Esempio di configurazione della funzionalità di gestione del DNS sull'appliance ASA

Sommario

Introduzione

In questo documento viene illustrato l'utilizzo della funzionalità di protezione DNS su ASA (Adaptive Security Appliance) per modificare gli indirizzi IP incorporati nelle risposte DNS (Domain Name System) in modo che i client possano connettersi all'indirizzo IP corretto dei server.

Prerequisiti

Requisiti

Il servizio di archiviazione DNS richiede la configurazione di Network Address Translation (NAT) sull'appliance ASA, nonché l'abilitazione dell'ispezione DNS.

Componenti usati

Le informazioni fornite in questo documento si basano su Adaptive Security Appliance.

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.

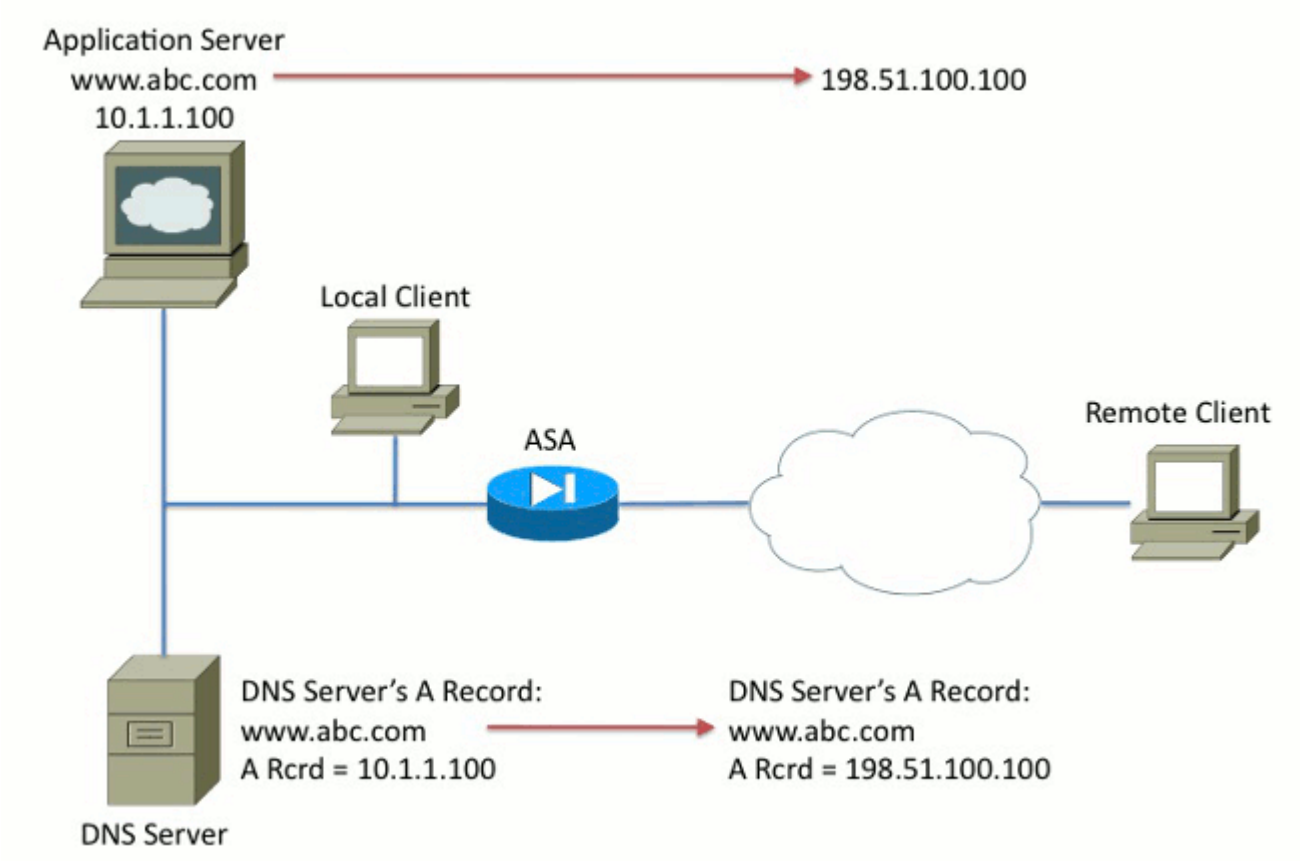
Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Esempi di gestione DNS

