

SAML ل ةومجمل جهن نيي عت نيوكت Microsoft فرعمو نمآال ةيامل راج مادختساب Entra

تايوت حملال

[ةمدقملا](#)

[ةيساسال تابل طتملا](#)

[تابل طتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسا تامولعم](#)

[نيوكتل](#)

[FMC SAML نيوكت](#)

[FMC RAPN قف نل ةومجم نيوكت](#)

[RAPN ل FMC ةومجم جهن نيوكت](#)

[FTD فيرعت تانايب](#)

[Microsoft Entra فرع](#)

[ةحصلال نم ققحتلا](#)

[Firepower Threat Defense \(FTD\) ماطن](#)

[اهجالص او عا طخأل افاشكتسا](#)

[ةلص تاذا تامولعم](#)

ةمدقملا

Microsoft ةقاطب فرعمو مادختساب ةومجمل تاسايس نيي عت ةيفيك دنتسملا اذه فصي Cisco. نم نمآال ةيامل راج ىلع Cisco Secure Client ل SAML ةقداصل

ةيساسال تابل طتملا

تابل طتملا

ةيلاتل عيضاوملاب ةفرعم كي دل نوكت ناب Cisco ي صوت:

- Cisco Secure Client AnyConnect VPN
- Cisco Secure Firewall ASA Remote Access VPN و Cisco Firepower Threat Defense (FTD) Single Sign-On (SSO) Server Object
- Microsoft Entra (IDp) فرعمو ةي وه رفوم نيوكت

ةمدختسملا تانوكملا

ةغيص ةيجمر بو زاهج اذه ىلع دشرم اذه يف ةمولعملا تسسا

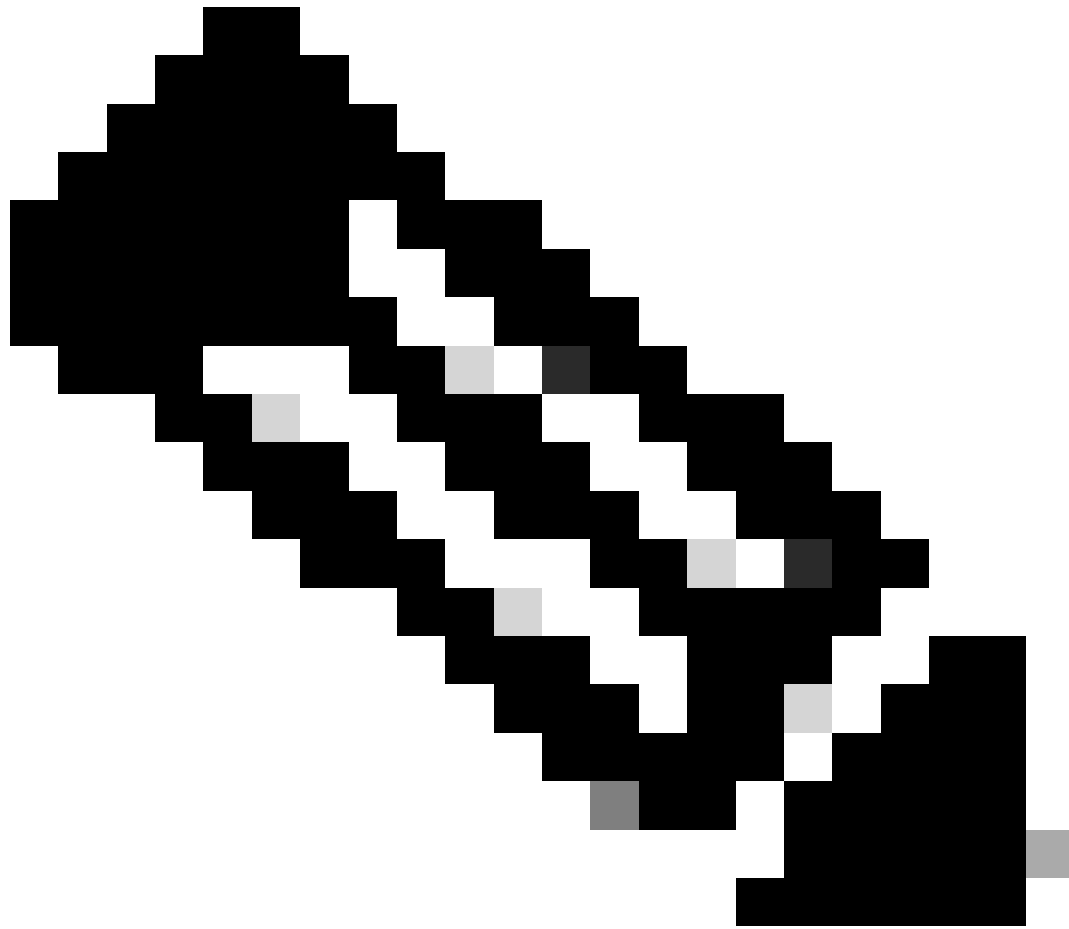
- 7.6 رادصلإال FTD
- 7.6 رادصلإال FMC،
- MS Entra ID SAML IDp

