لماكت نيوكت Active Directory عم ASDM ةباوبلا ةقداصمو يداحألا لوخدلا ةقداصمل (عبرملا يف ةرادإلا) ةديقملا

تايوتحملا

<u>ةمدقملا</u> <u>ةىساسألا تابلطتملا</u> <u>تابلطتملا</u> <u>ةمدختسملا تانوكملا</u> <u>ةىساساً تامولعم</u> نىوكترا <u>ىداحألا لوخدلا لىجستل Firepower مدختسم لىكو نىوكت 1. قوطخلا.</u> مدختسمال ليكو عم (FirePOWER (ASDM ةيطمنال قدحول جمد 2. قوطخال. جمد <u>SirePOWER</u> جمد <u>Active Dire</u>ctory. <u>لاجملا ئشناً 3.1 ةوطخلا.</u> <u>لىل المداخل فىضملا مسا/P المن فضأ 3.2 ةوطخلا.</u> <u>.قاطنلا نيوكت ليدعتب مق 3.3 ةوطخلا</u> <u>مدختسملا تاناىب ةدعاق لىزنت 3.4 ةوطخلا.</u> <u>.ةيوەلا جەن نيوكتب مق .4 ةوطخلا</u> <u>لوصولا ىف مكحتالا جەن نىوكت .5 قوطخاا.</u> <u>لوصولات مكحتانا ةسايس رشن .6 ةوطخانا.</u> <u>مدختسملا ثادحاً ةبقارم .7 ةوطخلا</u>. <u>ةحصلا نم ققحتلا</u> <u>(ةلماخلا ةقداصملا) مدختسملا ليكوو Firepower ةيطمنلا ةدحولا نيب لاصتالا</u> Active Directory و FMC نى لاصتال <u>(ةطشن) المصريا الماري الماري الماري (الماري الماري الماري) (المريد الماري) (المريد الماري) (المريد الماري) (ا</u> ةساىسالا رشنو ةساىسالا نىوكت <u>امحالصاو ءاطخألا فاشكتسا</u> <u>ةلص تاذ تامولعم</u>

ەمدقملا

لوخدلا ليجستو (ةطشنلاا ةقداصملا) ةديقملا ةباوبلا ةقداصم نيوكت دنتسملا اذه فصي ةزهجأ ريدم) ASDM مادختساب FirePOWER ةيطمنلا ةدحولا ىلع (قلماخلا ةقداصملاا) يداحألا (فيكترل لباقلا نامألاا.

ةيساسألا تابلطتملا

تابلطتملا

:ةيلاتا عيضاوملاب ةفرعم كيدل نوكت نأب Cisco يصوت

- (فيكتلل لباقلا نامألا زاهج) ASDM و ةيامح رادج ةفرعم •
- FirePOWER ةدحو ةفرعم •
- (LDAP) فيفخلا نزولا ليلد ةمدخ •
- Firepower UserAgent

ةمدختسملا تانوكملا

ةيلاتلا ةيداملا تانوكملاو جماربلا تارادصإ ىلإ دنتسملا اذه يف ةدراولا تامولعملا دنتست

- اةدحولا من الله المعرفي المعني المعرفي معرفي المعرفي ال

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجألاا نم دنتسملا اذه يف ةدراولا تامولعملا ءاشنإ مت. تناك اذإ .(يضارتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسُملا ةزهجألاا عيمج تأدب رمأ يأل لمتحملا ريثأتلل كمهف نم دكأتف ،ةرشابم كتكبش.

ةيساسأ تامولعم

رفوت مزليو لوخد ليجست ةحفصب ةطشنلا ةقداصملا وأ ةديقملا لخدملا ةقداصم زعوت تنرتنإلا يلإ لوصولل فيضملل مدختسملا دامتعا تانايب.

ةكبشلا دراومل مدختسمل ةسلس ةقداصم يداحألا لوخدلا وأ ةبلاسلا ةقداصملا رفوت ةقداصم قيقحت نكمي .تارم ةدع مدختسملا دامتعا تانايب لاخدا نود تنرتنإلا ىلإ لوصولاو مدختسم ليكو لالخ نم امإ يداحألا لوخدلا ليجست

.هجوملا عضولا يف ASA نوكي نأ بجي ،ةديقملا ةباوبلا ةقداصم:**قظحالم**

.ةرخأتملا تارادصإلاو ASA نم (2)9.5 رادصإلا يف Captive Portal رمألا رفوتي :**ةظحالم**