Server DNS all'interno dell'appliance ASA

Figura 1



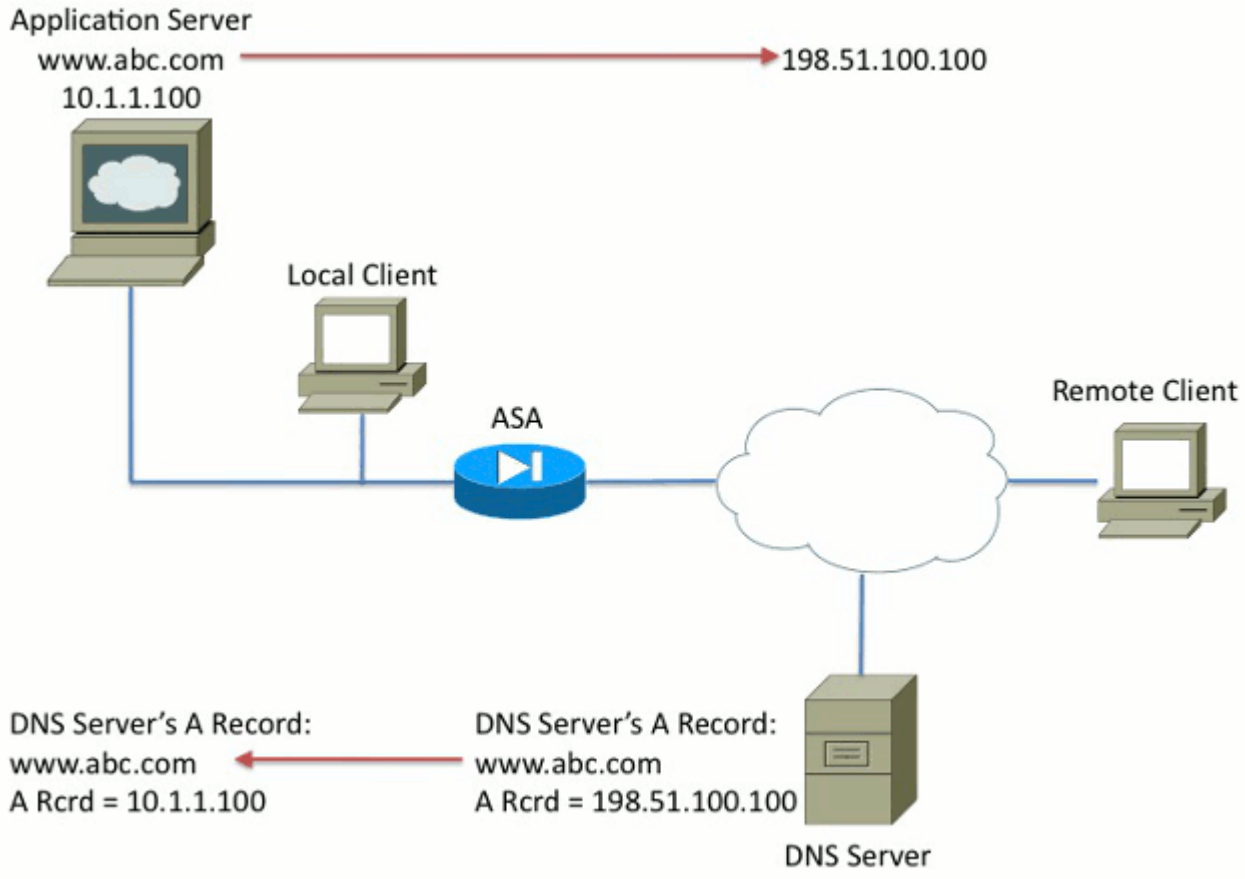

```
nat (inside,outside) source static 10.1.1.100 198.51.100.100 dns
!
policy-map global_policy
  class inspection_default
    inspect dns
```

Nella Figura 1 il server DNS è controllato dall'amministratore locale. Il server DNS deve distribuire un indirizzo IP privato, ovvero l'indirizzo IP *reale* assegnato al server applicazioni. Ciò consente al client locale di connettersi direttamente al server applicazioni.

