# زاهج مادختساب Active Directory لماكت نيوكت FirePOWER

## تايوتحملا

<u>قمدق مل ا</u>
<u>قي س اس أل ا ت اب ل طتم ل ا</u>
<u>ةمدختسملاا تانوكملا</u>
<u>قيساساً تامولعم</u>
<u>نې وك تا ا</u>
<u>يداحاًل، الوخدل، اليجستان FirePOWER مدختسم لييكو بنيوكت 1. ةوطخلا</u>
<u>مدختسملال الېكو عم FirePOWER (FMC) قرادا زكرم چمد .2 قوطخلا</u>
Active Directory جمد .3 قوطخلا
<u>ل اجمل ا عاش ن 3.1 ةوطخل ا</u>
<u>ل.ي.ل.دل.ا مداخ فـض.اً 3.2 ةوطخل.ا</u>
<u>قاطنالا نيوكت ليدعتب مق 3.3 قوطخا ا</u>
<u>مِدِخَتَسَمِلَ ا تَانَايَتِ مَدَعَاقَ لَيَزَنِتَ 3.4 مَوَطَخًا ا</u>
<u>قېومل ا چەن نېوكت .4 قوطخل ا</u>
<u>(قطش،نل، ا مَقدام مل) مدية مل ا مَباوبل، 4.1 مَوطخل، (مطش، نل، ا مَقدية مل ا مَباوبل، 4.1 مَوطخل، ا</u>
<u>(قل،ماخل،ا قق،داصمل،ا) يداحأل،ا ل،وخدل،ا ل،يچست 4.2 قوطخل،ا</u>
<u>لوصول يف مكحتا ا ةسايس نيوكت .5 ةوطخلا</u>
<u>لوصول ايف مكحتل ا ةسايس رش، ن .6 ةوطخل ا</u>
<u>تالاصتالا ثادحاًو مدختسملا ثادحاً قبقارم .7 ةوطخلا</u>
<u>امحال،صاو ءاطخألاا فاش كتساو ةحصلاا نم قرق حتايا</u>
<u>(قلىماخل، ققداصمل) مدختسمل، ليكوو FMC نيب ل.اصتال.ا نم ق.قرحتل.</u>
Active Directory و FMC <u>نېب ل.اص.تال.ا نم ق.ق.حتل.ا</u>
<u>(قطشنارا ةقداصملا) يفرطا ماظناراو FirePOWER رعشتسم نيب الصتالا نم ققرحتارا</u>
<u>چەنلا رش،نو چەنلا نېوكت نىم قىقرچىلا</u>
<u> شادچاليا تاليچس ليپليچت</u>
<u>ةلص تاذ تامولعم</u>

## ةمدقملا

ليجستو (ةطشنلاا ةقداصملا) ديقملا لخدملا ةقداصم نيوكت ةيفيك دنتسملا اذه حضوي (ةلماخلا ةقداصملا) يداحألا لوخدلا.

ةيساسألا تابلطتملا

تابلطتملا

:ةيلاتا عيضاوملاب ةفرعم كيدل نوكت نأب Cisco يصوت

- آزەجأ Sourcefire Firepower
- قيرهاظلا ةزهجألا جذامن
- ليا فيفخلا نزولا ليلد ةمدخ (LDAP)
- Firepower UserAgent

### ةمدختسملا تانوكملا

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

- ثدحألاا تارادصإلاو 6.0.0 رادصإلاا ، Firepower (FMC) ةرادإ زكرم •
- ثدحألًا رادصإلاو 6.0.0 رادصإلا Firepower رعشتسم •

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

# ةيساسأ تامولعم

امك ،لوخد ليجست ةحفص ةبلاطمب ةطشنلاا ةقداصملا وأ ةديقملا لخدملا ةقداصم موقت .تنرتنإلاا ىلإ لوصولا ىلع لوصحلل فيضملل ةبولطم مدختسملا دامتعا تانايب نوكت

ةكبشلا دراومل مدختسمل ةسلس ةقداصم يداحألا لوخدلا وأ ةلماخلا ةقداصملا رفوت قيقحت نكمي .ةددعتملا مدختسملا دامتعا تانايب راركت نود تنرتنإلا ىلإ لوصولاو ضرعتسم ةقداصم وأ FirePOWER مدختسم ليكو لالخ نم امإ يداحألا لوخدلا ليجست ةقداصم NTLM.

