

# تامدختي وکت FTP/TFTP: ASA 9.x

تایوتیم

مقدمة

## ةيسي اس، ألا تابلط تتملا

تاتل طت ملا

## قسم ملائکہ و تابوت

قیس اس اتامولعمر

## **قسم تعلم الـLock وـRBL**

نیوکرک

## ةكبش للى طختلا مسرلا

لـما خلا عضـولـلـنـوـكـمـلـاـFTPـلـيـمـعـ.ـ2ـوـرـانـيـسـلـاـ

## ةكبش للى طختلا مسرلا

لایسنس اینترنتی وکت متن 3. ویرانی سیستم

## ةكبش للى طختلا مسرلا

## ةكبش للى طختلا مسرا

ایق لاریغ TCP ذفنم یلع FTP لوكوتورب صحف نیوکت

ةحصـلـانـمـقـقـحتـلـا

TFTP

یس اس ال ا TFTCP قیب طت صحف نیوک

## ةكبش للى طختلا مسرلا

ةحصـلـانـمـقـقـحتـلـا

## اہم احوالوں کی تعریف

## ةكبش لالخادل يمعلما

## قىجراخ ئىكباش يەلىم علا

ةمدقم

ASA و ASA صحف نیوکت یل ع ۃفلتخم TFTP و FTP صحف تاھویرانیس دنتسمل اذه فصی  
یس اس ا لکش ب اوحالص او ءاطخآلما فاشکتس او FTP/TFTP

## ةيسيس ألا تابلطت ملا

تابلطتما

يصلوCisco مبرعه وملات اتعوضات لالات:

- ةبولطملا تاهج اولا نيب يس اسألا لاصت اala

- ڈاکس یف دوجو مل ا DMZ مداخ نیوکت

ةمدختسملا تانوكمل

لباقل ناما زاهج ىلع ۋە فلتخم TFTP و FTP صحف تاھویرانیس دنتسىملا اذه فصىي اھالىسى او عاطخاًلا فاشكىتسا او ASA FTP/TFTP صحف نىوكت يىطغى امك (ASA) فيكتلى لىس اسأ لىكشىب.

- جم انربلا ۃروص لغشی یذلا ASA 5500-X Series ASA 9.1(5)
  - مدادخ یا FTP
  - لیمع یا FTP

ڦڻا خ ڦيلمعم ڦئيپ يف ڦدوجوملا ڙزهچ ڳالا نم دنتس ملما اذه يف ڦدراولما تامولعملما ٽاشنامت  
تناك اذا (يضارتفا) حوس مم نيوكتب دنتس ملما اذه يف ڦمدختس ملما ڙزهچ ڳالا عيمج تأدب  
رمأ يأ لـ ڦمتـ حـملـا رـيـثـ ڦـتلـ لـ ڪـمـ هـ فـ نـمـ دـڪـأـتـ فـ ،ـ ڦـيـغـ شـ تـ لـاـ دـيـقـ ڪـتـ ڪـبـ شـ

ةيسياسة اسلامیہ

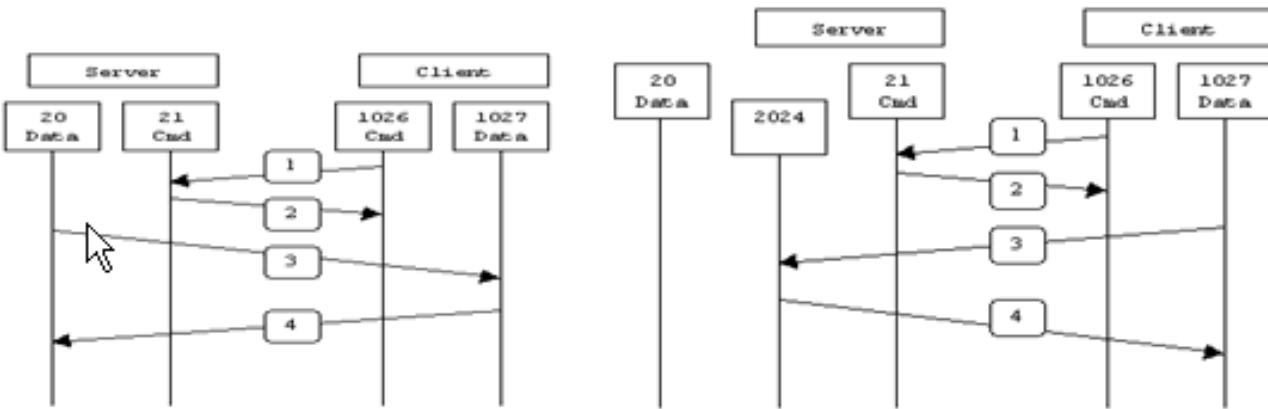
عېتتى، ئەلدىعەملا نامألا ۋىزمىزراو خەممىد خەستىت يىذلا ئەللا دەھىي يىذلا تاقىيىب طەتلە صەھىف لەلخ نەم  
وەتىچەلەص نەمىضىي و ۋەتىچەلە رادىج ربۇعى لاصىتالك نامألا زاھىج.

تمولعمل اعيمجتل لاصتالا ةلاح ،ةلاحلا نع ربعملها صحفلا لالخ نم ،ةيامحلا رادج بقاري امك ةلاح لودج يف اهعضول.

تارارق دنتس ت ،ل وؤس ملا لب ق نم ڏدھمل ا دعاوچلا یل ا ڦفاض ٻالاب ڦل ا حل ا لودج مادخت س ا ب را ڏج ربع اقب س م اهري رمت مت یتل ا مزح ل ا ڦطس اوب هؤا شن ا مت یذل ا قاي س ل ا یل ا ڦي فص ت ل ا ڦي ا مح ل ا.

•**فلا ينفع**: ينبع من عدم القدرة على إثبات المدعى به، أو عدم توفر أدلة تؤكّد المدعى به.

- رورملا ۃکرح دیدحت
  - رورملا ۃکرح یلع شیتفتلا تایلمع قیبٹت
  - ۃھجاو یلع شیتفتلا تایلمع طیشنت
  - ۃروصلالا یف حضوم وہ امک FTP نم نالکش کا
  - طشنللا عضولما
  - لمالاخنلا عضولما



**Active FTP**

**Passive FTP**

Active FTP :

command : client >1023 -> server 21  
data : client >1023 <- server 20

Passive FTP :

command : client >1023 -> server 21  
data : client >1023 -> server >1023

## طشن FTP

ىلإ (N>1023) تازاييتما يذريغ يئاوشع ذفنم نم ليجعل لاصتي ، طشنلا FTP عضوييف لاسراو N>1023 ذفنملا ىلإ عامتسا لاف ليمعل ادبى مث. FTP مداخن (21) رمألا ذفنم ڈدحملاتانايبلالا ذفانمب ىرخأ ڈرم مداخلا لاصتى مث. FTP N>1023 رمأ ذفنم 20 ذفنملا وه يذلار، بصالا يلحملا تانايبلالا ذفنم نم ليجعل.

## يبلس FTP

رادج ڈلكشم لحى امم ، مداخلاب تالاصتالا الک ڈئي هتب ليمعلاب موقى ، يبلسلا FTP عضوييف حتف دنع . مداخلاب نم ليمعلاب ڈراولاتانايبلالا ذفنم لاصتا ڈيفصتبا موقى يذلا ڈيامحلا لوالا ذفنملا لاصتى . ايلاحم ني ظوظحم رىغ ايئاوشع نيدفنم ليمعلا حتفى ، لاصتا ىرخأ ڈرم لاصتالاب مداخلل حامسل او port رمألا ليمعلاردىصى ، بصالا ىلع مداخلاب كلذ دعب مداخلا نأ اذه نم ڈجيتنل او PASV . رمألا ليمعلا لسرىو (P>1023) تازاييتما يذريغ ايئاوشع اذفنم حتفى . ليمعلا ىلإ ىرخأ ڈرم port P رمألا ليمعلاردىصى ، نامألا زاهج ىلع صحفلا رمأ نيوكت نودب . تانايبلالا لقnel مداخلا ىلع P ذفنملا ىلإ N>1023 ذفنملا نم لاصتالا عدباب ليمعلاموقى كلذ دعب نيذلا نيمدختسملا لخاد نم FTP لمعى ، نامألا زاهج ىلع صحفلا رمأ نيوكت نودب . تانايبلالا جاجت إللا جراخ نيمدختسملا لوصوض فرمتى امك . لماخلا عضولاي ف طقف رداصلانوسارتى مداخ ىلإ دراولالا FTP .

## TFTP

نيب اهتاباتك و تافلملا ئعارقل اطيسب الوكوتورب ، RFC 1350 يف حضوم و هامك ، دعي TFTP ذفنم UDP 69. مداخ تفتسى .

## ةمدقتملا لوكوتوربلا ةجلاعم

## اذا مل جات حت فیل صحف

نام آلă زاهج قي بطبت صحف ةفي طاو ةطس اوب ةصالخ ةجل اعم تاقي بطبتلă ضع ب بل طبت تان اي ب ةمزح يف IP ةنونع تامولعم نيمضتب تاقي بطبتلă نم عاونآلă هذه موقف Cisco. لمعت. يكيماني دل كشب ةنيعمل ملا ذفان ملا ىلع ئيوناث لاتاون قل احتف وأ مدخلت سملأ عقوم دي دجت يف ةدعاسم ل (NAT) ةكبش لاناونع ةمجرت عم قي بطبتلă صحف ةفي طاو ةنمضم ملا ةنونعل ا تامولعم.

قىيىب طتلىا صحف ئەفييظو بقارت، ئەنم مىز ملا ئەنون علا تام وولعەم فيرعت ىلإ ئەفاض إلاب ذفانم تالا وكتور بىلا نم دىي دەعلا حەفت. ئەيون اشلىا تاون قىلل ذفانملا ما قرا دىي دەختل تاسلىجلا فورعەم ذفانم ىلىع ئېلىل وڭلا ئەسلىجلا مادختسىا مەتىي. ئادألا نى سەختل ئەيون اشلىا UDP وTCP يەكيمان يىدى لىك شىپ ئەن يەعمەل ذفانملا ما قرا ىلىع ضوافتلىل.

ةيكيمانى دلا ذفنملاتانىي عت فرعتو، تاسلجلالا هذه قىب طتلاصحف ةفيظو بقارت تاقىب طت ضرعت. ةددجملا تاسلجلالا ۆدم لاوەت ذفانملالا هذه ئىلع تانايىبلالا لدابتب حمسەت و كولسلا نم عونلما اذه FTP و ئەددۇتمەلە طەسىسەنلە.

تاسلچ موقت الوبطل اذه لهاجت متيس، نامألا زاهج ىلع FTP صحف نيكمت متى مل اذا ٽبولطم تانايي ب يالاسراب.

بلط ىلع فرع تلا لواح يو مكحتلا ٽانق بقاري ASA ناف، ىلع FTP صحف نيك مت مت اذا رورم ٽكرح يف تانايبل ٽانق ذفنم تافص اوام FTP لوكوت ورب جمدي. تانايبل ٽانق حتفل تانايبل ٽذفانم تارييغتل مكحتلا ٽانق صحف ناما ال زاهج نم بلطتي و، مكحتلا ٽانق

ةانق رورم ةكرحل تقوف حتف عاشناب موقى هناف، ام بلطىل ع فرعتلاب ASA موقى نأ درجمب ةانق شىيتفت FTP لابقاري، ئقيرطلما ھذھب .لمعلا ئسلىج ۋەدم لاووط رمتست يېتلاتانايبلالووطل ءانىيم تايىطعلملا ىلۇغ تىلداپت نوكىي نأ تايىطعم حمسىي، لزانت data-port نىيعي، مكحتلا ئسلىجلا.

