

# Configurazione di BW AS per il proxy di intestazioni e opzioni sconosciute

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Verifica](#)

[Risoluzione dei problemi](#)

---

## Introduzione

In questo documento viene descritto come configurare i criteri proxy sull'appliance BW ASA per inviare tramite proxy intestazioni SIP sconosciute o parametri obbligatori/supportati.

## Prerequisiti

- Conoscenze base del protocollo SIP (Session Initiation Protocol)
- Conoscenze base di Application Server (AS)
- Conoscenze base di Broadworks (BW) bwcli

## Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Possibilità di utilizzare AS bwcli come utente amministratore
- Essere in grado di rivedere gli AS XSLogs
- Generare un INVITE (tramite un client o un simulatore) che consenta di configurare le intestazioni e i parametri Richiedi/Supportato.

## Componenti usati

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

- Cisco BW AS

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.

## Premesse

In qualità di agente utente back-to-back (B2BUA), l'ASA normalmente non invia tramite proxy le intestazioni SIP o i parametri nelle intestazioni Require e Supported, se questi sono considerati sconosciuti.

Se ad esempio l'AS riceve questo INVITE SIP, ignora l'intera intestazione MyUnknownHeader e il parametro MyUnknownParameter nell'intestazione Supported.

```
INVITE sip:+1555123456@cisco.com;user=phone SIP/2.0
Via: SIP/2.0/TCP 10.1.2.3:5060;branch=z9hG4bKva8in830cgv4i2mj6m20.1
Max-Forwards: 69
To: <sip:+1555123456@cisco.com;user=phone>
From: <sip:+1555654321@cisco.com;user=phone>;tag=SDq4k7b01-1
Contact: <sip:+155565432@172.16.0.1:5060;transport=tcp>
Call-ID: Testcall-456000001
CSeq: 101 INVITE
Supported: 100rel,MyUnknownParameter
MyUnknownHeader: MyStuff
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO, REGISTER
Content-Length: 0
```

Le impostazioni di ProxyPolicy nel server di autenticazione consentono di configurare intestazioni e parametri sconosciuti da inserire in modo trasparente nel proxy dal server di autenticazione.

La [Cisco BroadWorks SIP Access Interface Interworking Guide](#) contiene un elenco delle intestazioni e dei parametri noti che non possono mai essere inseriti in un proxy trasparente quando vengono elaborati dal server ASA.

Le intestazioni e i parametri noti vengono elaborati e possono o non possono essere inviati tramite proxy (a seconda del risultato dell'elaborazione AS) e non possono essere controllati con la configurazione descritta in questo articolo.

## Configurazione

Tutte le impostazioni necessarie per ProxyPolicy sono disponibili nella bwcli in AS\_CLI/Interface/SIP/ProxyPolicy>.

Per consentire all'AS di inoltrare l'intestazione MyUnknownHeader, passare prima a AS\_CLI/Interface/SIP/ProxyPolicy/Rule> dall'AS bwcli e aggiungere una nuova regola:

```
<#root>
```

```
AS_CLI>
```

```
cd /Interface/SIP/ProxyPolicy/Rule
```

```
AS_CLI/Interface/SIP/ProxyPolicy/Rule>
```

```
add MyUnknownHeaderRule true true true true true true true true
```

```
...Done
```

Eseguire il comando get per visualizzare la configurazione corrente.

La configurazione ora ha questo aspetto (a causa delle numerose opzioni, la larghezza dell'output di questo comando è molto grande; scorrere orizzontalmente per visualizzarlo completamente):

```
<#root>
```

```
AS_CLI/Interface/SIP/ProxyPolicy/Rule>
```

```
get
```

```
Rule Name Keep On Redirection Keep On Egress Access Keep On Egress Network On-net Keep On Egress Network
```

```
=====
```

MyUnknownHeaderRule	true		true			true
---------------------	------	--	------	--	--	------

Al termine, è necessario creare l'oggetto HeaderPolicy. Passare a AS\_CLI/Interface/SIP/ProxyPolicy/HeaderPolicy> ed eseguire questo comando:

```
<#root>
```

```
AS_CLI/Interface/SIP/ProxyPolicy/HeaderPolicy>
```

```
add MyUnknownHeader MyUnknownHeaderRule
```

```
...Done
```

In questo esempio, la regola è stata configurata in modo da mantenere l'intestazione in tutte le direzioni, per tutti i servizi e negli URI di reindirizzamento, ma questa impostazione dipende dal case reale.

