ASA/PIX: Esempio di configurazione Internet per consentire al traffico di rete di accedere al server MMS (Microsoft Media Server) o allo streaming video

Sommario

Introduzione

In questo documento viene descritto come configurare l'appliance ASA (Adaptive Security Appliance) in modo da consentire al client o all'utente da Internet di accedere al server Microsoft Media (MMS) o al video streaming posizionato nella rete interna dell'appliance ASA.

Prerequisiti

Requisiti

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

- Configurazione base dell'ASA
- MMS è configurato e funziona correttamente

Componenti usati

Per questo documento, è stato usato un Cisco ASA con software versione 7.x e successive.

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.

Prodotti correlati

Le informazioni riportate in questo documento sono valide anche per Cisco PIX Firewall con software versione 7.x e successive.

Convenzioni

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

Informazioni sul firewall per Windows Media Services serie 9

Usa protocolli multimediali di streaming

Microsoft® Windows Media® Services 9 Series utilizza due protocolli multimediali per la trasmissione di contenuti come flusso unicast ai client:

- Protocollo RTSP (Real Time Streaming Protocol)
- Protocollo MMS (Microsoft Media Server)

Questi protocolli supportano le azioni di controllo client, ad esempio arresto, pausa, riavvolgimento e avanzamento rapido dei file Windows Media indicizzati.

RTSP è un protocollo applicativo creato specificatamente per fornire dati controllati in tempo reale, come contenuti audio e video. È possibile utilizzare RTSP per inviare contenuto in streaming a computer che eseguono Windows Media Player 9 Series o versioni successive, a client che utilizzano il controllo ActiveX® serie 9 di Windows Media Player o ad altri computer che eseguono Windows Media Services 9 Series. Il protocollo RTSP lavora in tandem con il protocollo RTP (Real-Time Transport Protocol) per formattare i pacchetti di contenuti multimediali e negoziare il protocollo del livello di trasporto più efficiente, UDP (User Datagram Protocol) o TCP (Transport Control Protocol), da utilizzare quando si invia il flusso ai client. È possibile implementare RTSP tramite il plug-in WMS RTSP Server Control Protocol in Amministrazione servizi Windows Media. Questo plug-in è attivato per impostazione predefinita.

MMS è un protocollo proprietario a livello di applicazione sviluppato per le versioni precedenti di Windows Media Services. È possibile utilizzare MMS per inviare contenuto a computer che eseguono Windows Media Player per Windows® XP o versioni precedenti. È possibile implementare MMS tramite il plug-in WMS MMS Server Control Protocol in Amministrazione servizi Windows Media. Questo plug-in è attivato per impostazione predefinita.

Usa HTTP

Se non è possibile aprire le porte del firewall, i servizi Windows Media® possono inviare flussi di contenuto tramite HTTP sulla porta 80. È possibile utilizzare HTTP per inviare flussi a tutte le versioni di Windows Media Player. È possibile implementare HTTP tramite il plug-in WMS HTTP Server Control Protocol in Amministrazione servizi Windows Media. Questo plug-in non è attivato per impostazione predefinita. Se un altro servizio, ad esempio Internet Information Services (IIS), utilizza la porta 80 sullo stesso indirizzo IP, non sarà possibile attivare il plug-in.

Il protocollo HTTP può essere utilizzato anche per:

- Distribuire flussi tra server Windows Media
- Contenuto di origine da un codificatore Windows Media
- Scarica playlist generate dinamicamente da un server Web

I plug-in delle origini dati devono essere configurati in Amministrazione servizi Windows Media per supportare questi scenari di flusso HTTP aggiuntivi.

Informazioni sul rollover del protocollo

Se i client che supportano RTSP si connettono a un server che esegue i servizi Windows Media® con un moniker URL RTSP (ad esempio, rtsp://) o un moniker URL MMS (ad esempio, mms://), il server utilizza il rollover del protocollo per inviare il contenuto al client in modo da ottimizzare l'esperienza di streaming. Il rollover automatico del protocollo da RTSP/MMS a RTSP con trasporti basati su UDP o TCP (RTSPU o RTSPT) o anche HTTP (se il plug-in WMS HTTP Server Control Protocol è abilitato) può verificarsi quando il server tenta di negoziare il protocollo migliore e fornire un'esperienza di streaming ottimale per il client. I client che supportano RTSP includono Windows Media Player 9 Series o versioni successive o altri lettori che utilizzano il controllo ActiveX di Windows Media Player 9 Series.

