ASA 8.3及更高版本：啟用FTP/TFTP服務配置示例

目錄

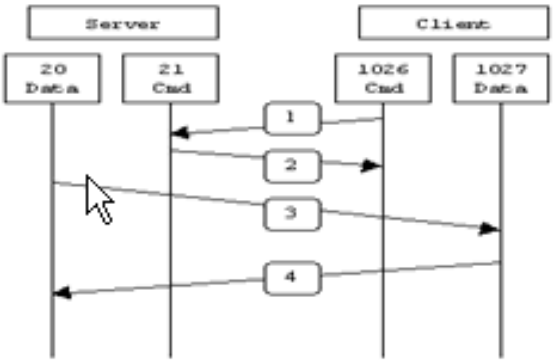
簡介

本檔案將說明網路外部使用者在DMZ網路中存取FTP和TFTP服務所需的步驟。

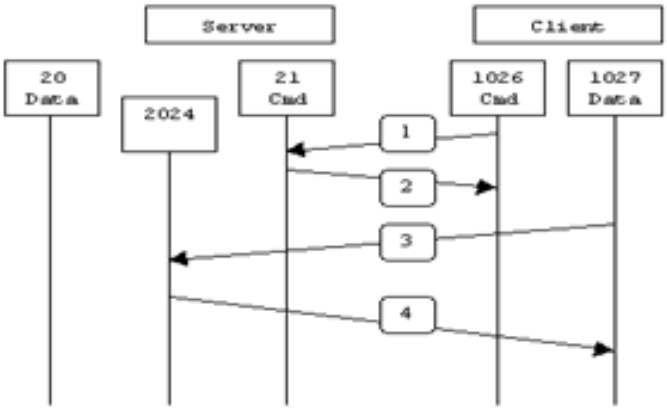
檔案傳輸通訊協定 (FTP)

FTP有兩種形式：

- 活動模式
- 被動模式



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

在主動式FTP模式下，使用者端從隨機非特權連線埠(N>1023)連線到FTP伺服器的指令連線埠(21)。然後使用者端開始監聽連線埠N+1，並將FTP命令連線埠N+1傳送到FTP伺服器。然後，伺服器從其本地資料埠（即埠20）連線回客戶端的指定資料埠。

在被動式FTP模式下，客戶端發起到伺服器的兩個連線，這解決了防火牆過濾從伺服器到客戶端的傳入資料埠連線的問題。開啟FTP連線時，客戶端會在本地開啟兩個隨機無許可權埠（N>1023和N+1）。 第一個埠與埠21上的伺服器聯絡。但是，客戶端不會發出**port**命令並允許伺服器連線回其資料埠，而是發出**PASV**命令。如此一來，伺服器就會開啟一個隨機的未授權連線埠(P>1023)，並將**port P**命令傳送回使用者端。然後客戶端啟動從埠N+1到伺服器埠P的連線以傳輸資料。如果安全裝置上未配置**inspection**命令，則從內部使用者傳出的FTP僅在被動模式下工作。此外，外部使用者傳入FTP伺服器時，會遭到拒絕存取。

請參閱PIX/ASA 7.x:在版本8.2及更低版本的思科自適應安全裝置(ASA)上為相同配置啟用FTP/TFTP服務配置示例。

簡單式檔案傳輸通訊協定(TFTP)

