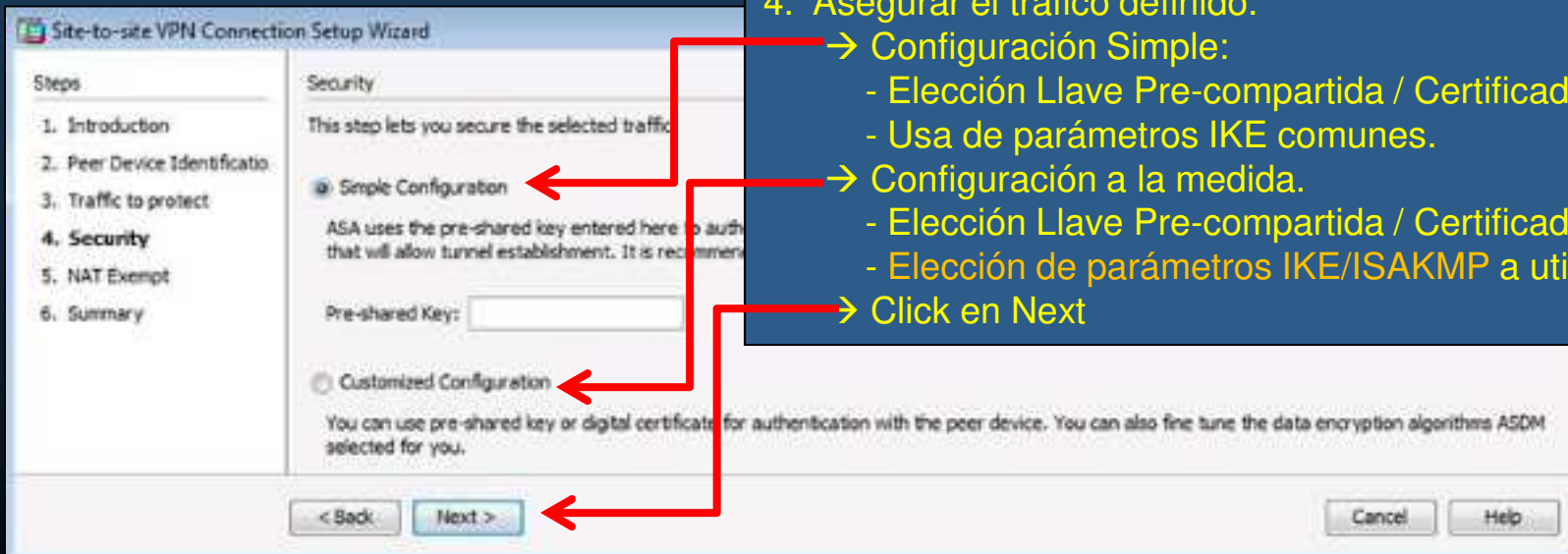
10.2 Configuración VPN en ASA.

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



3. Identificar Tráfico Interesante.

- Elegir Red Local
- Elegir Red Remota
- Click en Next

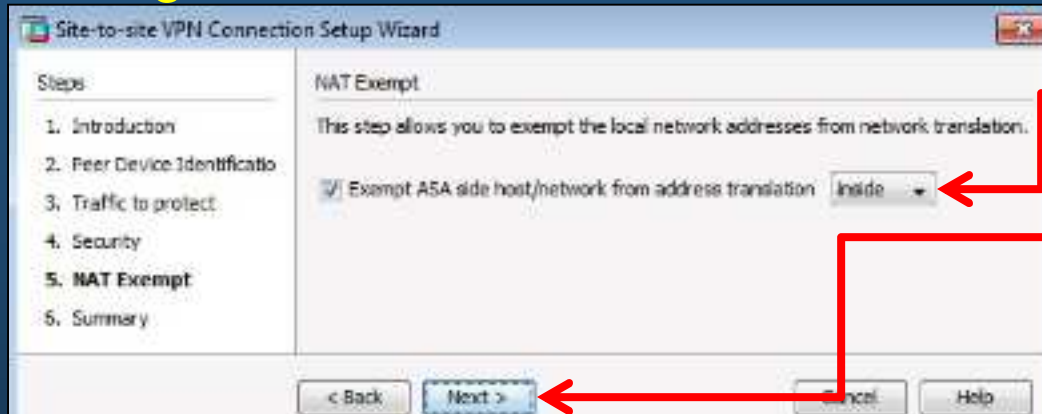


4. Asegurar el tráfico definido.

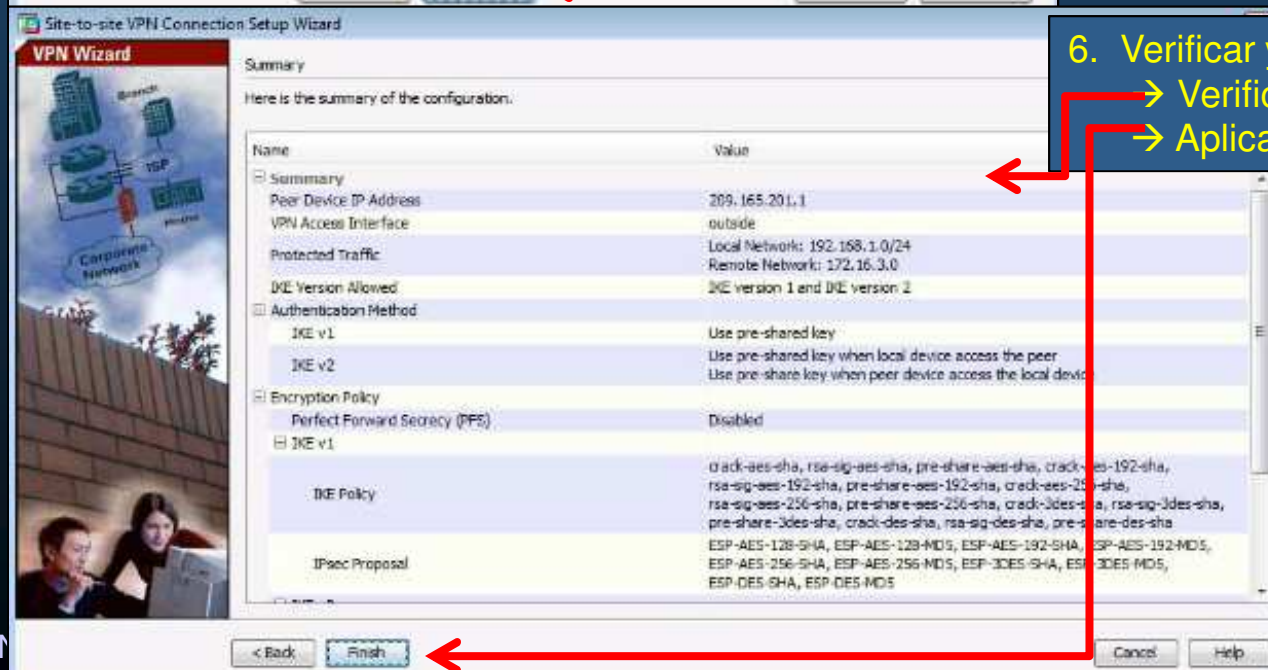
- Configuración Simple:
 - Elección Llave Pre-compartida / Certificado Digital
 - Usa de parámetros IKE comunes.
- Configuración a la medida.
 - Elección Llave Pre-compartida / Certificado Digital
 - Elección de parámetros IKE/ISAKMP a utilizar.
- Click en Next

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.

Manage site-to-site VPN connections. Here is a [video](#) on how to setup a site-to-site VPN connection.

Access Interfaces
Enable interfaces for IPsec access.

Interface	Allow IKE v1 Access	Allow IKE v2 Access
outside	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
dmz	<input type="checkbox"/>	<input type="checkbox"/>
inside	<input type="checkbox"/>	<input type="checkbox"/>

Bypass interface access lists for inbound VPN sessions
Access lists from group policy and user policy always apply to the traffic.

Connection Profiles
Connection profile identifies the peer of a site-to-site connection. It specifies what data traffic is to be encrypted, how the data traffic is to be encrypted, and other parameters. You can configure the mapping from certificate to connection profile [here](#).

Name	Interface	Local Network	Remote Network	IKEv1 Enabled	IKEv2 Enabled	Group Policy	NAT Exempt
209.165...	outside	inside-netwo...	172.16.1.0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	GroupPolicy_20...	<input checked="" type="checkbox"/>

Find: Match Case

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.