Il client remoto non può accedere al server applicazioni con l'indirizzo privato. Di conseguenza, la funzionalità di protezione DNS viene configurata sull'appliance ASA per modificare l'indirizzo IP incorporato nel pacchetto di risposta DNS. In questo modo, quando il client remoto effettua una richiesta DNS per www.abc.com, la risposta che riceve si riferisce all'indirizzo tradotto del server applicazioni. Senza la parola chiave DNS nell'istruzione NAT, il client remoto tenta di connettersi a 10.1.1.100, che non funziona perché l'indirizzo non può essere instradato su Internet.

Server DNS all'esterno dell'appliance ASA

Figura 2



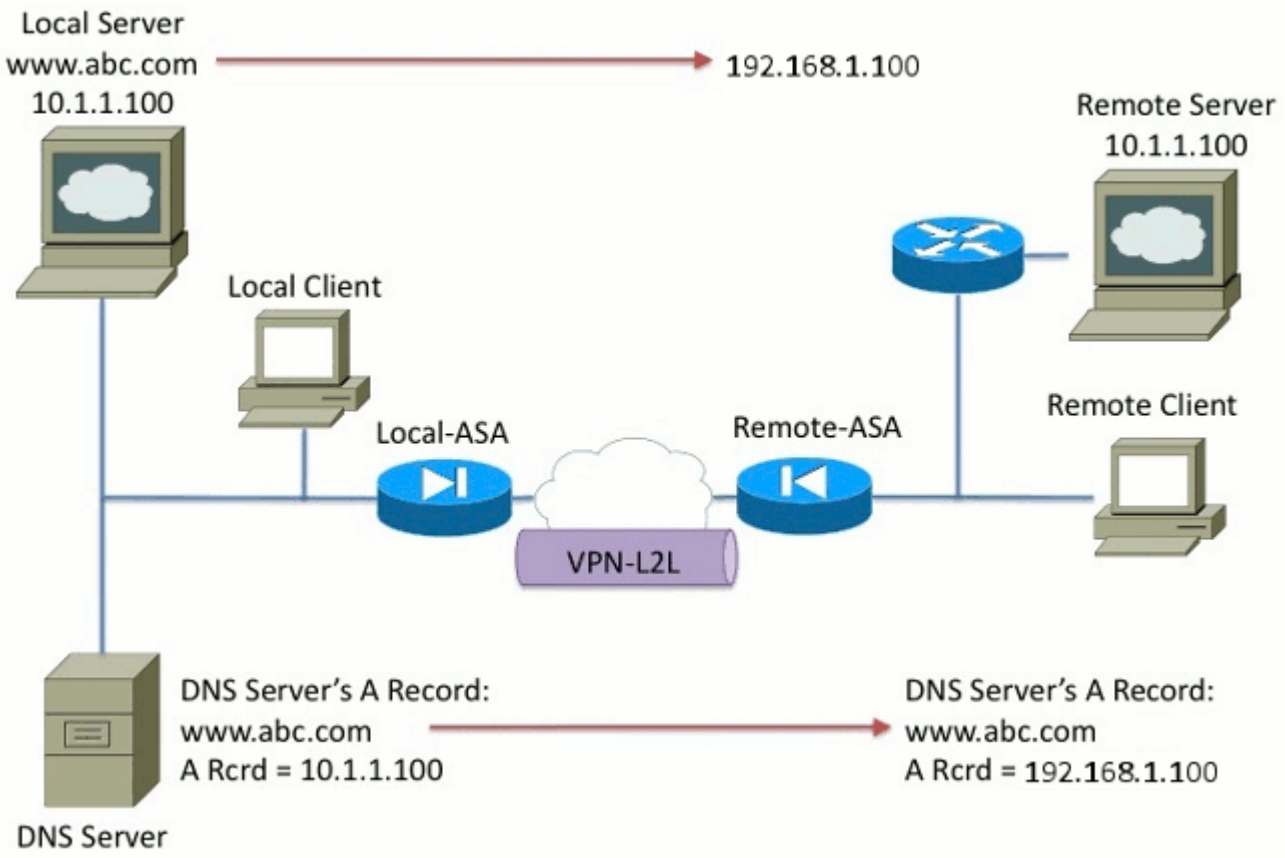

```
nat (inside,outside) source static 10.1.1.100 198.51.100.100 dns
!
policy-map global_policy
  class inspection_default
    inspect dns
```