ة طيرخ لالخ نم يض ارت فا للكشب FTP رورم ةكرحل 21 ذفنملات الاصتا صحفب ASA موقى ئيبلس و ئاطشنى سلچ نېيپ قرفلا ئىلع اضي ئانامألا زاهج فرعتى . ماعلا صحفلا ئيف

رمألا لالخ نم ASA نإف ،يبلسلا FTP تاناياب لقن مععدت FTP تاسلجم تناك اذا 1023 نم ربكأ ديدج تاناياب ذفنم حتفي و مدخلتسملأا نم تانايابلا ذفنم بـلـطـىـلـع فـرـعـتـيـ.

ماهیات این فایلها ممکن است از موارد زیر باشد:

- یکیمانید یوناٹ تانایب لاصت ادادع
  - ڈباجتسا-رمأ لسلست بقعت
  - قیقدت لجس عاشنا
  - NAT مادختساپ جمدم ناونعلما مجرتی

تاونقل اصي صخت متي .FTP تاناي ب لقnel ئيونا ثلا تاونقلا قىب طت صحف دعى ض وافت لل ئاعضاخ نوكت نأ بجيو، ليلى د ئامئا قىدح وأ فلم ليزنت وأ فلم لي محتل ئاباجتسا PASV وأ ذفنمل رمأوا لالخ نم ذفنمل اىلع ض وافتلا متي .قبس ملا (227).

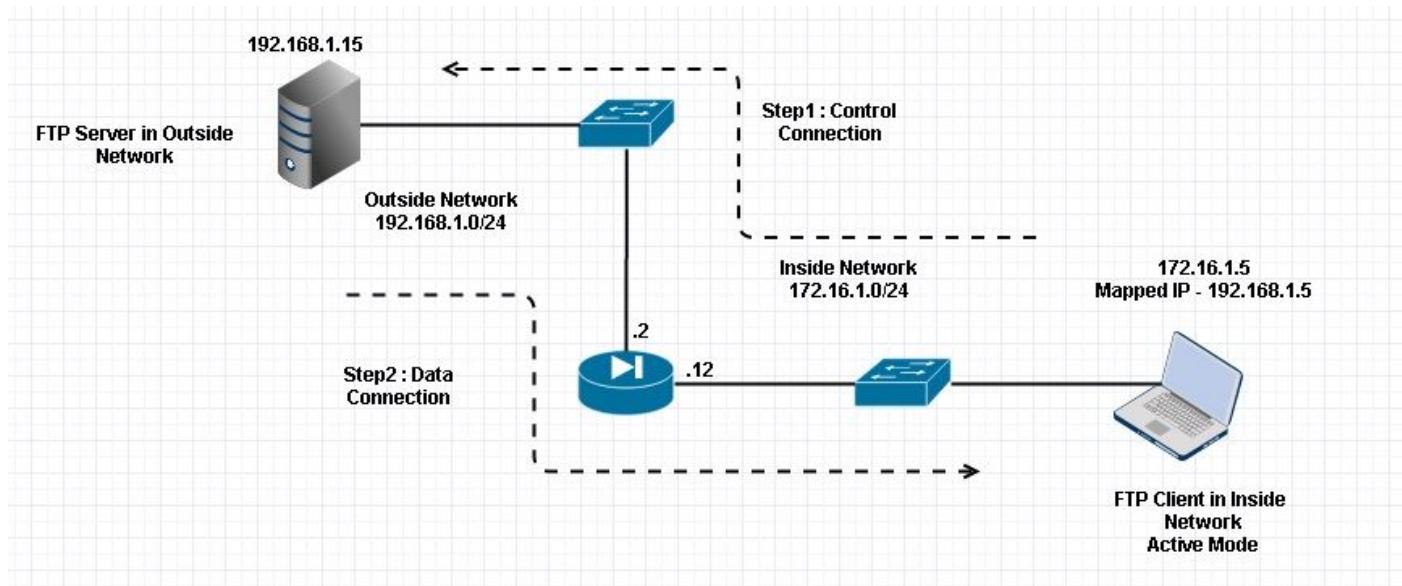
# نیوکتل

اىلع FTP صحف نېكمت عم ۋە كېشلە تاھويرانىسىم حىرىش مەتى ئەظحالىم ASA.

## طشنلۇ اعضوللۇ لىيمۇن ئېوكت مەت 1. ويرانىسىلە

ئەيجراخ ۋە كېش يەف مداخلاو ASA نەم ۋە لىخاد ۋە كېش لىصتمەتلىك لىيمۇن.

### ۋە كېشلە ئەيجراخ ئەنۋەتلىك مەسەرلە



اىلنوناقلىكشت اذە يەف لەمعتسىي ئەطاخى سىيل ip لە ئەظحالىم تىرنەنەلە.

يەف لەمعلا ئەلە ASA ئەلە مەختىمىلە دادعا يەوتتەي، ئەرسىلە ھەذە يەف حەضورم وە امك عەم ئەيجراخلا ۋە كېشلە يەف دەچۈم مداخلا IP 172.16.1.5 مادختىساب ئەلە كېشلە 192.168.1.15 . ئەيجراخلا ۋە كېشلە يەف 192.168.1.5 نىعەم IP ھىدىل لەمعلا.

ۋە ئەنۋەتلىك ئەيجراخلا ئەھجىلە ئەلە لەوصو ئەمئاقي يەپ حامىسىل ئەجەج دەجوت ئەل يەكىمانىدىلە ذەنەملىلە.

نېوكتلە لاثم:

<#root>

```
ASA Version 9.1(5)
!
hostname ASA
domain-name corp. com
enable password WwXYvtKrnjXqGbu1 encrypted
names
!
interface GigabitEthernet0/0
```

```
nameif Outside
security-level 0
ip address 192.168.1.2 255.255.255.0
!
interface GigabitEthernet0/1
nameif Inside
security-level 50
ip address 172.16.1.12 255.255.255.0
!
interface GigabitEthernet0/2
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/3
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
management-only
shutdown
no nameif
no security-level
no ip address
```

!--- Output is suppressed.

!--- Object groups is created to define the host.

```
object network obj-172.16.1.5
subnet 172.16.1.0 255.255.255.0
```

!--- Object NAT is created to map Inside Client to Outside subnet IP.

```
object network obj-172.16.1.5
nat (Inside,Outside) dynamic 192.168.1.5

class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
 message-length maximum 512

policy-map global_policy
```

```
class inspection_default
```

```

inspect dns preset_dns_map

inspect ftp

inspect h323 h225
inspect h323 ras
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
!

!--- This command tells the device to
!--- use the "global_policy" policy-map on all interfaces.

service-policy global_policy global

prompt hostname context
Cryptochecksum:4b2f54134e685d11b274ee159e5ed009
: end
ASA(config)#

```

QQ حصلنا نم ققحتل  
 لاصتا

```
<#root>
Client in Inside Network running ACTIVE FTP:
```

```
Ciscoasa(config)# sh conn
3 in use, 3 most used

TCP Outside
192.168.1.15:20 inside 172.16.1.5:61855
, idle 0:00:00, bytes 145096704, flags UIB
<---- Dynamic Connection Opened
```

```
TCP Outside
192.168.1.15:21 inside 172.16.1.5:61854
, idle 0:00:00, bytes 434, flags UIO
```

لسری 21 ئان يم ئياغلا ىلى 61854 ئان يم ردىص م عم ليص و تلا ييلخاد يف نوب زلا أدب ي انه ئيون اثللا / تان اي بلا لاصتا ھرودب م داخللا رشابي 6. ئعومجم ۋەميق عم ذفنم رمأ كل ذ دعب لىمعلا طاق تللا ھذه دعب ۋەرۈك ذەمللا تاوطخلا نم ئەھجوللا ذفنم باس، ح متى و 20 ردىص مللا ذفنم ب.

•**روصـلـا هـذـه يـف حـضـرـوم وـه اـمـكـ ةـيـلـخـادـلـا ةـهـجـاـوـلـا طـاقـتـلـا**

No.	Time	Source	Destination	Protocol	Length	Info
15	12.10.101618	172.16.1.5	192.168.1.15	TCP	66	61854+21 [SYN] Seq=1052038301 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
16	12.10.22228	192.168.1.15	172.16.1.5	TCP	66	21-61854 [SYN, ACK] Seq=1737976540 Ack=1052038302 Win=8192 Len=0 MSS=1380 WS=256 SACK_PERM=1
17	12.10.24727	172.16.1.5	192.168.1.15	TCP	54	61854+21 [ACK] Seq=1052038302 Ack=1737976541 Win=131100 Len=0
18	12.10.4013	192.168.1.15	172.16.1.5	FTP	96	Response: 220 Filezilla Server version 0.9.33 beta
19	12.10.42227	192.168.1.15	172.16.1.5	FTP	99	Response: 220-written by Tim Kosse (Tim.Kosse@gmx.de)
20	12.10.4395	192.168.1.15	172.16.1.5	FTP	115	Response: 220 Please visit <a href="http://sourceforge.net/projects/filezilla/">http://sourceforge.net/projects/filezilla/</a>
21	12.10.4456	172.16.1.5	192.168.1.15	TCP	54	61854+21 [ACK] Seq=1052038302 Ack=1737976628 Win=131012 Len=0
22	12.10.86698	172.16.1.5	192.168.1.15	FTP	66	Request: USER cisco
23	12.10.9461	192.168.1.15	172.16.1.5	FTP	87	Response: 331 Password required for cisco
24	12.11.2726	172.16.1.5	192.168.1.15	FTP	69	Request: PASS cisco123
25	12.11.3611	192.168.1.15	172.16.1.5	FTP	69	Response: 230 Logged on
26	12.11.5640	172.16.1.5	192.168.1.15	FTP	61	Request: CWD /
27	12.11.6311	192.168.1.15	172.16.1.5	FTP	101	Response: 250 CWD successful. "/" is current directory.
28	12.327680	172.16.1.5	192.168.1.15	TCP	54	61854+21 [ACK] Seq=1052038336 Ack=1737976784 Win=130856 Len=0
29	13.761258	172.16.1.5	192.168.1.15	FTP	62	Request: TYPE I
30	13.762311	192.168.1.15	172.16.1.5	FTP	73	Response: 200 Type set to I
31	13.764135	172.16.1.5	192.168.1.15	FTP	79	Request: PORT 172.16.1.5,241,159
32	13.765179	192.168.1.15	172.16.1.5	FTP	83	Response: 200 Port command successful
33	13.766278	172.16.1.5	192.168.1.15	FTP	84	Request: RETR n7000-s2-dk9.6.2.12.bin
34	13.767849	192.168.1.15	172.16.1.5	TCP	66	20-61855 [SYN] Seq=2835235612 Win=8192 Len=0 MSS=1380 WS=4 SACK_PERM=1
35	13.768109	172.16.1.5	192.168.1.15	TCP	66	61855+20 [SYN, ACK] Seq=266238504 Ack=2835235613 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM=1
36	13.768170	192.168.1.15	172.16.1.5	FTP	99	Response: 150 Opening data channel for file transfer.
37	13.768551	192.168.1.15	172.16.1.5	TCP	54	20-61855 [ACK] Seq=2835235613 Ack=266238505 Win=131100 Len=0
38	13.769787	192.168.1.15	172.16.1.5	FTP-DATA	1434	FTP Data: 1380 bytes
39	13.769802	192.168.1.15	172.16.1.5	FTP-DATA	1434	FTP Data: 1380 bytes