The screenshot shows the Cisco ASDM 7.4 for ASA interface. The left sidebar contains a tree view with categories like VPN Statistics, Interfaces, VPN, Routing, Properties, and Logging. The main window displays the 'Monitoring > VPN > VPN Statistics > Sessions' page. At the top, there is a summary table:

Type	Active	Cumulative	Peak Concurrent	Inactive
Site-to-Site VPN		1	1	1
IKEv1 IPsec		1	1	1

Below this is a filter section: 'Filter By: IPsec Site-to-Site' and 'All Sessions'. The main table shows active sessions:

Connection Profile	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
172.16.3.1	172.16.3.1	IKEv1 IPsec	12800-41 UTC Tue Apr 21 20:13			100	100
172.16.3.1	172.16.3.1	IKEv1 (1130ES IPsec)	1131 17:03:45				

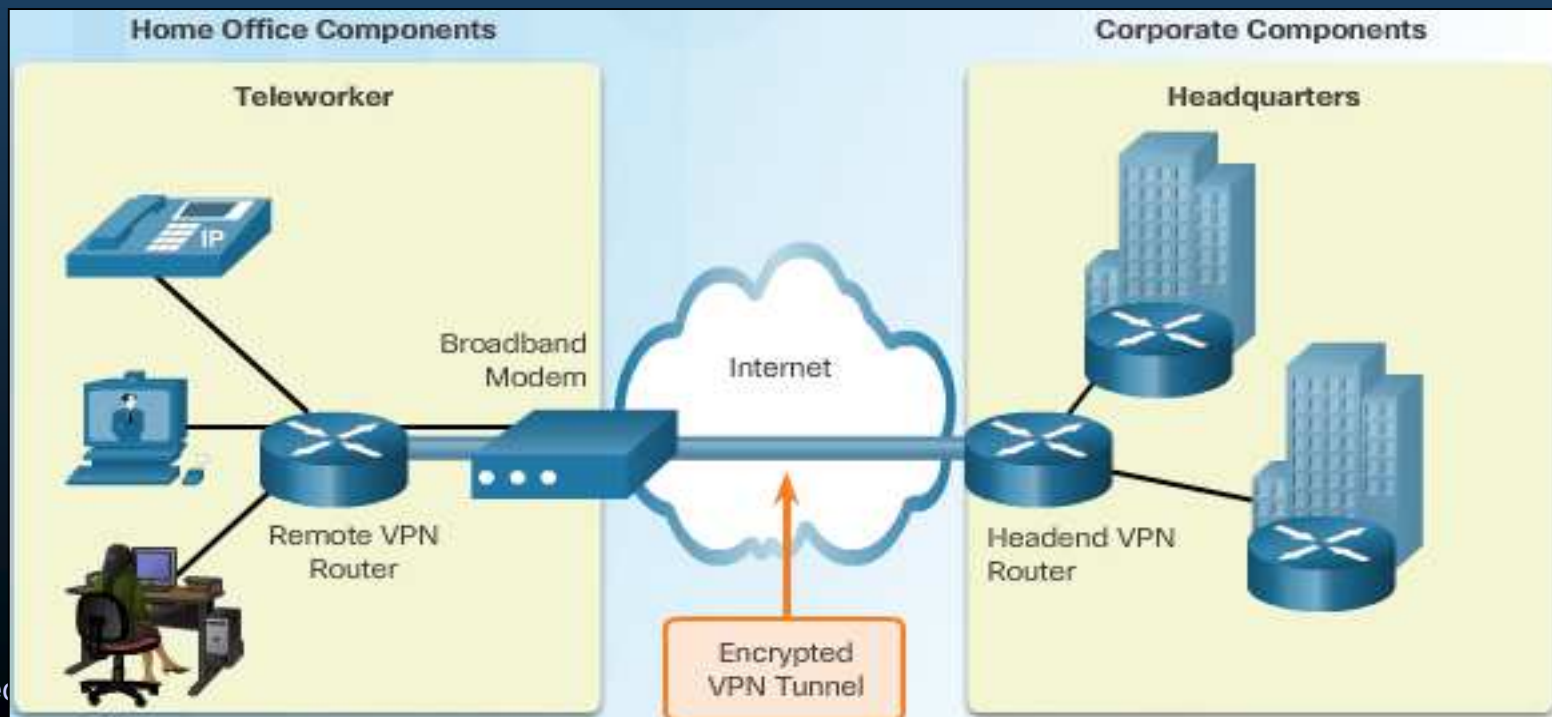
The second row of the active sessions table is circled in red. Below the table, there are options for 'Logout By: All Sessions' and a 'Logout Sessions' button. A 'Refresh' button is at the bottom. The status bar at the bottom shows 'Data Refreshed Successfully', 'ADMIN', and the time '4/21/15 10:23:17 PM UTC'.

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 transporte (Trabajadores llevan la oficina consigo).



10.2 Configuración VPN en ASA.

- IPsec vs SSL.

No son excluyentes sino complementarias.

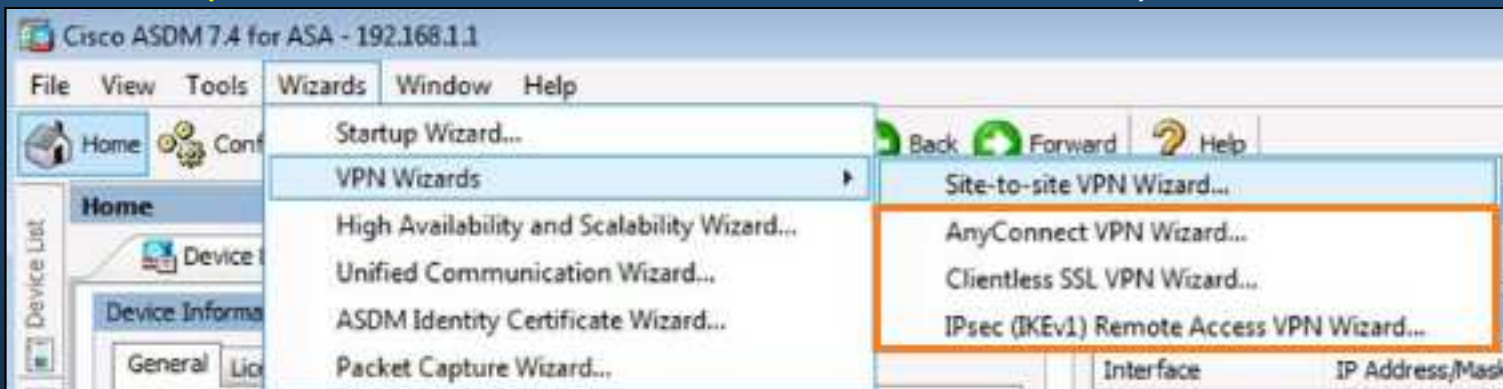
- Principales tecnologías para VPNs de acceso remoto.
 - IPsec. Solución convencional para accesos remotos por teletrabajadores.
 - SSL. Diseñada (1990s) para habilitar comunicaciones http seguras.
 - 1. El cliente y servidor negocian autenticación, cifrado y llaves.
 - 2. Servidor envía certificado 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