ةصاخ ةي لمعم ةئي ب ي ف ةدوجومال ةزهجال نم دنتسمل اذه ي ف ةدراول تامولعمل عاشنإ م ت تناك اذا .(يضا رتفا) حوسمم نيوك تب دنتسمل اذه ي ف ةمدختسمل ةزهجال عيمج ت ادب رما يال لم تحمل ري ثاتلل كمهف نم دكأت ف ،ليغشتال دي ق ك تكبش

ةيساسأ تامولعم

ةقداصلال تانايب لدابل XML ىل دنتسي لمع راطإ يه (نامال دي كأت زيي مت ةغل) SAML دوزمو مدختسمل ني ب ةقثل نم ةرئاد عاشنإ ىل ع لمعي وهف . نامال تالاجم ني ب ضيوفتالو تامدخ ةدعل ةدحاو ةرم لوخدل ليجستب مدختسملل حمسي امم (IDp) ةي وهال دوزمو (SP) ةمدخل VPN ل Cisco Secure Client Connections to دع ب نع لوصول ةقداصلال SAML مادختسإ نكمي ةقثل ةرئاد نم SP عزج FTD وأ ASA نو كي شيح ، FTD VPN HeadEnd و ASA

اضيأ نكممل نم ،كلذ عمو . IdP ك Microsoft Entra ID/Azure مادختسإ متي ، دنتسمل اذه ي ف نكممي ةيساي ق تامس ىل دنتست اهنأل ىرخأ تافرع مادختساب ةعومجم تاسايس نيي عت SAML دي كأت ي ف اهلاسرا



ىلع ةدحاو ني مدختسم ةعومجم ىلإ طقف يمتني نأ بجي مدختسم لك نأ كردم :ةظحالم
FTD وأ ASA ىلإ اهل اسرا متي يتل ةددعتمل SAML تامس نأ ثيح ،MS Entra فرع
م في لصفم وه امك ةعومجملا ةسايس نيينعت عم لكاشم ثودح في ببستت نأ نكمي
Cisco [CSCwm33613](#) نم ءاطخأل احيصت فرع

نيوكتلا

نيوكت FMC SAML

متي .ي دأخأل لوخدلا ليچست مداخ > AAA مداخ > نئاكلل قرادإ > تانئاكلل ىلإ لقتنا ،FMC في
دوزم ةداهشو ،جورخل ليچستل URL ناونعو ،URL SSO ناونعو ،ةدحولل فرع ىلع لوصحل
تامولعملل عقوم ددحم .Microsoft Entra فرع مسق في 6 ةوطخلل عجار ،فرعملل نم ةي وهلا
هـ. ىلإ هتفاضل مت يذلا نيوكتل FTD ل ناددحم ةمدخلل دوزم ةداهشو ىساسألا

Edit Single Sign-on Server

Name*
SAMLtest

Identity Provider Entity ID*
https://sts.windows.net/af42ba...