• ةروصلـا هـذه يـف حـضـوم وـه اـمـك ةـيـجـراـخـلـا ةـهـجـاـوـلـا طـاقـتـلـا

No.	Time	Source	Destination	Protocol	Length	Info
15	12.101633	192.168.1.5	192.168.1.15	TCP	66	61854+21 [SYN] Seq=1859474367 Win=8192 Len=0 MSS=1380 WS=4 SACK_PERM=1
16	12.102091	192.168.1.15	192.168.1.5	TCP	66	21->61854 [SYN, ACK] Seq=213433641 Ack=1859474368 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
17	12.102366	192.168.1.5	192.168.1.15	TCP	54	61854+21 [ACK] Seq=1859474368 Ack=213433642 Win=131100 Len=0
18	12.103876	192.168.1.15	192.168.1.5	FTP	96	Response: 220-Filezilla Server version 0.9.33 beta
19	12.104105	192.168.1.15	192.168.1.5	FTP	99	Response: 220-written by Tim Kosse (Tim.Kosse@gmx.de)
20	12.104273	192.168.1.15	192.168.1.5	FTP	115	Response: 220 Please visit <a href="http://sourceforge.net/projects/filezilla/">http://sourceforge.net/projects/filezilla/</a>
21	12.104334	192.168.1.5	192.168.1.15	TCP	54	61854+21 [ACK] Seq=1859474368 Ack=213433729 Win=131012 Len=0
22	12.108591	192.168.1.5	192.168.1.15	FTP	66	Request: USER cisco
23	12.109323	192.168.1.15	192.168.1.5	FTP	87	Response: 331 Password required for cisco
24	12.112604	192.168.1.5	192.168.1.15	FTP	69	Request: PASS cisco123
25	12.113489	192.168.1.15	192.168.1.5	FTP	69	Response: 230 Logged on
26	12.115518	192.168.1.5	192.168.1.15	FTP	61	Request: CWD /
27	12.116174	192.168.1.15	192.168.1.5	FTP	101	Response: 250 CWD successful. "/" is current directory.
28	12.327574	192.168.1.5	192.168.1.15	TCP	54	61854+21 [ACK] Seq=1859474402 Ack=213433885 Win=130856 Len=0
29	13.761166	192.168.1.5	192.168.1.15	FTP	62	Request: TYPE I
30	13.762173	192.168.1.15	192.168.1.5	FTP	73	Response: 200 Type set to I
31	13.764294	192.168.1.5	192.168.1.15	FTP	80	Request: PORT 192.168.1.5,241,159
32	13.765057	192.168.1.15	192.168.1.5	FTP	83	Response: 200 Port command successful
33	13.766171	192.168.1.5	192.168.1.15	FTP	84	Request: RETR n7000-s2-dk9.6.2.12.bin
34	13.767636	192.168.1.15	192.168.1.5	TCP	66	20->61855 [SYN] Seq=1406112684 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
35	13.768002	192.168.1.5	192.168.1.15	TCP	66	61855+20 [SYN, ACK] Seq=785612049 Ack=1406112685 Win=65535 Len=0 MSS=1380 WS=128 SACK_PERM=1
36	13.768032	192.168.1.15	192.168.1.5	FTP	99	Response: 150 Opening data channel for file transfer.
37	13.768429	192.168.1.15	192.168.1.5	TCP	54	20->61855 [ACK] Seq=1406112685 Ack=785612050 Win=131100 Len=0
38	13.769665	192.168.1.15	192.168.1.5	FTP-DATA	1434	FTP Data: 1380 bytes
39	13.769680	192.168.1.15	192.168.1.5	FTP-DATA	1434	FTP Data: 1380 bytes

جاحس 2 ونانونع رسیا 4 لـا .ةتس لصأ نم نیسملم رخآ مادختس اب ذفنملـا ةميـق باـسـح متـي  
= 241\*256 + 159 = 61855.  
IP نانونع ،ةروصلـا هـذـه يـف حـضـوم وـه اـمـك .عـانـيـمـلـلـ دـيـدـخـتـ

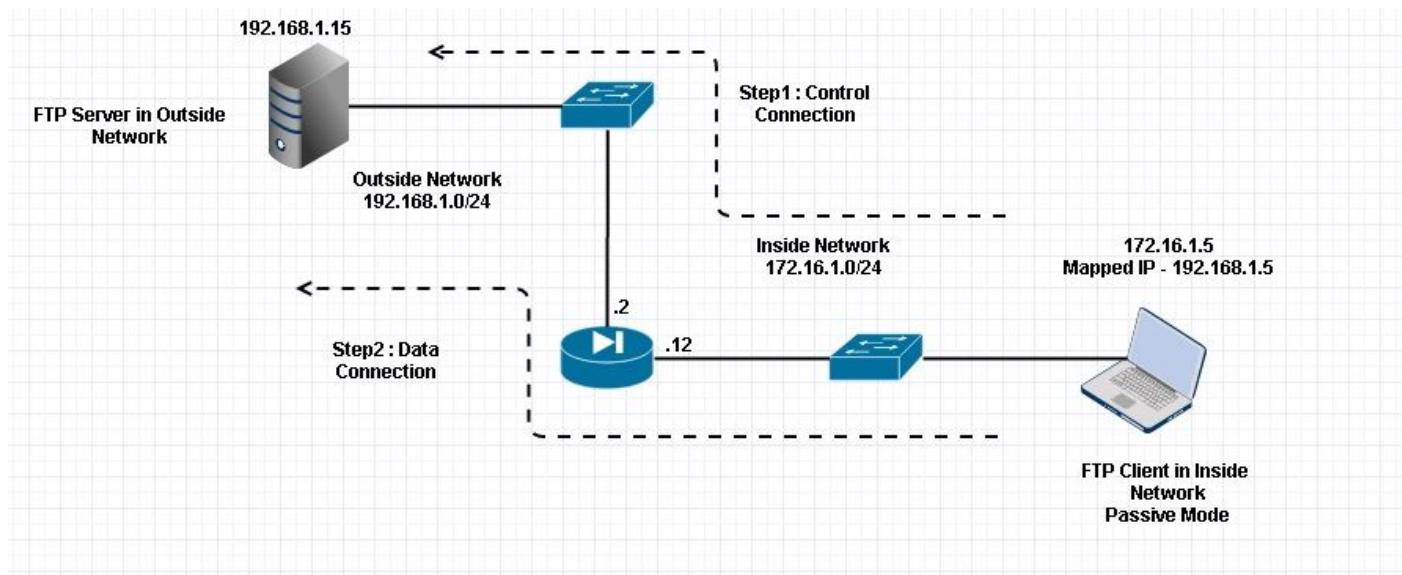
رهظي FTP صحف نيكمت دناع ريغت ذفنملارماوع ميقلا نا اضيأ طاقتل الا حضوي  
ليمعلا ةطساوب هلاسرا مت يذلا ذفنمل او IP ل ئيقيقحلا ئميقلا ئيلخادلا ئهجاول طاقتلا  
ناونعلاب ضرع ئيجراخل ئهجاول طاقتلا ئانايبلار ئانقول ليمعلا بلاص بتاول مداخلل

نـيـعـمـاـ.

## لـمـاخـلـا عـضـوـلـل نـوـكـمـلـا F~T~P لـيـمـعـ 2. وـيـرـانـيـسـلـا

ةـيـجـرـاخـلـا ةـكـبـشـلـا يـف مـدـاخـلـا وـأـS~A نـم ةـيـلـخـادـلـا ةـكـبـشـلـا يـف لـيـمـعـلـا.

### ةـكـبـشـلـل يـطـيـطـخـتـلـا مـسـرـلـا



### لـاصـتـالـا

<#root>

Client in Inside Network running Passive Mode FTP:

```
ciscoasa(config)# sh conn
3 in use, 3 most used

TCP Outside
192
.168.1.15:60142 inside 172.16.1.5:61839
, idle 0:00:00, bytes 184844288, flags UI
<--- Dynamic Connection Opened.
```

```
TCP Outside
192.168.1.15:21 inside 172.16.1.5:61838
, idle 0:00:00, bytes 451, flags UIO
```

هـنـأـ اـمـبـ 21ـ نـمـ عـانـيـمـ ةـيـاغـلـاـ 61838ـ ءـانـيـمـ رـدـصـمـ عـمـ لـيـصـوـتـ لـخـادـ نـوبـزـلـاـ أـدـبـيـ اـنـهـ درـيـ،ـ رـمـأـلـاـ لـيـمـعـلـاـ لـسـرـيـ نـأـ دـعـبـ،ـ كـلـذـلـ نـيـتـلـصـوـلـاـ الـكـ ةـئـيـهـتـبـ لـيـمـعـلـاـ مـوـقـيـ،ـ يـبـلـسـ تـانـايـبـلـاـ لـاـصـتـالـ سـبـقـمـلـاـ اـذـبـ لـيـمـعـلـاـ لـصـتـيـوـ 6ـ ةـلـسـلـسـلـاـ ةـمـيـقـبـ مـدـاـخـلـاـ.

## ةـروـصـلـاـ هـذـهـ يـفـ حـضـوـمـ وـهـ اـمـكـ ةـيـلـخـادـلـاـ ةـهـجـاـوـلـاـ طـاقـتـلـاـ.

No.	Time	Source	Destination	Protocol	Length	Info
48	35.656329	192.168.1.5	192.168.1.15	TCP	66	61838-21 [SYN] Seq=1456310600 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
49	35.657458	192.168.1.15	192.16.1.5	TCP	66	21-61838 [SYN, ACK] Seq=1456310601 Win=8192 Len=0 MSS=1380 WS=256 SACK_PERM=1
50	35.657717	192.16.1.5	192.168.1.15	TCP	54	61838-21 [ACK] Seq=1456310601 Ack=700898683 Win=131100 Len=0
51	35.659701	192.168.1.15	192.16.1.5	FTP	96	Response: 220-FileZilla Server version 0.9.33 beta
52	35.659853	192.168.1.15	192.16.1.5	FTP	99	Response: 220-written by Tim Kosse (Tim.Kosse@gmx.de)
53	35.660036	192.16.1.5	192.168.1.15	TCP	54	61838-21 [ACK] Seq=1456310601 Ack=700898770 Win=131012 Len=0
54	35.660677	192.168.1.15	192.16.1.5	FTP	115	Response: 220 Please visit http://sourceforge.net/projects/filezilla/
55	35.661837	192.16.1.5	192.168.1.15	FTP	66	Request: USER cisco
56	35.664904	192.168.1.15	192.16.1.5	FTP	87	Response: 331 Password required for cisco
57	35.665621	192.16.1.5	192.168.1.15	FTP	69	Request: PASS cisco123
58	35.666521	192.168.1.15	192.16.1.5	FTP	69	Response: 230 Logged on
59	35.668825	192.16.1.5	192.168.1.15	FTP	61	Request: CWD /
60	35.669496	192.168.1.15	192.16.1.5	FTP	101	Response: 250 CWD successful. "/" is current directory.
61	35.670351	192.16.1.5	192.168.1.15	FTP	59	Request: PWD
62	35.671022	192.168.1.15	192.16.1.5	FTP	85	Response: 257 "/" is current directory.
63	35.873908	192.16.1.5	192.168.1.15	TCP	54	61838-21 [ACK] Seq=1456310640 Ack=700898957 Win=130824 Len=0
64	37.549675	192.16.1.5	192.168.1.15	FTP	62	Request: TYPE I
65	37.550789	192.168.1.15	192.16.1.5	FTP	73	Response: 200 Type set to I
66	37.551399	192.16.1.5	192.168.1.15	FTP	60	Request: PASV
67	37.559015	192.168.1.15	192.16.1.5	FTP	104	Response: 227 Entering Passive Mode (192.168.1.15,234,238)
68	37.556114	192.16.1.5	192.168.1.15	FTP	84	Request: RETR n7000-s2-dk9.6.2.12.bin
69	37.559150	192.16.1.5	192.168.1.15	TCP	66	61839-60142 [SYN] Seq=597547299 Win=65535 Len=0 MSS=1460 WS=4 SACK_PERM=1
70	37.55978	192.168.1.15	192.16.1.5	TCP	66	60142-61839 [SYN, ACK] Seq=2027855230 Ack=597547300 Win=8192 Len=0 MSS=1380 WS=256 SACK_PERM=1
71	37.559791	192.16.1.5	192.168.1.15	TCP	54	61839-60142 [ACK] Seq=597547300 Ack=2027855231 Win=262140 Len=0
72	37.560524	192.168.1.15	192.16.1.5	FTP	79	Response: 150 Connection accepted
73	37.578223	192.168.1.15	192.16.1.5	FTP-DATA	1434	FTP Data: 1380 bytes
74	37.578238	192.168.1.15	192.16.1.5	FTP-DATA	1434	FTP Data: 1380 bytes
■ Internet Protocol Version 4, Src: 192.168.1.15 (192.168.1.15), Dst: 172.16.1.5 (172.16.1.5)						
■ Transmission Control Protocol, Src Port: 21 (21), Dst Port: 61838 (61838), Seq: 700898976, Ack: 1456310654, Len: 50						
■ File Transfer Protocol (FTP)						
■ 227 Entering Passive Mode (192.168.1.15,234,238)\r\n						
Response code: Entering Passive Mode (227)						
Response arg: Entering Passive Mode (192.168.1.15,234,238)						
Passive IP address: 192.168.1.15 (192.168.1.15)						
Passive port: 60142						
0030	01 ff d0 fb 00 00 32 32	37 20 45 6e 74 65 72 69	.....22 7 Enteri			
0040	6e 67 20 50 61 73 73 69	76 65 20 4d 6f 64 65 20	ng Passi ve Mode			
0050	28 31 39 32 21 31 36 38	2c 31 2c 31 35 2c 32 33	(192.168 .1.15,23			
0060	34 2c 32 33 38 29 0d 0a	4,238)..				

## ةـروـصـلـاـ هـذـهـ يـفـ حـضـوـمـ وـهـ اـمـكـ ةـيـجـرـاـخـلـاـ ةـهـجـاـوـلـاـ طـاقـتـلـاـ.

No.	Time	Source	Destination	Protocol	Length	Info
48	35.656299	192.168.1.5	192.168.1.15	TCP	66	61838-21 [SYN] Seq=2543303555 Win=8192 Len=0 MSS=1380 WS=4 SACK_PERM=1
49	35.657290	192.168.1.15	192.168.1.5	TCP	66	21-61838 [SYN, ACK] Seq=599740450 Ack=2543303556 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
50	35.657580	192.168.1.5	192.168.1.15	TCP	54	61838-21 [ACK] Seq=2543303556 Ack=599740451 Win=131100 Len=0
51	35.659533	192.168.1.15	192.168.1.5	FTP	96	Response: 220-FileZilla Server version 0.9.33 beta
52	35.659686	192.168.1.15	192.168.1.5	FTP	99	Response: 220-written by Tim Kosse (Tim.Kosse@gmx.de)
53	35.659884	192.168.1.15	192.168.1.15	TCP	54	61838-21 [ACK] Seq=2543303556 Ack=5997404538 Win=131012 Len=0
54	35.660510	192.168.1.15	192.168.1.15	FTP	115	Response: 220 Please visit http://sourceforge.net/projects/filezilla/
55	35.661700	192.168.1.15	192.168.1.15	FTP	66	Request: USER cisco
56	35.664736	192.168.1.15	192.168.1.15	FTP	87	Response: 331 Password required for cisco
57	35.665484	192.168.1.15	192.168.1.15	FTP	69	Request: PASS cisco123
58	35.666369	192.168.1.15	192.168.1.15	FTP	69	Response: 230 Logged on
59	35.668673	192.168.1.15	192.168.1.15	FTP	61	Request: CWD /
60	35.669344	192.168.1.15	192.168.1.15	FTP	101	Response: 250 CWD successful. "/" is current directory.
61	35.670199	192.168.1.15	192.168.1.15	FTP	59	Request: PWD
62	35.670870	192.168.1.15	192.168.1.15	FTP	85	Response: 257 "/" is current directory.
63	35.873786	192.168.1.15	192.168.1.15	TCP	54	61838-21 [ACK] Seq=2543303595 Ack=599740725 Win=130824 Len=0
64	37.549569	192.168.1.15	192.168.1.15	FTP	62	Request: TYPE I
65	37.550622	192.168.1.15	192.168.1.15	FTP	73	Response: 200 Type set to I
66	37.551262	192.168.1.15	192.168.1.15	FTP	60	Request: PASV
67	37.554818	192.168.1.15	192.168.1.15	FTP	104	Response: 227 Entering Passive Mode (192.168.1.15,234,238)
68	37.55977	192.168.1.15	192.168.1.15	FTP	84	Request: RETR n7000-s2-dk9.6.2.12.bin
69	37.559075	192.168.1.15	192.168.1.15	TCP	66	61839-60142 [SYN] Seq=737544148 Win=65535 Len=0 MSS=1380 WS=4 SACK_PERM=1
70	37.559410	192.168.1.15	192.168.1.15	TCP	66	60142-61839 [SYN, ACK] Seq=4281507304 Ack=737544149 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
71	37.559654	192.168.1.15	192.168.1.15	TCP	54	61839-60142 [ACK] Seq=737544149 Ack=4281507305 Win=262140 Len=0
72	37.560356	192.168.1.15	192.168.1.15	FTP	79	Response: 150 Connection accepted
73	37.578071	192.168.1.15	192.168.1.15	FTP-DATA	1434	FTP Data: 1380 bytes
74	37.578086	192.168.1.15	192.168.1.15	FTP-DATA	1434	FTP Data: 1380 bytes
■ Internet Protocol Version 4, Src: 192.168.1.15 (192.168.1.15), Dst: 192.168.1.5 (192.168.1.5)						
■ Transmission Control Protocol, Src Port: 21 (21), Dst Port: 61838 (61838), Seq: 599740744, Ack: 2543303609, Len: 50						
■ File Transfer Protocol (FTP)						
■ 227 Entering Passive Mode (192.168.1.15,234,238)\r\n						
Response code: Entering Passive Mode (227)						
Response arg: Entering Passive Mode (192.168.1.15,234,238)						
Passive IP address: 192.168.1.15 (192.168.1.15)						
Passive port: 60142						
0030	01 ff dc bd 00 00 32 32	37 20 45 6e 74 65 72 69	.....22 7 Enteri			
0040	6e 67 20 50 61 73 73 69	76 65 20 4d 6f 64 65 20	ng Passi ve Mode			
0050	28 31 39 32 2c 31 36 38	2c 31 2c 31 35 2c 32 33	(192.168 .1.15,23			
0060	34 2c 32 33 38 29 0d 0a	4,238)..				

## وهـ اـمـكـ ذـفـانـمـلـابـ صـاخـلـاـ باـسـحـلـاـ يـقـبـيـ.

امـكـ صـحـفـ نـيـكـمـتـ مـتـ اـذـ ةـنـمـضـمـلـاـ IPـ مـيـقـ ةـبـاتـكـ ةـدـاعـإـبـ ASAـ مـوـقـيـ،ـ اـقـبـاسـ اـنـرـكـذـ اـمـكـ وـهـ تـانـايـبـلـاـ لـاـصـتـالـ سـبـقـمـلـاـ اـذـبـ لـيـمـعـلـاـ لـصـتـيـوـ 6ـ ةـلـسـلـسـلـاـ ةـمـيـقـبـ مـدـاـخـلـاـ.

## صـحـفـ لـيـطـعـتـ مـتـ اـذـ لـاـصـتـالـ اـلـيـصـافـتـ يـهـ هـذـهـ.

الا صت ل:

```
<#root>

ciscoasa(config)# sh conn
2 in use, 3 most used

TCP Outside
192.168.1.15:21 inside 172.16.1.5:61878
, idle 0:00:09, bytes 433, flags UIO
TCP Outside
192.168.1.15:21 inside 172.16.1.5:61875
, idle 0:00:29, bytes 259, flags UIO
```

ثيچ در دجوي ال نكلى وىرخأ ئرم وىرخأ ئرم ذفنملا رمأ لاسرا طقف لواحي، صحف نودب يف ئيشلا سفن راهظا مت. دح او مادختساب سيلو يلصألا IP عم ذفنملا جراخلاملىتسى غيرفتلا.

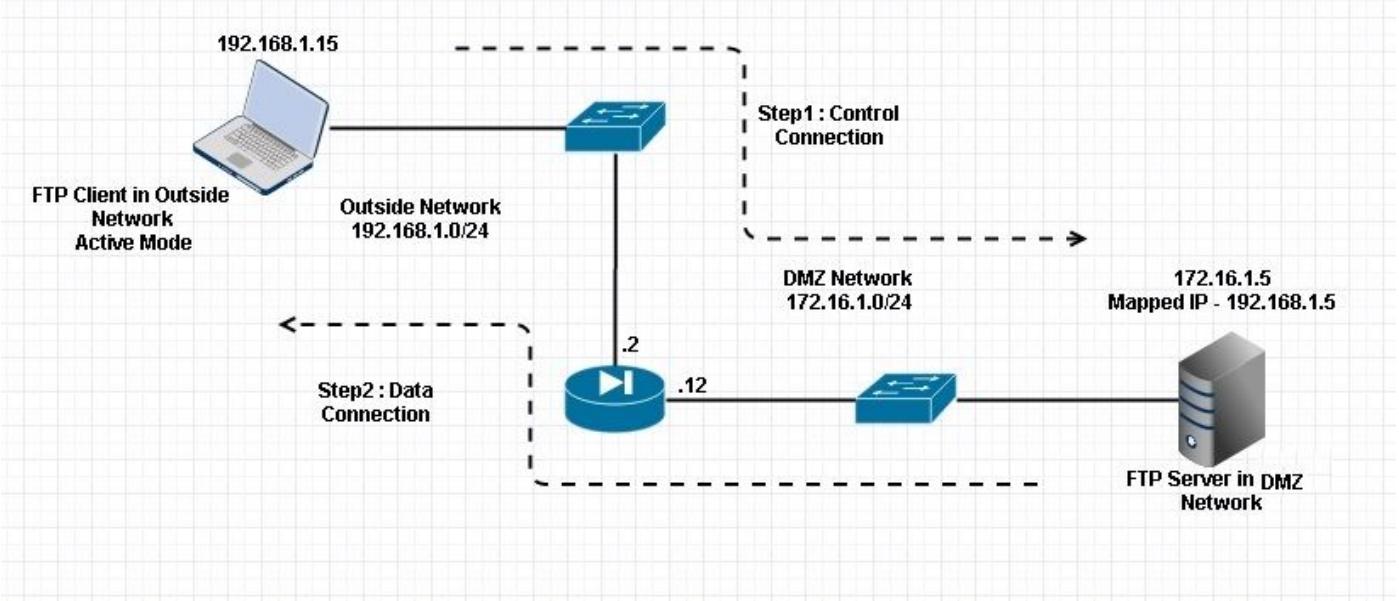
ةيفرطللا ئدحولا عضوي ف FTP رمألا مادختساب no fix protocol ftp 21 ليطعت نكمى نيوكتلل.

ال امك لخادلا يف ليجعلنا نوكى امدعن ظقف PASV رمألا لمعي، لوكوتورب صحف نودب لخادلا نم تالاصتالا الك عدب متىو هنيممضت بجي لخادلا نم مدق ذفنم رمأ دجوي.

طشنلا عضولل FTP ليمع نيوكت مت. ويرانيسلا

ةكبش يف مدخل او ASA نم ئيجراخل ةكبشلا يف ليجعلنا DMZ.