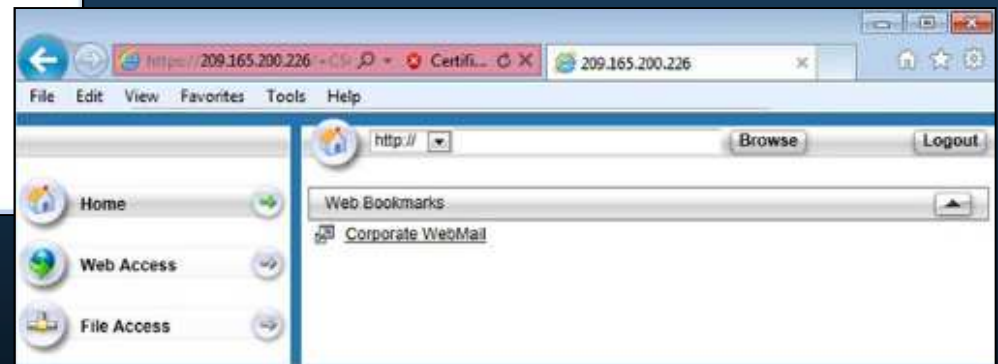
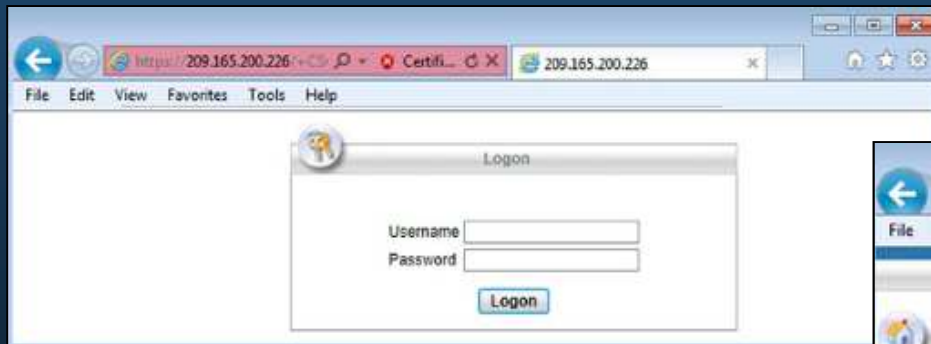
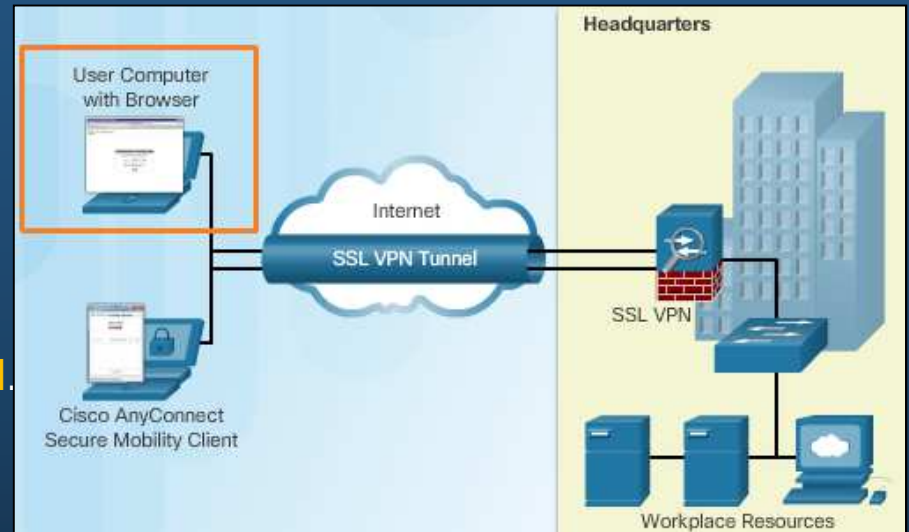
- Soportadas por ISR y ASA (ASA puede soportar hasta 10,000 conexiones).
 - Tres tipos de soluciones, cada una con un asistente disponible:



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

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.



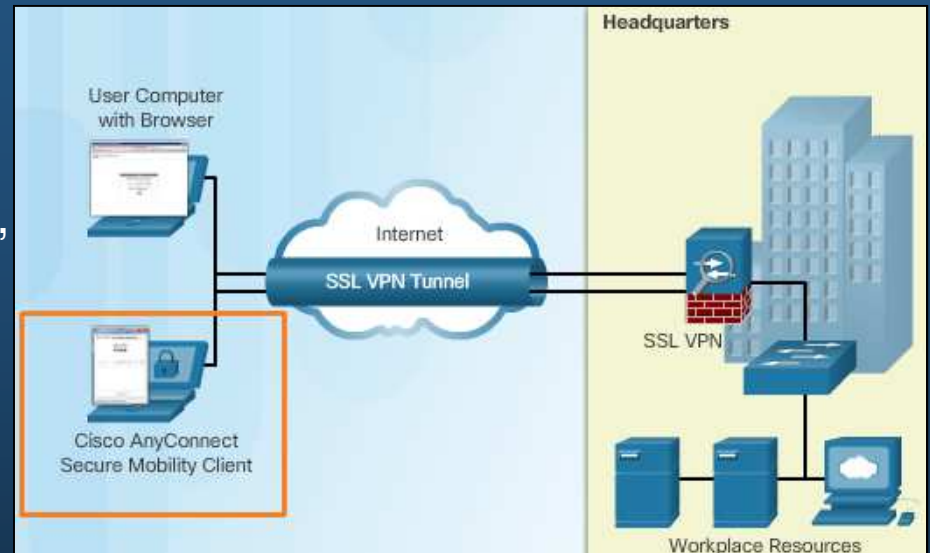
- Tras autenticarse, los usuarios acceden a recursos internos de la corporación mediante web.
- ASA funge como servidor proxy a los recursos de red y genera el portal web.
- Clientes requieren navegador web con capacidades SSL.
- Fácil de implementar vs Acceso limitado a recursos y Riesgos de Seguridad.

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.

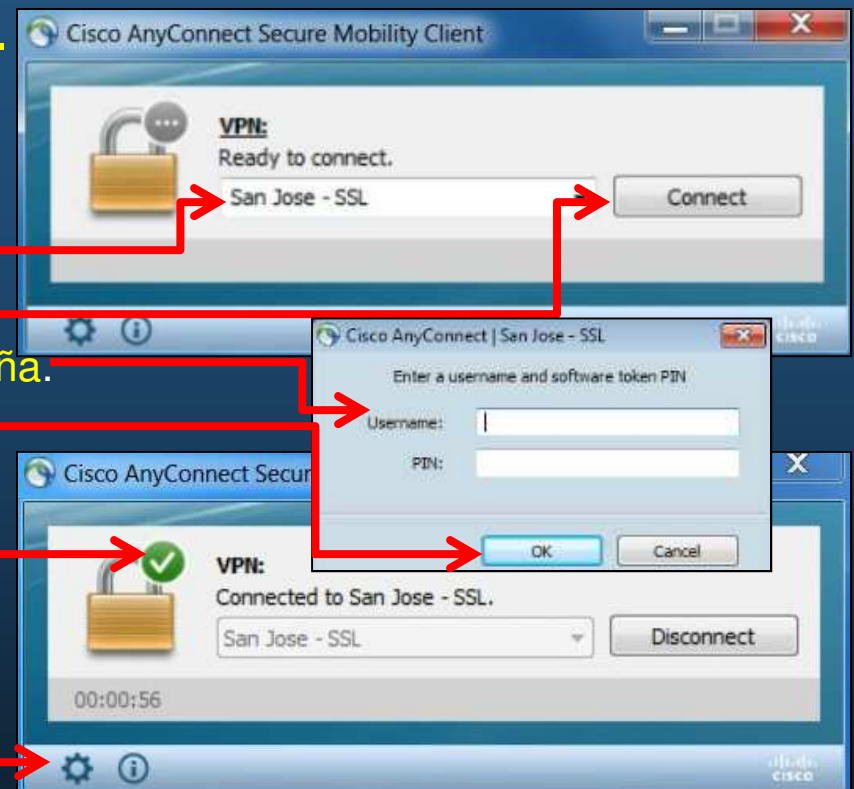


10.2 Configuración VPN en ASA.

- 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:

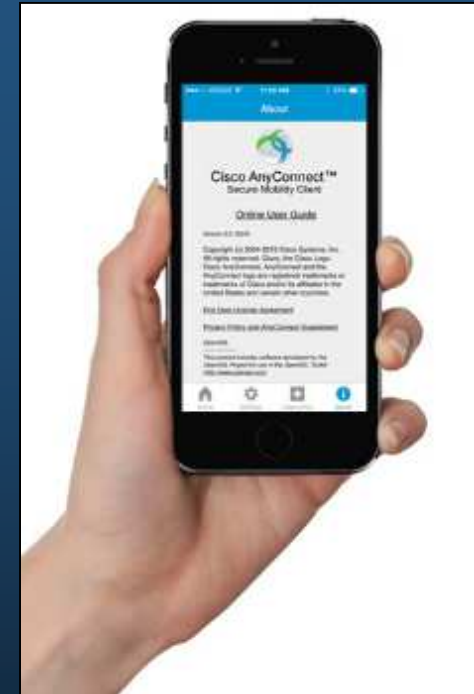
- iOS (iPhone, iPad, y iPod Touch)
 - Android
 - BlackBerry
 - Windows Mobile

- Solo disponible para determinados modelos.

- Incluido como App nativa por algunas marcas.