Nella figura 2 il server DNS è controllato dall'ISP o da un provider di servizi simile. Il server DNS deve distribuire l'indirizzo IP pubblico, ovvero l'indirizzo IP *tradotto* del server applicazioni. Questo consente a tutti gli utenti di Internet di accedere al server dell'applicazione tramite Internet.

Il client locale non può accedere al server applicazioni con l'indirizzo pubblico. Di conseguenza, la funzionalità di protezione DNS viene configurata sull'appliance ASA per modificare l'indirizzo IP incorporato nel pacchetto di risposta DNS. In questo modo, quando il client locale effettua una richiesta DNS per www.abc.com, la risposta ricevuta corrisponde all'indirizzo reale del server applicazioni. Senza la parola chiave DNS nell'istruzione NAT, il client locale tenta di connettersi a 198.51.100.100. Questo non funziona perché il pacchetto viene inviato all'appliance ASA, che lo rifiuta.

Documentazione VPN NAT e DNS

Figura 3



Si consideri una situazione in cui vi sono reti che si sovrappongono. In questa condizione, l'indirizzo 10.1.1.100 vive sia sul lato remoto che sul lato locale. Di conseguenza, è necessario eseguire NAT sul server locale in modo che il client remoto possa ancora accedervi con l'indirizzo IP 192.1.1.100. Per il corretto funzionamento di questa funzionalità, è necessaria la funzionalità di protezione DNS.

Impossibile eseguire la funzionalità di archiviazione DNS in questa funzione. La parola chiave DNS può essere aggiunta solo alla fine di un NAT di oggetto o NAT di origine. Il NAT double non supporta la parola chiave DNS. Sono possibili due configurazioni ed entrambe hanno esito negativo.

Configurazione non riuscita 1: se si configura il risultato finale, viene convertito da 10.1.1.1 a 192.1.1.1, non solo per il client remoto, ma per tutti gli utenti di Internet. Poiché 192.1.1.1 non è instradabile su Internet, nessuno su Internet può accedere al server locale.

```
nat (inside,outside) source static 10.1.1.100 192.168.1.100 dns
nat (inside,outside) source static 10.1.1.100 192.168.1.100 destination
   REMOTE_CLIENT REMOTE_CLIENT
```

Configurazione 2 non riuscita: se si configura la riga NAT di gestione del DNS dopo il doppio della riga NAT necessaria, si verificherà una situazione in cui la gestione del DNS non funziona mai. Di conseguenza, il client remoto tenta di accedere a www.abc.com con l'indirizzo IP 10.1.1.100, che non funziona.

```
nat (inside,outside) source static 10.1.1.100 192.168.1.100 destination
   REMOTE_CLIENT REMOTE_CLIENT
nat (inside,outside) source static 10.1.1.100 64.1.1.100 dns
```

Informazioni correlate

- **Cisco ASA serie 5500 Adaptive Security Appliance**
- **Cisco ASA serie 5500 Adaptive Security Appliance > Download di software**
- **Documentazione e supporto tecnico â€“ Cisco Systems**

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).