ةكبشلل يطيطختلا مسرا



نیوکتلا:

<#root>

```
ASA(config)#  
show running-config
```

```
ASA Version 9.1(5)  
!  
hostname ASA  
domain-name corp .com  
enable password WwXYvtKrnjXqGbu1 encrypted  
names  
!  
interface GigabitEthernet0/0  
nameif Outside  
security-level 0  
ip address 192.168.1.2 255.255.255.0  
!  
interface GigabitEthernet0/1  
nameif DMZ  
security-level 50  
ip address 172.16.1.12 255.255.255.0  
!  
interface GigabitEthernet0/2  
shutdown  
no nameif  
no security-level  
no ip address  
!  
interface GigabitEthernet0/3  
shutdown  
no nameif  
no security-level  
no ip address  
!  
interface Management0/0  
management-only
```

```
shutdown
no nameif
no security-level
no ip address

!--- Output is suppressed.

!--- Permit inbound FTP control traffic.

access-list 100 extended permit tcp any host 192.168.1.5 eq ftp

!--- Object groups are created to define the hosts.

object network obj-172.16.1.5
host 172.16.1.5

!--- Object NAT is created to map FTP server with IP of Outside Subnet.

object network obj-172.16.1.5
nat (DMZ,Outside) static 192.168.1.5

access-group 100 in interface outside

class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
 message-length maximum 512

policy-map global_policy

class inspection_default
inspect dns preset_dns_map

inspect ftp

inspect h323 h225
inspect h323 ras
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
```

```

inspect sip
inspect xdmcp
!
!--- This command tells the device to
!--- use the "global_policy" policy-map on all interfaces.

service-policy global_policy global

prompt hostname context
Cryptochecksum:4b2f54134e685d11b274ee159e5ed009
: end
ASA(config)#

```

ةحصل ا نم ققحتل

لاصتال:

```

<#root>

Client in Outside Network running in Active Mode FTP:

ciscoasa(config)# sh conn
3 in use, 3 most used

TCP outside 192.168.1.15:55836 DMZ 172.16.1.5:21,
idle 0:00:00, bytes 470, flags UIOB

TCP outside 192.168.1.15:55837 DMZ 172.16.1.5:20,
idle 0:00:00, bytes 225595694, flags UI
<---- Dynamic Port channel

```

ةروصل ا هذه يف حضوم وہ امک DMZ ةجھ او طاقتل.

No.	Time	Source	Destination	Protocol	Length	Info
15	12.032774	192.168.1.15	172.16.1.5	TCP	66	55836-21 [SYN] Seq=3317358682 Win=8192 Len=0 MSS=1380 WS=4 SACK_PERM=1
16	12.033598	172.16.1.5	192.168.1.15	TCP	66	21-55836 [SYN, ACK] Seq=3073360302 Ack=3317358683 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
17	12.037214	192.168.1.15	172.16.1.5	TCP	54	55836-21 [ACK] Seq=3317358683 Ack=3073360303 Win=131100 Len=0
18	12.038297	172.16.1.5	192.168.1.15	FTP	96	Response: 220-FileZilla Server version 0.9.33 beta
19	12.038434	172.16.1.5	192.168.1.15	FTP	99	Response: 220-written by Tim Kosse (Tim.Kosse@gmx.de)
20	12.038511	172.16.1.5	192.168.1.15	FTP	115	Response: 220 Please visit http://sourceforge.net/projects/filezilla/
21	12.038770	192.168.1.15	172.16.1.5	TCP	54	55836-21 [ACK] Seq=3317358683 Ack=3073360390 Win=131012 Len=0
22	12.039228	192.168.1.15	172.16.1.5	FTP	66	Request: USER cisco
23	12.040677	172.16.1.5	192.168.1.15	FTP	87	Response: 331 Password required for cisco
24	12.044767	192.168.1.15	172.16.1.5	FTP	69	Request: PASS cisco123
25	12.045575	172.16.1.5	192.168.1.15	FTP	69	Response: 230 Logged on
26	12.049313	192.168.1.15	172.16.1.5	FTP	61	Request: CWD /
27	12.049939	172.16.1.5	192.168.1.15	FTP	101	Response: 250 CWD successful. "/" is current directory.
28	12.053036	192.168.1.15	172.16.1.5	FTP	59	Request: PWD
29	12.053677	172.16.1.5	192.168.1.15	FTP	85	Response: 257 "/" is current directory.
30	12.274888	192.168.1.15	172.16.1.5	TCP	54	55836-21 [ACK] Seq=3317358722 Ack=3073360577 Win=130824 Len=0
31	13.799702	192.168.1.15	172.16.1.5	FTP	62	Request: TYPE I
32	13.800526	192.168.1.15	172.16.1.5	FTP	73	Response: 200 Type set to I
33	13.800592	192.168.1.15	172.16.1.5	FTP	80	Request: PORT 192.168.1.15,218,29
34	13.802540	172.16.1.5	192.168.1.15	FTP	83	Response: 200 Port command successful
35	13.803959	192.168.1.15	172.16.1.5	FTP	84	Request: STOR n7000-s2-dk9.6.2.12.bin
36	13.805286	172.16.1.5	192.168.1.15	TCP	66	20-55837 [SYN] Seq=1812810161 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
37	13.805454	172.16.1.5	192.168.1.15	FTP	99	Response: 150 Opening data channel for file transfer.
38	13.805805	192.168.1.15	172.16.1.5	TCP	66	55837-20 [SYN, ACK] Seq=177574185 Ack=1812810162 Win=65535 Len=0 MSS=1380 WS=128 SACK_PERM=1
39	13.806049	172.16.1.5	192.168.1.15	TCP	54	20-55837 [ACK] Seq=1812810162 Ack=177574186 Win=131100 Len=0
40	13.820321	192.168.1.15	172.16.1.5	FTP-DATA	1434	FTP Data: 1380 bytes
41	13.820321	192.168.1.15	172.16.1.5	FTP-DATA	1434	FTP Data: 1380 bytes

Internet Protocol Version 4, Src: 192.168.1.15 (192.168.1.15), Dst: 172.16.1.5 (172.16.1.5)  
Transmission Control Protocol, Src Port: 55836 (55836), Dst Port: 21 (21), Seq: 3317358730, Ack: 3073360596, Len: 26  
File Transfer Protocol (FTP)  
PORT 192.168.1.15,218,29\r\n  
Request command: PORT  
Request arg: 192.168.1.15,218,29  
Active IP address: 192.168.1.15 (192.168.1.15)  
Active port: 55837

```
0010 00 42 7a 10 40 00 80 06 11 d9 c0 a8 01 0f ac 10 .Bz.0. . . . .  

0020 01 05 da 1c 00 15 c5 ba e0 8a b7 2f c2 d4 50 18 .....  

0030 7f bd 31 od 00 00 50 4f 52 54 20 31 39 32 2c 31 ..1..PO RT 192.1  

0040 36 38 2c 31 2c 31 35 2c 32 31 38 2c 32 39 0d 0a 68.1.15, 218,29..
```

روصلـا هـذـه يـف حـضـوـم وـه اـمـك ةـيـجـراـخـلـا ةـهـجـاـولـا طـاقـتـلـا

No.	Time	Source	Destination	Protocol	Length	Info
21	12.045240	192.168.1.15	192.168.1.15	TCP	66	55836-21 [SYN] Seq=2466096898 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
22	12.046232	192.168.1.15	192.168.1.15	TCP	66	21-55836 [SYN, ACK] Seq=726281311 Ack=2466096899 Win=8192 Len=0 MSS=256 SACK_PERM=1
23	12.049803	192.168.1.15	192.168.1.15	TCP	54	55836-21 [ACK] Seq=2466096899 Ack=726281312 Win=131100 Len=0
24	12.050916	192.168.1.15	192.168.1.15	FTP	96	Response: 220-FileZilla Server version 0.9.33 beta
25	12.051054	192.168.1.15	192.168.1.15	FTP	99	Response: 220-written by Tim Kosse (Tim.Kosse@gmx.de)
26	12.051115	192.168.1.15	192.168.1.15	FTP	115	Response: 220 Please visit http://sourceforge.net/projects/filezilla/
27	12.051359	192.168.1.15	192.168.1.15	TCP	54	55836-21 [ACK] Seq=2466096899 Ack=726281399 Win=131012 Len=0
28	12.051817	192.168.1.15	192.168.1.15	FTP	66	Request: USER cisco
29	12.053281	192.168.1.15	192.168.1.15	FTP	87	Response: 331 Password required for cisco
30	12.057355	192.168.1.15	192.168.1.15	FTP	69	Request: PASS cisco123
31	12.058194	192.168.1.15	192.168.1.15	FTP	69	Response: 230 Logged on
32	12.061902	192.168.1.15	192.168.1.15	FTP	61	Request: CWD /
33	12.062558	192.168.1.15	192.168.1.15	FTP	101	Response: 250 CWD successful. "/" is current directory.
34	12.065640	192.168.1.15	192.168.1.15	FTP	59	Request: PWD
35	12.066281	192.168.1.15	192.168.1.15	FTP	85	Response: 257 "/" is current directory.
36	12.287476	192.168.1.15	192.168.1.15	TCP	54	55836-21 [ACK] Seq=2466096938 Ack=726281586 Win=130824 Len=0
37	13.812275	192.168.1.15	192.168.1.15	FTP	62	Request: TYPE I
38	13.813145	192.168.1.15	192.168.1.15	FTP	73	Response: 200 Type set to I
39	13.814610	192.168.1.15	192.168.1.15	FTP	80	Request: PORT 192.168.1.15,218,29
40	13.815159	192.168.1.15	192.168.1.15	FTP	83	Response: 200 Port command successful
41	13.816548	192.168.1.15	192.168.1.15	FTP	84	Request: STOR n7000-s2-dk9.6.2.12.bin
42	13.817967	192.168.1.15	192.168.1.15	TCP	66	20-55837 [SYN] Seq=3719615815 Win=8192 Len=0 MSS=1380 WS=4 SACK_PERM=1
43	13.818058	192.168.1.15	192.168.1.15	FTP	99	Response: 150 Opening data channel for file transfer.
44	13.818409	192.168.1.15	192.168.1.15	TCP	66	55837-20 [SYN, ACK] Seq=2377334290 Ack=3719615816 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM=1
45	13.818653	192.168.1.15	192.168.1.15	TCP	54	20-55837 [ACK] Seq=3719615816 Ack=2377334291 Win=131100 Len=0
46	13.832910	192.168.1.15	192.168.1.15	FTP-DATA	1434	FTP Data: 1380 bytes
47	13.832925	192.168.1.15	192.168.1.15	FTP-DATA	1434	FTP Data: 1380 bytes