- Mas información:

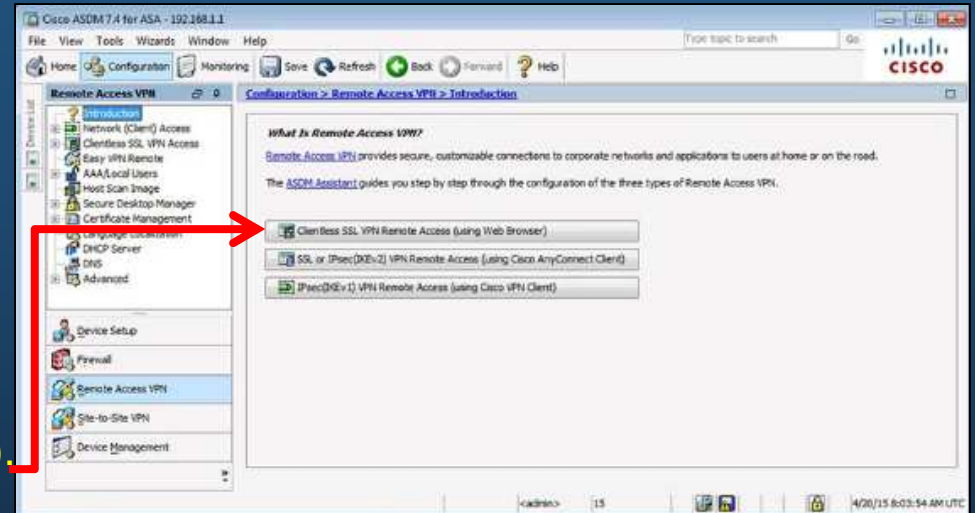
- <http://www.cisco.com/c/en/us/products/security/anyconnect-secure-mobility-client/index.html>



10.2 Configuración VPN en ASA.

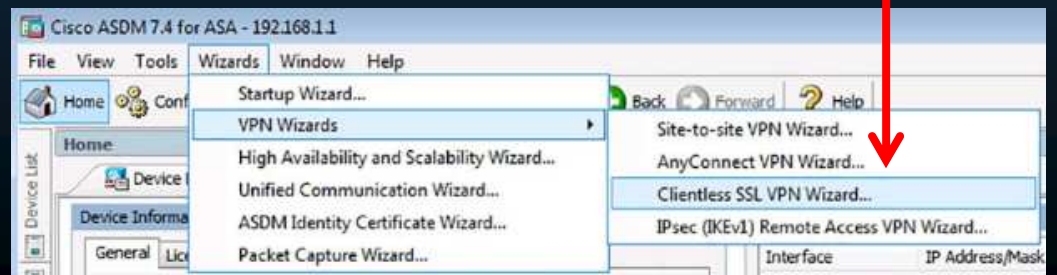
- Configuración de VPN SSL Sin Clientes en ASA.

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



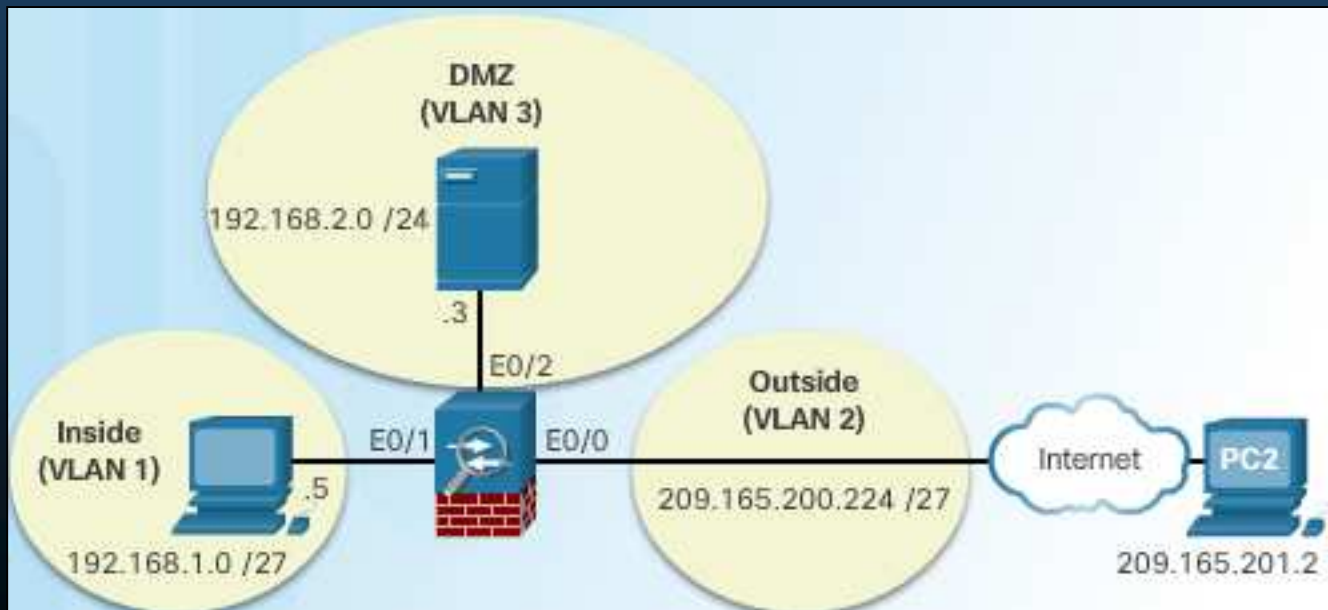
- Asistente VPN: Simplifica la configuración de la VPN SSL.
 - Wizards > VPN Wizards > Clientless SSL VPN Wizard

- 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.

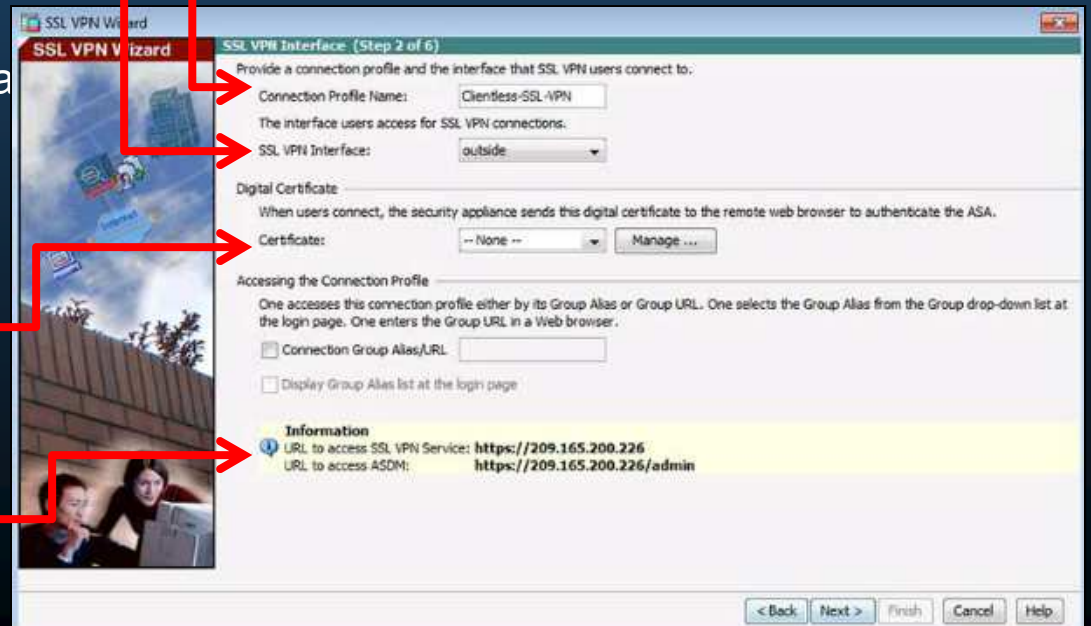
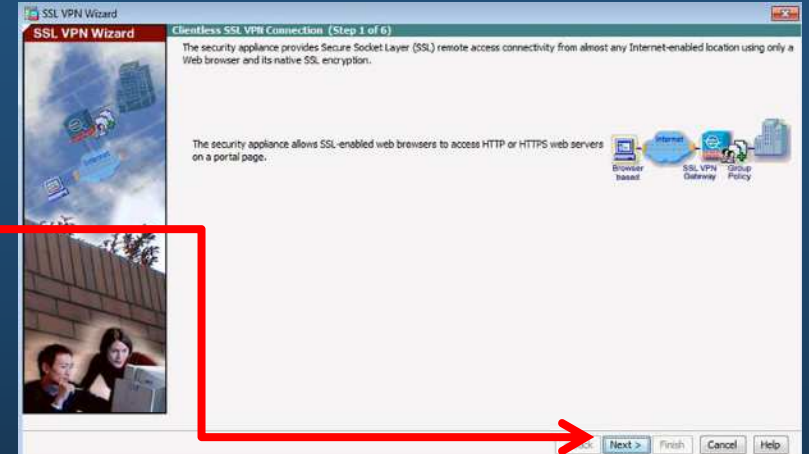
• Creación de VPN SSL Sin Clientes en ASDM.

- 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.