. وجوما عضول ايف ز اوجل نوكي نأ بجي ، قديق مل قباوبل ققداصمل قبس ن لاب : قطح الم

## نيوكتلا

يداحألا لوخدلا ليجستل FirePOWER مدختسم ليكو نيوكت .1 ةوطخلا

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

<u>ەتيبثت ءاغلإو Sourcefire مدختسم ليكو تيبثت</u>

### مدختسملا ليكو عم FirePOWER (FMC) ةرادإ زكرم جمد .2 ةوطخلا

ةرادإ زكرم ىلإ لوخدلا لجس Firepower، كلإ لقتنا System > Integration ((ماظنلا) > Identity ليكو ماظنل IP ناونع نيوكتب مق ديدجلا ليكولا رايخ قوف رقنا ةفاضإ رزلا قوف رقناو مدختسملا.

تارييغتلا ظفحل ظفح رزلا قوف رقنا.

Overview A	nalysis I	Policies Devices	Objects AM	1P							Deplo	💧 🗛 Sy	stem Help 🔻	admin 🔻
						Configuration	Users	Domains	Integration	Updates	Licenses v	Health +	Monitoring •	Tools •
Cisco CSI	Realms	Identity Sources	eStreamer	Host Input Client	Smart Softwar	e Satellite								
											You have unsave	d changes	🔀 Cancel	Save
Identity So	ources													
Service Type		None	Identity Services	Engine User Age	nt									
						New Agent								
Host Name/	User A	Agent			? ×									
	Host	Name/IP Address 192.1	68.10.11											
			(	Add Cano	el									

Active Directory عم FirePOWER جمد .3 ةوطخلا

لاجملا ءاشنإ 3.1 ةوطخلا

زيح ةفاضإ رايخ قوف رقنا .قاطنلا < لماكتلا < ماظنلا ىلإ لقتنا ،FMC ىلإ لوخدلا لجس ديدج.

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

نالعإلا :ةباتكلا

Active Directory لاجم مسا AD: ليساسألاا لاجمل

<username> :ليلدلا مدختسم مسا

<password> :ليلدلا رورم ةملك

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

ةعومجملل DN :ةعومجملل DN

وضع :ةعومجملا ةمس



.ةعومجملاب ةصاخلا DN و ةيساسألا DN ميق ةفرعم ىلع ةلاقملا هذه كدعاست

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

ليلدلا مداخ فضأ 3.2 ةوطخلا

ليلد ةفاضإ رايخ قوف رقنا ،اهدعب امو ةيلاتلا ةوطخلا يلإ لقنتلل ةفاضإ رزلا قوف رقنا.

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

Active Directory) ب صاخلا LDAP ذفنم مقر) 389 :ذفنملا

ىلإ عجرا ،AD و FMC مداخ نيب لاصتالا ريفشتل (يرايتخإ) :SSL/ريفشتلا ةداهش

ربع Microsoft AD ةقداصمل FireSIGHT ماظن يف ةقداصملا نىئاك نم ققحتليا :ةلاقملا SSL/TLS.

Overvie	w Analysis Po	licies Devices Objects AMP							Deploy	A Sys	tem Help	▼ admin ▼
				Configuration	Users	Domains	Integration	Updates	Licenses 🔻	Health 🔻	Monitorin	▼ Tools ▼
Serve Enter a de	ertest											Cancel
Director	Realm Configur	ration User Download										
	Edit directory		? ×								6	Add directory
URL (Hos	Hostname / IP	192 168 10 11						Encryptic	on			
192.168.1	Address	176.100.10.11						none				00
	Port	389										
	Encryption	STARTTLS OLDAPS None										
	SSL Certificate	▼ ○										
		ок	Test Cancel									

.AD مداخب لاصتالا ىلع FMC ةردق نم ققحتلل رابتخالاا رز قوف رقنا

قاطنلا نيوكت ليدعتب مق 3.3 ةوطخلا

نيوكت ليدعت كنكميو AD مداخل لماكتلا نيوكت نم ققحتلل قاطنلا نيوكت ىلإ لقتنا AD.