Internet Protocol Version 4, Src: 192.168.1.15 (192.168.1.15), Dst: 192.168.1.5 (192.168.1.5)  
Transmission Control Protocol, Src Port: 55836 (55836), Dst Port: 21 (21), Seq: 2466096946, Ack: 726281605, Len: 26  
File Transfer Protocol (FTP)  
PORT 192.168.1.15,218,29\r\n  
Request command: PORT  
Request arg: 192.168.1.15,218,29  
Active IP address: 192.168.1.15 (192.168.1.15)  
Active port: 55837

```
0010 00 42 7a 10 40 00 80 06 fd 40 c0 a8 01 0f c0 a8 .8z.0. .@....  

0020 01 05 da 1c 00 15 c5 ba a7 32 2b 4a 2d 85 50 18 .....  

0030 7f bd 31 bf 00 00 50 4f 52 54 20 31 39 32 2c 31 ..1..PO RT 192.1  

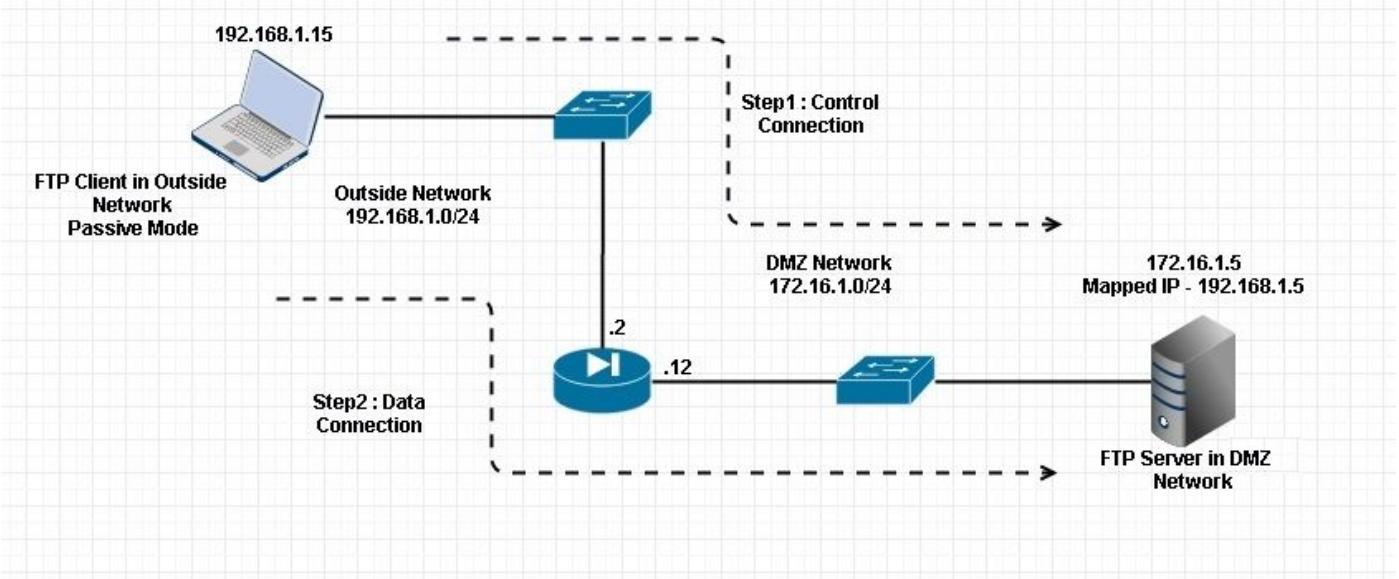
0040 36 38 2c 31 2c 31 35 2c 32 31 38 2c 32 39 0d 0a 68.1.15, 218,29..
```

يـف مـدـاـخـلـا لـاـصـتـالـا أـدـبـيـوـمـ طـشـنـلـا عـضـوـلـا لـيـمـعـ لـيـغـشـتـبـ لـيـمـعـ لـيـوـقـيـ، اـنـهـ مـدـاـخـلـا إـلـا فـاعـضـأـ تـسـ ةـمـيـقـبـ ذـفـنـمـلـا رـمـأـ لـيـمـعـلـا لـسـرـيـ، كـلـذـدـعـبـ 21ـ ذـفـنـمـلـا إـلـعـ تـانـاـيـبـلـا لـاـصـتـاـ عـدـبـ بـ كـلـذـدـعـبـ مـدـاـخـلـا يـفـ لـيـمـعـلـا ذـفـنـمـلـا كـلـذـبـ لـاـصـتـاـلـلـ 20ـ كـرـدـصـمـلـا ذـفـنـمـبـ.

## لمـاـخـلـا عـضـوـلـا لـيـغـشـيـ يـذـلـا F~T~P لـيـمـعـ 4ـ وـيـرـانـيـسـلـا

ةـكـبـشـ يـفـ مـدـاـخـلـا ةـيـجـراـخـلـا ةـهـجـاـولـا يـفـ لـيـمـعـلـا

ةـكـبـشـلـلـ يـطـيـطـخـتـلـا مـسـرـلـا



## لاصتالا

<#root>

Client in Outside Network running in Passive Mode FTP:

```
ciscoasa(config)# sh conn
3 in use, 3 most used
```

TCP

```
outside 192.168.1.15:60071 DMZ 172.16.1.5:61781
, idle 0:00:00, bytes 184718032, flags UOB
```

```
<--- Dynamic channel Open
```

TCP

```
outside 192.168.1.15:60070 DMZ 172.16.1.5:21
, idle 0:00:00, bytes 413,
flags UIOB
```

ةروصل اهذه يف حضوم وہ امک DMZ ۃجھ او طاقتلہ.

No.	Time	Source	Destination	Protocol	Length	Info
15	23.516688	192.168.1.15	172.16.1.5	TCP	66	60070>21 [SYN] Seq=3728695688 Win=8192 Len=0 MSS=1380 WS=4 SACK_PERM=1
16	23.517161	172.16.1.5	192.168.1.15	TCP	66	21>60070 [SYN, ACK] Seq=397133843 Ack=3728695689 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
17	23.517527	192.168.1.15	172.16.1.5	TCP	54	60070>21 [ACK] Seq=3728695689 Ack=397133844 Win=131100 Len=0
18	23.521479	172.16.1.5	192.168.1.15	FTP	96	Response: 220-Filezilla Server version 0.9.33 beta
19	23.521708	172.16.1.5	192.168.1.15	FTP	99	Response: 220-written by Tim Kosse (Tim.Kosse@gmx.de)
20	23.521967	172.16.1.5	192.168.1.15	FTP	115	Response: 220 Please visit http://sourceforge.net/projects/filezilla/
21	23.522196	192.168.1.15	172.16.1.5	TCP	54	60070>21 [ACK] Seq=3728695689 Ack=397133931 Win=131012 Len=0
22	23.523737	192.168.1.15	172.16.1.5	FTP	66	Request: USER cisco
23	23.524546	172.16.1.5	192.168.1.15	FTP	87	Response: 331 Password required for cisco
24	23.526468	192.168.1.15	172.16.1.5	FTP	69	Request: PASS cisco123
25	23.528284	172.16.1.5	192.168.1.15	FTP	69	Response: 230 Logged on
26	23.531885	192.168.1.15	172.16.1.5	FTP	61	Request: CWD /
27	23.532602	172.16.1.5	192.168.1.15	FTP	101	Response: 250 CWD successful. "/" is current directory.
28	23.536661	192.168.1.15	172.16.1.5	FTP	62	Request: TYPE I
29	23.537378	172.16.1.5	192.168.1.15	FTP	73	Response: 200 Type set to I
30	23.538842	192.168.1.15	172.16.1.5	FTP	60	Request: PASV
31	23.539860	172.16.1.5	192.168.1.15	FTP	101	Response: 227 Entering Passive Mode (172.16.1.5,241,85)
32	23.541726	192.168.1.15	172.16.1.5	FTP	84	Request: RETR n7000-s2-dk9.6.2.12.bin
33	23.543984	192.168.1.15	172.16.1.5	TCP	66	60071>61781 [SYN] Seq=4174881931 Win=65535 Len=0 MSS=1380 WS=4 SACK_PERM=1
34	23.544229	172.16.1.5	192.168.1.15	TCP	66	61781>60071 [SYN, ACK] Seq=4186544816 Ack=4174881932 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
35	23.544518	192.168.1.15	172.16.1.5	TCP	54	60071>61781 [ACK] Seq=4174881932 Ack=4186544817 Win=262140 Len=0
36	23.546029	172.16.1.5	192.168.1.15	FTP	79	Response: 150 Connection accepted
37	23.549172	172.16.1.5	192.168.1.15	FTP-DATA 1434	1380	FTP Data: 1380 bytes
38	23.549187	172.16.1.5	192.168.1.15	FTP-DATA 1434	1380	FTP Data: 1380 bytes
39	23.549569	192.168.1.15	172.16.1.5	TCP	54	60071>61781 [ACK] Seq=4174881932 Ack=4186547577 Win=262140 Len=0
40	23.549813	172.16.1.5	192.168.1.15	FTP-DATA 1434	1380	FTP Data: 1380 bytes
41	23.549828	172.16.1.5	192.168.1.15	FTP-DATA 1434	1380	FTP Data: 1380 bytes
⑧ Internet Protocol Version 4, Src: 172.16.1.5 (172.16.1.5), Dst: 192.168.1.15 (192.168.1.15)						
⑨ Transmission Control Protocol, Src Port: 21 (21), Dst Port: 60070 (60070), Seq: 397134106, Ack: 3728695737, Len: 47						
⑩ File Transfer Protocol (FTP)						
■ 227 Entering Passive Mode (172.16.1.5,241,85)\r\n						
Response code: Entering Passive Mode (227)						
Response arg: Entering Passive Mode (172.16.1.5,241,85)						
Passive IP address: 172.16.1.5 (172.16.1.5)						
Passive port: 61781						
0030 01 ff d8 3f 00 00 32 32 37 20 45 6e 74 65 72 69 ...?..22 7 Enteri						
0040 6e 67 20 50 61 73 73 69 76 65 20 4d 6f 64 65 20 ng Passi ve Mode						
0050 28 31 37 32 2c 31 36 2c 31 2c 35 2c 32 34 31 2c (192.168 .1,5,241,						
0060 85)..						

## رورصللا ھذه يف حضوم وه امك ۃيجراخلا ۃهجاولما طاقتلما

No.	Time	Source	Destination	Protocol	Length	Info
29	23.528818	192.168.1.15	192.168.1.5	TCP	66	60070>21 [SYN] Seq=2627142457 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
30	23.529413	192.168.1.5	192.168.1.15	TCP	66	21>60070 [SYN, ACK] Seq=1496461807 Ack=2627142458 Win=8192 Len=0 MSS=1380 WS=256 SACK_PERM=1
31	23.529749	192.168.1.15	192.168.1.5	TCP	54	60070>21 [ACK] Seq=2627142458 Ack=1496461808 Win=131100 Len=0
32	23.533731	192.168.1.5	192.168.1.15	FTP	96	Response: 220-Filezilla Server version 0.9.33 beta
33	23.533960	192.168.1.5	192.168.1.15	FTP	99	Response: 220-written by Tim Kosse (Tim.Kosse@gmx.de)
34	23.534219	192.168.1.5	192.168.1.15	FTP	115	Response: 220 Please visit http://sourceforge.net/projects/filezilla/
35	23.534433	192.168.1.5	192.168.1.5	TCP	54	60070>21 [ACK] Seq=2627142458 Ack=1496461895 Win=131012 Len=0
36	23.535974	192.168.1.5	192.168.1.5	FTP	66	Request: USER cisco
37	23.536798	192.168.1.5	192.168.1.5	FTP	87	Response: 331 Password required for cisco
38	23.538705	192.168.1.5	192.168.1.5	FTP	69	Request: PASS cisco123
39	23.540521	192.168.1.5	192.168.1.15	FTP	69	Response: 230 Logged on
40	23.544122	192.168.1.15	192.168.1.5	FTP	61	Request: CWD /
41	23.544854	192.168.1.5	192.168.1.15	FTP	101	Response: 250 CWD successful. "/" is current directory.
42	23.548898	192.168.1.15	192.168.1.5	FTP	62	Request: TYPE I
43	23.549630	192.168.1.5	192.168.1.15	FTP	73	Response: 200 Type set to I
44	23.551064	192.168.1.15	192.168.1.5	FTP	60	Request: PASV
45	23.552169	192.168.1.15	192.168.1.15	FTP	102	Response: 227 Entering Passive Mode (192.168.1.5,241,85)
46	23.553948	192.168.1.15	192.168.1.5	FTP	84	Request: RETR n7000-s2-dk9.6.2.12.bin
47	23.556176	192.168.1.15	192.168.1.5	TCP	66	60071>61781 [SYN] Seq=3795016102 Win=65535 Len=0 MSS=1460 WS=4 SACK_PERM=1
48	23.556466	192.168.1.15	192.168.1.5	TCP	66	61781>60071 [SYN, ACK] Seq=1047360618 Ack=8192 Len=0 MSS=1380 WS=256 SACK_PERM=1
49	23.556740	192.168.1.15	192.168.1.5	TCP	54	60071>61781 [ACK] Seq=3795016103 Ack=1047360619 Win=262140 Len=0
50	23.558281	192.168.1.5	192.168.1.15	FTP	79	Response: 150 Connection accepted
51	23.561409	192.168.1.5	192.168.1.15	FTP-DATA 1434	1380	FTP Data: 1380 bytes
52	23.561424	192.168.1.5	192.168.1.15	FTP-DATA 1434	1380	FTP Data: 1380 bytes
53	23.561806	192.168.1.5	192.168.1.15	TCP	54	60071>61781 [ACK] Seq=3795016103 Ack=1047363379 Win=262140 Len=0
54	23.562065	192.168.1.5	192.168.1.15	FTP-DATA 1434	1380	FTP Data: 1380 bytes
55	23.562081	192.168.1.5	192.168.1.15	FTP-DATA 1434	1380	FTP Data: 1380 bytes
⑧ Frame 45: 102 bytes on wire (816 bits), 102 bytes captured (816 bits)						
⑨ Ethernet II, Src: Cisco_c9:92:88 (00:19:e8:c9:92:88), Dst: Vmware_ad:ad:24:76 (00:50:56:ad:24:76)						
⑩ Internet Protocol Version 4, Src: 192.168.1.5 (192.168.1.5), Dst: 192.168.1.15 (192.168.1.15)						
⑪ Transmission Control Protocol, Src Port: 21 (21), Dst Port: 60070 (60070), Seq: 1496462070, Ack: 2627142506, Len: 48						
⑫ File Transfer Protocol (FTP)						
■ 227 Entering Passive Mode (192.168.1.5,241,85)\r\n						
Response code: Entering Passive Mode (227)						
Response arg: Entering Passive Mode (192.168.1.5,241,85)						
0030 01 ff c3 f5 00 00 32 32 37 20 45 6e 74 65 72 69 .....22 7 Enteri						
0040 6e 67 20 50 61 73 73 69 76 65 20 4d 6f 64 65 20 ng Passi ve Mode						
0050 28 31 39 32 2c 31 36 38 2c 31 2c 35 2c 32 34 31 2c (192.168 .1,5,241,						
0060 85)..						