Le versioni precedenti di Windows Media Player, ad esempio Windows Media Player per Windows XP, non supportano il protocollo RTSP, ma il protocollo MMS fornisce il supporto per il rollover del protocollo per tali client. Pertanto, quando una versione precedente di Windows Media Player tenta di connettersi al server con un moniker URL MMS, è possibile eseguire il rollover automatico del protocollo da MMS a MMS con trasporti basati su UDP o TCP (MMSU o MMST) o anche HTTP (se il plug-in WMS HTTP Server Control Protocol è abilitato) quando il server tenta di negoziare il protocollo migliore e fornire un'esperienza di streaming ottimale per questi client.

Per assicurarsi che il contenuto sia disponibile per tutti i client che si connettono al server, è necessario aprire le porte del firewall per tutti i protocolli di connessione che possono essere utilizzati nel rollover del protocollo.

Se si identifica il protocollo da utilizzare nel file di annuncio, ad esempio rtspu://server/publishing_point/file, è possibile forzare l'utilizzo di un protocollo specifico da parte del server Windows Media. Per garantire un'esperienza di streaming ottimale per tutte le versioni client, si consiglia di utilizzare l'URL con il protocollo generale MMS. Se i client si connettono al flusso con un URL con un moniker URL MMS, il rollover del protocollo necessario viene eseguito automaticamente. Tenere presente che gli utenti possono disattivare i protocolli di streaming nelle impostazioni delle proprietà di Windows Media Player. Se un utente disattiva un protocollo, questo viene ignorato durante il rollover. Ad esempio, se HTTP è disabilitato, gli URL non vengono riportati su HTTP.

Allocazione delle porte per i servizi Windows Media

La maggior parte dei firewall viene utilizzata per controllare il "traffico in entrata" verso il server; generalmente non controllano il "traffico in uscita" verso i client. Le porte del firewall per il traffico in uscita possono essere chiuse se nella rete del server vengono implementati criteri di protezione più rigidi. In questa sezione viene descritta l'allocazione predefinita delle porte per i servizi Windows Media® sia per il traffico in entrata che per il traffico in uscita (indicati nelle tabelle come "In" e "Out"), in modo che sia possibile configurare tutte le porte come necessario.

In alcuni scenari, il traffico in uscita può essere indirizzato a una porta in un intervallo di porte disponibili. Gli intervalli di porte mostrati nelle tabelle indicano l'intero intervallo di porte disponibili, ma è possibile allocare un numero inferiore di porte nell'intervallo di porte. Quando si decide il numero di porte da aprire, bilanciare la protezione con l'accessibilità e aprire un numero di porte sufficiente per consentire a tutti i client di stabilire una connessione. Determinare innanzitutto il numero di porte che si prevede di utilizzare per i servizi Windows Media, quindi aprire un altro 10% per tenere conto della sovrapposizione con altri programmi. Dopo aver stabilito questo numero, monitora il traffico per determinare se sono necessarie modifiche.

Le restrizioni relative agli intervalli di porte possono influire su tutte le applicazioni RPC (Remote Procedure Call) e DCOM (Distributed Component Object Model) che condividono il sistema, non solo su Servizi Windows Media. Se l'intervallo di porte allocato non è sufficientemente ampio, i servizi della concorrenza, ad esempio IIS, possono non riuscire con errori casuali. L'intervallo di porte deve essere in grado di supportare tutte le potenziali applicazioni di sistema che utilizzano servizi RPC, COM o DCOM.

Per semplificare la configurazione del firewall, è possibile configurare ogni plug-in del protocollo di controllo del server (RTSP, MMS e HTTP) in Amministrazione servizi Windows Media per l'utilizzo di una porta specifica. Se l'amministratore di rete ha già aperto una serie di porte per il server Windows Media, è possibile allocare tali porte ai protocolli di controllo di conseguenza. In caso contrario, è possibile chiedere all'amministratore di rete di aprire le porte predefinite per ciascun protocollo. Se non è possibile aprire le porte del firewall, i servizi Windows Media possono trasmettere il contenuto con il protocollo HTTP sulla porta 80.