SSO URL*
https://login.microsoftonline.co...

Logout URL
https://login.microsoftonline.co...

Base URL
https://vpn.example.com

Identity Provider Certificate*
SAMLtest +

Service Provider Certificate
+

Request Signature
--No Signature--

Request Timeout
Use the timeout set by the provi...

Cancel Save

FMC ل SSO نئاك نيوكات

FMC RAPN ق فنللا ةعومجم نيوكات

مق وأ، ددحو لاصتاللا فيرعت فلم > دع ب نع لوصولا > VPN > ةزهجالا ىلإ لقتنا، FMC في فيصوت عاشناب مق، هديدت درجم ب. هنيوكتب موقت يذلا FTD ل VPN ةسايس، عاشناب في: امل هباشم ليصوت

Edit Connection Profile

Connection Profile:*

SAMLtest

Group Policy:*

DfltGrpPolicy

+

Edit Group Policy

Client Address Assignment

AAA

Aliases

IP Address for the remote clients can be assigned from local IP Address pools/DHCP Servers/AAA Servers. Configure the 'Client Address Assignment Policy' in the Advanced tab to define the assignment criteria.

Address Pools:

+

Name	IP Address Range	
SAML_pool	192.168.55.1-192.168.55.10	 

DHCP Servers:

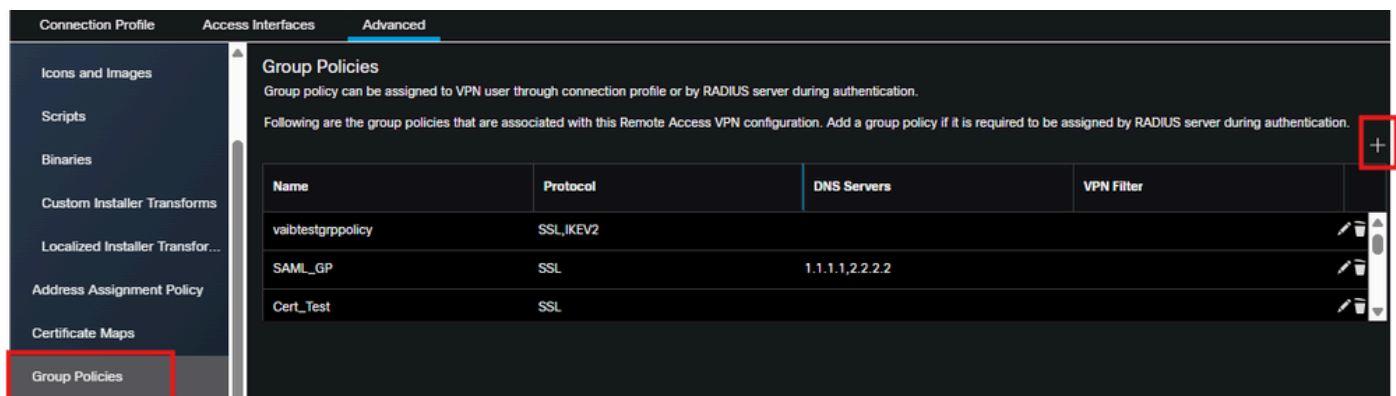
+

Name	DHCP Server IP Address	

Cancel

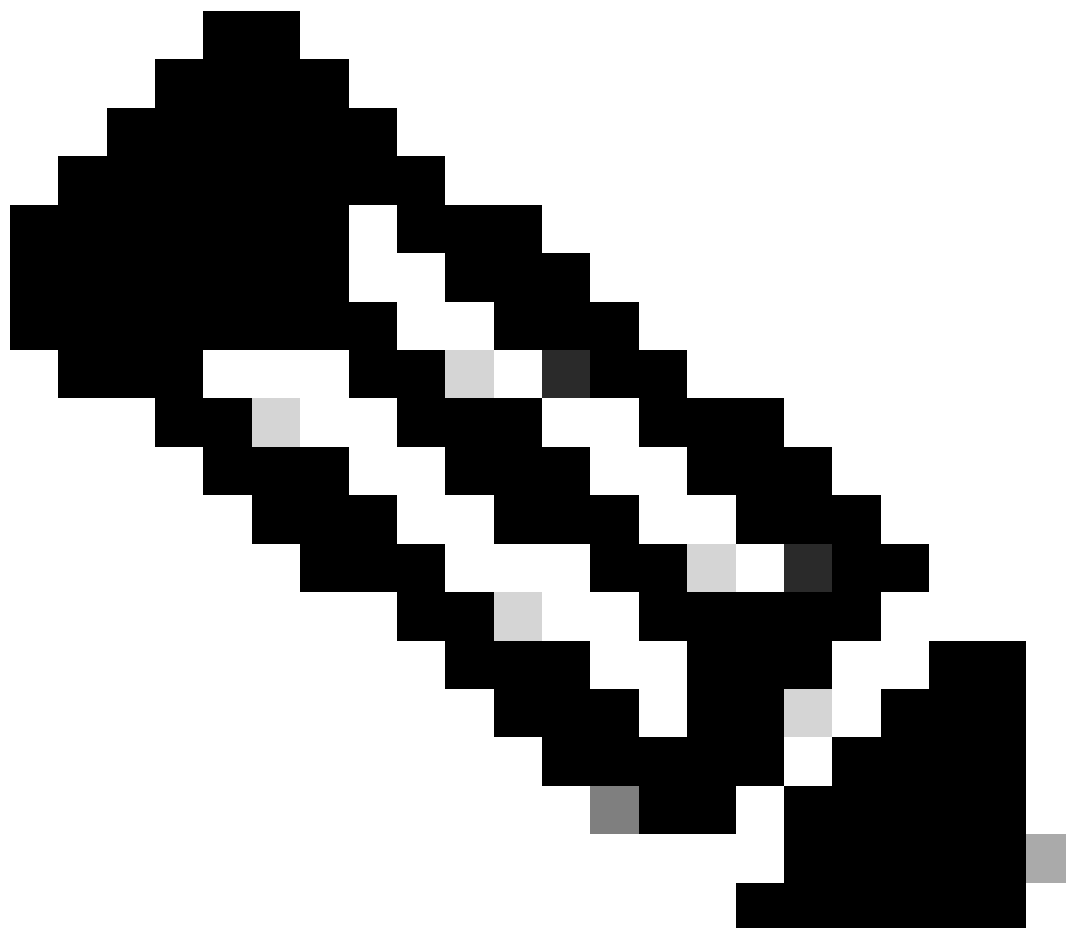
Save

FMC الاتصال في رعت فلم ناونع نبيعت



ةومجم جهن ةفاض | FMC

مق. ديدج ةومجم جهن عاشنإل راوخل ع برم ضرعل ةقثبنم الم ةمئاقلا يف + قوف رقنا 2. اهظفحو ةبولطم الم تارايخل ةئبعتب



ي طخت كنكم يف ،لعللاب بولطم الم ةومجم الم جهن عاشنإب تمق دق تنك اذا :ةطحالم
3 ةوطخل مادختساب ةعباتملاو ةوطخل هذه

Group Policy

Available Group Policy



Search

ديدج ةعومحم جهن عاشنا

Add Group Policy

Name:*

SAMLtest-GP

Description:

General

Secure Client

Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

VPN Tunnel Protocol:

Specify the VPN tunnel types that user can use. At least one tunneling mode must be configured for users to connect over a VPN tunnel.