如RFC 1350所述，TFTP是一種在TFTP伺服器和使用者端之間讀取和寫入檔案的簡單通訊協定。TFTP使用UDP埠69。

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

- 所需介面之間具有基本通訊。
- 您已在DMZ網路中設定了FTP伺服器。

採用元件

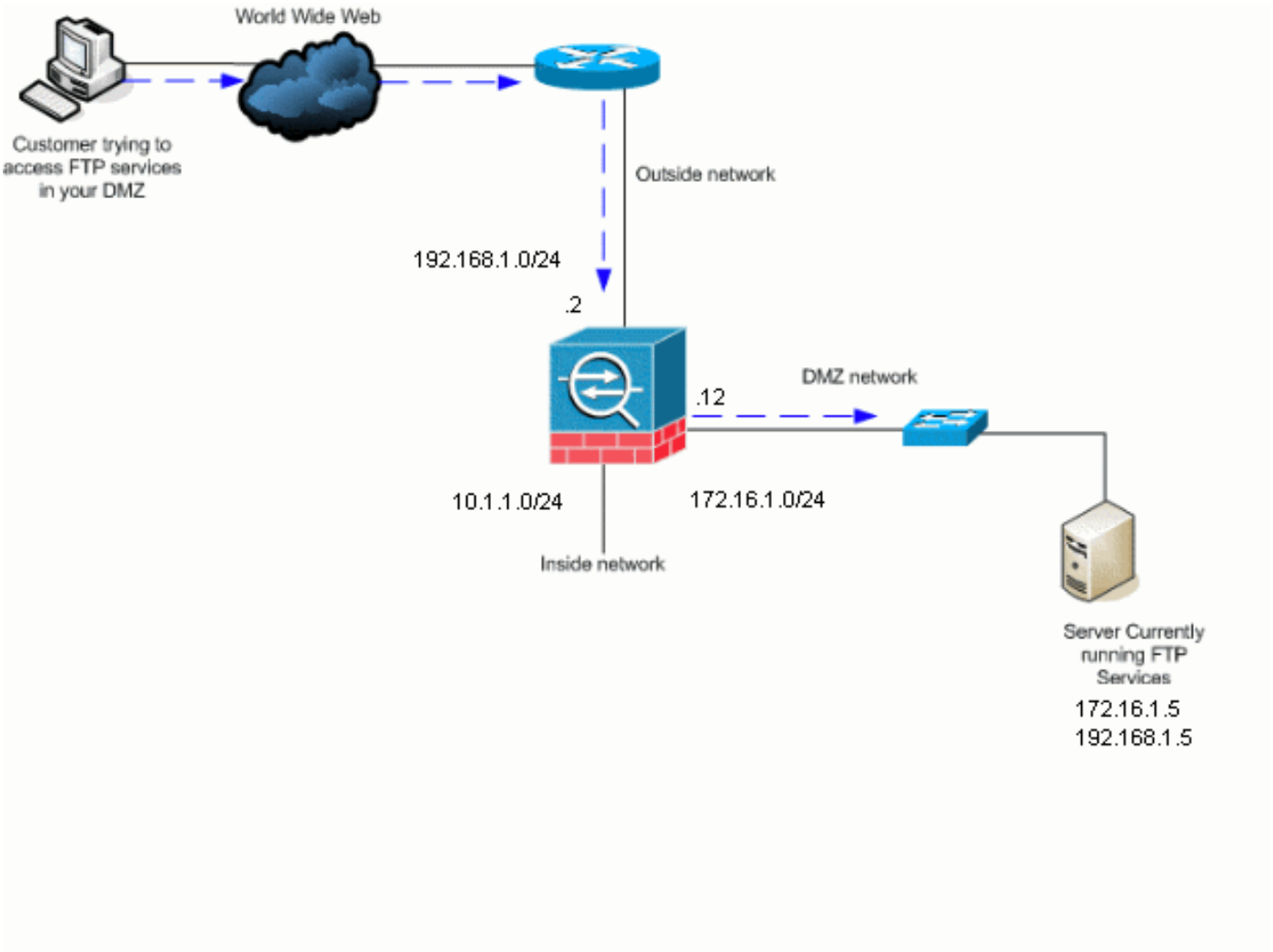
本文中的資訊係根據以下軟體和硬體版本：

- 執行8.4(1)軟體映像的ASA 5500系列調適型安全裝置
- 運行FTP服務的Windows 2003 Server
- 運行TFTP服務的Windows 2003 Server
- 位於網路外部的客戶端PC

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

網路圖表

本檔案會使用以下網路設定：



注意：此配置中使用的IP編址方案在Internet上不能合法路由。這些地址是在實驗室環境中使用的RFC 1918地址。

相關產品

此配置還可以與思科自適應安全裝置8.3及更高版本配合使用。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

背景資訊

安全裝置通過自適應安全演算法功能支援應用檢測。通過自適應安全演算法使用的狀態應用檢測，安全裝置會跟蹤穿越防火牆的每個連線，並確保它們有效。通過狀態檢查，防火牆還會監視連線的狀態，以編譯資訊以放入狀態表中。除了使用管理員定義的規則外，還使用狀態表，過濾決策將基於以前通過防火牆的資料包建立的上下文。應用檢查的實施包括以下操作：