Allocazione predefinita delle porte del firewall per i servizi Windows Media per il recapito di un flusso unicast:

Protocollo applicativo	Protocollo	Port	Descrizione
RTSP	TCP	554 (In/Out)	Consente di accettare connessioni client RTSP in entrata e di consegnare pacchetti di dati ai client che eseguono lo streaming con RTSPT.
RTSP	UDP	5004 (uscita)	Utilizzato per consegnare pacchetti di dati ai client in streaming con RTSPU.
RTSP	UDP	5005 (In/Out)	Utilizzato per ricevere informazioni sulla perdita di pacchetti dai client e fornire informazioni di sincronizzazione ai client in streaming con RTSPU.

MMS	TCP	1755 (In/Out)	Utilizzato per accettare connessioni client MMS in ingresso e per consegnare pacchetti di dati ai client che eseguono lo streaming con MST.
MMS	UDP	1755 (In/Out)	Utilizzato per ricevere informazioni sulla perdita di pacchetti dai client e fornire informazioni di sincronizzazione ai client che eseguono lo streaming con MSU.
MMS	UDP	1024 - 5000 (uscita)	Utilizzato per fornire pacchetti di dati ai client che eseguono lo streaming con MSU. Aprire solo il numero di porte necessario.
HTTP	TCP	80 (In/Out)	Utilizzato per accettare connessioni client HTTP in ingresso e per consegnare pacchetti di dati ai client che eseguono flussi con HTTP.

Per assicurarsi che il contenuto sia disponibile per tutte le versioni client che si connettono al server, aprire tutte le porte descritte nella tabella per tutti i protocolli di connessione che possono essere utilizzati nel rollover del protocollo. Se si esegue Servizi Windows Media in un computer che esegue Windows Server™ 2003 Service Pack 1 (SP1), è necessario aggiungere il programma Servizi Windows Media (wmserver.exe) come eccezione in Windows Firewall per aprire le porte in ingresso predefinite per i flussi unicast, anziché aprire manualmente le porte nel firewall.

Nota: per ulteriori informazioni sulla configurazione del firewall MMS, consultare il sito Web Microsoft.

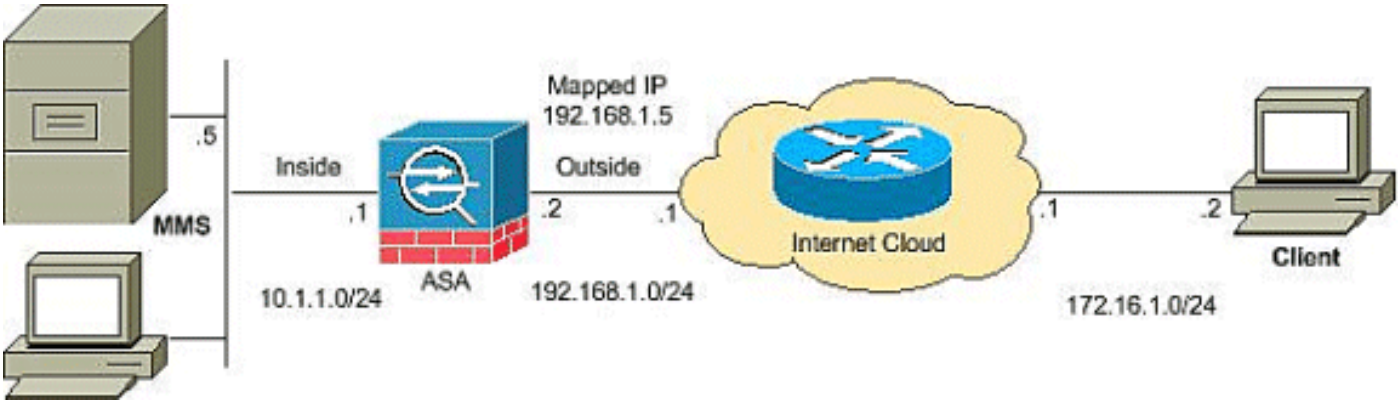
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

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.