☒ SSL

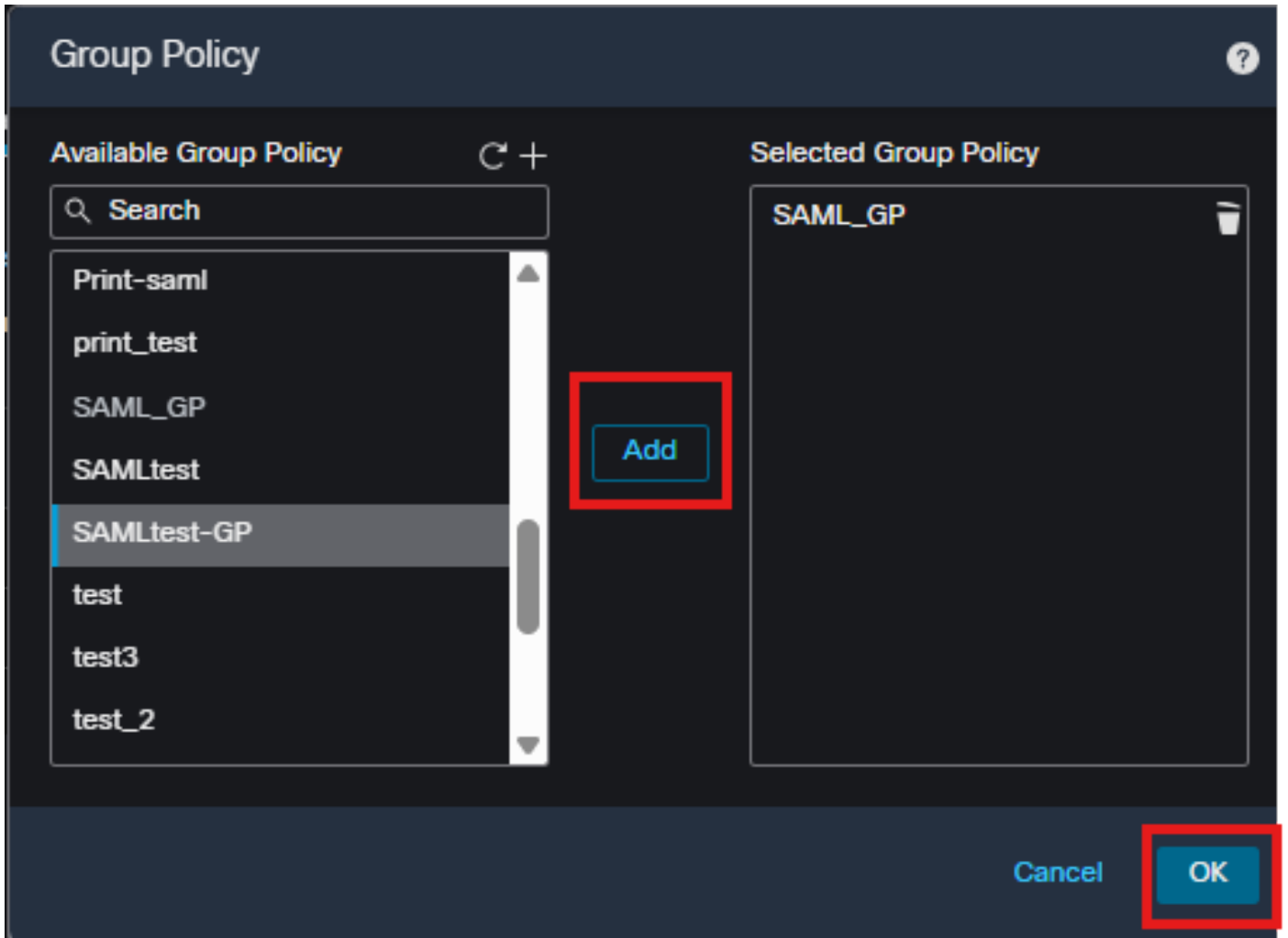
☒ IPsec-IKEv2

Cancel

Save

ةومجممل جهن تارايخ

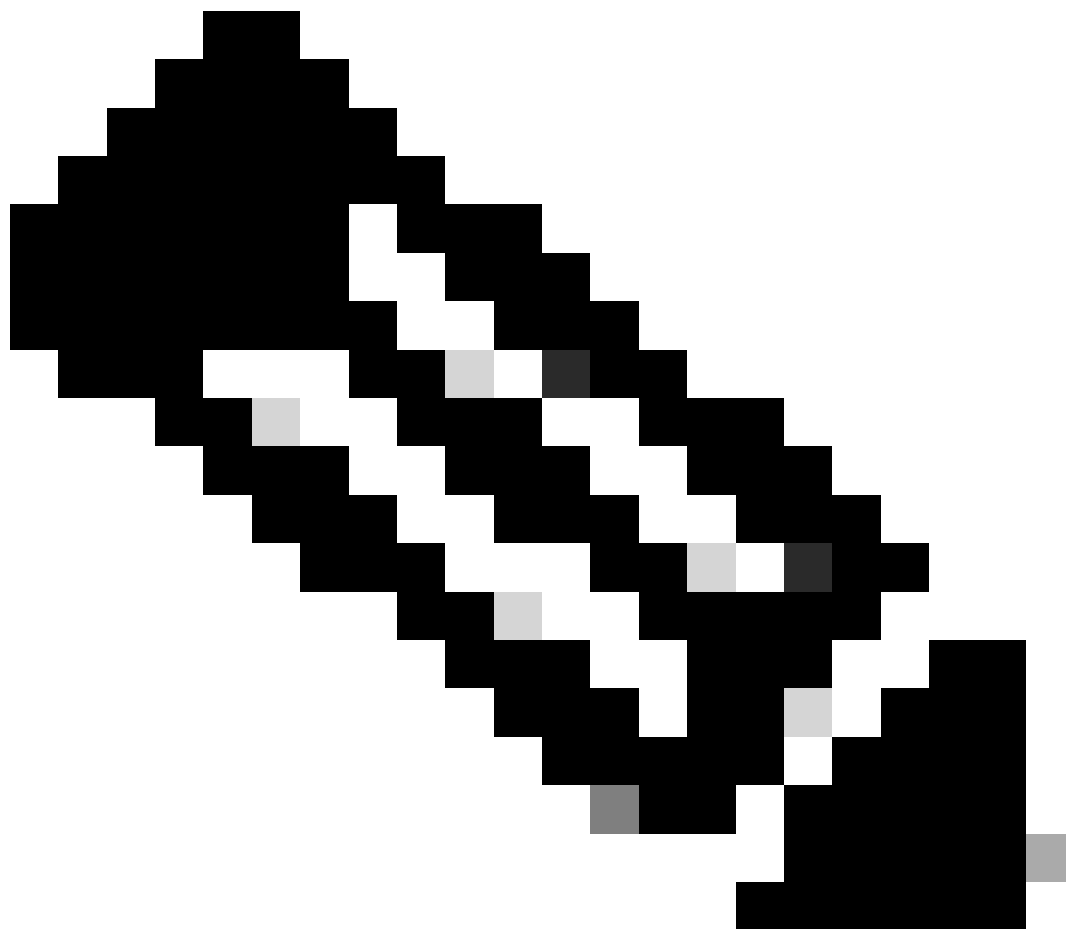
رزللا قوف رقناو راسيلا ىلع ةدوجوملا ةمئاقلا يف اثيدح هؤاشنإ مت يذلا ةومجممل جهن ددح. 3. ةمئاقلا ظفحل قفاوم قوف رقنا م، ةفاضإ



ةعومحمل اجهن ةفاضل

FTD في رعت تانايب

show رمأل اذفنو FTD في (CLI) رماوأل رطس ةهجاو لى لقتنا FTD، في نيوكتلارشن درجب ACS URL ناوونعو FTD نايبك فرعم عمجاو "saml metadata <tunnel group name>".



زاجي إلل فيرعتللا تانايب في ةدوجوملا ةداهشللا عاطتقا مت :ةظحالم

<#root>

FTD# show saml metadata SAMLtest
SP Metadata

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<EntityDescriptor entityID="