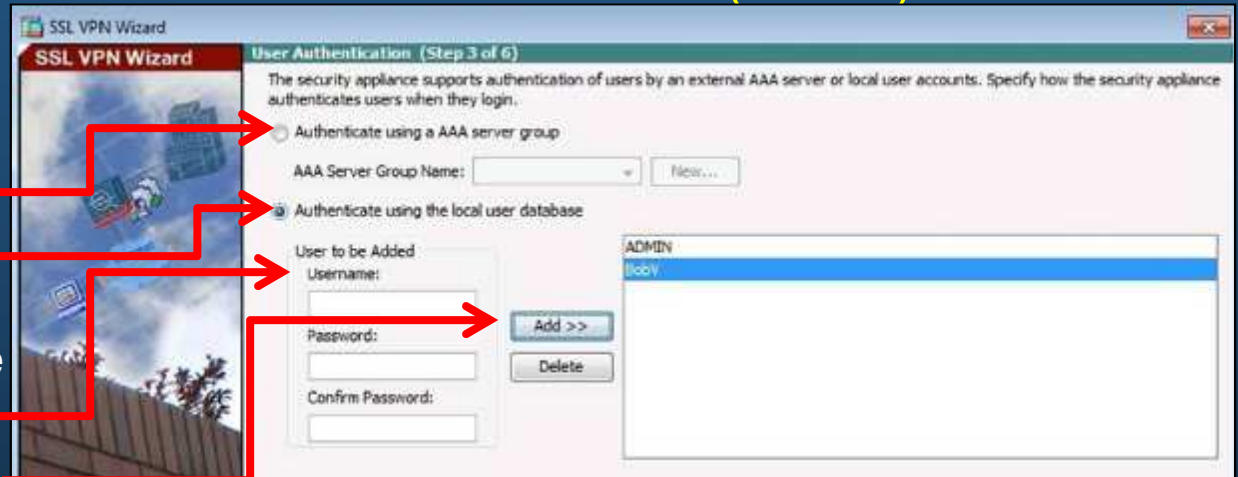


10.2 Configuración VPN en ASA.

• 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.

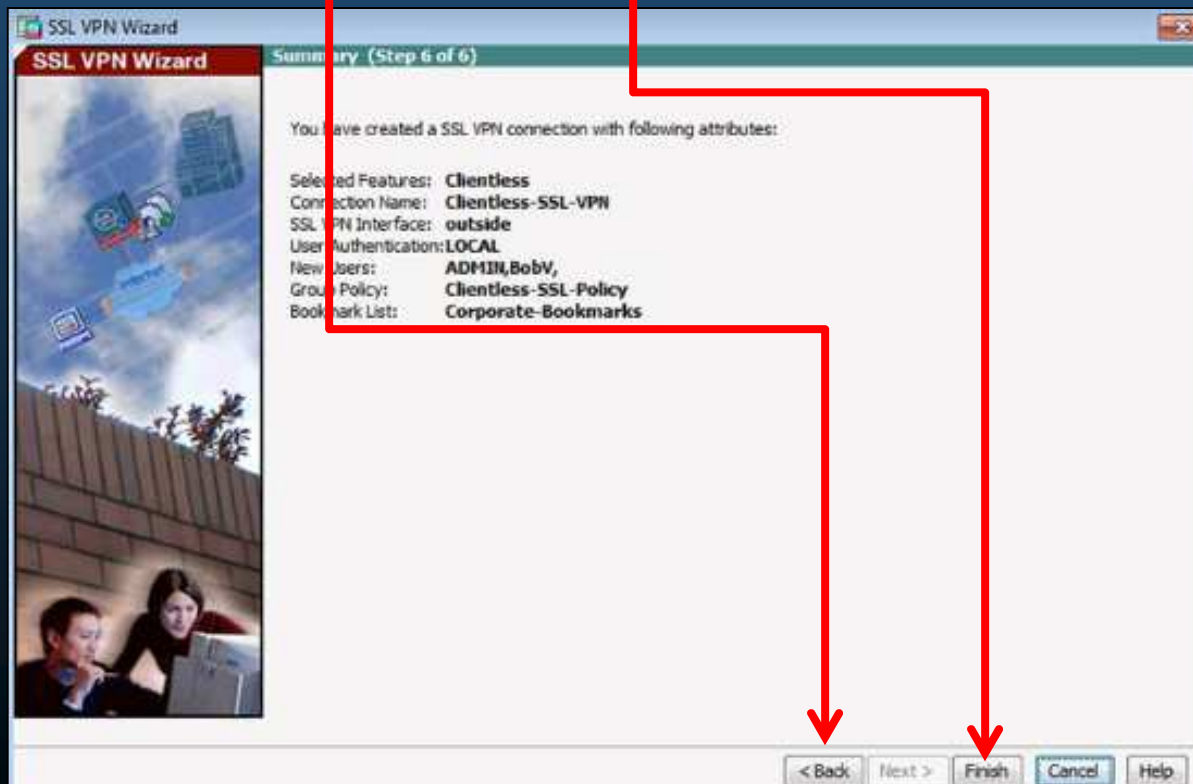
- Crear nueva política de grupo.
 - El nombre no debe tener espacios.
- Modificar política de grupo existente.

Modificar configuraciones 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.).
 - 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.

The screenshot shows the Cisco ASDM 7.4 interface for configuring Clientless SSL VPN Access. The left sidebar shows the navigation tree with 'Remote Access VPN' selected. The main pane displays the 'Connection Profiles' configuration page. The 'Access Interfaces' section has a table for enabling interfaces for clientless SSL VPN access:

Interface	Allow Access
outside	<input checked="" type="checkbox"/>
dmz	<input type="checkbox"/>
inside	<input type="checkbox"/>

Below this table, there are buttons for 'Device Certificate ...' and 'Port Setting ...'. A checkbox 'Bypass interface access lists for inbound VPN sessions' is checked. The 'Login Page Setting' section has three unchecked checkboxes: 'Allow user to select connection profile on the login page.', 'Allow user to enter internal password on the login page.', and 'Shutdown portal login page.'. The 'Connection Profiles' section includes a table of existing profiles:

Name	Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	<input checked="" type="checkbox"/>		AAA(LOCAL)	DfltGrpPolicy
DefaultVEEVPNGroup	<input checked="" type="checkbox"/>		AAA(LOCAL)	DfltGrpPolicy
Clientless-SSL-VPN	<input checked="" type="checkbox"/>		AAA(LOCAL)	Clientless-SSL-Policy

At the bottom of the page, there are 'Apply' and 'Reset' buttons.

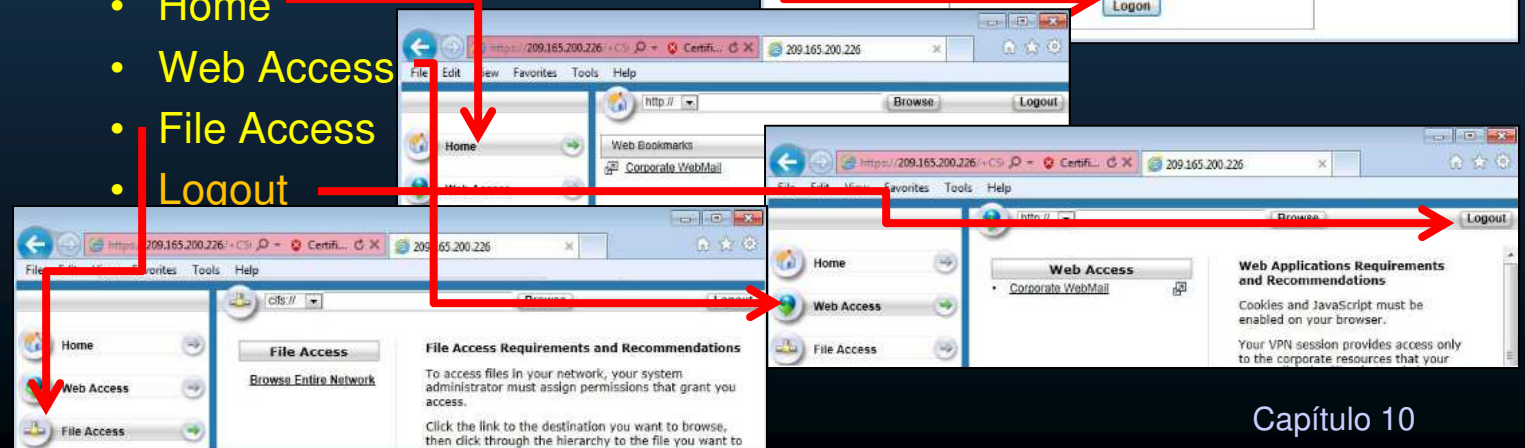
10.2 Configuración VPN en ASA.

