مادختساب VPN ليمع لمح ديصر نيوكت ASA ىلع ASA

تايوتحملا

ةمدقملا

يرودلا بيترتلا عم AnyConnect VPN ليمع لامحأ نزاوت نيوكت ةيفيك دنتسملا اذه حضوي ASA. يام SA.

ةيساسألا تابلطتملا

تابلطتملا

نيوكتلا اذه ءارجإ لواحت نأ لبق ةيلاتلا تابلطتملا ءافيتسا نم دكأت:

- قباوبلا تلكشو كب ةصاخلا ASA تادجو ىلع IP نيوانع نييعتب تمق دقل
 قيضارتفالا
- ىلع AnyConnect VPN نيوكت مت
- صصخملا IP ناونع مادختساب ASAs عيمجب لاصتالا VPN ةكبش يمدختسمل نكمي يدرف لكشب مهل.
- يرودلا بيترتلا ىلع رداق VPN يمدختسمب صاخلا DNS مداخ.

ةمدختسملا تانوكملا

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

- 4.10.08025 تارادصإلI AnyConnect VPN Client جمانرب
- Cisco نم 9.18.2 تارادصإلI ASA جمانرب •
- Window Server 2019

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجألاا 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.

نيوكتلا





ةكبشلل يطيطختلا مسرلا

تانيوكتلا

ASA ىلع AnyConnect VPN نيوكت .1 ةوطخلا

دنټسملا اذه ېل عجرا ،ASA د الع AnyConnect VPN نيوكټ ةيفيك يل لوصحل.

• <u>ASA 8.x: ةعقوم ةداەش نيوكت ل اثم مادختساب AnyConnect VPN ليمع عم VPN لوصو</u> <u>ايتاذ</u>

:لاثملا اذه يف ASAs نم لك نيوكت يلي اميفو

ASA1:

ip local pool anyconnect 10.4.0.100-10.4.0.200 mask 255.255.255.0

```
interface GigabitEthernet0/0
```

nameif outside security-level 0 ip address 10.1.1.1 255.255.255.0 interface GigabitEthernet0/1 nameif inside security-level 100 ip address 192.168.1.1 255.255.255.0 route outside 0.0.0.0 0.0.0.0 10.1.1.2 1 webvpn enable outside anyconnect enable tunnel-group-list enable group-policy anyconnect internal group-policy anyconnect attributes dns-server value 192.168.1.99 vpn-tunnel-protocol ssl-client default-domain value example.com username example1 password ***** username example1 attributes vpn-group-policy anyconnect service-type remote-access tunnel-group anyconnect-tunnel-group type remote-access tunnel-group anyconnect-tunnel-group general-attributes address-pool anyconnect default-group-policy anyconnect tunnel-group anyconnect-tunnel-group webvpn-attributes group-alias example enable ASA2: ip local pool anyconnect 10.4.0.100-10.4.0.200 mask 255.255.255.0 interface GigabitEthernet0/0 nameif outside security-level 0 ip address 10.2.1.1 255.255.255.0 interface GigabitEthernet0/1 nameif inside security-level 100 ip address 192.168.1.1 255.255.255.0 route outside 0.0.0.0 0.0.0.0 10.2.1.2 1 webvpn enable outside anyconnect enable tunnel-group-list enable group-policy anyconnect internal group-policy anyconnect attributes dns-server value 192.168.1.99

```
vpn-tunnel-protocol ssl-client
default-domain value example.com
username example1 password *****
username example1 attributes
vpn-group-policy anyconnect
service-type remote-access
tunnel-group anyconnect-tunnel-group type remote-access
tunnel-group anyconnect-tunnel-group general-attributes
address-pool anyconnect
default-group-policy anyconnect
tunnel-group anyconnect-tunnel-group webvpn-attributes
group-alias example enable
```

يدرف لكشب نيعملا IP ناونع مادختساب ASAs نم لكب لاصتالا ىلع ارداق نوكت نأ بجي 2. ةوطخلا ىلإ لاقتنالا لبق امەب صاخلا

DNS مداخ ىلع Round Robin DNS نيوكت .2 ةوطخلا

مداخ يأ مادختسإ كنكمي DNS مداخ مادختسإ متي ،لاثملا اذه يف ،يرئاد Capble DNS مداخ يأ مادختسإ كنكمي عجرا ،Windows مداخ ىلع ەنيوكتو DNS مداخ تيبثت ةيفيك ةفرعمل .Windows Server 2019 دنتسملا اذه ىلإ:

