

Capítulo 10

Dispositivo Avanzado de Seguridad Adaptable de Cisco

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

CCNA Sec-1 / 65

Capítulo 10

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.

0	Home 🖓 Configuration [Honstoring 📊 Save 🚱 Refresh 🔇 Book 🔇 Fo	rward 🦻 Helo				CISCO	
12	Nome						
ET Device	Call Device Dashboard 🛛 🔮 Firewall Dashboard						
	Devce Information	Interface Status					
	General License	Interface	IP Address,Mask	ress,Mask Unie Link		Kbpe	
	Host Name: classesa AGN resion: 5-2(3) Device Lptma: 6d 6h 28im 30s ASDN Vireion: 7-4(3) Device Tym:: ASA 5505 Friend Trida: Roated Context Media: Single Tool Friend: 1284 HII Totel Memory: 522 HIII	arside	192.168.1.1/24	0 φ	О цр	1	
		Select an interface to view input and output Klops					
	VPN Sessions	traffic Status					
	Prec: 0 Clenters SS, VPI: 0 AnyConnect Clent: 0 Datail	Connections Per Second Usage					
	System Resources Status CPULIkeys (prictref) 7% 00 00 00 00 00 00 00 00 00 00	2- 1- 0- 07:00	07.07 TCP: 0 Total: 0	87.05	07.00	07:10	
	0710-36 07:06 07:07 07:08 07:00 07:10	- Voide Interface Tooffic Linuxe Official					
	Menory Usage (HB)	400	Contra and a suboli				
		300 1 200 1 100 1					
	Latest ASDH Syslog Hessages					D d	
	ASCM logging is disabled. To enable ASDM	logging with informati hable Logging	onal level, dick the button	below.			

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

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.



CCNA Sec-3 / 65

• 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: CCNA Sec-4 / 65



Envío de datos de uso a Cisco

- Do not Enable



• 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.