- 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 AOvleG/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 Tunnel:

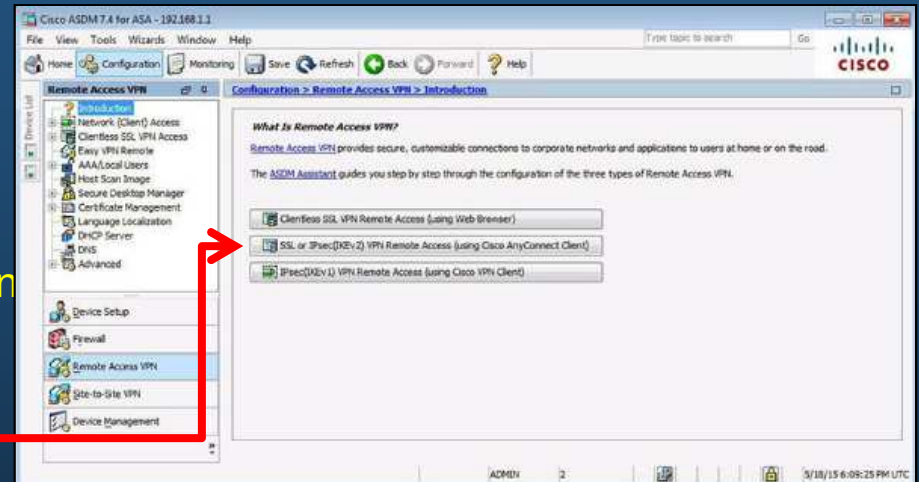
- Los usuarios se conectan por IPsec o SSL.
- Especifica los atributos que el usuario hereda por defecto.

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

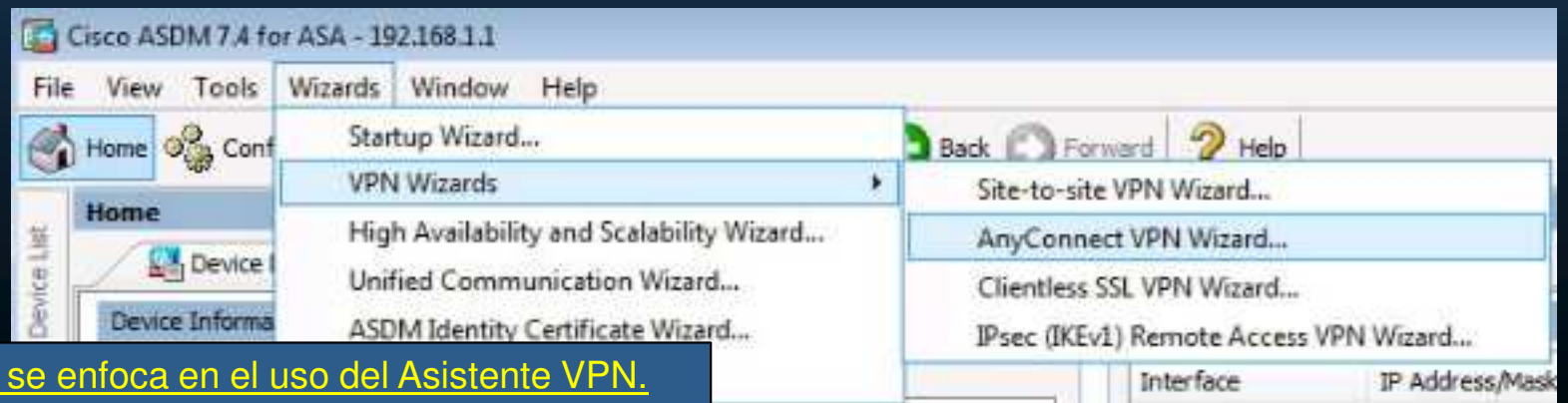
10.2 Configuración VPN en ASA.

- 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)



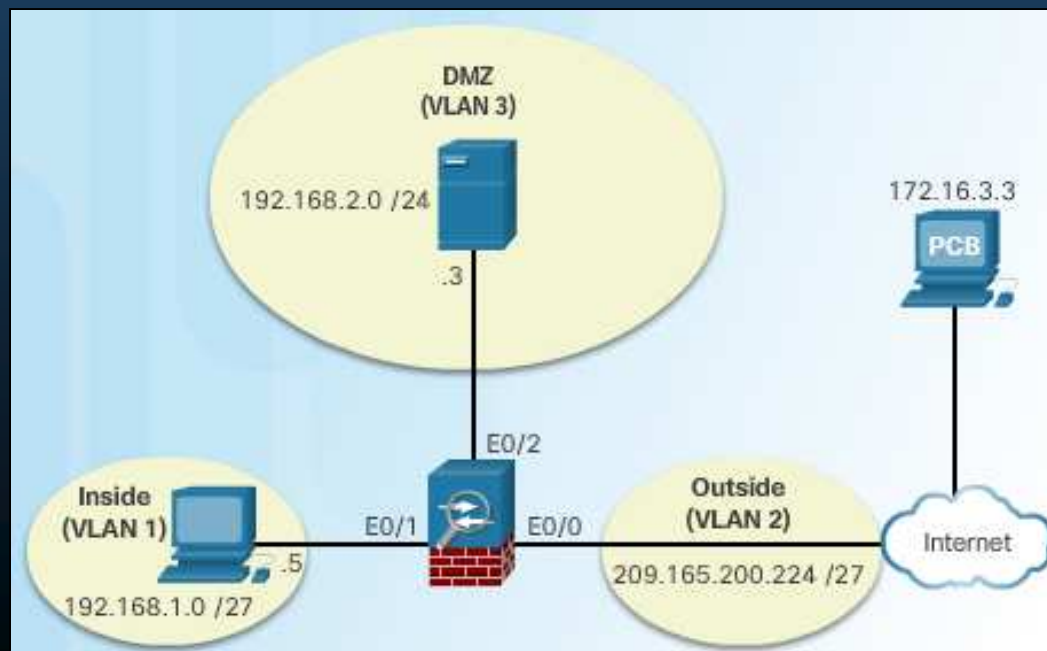
- Asistente VPN: simplifica la configuración de VPN por SSL.
 - Wizards > VPN Wizards > AnyConnect VPN Wizard.



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

10.2 Configuración VPN en ASA.

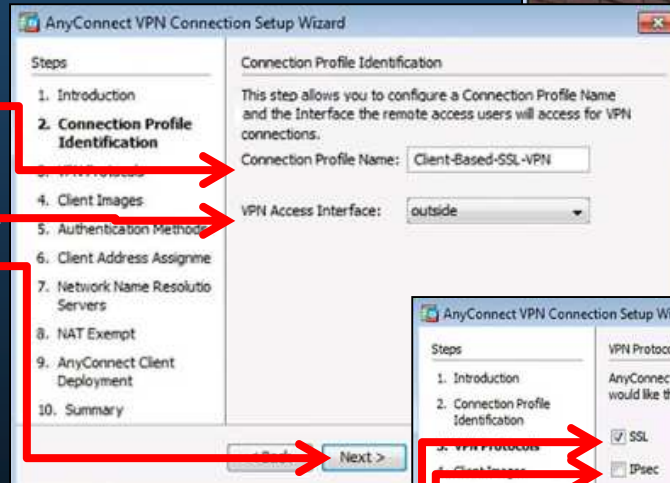
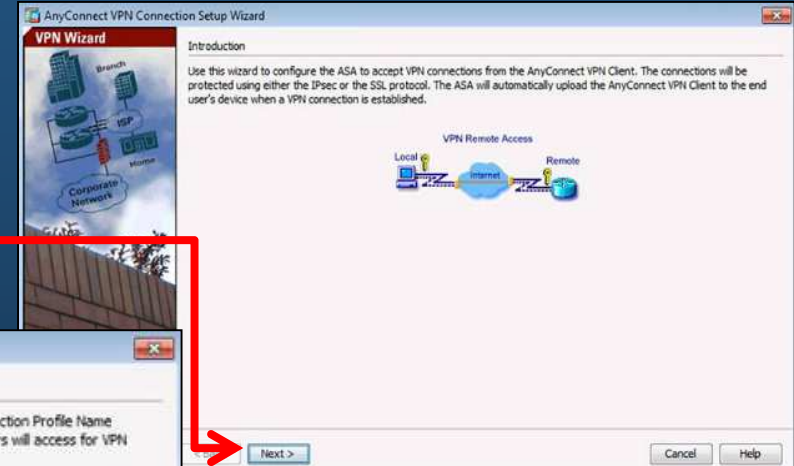
- Topología de Ejemplo para VPN SSL AnyConnect.
 - Una red interna con nivel de seguridad 100.
 - Una zona DMZ con nivel de seguridad 50.
 - Acceso a servidor mediante NAT estático.
 - Una red exterior con nivel de seguridad 0.
 - Un host externo que requiere acceso a la red interna.
 - No cuenta con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



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.

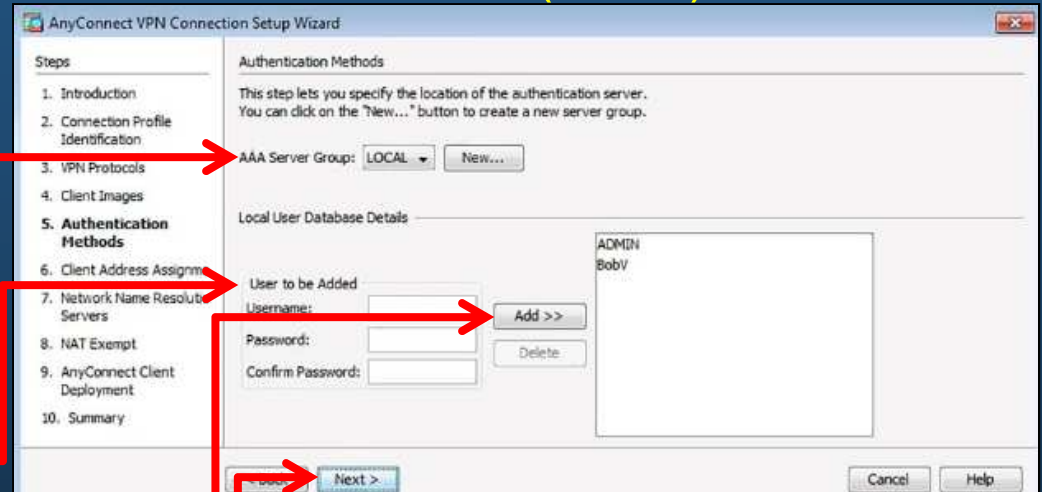
The screenshot shows the 'AnyConnect VPN Connection Setup Wizard' in ASDM. The 'Client Images' step is active, showing a list of client images. A 'Browse Flash' dialog is open, displaying a file list with 'anyconnect-win-2.5.2014-k9.pkg' selected. A 'Add AnyConnect Client Image' dialog is also open, showing the selected file path 'disk0:/anyconnect-win-2.5.2014-k9.pkg' in the 'AnyConnect Image' field. Red arrows indicate the flow of the configuration process.

FileName	Size (bytes)	Date Modified
coredumpinfo		08/29/11 13:52:54
log		08/29/11 13:55:46
crypto_archive		08/29/11 13:55:28
sdesktop		08/29/11 14:00:18
anyconnect-linux-2.5.2...	6,689,498	08/29/11 14:00:22
anyconnect-macosx-i3...	6,487,517	08/29/11 14:00:20
anyconnect-win-2.5.20...	4,678,691	08/29/11 14:00:26
asa923-k8.bin	30,468,096	02/14/15 00:10:24
asdm-741.bin	26,350,916	03/27/15 00:03:04
csd_3_5_2008-k9.pkg	12,998,641	08/29/11 14:00:16
nat_ident_migrate	0	08/29/11 14:00:26
original	1,863	09/13/11 15:51:50

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. 6

• New.

- Dar Nombre.
- Dirección IP de Inicio.
- Dirección IP Final.
- Mascara de Subred.

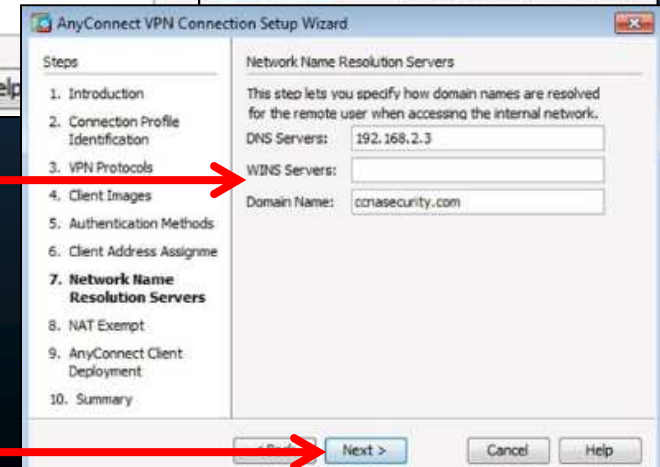
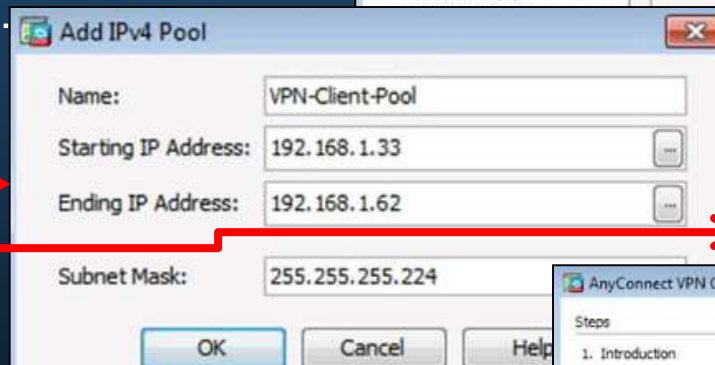
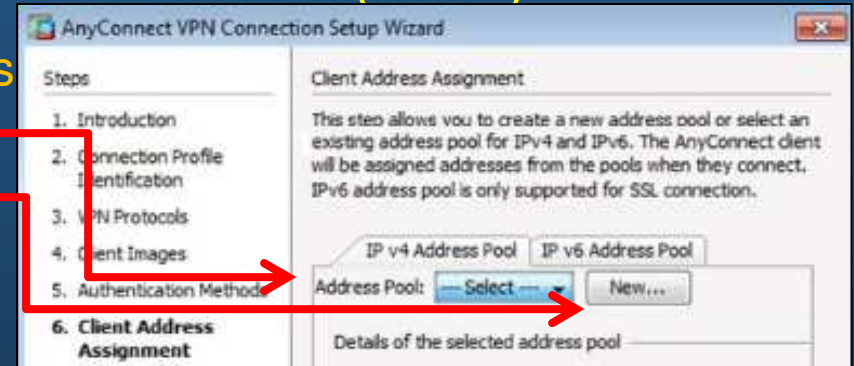
• OK

• 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 exentos de NAT. Pues al encriptar ya conocen la IP interna.

• Exempt VPN traffic...

• Inside Interface.

• Direcciones Accesibles.

• Next.

AnyConnect VPN Connection Setup Wizard

Steps

1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. Client Address Assignment
7. Network Name Resolution Servers
8. NAT Exempt
9. AnyConnect Client Deployment
10. Summary

NAT Exempt

If network address translation is enabled on the ASA, the VPN traffic must be exempt from this translation.

Exempt VPN traffic from network address translation

Inside Interface is the interface directly connected to your internal network.

Inside Interface:

Local Network is the network address(es) of the internal network that client can access.

Local Network:

The traffic between AnyConnect client and internal network will be exempt from network address translation.

< Back Next > Cancel Help

• 9. Implantación de Cliente AnyConnect.

- Información para Descargar AnyConnect en clientes.

• Next.

• 10. Verificar y Guardar.

- Back si hay cambios / Finish para guardar.

AnyConnect VPN Connection Setup Wizard

Steps

1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. Client Address Assignment
7. Network Name Resolution Servers
8. NAT Exempt
9. AnyConnect Client Deployment
10. Summary

AnyConnect Client Deployment

AnyConnect client program can be installed to a client device by one of the following two methods:

- 1) Web launch - On accessing the ASA using a Web Browser, the AnyConnect client package will be automatically installed.
- 2) Pre-deployment - Manually install the AnyConnect client package.

Next >

AnyConnect VPN Connection Setup Wizard

Summary

Here is the summary of the configuration.

Name	Value
Summary	
Name/Alias of the Connection Profile	Client-Based-SSL-VPN
VPN Access Interface	outside
Device Digital Certificate	-- none --
VPN Protocols Enabled	SSL only
AnyConnect Client Images	1 package
Authentication Server Group	LOCAL
Address Pool for the Client	192.168.1.33 - 192.168.1.62
DNS Servers	Domain Name:
Network Address Translation	The protected traffic is not subjected to network address translation

< Back Finish Cancel Help

10.2 Configuración VPN en ASA.

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

The screenshot displays the Cisco ASDM 7.4 for ASA interface. The breadcrumb navigation is 'Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles'. The main content area contains a table for 'Access Interfaces' and a table of connection profiles.

Access Interfaces Table:

Interface	SSL Access	IPsec (IKEv2) Access	Enable Client Services
any	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Connection Profiles Table:

Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	<input type="checkbox"/>	<input checked="" type="checkbox"/>		AAA(LOCAL)	DfltGrpPolicy
DefaultWEBVP...	<input type="checkbox"/>	<input checked="" type="checkbox"/>		AAA(LOCAL)	DfltGrpPolicy
Clientless-SSL+...	<input type="checkbox"/>	<input type="checkbox"/>		AAA(LOCAL)	Clientless-SSL-Policy
Client-Based-S...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Client-Based-SS...	AAA(LOCAL)	GroupPolicy_Client-Ba...

Below the table, there is a checkbox option: 'Let group URL take precedence if group URL and certificate map match different connection profiles. Otherwise, the connection profile that matches the certificate map will be used.'

10.2 Configuración VPN en ASA.

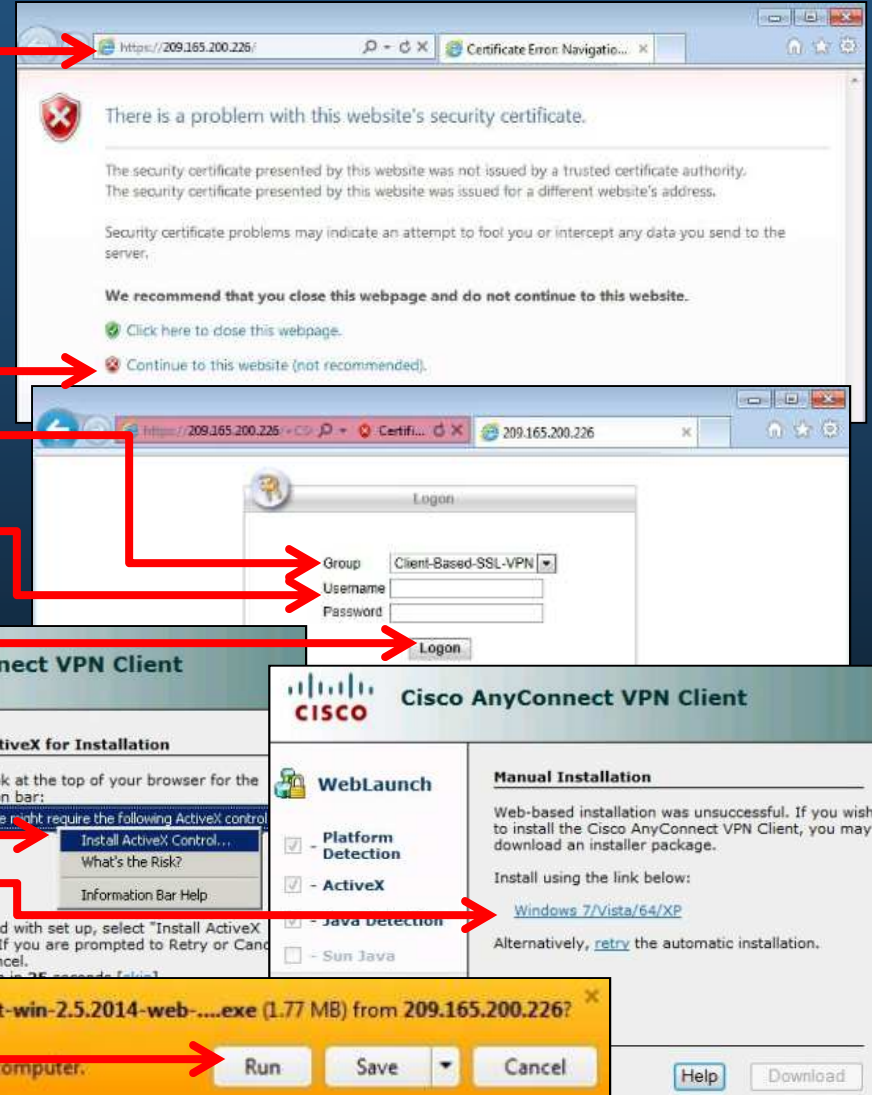
- **Instalación del Cliente AnyConnect.**

- 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.

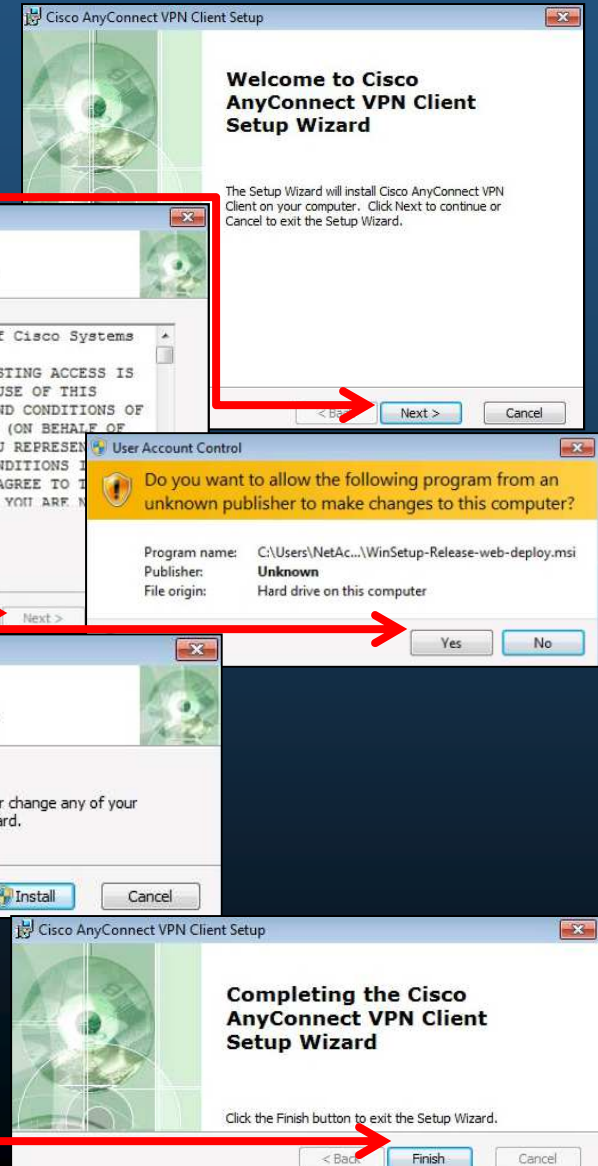
- Instalar control ActiveX para autoinstalar.
- Ó Descargar Manualmente.
 - Run para instalar.



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 Derecho) > Open AnyConnect.
- Verificar IP con ipconfig / ping

The screenshot shows the Cisco AnyConnect VPN Client interface at the top, with a 'Connection' tab selected. Below it, a Windows command prompt window displays the output of the 'ipconfig' command. The output shows two network adapters: 'Ethernet adapter Local Area Connection 3' and 'Ethernet adapter Local Area Connection'. The first adapter is labeled 'Conexión VPN.' and has an IPv4 address of 192.168.1.33. The second adapter is labeled 'Conexión LAN.' and has an IPv4 address of 172.16.3.3. Below the ipconfig output, the 'ping' command is executed, showing successful replies from 192.168.1.3 with a time of 85ms and TTL of 128. A small security alert window is also visible in the background, partially obscured by red arrows pointing to the 'ipconfig' command and the 'Connect' button in the AnyConnect client.

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

C:\Users\NetAcad> ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection 3:    Conexión VPN.

   Connection-specific DNS Suffix  . : ccnasecurity.com
   IPv4 Address. . . . . : 192.168.1.33
   Subnet Mask . . . . . : 255.255.255.224
   Default Gateway . . . . . : 192.168.1.34

Ethernet adapter Local Area Connection:    Conexión LAN.

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::70F5:f35c:59de:53a7%11
   IPv4 Address. . . . . : 172.16.3.3
   Subnet Mask . . . . . : 255.255.255.0
   Default Gateway . . . . . : 172.16.3.1

C:\Users\NetAcad> ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:
Reply from 192.168.1.3: bytes=32 time=85ms TTL=128
Reply from 192.168.1.3: bytes=32 time=84ms TTL=128
Reply from 192.168.1.3: bytes=32 time=84ms TTL=128
Reply from 192.168.1.3: bytes=32 time=84ms TTL=128
```


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 usuarios 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.