Windows مداخ <u>ىلع ەنيوكتو DNS مداخ تيبثت</u>

.example.com لاجملل DNS مداخ نيكمت عم Windows مداخ وه 10.3.1.4 نوكي ،لاثملا اذه يف

Å	DNS M	anager		_ 🗆 X
File Action View Help				
🗢 🄿 🙇 📰 🤉 🔹				
🚊 DNS	Name	Туре	Status	DNSSEC Status
 WIN-RTR8ICOV77A Forward Lookup Zones extemple.com Reverse Lookup Zones Trust Points Conditional Forwarders Global Logs 	example.com	Standard Primary	Running	Not Signed
	<	Ш		>

DNS مداخ

DNS: مداخل يرودلا بيترتلا نيكمت نم دكأت

- 1. مي الما حص الما المات ا
- ،نميألاا سواملا رزب رقنا ،ەترادإ يف بغرت يذلا DNS مداخ رتخأ ،مكحتلا ةدحو ةرجش يف .2 صئاصخ ددح مث.
- ددجم يرودلا بيترتلا نيكمت نأ نم دكأت ،مدقتم بيوبتلا ةمالع تحت .

Å		DI	NS Manager	_ _ X
File Action Vie	w Help			
🗢 🌩 🛛 🖂	🗙 🖾 🗟 🕞	2 🖬 🗄 🗐 🖏		
👗 DNS		Name		
■ WIN-R ■ For ■ Rev ■ Cor ■ Cor ■ Cor ■ Glo	Configure a DNS New Zone Set Aging/Scave Scavenge Stale F Update Server D Clear Cache Launch nslooku All Tasks View Delete Refresh Export List Proper Ses Help	Server Server Resource Records ata Files P		
Opens the properties	s dialog box for th	e current selection.		

1 نٻور

WIN-RTR8IC0V77A Properties

9

30

Debug Logging	1	EventLoggin	g	Monitoring
Interfaces	Forwarder	ns Ad	vanced	Root Hints
Server version number: 6.3 9600 (0x2580)				
Server options: Disable recursion Enable 50ND set Fail on load if b Enable round n Chable netmas	on (also disabi condaries ad zone data obin	es forwarden	9	×
Secure cache against polution Finable DNSSEC validation for remote responses				
Name checking:		Multibyte ()	UTF8)	~
Load zone data or	startup:	From Active	e Directory a	and registry 🛛 🛩
Enable automatic scavenging of stale records				
Scavenging pe	riod:	0	days	Ŷ
Reset to Default				
(ж	Cancel	Apply	Help

ةيناثلا ةلوجلا

مداوخل ةفيضملا ةزهجألل نيلجس ءاشنإ ASA VPN:

- 1. ميرادإ تاودأ ددح ،أدبا ةمئاق حتفا ،Windows بتكم حطس نم DNS.
- عسوو ،DNS مداخ عسوو ،ەترادا يف بغرت يذلا DNS مداخب لصتا ،مكحتلا ةدحو ةرجش يف .2 (A AA وأ A) ديدجلا فيضملا ددح مث ،نميألا سواملا رزب رقناو ،يمامألا ثحبلا ةقطنم.
- VPN ،لاثملا اذه يف .فيضملا لجسل IP ناونع و مسالا ددح ،ديدج فيضم ةشاشلا ىلع .3

.10.1.1 و

.لجسلا ءاشنإل فيضم ةفاضإ ددح .

👗 DNS Manager 📃 🗖 🗙			
File Action View Help			
🗢 🔿 🖄 📷 🗶 🖾 🧔	è 🛛 🖬 🗏 🕄		
A DNS	Name	Туре	Data
⊿ ↓ WIN-RTR8IC0V77A	📒 (same as parent folder)	Start of Authority (SOA)	[3], win-rtr8ic0v77a., host
a 📔 Forward Lookup Zones	📒 (same as parent folder)	Name Server (NS)	win-rtr8ic0v77a.
example com	over Data Eile		
Reverse Opdate 5	erver Data File		
Frust Po Reload			
b Global New Hos	(A or AAAA)		
New Alia	(CNAME)		
New Mai	Exchanger (MX)		
New Don	nain		
New Dele	gation		
Other Ne	w Records		
DNSSEC	•		
All Tasks	•		
View	•		
Delete			
Refresh			
Evport Lie			
Export en	5.00		
Propertie	5		
Create a new host n Help			