Le opzioni disponibili sono spiegate nel seguente elenco:

- keepOnRedirection: Questo parametro determina se l'intestazione viene mantenuta in caso di reindirizzamento.
- keepOnEgressAccess: Questo parametro determina se l'intestazione viene mantenuta per i messaggi in uscita sul lato accesso.
- keepOnEgressNetworkOnNet: Questo parametro determina se l'intestazione viene

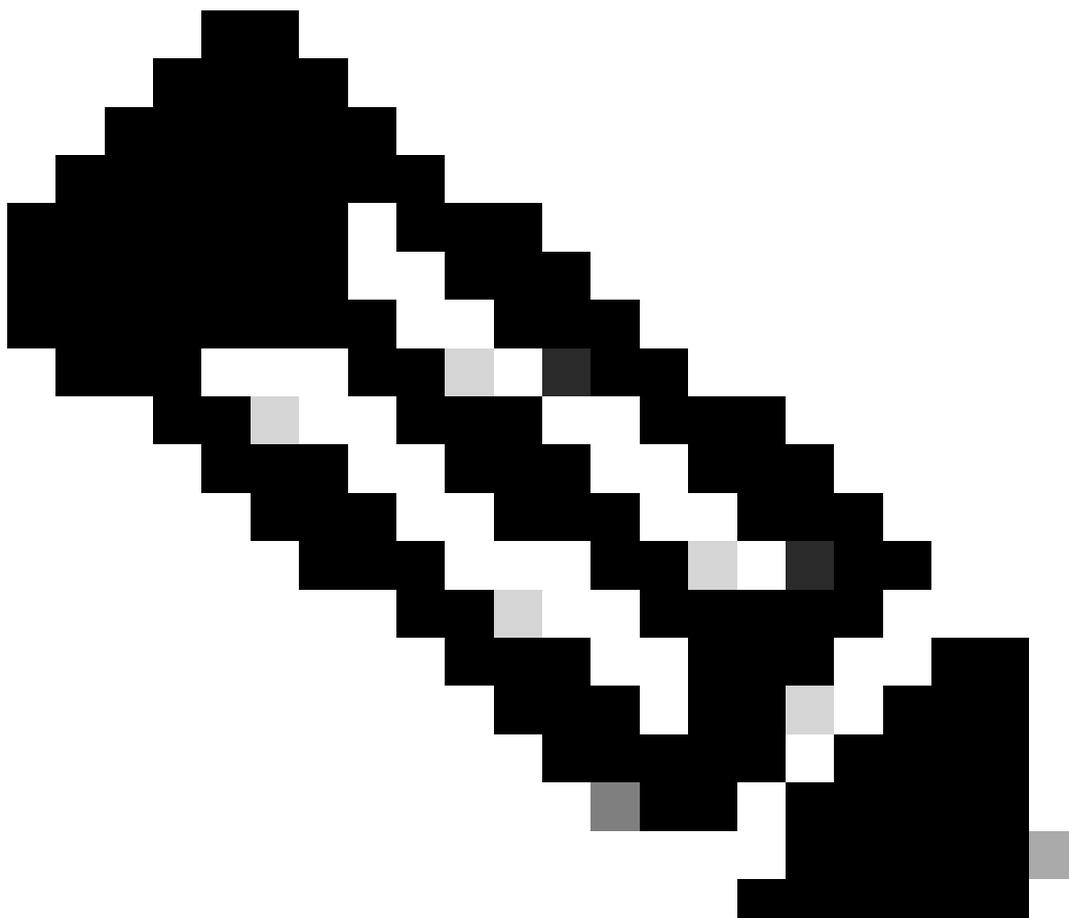
propagata per i messaggi in uscita su rete associati alla rete.

- `keepOnEgressNetworkOffNet`: Questo parametro determina se l'intestazione viene propagata per i messaggi fuori rete in uscita associati alla rete.
- `KeepOnEgressAccessSharedCallAppearance`: Questo parametro determina se l'intestazione viene mantenuta per i messaggi in uscita in una posizione secondaria dell'aspetto chiamata condivisa.
- `KeepOnEgressNetworkBroadWorksAnywhereOnNet`: Questo parametro determina se l'intestazione viene mantenuta per i messaggi in uscita su rete in una posizione `BroadWorks Anywhere`.
- `KeepOnEgressNetworkBroadWorksAnywhereOffNet`: Questo parametro determina se l'intestazione viene mantenuta per i messaggi fuori rete in uscita verso una posizione `BroadWorks Anywhere`.
- `acceptFromRedirectToURI`: Questo parametro determina se un'intestazione sconosciuta incorporata in un URI di destinazione di reindirizzamento può essere accettata per l'inserimento in un messaggio in uscita.

Il parametro sconosciuto può essere configurato nello stesso modo, ma è configurato in `AS_CLI/Interface/SIP/ProxyPolicy/OptionTagPolicy` .

Creare innanzitutto una regola.

---



Nota: Nell'esempio, il primo switch è impostato su false.