Configurazioni

Nel documento vengono usate queste configurazioni:

Configurazione ASA

```
CiscoASA#Show running-config
: Saved
:
ASA Version 8.0(2)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 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
!
!--- Output suppressed access-list outside_access_in
extended permit icmp any any
access-list outside_access_in extended permit udp any
host
 192.168.1.5 eq 1755
!--- Command to open the MMS udp port access-list
outside_access_in extended permit tcp any host
 192.168.1.5 eq 1755
!--- Command to open the MMS tcp port access-list
outside_access_in extended permit udp any host
 192.168.1.5 eq 5005
!--- Command to open the RTSP udp port access-list
outside_access_in extended permit tcp any host
 192.168.1.5 eq www
!--- Command to open the HTTP port access-list
outside_access_in extended permit tcp any host
 192.168.1.5 eq rtsp
!--- Command to open the RTSP tcp port !--- Output
suppressed static (inside,outside) 192.168.1.5 10.1.1.5
```

```
netmask
 255.255.255.255
!--- Translates the mapped IP 192.168.1.5 to the
translated IP 10.1.1.5 of the MMS. access-group
outside_access_in in interface outside
!--- Output suppressed telnet timeout 5 ssh timeout 5
console timeout 0 threat-detection basic-threat threat-
detection statistics access-list ! 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
!--- RTSP inspection is enabled by default inspect
skinny inspect esmtp inspect sqlnet inspect sunrpc
inspect tftp inspect sip inspect xdmcp ! service-policy
global_policy global
```

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

- **Show access-list**: visualizza gli ACL configurati nell'appliance ASA/PIX

```
ciscoASA#show access-list
access-list outside_access_in; 6 elements
access-list outside_access_in line 1 extended permit
   icmp any any (hitcnt=0) 0x71af81e1
access-list outside_access_in line 2 extended permit
   udp any host 192.168.1.5 eq 1755 (hitcnt=0) 0x4
2606263
access-list outside_access_in line 3 extended permit
   tcp any host 192.168.1.5 eq 1755 (hitcnt=0) 0xa
0161e75
access-list outside_access_in line 4 extended permit
   udp any host 192.168.1.5 eq 5005 (hitcnt=0) 0x3
90e9949
access-list outside_access_in line 5 extended permit
   tcp any host 192.168.1.5 eq www (hitcnt=0) 0xe5
db0efc
access-list outside_access_in line 6 extended permit
   tcp any host 192.168.1.5 eq rtsp (hitcnt=0) 0x5
6fa336f
```

- **Show nat**: visualizza i criteri e i contatori NAT.

```
ciscoASA(config)#show nat
NAT policies on Interface inside:
  match ip inside host 10.1.1.5 outside any
    static translation to 192.168.1.5
    translate_hits = 0, untranslate_hits = 0
```

Video in streamingRisoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Ispect RTSP è una configurazione predefinita sull'appliance ASA. Interrompe il traffico MMS in quanto l'appliance di sicurezza non può eseguire NAT sui messaggi RTSP poiché gli indirizzi IP incorporati sono contenuti nei file SDP come parte dei messaggi HTTP o RTSP. È possibile frammentare i pacchetti e l'appliance di sicurezza non può eseguire NAT sui pacchetti frammentati.

Soluzione temporanea: Per risolvere il problema, disabilitare l'ispezione RTSP per il traffico MMS specifico come mostrato:

```
access-list rtsp-acl extended deny tcp
   any host 192.168.1.5 eq 554
access-list rtsp-acl extended permit tcp any any eq 554
class-map rtsp-traffic
match access-list rtsp-acl
policy-map global_policy
class inspection_default
no inspect rtsp
class rtsp-traffic
inspect rtsp
```

Informazioni correlate

- Software Cisco PIX Firewall
- Riferimenti per i comandi di Cisco Secure PIX Firewall
- Avvisi sui prodotti per la sicurezza (inclusi PIX)
- RFC (Requests for Comments)
- Supporto tecnico – Cisco Systems
- Pagina di supporto per Cisco ASA
- Documentazione e supporto tecnico – Cisco Systems