مدختسملا تانايب ةدعاق ليزنت 3.4 ةوطخلا

AD. مداخ نم مدختسملاً تانايب ةدعاق بلجل مدختسملاً ليزنت رايخ يلإ لقتناً

لصافلا ديدحتو تاعومجملاو نيمدختسملا ليزنت ليزنتل رايتخالا ةناخ نيكمتب مق مدختسملا تانايب ةدعاق ليزنتل FMC AD لاصتا تامج راركت لوح ينمزلا.

هل ةقداصملا نيوكت ديرت يذلا نيمضتلا رايخ يف اهعضوو ةعومجملا ددح.

Directory Realm Configuration User Download		
Download users and groups Begin automatic download at     12     AM     America/New York Repeat Every     24	Hours	
Available Groups 😋	Groups to Include (1)	Groups to Exclude (0)
Search by name      Add to      Include      Add to      Exclude	TAC	None
	Enter User Inclusion Add	d Enter User Exclusion Add

AD: ةلاح نيكمتب مق ،ةروصلا يف حضوم وه امك

Overview Analysis Policies Devices Objects AMP Dashboards • Reporting Summary •						Deploy 01 Sys	item He	p <del>v</del> admin <del>v</del>
Cisco CSI Realms Identity Sources eStreamer	Host Input Client	Smart Software Satellite				Comp	are realms	New realm
Name	Description	Domain	Туре	Base DN	Group DN	Group Attribute	State	
servertest-1		Global	AD	dc=servertest,dc=com	cn=TAC,ou=Security-Tea	member		ታ 🥒 🔁 🖯

### ةيوەلا جەن نيوكت .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 ىلٍ لوصولا (RBAC) اهدراومو كتسسؤم ةكبش ىلع (RBAC)

(ةطشنلا ةقداصملا) ةديقملا ةباوبلا 4.1 ةوطخلا

ةيوه فيرعتل ضرعتسملا يف رورملا ةملك/مدختسملا مسا ةطشنلاا ةقداصملا بلطت ةحفص مادختساب مدختسملا ةقداصمب ضرعتسملا موقي .لاصتا يأب حامسلل مدختسملا تامولعم لاسرال بيولا ضرعتسم NTLM مدختسي .متكت نود NTLM ةقداصمب وأ ةقداصم ةيوه نم ققحتلل ةفلتخم اعاونأ ةطشنلا ةقداصملا مدختست .اهلابقتساو ةقداصملا يه ةقداصملل ةفلتخما عاونألا .مدختسما

- ا. مدختسملا دامتعا تانايب لاخدإب ضرعتسملا زعوي ،ةقيرطلا هذه يف 1. http basic
- 2. كات الماي عن ما المي عن الماي عن الماي عن الماي الم الماي الم الماي الم
- ةلاح يف .NTLM مادختساب ةقداصملا ماظنلا لواحي ،عونلا اذه يفَ :HTTP ضَوَّافت .3 ةيطايتحا ةقيرطك ةيساسألا HTTP ةقداصم عون رعشتسملا مدختسي ،هلشف .مدختسملا دامتعا تانايبل راوح عبرم بلطيو
- ةبلاطم متي ،كلذ عمو ،HTTP يساسألاً عونلل لثامم اذه :HTTP ةباجتساً ةحفص .4

.ەصيصخت نكمي HTML جذومن يف ةقداصملا ةئبعتب انە مدختسملا

ديقتي ەنإف يلاتلابو NTLM ةقداصم نيكمتل ةصاخ ةقيرط ىلع ضرعتسم لك يوتحي قوداصم نيكمتل ضرعتسملا تاداشرإب NTLM.

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.

```
Generate a simple self-signed certificate using openSSL -
Step 1. Generate the Private key
        openssl genrsa -des3 -out server.key 2048
Step 2. Generate Certificate Signing Request (CSR)
        openssl req -new -key server.key -out server.csr
Step 3. Generate the self-signed Certificate.
        openssl x509 -req -days 3650 -sha256 -in server.csr -signkey server.key -out server.crt
```

امسا طعأو جەن ةفاضإ قوف رقنا .ةيوەلا < لوصولا يف مكحتلا < تاسايسلا ىلإ لقتنا ەظفحب مقو جەنلل.