---

```
<#root>
```

```
AS_CLI/Interface/SIP/ProxyPolicy/Rule>
```

```
add MyUnknownParameterRule false true true true true true true true
```

Questa è la regola risultante, con Keep On Redirection impostato su false, in modo che MyUnknownHeader non venga aggiunto all'INVITE in uscita in caso di reindirizzamenti.

```
<#root>
```

```
AS_CLI/Interface/SIP/ProxyPolicy/Rule>
```

```
get
```

Rule Name Keep On Redirection Keep On Egress Access Keep On Egress Network On-net Keep On Egress Network

```
=====
MyUnknownHeaderRule      true           true           true
MyUnknownParameterRule  false          true           true
```

Per completare la configurazione, aggiungere OptionTagPolicy.

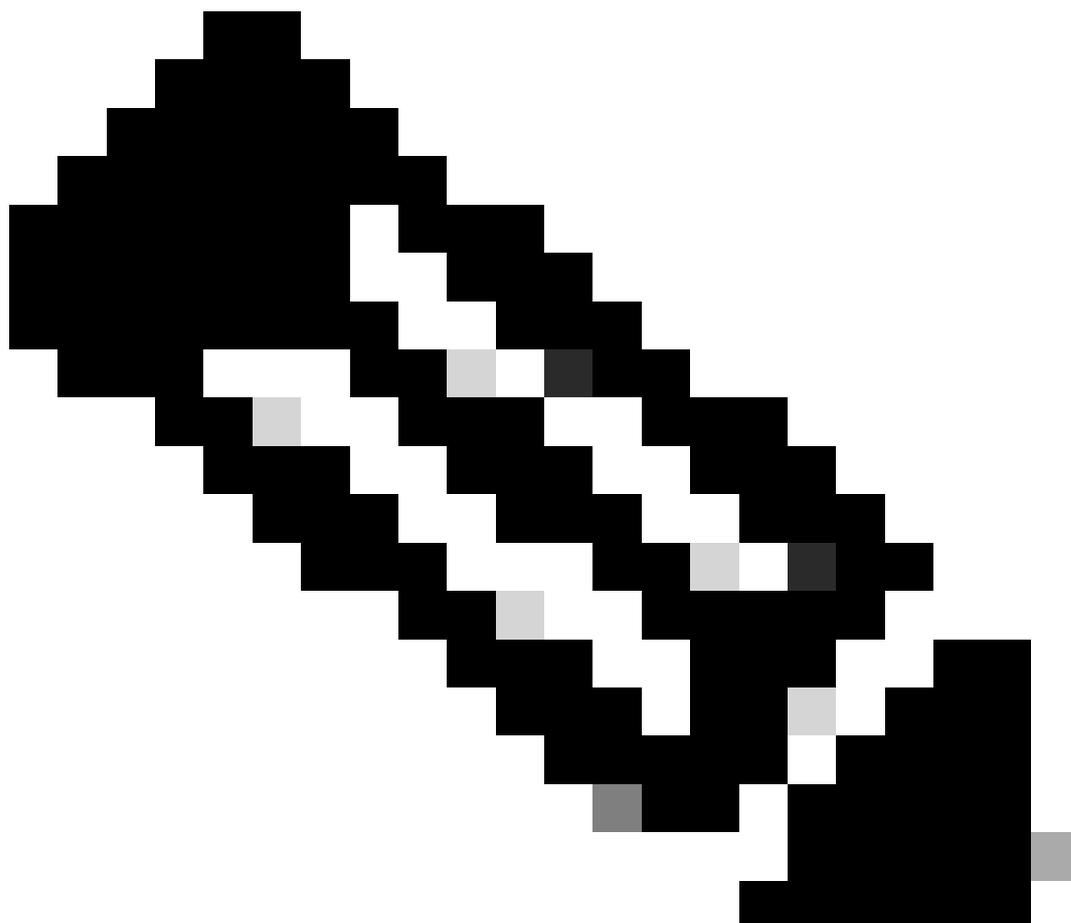
```
<#root>
```

```
AS_CLI/Interface/SIP/ProxyPolicy/OptionTagPolicy>
```

```
add MyUnknownParameter MyUnknownParameterRule
```

L'AS ora invia tramite proxy l'intestazione sconosciuta MyUnknownHeader e il parametro sconosciuto MyUnknownParameter.

---



---

Nota: Il SA non comprende la semantica né elabora in alcun modo le intestazioni e i parametri sconosciuti.

---

## Verifica

Inviare all'AS l'INVITE contenente l'intestazione SIP e il tag di opzione sconosciuti configurati nel criterio proxy e verificare che l'INVITE in uscita abbia mantenuto l'intestazione sconosciuta, in base alla configurazione della regola.

## Risoluzione dei problemi

Se l'INVITE in uscita non contiene il tag di intestazione o di opzione previsto, è possibile controllare questo elenco:

- Verificare che l'intestazione o il parametro configurato non sia incluso nell'elenco delle intestazioni o dei parametri noti.
- Verificare che l'intestazione o il parametro in INVITE corrisponda esattamente a quelli configurati in bwcli (senza distinzione tra maiuscole e minuscole).
- Verificare che la regola configurata consenta il proxy dell'intestazione o del parametro.

## 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).