## يـسـاسـالـا قـيـبـطـلـا صـحـفـ نـيـوـكـتـ

No.	Time	Source	Destination	Protocol	Length	Info
1	23.562081	192.168.1.15	192.168.1.5	TCP	66	60070>21 [SYN] Seq=2627142457 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
2	23.562413	192.168.1.5	192.168.1.15	TCP	66	21>60070 [SYN, ACK] Seq=1496461807 Ack=2627142458 Win=8192 Len=0 MSS=1380 WS=256 SACK_PERM=1
3	23.562749	192.168.1.15	192.168.1.5	FTP	54	Response: 220-Filezilla Server version 0.9.33 beta
4	23.563060	192.168.1.5	192.168.1.15	FTP	99	Response: 220-written by Tim Kosse (Tim.Kosse@gmx.de)
5	23.563378	192.168.1.15	192.168.1.5	FTP	115	Response: 220 Please visit http://sourceforge.net/projects/filezilla/
6	23.563737	192.168.1.5	192.168.1.15	TCP	54	60070>61781 [ACK] Seq=4174881932 Ack=4186544817 Win=262140 Len=0
7	23.564122	192.168.1.15	192.168.1.5	FTP	66	Request: RETR n7000-s2-dk9.6.2.12.bin
8	23.564433	192.168.1.5	192.168.1.15	TCP	66	60071>61781 [ACK] Seq=4186544817 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
9	23.564854	192.168.1.15	192.168.1.5	FTP	66	Request: USER cisco
10	23.565188	192.168.1.15	192.168.1.5	FTP	87	Response: 331 Password required for cisco
11	23.565493	192.168.1.15	192.168.1.5	FTP	69	Request: PASS cisco123
12	23.565813	192.168.1.15	192.168.1.5	FTP	69	Response: 230 Logged on
13	23.566104	192.168.1.5	192.168.1.15	TCP	61	Request: CWD /
14	23.566422	192.168.1.15	192.168.1.5	101	Response: 250 CWD successful. "/" is current directory.	
15	23.566740	192.168.1.15	192.168.1.5	TCP	54	60071>61781 [ACK] Seq=3795016103 Ack=1047360619 Win=262140 Len=0
16	23.567164	192.168.1.5	192.168.1.15	FTP	79	Response: 150 Connection accepted
17	23.567489	192.168.1.15	192.168.1.5	FTP-DATA 1434	1380	FTP Data: 1380 bytes
18	23.567805	192.168.1.15	192.168.1.5	FTP-DATA 1434	1380	FTP Data: 1380 bytes
19	23.568104	192.168.1.5	192.168.1.15	TCP	54	60071>61781 [ACK] Seq=3795016103 Ack=1047363379 Win=262140 Len=0
20	23.568421	192.168.1.15	192.168.1.5	FTP-DATA 1434	1380	FTP Data: 1380 bytes
21	23.568737	192.168.1.15	192.168.1.5	FTP-DATA 1434	1380	FTP Data: 1380 bytes
22	23.56905					

1. policy-map global\_policy. رمألا ليغشتب مق.

```
<#root>  
ASA(config)#  
policy-map global_policy
```

2. class inspection\_default. رمألا ليغشتب مق.

```
<#root>  
ASA(config-pmap)#  
class inspection_default
```

### 3. صفحه رمآلایی غشت ب مق.

```
<#root>  
  
ASA(config-pmap-c)#  
  
inspect FTP
```

4. ئەيمەنلا تاكبىشلا نامأ نم رمألا اذه دېزى. FTP strict. صحف رمألا مادختسال رايىخ كانه تابلط يف ئەنمىضم رمألا سىرا نم بىولا حفصىتم عىنم بىـ FTP.

کولسلا اذه FTP صحف ضرفي، هجأو لع ديقمل رايخلا نيكمت دعوب

- ديدج رمأب نامألا زاهج حمسى نأ لبوق FTP رمأب فارتعدالا بجي
  - ةنمضم رمأواً لسري الاشتا نامألا زاهج طقسى
  - أطخ ئلسلىس يف اهروهظ مدع نامضل port 227 رمأواً نم ققحتلا متى

**⚠️** ني ذلا FTP ئالىم لش ف يف دىقملاراي خلا مادختسا ببستي نأ نكمملانم: ريدح لوصحلل [دىقملاراي خلا مادختسا](#) عجار FTP RFCs عم مراص لكشب نوقفتىي ال دىقملاراي خلا مادختسا لوح تامولعملانم ديزمىلىع.

يىس ايقلا رىغ TCP ذفنم ىلע FTP لوكوتورپ صحف نىوكت

لیکشت اذه عم ۃیسایق ریغ TCP ذفانمل شیتفت لوكوتورب FTP لـ ا تلکش عیطتسی تنأ (مقر ءانیم دیدجلا عم XXXX تلدبتسا) طخ

```
<#root>

access-list ftp-list extended permit tcp any any eq XXXX
!
class-map ftp-class
  match access-list ftp-list
!
policy-map global_policy
  class ftp-class

inspect ftp
```

## وحصلنا نم ققحتلا

کنكمي امک show service-policy. رمألا ليغشت بموقعي، حاجنب هذاختا مت دق نيوكتلا نأ نامضل show service-policy inspection ftp.

```
<#root>

ASA#
show service-policy inspect ftp

Global Policy:
  Service-policy: global_policy
  Class-map: inspection_default
    Inspect: ftp, packet 0, drop 0, reste-drop 0
ASA#
```

## TFTP

يضارتفا لکشب TFTP صحف نیکمت متی.

تامجرتل او تالاصلتالا عاشناب موقیو TFTP تانایب رورم ڈکرچ صحفب نامألا زاهج موقی جویلعلو. مداخلل او TFTP لیممع نیب تافلملا لقنب حامسلل، رمألا مزل اذا، یکیمانید لکشب ڈعاتکللا ثابلطو (RRQ) (WRQ) TFTP ڈعارق تابلط صحفب صحفل کرحم موقی، صوصخل (أطخلا) اطخللا تامالع او.

وأ لابقتسا یلعل، رمألا مزل اذا، ڈمجرتو ڈیکیمانید ڈیوناث ڈانق صیصخت متی وأ تافلملا لقnel TFTP لباق نم ڈیوناثلا ڈانقللا هذه مادختسا متی کلذ دعبو. حلاص WRQ ڈاعطخأ لاب مالع إالا.

ڈانق دجوت نأ نکمیو، ڈیوناثلا ڈانقللا رباع تانایبلا رورم ڈکرچ عدب طقف TFTP مداخل نکمی

مداخلا نم أطخلا مالع يدؤي .مداخل او TFTP ليمع نيب رثكألا ىلع ةدح او ةلمتكم ريع ئيونات ئيوناثلا قاائقلا قايلغا.

TFTP رورم ةكرح هيجوت ةداعإ تباث برض مادختسا مت اذا صحف نيكمت بجي.

## يساسألا TFTP قيبرطت صحف نيكوت

قيبرطتلا صحف رورم ةكرح لك قباطت ئاساييس نيكوتلا نمضت ،يضرارت فا لكتشب نمضت .(مامع ئاساييس) تاهج اولا عيمج ىلع رورملار ةكرح ىلع صحفلا قبطة و ئيضرارت فالا لك ئيضرارت فالا ذفانملا ىلا تانايبلار رورم ةكرح ئيضرارت فالا صحف رورم ةكرح لوكوتورب.

،مامعلا ئاسايسلار ييغت ديرت تنك اذا كلذل .طقف ةدح او ئيمومع ئاساييس قيبرطت كنكمي شيتفت تايلمع ئفاض إل وأ ،ئيسياق ريع ذفانم ىلع صحف قيبرطت ،لاثملار ليبس ىلع اهليطعات وأ ئيضرارت فالا ئاسايسلار ييرحتل اما جاتحت ،يضرارت فا لكتشب ئنكمم ريع ىلا عجرا ،ئيضرارت فالا ذفانملا عيمجب ئمئاق ىلع لوصحلل .ةديج ئاساييس قيبرطت و [ئيضرارت فالا شيتفتلا ئاساييس](#).