CCNA Sec-5 / 65

					10-1-0
View Tools Wizards Window Help	1		Type liquid to search		· 1/11
None 🖓 Configuration 🔄 Monitoring 🥁 Save 🔇 Refresh 🔇 Back 🔇 Forward	3 Help				CISC
termine and the second s					
B Device Dashboard B Preval Dashboard					
Device Information Device	erfoce Status				
General License	nterface	IP Address/Mask	Une	LHA	Kbos
and the second se	sóe	192.168.1.1/24	0 40	0 up	4
ASA Version: 9.2(3) Device Uptime: 0d 0h 28m 10s					
ASDM Version: 7.4(1) Device Type: ASA 5565					
Firewal Mode: Routed Context Node: Single					
Total Plash: 128 HB Total Memory: 512 HB	half an er a		a churc		
20	sect an intertace	to view input and outp	ut kape		
VPN Sessons	offic Status				
IPsec: 0 Clendess SS, VPI: 0 AnyConnect Clent: 0 Octobe	Connections Per 5	Second Usage			
System Resources Status					
CPU Usage (percent)					
40	anna				
7% 30	UDP: 0	TCP: 0 50tal: 0	07:08	01:09	07:10
07.33.06 07.06 07.07 07.06 07.06 07.10	inside' Interface 1	Fraffic Usage (Vbea)			
Menory Usage (MS)	400				
400	300				
	100				
	diction			-	
o ASDM 7.4 for ASA - 192.108.1.1			Tor too to see A		
co ASDM 7.4 for ASA - 192.168.1.1 View Teols Wizards Window Help me 🚱 Configuration 📄 Monitoring 🔚 Save 🔇 Retherin 🌑 Badi 🕥 Forward	3 ma		Type tops to stard		ind a
to ASDM 7.4 for ASA - 192.168.1.1 View Teols Wizzeds Window Help and Og Configuration [2] Hontores [3] Sive Q+ Refresh (2) Back (2) Forward	? Heb		Type tops to see ch		· ····································
to ASDM 7.4 for ASA - 192.168.1.3 View Teols Wizards Window Help and Configuration [] Monitoring [] Save Q Refresh Q Rads Q Forward Sof Device Distributor () Prevail Distributord	3 Helo		Type tops to start		 Allar Cisc
to ASDM 7.4 for ASA - 192.188.1.1 View Tools Witards Window Halp Go Conforston (2014) Halp Conforston (2014) Handboard (2014) Mill Charmien Last updated: 909.26 An Institution	? Heb 1 Top 30/4	context Rubers	Type task to start	Laitue	CISC
co ASDM 7.4 for ASA - 192.168.1.1 View Tools Witards Window Help Tools Ontgaration () Montaining () Save () Refresh () Tools () Forward () Device Distribution () Prevail Distribution () Device Distribution () Prevail Distribution () Prevail () Device Distribution () Prevail Distribution () Prevail Distribution () Prevail () Device Distribution () Prevail Distribution () Prevail Distribution () Prevail Distribution () Prevail Distribution () Prevaile	7 Heb	une Fuint [ant (from] +]	Trans lass la sterit	Last upo t Hits Do	e
to ASDM 7.4 for ASA - 192.168.1.1 View Tools Witards Window Help and Carlspraton I Hontorray I Save Arthren I take I forward Save Save Exat/Dav/Court I Save I S	Pieto foo 10 Ar Intervals Intervals	const Rules Last Linus + - Rule# Hits Sco	Dare Cost Trans tas search Based on: Padae rice Desti	Last up t Hits Do vation Se	e .iliii CISC select 5:09:25 A* slop: Table + ruka Action
to ADM 7.4 for ASA - 192.168.1.1 View Tools Wizards Window Help Def Configuration I Henderic Serie & Refears I too East I Forward I too I too	7 Help Inc 10 A Interval Interval	comes Rules Last linus + . Rule# Hts Sou	Dave Cost Trans tas search Based on: Roda Des5	Last upo Last upo Last upo Last upo Last upon Se	e
to ASDM 7.4 for ASA - 192.188.1.1 View Tools Waards Window Help and Configuration (2) Hondorry (2) Save (2) Refresh (2) Rad: (2) Parsard (2) Denice Diabloand (2) Pre-val Diabloand Tailfe Oriennem Liast updated: 9:09:28 AP Convection Diabloa 2 1 1	Pieto Too 30 A Intervali Intervali	ooma Ruber Lastibur ≠ . Rube# Hits Sou	Type took to see of Based on: Pada ree Destr	Lastiev Lastiev I Hits De Nation Se	e
to ASDM 7.4 for ASA - 192.1681.1 View Tools Witards Window Help Configuration I Hentering I Save R Refrech D East I Forward Device Dashboard Bashboard Traffic Overview Last updated: 909-26 AP Connection Statistics	7 Help Top 30 A Interval Interval	nnes Rúdei Lastifuar (* . Rudei Mits Sou	There than the second Based on: Packet	Lantius Hits Da	tered 30926 Av
to ASDM 7.4 for ASA - 192.168.1.1 View Tools Witards Window Help Tools Waters I Window Help Software Cardparaton I Hentarray I Save Refresh Stadi I Torrard Software Distributor I Tools Tools I I I I I I I I I I I I I I I I I I I	9 Help Rep 10 A Interval Interval	come Point Lastifuer + . Rule# Hts Sou	Tion toos to see of Based on: Pada Cree Desti	Lanting Lanting Links Do Lation Se	enter Attor
to ASDM 7.4 for ASA - 192.168.1.1 View Tools Wizards Window Help Tell Configuration I Help Save & Refrech & Last Industries I Soviet & Refrech & Save I Sa	PHeb Rep 10 A Interval Interf.	const Rules Last Linux	Based on: Pede	Lantinge I Hits De nation Se	e
to ASDM 7.4 for ASA - 192.168.1.1 View Tools Wisards Window Help Conforation Prevail Sale and Prevail Darboard Prevail Darboard Prevail Darboard Triffe Overview Convection Salestica 2 0 00.06 00.00 00.07 00.00 00.0	9 Heb 1 Teo 10 A Diter vol Dater f.	come Rules Last thos + , Rule# HYts Sou	Deset on: Packet	Lastice LMIs Do nation Se	e ilini cisc and 500 25 AU glay: Table e noize Action
to ASDM 7.4 for ASA - 192.1581.1 View Tools Witards Window Help Device Distributers I herewal Distributed Device Distributers I herewal Distributed Table Overniew Last updated: 9009-20 AP Connection Distribute 0 006 00.00 00.00 00.00 Connections 1 1 Visit States 0 Drogent Publish Babe	🦉 Heb Marcold Starvel Intervel	comes Ruben Last linus + , Rube# Mits Sou	Based on: Pada Reset on: Pada rce Destr	Lastuce LHIs De retion Se	e .ili.i CISC statut Total & A
to ASDM 7.4 for ASA - 192.168.1.1 View Tools Witards Window Help Configuration Prevail Dashboard Spence Dashboard Prevail Dashboard Traffic Overneer Connection Statistics 2 0 00.06 00.07 00.08 00.00 Connection Statistics 2 0 00.00	7 Help	const Rules Last Thor + . Rules Hits Sou No	Based on: Pack ree Dest	Lastup Links Dis nation Se	e ultra CISC
to ASDM 74 for ASA - 192.158.1.1 View Tools Wiszels Window Help and Configuration () Hontorry () Save () Refresh () Radi () Forward Spence Dashboard () Pre-wal Dashboard Taffic Overseen Convection Statistics 2 0 00.05 00.05 00.05 00.00	PHOD Intervoli Intervoli	constitues Lastitues + , Rules Hits Sou	Based on: Pada Resed on: Pada ree Desta	Lanting Linkin Dis Justion Se play	e utilitati CISC and S0025 A Solar Table + noice Action
to ASDM 7.4 for ASA - 192.1681.1 View Tools Witards Window Help Device Subboard Immunol Immu	Preto	comes Rident Last 1 hour + , Ride# HVis Sou	Based on: Packet	Lattur IHTs Do ation Se	e ilini cisc andre 500 25 AU ofer Table • nice Athon
to ASDM7.4 for ASA - 192.1581.1 View Tools Witards Window Help Device Distributers I herewal Distributed Device Distributers I herewal Distributed Table Overview Connection Distribute 0 006 00.00 00.00 00.00 Connections Distribute Connections Distribute 0 006 00.00 00.00 00.00 Connections Distribute 0 006 00.00 00.00 Connections Distribute 0 006 00.00 Connections Distribute Connections Distribute Connecti	Press	come Point Lastilhor + . Rule# Hts Sou	Based on: Packet	Lentupo Linita nation Se play	inter Action
to ASDM 7.4 for ASA - 192.168.1.1 View Tools Witards Window Help Configuration Prevail Darbboard Schweitz Darbboard Prevail Darbboard Traffic Overniee Connection Statistics	Press	constRuies LastLibur • . Ruies Hits Sou No	Based on: Pada Reset on: Pada	Latture 1985 Dis play Latture	e
to ASDM 7.4 for ASA - 192.1581.1 View Tools Wisards Window Help Configuration () Hondorry () Save () Refresh () Radi () Pornard Dence Darboard () Preval Darboard Triffe Cherneter Convectors Darboard () Convectors Darboard 2 0 0005 0000 0007 0000 0000 Convectors 1 autocated 9009.20 A Convectors 1 autoc	Peeb Resident Intervision I	const Rules Last Lines + , Rules Hits Sou No e Stable Service Top 10 Sou	Based on: Packe Reset on: Packe rore Desta	Lasting THIS Do aution Se play Lasting	e
to ASDM 7.4 for ASA - 132.1581.1 View Tools Witards Window Help Dence Subbard Mentang Sare & Refeat & Refeat & Toward Spence Darboard & Preval Darboard Darboard Subbard Convector Substata Convector Su	Press Internet Internet Internet Internet Internet Internet Top Upgy Top 30 Internet	come Rules Last 1 hour] + , Rule# HVts Sou No e Status Service: Top 10 Sec # [Lett 1 hour -]	Based on: Packet	Lestuce Littles De nation Se play Lestuce Tage 10 L	e ilini cisc and son 25 A glay Table e roke Action solel 500 35 A been
to ASDM7.4 for ASA - 192.1581.1 View Tools Witards Window Help Configuration Prevail Dis/board Device Dis/board Prevail Dis/board Taffic Overview Dis/board Connection Dis/stoca Connection Dis/	Peep Ince 10 A Interval Interval Interval Interval Interval Interval Interval Interval Interval	const Rules Last Thor + , Rules Mts Sou No e Status Service Tep 10 Secu at [Inst 10 Gr -]	Based on: Pade Reset on: Pade Core Destination of the second of the seco	Last up 1985 De retion Se play Last up toos [30:10 L	e
to ASDM 7.4 for ASA - 192.158.1.1 View Tools Wisards Window Help Configuration () Hontoring () Save () Refresh () Radi () Pornard Dence Darbbaard () Pre-val Darbbaard Table Convectors Darbbaard () Pre-val Darbbaard Convectors Darbbaard () Pre-val Darb	Peeb Republic Interval Poterf.	const Rules Last Linux • , Rules Hits Sou No e Status Services Top 10 Sex & Last Linux •	Based on: Packet office available to de cos Top 10 Destina Based on: Packet	Lieft Loo 1985 Die netion Se play Lieft Loo tors (Top 10 Ll Hits -) Depla	Image: State of the second st
to ASDM 7.4 for ASA - 132.1581.1 View Tools Wisards Window Help Device Disabbany () Prevail Disabband Device Disabband Device Disabbany () Prevail Disabband Device Disabbany () Prevail Disabband Device Disabban	Prec 10 A Diternal Diternal Diternal Diternal Diternal Diternal Diternal Diternal Diternal Diternal Diternal	comes Ruines Land Libber + , Ruine # Hits Sou No e Status Services Top 10 Secu de Land Libbur -	Based on: Packet	Laston 1His Do ation Se play Laston Sons Tap Doub	e
to ASDM7.4 for ASA - 192.1581.1 View Tools Witards Window Help Device Distributer () Hentering () Sale () Referent () Radi () Forward Device Distributer () Hentering () Sale () Referent () Radi () Forward Device Distributer () Hentering () Referent () Re	Press Used Intervali Intervali Intervali Intervali Intervali Intervali	roman Ruber Land I hour (*) . Ruber (*) . Ruber (*) . Ruber (*)	Based on: Pack Reserved on: Pack Reserved on: Pack Same analytic to de Reserved on: Packet	Last Loo 1985 De netton Se play Last Loo Last Loo Last Loo Last Loo Last Loo	e cisc cisc sier Table e nice Action
to ASDM 7.4 for ASA - 192.158.1.1 View Tools Waards Window Help Configuration () Hontorry () Save () Behavior () Back () Forward () Dence Dastebach ⁴ () Pre-wal Dastebach Dence Dastebach ⁴ () Pre-wal Dastebach Convection Dastebach ⁴ () Dence Dastebach ⁴ (Press 20 A	const Rules Last J. Your	Based on: Pede Reset on: Pede ree Desti dots available to de cos Top 30 Destina Based on: Pudet	Lastice 1985 Dep 1985 Sec. 5 989 Lastice Sec. Top 10 L 1985 - Depl	Cisc Cisc Cisc Cisc Cisc Cisc Cisc Cisc

• 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.

CCNA Sec-6 / 65 •

	W G	100
10	Desire Daildoard 10.5	ennal Parkhow
21	The set of	
4	Canada Language	_
	General License:	
1996	Host Name: ciscoasa	
	ASA Version: 9.2(3)	Device Up
	ASDM Version: 7.4(1)	Device Typ
	Firewal Mode: Routed	Context M
	VPN Sessions Prac:	0 AnyC
	97:10:36 07:00	07.07 0
	Memory Lisage (HB)	
	400 200 RRAAAAA	-
6	Latest ASOH Syslog Plessages	

• 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.



CCNA Sec-7 / 65

• Asistentes ASDM.

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

ile	View Tools \	Nizards	Window Help
1	Home 🤗 Conf	Star	tup Wizard Back
	Home	Hig Unit	h Availability and Scalability Wizard
	Device Informa General Lice	ASD Pac	M Identity Certificate Wizard ket Capture Wizard
	Host Name:	ciscoa	sa
	ASA Version:	9.2(3)	Device Uptime: 0d 0h 37m 29s
	ASDM Version	7.4(1)	Device Type: ASA 5505
	Firewall Mode:	Route	Context Mode: Single
	the second second second		

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. •

Choose a VLAN

G Create new VLAN 2

vian1

Enable VLAN

Field VLAN

- 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).

inside VLAV Paso 4. Asignación de Puertos Switcheados Choose a VLAN vian1 + Create new VLAN

- 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.