Overview Analysis Policies Devices Obj	ects AMP					Deplo	y 🔺 A3 System Help 🔻	admin 🔻
Access Control > Identity Network Discovery	Application Detectors	Correlation	Actions 🔻					
							Object Management Ac	cess Control
							Compare Policies	New Policy
Identity Policy	Domain			Statu	•	Last Modified		
		New Identity	y policy	? ×	Add a new policy			
		Name	Identity_Policy		Add a new policy			
1		Description						-
			Save Canc	el				

(+) زمرلا ىلع رقنا ،مداخلا ةداەش رايخ يفو ةطشنلا ةقداصملا بيوبتلا ةمالع ىلإ لقتنا ةقباسلا ةوطخلا يف امەديلوتب تمق نيذللا صاخلا حاتفملاو ةداەشلا ليمحتب مقو مادختساب OpenSSL.



مق .ةطشن ةقداصمك ءارجإلا رتخاو ةدعاقلل امسا طعأو ةدعاق ةفاضإ رزلا ىلع نآلا رقنا

#### ةقداصم نيكمت ديرت يتلا ةەجولا/ردصملا ةكبشو ،ةەجولا/ردصملا ةقطنم فيرعتب اەل مدختسملا.

كتئيب بساني يذلا ةقداصملا عونو ةقباسلا ةوطخلا يف ەنپوكتب تمق يذلا ،قاطنلا ددح ەجو لـضفأ ىلع.



ديقملا لخدملل ASA نيوكت

نيوكتل ASA ىلع رماوألا ەذە نيوكتب مق ،ASA FirePOWER ةيطمنلا ةدحولل ةبسنلاب روسأملا لخدملا

ASA(config)# captive-portal global port 1055

مداخلا ذفنم نيوكت نم دكأت ، TCP مداخلا ذفنم نيوكت نم دكأت ، قاداصم بيوبتلا ةمالعب صاخلا ذفنملا رايخ يف قارين قارين

:رمألا ليغشتب مق ،اهيلإ لوصولا تارم ددعو ةطشنلا دعاوقلا نم ققحتلل

ASA# show asp table classify domain captive-portal

شدحال اتار ادص إلى او ASA نم (2).95 رادص إلى ايف Captive Portal رمال ارفوتي : مخطح الم 💊

(ةلماخلا ةقداصملا) يداحألا لوخدلا ليجست 4.2 ةوطخلا

ىلع ارداق نوكيو لوخدلا ليجستب لاجملا مدختسم موقي امدنع ،ةيبلسلا ةقداصملا يف نم IP-مدختسملا طيطخت ليصافت صحفب "FirePOWER مدختسم ليمع" موقي AD ةقداصم هذه Firepower (FMC). هزام عم تامولعملا هذه كراشيو AD نامأ تالجس لوصولا يف مكحتلا ضرفل رعشتسملا ىلإ ليصافتلا.

فيرعتب مق .ةلماخ ةقداصمك ءارجإلا رتخاو امسا ةدعاقلا طعأو ةدعاق ةفاضإ رزلا قوف رقنا اهل مدختسملا ةقداصم نيكمت ديرت يتلا ةهجولا/ردصملا ةكبشو ،ةهجولا/ردصملا ةقطنم.

لضفأ ىلع لمعي يذلا ةقداصملا عونو ةقباسلا ةوطخلا يف ەنيوكتب تمق يذلا قاطنلا ددح ةروصلا ەذە يف حضوم وە امك ،كتىئيبل عيمجت.

نم ةلماخلا ةقداصملا نكمتت مل اذإ ةطشن ةقداصمك عجارتلا ةقيرط رايتخإ كنكمي انه مدختسملا ةيوه فيرعت.