<https://vpn.example.net/saml/sp/metadata/SAMLtest>

" xmlns="urn:oasis:names:tc:SAML:2.0:metadata">
<SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
<KeyDescriptor use="signing">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>
MIIFWzCCBE0gAwIBAgITRwAAAAGZ9Nmfv5mpJQAAAAACDANBgkqhkiG9w0BAQsF
ADBJMRMwEQYKCZImiZPyLGQBGRYDY29tMRYwFAYKCZImiZPyLGQBGRYGcnRwdnBu
MRowGAYDVQQDExFydHB2cG4tV010QVVUSC1DQTAeFw0yNTAzMjUxNzU5NDZaFw0y
NzAzMjUxNzU5NDZaMDAxDzANBgNVBAoTB1JUUUFZQTJEdMBsGA1UEAxMUcnRwdnBu

LWZ0ZC5jaXNjby5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC5
5B0tH9RIjvG0MxhpDT3/BpDEffTcVE2w2fxu5m8gZFTeezyF5B93rWx+N26V8JE
sB5I1KLTGRj8b9TK6L357cdbgr692Wl952TLFB3XC43gpe0fnN3+Uas/HJ3IudsF
N+QPC9F04LE88attuGuVMquV+10DRPA06a6QNwkehB0Un7XzTNepJ02JQtxdNR2t

</ds:X509Certificate>

</ds:X509Data>

</ds:KeyInfo>

</KeyDescriptor>

<AssertionConsumerService index="0" isDefault="true" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP

https://vpn.example.net/+CSCOE+/saml/sp/acs?tgname=SAMLtest

" />

<SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://vpn

</EntityDescriptor>

رفع Microsoft Entra

1. راسي الى لىل عة دوجومل اةمئاقول ن Microsoft Entra رفع ددح، Microsoft Azure لخدم ي ف.