نيوكتلا

.يداحألا لوخدلا ليجستل Firepower مدختسم ليكو نيوكت .1 ةوطخلا

:Windows زاهج يف "FirePOWER مدختسم ليكو" نيوكت ةيفيك لاقملا اذه حرشي

<u>ەتيبثت ءاغل|و Sourcefire مدختسم ليكو تيبثت</u>

.مدختسملا ليكو عم FirePOWER (ASDM) ةيطمنلا ةدحولا جمد .2 ةوطخلا

ح **لماكتلا <** ASDM، كن**يوكتلا** علام لوقتنا ASA FirePOWER Configuration > كما ل جس مدختسملا ليكو رايخ قوف رقنلا دعب .مدختسملا ليكو رايخ قوف رقناو **ةيوهلا رداصم** ةروصلا يف حضوم وه امك ،**قفاضإ** قوف رقنا .مدختسملا ليكو ماظنل IP ناونع نيوكتو:

○ ○ ○ ASA FirePOWER Configurat	OOO <u>Configuration > ASA FirePOWER Configuration > Integration</u> > <u>Identity Sources</u>	
Policies		
🕨 📑 Device Management	Cisco CST Realms Identity Sources Remote Management eStreamer	
🕨 🧒 Object Management		
🕨 🏠 Local		You have unsaved changes 🛛 🔀 Cancel
ன System Information		
📑 Updates		
🖺 Licenses	Identity Sources	
🔻 🧰 Tools	Service Type None Identity Services Engine User Agent	
🗑 Backup Restore		
Scheduling		New Agent
健 Import Export	Host Name/IP Address User Agent ? X	
P Troubleshooting		
🔻 🍡 Integration		
Cisco CSI	Host Name/IP Address 192.168.10.11	
💑 Realms		
🌡 Identity Sources		
Remote Management	Add Cancel	
📝 eStreamer		

.تارييغتلا ظفحل **ظفح** رزلا قوف رقنا

Active Directory. عم FirePOWER جمد 3. ةوطخلا

لاجملا ئشنأ 3.1 ةوطخلا.

ىلإ لوخدلا لجس ASDM، الماكتلا حال القتنا ASDM، الماكتلا حال الع الماكتلا > ASDM، الماكتلا حال الجس Realms. ديدج زيح قفاضإ قوف رقنا.

ديرف لكشب قاطنلا فيرعتل فصو/مسا ءاطعإب مق :فصولاو مسالا.

نالعإلا :ةباتكلا

NETBIOS). مسا :يساسألا AD لاجم مسا يساسألا AD لاجم

ددح :ليلدلا مدختسم مسا *(username*>.

.<*رورملا ةملك*> ددح :ليلدلا رورم ةملك.

ةدعاق يف ثحبلا ماظنلاا أدبيس ثيح نم ةددحم OU ةكبش وأ لاجملا :ةيساسألاا DN ةكبش تانايب LDAP.

.ةعومجملل DN ددح :ةعومجملل DN

ةلدسنملا ةمئاقلا نم رايخلا وضع ددح :ةعومجملا ةمس.

O O ASA FirePOWER Configurat	🗅 🔿 🔿 <u>Config</u> i	uration > A	SA Fir	ePOWER Co	nfiguratio	n > Integration	> <u>Re</u>	<u>alms</u>						
Policies														
🕨 🔜 Device Management	Cisco CSI	Realms	Ide	ntity Source	es Rem	ote Managemer	t	eStreamer						
🕨 🧒 Object Management	0.000 001	Ittuinio		intry bourt						_	_	B .C		
▶ 🏠 Local												M Compare re	alms 😳	New realm
System Information	Name			Description		Type	Bas	e DN	Group DN		Group Att	ribute	State	
🛒 Updates		-				.,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,				_	- croup rad			
Licenses		Add Nev	v Rea	lm						? X				
Tools														
🖉 Backup Restore		Name *			servertest									
Scheduling							_							
🕼 Import Export		Descript	ion											
Troubleshooting		Type *			AD		~							
🔻 🍡 Integration		AD Brim	any Do	main 👗	convertent o			ev: domain.com						
Cisco CSI		AD FIIII			servertest.c	om		ex. domain.com						
la Realms		Director	y Userr	name *	servertest\a	ıdmin		ex: user@domain						
ldentity Sources		Director	v Pass	vord *			_							
🙆 Remote Management							_							
📴 eStreamer		Base DN	*		dc=serverte	st,dc=com		ex: ou=user,dc=cis	sco,dc=com					
		Group D	N *		cn=TAC,ou=	=Security-Team,dc=	serv	ex: ou=group,dc=c	cisco,dc=com					
		Group A	ttribute	9	Member		~							
		* Requir	ed Fiel	d										
								ОК	Cancel					

نيوكتلا ظفحل **قفاوم** ىلع رقنا.