- 識別流量。
- 對流量應用檢查。
- 啟用介面上的檢測。

進階通訊協定處理

FTP

某些應用需要思科安全裝置應用檢查功能進行特殊處理。這些型別的應用程式通常在使用者資料包中嵌入IP編址資訊，或在動態分配的埠上開啟輔助通道。應用程式檢查功能與網路地址轉換(NAT)配合使用，可幫助識別嵌入編址資訊的位置。

除了識別嵌入式編址資訊外，應用檢測功能還監控會話以確定輔助通道的埠號。許多協定會開啟輔助TCP或UDP埠以提高效能。已知埠上的初始會話用於協商動態分配的埠號。應用檢查功能會監視這些會話、識別動態埠分配並在特定會話期間允許在這些埠上進行資料交換。多媒體和FTP應用都表現出這種行為。

FTP通訊協定需要一些特殊處理，因為每個FTP作業階段使用兩個連線埠。啟用用於傳輸資料時，FTP協定使用兩個埠：分別使用埠21和20的控制通道和資料通道。通過控制通道發起FTP會話的使用者會通過該通道發出所有資料請求。然後，FTP伺服器發起一個請求，開啟從伺服器埠20到使用者電腦的埠。FTP總是使用埠20進行資料通道通訊。如果未在安全裝置上啟用FTP檢測，則會放棄此請求，並且FTP會話不會傳輸任何請求的資料。如果在安全裝置上啟用了FTP檢查，安全裝置將監視控制通道並嘗試識別開啟資料通道的請求。FTP協定將資料通道埠規範嵌入控制通道流量，要求安全裝置檢查控制通道的資料埠更改。如果安全裝置識別到請求，它會臨時為會話期間持續的資料通道流量建立一個開口。這樣，FTP檢查功能監視控制通道，識別資料埠分配，並允許資料埠上交換會話長度的資料。

預設情況下，安全裝置會通過global-inspection class-map檢查埠21連線以檢測FTP流量。安全裝置還可以識別主動和被動FTP會話之間的區別。如果FTP會話支援被動FTP資料傳輸，安全裝置將通過**inspect ftp**命令識別使用者的資料埠請求，並開啟一個大於1023的新資料埠。

FTP應用程式檢查會檢查FTP會話並執行四項任務：

- 準備動態輔助資料連線
- 跟蹤FTP命令 — 響應序列
- 生成稽核跟蹤
- 使用NAT轉換嵌入式IP地址

FTP應用檢查為FTP資料傳輸準備輔助通道。通道是響應於檔案上傳、檔案下載或目錄清單事件而分配的，並且它們必須預先協商。連線埠是透過**PORT**或**PASV**(227)命令交涉。

TFTP

預設情況下啟用TFTP檢測。

安全裝置會檢查TFTP流量，並在必要時動態建立連線和轉換，以允許在TFTP客戶端和伺服器之間傳輸檔案。具體來說，檢查引擎檢查TFTP讀取請求(RRQ)、寫入請求(WRQ)和錯誤通知(ERROR)。

如果需要，在接收有效RRQ或WRQ時分配動態輔助通道和PAT轉換。TFTP隨後會使用此輔助通道進行檔案傳輸或錯誤通知。

只有TFTP伺服器可以通過輔助通道發起流量，而且TFTP客戶端和伺服器之間最多只能存在一個不完整的輔助通道。來自伺服器的錯誤通知將關閉輔助通道。

如果使用靜態PAT重定向TFTP流量，則必須啟用TFTP檢查。

配置基本FTP應用檢測

預設情況下，配置包含與所有預設應用檢測流量匹配並將檢測應用於所有介面上的流量的策略（全域性策略）。 預設應用檢測流量包括到每個協定的預設埠的流量。您只能應用一個全域性策略，因此，如果要更改全域性策略（例如，將檢測應用於非標準埠，或新增預設情況下未啟用的檢測），則需要編輯預設策略或禁用該策略並應用新的策略。有關所有預設埠的清單，請參閱預設檢測策略。

1. 發出policy-map global_policy命令。
   ```
   ASA(config)#policy-map global_policy
   ```

2. 發出class inspection_default 命令。
   ```
   ASA(config-pmap)#class inspection_default
   ```

3. 發出inspect FTP 指令。
   ```
   ASA(config-pmap-c)#inspect FTP
   ```

   有一個選項可用於使用inspect FTP strict命令。此命令通過阻止Web瀏覽器在FTP請求中傳送嵌入式命令，提高了受保護網路的安全。在介面上啟用*strict*選項後，FTP檢查會強制執行以下行為：必須在安全裝置允許新命令之前確認FTP命令。安全裝置會丟棄傳送嵌入式命令的連線。將檢查227和PORT命令，以確保它們不會顯示在錯誤字串中。**警告：**使用*strict*選項可能會導致嚴格符合FTP RFC的FTP客戶端出現故障。請參閱使用strict選項，瞭解有關使用*strict*選項的詳細資訊。

組態範例

裝置名稱1
ASA(config)#**show running-config** ASA Version 8.4(1)

```
!
hostname ASA
domain-name corp.com
enable password WwXYvtKrnjXqGbu1 encrypted
names
!
interface Ethernet0/0
 nameif Outside
 security-level 0
 ip address 192.168.1.2 255.255.255.0
!
interface Ethernet0/1
 nameif Inside
 security-level 100
ip address 10.1.1.1 255.255.255.0
!
interface Ethernet0/2
 nameif DMZ
  security-level 50
  ip address 172.16.1.12 255.255.255.0
!
interface Ethernet0/3
 no nameif
 no security-level
 no ip address
!
interface Management0/0
  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
!--- Permit inbound FTP data traffic. access-list 100
extended permit tcp any host 192.168.1.5 eq ftp-data
!
!--- Object groups are created to define the hosts.
object network DMZ
host 172.16.1.5
object network DMZ-out
host 192.168.1.5
!--- Configure manual NAT nat (DMZ,outside) source
static DMZ DMZ-out
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)#
```

在非標準TCP埠上配置FTP協定檢測

您可以使用以下配置行為非標準TCP埠配置FTP協定檢測（用新埠號替換XXXX）：

```
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
```

配置基本TFTP應用檢測

預設情況下，配置包含與所有預設應用檢測流量匹配並將檢測應用於所有介面上的流量的策略（全域性策略）。 預設應用檢測流量包括到每個協定的預設埠的流量。只能應用一個全域性策略。因此，如果要更改全域性策略，例如將檢測應用於非標準埠，或新增預設情況下未啟用的檢測，則需要編輯或禁用預設策略並應用新的策略。有關所有預設埠的清單，請參閱預設檢測策略。

1. 發出policy-map global_policy命令。
   ```
   ASA(config)#policy-map global_policy
   ```
2. 發出class inspection_default 命令。
   ```
   ASA(config-pmap)#class inspection_default
   ```
3. 發出inspect TFTP 命令。
   ```
   ASA(config-pmap-c)#inspect TFTP
   ```

組態範例

裝置名稱1

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

 ASA Version 8.4(1)
!
hostname ASA
```

```
domain-name corp.com
enable password WwXYvtKrnjXqGbu1 encrypted
names
!
interface Ethernet0/0
 nameif Outside
 security-level 0
 ip address 192.168.1.2 255.255.255.0
!
interface Ethernet0/1
 nameif Inside
 security-level 100
ip address 10.1.1.1 255.255.255.0
!
interface Ethernet0/2
 nameif DMZ
  security-level 50
  ip address 172.16.1.12 255.255.255.0
!
interface Ethernet0/3
 no nameif
 no security-level
 no ip address
!
interface Management0/0
  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 DMZ
host 172.16.1.5
object network DMZ-out
host 192.168.1.5
!--- Configure manual NAT nat (DMZ,outside) source
static DMZ DMZ-out
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)#
```

驗證

要確保配置已成功執行，請使用**show service-policy**命令。此外，僅使用show service-policy inspect ftp 命令將輸出限製為FTP檢查。

```
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#
```

疑難排解

目前尚無適用於此組態的具體疑難排解資訊

相關資訊

- 思科調適型資安裝置管理員
- Cisco ASA 5500系列調適型安全裝置
- 要求建議 (RFC)
- 技術支援與文件 - Cisco Systems