1. رمألا ليغشت بمق policy-map global\_policy.

```
<#root>
ASA(config)#
policy-map global_policy
```

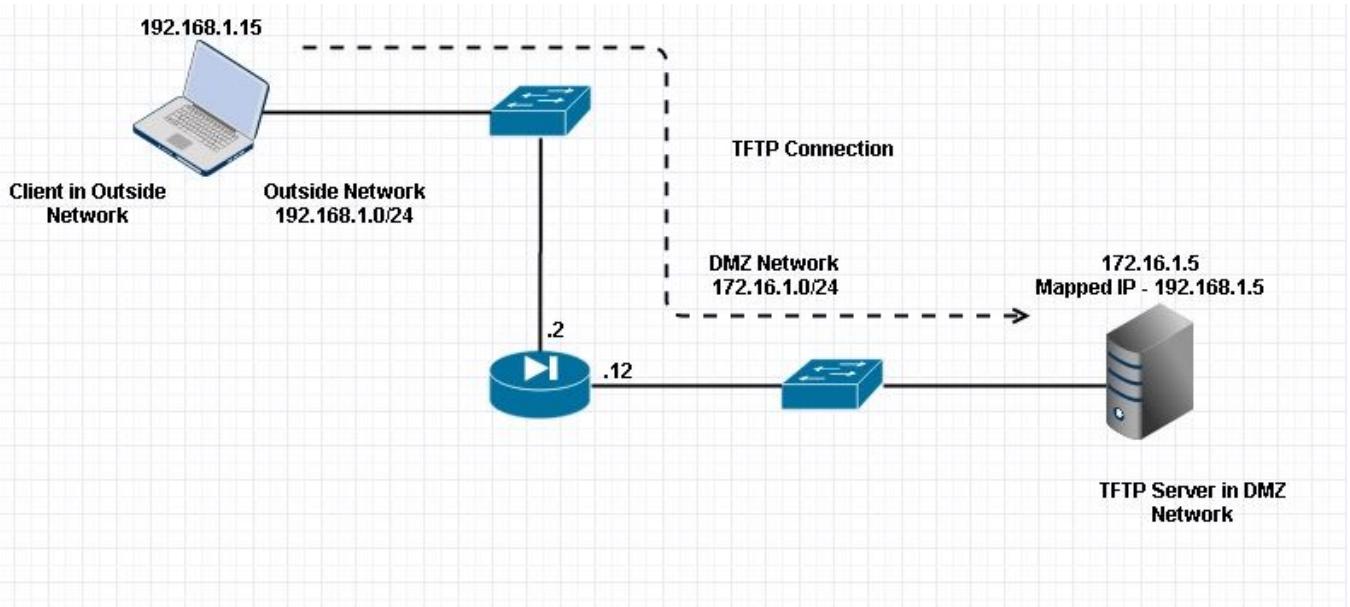
2. رمألا ليغشت بمق class inspection\_default.

```
<#root>
ASA(config-pmap)#
class inspection_default
```

3. رمألا ليغشت بمق inspection TFTP.

```
<#root>
ASA(config-pmap-c)#
inspect TFTP
```

## ةكبشلل يطي طختلا مس رلا



نېيىعت مت ئەكپش يىف TFTP مداخ عضومتى. ئىجراخ ئەكپش يىف لىكشى يىف لىيمىعىلا انھ ئىجراخلا ئىعرفلى ئەكپشلارا يىف ئەدوجوملارا ئەكپشلىع مداخلا.

نىوكىتلارا لاثم:

```
<#root>
ASA(config)#
show running-config

ASA Version 9.1(5)
!
hostname ASA
domain-name corp. com
enable password WwXYvtKrnjXqGbu1 encrypted
names
!
interface GigabitEthernet0/0
nameif Outside
security-level 0
ip address 192.168.1.2 255.255.255.0
!
interface GigabitEthernet0/1
nameif DMZ
security-level 50
ip address 172.16.1.12 255.255.255.0
!
interface GigabitEthernet0/2
shutdown
no nameif
security-level 100
ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet0/3
```

```
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
management-only
shutdown
no nameif
no security-level
no ip address

!--- Output is suppressed.

!--- Permit inbound TFTP traffic.

access-list 100 extended permit udp any host 192.168.1.5 eq tftp
!

!--- Object groups are created to define the hosts.

object network obj-172.16.1.5
host 172.16.1.5

!--- Object NAT      to map TFTP server to IP in Outside Subnet.

object network obj-172.16.1.5
nat (DMZ,Outside) static 192.168.1.5

access-group 100 in interface outside

class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum 512

policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
```

```

inspect tftp

inspect sip
inspect xdmcp
!

!---- This command tells the device to
!---- use the "global_policy" policy-map on all interfaces.

service-policy global_policy global
prompt hostname context
Cryptochecksum:4b2f54134e685d11b274ee159e5ed009
: end
ASA(config)#

```

## وتحصلنا نم ققحتلا

كـنـكـمـيـ اـمـكـ show service-policy. رـمـأـلـاـ لـيـغـشـتـبـ مـقـ،ـ حـاجـنـبـ هـذـاخـتـاـ مـتـ دقـ نـيـوـكـتـلـاـ نـأـ نـامـضـلـ  
رـمـأـلـاـ لـيـغـشـتـ لـالـخـ نـمـ طـقـفـ TFTPـ صـحـفـ ئـلـعـ جـارـخـ إـلـاـ دـيـيـقـتـ  
tftpـ.

```

<#root>

ASA#

show service-policy inspect tftp

    Global Policy:
        Service-policy: global_policy
        Class-map: inspection_default
        Inspect: tftp, packet 0, drop 0, reste-drop 0
ASA#

```

## اهـحـالـصـ اوـعـاطـخـ أـلـاـ فـاشـكـتـسـاـ

اهـحـالـصـ اوـنـيـوـكـتـلـاـ عـاطـخـ أـلـاـ فـاشـكـتـسـاـ كـنـكـمـيـ تـامـوـلـعـمـ مـسـقـلـاـ اـذـهـ رـفـوـيـ.

اهـحـالـصـ اوـعـاطـخـ أـلـاـ فـاشـكـتـسـاـ قـيـبـطـ

## ةـكـبـشـلـاـ لـخـادـ لـيـمـعـلـاـ

```

<#root>

FTP client Inside - Packet Tracer for Control Connection : Same Flow for Active and Passive.

# packet-tracer input inside tcp 172.16.1.5 12345 192.168.1.15 21 det

```

-----Omitted-----

Phase: 5

Type: INSPECT

Subtype: inspect-ftp

Result: ALLOW

Config:

```
class-map inspection_default
  match default-inspection-traffic
policy-map global_policy
  class inspection_default
    inspect ftp
service-policy global_policy global
```

Additional Information:

Forward Flow based lookup yields rule:

```
in id=0x76d9a120, priority=70, domain=inspect-ftp, deny=false
hits=2, user_data=0x76d99a30, cs_id=0x0, use_real_addr, flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0
dst ip/id=0.0.0.0, mask=0.0.0.0, port=21, dscp=0x0
input_ifc=inside, output_ifc=any
```

Phase: 6

Type: NAT

Subtype:

Result: ALLOW

Config:

```
object network obj-172.16.1.5
```

```
nat (inside,outside) static 192.168.1.5
```

Additional Information:

```
NAT divert to egress interface DMZ
translate 172.16.1.5/21 to 192.168.1.5/21
```

Phase: 7

Type: NAT

Subtype: rpf-check

Result: ALLOW

Config:

```
object network obj-172.16.1.5
```

```
nat (inside,outside) static 192.168.1.5
```

Additional Information:

Forward Flow based lookup yields rule:

```
out id=0x76d6e308, priority=6, domain=nat-reverse, deny=false
hits=15, user_data=0x76d9ef70, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0
dst ip/id=172.16.1.5, mask=255.255.255.255, port=0, dscp=0x0
input_ifc=inside, output_ifc=outside
```

----Omitted----

Result:

input-interface:

**inside**

```
input-status: up
input-line-status: up
output-interface:
```

**outside**

```
output-status: up
output-line-status: up
Action: allow
```

## ةيجراخ ةكبش يف ليمعلا

<#root>

FTP client Outside - Packet Tracer for Control Connection : Same Flow for Active and Passive

```
# packet-tracer input outside tcp 192.168.1.15 12345 192.168.1.5 21 det
```

Phase: 1

Type: UN-NAT

Subtype: static

Result: ALLOW

Config:

```
object network obj-172.16.1.5
```

```
nat (DMZ,outside) static 192.168.1.5
```

Additional Information:

NAT divert to egress interface DMZ

Untranslate 192.168.1.5/21 to 172.16.1.5/21

-----*Omitted*-----

Phase: 4

Type: INSPECT

Subtype:

**inspect-ftp**

**Result: ALLOW**

**Config:**

```
class-map inspection_default
  match default-inspection-traffic
policy-map global_policy
  class inspection_default
    inspect ftp
service-policy global_policy global
```

Additional Information:

Forward Flow based lookup yields rule:

```
in id=0x76d84700, priority=70, domain=inspect-ftp, deny=false
hits=17, user_data=0x76d84550, cs_id=0x0, use_real_addr, flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0
dst ip/id=0.0.0.0, mask=0.0.0.0, port=21, dscp=0x0
input_ifc=outside, output_ifc=any
```

Phase: 5

Type: NAT

**Subtype: rpf-check**

**Result: ALLOW**

**Config:**

```
object network obj-172.16.1.5
```

```
nat (DMZ,outside) static 192.168.1.5
```

Additional Information:

Forward Flow based lookup yields rule:

```
out id=0x76d6e308, priority=6, domain=nat-reverse, deny=false
hits=17, user_data=0x76d9ef70, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0
dst ip/id=172.16.1.5, mask=255.255.255.255, port=0, dscp=0x0
input_ifc=outside, output_ifc=DMZ
```

-----*Omitted*-----

**Result:**

input-interface:

**outside**

```
input-status: up  
input-line-status: up  
output-interface:
```

DMZ

```
output-status: up  
output-line-status: up  
Action: allow
```

مەب ئەصاخلا NAT تاھىرەت بىرپەت رورمەل ئەكىنچەن نەف، مزحلا بقۇغۇم نەم لەك يىف حەضووم وە امك  
ۋە بولطمەل لاصتاالا تاھىج او اپسىن نوكىرتى مەن امك. FTP صەحف جەن و.

ام ئەفرۇم و ASA جەرمەنلىخەم تاھىج او طاقىتلە ئەلواجم كەنگەمىي، اەحالىص او ئاطاخ ئەلە فاشكەتسا ئانىڭ  
اذا لاصتاالا نەم قىقەتلىا و حېھىص لەكشەب لەمعەت ASA نەم ضەمەلە IP ناونع ئەباتك ئەداعى تەنەك اذا  
ئىلۇي يەكىيەمانى دلە ذەنەنەمەلاب حامىسلا مەتىي نەك ASA.

## هـ لـ وـ لـ جـ رـ تـ لـ اـ هـ ذـ هـ

ةـ يـ لـ آـ لـ اـ تـ اـ يـ نـ قـ تـ لـ اـ نـ مـ مـ جـ مـ وـ عـ مـ اـ دـ خـ تـ سـ اـ بـ دـ نـ تـ سـ مـ لـ اـ اـ ذـ هـ تـ مـ جـ رـ تـ  
لـ اـ عـ لـ اـ ءـ اـ حـ نـ اـ عـ يـ مـ جـ يـ فـ نـ يـ مـ دـ خـ تـ سـ مـ لـ لـ مـ عـ دـ ئـ وـ تـ حـ مـ يـ دـ قـ تـ لـ ةـ يـ رـ شـ بـ لـ اـ وـ  
اـ مـ كـ ةـ قـ يـ قـ دـ نـ وـ كـ تـ نـ لـ ةـ يـ لـ آـ ةـ مـ جـ رـ تـ لـ ضـ فـ اـ نـ اـ ةـ ظـ حـ اـ لـ مـ ئـ جـ رـ يـ .ـ صـ اـ خـ لـ اـ مـ هـ تـ غـ لـ بـ  
يـ لـ خـ تـ .ـ فـ رـ تـ حـ مـ مـ جـ رـ تـ مـ اـ هـ دـ قـ يـ يـ تـ لـ اـ ةـ يـ فـ اـ رـ تـ حـ اـ لـ اـ ةـ مـ جـ رـ تـ لـ اـ عـ مـ لـ اـ حـ لـ اـ وـ  
ىـ لـ إـ أـ مـ ئـ اـ دـ عـ وـ جـ رـ لـ اـ بـ يـ صـ وـ تـ وـ تـ اـ مـ جـ رـ تـ لـ اـ هـ ذـ هـ ةـ قـ دـ نـ عـ اـ هـ تـ يـ لـ وـ ئـ سـ مـ  
(رـ فـ وـ تـ مـ طـ بـ اـ رـ لـ اـ)ـ يـ لـ صـ أـ لـ اـ يـ زـ يـ لـ جـ نـ إـ لـ اـ دـ نـ تـ سـ مـ لـ اـ).