لوصولا يف مكحتلا ةسايس نيوكت .5 ةوطخلا

.ةسايس ريرحت/ءاشنإ < لوصولا يف مكحتلا < تاسايسلا ىلإ لقتنا

تمق يذلا جەنلا فيرعت رتخاو ،(يولعلا نكرلا يف رسيألا بناجلا) ةيوەلا جەن قوف رقنا ةروصلا ەذە يف حضوم وە امك ،قفاوم رزلا قوف رقناو ،ةقباسلا ةوطخلا يف ەنيوكتب.

Overview Analysis Polic	ies Devices Objects	AMP		Deploy 🔍 System Help 🔻 admin 🔻
Access Control > Access Cont	rol Network Discovery	Application Detectors	Correlation	Actions 🔻
NGFW_Policy				🔝 Show Warnings 🛛 🔚 Save 🛛 🔇 Cancel
Enter a description				
Identity Policy: None	SSL Policy: None			
	Identity Policy		? ×	Tinheritance Settings   🕎 Policy Assignments (1)
Rules Security Intelligence General Settings	Identity_Policy		• @	Insport/Network Layer Preprocessor Settings
Maximum URL characters to sto	Revert to Defaults	ок	Cancel	nore the VLAN header when tracking connections No

ددحو نيمدختسملا ىلا لقتنا .ةديدج ةدعاق ةفاضإل ةدعاق ةفاضإ رزلا قوف رقنا يف حضوم وه امك ،مهب ةصاخلا لوصولا يف مكحتلا ةدعاق ضرف متي نيذلا نيمدختسملا تارييغتلا ظفحل ظفح قوف رقناو قفاوم قوف رقنا .قروصلا هذه.

Overview Analy	ysis Policies	Devices Objects	AMP					Deploy	🛕 System I	Help 🔻 🏼 a	dmin 🔻
Access Control >	Access Control	Network Discovery	Application Detectors	Correlation	Actions 🔻						
NGFW_Polic	ÿ									ave 🔀	Cancel
Enter a description											
Identity Policy: Ide	ntity_Policy	SSL Policy: None									
Rules Securit	Editing Rule -	Allow_LAN_User							? ×	y Assignmi	ents (1)
# Filter by Devic	Name Allow_LA	N_User		Enabled	Move	2					×
# Name	Action Allow	1	<ul> <li>IPS: no po</li> </ul>	licies Variables:	n/a Files: no insp	ection Loggin	g: connections: Event \	/iewer			
👻 Mandatory - I	Zones Net	works VLAN Tags	Users Applications	Ports URLs	🔺 ISE Attributes		Inspection	Logging	Comments		
1 Allow LAN LI	Available Realms	Ċ	Available Users	Ċ			Selected Users (2)				
I MIGH_DAN_O	Search by nar	me or value	Search by nam	e or value			Servertest/sunil			- ·	ø U
🗢 Default - NGF	🌐 Special Identi	ties					Servertest/admin				
2 IPS_test	Servertest									0	08
Default Action										×	\$ 🔳
								OK	Cancel		
									cancer		

لوصولا يف مكحتلا ةسايس رشن .6 ةوطخلا

ىلإ نيوكتلا رييغت عفدل رشنلا رايخ قوف رقناو زاهجلا رتخأ .رشنلا رايخ ىلإ لقتنا (ماظنلاو رشنلا رايخ نيب زمر) لئاسرلا زكرم زمر نم جەنلا رشن ةبقارمب مق .رعشتسملا ةروصلا ەذە يف حضوم وە امك ،حاجنب جەنلا قيبطت بجي ەنأ نم دكأتو.

	Deploy 🔒 Sys	tem Help 🔻 admin 🔻
C Deploy Policies Version: 2015-12-10 09:29 PM		? ×
Device	Group	Current Version
□ □ NGFW ⊘ NGFW Settings: NGFW		2015-12-10 09:14 PM
<ul> <li>Access Control Policy: NGFW_Policy</li> <li>Intrusion Policy: Balanced Security and Connectivity</li> <li>Intrusion Policy: No Rules Active</li> <li>Identity Policy: Identity_Policy</li> <li>Identity Policy: Default DNS Policy</li> <li>Network Discovery</li> <li>Device Configuration (Details)</li> </ul>		
Selected devices: 0		Deploy Cancel

### تالاصتالا ثادحأو مدختسملا ثادحاً ةبقارم .7 ةوطخلا

.مسق لمعتسم < لمعتسم < ليلحتلا يف رفوتي ةسلج طشن مدختسملا ،ايلاح

متي فيكو IP ناونع يأب نرتقملا مدختسملا ديدحت يف مدختسملا طاشن ةبقارم دعاست < ليلحت :ةيبلسلا وأ ةطشنلا ةقداصملا لالخ نم امإ ماظنلا ةطساوب مدختسملا فاشتكا مدختسملا طاشن < نومدختسم

#### User Activity

Table View of Events > Users

No Search Constraints (Edit Search)

	<u>▼ Time</u> ×	Event ×	<u>Realm</u> ×	<u>Username</u> ×	<u>Type</u> ×	Authentication ×	IP Address X
4	2015-12-10 11:15:34	<u>User Login</u>	<u>Servertest</u>	📑 <u>sunil</u>	LDAP	Active Authentication	192.168.20.20
4	2015-12-10 10:47:31	<u>User Login</u>	<u>Servertest</u>	💐 <u>admin</u>	<u>LDAP</u>	Passive Authentication	<u>192.168.0.6</u>

تانايبلا رورم ةكرح عون ةبقارمل (ثادحأ) Connections > Events (ليلحت) Analysis ىلإ لقتنا مدختسملا اهمدختسي يتلا.

0	Overview Analysis Policies Devices Objects   AMP Deploy 👍 System Help 🕶 admin													
Co	ntext E	xplorer Connectio	ns • Events Intr	rusions 🔻 Fi	les 🔹 Hosts 👻	Users • Vulnerabilities •	Correlation • Cust	tom • Search						
	Bookmark This Page Report Designer Dashboard View Bookmarks Search •													
	Connection Events (switch workflow) Connections with Application Details > Table View of Connection Events  • Search Constraints ( <u>Edit Search Save Search</u> )													
1	Jump to 🔻													
		✓ First Packet ×	Last Packet ×	Action ×	Initiator IP ×	Initiator User ×	Responder IP ×	Access Control Rule ×	Ingress Interface ×	Egress Interface ×	Count			
1		2015-12-11 10:31:59	2015-12-11 10:34:19	Allow	192.168.20.20	Sunil (Servertest\sunil, LDAP)	74.201.154.156	Allow LAN User	Inside-2	Outside	1			
4		2015-12-11 10:31:59		Allow	192.168.20.20	📇 sunil (Servertest\sunil, LDAP)	74.201.154.156	Allow LAN User	Inside-2	Outside	1			
4		2015-12-11 09:46:28	2015-12-11 09:46:29	Allow	192.168.20.20	Sunil (Servertest\sunil, LDAP)	173.194.207.113	Allow LAN User	Inside-2	Outside	1			
4		2015-12-11 09:46:28		Allow	192.168.20.20	📇 sunii (Servertest\sunii, LDAP)	173.194.207.113	Allow LAN User	Inside-2	Outside	1			
1		2015-12-11 09:46:07	2015-12-11 09:46:58	Allow	192.168.20.20	📇 sunil (Servertest\sunil, LDAP)	173.194.207.113	Allow LAN User	Inside-2	Outside	1			
4		2015-12-11 09:46:07		Allow	192.168.20.20	📇 sunil (Servertest\sunil, LDAP)	173.194.207.113	Allow LAN User	Inside-2	Outside	1			
4		2015-12-11 09:45:46	2015-12-11 09:46:36	Allow	<u>192.168.20.20</u>	Sunil (Servertest\sunil, LDAP)	173.194.207.113	Allow LAN User	Inside-2	Outside	1			
Las	t login o	n Thursday, 2015-12-10 at	11:17:25 AM from 10.65	.39.169 Right-clic	ck for menu						altaha			

ادحالص إو عاطخ أل فاشكتس او ة حصل انم قق حتل

.رورمالا قلى حقفدتب قان تقاما المدختسمال IP لوصو قدعاق/نيي عت/مدختسمالا فقداصم/ققداصم عون نم قق حتال نومدختسم < لي لحت عالا لقتا

#### (ةلماخلا ةقداصملا) مدختسملا ليكوو FMC نيب لاصتالا نم ققحتلا

ةرادإ زكرم مدختسي Firepower (FMC) مدختسملا طاشن لجس تانايب يقلتل ،TCP 3306 خفنم (Fmc) مدختسي مدختسملا ليكو نم.