Create a resource



Home



Dashboard



All services



FAVORITES



All resources



Resource groups



App Services



Function App



SQL databases

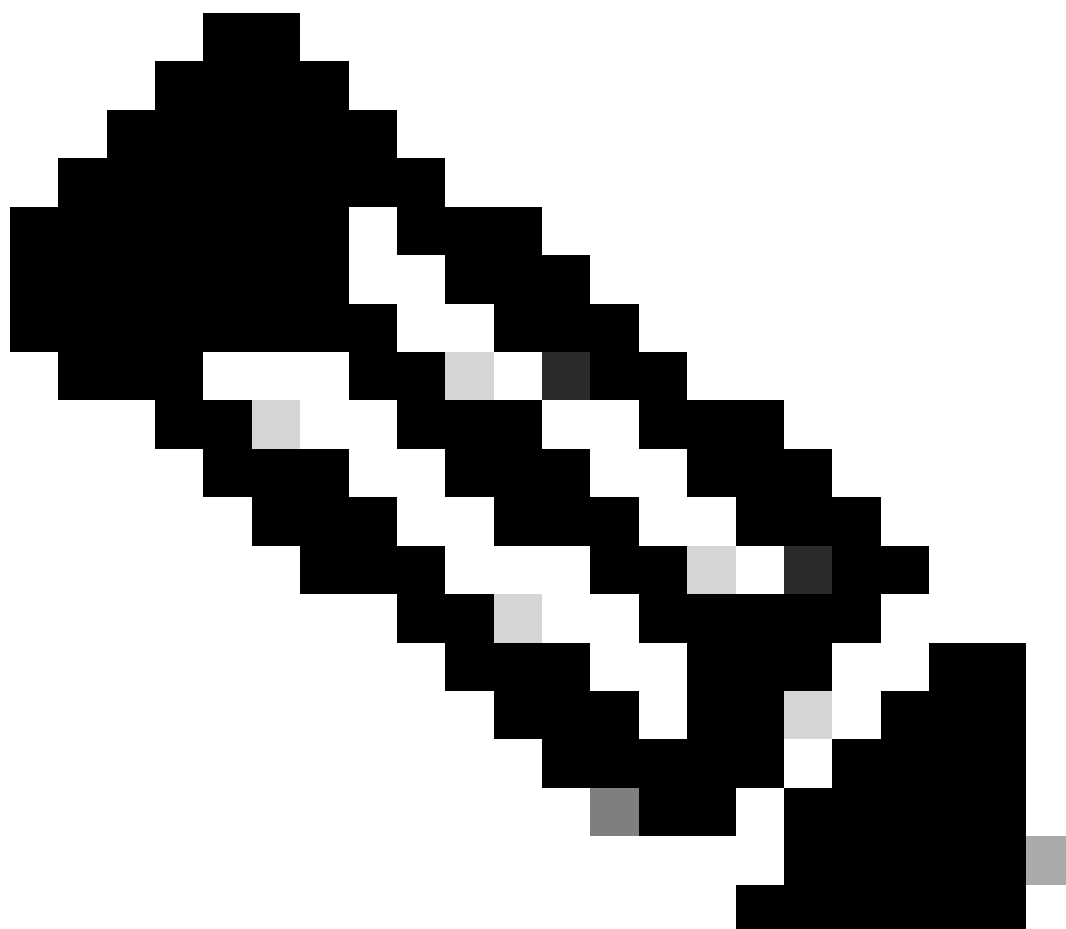


Azure Cosmos DB



Virtual machines

جهن مسا فضاً أو ردصم لل ةمسلال رتخاً م ث ،قاطنللا تاذ تاعومجم لال او مدختسم لال عون ددح .
ظفح قوف رقناو ةميقلال لقح في FTD نيوكت نم حيحصلال ةعومجم لال



جهن وه لاثم لال اذه في مدختسم لال FTD نم صصخم لال ةعومجم لال جهن مسا :ةظحال م
FMC ةعومجم جهن نيوكت مسق في هؤاشنإ م ت يذل SAMLtest-GP ىمسم لال ةعومجم لال
يذل FTD نم ةعومجم لال جهن مساب ةميقلال هذو لادبتسإ بجي .لليدللا اذه في RAPN
IdP. في ني مدختسم ةعومجم لك عم قفاوتي

User type	Scoped Groups	Source	Value
Any	1 groups	Attribute	"SAMLtest-GP"

MS Entra فرعم ةبل اطم طارش

ةحصلال نم ققحتلال

ماظن Firepower Threat Defense (FTD)

show vpn-sessiondb AnyConnect. ةب ول طم ل ةوم جم ل ةس ايس نم ق قحت لل

<#root>

FTD# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username : RTPVPNtest

Index : 7110

Assigned IP : 192.168.55.3 Public IP : 10.26.162.189

Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel

License : AnyConnect Premium

Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256

Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA256

Bytes Tx : 105817 Bytes Rx : 63694

Group Policy :

SAMLtest-GP

Tunnel Group : SAMLtest

Login Time : 16:54:17 UTC Fri May 9 2025

Duration : 0h:11m:19s

Inactivity : 0h:00m:00s

VLAN Mapping : N/A VLAN : none

Audt Sess ID : ac127ca101bc6000681e3339

Security Grp : none Tunnel Zone : 0

ءانثأ 255 debug webVPN saml ةب ول طم ل ةب لاطم ل لس ري IdP نأ نم ق قحت لل ةم سل م سق نراق وءاطخأ ل ءي حصت ي ف دي كأت ل ءارخ ل لحت ب م ق VPN. ةكبشب لاصت ل ل IdP. ل لع هنيوكت مت ام ب

<#root>

<Attribute Name="cisco_group_policy">

<AttributeValue>

SAMLtest-GP

</AttributeValue>

</Attribute>

ءءال صء وءاطخأ ل فاشك تساء

<#root>

firepower#

show run webvpn

firepower#

```
show run tunnel-group
```

```
firepower#
```

```
show crypto ca certificate
```

```
firepower#
```

```
debug webvpn saml 255
```

```
firepower#
```

```
debug webvpn 255
```

```
firepower#
```

```
debug aaa authorization
```

ةلص تاذا تامولعم

[Cisco نم تاليزنت لاوي نفللا معدلا](#)

[ASA نيوكتة لدا](#)

[FMC/FDM نيوكتة لدا](#)

ةمچرتل هذه ل و ح

ةل آل ا ت ا ي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت
م ل ا ع ل ا ا ح ن ا ع ي م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل آل ا ة م چ ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا ة ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems
(ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا