ASA 8.3 e versioni successive: Esempio di configurazione dell'abilitazione dei servizi FTP/TFTP

Sommario

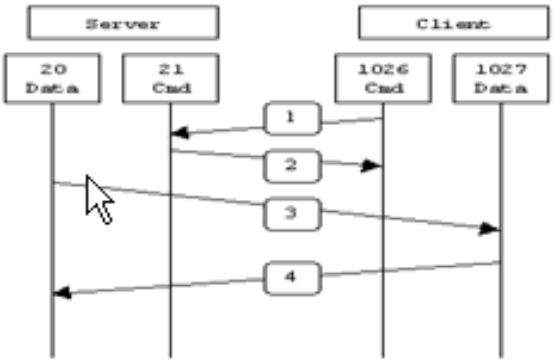
Introduzione

Questo documento spiega i passaggi richiesti agli utenti esterni alla rete per accedere ai servizi FTP e TFTP nella rete DMZ.

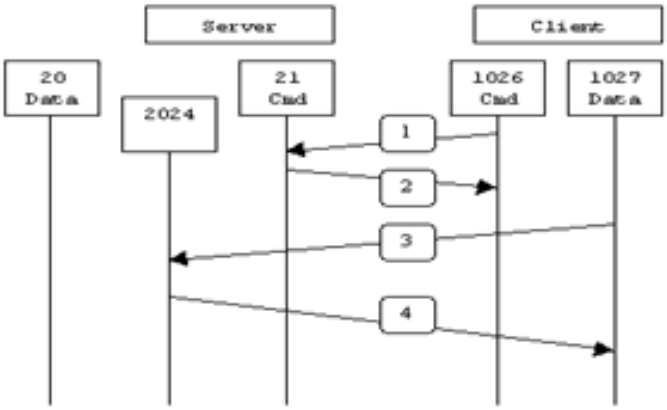
FTP (File Transfer Protocol)

Sono disponibili due tipi di FTP:

- Modalità attiva
- Modalità passiva



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

In modalità FTP attivo, il client si connette da una porta casuale senza privilegi (N>1023) alla porta di comando (21) del server FTP. Quindi il client inizia ad ascoltare la porta N+1 e invia la porta di comando FTP N+1 al server FTP. Il server si connette quindi alle porte dati specificate del client dalla porta dati locale, ovvero la porta 20.

In modalità FTP passivo, il client avvia entrambe le connessioni al server, risolvendo il problema di un firewall che filtra la connessione della porta dati in ingresso dal server al client. Quando si apre una connessione FTP, il client apre localmente due porte casuali senza privilegi (N>1023 e N+1). La prima porta contatta il server sulla porta 21. Tuttavia, anziché eseguire un comando **port** e consentire al server di riconnettersi alla porta dati, il client esegue il comando **PASV**. Di conseguenza, il server apre una porta casuale senza privilegi (P>1023) e invia il comando **port P** al client. Il client avvia quindi la connessione dalla porta N+1 alla porta P sul server per trasferire i dati. Se non si configura il comando **survey** sull'appliance di sicurezza, l'FTP inviato dagli utenti verso l'esterno funziona solo in modalità passiva. Inoltre, agli utenti esterni al server FTP viene negato l'accesso.

Per ulteriori informazioni, fare riferimento al documento PIX/ASA 7.x: Abilitare l'esempio di configurazione dei servizi FTP/TFTP per la stessa configurazione su Cisco Adaptive Security Appliance (ASA) con le versioni 8.2 e precedenti.

Protocollo TFTP (Trivial File Transfer Protocol)

Il protocollo TFTP, come descritto nella RFC 1350, è un protocollo semplice per leggere e scrivere file tra un server TFTP e un client. Il TFTP utilizza la porta UDP 69.

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Tra le interfacce richieste esiste una comunicazione di base.
- Èstato configurato un server FTP nella rete DMZ.

Componenti usati

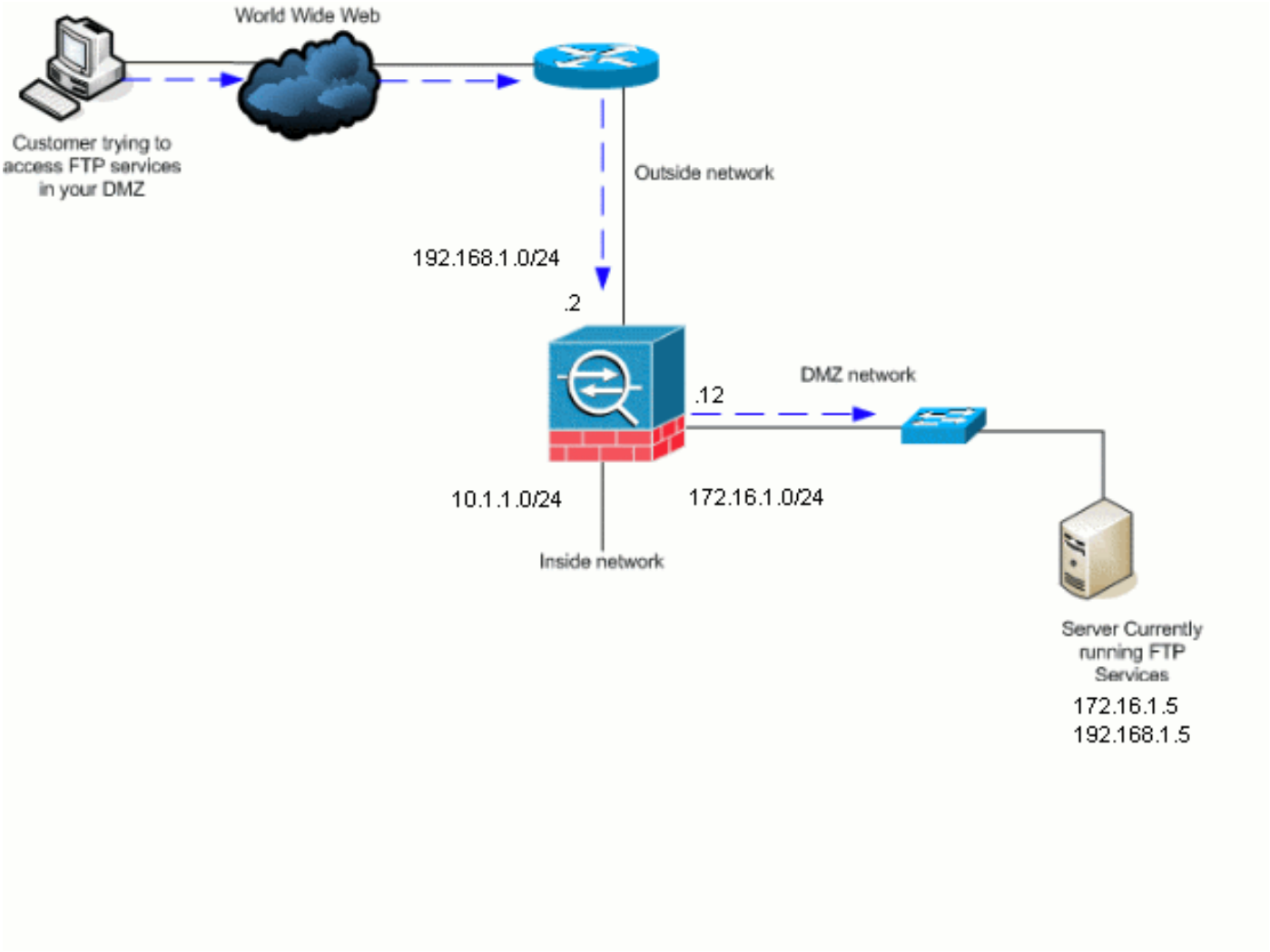
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- ASA serie 5500 Adaptive Security Appliance con immagine software 8.4(1)
- Windows 2003 Server con servizi FTP
- Windows 2003 Server con servizi TFTP
- PC client situato all'esterno della rete

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Nota: gli schemi di indirizzamento IP utilizzati in questa configurazione non sono legalmente instradabili su Internet. Si tratta degli indirizzi RFC 1918 utilizzati in un ambiente lab.

Prodotti correlati

Questa configurazione può essere utilizzata anche con Cisco Adaptive Security Appliance 8.3 e versioni successive.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Premesse

Appliance di sicurezza supporta l'ispezione delle applicazioni mediante la funzione Adaptive Security Algorithm. Mediante l'ispezione delle applicazioni con conservazione dello stato utilizzata dall'algoritmo Adaptive Security, Appliance di sicurezza tiene traccia di tutte le connessioni che attraversano il firewall e ne verifica la validità. Tramite l'ispezione con conservazione dello stato, il firewall controlla inoltre lo stato della connessione per compilare le informazioni da inserire in una tabella di stato. Se si utilizza la tabella di stato oltre alle regole definite dall'amministratore, le decisioni di filtraggio si basano sul contesto stabilito dai pacchetti passati precedentemente attraverso il firewall. L'esecuzione delle ispezioni delle applicazioni comprende le seguenti azioni:

- Identificare il traffico.
- Eseguire controlli sul traffico.
- Attiva le ispezioni su un'interfaccia.

Gestione avanzata del protocollo

FTP

alcune applicazioni richiedono una gestione speciale da parte della funzione di ispezione delle applicazioni di Cisco Security Appliance. Questi tipi di applicazioni in genere incorporano le informazioni sugli indirizzi IP nel pacchetto dati utente o nei canali secondari aperti su porte assegnate dinamicamente. La funzione di ispezione delle applicazioni utilizza Network Address Translation (NAT) per identificare la posizione delle informazioni sull'indirizzamento incorporate.

Oltre all'identificazione delle informazioni di indirizzamento incorporate, la funzione di ispezione delle applicazioni controlla le sessioni per determinare i numeri di porta per i canali secondari. Molti protocolli aprono porte TCP o UDP secondarie per migliorare le prestazioni. La sessione iniziale su una porta nota viene utilizzata per negoziare i numeri di porta assegnati in modo dinamico. La funzione di ispezione delle applicazioni controlla queste sessioni, identifica le assegnazioni dinamiche delle porte e consente lo scambio di dati su queste porte per la durata delle sessioni specifiche. Le applicazioni multimediali e FTP mostrano questo tipo di comportamento.

Il protocollo FTP richiede una gestione speciale poiché utilizza due porte per sessione FTP. Quando viene attivato per il trasferimento dei dati, il protocollo FTP utilizza due porte: un canale di controllo e un canale dati che utilizzano rispettivamente le porte 21 e 20. L'utente, che avvia la sessione FTP sul canale di controllo, effettua tutte le richieste di dati attraverso tale canale. Il server FTP avvia quindi una richiesta di apertura di una porta dalla porta 20 del server al computer dell'utente. L'FTP utilizza sempre la porta 20 per le comunicazioni del canale dati. Se l'ispezione FTP non è stata abilitata sull'appliance di sicurezza, la richiesta viene ignorata e le sessioni FTP non trasmettono i dati richiesti. Se l'opzione di ispezione FTP è attivata sull'appliance di sicurezza, quest'ultima controlla il canale di controllo e tenta di riconoscere una richiesta di apertura del canale dati. Il protocollo FTP incorpora le specifiche delle porte del canale dati nel traffico del canale di controllo, richiedendo all'appliance di sicurezza di ispezionare il canale di controllo per verificare se sono state apportate modifiche alle porte dati. Se Security Appliance riconosce una richiesta, crea temporaneamente un'apertura per il traffico del canale dati che dura per la durata della sessione. In questo modo, la funzione di ispezione FTP controlla il canale di controllo, identifica l'assegnazione di una porta dati e consente lo scambio dei dati sulla porta dati per la durata della sessione.

Per impostazione predefinita, Security Appliance controlla le connessioni alla porta 21 per il traffico FTP tramite la mappa delle classi di ispezione globale. Security Appliance riconosce inoltre la differenza tra una sessione FTP attiva e una passiva. Se le sessioni FTP supportano il trasferimento di dati FTP passivo, tramite il comando **inspect ftp** l'appliance di sicurezza riconosce la richiesta della porta dati proveniente dall'utente e apre una nuova porta dati maggiore di 1023.

L'ispezione dell'applicazione FTP controlla le sessioni FTP ed esegue quattro operazioni:

- Prepara una connessione dati secondaria dinamica
- Tiene traccia della sequenza di risposta dei comandi FTP
- Genera un audit trail

- Traduce l'indirizzo IP incorporato utilizzando NAT

L'ispezione dell'applicazione FTP prepara i canali secondari per il trasferimento dei dati FTP. I canali vengono allocati in risposta a un evento di caricamento di file, di download di file o di elencazione di directory e devono essere pre-negoziati. La porta viene negoziata tramite i comandi **PORT** o **PASV** (227).

TFTP

L'ispezione TFTP è abilitata per impostazione predefinita.

L'appliance di sicurezza controlla il traffico TFTP e, se necessario, crea connessioni e conversioni dinamiche per consentire il trasferimento di file tra un client TFTP e un server. In particolare, il modulo di controllo controlla le richieste di lettura (RQ) TFTP, le richieste di scrittura (WRQ) e le notifiche di errore (ERROR).

Un canale secondario dinamico e una traduzione PAT, se necessario, vengono allocati su una ricezione di una RRQ o WRQ valida. Questo canale secondario viene successivamente utilizzato dal TFTP per il trasferimento di file o la notifica degli errori.

Solo il server TFTP può avviare il traffico sul canale secondario e tra il client TFTP e il server può esistere al massimo un canale secondario incompleto. Una notifica di errore dal server chiude il canale secondario.

L'ispezione TFTP deve essere abilitata se si utilizza un percorso statico per reindirizzare il traffico TFTP.

Configura ispezione applicazione FTP di base

Per impostazione predefinita, la configurazione include un criterio che corrisponde a tutto il traffico di ispezione delle applicazioni predefinito e applica l'ispezione al traffico su tutte le interfacce (un criterio globale). Il traffico di ispezione delle applicazioni predefinito include il traffico verso le porte predefinite per ogni protocollo. È possibile applicare un solo criterio globale, pertanto se si desidera modificare il criterio globale, ad esempio per applicare l'ispezione a porte non standard o per aggiungere ispezioni non abilitate per impostazione predefinita, è necessario modificare il criterio predefinito oppure disabilitarlo e applicarne uno nuovo. Per un elenco di tutte le porte predefinite, vedere Criteri di ispezione predefiniti.

1. Eseguire il comando policy-map global_policy.
   ```
   ASA(config)#policy-map global_policy
   ```

2. Eseguire il comando class inspection_default.
   ```
   ASA(config-pmap)#class inspection_default
   ```

3. Eseguire il comando inspect FTP.
   ```
   ASA(config-pmap-c)#inspect FTP
   ```

   È possibile utilizzare il comando inspect FTP strict. Questo comando aumenta la sicurezza delle reti protette impedendo a un browser Web di inviare comandi incorporati nelle richieste FTP.Dopo aver abilitato l'opzione *strict* su un'interfaccia, l'ispezione FTP applica questo comportamento:Affinché l'appliance di sicurezza riconosca un nuovo comando, è necessario

che il comando FTP venga riconosciuto.Appliance di sicurezza interrompe una connessione che invia comandi incorporati.I comandi **227** e **PORT** vengono controllati per verificare che non vengano visualizzati in una stringa di errore.**Avviso:** l'utilizzo dell'opzione *strict* potrebbe causare il malfunzionamento dei client FTP non strettamente conformi alle RFC FTP. Per ulteriori informazioni sull'uso dell'opzione *strict*, consultare Uso dell'opzione *strict*.

Esempio di configurazione

Nome dispositivo 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)#
```

Configura ispezione protocollo FTP su porta TCP non standard

Èpossibile configurare l'ispezione del protocollo FTP per le porte TCP non standard con queste righe di configurazione (sostituire XXXX con il nuovo numero di porta):

```
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
```

Configura ispezione applicazione TFTP di base

Per impostazione predefinita, la configurazione include un criterio che corrisponde a tutto il traffico di ispezione delle applicazioni predefinito e applica l'ispezione al traffico su tutte le interfacce (un criterio globale). Il traffico di ispezione delle applicazioni predefinito include il traffico verso le porte predefinite per ogni protocollo. È possibile applicare un solo criterio globale. Pertanto, se si desidera modificare il criterio globale, ad esempio per applicare l'ispezione a porte non standard o per aggiungere ispezioni non abilitate per impostazione predefinita, è necessario modificare il criterio predefinito oppure disabilitarlo e applicarne uno nuovo. Per un elenco di tutte le porte predefinite, vedere Criteri di ispezione predefiniti.

1. Eseguire il comando policy-map global_policy.
   ASA(config)#**policy-map global_policy**

2. Eseguire il comando class inspection_default.
   ASA(config-pmap)#**class inspection_default**

3. Eseguire il comando inspect TFTP.
   ASA(config-pmap-c)#**inspect TFTP**

Esempio di configurazione

Nome dispositivo 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)#
```

Verifica

Per verificare che la configurazione sia stata eseguita correttamente, utilizzare il comando **show service-policy**. Inoltre, limitare l'output all'ispezione FTP usando solo il comando show service-policy inspect ftp.

```
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#
```

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione

Informazioni correlate

- Cisco Adaptive Security Device Manager
- Cisco ASA serie 5500 Adaptive Security Appliance
- RFC (Requests for Comments)

- Documentazione e supporto tecnico – Cisco Systems