.FMC يف رمألاا اذه مدختسأ ،FMC ةمدخ ةلااح نم ققحتلل

admin@firepower:~\$ netstat -tan | grep 3306

مدختسملا ليكو عم لاصتالا نم ققحتلل FMC ىلع ةمزحلا طاقتلا ليغشتب مق

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

ىلإ لقتنا (مدختسمل طاشن) User Activity (نومدختسم) Users < (ليلحت) Analysis يل لقتنا ليصافت ىقلتت (FMC) ةيساسألا ةحوللا ةرادإ يف مكحتلا ةدحو تناك اذإ امم ققحتلل مدختسمل ليكو نم مدختسمل لوخد ليجست.

Active Directory و FMC نيب لاصتالا نم ققحتلا

.طشنلاا ليلدلا لا نم مدختسملا تانايب ةدعاق دادرتسال TCP 389 خفنم FMC مدختست

Active Directory. ب لاصتالا نم ققحتال FMC ىلع ةمزحلا طاقتال ليغشتب مق

admin@firepower:~\$ sudo tcpdump -i eth0 -n port 389

فاك زايتما اهب FMC قاطن نيوكت يف ةمدختسملا مدختسملا دامتعا تانايب نأ نم دكأت

.AD مدختسم تانايب ةدعاق بلجل

قاطن نيوكت نم ققحت قلام نيوكت نمو تاعومجملا/نيمدختسملا ليزنت نم دكأتو ،FMC قاطن نيوكت نم ققحت حيحص لكشب مدختسملا لمع ةسلج.

حاجنب ماهملا تاعومجم/يمدختسم ليزنت لامتكا نم دكأتو ماهملا < لئاسرلا زكرم ىلإ لقتنا، قروصلا هذه يف حضوم وه امك.

(	Deploy 0 S	ystem Help	admin
Deployments 🔥 Health 🛛 Tasks			<b>0</b> ?
20+ total 0 waiting 0 running 0 ret	ying 20+ succes	s 1 failure	
<ul> <li>LDAP Download – Global</li> <li>Download users/groups from serverter</li> <li>successful: 1 groups, 0 users downloaded</li> </ul>	<b>st-1.</b> LDAP downlo	ad	2s X
<ul> <li>LDAP Download - Global</li> <li>Download users/groups from serverter</li> <li>successful: 1 groups, 5 users downloaded</li> </ul>	<b>st-1.</b> LDAP downlo	ad	4m 52s 🗙

ةقداصملا) يفرطلا ماظنلاو FirePOWER رعشتسم نيب لاصتالا نم ققحتلا (ةطشنلا

FMC. فيرعت جەن يف حيحص لكشب ذفنملاو ةداەشلا نيوكت نم دكأت ،ةطشنلا ةقداصملل FMC. .ةطشنلا ةقداصملل TCP 885 ذفنم ىلع Firepower رعشتسم عمتسي ،يضارتفا لكشب

جەنلا رشنو جەنلا نيوكت نم ققحتلا

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

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

جاجنب جەنلا رشن لامكإ نم دكأتو ماەملا < لئاسرلا زكرم ىلإ لقتنا.

ثادحألا تالجس ليلحت

لوخد ليجست ناك اذإ ام صيخشتل "مدختسملا طاشن" ثادحأو "لاصتالا" مادختسإ نكمي ثادحألا هذه .ال مأ احجان مدختسملا

قفدتلا ىلع اەقىبطت متي يتلا لوصولا يف مكحتلا ةدعاق نم ققحتلا نكمي امك.

مدختسملا ثادحاً تالجس نم ققحتلل مدختسم < ليلحت ىلإ لقتنا.

لاصتالا ثادحاً نم ققحتلل لاصتالا ثادحاً < (ليلحت) Analysis ىلإ لقتنا.

ةلص تاذ تامول عم

<u>- تادنتسملاو ينقتلا معدلا</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