.ةعومجملاب ةصاخلا DN و ةيساسألا DN ميق فاشتكا ىلع ةلاقملا هذه كدعاست نأ نكمي

<u>Active Directory ةمدخل LDAP نئاك تامس فيرعت</u>

ليلدلا مداخل فيضملا مسا/PI ناونع فضأ 3.2 ةوطخلا.

لي الما الما الما الما AD Server IP/I مسا مسا AD Server IP/I ديدحتل.

AD. مداخل فيضملا مسا/IP ناونع نيوكتب مق :IP ناونع/فيضملا مسا

.(389 يضارتفالا) Active Directory ب صاخلا LDAP ذفنم مقر ددح :ذفنملا

ەذە ىلاٍ عجرا ،AD مداخو FMC مداخ نيب لاصتالا ريڧشتل **(يرايتخإ) :SSL/ريڧشتلا ةداەش** ةلاقملا:

<u>...SSL/T... ةقداصمل Microsoft AD ماظن ىلع ةقداصملا نىاك نم ققحتلا</u>

O O O ASA FirePOWER Configurat	_	iguration > ASA Fi	rePOWER Configuration >	> Integration > Realms				
Policies								
🕨 📑 Device Management	servertest							
🕨 🧒 Object Management	Enter a description							
▶ 🏠 Local	Enter a description							
🔄 System Information								
📑 Updates	Directory	Realm Configuration	on User Download					
🛂 Licenses								
🔻 💼 Tools								
🗑 Backup Restore	URL (Hostna	me/IP Address and I	Port)			Encryption		
Scheduling		Add directory			2 2			
健 Import Export		Add directory			: ^			
Troubleshooting		Hostname / IP	102 169 10 11					
🔻 🔌 Integration		Address	192.100.10.11					
Cisco CSI		Port	389					
🍰 Realms								
凝 Identity Sources		Encryption	STARTTLS UDAPS	None				
🔯 Remote Management		SSL Certificate	v	0				
📝 eStreamer				-				
			ОК	K Test	Cancel			

.نيوكتلا ظفحل **قفاوم** قوف نآلا رقنا .AD مداخب FMC لاصتا نم ققحتلل **رابتخإ** رقنا

.قاطنلا نيوكت ليدعتب مق 3.3 ةوطخلا

.قاطنلا نيوكت ىلإ لقتنا ،ەتحص نم ققحتلاو AD مداخل لماكتلا نيوكت ليدعتل

مدختسملا تانايب ةدعاق ليزنت 3.4 ةوطخلا.

AD. مداخ نم مدختسملا تانايب ةدعاق بلجل **مدختسملا ليزنت** ىلإ لقتنا

لصافلا ديدحتو **تاعومجملاو نيمدختسملا ليزنت** ليزنتل رايتخالا ةناخ نيكمتب مق تانايب ةدعاق ليزنتل AD مداخب ةيطمنلا FirePOWER ةدحو لاصتا تارم ددع لوح ينمزلا مدختسملا.

،يضارتفا لكشب .ەل ةقداصملا نيوكت ديرت يذلا **نيمضتلا** رايخ ىلإ اەفضأو ةعومجملا ددح تاعومجملا نيمضتب موقت نأ رايتخاب مقت مل اذإ تاعومجملا لك ديدحت متي.

○ ○ ○ ASA FirePOWER Configurat	O O Configuration > ASA FirePOWER Config	uration > Integration > Realms								
► 🗐 Policies										
🕨 🐻 Device Management	servertest	You have unsaved cha	anges							
🕨 🧒 Object Management	Enter a description									
▶ 🏠 Local	Ence a description									
System Information										
📑 Updates	Directory Realm Configuration User Downlo	bad								
Licenses										
🔻 📴 Tools	Download users and groups									
Backup Restore	Begin automatic download at 12 💙 AM 💙 Ame	erica/New York Repeat Every 24 💙 Hours								
Scheduling	Download Now									
Emport Export										
Troubleshooting	Available Groups 💣	Groups to Include (0)	Groups to Exclude (0)							
Cisco CSI	Search by name	All available groups	None							
Realing										
	AC State Sta									
Remote Management										
estreamer										
estreamen										
		Add to								
		Include								
		Add to								
		Exclude								
💑 <u>D</u> evice Setup										
Firewall										
Remote Access VPN										
Site-to-Site VPN		Enter User Inclusion	Add Enter User Exclusion	Add						
ASA FirePOWER Configur										
詞 Device <u>M</u> anagement		Store ASA FirePOWER Changes	Cancel							

قاطنالا نيوكت ظفحل Store ASA FirePOWER تارييغت قوف رقنا.

وه امك ،تاعومجملاو نيمدختسملا ليزنتل ليزنتلا رز قوف رقناو قاطنلا ةلاح نيكمتب مق ةروصلا يف حضوم.

O O ASA FirePOWER Configurat	○ ○ O Config	uration > ASA F	irePOWER Config	uration	> Integration >	<u>Realms</u>						
Policies												
🕨 🔜 Device Management	Cisco CSI	Realms Id	entity Sources	Remo	ote Management	eStreamer						
🕨 🧐 Object Management	0.000 001											
🕨 🏠 Local								K	Compare realms		New r	realm
ன System Information	Namo		Description		Type	Raco DN	Group DN	Group Attribu	ito Str	to		
🚅 Updates	Name		Description		туре	base DN	Group DN	Group Attribu		ite		
🛂 Licenses	servertest				AD	dc=servertest,dc=com	cn=TAC,ou=Security-Tear	member			₽	🥒 📭
🔻 💼 Tools										_	Downlo	ad button
🗑 Backup Restore												
Scheduling												
🕼 Import Export							•					
HTroubleshooting												
🔻 🍡 Integration												
Cisco CSI												
Sealms												

ةيوەلا جەن نىوكتب مق .4 ةوطخلا.

ضفر متي ،مدختسملا ةقداصم مدع ةلاح يف .مدختسملا ةقداصم ءارجإب ةيوهلا جهن موقي راودألا ىلٍ دنتسملا لوصولا يف مكحتلا ضرف ىلإ اذه يدؤي .ةكبشلا دراوم ىلإ لوصولا (RBAC) اهدراومو كتسسؤم ةكبش ىلع (RBAC)

(ةطشنلا ةقداصملا) ةديقملا ةباوبلا 4.1 ةوطخلا.

ةيوه فيرعتل ضرعتسملاا يف رورملا ةملكو مدختسملا مسا ةطشنلاا ةقداصملا بلطتت ضرع قيرط نع اما مدختسملا ةقداصمب ضرعتسملا موقي .لاصتا يأب حامسلل مدختسملا لاسرال بيولا ضرعتسم NTLM مدختسي .تمص يف NTLM ةقداصمب وأ ةقداصملا ةحفص نم ققحتلل ةفلتخم اعاونا ةطشنلا ةقداصملا مدختست .اهلابقتساو ةقداصملا تامولعم يه ةقداصملل ةفلتخملا عاونالا .مدختسملا

ا. مدختسملا دامتعا تانايب لاخدإب ضرعتسملا زعوي ،ةقيرطلا هذه يف :1. http basic

- 2. NTLM: عم اهيلع ضوافيو Windows لمع ةطحم دامتعا تانايب NTLM مدختسي Active Directory ققداصم نيكمت ىلإ جاتحت .بيو ضرعتسم مادختساب Directory قبرجت رفوي وهو .دامتعالا تانايب قبلاطم نود ةيفافشب مدختسملا ةقداصم ثدحت نيمدختسملل ةدحاو لوخد ليجست.
- 3. مث لشف اذإ ،NTLM مادختساب ةقداصملا ماظنلا لواحي ،عونلا اذه يف **:HTTP ضوافت** عبرم بلطيو ةيطايتحإ ةقيرطك ةيساسألا HTTP ةقداصم عون رعشتسملا مدختسي مدختسملا دامتعا تانايبل راوح.
- ة باجتسإ ةحفص .4 BTTP مي الله عون ل لثامم اذه (HTTP قباجتس المعني .4 جنومن يف ةقداصملا ةئبعتب انه مدختسملا .

عابتا كنكمي ،يلاتلابو ،NTLM ةقداصم نيكمتل ةصاخ ةقيرط ىلع ضرعتسم لك يوتحي NTLM توابتا كنكمي ،يلاتل في عنه من يك قوداصم نيكمتل ضرعتسملا تاداشرا

ةداەش امإ تيبثت ىلإ جاتحت ،ەجوملا رعشتسملا عم نمآ لكشب دامتعالا تانايب ةكراشمل ةيوەلا جەن يف ماع لكشب ةعقوم مداخ ةداەش وأ ايتاذ ةعقوم مداخ.

Step 3. Generate the self-signed Certificate.

openssl x509 -req -days 3650 -sha256 -in server.csr -signkey server.key -out server.crt

لقتنا .**قيوملا قسايس < تاسايسلا < ASA FirePOWER Configuration > نيوكتلا** ىلإ لقتنا (+) **قنوقيألا** ىلع رقنا **مداخلا قدامش** رايخ يفو **قطشنلا ققداصملا** بيوبتلا قمالع ىلإ نآلا مادختساب ققباسلا قوطخلا يف امەديلوتب تمق نيذللا صاخلا حاتفملاو قدامشلا ليمحتو OpenSSL، قروصلا يف حضوم وه امك

O O ASA FirePOWER Configurat	• • • • • • • • • • • • • • • • • • •	olicies > Jdentity Policy
Policies	Default Identity Policy	You have unsaved changes
Intrusion Policy	Identity Policy	
SSL SSL SL Lentity Policy		Add Known Internal Certificate ? ×
 DNS Policy Device Management 	Rules Active Authentication	
🕨 🧒 Object Management		
Local System Information	Server Certificate * None 🗸	BEGIN CERTIFICATE MIDK0CCAURAGUIAPTISTIH1y8dMA0GCSqGSIb3DQEBBQUAMIGNMQswCQYD V00CFw13TFEIAMcCa1LECPMCSEx=EXADBabN@acTCLUBTxdPTECEDETECMAurCa1LE
■ Updates	Port * 1025 (i	38 ChMFQ0ITQ08xDDAKBgNVBAsTA1RBQzEaMBgGA1UEAxMRQ0Euc2VydmVydGVzdC5j
🛂 Licenses	Maximum login attempts * 3	b20xIzAhBgkqhkiG9w0BCQEWFGFkbWluQHNlcnZlcnRlc3QuY29tMB4XDTE2MDUx
🔻 🧰 Tools	· · · · · · · · · · · · · · · · · · ·	EWJLQTESMBAGA1UEBxMJQkFOR0FMT1JFMQ4wDAYDVQQKEwVDSVNDTzEMMAoGA1UE
🥘 Backup Restore	Active Authentication Response Page	CxMDVEFDMRowGAYDVQQDExFDQS5zZXJ2ZXJ0ZXN0LmNvbTEjMCEGCSqGSIb3DQEJ
Scheduling	This page will be displayed if a user triggers an identity rule with HTTP	
🕼 Import Export		Key or, choose a file: Browse
Troubleshooting	System-provided	BEGIN RSA PRIVATE KEY
🔻 🍡 Integration		Proc-Type: 4,ENCRYPTED
Cisco CSI	* Required when using Active Authentication	DEK-Info: DES-EDE3-CBC,B3542C7C670DC917
🔏 Realms		mLeuBJX5T2apbAnOLR+sLYAPqJKxiXigDjR/1RM3WDPK3WHnCvn7Rdwkvw3xbdBC
Videntity Sources		G6u2y+J9wNIIC6sfg4ItjX2Imbkp6LaX0fhlJunUbktSjAKvmi7cIno0JipkfQi3
Remote Management		LDFOB421faxaALiVNKcfuXXzY7x6cboc0ZiB8duJaKlRABwcaSKvP+4ZE/I77NVi
estreamer		tbYSoMw8uKR8BljLTJ1/+YpWFT2bBx4g6iQn9UO4RosakCBKdQLIJwIi49GpOIP2
		Encrypted, and the password is:
		Store ASA FirePOWER Changes Cancel
ASDM-IDM		
www.incwait		
Remote Access VPN		
Site-to-Site VPN		
ASA FirePOWER Configur		Store ASA FirePOWEP Changes Cancel

مق .**ةطشن** ةقداصمك ءارجإلاا رتخاو ةدعاقلل مسا ءاطعإل **ةدعاق ةفاضاٍ** قوف نآلا رقنا ققداصم نيكمت ديرت يتلا ةهجولا/ردصملا ةكبشو ،ةهجول/ردصملا ةقطنم فيرعتب اەل مدختسملا.

تمق يتلا ةلدسنملا ةمئاقلا نم **قاطنلا** ددح .**تادادعإلاو قاطنلا** بيوبتلا ةمالع ىلإ لقتنا مئالت يتلا ةلدسنملا ةمئاقلا نم **ققداصملا عون** ددحو ةقباسلا ةوطخلا يف اهنيوكتب مجو لضفأ ىلع ةكبشلا ةئيب.

O O ASA FirePOWER Configurat	O O O Configuration > AS	A FirePOWER Confi	guration > Policies > Ident	ity Policy					
Policies									
🚦 Access Control Policy	Default Identity	Policy					You have	unsaved change	es
Intrusion Policy	Add Rule							? ×	
💾 Files									
🔒 SSL	Name Active Authenticatio	nl			Insert into Catego		Standard Pules	~	
🔯 Actions Alerts	interve_rationaledate	ч —			into catego	51 y	Standard Rules		
🚨 Identity Policy	Action Passive Authentication	on	 Realm: servertest (AD) 	Authentication 1	Type: HTTP Basic E	Exclude HTTP User-/	Agents: None		
DNS Policy									
🕨 📕 Device Management	Zones Networks P	orts					Realm &	Settings	
🕨 🧒 Object Management									
🕨 🏠 Local	Realm *	servertest (AD)		× 🥔					×
ன System Information	Use active authentication	i if passive authenticatio	n cannot identify user						
📑 Updates	Identify as Special Identi	tion/Cuast if authoriticat	ion connet identify year						
🔛 Licenses	Identity as Special Identi	ties/Guest in authenticat	ton carnot identity user						
🔻 🧰 Tools	Authentication Type	HTTP Basic		~					
lackup Restore	Application Filters 🖒		Available Applications (83)	Ċ		Exclude HTTP Use	r-Agents (0)		
Jene Scheduling	Search by name		Search by name			any			
🔛 Import Export					_				
Trouble shooting	A 🛃 Risks (Any Selected)		ABC						
🔻 🍡 Integration	Very Low	19	AdobeAIR		Add to Rule				
Cisco CSI	Low	40	Advanced Packaging Tool						
🚲 Realms	🕅 🗾 Medium	11	AirPlay						
Jdentity Sources	🗐 🧾 High	6	Amazon Instant Video	(1)					
Remote Management	- ·								
🛃 eStreamer	* Required Field								
	- Required Field								
						(Add	Cancel	

لقنتملا لخدملل ASA نيوكت 4.2 ةوطخلا.

ىلا اەەيجوت ةداعإ متيس يتلا مامتەالل ةريثملا رورملا ةكرح ددح **.1 ةوطخلا** Sourcefire ىل اەەيجوت قداعإ متيس يتل

ASA(config)# access-list SFR_ACL extended permit ip 192.168.10.0 255.255.255.0 any ASA(config)# ASA(config)# class-map SFR_CMAP ASA(config-cmap)# match access-list SFR_ACL

ASA(config)# captive-portal interface inside port 1025

```
. قەجاو لىكل وأ ماع لىكشب قديقملا قباوبلا نيكمت نىكمي : حيملت
```

```
رايخ يف ةيو ها جونب مصاخلاا "مطشنلاا متي دلكانت : حي ملت للعن عيف 1025 TCP لوكوتورب ،مداخلاا ذف من ني وكت نم دلكانت : حي ملت
دف مها
```

ا(قلماخلا ةقداصملا) يداحألا لوخدلا ليجست 4.3 ةوطخلا.

ىلع ارداق نوكيو لوخدلا ليجستب لاجملا مدختسم موقي امدنع ،ةيبلسلا ةقداصملا يف

نم IP-مدختسملا نييعت ليصافت صحفب "FirePOWER مدختسم ليمع" موقي ،AD ةقداصم قدحو عم تامولعملا هذه انكراشيو AD نامأ تالجس Firepower قدحولا يف مكحتلا ضرف لجأ نم ليصافتلا هذه ات

رتخأ مث ةدعاقلل مسا ءاطعإل **ةدعاق ةفاضإ** ىلع رقنا ،ةلماخلا ةقداصملا ةدعاق نيوكتل يتلا ةهجولا/ردصملا ةكبشو ،ةهجولا/ردصملا ةقطنم فيرعتب مق .**قلماخ** ةقداصمك **ءارجإلا** اهل مدختسملا ةقداصم نيكمت ديرت.

تمق يتلا ةلدسنملا ةمئاقلا نم **ةكلمم** ددح .بيوبت ةمالع **تادادعإلاو قاطنلا** ىلإ لقتنا ةقباسلا ةوطخلا يف اهنيوكتب.

نم ةلماخلا ةقداصملا نكمتت مل اذا ةطشن ةقداصمك عجارتلا ةقيرط رايتخإ كنكمي انه ةروصلا يف حضوم وه امك ،**مدختسملا ةيوه فيرعت**:

O O ASA FirePOWER Configurat	O O Configuration > ASA FirePOWER Configuration > Policies > Identity Policy	
V Dolicies		
🐉 Access Control Policy	Default Identity Policy	You have unsaved change
Intrusion Policy		
💾 Files	Add Rule	? ×
🔒 SSL		
🔯 Actions Alerts	Name Passive_Authentication 🗹 Enabled Insert below rule 🗡 1	
🚨 Identity Policy	Action Parchy Authentication Type: HTTP Basic Exclude HTTP User-Agents:	
DNS Policy		
🕨 🔜 Device Management	Zones Networks Ports	Realm & Settings
🕨 🧒 Object Management		
🕨 🏠 Local	Realm * servertest (AD)	
🔄 System Information		
📑 Updates	Use active authentication if passive authentication cannot identify user	
🔛 Licenses		
🔻 🧰 Tools		
🞯 Backup Restore		
Scheduling		
🔐 Import Export		
Troubleshooting		
🔻 🍡 Integration		
Cisco CSI		
🚲 Realms		
🕹 Identity Sources		
Remote Management		
de Streamer		
	* Required Field	
	bA	d Cancel

.ةيوەلا جەن نيوكت ظفحل **Store ASA FirePOWER تارىيغت** ىلع نآلا رقنا

لوصولا يف مكحتلا جەن نيوكت .5 ةوطخلا.