ديدج فيضم ءاشنإ

New Host		
Name (uses parent domain name if blank):		
vpn		
Fully qualified domain name (FQDN):		
vpn.example.com.		
IP address:		
10.1.1.1		
Create associated pointer (PTR) record		
R		
Add Host Cancel		

1 فيضملا لجس

،لاثملا اذه يف ،هسفن وه مسالا نأ نم دكأتو رخآ فيضم لجس ءاشنإل ةلثامملا تاوطخلا ررك، وه مسالاا ID،2.1.1 وه IP وه مسالاا

New Host	x
Name (uses parent domain name if blank):	
vpn	
Fully qualified domain name (FQDN):	
vpn.example.com.	
IP address:	_
10.2.1.1	
Create associated pointer (PTR) record	
_	
R	
Add Host Done	

2 فيضملا لجس

.vpn.example.com لِجسِلا سِفْنِب نانرتقي 10.2.1.1 و 10.1.1.1 نِيفَيضِم يَلْع روثعِلاً كَنْكَمِي

å	DNS M	anager	_ 0 X
File Action View Help			
🗢 🏟 🙋 🛅 🖾 🙆			
 DNS WIN-RTR&ICOV77A Forward Lookup Zones example.com Reverse Lookup Zones Trust Points Conditional Forwarders Global Logs 	Name (same as parent folder) (same as parent folder) vpn vpn k	Type Start of Authority (SOA) Name Server (NS) Host (A) Host (A)	Data [6], win-rtr8ic0v77a., host win-rtr8ic0v77a. 10.1.1.1 10.2.1.1
	p		

نافيضم نالجس

ةحصلا نم ققحتلا

اذه يف ،Cisco AnyConnect Secure Mobility Client تيبثت مت ثيح ليمعلا زاهج ىلإ لقتنا لائملا مداخ نأ نم ققحت ،Test-PC-1 لاثملا

Network Connection Details

Network Connection Details:

Property	Value
Connection-specific DN	
Description	Intel(R) PRO/1000 MT Network Connecti
Physical Address	52-54-00-0B-68-6F
DHCP Enabled	No
Pv4 Address	10.3.1.2
IPv4 Sult vet Mask	255.255.255.0
Pv4 Default Gateway	10.3.1.1
Pv4 DNS Server	10.3.1.4
IPv4 WINS Server	
NetBIOS over Topip En	Yes
Link-local IPv6 Address	fe80::6147:aeeb:9647:9004%16
IPv6 Default Gateway	
IPv6 DNS Server	
<	>
	Close

PC1 IP ناونع

 \times



نأ نكمي ،اەسفن فيرعتل ةرابعلل ايتاذ ةعقوم ةداەش مادختسال ارظن :ةظحالم اەلوبق بجيو ةعقوتم ەذە .ليصوتلا ةلواحم ءانثأ ةددعتم تاداەش تاريذحت رەظت ةيتاذ ةداەشلا نوكت نأ بجي ،ەذە صيخرتلا تاريذحت بنجتل .لاصتالا ةعباتمل زاەجب صاخلا ەب قوثوملا تاداەشلا نزخم يف ةتبثم اەميدقت متي يتلا عيقوتلا عجرملا ةداەش نوكت نأ بجيف ،مادختسالا ديق ةيجراخ ةەج ةداەش تناكا ذا وأ ،ليمعلا .

مدختسملا مسا لخدأو vpn.example.com كب ةصاخلا ثبلاو لابقتسالا ةدحو VPN ىلإ تطبر دامتعالا تانايبو.



مادختسإ متي ،يضارتفا لكشب ؛ةعونتم ءاطخأ حيحصت تايوتسم نييعت كنكمي ءاطخألا حيحصت عاستا نإف ،ءاطخألا حيحصت ىوتسم رييغتب تمق اذإ .1 ىوتسملا جاتنإلاا تائيب يف ًةصاخو ،رذحب كلذب مق .دادزي.

ASA. ىلع يصيخشتلا VPN لاصتال ءاطخألاا حيحصت نيكمت كنكمي

• debug webvpn anyconnect - االمعب تالاصتال لوح عاطخألا حيحصت لئاسر ضرعي AnyConnect VPN.

امحالصإو ليمعلا بناج يلع اميلع روثعلا مت يتلا ةعئاشلا لكاشملا فاشكتسال دنتسملا <u>اذه</u> يل عجرا.

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