Choose a starting point for the wizard Modify existing configuration ID Address: 193.169.1.1 a and the d one of the ASA. If your Inte res that your host uses DHCP, you may need to use the device name supplied by the I ged mode (enable) password is required to administer the ASA using ASDM cal VLAN interfaces can divide the eight, Fast Ethernet switch ports of the ASA 5505 into mand Line Interface (CLI). rate, Layer-3 network groups. Switch ports exchange packets at Layer 2 if they are o Change privileged mode (enable) password VLAN. Choose or create VLAN identifiers to define these locically named net ofern New Password: Security Level: 0 Security Level: 10 face IP Address Confi ssign IP addresses to each named VLAN utside IP Address Use the following IP address IP Address: 209.165.200.226 Mask: 255,255,255,248 C Use DHCP C Obtain default route using DHCP Use PPPo8 side IP Address Use the following IP address IP Address: 192.168.1.1 Mask: 255.255.255.0 Use DHCP Obtain route using DHCP CLIKA PPPOE

CCNA Sec-9 / 65

Add >>

<<Rendve

Ethernet0/5

Ethernethil

lect Port Addre nside interface. S addresses for dev desired bety

This NAT config nside interfa-No Address Tr

Use Port Addr

(ii) Use the IP 5 pectfy an IP Address Lise Network IP Address RA

Asistente de Configuración Inicial (C \bigcirc

- Paso 6. Opciones DHCP. •
 - Habilitar DHCP para red Interna. Y adr • opciones.
- Paso 7. NAT / PAT. •
 - Habilita NAT / PAT. Y administra • sus opciones.
- Paso 8. Acceso Adminitrativo. •
 - Especifica Hosts que podrán acceder • HTTPS/ASDM; SSH; Telnet.
- Paso 9. Resumen. •
 - Permite revisar la configuración • propuesta.
 - Back para hacer cambios. •
 - Finish para establecer configuración. 0

	DHCP Se	erver (Stee	6 of 9)				
						North Constant	
	The ASA network.	can act as a Di To configure a	HCP server DHCP serv	and provide IP er on an interf	addresses to the hos ace other than the ins	ts on your inside side interface, go t	
	Configura	stion > Device	Managemer	at > DHCP > D	HCP Server in the mai	in ASDM window.	
	V Enabl	e DHOP server	on the insid	de interface			
	DHOP Address Pool						
	Starting	g IP Address:	192.168.1.	10	Ending IP Address:	192.168.1.41	
	DHOP Par	ameters			DAIL Course To	ľ	
	UNUS SC				URUE Course 2		
ministrar que	interes a	enativ	1955		Neo Terrendo		1.
ininistrat Sus	Leese	.engin:	1000	sec	Ping Timeous:		-1"
	Doman	Name:	conasecuna	y.com			
ress Translation (PAT) to share a single external IP address . Select Network Address Translation (NAT) to share sovera levices on the inside interface. Select the first option. If no a	for devices on the Lexternal IP address translation	e auto-confi	iguration fro	m interface:			
een the inside and outside interfaces.		Administrativ	e Access (!	Step 8 of 9)			
figuration applies to all the traffic from the inside in	terface to the	Specify the addr	esses of all h	osts or network	s, which are allowed to a	access the ASA using	
ce.	,	HTTPS/ASDM, SI	SH or Teinet.				
Translation	[Type	Interface	IP Address	Mask	/ Ad	1
dress Translation (PAT)		HTTPS/ASDM	nade	192,108,115	Pretix Le	Edit	tai
IP address on the inside interface		And the Design of the second sec		Lower Lower Low		Dele	te
an IP address							
tse:	0						
rk Address Translation (NAT)							
Range: 209.165.200.240-209.165.200.248	1						
al ASA por:							
		2) Enable HTTP	server for H	TTP5/ASDM acc	155		
		Disabling HT	TP server wi	prevent HTTPS	ASDM access to this AS	sa.	
tartup Wicard Summary (Step 9 of 9)			I bistory mat	ine .			
Contract and the second second second second	s to the ASA , click F	inish. If you	(Hastor y Inde				
ou have completed the Startup Waard. To send your changes ant to modify any of the data, click Back.							
u have completed the Startup Witard. To send your changes int to modify any of the data, clck Back. infiguration Summary:							
u have completed the Starby Woard. To send your changes int to modify any of the data, cick Back. infguration Summary: set Name: CCNAS-ASA owan Name: crossecurity.com							
ur have completed the Startup Wizard. To send your changes influent to modify any of the data, click Back, influent of the startup of the data, click Back, influent Startup of the startup of	e10/2,Ethernet0/3,E	themet0/4,E					
su have completed the Startup Wrand. To send your changes and to modify any of the data, click Back. Infiguration Summary: lost Name: CONS-ASA lonan Name: consecurity.com witch Port Allocation: Outside Interface (vlan1): Switch Ports - Ethernet()(), Inside Interface (vlan1): Switch Ports - Ethernet()(), Ethernet(vlan2): outside, Interface (vlan2): outside, Interface (vlan2): outside, Interface (vlan2):	et0/2,Ethernet0/3,E	themet0/4,E					
ur have completed the Startup Witard. To send your changes infiguration Summary: ost Name: CDNAS-ASA onan Name: CDNAS-ASA onan Name: CDNAS-ASA Unutide Interface (vian I): Switch Ports - Ethernet0)0, Inside Interface (vian I): Switch Ports - Ethernet0/1,Etherne utside Interface (vian I): outside Interface (vian I): outside Interface (vian I): inside (vian I): soutside, 192, 168, 1, 1	et0/2,Ethernet0/3,E	themet0/4,E					
u have completed the Startup Woard. It send your changes int to modify any of the data, click Bad. infiguration Summary: ost Name: COIN65-ASA mann Name: COIN65-ASA mann Name: COIN66-ASA mann Name: COIN66-ASA mann: COIN66-ASA mannn: COIN66-ASA mann: COIN66-ASA mannn: COIN66-ASA mann: COIN	10 - 192.168.1.41	themet0/4,E					
ou have completed the Startup, Woard. To send your changes antit to modify any of the data, click Back. antiguration Summary: both Name: CONAS-ASA Jonnan Name: CONAS-ASA Jonnan Name: CONAS-ASA Jonnan Name: CONAS-ASA Jonan Name: CONAS-ASA Jonashi Contractor: Outside Interface (Van1): Switch Ports - Ethernet(J), Ethernet(Van1): Switch Ports - Ethernet(J), Inside Interface(Van1): Inside Interface(Van1): Inside Interface, Van1): Inside Interface	10/2,Ethernet0/3,E 10 - 192.168.1.41	themet0/4,E		0		0	

CCNA Sec-10 / 65

• Asistentes VPN.

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

File View Tools	Wizards Window Help				
Home Ra Conf	Startup Wizard	Back C Forw	ard 🛛 Help		
	VPN Wizards	Site-to-site VPN Wizard			
Device Informa	High Availability and Scalability Wizard Unified Communication Wizard ASDM Identity Certificate Wizard	AnyConnect VPN Wizard Clientless SSL VPN Wizard IPsec (IKEv1) Remote Access VPN Wizard			
General Lice	Packet Capture Wizard		Interface	IP Address/Mask	
Host Name: ASA Version ASDM Versio Firewall Mod Total Flash:	ciscoasa 9.2(3) Device Uptime: 0d 0h 33m 13s n: 7.4(1) Device Type: ASA 5505 e: Routed Context Mode: Single 128 MB Total Memory: 512 MB		inside	192. 168. 1. 1/24	
TO SHE FROM IS	The first of the f		Calent an interfac	a be used in the stand	

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



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

CCNA Sec-11 / 65

Capítulo 10

• 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; CCNA Sec-12 / 65sentido; etc...
 Capítulo 10



• 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
 - ...

CCNA Sec-13 / 65

Configuraciones Básicas en ASDM. \bigcirc

- Configuration > Device Setup > Device Name/Password.
 - hostname, 0
 - domain name, 0
 - enable password. 0
- Configuration > Device Management > • Advanced > Master Passphrase.

View Tools Witards Window Help

ragement Access

Command Line (CLI) देवी 🖉

BI CLI Prompt Console Timeout

File Access ICHP 23 Management Interface langement Session Quots

2440

Management censing System Image/Configuratio Logging Smart Call-Home

Cloud Web Security Users/AAA Certificate Masan

OF DHOP

ASDM/HTTPS/Teinet/SSH

4 (1) (1)

an > Des

Message of The Day (motd) Same

Second (ever) Ranner

Login Bannes

at > 75

- PassPhase (Cifrado AES) •
- Re-cifra llaves compartidas en ASA. •
- Configuration > • Device Management > Management Access > Command Line (CLI) > Banner.
 - Varios Banners •

Capítulo 10

Configuración de Interfa \bigcirc

- Elegir Pestaña "Adv
 - Indicar VLAN 2
 - Click en OK
- ASDM muestra con • actualizada:
- La Pestaña • Switchport muestra varias configuraciones para puertos.

ance	ed"	General Advance	ed Pv6	ID: 2				E
		MAC Address Ck Enter MAC add Active MAC Ad	oning dresses for 1 ddress:	the active and	d standby interfaces in Standby MAC	hexadecimal format. Ex	ample: 0123.4567.89	GAB.
igur maurat	ación	Block Traffic	om this inter	face to:	•]			
igur nfigurat 1terfaces	ación	Block Traffic — Block traffic fri tup > Interface	om this inter	face to:	•			
igur nfigurat Iterfaces Name	ación Ion > Device Se Switch Ports Switch Ports	Block Traffic — Block traffic fr tup > Interface	om this inter	face to: Security	TP Address	Subnet Mask Prefix Length	Restrict Traffic flow	Add
igur nfigurat iterfaces Name inside	ación Ion > Device Se Switch Ports Switch Ports Etherneto/0, E	Block Traffic	om this inter Enabled Yes	face to: Security Level 100	• IP Address 192.168.1.1	Subnet Mask Prefix Length 255.255.255.0	Restrict Traffic flow	Add Edit

Associated

LL MAR

inside

inside

inside

inside

inside

inside

inside

Mode

Access

Access

Access

Access

Access

Access

Access

Protected

No

No

No

No

No

No

No

Duplex

auto

auto

auto

auto

auto

auto

auto

Interfaces Eth 0/0 no está • Switch Port habilitada.

figuration > D

Ethernet0/1

Ethernet0/2

Ethernet0/3

Ethernet0/4

Ethernet0/6

Ethernet0/7

Switch Ports

Enabled

No

No

No

No

e Setup > Interfaces

Associated

VLANs

1

1

1

1

1

1

Click en Edit

CCNA Sec-16 / 65

auto

Speed

auto

auto

auto

auto

auto

auto:

Edit

• Configuración de Interfaces en ASDM (Cont 2.).

- Click en "Enable SwitchPort" —
- Click en OK

Configuration > Device Setup > Interfaces

- Aplicar la Configuración.
- ASDM muestra configuración actualizada:

VLA	N ID: 2			
Trunk				
VLA	N IDs:			
	Configure Nati	IVE VLAN	lative VLAN ID:	
VLAN ID must allowed. For t	be in the rang trunk mode, up	e of 1 to 4090. I to 20 comma-se	For access mode, parated VLAN IDs	only one VLAN ID is can be entered.
Isolated				
An isolated the same V	i d/protected por /LAN	t does not forw	ard any traffic to	any other isolated por
Dupl aut	o ,	•]	Speed:	auto 💌
	> _	ж с	ancel H	eip

	244017010		158 1 - AR		111521072605	L SECONDON	1
Name	Switch Ports	Enabled	Security Level	IP Address	Subnet Mask Prefix Length	Restrict Traffic flow	Add
naide	Elhemet0/1, Elhemet0/2, Et.	Yesi	10	0 192.168.1.1	255.255.255.0		Edit
outside	Ethernet0/0	Yes	(0 209.165.200.226	255.255.255.248	-	Deletr

• Configurar Fecha / Hora en ASDM.

- Configuration > Device Setup > System Time > Clock.
 - Zona Horaria. -
 - Fecha. —
 - Hora.-

Type

Add

Edit

Delete

Configuration > Device Setup > System Time > NTP.

Home On Configuration

Startup Wizard

Interfaces

Device Setur

4 F3

OK

- Añadir; Editar; Eliminar.
- Add
 - Entrar parámetros de Servidor NTP.
 - Ok
- Actualizará la vista de servidores NTP.
- · Routing **IP** Address Interface Preferred? Trusted Key? P Device Name/Password Key Number System Time Add NTP Server Configuration Clock IP Address: 192.168.1.254 Preferred Interface: inside Authentication Key ▼ V Trusted Key Number: 1 Key Value: Re-enter Key Value: ••••••• Capítulo 10

Cancel

Help

🔯 Monitoring 🔚 Save 🔇 Refresh 🔇 Back 🔘 Forward

Configuration > Device Setup > System Time > NTP

Configure NTP servers and define authentication keys and values.

CCNA Sec-18 / 65

- 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.

ACLs e	n ASDM.	Carce ASDM 7.4 for ASA - 192166 File View Tools Witards Win Cardguston II and Cardguston II and Card	Help Help Torrest Q+Refeats O Sack O Focust ? Help Continuention > Trevent > Access Bales Addr g Ent (ones) + 4 (1 ≥ 10 € - (0 Fed Fillion)	Type tops to search 00
Conf Add Access F	iguration > Firewall > Access Rules Ver / Añadir / Editar / Eliminar / / Diagramar reglas.	Service Policy Rules AAA Rules AAAA Rules AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	a Enabled Source Criteria: borre User borre Criteria: borre C	And - I List I Deter R, Where User Q, Hot Used Plan: Plan:
Interface: Action: • Perm Source Criteria Source: User: Security Group:	Inside Inside	Revice Setup Revise Prevail Prevail Revise Revise VPI Revise Revise VPI Revise Revise VPI Device Revise Revise	z Appy Reset Advanced	
Destination Crite	ria	Configuratio	on > Firewall > Access Rules	
Destination: Security Group: Service:	any	🗣 Add - 🗐	abled Bource Criteria: Source Use	r Security Grou
Description:	ng et Default 🔹	1 St outsid St Global	(Emplot incoming rule)	
More Options	Cancel Help Diagrama muestra ayuda visual par	a e Address	Service	Destination

• NAT Dinámico en ASDM.

Dos Objetos Network.

Add Network Object

Name: Type:

IP Version:

Start Address:

End Address:

Description:

NAT

PUBLIC

Range

IPv4 DIPv6

209.165.200.240

209.165.200.248

OK

• Configurations > Firewall > Objects > Network Objects/Groups > Add > Network Object.

*

•	Objeto 1:	Identifica el rango público.
•	Objeto 2 internas y (Click en	Identifica las direcciones / el método de traducción. NAT)

List of valid public IP addresses to be used by Dynamic NAT

Cancel

Help

Iame: DYNAMIC-NAT ype: Network P Version: IPv4 DPv6 P Address: 192.168.1.0 P Address: 255.255.255.224 vescripton: Inde Hosts to use Dynamic NAT NAT MAT MAT Image: Dynamic Image:	Add Netwo	nk Object	ES
Network P Version: IPv4 P Address: 192, 168, 1.0 P Address: 192, 168, 1.0 Version: 255, 255, 224 vescripton: Indee Hosts to use Dynamic NAT INAT Indee Hosts Translation Rules Type: Dynamic Type: Dynamic Interslated Addr: PUBLIC Use one-to-one address: Impact Interslation PAT Pool Translated Address: Impact Interslated Interslation Interslated ToP and UDP ports into flot range: 1024-65835 Include range 1-1023	lame:	DYNAMIC-NAT	j
P Version: IPv4 IPv6 P Address: 192.168.1.0 letmask: 255.255.254 lecomption: Inside Hosts to use Dynamic NAT NAT NAT V Add Automatic Address Translation Rules Type: Dynamic Translated Addr: PUBLIC Use one-to-one address translation PAT Pool Translated Address: Round Robin Dictand PAT unqueness to per destinuation instead of per interface Translete TCP and UDP ports into flot range 1024-65835 Include range 1-1023	ypei	Network	
P Address: 192. 168. L.0 etmadk: 255. 255. 255. 224 escription: Inside Hosts to use Dynamic NAT NAT NAT V Add Automatic Address Translation Rules Type: Dynamic Translated Addr: PUBLIC Use one-to-one address translation PAT Pool Translated Address: Round Robin Extend PAT unqueness to per destination instead of per interface Translate TCP and UDP ports into flot range 1024-65835 Include range 1-1023	P Version:	💩 IPv4 💮 IPv6	
Jestimaski: 255.255.254 escription: Inside Hosts to use Dynamic NAT NAT Inside Hosts Translation Rules Type: Dynamic Translated Addr: PUBLIC Use one-to-one address: Image and Robin Round Robin Extend PAT unqueness to per destinuation instead of per interface Translate TCP and UDP ports into flot range 1024-65835 Include range 1-1023	P Addressi	192, 168, 1.0	
escripton: Inde Hosts to use Dynamic NAT NAT NAT NAT NAT Dynamic Dynamic Translated Address Translation Rules Type: Dynamic Translated Address PAT Pool Translated Address: Round Robin Extand PAT unquenees to per destination instead of per interface Translate TCP and UDP ports into flot range 102+65535 Dictude range 1-1023	letmaski	255.255.255.224	+
NAT Add Automatic Address Translation Rules Type: Dynamic Translated Addr: PUBLIC Use one-to-one address translation PAT Pool Translated Address: Round Robin Extend PAT unqueness to per destination instead of per interface Translete TCP and UDP ports into flot range 1024-65535 Include range 1-1023	escription;	Inside Hosts to use Dynamic NAT	
Add Automatic Address Translation Rules Type: Dynamic Translated Addr: PUBLIC Data one-to-one address translation PAT Pool Translated Address: Round Robin Dictand PAT unqueness to per destination instead of per interface Translete TCP and UDP ports into flot range 1024-65535 Include range 1-1023	NAT ::		\$
Type: Dynamic Translated Addr: PUBLIC Use one-to-one address translation PAT Pool Translated Address: Round Robin Extand PAT unspaceess to per destination instead of per interface Translete TCP and UDP ports into flot range 102+65535 Include range 1-1023	😨 Add Auto	omatic Address Translation Rules	
Translated Addr: PUBLIC Use one-to-one address translation PAT Pool Translated Address: Round Robin Extend PAT unqueness to per destination instead of per interface Translate TCP and UDP ports into flot range 1024-65535 Include range 1-1023	Type:	Dynamic] +	
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 102+65535 Include range 1-1023	Translated	Addr: PUBLIC	6
PAT Pool Translated Address: Round Robin Extand PAT unqueness to per destination instead of per interface Translate TCP and UDP ports into flat range 1024-65535 Include range 1-1023	Use on	re-to-one address translation	
Round Robin Schand PAT uniqueness to per destination instead of per interface Translate TCP and UDP ports into flat range 1024-65535 Dickude range 1-1023	PAT Pa	ool Translated Address:	F
Extand PAT uniqueness to per destination instead of per interface Translete TCP and UDP ports into flat range 1024-65535 Discude range 1-1023	Rou	nd Robin	
Translete TCP and UCP ports into Rot range 1024-65535 🗌 Include range 1-1023	Exte	and PAT uniqueness to per destination instead of per interface	
	Tran	slate TCP and UDP ports into Rat range 1024-65535	ge 1-1023
Fall through to interface PAT(dest intf): Inside	Tal ty	rough to interface PAT(dest intf): inside	*
Use IPv6 for interface PAT	[] Use IP	vei fer interface PAT	
- the second -	in the second second	[Advanced]	

• 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.

Туре:	Host	Network	
IP Version;	🗶 IPv4 🕐 IPv6		
IP Address:	192.168.1.0		
Description:	255.255.255.224		
NAT			8
Add Autom	atic Address Translation a	Rules	
Type:	Dynamic PAT (Hide)		
Translated A	iddr: outside		R
Use one	to one address translatio	in .	
PAT Poo	Translated Address:		12
Round	IRobin		
Electro	d PAT uniqueness to per e	sestination instead of per interface.	
Thrand	ate TCP and LIDP ports in	to flat cance 1034-65535	le ranne 1-1023
- Internet	under der andere der andere der er	need lands	and the second
Clear data	agri to muscaka PATQASI	ratette fuore-	
Use Pv	5 for interface PAT		

• 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.

Translate DNS repl			
Disable Proxy ARP	on egress interface		
Lookup route table	to locate egress interface		
Interface			
Source Interface: dmz			
Destination Interface:	outside	-j	
Service			
Protocol:	100- tcp	•	
Real Port:			
Manand Dark			

Add Netwo	rk Object	
lame:	STATIC-NAT	
vpe:	Hest	÷
P Version:	@ Pv4 💮 Pv6	
P Address:	192, 168, 2, 3	
escription:	Static NAT translation to the DM2 server	
NAT		*
Add Auto	matic Address Translation Rules	
Type:	State 👻	
Translated	Addr: 209.165.200.227	(m)
Use on	e-to-one address translation	
PAY Pa	of Translated Address:	12
TRea	nd Roben	
Text	nd PAT uniqueness to per destination instead of per interfa	œ
17Die	siale TOP and UDP ports into flat range 1024-65535	ndude range 1-1923
The the	rauch in order face PAT/dest with:	- 197 191
Cities IN	of fire starfare DAT	
C Case of		
	Advances	
	CK Cancel Help	
		- (1 1 1 1 0

CCNA Sec-

add User Acces

Authentication Authorization Accourt

Enable authentication for administrate

Require authentication to allow use of

Require authentication for the followin

Serial

SSH

Telnet

V HTTP/ASDM Server Group: RJ

Server Group: RA

Server Group: LC

Server Group: RJ

Server Group: LO

Public Key Authentication Public Key Using PKF VMN Policy

• Configurar AAA en ASDM.

- Paso 1. Configurar cuentas de usuarios locales.
 - Configuration > Device Management
 > Users/AAA > User Accounts > Add
- 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 -

CCNA Sec-28 / 65

<u></u>					
Username:	ADMON				
Password:	••••••				
Confirm Password:	******				
User authentics	sted using MSCHAP				
Access Restriction					
Select one of the	options below to restrict ASOM, SSH, Te	ehet and Console access.			
Fill access(4	SDM, SSH, Telnet and Cansole)	seturigs.			
Privlege le	vel is used with command authoritation.				
Privlege L	evek 🔟 🔹 🔹				
CLI login pro	npit for SSH, Telnet and console (no ASD	M access)			
The setting	g is effective only if "aaa authentication.	http console LOCAL* comman	d is configured.		
No ASDM, SS	H, Telnet or Console access				
This setting	g is effective only if "aaa authentication	http console LOCAL* and *sa	a authorization exec	* commands are o	ordgured.
* (🔁 Add AAA Server Group			E
10	🖗 Nest 🛛 🖗 Presious	AAA Server Group: RAD	US-SERVERS		
	OK	Protocol: RAD	ius 🔤 👻		
		Accounting Mode: 💮 S	imultaneous 🔘 Si	ngle	
		Reactivation Mode:	epletion 🔘 Timed	C.	
		Dead Time:	0 minutes		
٨٨		Max Failed Attempts: 3			
		Enable interim accountin	ig update		
aruno		Update Interval:	24 Hours		
grupo		Enable Active Directory	Agent mode		
		ISE Policy Enforcement			
		Enable dynamic authoriz	ation		
es.		Dynamic Authorization P	ort: 1700		
		Use authorization only n	node (no common pa	assword configura	ition required)
AA		VPN3K Compatibility Option	1		*
A dd		Add AAA Server			23
Auu –		Server Group:	RADIUS-SERVERS		
		Interface Name:	dmz 👻		
		Server Name or IP Address	: 192.168.2.3		1
USCISTANA > NAV	Access > Autoentication	fimeout:	10 seconds		
ess to the ASA.		RADIUS Parameters	rt: 1645		
leged mode comman	ds	Server Accounting Port:	1646		
S-SERVERS -	Use LOCAL when server group fails	Retry Interval:	10 seconds		
		Server Secret Key:			
es of connections		Common Password:			
IS-SERVERS V	Use LOCAL when server group fails	ACL Netmask Convert:	Standard	-	
· · · ·] []	Use LOCAL when server group fails	Microsoft CHAPv2 Capab	le: 🔽		
S-SERVERS 👻 📝	Use LOCAL when server group fails	SDI Messages			-
· •	Use LOCAL when server group fails	Message Table			×
- Johnson	÷	ОК	Cancel	Help	

• 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.

ion Settings QoS NetFlow User Statistics
•
Configure
Configure

• 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)

1	isco ASDM 7.4 fo	r ASA - 19	2.168.1.1			
File	View Tools	Wizards	Window Help			
1	Home Conf	Star	tup Wizard	Back C For	ward 🥎 Help	
	Ψ	VPN	l Wizards 🔹 🕨	Site-to-site	e VPN Wizard	
evice List	Device I	Higi Unit	h Availability and Scalability Wizard fied Communication Wizard	AnyConne Clientless	ect VPN Wizard SSL VPN Wizard	
0	Device priorina	ASD	M Identity Certificate Wizard	IPsec (IKEv	 Remote Access 	VPN Wizard
	General Lip	Pac	ket Capture Wizard		Interface	IP Address/Mask

CCNA Sec-30 / 65

• 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.

• Configuración del Router ISR para VPN Sitio a Sitio.

R3 (config) # interface GigabitEthernet R3 (config-if) # description R3 LAN R3 (config-if) # ip address 172.16.3.1 R3 (config-if) # exit 0. Col R3 (config) # interface Serial0/0/1 R3 (config-if) # description WAN Connec R3 (config-if) # ip address 209.165.201 R3 (config-if) # exit R3 (config-if) # exit R3 (config-if) # exit	:0/1 255.255.255.0 nfiguración Básica ted to the Internet 1 255.255.255.252	R3 (config) # crypto map S2S % NOTE: This new crypto ma and a valid access list ha R3 (config-crypto-map) # set R3 (config-crypto-map) # set R3 (config-crypto-map) # mat R3 (config-crypto-map) # exi R3 (config) # R3 (config) # R3 (config) # interface Seri R3 (config-if) # crypto map P2 (config-if) #	-MAP 10 ipsec-isakmp p will remain disabled until a peer ve been configured. peer 209.165.200.226 transform-set ESP-TUNNEL ch address VPN-ACL t a10/0/1 \$28-MAP
R3 (config) # ip route 0.0.0.0 0.0.0.0 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 parts R3 (config-isakmp) #	1. Políti Cifrado 3 grupo 2 (de llave p KEY" cor	ica ISAKMP para IKEv1 3DES; Hashing SHA; DH (1024 bits), Autenticación pre-compartida "SECRET- n el par: 209.165.200.226	 4. Configura mapa criptográfico para la política IPSec y Define tráfico interesante (ACL). 5. Aplica Criptomapa a la interface de salida.
R3 (config-isakmp) # crypto isakmp key R3 (config) # crypto ipsec transform- R3 (cfg-crypto-trans) # mode tunnel R3 (cfg-crypto-trans) # exit R3 (config) # R3 (config) # ip access-list extended R3 (config-ext-nacl) # remark VPN ACL R3 (config-ext-nacl) # permit ip 172.3 R3 (config-ext-nacl) # permit ip 172.3 R3 (config-ext-nacl) # exit R3 (config) #	y SECRET-KEY address set ESP-TUNNEL esp- 2. Política IPSec p VPN-ACL defining interesti 16.3.0 0.0.0.255 19 3. ACL para tráfico de R3 interna a A	as 209.165.200.226 -3des esp-sha-hmac para IKE Fase 2 ang traffic 22.168.1.0 0.0.0.255 0 Interesante: ASA interna	Capítulo 10

Configuración de VPN Sitio-a-Sitio en ASA con ASDM. CNAS-ASA(config)# enable password class 0. Configuración VPN Wizard CCNAS-ASA (config) # Use this uppart to set in new site to site VDN transf. A transf between two devices is railed a site-to-site transf and is bidgertional. A site-to-site VDN transf CCNAS-ASA (config) # interface vlan 1 Básica protects the data using the IPsec protocol. CCNAS-ASA(config-if) # nameif inside Grean-Site VPN 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 Here is a store on how to setup a site-to-site VPN connection. CCNAS-ASA (config-if) # no shut 1 Wizards > VPN Wizards > Site-to-Site VPN Wizard CCNAS-ASA (config-if) # exit CCNAS-ASA (config) # CCNAS-ASA (config) # interface vlan 2 CCNAS-ASA (config-if) # nameif outside → Click en Next 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) # < Back Next > Cancel Help CCNAS-ASA(config-if) # interface e0/0 CCNAS-ASA (config-if) # switchport access vlan 2 2. Identificar el dispositivo par. CCNAS-ASA (config-if) # no shut CCNAS-ASA (config-if) # exit → Ingresar IP alcanzable del dispositivo par. CCNAS-ASA (config) # \rightarrow Identificar interfaces para acceder al par. CCNAS-ASA(config) # route outside 0.0.0.0 0.0.0.0 209.165.200.225 CCNAS-ASA (config) # (para aplicar el criptomapa) CCNAS-ASA (config) # object network INSIDE-NET \rightarrow Clic en Next. CCNAS-ASA (config-network-object) # subnet 192.168.1.0 255.255.255.0 CCNAS-ASA(config-network-object) # nat (inside,outside) dynamic interface This step lets you identify the peer VPN drvice by its IP address and the init ance used to access the peer 1. Introduction CCNAS-ASA (config-network-object) # 2. Peer Device CCNAS-ASA (config-network-object) # policy-map global policy 209.165.201.1 Peer IP Address: Identification CCNAS-ASA (config-pmap) # class inspection default 3. Traffic to protect CCNAS-ASA (config-pmap-c) # inspect icmp VPN Access Interface: outside 4: Security CCNAS-ASA (config-pmap-c) # exit 5. NAT Exempt CCNAS-ASA (config-pmap) # exit 6. Summary CCNAS-ASA (config) # CCNAS-ASA (config) # http server enable < Back Next > Cancel Help CCNAS-ASA(config) # http 192.168.1.0 255.255.255.0 inside CCNAS-ASA (config)

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

Steps	Traffic to protect	
 Introduction Peer Device Identificatio Traffic to protect Security NAT Exempt Summary 	This step lets you identify the local network and remote Local Network: inside-network/24 Remote Network: 172, 16, 3, 0	network between which the traffic is to be protected using iPisc encryption. 3. Identificar Tráfico Interesante. → Elegir Red Local → Elegir Red Remota → Click en Next
Site-to-site VPN Connection Steps 1. Introduction 2. Peer Device Identificatio	on Setup Wizard Security This step lets you secure the selected traffic	 4. Asegurar el tráfico definido. → Configuración Simple: Elección Llave Pre-compartida / Certificado Digital Usa de parámetros IKE comunes.
3. Traffic to protect 4. Security 5. NAT Exempt 6. Summary	Simple Configuration ASA uses the pre-shared key entered here to auth that will allow tunnel establishment. It is recomment Pre-shared Key:	 Configuración a la medida. Elección Llave Pre-compartida / Certificado Digital Elección de parámetros IKE/ISAKMP a utilizar. Olick en Next
	Customized Configuration You can use pre-shared key or digital certificate for a selected for you.	uthentication with the peer device. You can also fine tune the data encryption algorithms ASDM

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

CC

• Verificación de VPNs Sitio-a-Sitio mediante ASDM.

Configuration > Site-to-Site VPN > Connection Profiles.

CCNA

View Tools Wizards Windo	w Help				Type topic to sea	rith (»lu
Home 🚳 Configuration 🗾 Mon	storing 🔜 Save 🕻	Refresh 🚫 Back 🔘	forward 🦻 Help				CISC
Site to Site VPN 0 0	Configuration	> Site to Site VPN > Conner	tion Profiles				
Group Polices Group Polices Certificate Management B G Advanced	Manage site-5 Access Interface Enable interfa	o-site VPN connections. Here is a is ces for IPsec access.	a <u>video</u> on how to setup	a site-to-site VPN co	nnection.		
	Interface	Allow DE v1 Access	Allow D/E v2 Acc	105			
	outside	12 1	[V]				
	idna .	(2)	13				
	riside		0				
	Connection Profil Connection pr encrysted	es offic identifies the peer of a site of other expaneters. You can co Edit (1) Delete	-to-site connection. It is infigure the mapping fro	pecifies what data tra in certificate to conn	effic is to be encrypte action profile <u>here</u> .	d, how the data to	effic is to be
	Add E						
	Name 3	nterface Local Network	Remote Network	D/Ev1Enabled	INEv2Enabled	Group Policy	NAT Exerpt
	P Add E	nterface Local Network	Renote Network	IXEv1Enabled	IVEv2 Enabled	Group Policy	NAT Exerpt
A Device Setup	Name I	interface Local Network	Renote Network	IKEv1 Enabled	iKEv2 Enabled ↓	Group Policy	NAT Exercit
Device Setup	9 Add [] Name 1 200/105	interfact Local Network	Renote Network	IXEv1 Enabled	IVEV2 Enabled	Group Policy	NAT Exempt
Device Setup Frewall Remote Access VPN	9- Add @f	interfact Local Network	Renote Network	IXEv1 Enabled	INEV2 Enabled	Group Policy	NAT Exerpt
Device Setup Forwall Remote Access VPN Ste-to-Site VPN	Add []	interface Local Network	Remote Network	IKEvil Enabled	IVEV2 Enabled	Group Policy	NAT Exempt

10

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 1. Verificar conectividad capa 3. Pinging 172.16.3.3 with 32 bytes of data: \rightarrow El primer ping puede fallar por el tiempo que tarda en Request timed out. Reply from 172.16.3.3: bytes=32 time=64ms TTL=127 establecerse el tunel. Reply from 172.16.3.3: bytes=32 time=63ms TTL=127 \rightarrow Que un ping conteste no implica que exista un tunel. Reply from 172.16.3.3: bytes=32 time=71ms TTL=127 Cipco ASDRA 7.4 fer ASA - 192 168.1.1 0 10 000 Type topic to exarch File View Tools Witards Window Help 0e .1 1.1 1. 🖑 Hone 🖓 Configuration 📝 Monitoring 📊 Save 🔇 Refresh 🔇 Each 🔘 Forward 🦻 Help CISCO Hamiltoning > VMI > VMI Statistics > Session VPN Statistics **Cum/ative** Type Active Feak Consument Inactive Crypto Statistics Concression Statistics Site-to-Site VPN Encryption Statistics D/Evit Effect Global DE/IPsec Statistics 2. Monitoreo de sesiones VPN. Protocol Statistics VLAN Mapping Sessions \rightarrow Monitoring > VPN > Sessions. Clentless SSL VPH Early VPN Clent VPN Connection Graphs Filter By: Psec Site-to-Site · ··· Al Sessiona ··· Filter • WSA Sessone **Details Connection Profile** Protocol Logn Tine Bytes Ta 12 Address Rotes Rul Engrador . piterfaces Apr-201001 Logout GIVEN Prio R, Bouting To sort VPN sessions, right-dick on the above table and select Table Sort Order from popup menu. S Properties Logout By: --- Al Sessons -Logout Sessione . Logana Refieth Last Updated: 4/21/15 3:24:15 PM Capítulo 10 CO Data Refreshed Successfully 2 R ACMON 4/21/15 10-23:17 PM UTC

• Opciones para VPNs de Acceso Remoto en ASA.

- Teletrabajo = Flexibilidad de horario y localidad.
 - Ahorra costos a las empresas \rightarrow 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).

• 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.

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:

Cisco ASDM 7.4 fo	r ASA - 192.168.1.1	
File View Tools	Wizards Window Help	
Home og Conf	Startup Wizard	Back 🕜 Forward 🦻 Help
	VPN Wizards	Site-to-site VPN Wizard
Device Informa	High Availability and Scalability Wizard Unified Communication Wizard ASDM Identity Certificate Wizard	AnyConnect VPN Wizard Clientless SSL VPN Wizard IPsec (IKEv1) Remote Access VPN Wizard
General Lio	Packet Capture Wizard	Interface IP Address/Mask

- 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

CCNA Sec-40 / 65

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

- 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.

CCNA Sec-41 / 65

Capítulo 10

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.

CCNA Sec-42 / 65

Cisco AnyConnect Security Client. Cisco AnyConnect Secure Mobility 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.

/irtual Pri	ivate Ne	twork (VPN	1)		Diagnost	ics.
Preferences	Statistics	Route Details	Frewal	Message History		
						-
Connec	tion Inform	nation			^	
State:		Con	nected			
Tunnel Ma	de (IPv4):	Turn	nel All Tra	ffic		1
Tunnel Mo	de (IPv6):	Turn	nel All Tra	ffic		
Duration:		00;0	13:19			u
Address	Informati	on			•	
Client (IP)	·•D:	10.2	4.241.29			
Client (IP)	(6):	200	1:420:000	C8: 1008:0:0:0:161		
Server:		171.	70.192.8	3		
Bytes					~	
Sent:		141	067			
12 Contractor						

- Puede configurarse Anyconnect para:
- Autoconectar a una VPN específica al iniciar equipo, y mantenerse activo hasta que éste se apague.

Ready to connect.

Connected to San Jose - SSL.

San Jose - SSL

Cisco AnyConnect | San Jose - SSL

Enter a username and software token PIN

San Jose - SSL

Connect

Cance

Disconnect

*

х

 Descargarse Clientless y autoconfigurarse tras instalarse (Windows/Mac/Linux)

0

00:00:56

Ö

Cisco AnvConnect Secu

• <u>Evaluar el host</u> tras instalarse y antes de autoconfigurarse (antivirus/antimalware/firewall instalados y operativos).

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

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.

CCNA Sec-45 / 65

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.

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.

The security appliance allows SSL-enabled web browsers to access on a portal page. Next > Finish Cancel SSL VPN We and SSL VPN V izard Provide a connection profile and the interface that SSL VPN users connect to Clientless-SSL-VPI he interface users access for SSE VPN connections SSL VPN Interface **Digital Certificate** When users connect, the security appliance sends this digital certificate to the remote web browser to authenticate the ASA Certificate: -None Manage Accessing the Connection Profile One accesses this connection profile either by its Group Alias or Group URL. One selects the Group Alias from the Group drop-down list at the login page. One enters the Group LRL in a Web browser. Connection Group Alias/URL Display Group Alias list at the login page Information URL to access SSL VPN Service: https://209.165.200.226 URL to access ASDM: https://209.165.200.226/admi <Back Next> Cancel

The security appliance provides Secure Socket Layer (SSL) remote access

Web browser and its native SSL encryption

CCNA Sec-47 / 65

• Creación de VPN SSL Sin Clientes en ASDM (Cont.).

- 3. Autenticación de Usuario.
 - Servidor AAA.
 - B.D. Local.
 - Ingresar credenciales de Usuario.
 - Añadir Usuario.

SL VPN Wizard User Authentication (Step 3 of 6) The security appliance supports authentication of users by an external AAA server or local user accounts. Specify how the security a authenticates users when they login. AAA Server Group Name: AAA Server	
The security applance supports authentication of users by an external AAA server or local user accounts. Specify how the security a authenticates users when they login. Authenticate using a AAA server group AAA Server Group Name:	_
AAA Server Group Name:	pplance
AAA Server Group Name:	
a Authenticate using the local user database	
Uter to be Added ADMIN	1
Username: BobV	
Add >>>	
Paspword:	
Confirm Password:	
	_

- 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

• Creación de VPN SSL Sin Clientes en ASDM (Cont.).

• Creación de VPN SSL Sin Clientes en ASDM (Cont.).

- 6. Verificar Resumen y Guardar Cambios
 - Back para modificar.
 - Finish para establecer marcadores.

CCNA Sec-50 / 65

• Verificar y Editar VPN SSL Sin Clientes.

CCNA Sec

 Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles.

HEINDLE ACCESE VPN Dr. 4	Configuration > Remote	Access VPH > Ch	entless SSL VPH Acc	ess > Connection Profiles		
Introduction Introduction Introduction Introduction Introduction Intervention Inter	Access Interfaces Enable interfaces for claim Interface Jutaide drug Inside IV Bypass interface acce Access lists from group po Login Page Setting IMov user to select co IM Allow user	tiess SSL VPN access Allow ss lists for inbound V licy and user policy i innection profile on t ternal password on t page. I group) specifies ho	Access	Device Certificate Port Setting Rc. and other perameters. You can config	aure the mapping from certificate to	
Device Setup	Add 🗹 Edt 📋 D	elete Find:	0	Match Case		-
🛃 Frenal	Name I	Enabled	Alases	Authentication Method	Group Policy Distrigation	
		101		AAAA OCAL)	DfltGrpPolicy	
Remote Access VPN	DetsutWEEVPWGroup	10.1		ALC: NOT THE OWNER OF THE OWNER OWNE	THE REAL PROPERTY AND ADDRESS	1.128

8

server.

File Edit

58

https://209.165.200.226

View Favorites Tools Help

Prueba de VPN SSL Sin Clientes . \mathbf{O}

- 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 er Logon

Web Access

cits // 📼

File Access

Browse Entire Network

To access files in your network, your syster

access.

administrator must assign permissions that grant you

Click the link to the destination you want to browse

then click through the hierarchy to the file you want to

File Access

Help

File Access

- Navegar la lista de marcadores:
 - Home
- We recommend that you close this webpage and do not continue to this website. Click here to dose this webpage. ntinue to this website (not recommended) 100 B 209.165.200.226 - Ci D + 😵 Centifi... C 🗙 🎯 209.165.200.226 4 File Edit View Eavorites Logo Usernam Password 1 ogon 109.165.200.226 - CS 🔎 + 😵 Centifi... C 🗙 🎒 209.165.200.226 Edit Favorites Tools Help http:// Neb Bookmarks Attps://209.165.200.226 (+ C5) D - Certifi. C X 209.165.200.226 Corporate WebMai - -209.165.200.226 - CS 🔎 - 😵 Centifi... C 🗙 🍯 209 65.200.226 60 Home Web Applications Requiremen Web Access ndation Corporate WebMail Cookies and JavaScript must be enabled on your browse Your VPN session provides access only File Access File Access Requirements and Record o the corporate resources that you

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority. The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the

🔎 🗝 🖒 🗙 🛛 🎒 Certificate Error: Navigatio... 🔅

Capítulo 10

CCNA Sec-52 / 65

• Ver en CLI la Configuración Generada.

• El Asistente genera las siguientes configuraciones:

webvpn	WebVPN: Habilita la VPN SSL en la interface especificada.			
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		<u>Grupo de Políticas</u> : - 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.		
Isername ADMIN password 3MBOT/Mpbpc4KbOv encrypted priv Isername ADMIN attributes vpn-group-policy Clientless-SSL-Policy Isername BobV password AOv1eG/KWkzEwhtN encrypted privi Isername BobV attributes vpn-group-policy Clientless-SSL-Policy		ege O ge O	<u>Usuario Remoto</u> : - Crear entrada en B.D. local para usuario. - Configura usuario para heredar atributos del grupo de políticas especificado.	
<pre>tunnel-group Clientless-SSL-VPN type remote-act tunnel-group Clientless-SSL-VPN general-attrib default-group-policy Clientless-SSL-Policy</pre>	 Grupo de Tunel: Los usuarios se conectan por IPSec o SSL. Especifica los atributos que el usuario hereda por defecto. 			
default-group-policy Clientless-SSL-Policy	- Esp de	pecific fecto.	a los atributos que el usuario hereda por	

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

CCNA Sec-53 / 65

Capítulo 10

Configuración de ASA para VPN SSL por AnyConnect.

Dos herramientas:

El presente cu

- 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.

File View Tools	Wizards Window Help				
Home 🖧 Conf	Startup Wizard	Back 🔿 Forward 🦻 Help			
107	VPN Wizards	Site-to-site VPN Wizard			
Home	High Availability and Scalability Wizard	AnyConnect VPN Wizard			
Device Informa	Unified Communication Wizard ASDM Identity Certificate Wizard	Clientless SSL VPN Wizard			

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.

Creación de VPN SSL AnyConnect en ASDM

AnyConnect VPN Connection Setup Wize 1. Lanzar Asistente AnyConnect. Use this wizard to configure the ASA to accept VPN connections from the AnyConnect VPN Client. The connections will be protected using either the IPsec or the SSL protocol. The ASA will automatically upload the AnyConnect VPN Client to the end user's device when a VPN connection is established. Wizards > VPN Wizards > AnyConnect • VPN Remote A **VPN Wizard** Next • 2. Configurar Perfil de Conexión. AnyConnect VPN Connection Setup Wizard × Entrar Nombre • Connection Profile Identification Steps de Perfil. 1. Introduction This step allows you to configure a Connection Profile Name and the Interface the remote access users will access for VPN 2. Connection Profile Next > Cancel Help connections Identification Identificar • Connection Profile Name: Client-Based-SSL-VPN interface outside. 4. Client Images VPN Access Interface: outside 6. Client Address Assignme Next. • 7. Network Name Resolutio Servere AnyConnect VPN Connection Setup Wizard a. NAT Exempt VDN Protocol Stens 9. AnyConnect Client 3. Protocolos VPN. 1. Introduction AnyConnect can use either the IPsec or SSL protocol to protect the data traffic. Please select which protocol or protocols you Deployment • would like this connection profile to support. 2. Connection Profile 10. Summary Identification SSL SSL Seleccionar • Next-5 **IPse** protocolo para proteger tráfico: Authentication Methods **Device Certificate Client Address Assignme** Device certificate identifies the ASA to the remote access clients. Certain Network Name Resolutio AnyConnect features (Always-On, IPsec/DEv2) require that valid device certificate SSL. be available on the ASA. • Servers MATEX Device Certificate: -- None -- Manage... AnyCon ect Client **IPSec.** Deploy 10. Summ Configurar certificado del dispositivo. • Next > Cancel Help CCNA Sec-56 / 65Next

Creación de VPN SSL AnyConnect en ASDM (Cont).

Steps

2. Connection Profile Identification

VPN Protocols

Client Images

5. Authentication Methods

6. Client Address Assignme

AnyConnect VPN Connection Setup Wizard

• 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.

 Image: Servers
 User to be Added Username:

 Servers
 8. NAT Exempt

 9. AnyConnect Client Deployment
 Delete

 10. Summary
 Next >

 Next >

 Cancel

Authentication Methods

Local User Database Details

This step lets you specify the location of the authentication server.

You can dick on the "New..." button to create a new server group.

ADMIN BobV

AAA Server Group: LOCAL + New...

- 25

Help

Creación de VPN SSL AnyConnect en ASDM (Cont).

AnyConnect VPN Connection Setup Wizard

NAT Exempt

network.

Inside Interface: inside

client can access.

Local Network:

Exempt VPN traffic from network address translation

any4

exempt from network address translation.

Next >

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

VON Wire

2) Pre-deployment - Manually install the At C AnyConnect VPN Connection Setup

Inside Interface is the interface directly connected to your internal

Local Network is the network address(es) of the internal network that

The traffic between AnyConnect client and internal network will be

tere is the summary of the configuration

Name/Alias of the Connection Profile

VPN Access Interface Device Digital Certificate

VPN Protocols Enabled

AnyConnect Client Images

Authentication Servier Group

Address Pool for the Client

Network Address Translatio

Back Finish

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

*

Cancel

Value

outside

- none -

SSL only

LOCAL

Server: Domain Name

1 package

Client-Based-SSL-VPM

192.168.1.33 - 192.168.1.62

The protected traffic is not subjected to network address tra

Help

Cancel Help

Creación de VPN SSL AnyConnect en ASDM (Cont).

Steps

1. Introduction

2. Connection Profile

3. VPN Protocols

4. Client Images

Servers

10. Summary

Steps

1. Introduction

2. Connection Profile

5. Authentication Methods

6. Client Address Assignme

7. Network Name Resolutio

9. AnyConnect Client

Deployment

Identification

3. VPN Protocols

4. Client Images

Servers

8. NAT Exempt

10. Summary

NAT Exempt
 AnyConnect Client

AnyConnect VPN Connection Setup Wizard

AnyConnect Client Deploymen

1) Web launch - On accessing the ASA usi

Next >

Authentication methods Client Address Assignme

Network Name Resolutio

- 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 Descarga AnnyConnect en clientes.
 - Next. -
- 10. Verificar y Guardar.
 - Back si hay cambios / Finish para guardar.

CCNA Sec-60 / 65

Verificar Conexión AnyConnect.

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

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 preregistrado.

11 111 11

CISCO

WebLaunch

Platform

Detection

ActiveX

Sun Tava

Download

This type of file could narm your computer.

Do you want to run or save anyconnect-win-2.5.2014-web-....exe (1.77 MB) from 209.165.200.226?

Run

Save

Cancel

Help

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

CCNA Sec-62 / 65

ver las Configuraciones Generada	as en la CLI. <u>Configuración NAT.</u>
ip local pool VPN-Client-Pool 192.168.1.33-192.168.1.62 m	- Pool de IPs locales. - Objeto Network para traducir.
object network NETWORK_OBJ_192.168.1.32_27 subnet 192.168.1.32 255.255.255.224	- Regla de traducción twice-NAT.
nat (inside, outside) source static any any destination st	atic NETWORK_OBJ_192.168.1.32_27
NEIWORK_OBJ_192.108.1.32_2/ no-proxy-arp route-tookup	
webypn	Configuración WEBVPN.
enable outside	- Habilita VPN SSL en outside.
anyconnect image disk0:/anyconnect-win-2.5.2014-k9.pkg 1 anyconnect enable	 Habilita AnyConnect para descarga y uso. Habilita tunnel-group-list
tunnel-group-list enable	
group-policy GroupPolicy Client-Based-SSL-VPN internal	Configuración de Políticas de Grupo
group-policy GroupPolicy Client-Based-SSL-VPN attributes	- Creación de Grupo de políticas con atributos
wins-server none	generales.
dns-server value 192.168.2.3	- Configuración de DNS e información de dominio.
vpn-tunnel-protocol ssl-client	- Conexión de usuariuos por VPN SSL
default-domain value ccnasecurity.com	
tunnel-group Client-Based-SSL-VPN type remote-access	
tunnel-group Client-Based-SSL-VPN general-attributes	Conliguración de Grupo de Tunel.
address-pool VPN-Client-Pool	- Identifica atributos del grupo de tunel.
default-group-policy GroupPolicy_Client-Based-SSL-VPN	-Asocia pool local con pool de usuarios externos.
tunnel-group Client-Based-SSL-VPN webvpn-attributes	- Identifica grupo de políticas por defecto (parámetros).
group-alias Client-Based-SSL-VPN enable	- Establece configuraciones comunes para webvpn.
CCNA Sec-65 / 65 La descripción de estos comandos está	fuera del alcance del curso. Capítulo 10