يف مكح<mark>تارا ةسايس < تاسايسارا < ASA Fire</mark>POWER Configuration > ن<mark>يوكتارا</mark> ىل القتنا لوصولا.

تمق يذلا جەنلا فيرعت ددحو ،(يولعلا نكرلا يف رسيألا بناجلا) **ةيوەلا جەن** قوف رقنا يف حضوم وہ امك ،**قفاوم** قوف رقناو ةلدسنملا ةمئاقلا نم ةقباسلا ةوطخلا يف ەنيوكتب ةروصلا ەذە.

O O ASA FirePOWER Configurat	○ ○ ○ ○ Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy	
Policies Access Control Policy	ASA FirePOWER	
 Thrusion Policy Files SL Actions Alerts Identity Policy 	Default Allow All Traffic Enter a description	
DNS Policy Device Management Object Management	M 📄 Status: Access Control policy out-of-date on device	
Coal System Information	Identity Policy: None SSL Policy: None Rules Security Intelligence HTTP Responses	
Licenses	General Settings // Transport/Network Layer Preprocessor Settings	Ø
Backup Restore	Maximum URL characters t Identity Policy ? X AN header when tracking connections	No
Import Export	Allow an Interactive Block Default Identity Policy	Ø
Troubleshooting	Retry URL cache miss lookt Revert to Defaults OK Cancel Iles	Disabled
Cisco CSI	Performance Settings	Ø

نيمدختسملا ددحو **نومدختسملا** ىلإ لقتنا ،ةديدج ةدعاق ةفاضإل **ةدعاق ةفاضإ** قوف رقنا مث ،ةروصلا هذه يف حضوم وه امك ،مهب ةصاخلا لوصولاب مكحتلا ةدعاق ضرف متيس نيذلا .**قفاضاٍ** قوف رقنا

O O ASA FirePOWER Configurat	○ ○ ○ Configuration > ASA FirePOWER Co	nfiguration > Policies > Access Control P	<u>Policy</u>	
Policies Access Control Policy Policy Difference Policy	ASA ASA FirePOWER			
Files	Default Allow All Traffic			You have unsaved changes
Sections Alerts	Add Rule			? ×
 DNS Policy Device Management 	Name	C Enabled	Insert below rule	▼ 1
 Gobject Management A Local 	Action 🖌 Allow	✓ IPS: no policies Variables: n/a Fi	iles: no inspection Logging: no logging	
ன System Information 🛋 Updates	Zones Networks Users Application	ons Ports 🔺 URLs 🔺 ISE Attributes	Insp	ection Logging Comments
Licenses	Available Realms	Available Users 🖒	Selected Users	s (1)
🔻 💼 Tools	 Search by name or value 	Search by name or value	and servertest/1	TAC 📋
Backup Restore	Identities	servertest/*		
Import Export	I servertest	A TAC		
Troubleshooting		🐣 sunil		
V 🔌 Integration			Add to Rule	
Cisco CSI				
🔏 Realms				
Jdentity Sources				
Remote Management	1			
eStreamer	1			
A Device Setup				Add Cancel

لوصولا يف مكحتايا جەن نيوكت ظفحل ASA FirePOWER تارىيغت نيزخت قوف رقنا.

لوصولاب مكحتلا ةسايس رشن .6 ةوطخلا.

لوصولاب مكحتالا جەن ىرتس ،جەنالا قىيبطت لىبق .لوصولاب مكحتالا جەن رشن بجي ر**شن** قوف رقنا ،رعشتسمالا ىلع تارىيغتالا رشنال .ةيطمنالا قدحولا ىلع مىدق قراشإلل قەتبنمالا راطإلا يف **رشن** قوف رقنا مە FirePOWER تارىيغت رايخ رشن</mark> رتخاو.

رادصإلا يف :**قظحالم** 5.4.x، رعشتسملا يلع لوصولا ةسايس قيبطتل مايي 5.4.x رادصإلا يف تارييغت قيبطت قوف ASA FirePOWER

نأ نم دكأت .ةمەملا ةلاح < ASA FirePOWER ةبقارم < ةبقارملا ىلا لقتنا :**ةظحالم** نيوكتلا رييغت قيبطت لمكت نأ بجي ةمەملا.

مدختسملا ثادحأ ةبقارم .7 ةوطخلا.

عون ةبقارمل ،**يلعفلا تقولا يف حاضيإلا < ASA FirePOWER ةبقارم < <mark>ةبقارملا</mark> ىلإ لقتنا مدختسملا اهمدختسي يتلا رورملا ةكرح.**

ةحصلا نم ققحتلا

حيحص لكشب نيوكتلا لمع ديكأتل مسقلا اذه مدختسا.

ةدعاق/نييعت/مدختسملا ةقداصم/ةقداصم عون نم ققحتلل **نومدختسم < ليلحت** ىلإ لقتنا رورملا ةكرح قفدتب ةنرتقملا مدختسملل IP لوصو

(ةلماخلا ةقداصملا) مدختسملا ليكوو Firepower ةيطمنلا ةدحولا نيب لاصتالا

ةيطمنلا قدحولا مدختست Firepower مدختسملا طاشن لجس تانايب يقلتل ،TCP 3306 خفنم Firepower قيطمنلا مدختسملا ليكو نم.

.FMC يف رمألاا اذه مدختسأ ،ةيطمنلا FirePOWER ةدحو ةمدخ ةلااح نم ققحتلل

admin@firepower:~\$ netstat -tan | grep 3306 مرحلا طاقتلا ليغشتب مق FMC مدختسمل ليكو عم لاصتالا نم ققحتلل.

admin@firepower:~\$ sudo tcpdump -i eth0 -n port 3306

Active Directory و FMC نيب لاصتال

نم مدختسملا تانايب ةدعاق دادرتسال TCP 389 خفنم Firepower ةيطمنلا ةدحولا مدختست Active Directory.

مق جتل اليغشتب مق Firepower ب لاصتال ان قرق الماقتل اليغشتب مق Active ب لاصتال ان مق Directory.

admin@firepower:~\$ sudo tcpdump -i eth0 -n port 389 بلجل فاك زايتما اهل قاطنلا نيوكت يف ةمدختسملا مدختسمل دامتعا تانايب نأ نم دكأت مدختسم تانايب ةدعاق AD.

ةسلج ةلەم نيوكت نمو تاعومجملا/نيمدختسملا ليزنت نم دكأتو ،قاطنلا نيوكت نم ققحت حيحص لكشب مدختسملا لمع.

ليزنت لامتكا نم دكأتو "ASA FirePOWER ةبقارم ةمەم ةلاح ةبقارم" ىلإ لقتنا ةروصلا ەذە يف حضوم وە امك ،حاجنب ماەملا تاعومجم/يمدختسم.

(ةطشنلا ةقداصملا) يفرطلا ماظنلاو ASA نيب لاصتالا

ةدحو فيرعت جەن يف حيحص لكشب ذفنملاو ةداەشلا نيوكت نم دكأت ،ةطشنلا ةقداصملا FirePOWER مأو ةيطمنلا متست ،يضارتفا لكشب ASA (Captive-portal) دمأو ةيطمنللا ASA و TCP 885 م SirePOWER و ASA

.ASA ىلع رمألا اذه ليغشتب مق ،اهيلإ لوصولا تارم ددعو ةطشنلا دعاوقلا نم ققحتلل

ASA# show asp table classify domain captive-portal

```
Input Table
in id=0x2aaadf516030, priority=121, domain=captive-portal, deny=false
    hits=10, user_data=0x0, cs_id=0x0, flags=0x0, protocol=6
    src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
    dst ip/id=19.19.19.130, mask=255.255.255.255, port=1025, tag=any, dscp=0x0
    input_ifc=inside, output_ifc=identity
Output Table:
```

L2 - Output Table:

L2 - Input Table:

Last clearing of hits counters: Never

ةسايسلا رشنو ةسايسلا نيوكت

يف حيحص لكشب ءارجإلا لوقحو مدختسملا ليكوو ةقداصملا عونو قاطنلا نيوكت نم دكأت ةيوهلا جهن.

لوصولاب مكحتاا جەنب حيحص لكشب طبترم ةيوەلا جەن نأ نم دكأت.

ة ماي من المتكان م دكأتو ةمهملا ةل معالية المعامية المعامية المعالية من المتكانية من المتكانية المتكانية المتن جاجنب.

اهحالصإو ءاطخألا فاشكتسا

نيوكتلا اذهل اهحالصإو ءاطخألا فاشكتسال ةددحم تامولعم أَيلاح رفوتت ال.

ةلص تاذ تامولعم

- <u>Cisco Systems تادنتسملاو ينقتلا معدلا</u>
- <u>يداحألا لوخدلا ةقداصمل FirePOWER زامج مادختساب Active Directory لماكت نيوكت</u> <u>ةديقملا ةباوبلا ققداصمو</u>

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما