Distribuzione dei telefoni SIP IP Office remoti con ASBCE

Versione 12.0
Edizione 14
Aprile 2024

Avviso

Nonostante l'impegno profuso per garantire la completezza e la precisione delle informazioni del presente documento al momento della stampa, Avaya declina qualsiasi responsabilità per eventuali errori. Avaya si riserva il diritto di apportare cambiamenti e correzioni alle informazioni contenute nel presente documento senza alcun obbligo di notifica degli stessi a persone e a organizzazioni.

Limitazioni di responsabilità per la documentazione

Per “Documentazione” si intendono le informazioni pubblicate su diversi supporti multimediali, che possono includere le informazioni sul prodotto, le descrizioni dell'abbonamento o del servizio, le istruzioni d'uso e le specifiche sulle prestazioni rese generalmente disponibili agli utenti dei prodotti. Nella documentazione non sono inclusi i materiali di marketing. Avaya non è responsabile per eventuali modifiche, aggiunte o eliminazioni alla versione originariamente pubblicata della documentazione, a meno che tali modifiche, aggiunte o eliminazioni non siano state eseguite da Avaya. L'Utente finale si impegna a risarcire e a non citare Avaya, i suoi agenti, funzionari e dipendenti, in eventuali reclami, azioni legali, richieste o sentenze, derivanti o correlate a modifiche, aggiunte o eliminazioni da essi apportate alla presente documentazione nei limiti di quanto effettuato.

Limitazioni di responsabilità per i link

Avaya non è responsabile del contenuto e dell'attendibilità dei siti Web cui si fa riferimento all'interno di questo sito o di questa documentazione fornita da Avaya. Avaya non è responsabile dell'accuratezza delle informazioni, dichiarazioni o contenuti forniti su questi siti e la loro inclusione non implica l'approvazione da parte di Avaya di prodotti, servizi o informazioni contenuti o offerti negli stessi. Avaya non garantisce che tali link siano attivi e non è in grado di controllarne la disponibilità.

Garanzia

Avaya fornisce una garanzia limitata sui propri componenti hardware e software Avaya. Per conoscere le condizioni della garanzia limitata, fare riferimento al contratto con Avaya. Sono, inoltre, disponibili a clienti e altre parti Avaya il testo standard della garanzia Avaya e le informazioni sull’assistenza relativa al presente prodotto nell'ambito del periodo coperto da garanzia. Per consultare questi documenti, visitare il sito Web dell'assistenza Avaya all'indirizzo: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 dal link “Warranty & Product Lifecycle” o un sito indicato successivamente da Avaya. Se il prodotto è stato acquistato da un partner di canale Avaya autorizzato al di fuori dei confini degli Stati Uniti e del Canada, la garanzia viene fornita dal suddetto partner di canale Avaya e non da Avaya.

Per “**Servizio ospitato**” si intende l'abbonamento a un servizio ospitato Avaya che l'utente acquista da Avaya o da un partner di canale Avaya autorizzato (a seconda dei casi), ulteriormente descritto nella sezione SAS ospitato o nella documentazione descrittiva di altri servizi, relativa al servizio ospitato applicabile. Se si acquista un abbonamento a un Servizio ospitato, la garanzia limitata di cui sopra potrebbe non essere applicabile; tuttavia, l'utente potrebbe avere diritto a usufruire dei servizi di supporto connessi al Servizio ospitato, come illustrato più avanti nei documenti descrittivi del servizio, in relazione al Servizio ospitato applicabile. Per ulteriori informazioni, contattare Avaya o un partner di canale Avaya (a seconda dei casi).

Servizio ospitato

QUANTO SEGUE SI APPLICA SOLO IN CASO DI ACQUISTO DI UNA SOTTOSCRIZIONE A UN SERVIZIO OSPITATO DA AVAYA O DA UN PARTNER DI CANALE AVAYA (SECONDO LE CIRCOSTANZE); I TERMINI DI UTILIZZO DEI SERVIZI OSPITATI SONO DISPONIBILI SUL SITO WEB DI AVAYA, ALL'INDIRIZZO HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, IN CORRISPONDENZA DEL COLLEGAMENTO “Termini di utilizzo Avaya per i servizi ospitati” O SU ALTRI SITI INDIVIDUATI SUCCESSIVAMENTE DA AVAYA, E SONO APPLICABILI A CHIUNQUE ACCEDA AL SERVIZIO OSPITATO O NE FACCIA USO. ACCEDENDO AL SERVIZIO OSPITATO O FACENDONE USO, O AUTORIZZANDO ALTRI A FARLO, L'UTENTE, PER CONTO PROPRIO E DELL'ENTITÀ PER CUI ESEGUE TALI OPERAZIONI (DA QUI IN POI DENOMINATI IN MODO INTERSCAMBIABILE “UTENTE” E “UTENTE FINALE”), ACCETTA I TERMINI DI UTILIZZO. SE L'UTENTE ACCETTA I TERMINI DI UTILIZZO PER CONTO DI UN'AZIENDA O DI UN'ALTRA ENTITÀ LEGALE, L'UTENTE DICHIARA DI AVERE L'AUTORITÀ PER VINCOLARE TALE ENTITÀ AI PRESENTI TERMINI DI UTILIZZO. SE L'UTENTE NON DISPONE DI TALE AUTORITÀ O NON INTENDE ACCETTARE I PRESENTI TERMINI DI UTILIZZO, NON DEVE ACCEDERE AL SERVIZIO OSPITATO NÉ FARNE USO NÉ AUTORIZZARE ALCUNO AD ACCEDERE AL SERVIZIO OSPITATO O A FARNE USO.

Licenze

I Termini di licenza Software Globale (“Termini di licenza del software”) sono disponibili sui seguenti siti web https://www.avaya.com/en/legal-license-terms/ o su un sito indicato successivamente da Avaya. I presenti Termini di licenza del Software sono applicabili a chiunque installi, scarichi e/o utilizzi il Software e/o la Documentazione. Installando, scaricando o utilizzando il software o autorizzando altri a farlo, l'utente finale accetta che i presenti termini di licenza del software stipulino un contratto vincolante tra l'utente finale e Avaya. Se accetta i presenti termini di licenza del software per conto di un'azienda o di un'altra entità legale, l'utente finale dichiara di avere il potere di vincolare tale entità a tali termini di licenza del software.

Copyright

Eccetto laddove esplicitamente dichiarato, non dovrà essere fatto alcun uso del materiale presente su questo sito, della Documentazione, del Software, del Servizio ospitato o dell'Hardware forniti da Avaya. Tutti i contenuti del sito, la documentazione, i Servizi ospitati e i prodotti forniti da Avaya, comprese la selezione, la disposizione e la progettazione dei contenuti, sono proprietà di Avaya o dei relativi concessori di licenza e sono protetti dalle leggi sul copyright e sulla proprietà intellettuale, inclusi i diritti sui generis relativi alla protezione dei database. È vietato modificare, copiare, riprodurre, ripubblicare, caricare, postare, trasmettere o distribuire in qualsiasi forma qualsiasi contenuto, in tutto o in parte, incluso qualsiasi codice o software, salvo espressamente autorizzato da Avaya. La riproduzione, la trasmissione, la diffusione, la memorizzazione o l'utilizzo non autorizzati esplicitamente e per iscritto da Avaya sono azioni perseguibili penalmente e civilmente in base alla legislazione vigente.

Virtualizzazione

Se il prodotto viene installato in una macchina virtuale, si applica quanto segue. Ogni prodotto è dotato del proprio codice di ordinazione e dei relativi tipi di licenza. Se non diversamente specificato, ciascuna Istanza di un prodotto deve essere concessa in licenza e ordinata separatamente. Ad esempio, se il cliente dell'utente finale o il Partner di canale Avaya volesse installare due istanze dello stesso tipo di prodotti, dovranno essere ordinati due prodotti di quel tipo.

Componenti di terzi

Quanto riportato di seguito si applica solo se il codec H.264 (AVC) viene distribuito con il prodotto. QUESTO PRODOTTO È CONCESSO IN LICENZA IN BASE ALLA LICENZA DEL PORTAFOGLIO BREVETTI AVC PER USO PERSONALE DEL CLIENTE O ALTRI UTILIZZI SENZA SCOPO DI LUCRO, PER LE ATTIVITÀ DI (i) CODIFICA VIDEO IN CONFORMITÀ ALLO STANDARD AVC (“VIDEO AVC”) E/O (ii) DECODIFICA DI VIDEO AVC, CODIFICATI DA UN CLIENTE PER ATTIVITÀ PERSONALI E/O OTTENUTI DA UN FORNITORE DI VIDEO IN POSSESSO DI LICENZA PER LA FORNITURA DI VIDEO AVC. NESSUNA LICENZA VIENE CONCESSA O È INTESA PER QUALSIASI ALTRO UTILIZZO. POTREBBERO ESSERE DISPONIBILI ULTERIORI INFORMAZIONI FORNITE DA MPEG LA, L.L.C. VISITARE IL SITO HTTP://WWW.MPEGLA.COM.

Provider di servizi

PER QUANTO RIGUARDA I CODEC, SE IL PARTNER DI CANALE AVAYA OSPITA PRODOTTI CHE UTILIZZANO O INTEGRANO IL CODEC H.264 O H.265, LO STESSO RICONOSCE E ACCETTA DI ESSERE RESPONSABILE PER TUTTE GLI ONERI E/O LE ROYALTY COLLEGATI. IL CODEC H.264 È CONCESSO IN LICENZA IN BASE ALLA LICENZA DEL PORTAFOGLIO BREVETTI AVC PER USO PERSONALE DEL CLIENTE O ALTRI UTILIZZI SENZA SCOPO DI LUCRO, PER LE ATTIVITÀ DI (i) CODIFICA VIDEO IN CONFORMITÀ ALLO STANDARD AVC (“VIDEO AVC”) E/O (ii) DECODIFICA DI VIDEO AVC, CODIFICATI DA UN CLIENTE PER ATTIVITÀ PERSONALI E/O OTTENUTI DA UN FORNITORE DI VIDEO IN POSSESSO DI LICENZA PER LA FORNITURA DI VIDEO AVC. NESSUNA LICENZA VIENE CONCESSA O È INTESA PER QUALSIASI ALTRO UTILIZZO. SONO DISPONIBILI ULTERIORI

INFORMAZIONI SUI CODEC H.264 (AVC) E H.265 (HEVC) DA PARTE DI MPEG LA, L.L.C. VISITARE IL SITO HTTP://WWW.MPEGLA.COM.

Conformità normativa

L'utente riconosce e accetta di essere responsabile del rispetto di leggi e regolamenti applicabili, compresi, ma non limitati a leggi e regolamenti relativi alla registrazione delle chiamate, alla privacy dei dati, alla proprietà intellettuale, al segreto commerciale, alle frodi e ai diritti di esecuzione musicale, nel paese o nel territorio dove è utilizzato il prodotto Avaya.

Prevenzione delle frodi tariffarie

“Frode telefonica” indica l'uso non autorizzato del sistema di telecomunicazione dell'utente, ad esempio da parte di persone che non sono dipendenti, agenti, subappaltatori dell'azienda o che non operano per suo conto. L'utente deve essere consapevole che il sistema potrebbe essere soggetto a rischio di frodi tariffarie che, se attuate, potrebbero far aumentare notevolmente i costi dei servizi di telecomunicazione.

Intervento di Avaya sulle frodi tariffarie

Se si ritiene di essere vittima di frode telefonica e si necessita di assistenza o supporto tecnico, contattare il proprio Rappresentante vendite Avaya.

Vulnerabilità di sicurezza

Le informazioni sulle politiche di supporto alla sicurezza di Avaya sono disponibili nella sezione Security Policies and Support all'indirizzo https://support.avaya.com/security.

Le vulnerabilità sospette della sicurezza dei prodotti Avaya sono gestite per il flusso di supporto della sicurezza dei prodotti Avaya (https://support.avaya.com/css/P8/documents/100161515).

Marchi commerciali

I marchi di fabbrica, i logo e i marchi di servizio (“Marchi”) visualizzati in questo sito, nella documentazione, nei Servizi ospitati e nei prodotti forniti da Avaya sono marchi registrati o non registrati di Avaya, delle sue consociate o di terzi. Agli utenti non è consentito utilizzare tali Marchi senza previo consenso scritto di Avaya o dei terzi possessori del Marchio. Nulla di quanto contenuto in questo sito, nella Documentazione, nei Servizi ospitati e nei prodotti garantisce, per implicazione, preclusione o in altro modo, alcuna licenza o diritto nei confronti dei Marchi, senza l'autorizzazione esplicita per iscritto di Avaya o delle terze parti applicabili.

Avaya è un marchio commerciale registrato di Avaya LLC.

Tutti gli altri marchi di fabbrica non Avaya appartengono ai rispettivi proprietari.

Linux® è un marchio registrato di Linus Torvalds negli Stati Uniti e in altri Paesi.

Download della documentazione

Per la versione più aggiornata della documentazione, visitare il sito Web dell'assistenza Avaya all'indirizzo https://support.avaya.com o un sito indicato successivamente da Avaya.

Contatta l'assistenza Avaya

Visitare il sito Web dell'assistenza di Avaya Avaya https://support.avaya.com per articoli e avvisi su servizi cloud o prodotti o per segnalare un problema con il servizio cloud o il prodotto Avaya in uso. Per un elenco dei numeri di telefono di assistenza e indirizzi di contatto, accedere al sito Web dell'assistenza Avaya all'indirizzo https://support.avaya.com (o a un sito indicato successivamente da Avaya), scorrere fino alla parte inferiore della pagina e selezionare Contact Avaya Support.

Sommario

Parte 1: Supporto degli interni SIP remoti

Capitolo 1: Supporto degli interni SIP remoti su IP Office

Questa sezione fornisce un esempio di processo per il supporto degli interni SIP remoti che si connettono a IP Office tramite Avaya Session Border Controller (ASBCE). ASBCE fornisce una serie di funzioni che forniscono una protezione aggiuntiva al processo di connessione.

- Questo documento si basa su IP Office R11.1.3.1 e ASBCE R10.1.2.
- Per IP Office R11.1.3.1, IP Office supporta gli interni remoti Avaya Workplace Client IPv6 iOS e Android che utilizzano IPv6. In caso contrario, IP Office supporta solo gli interni remoti IPv4.

Interni SIP remoti supportati

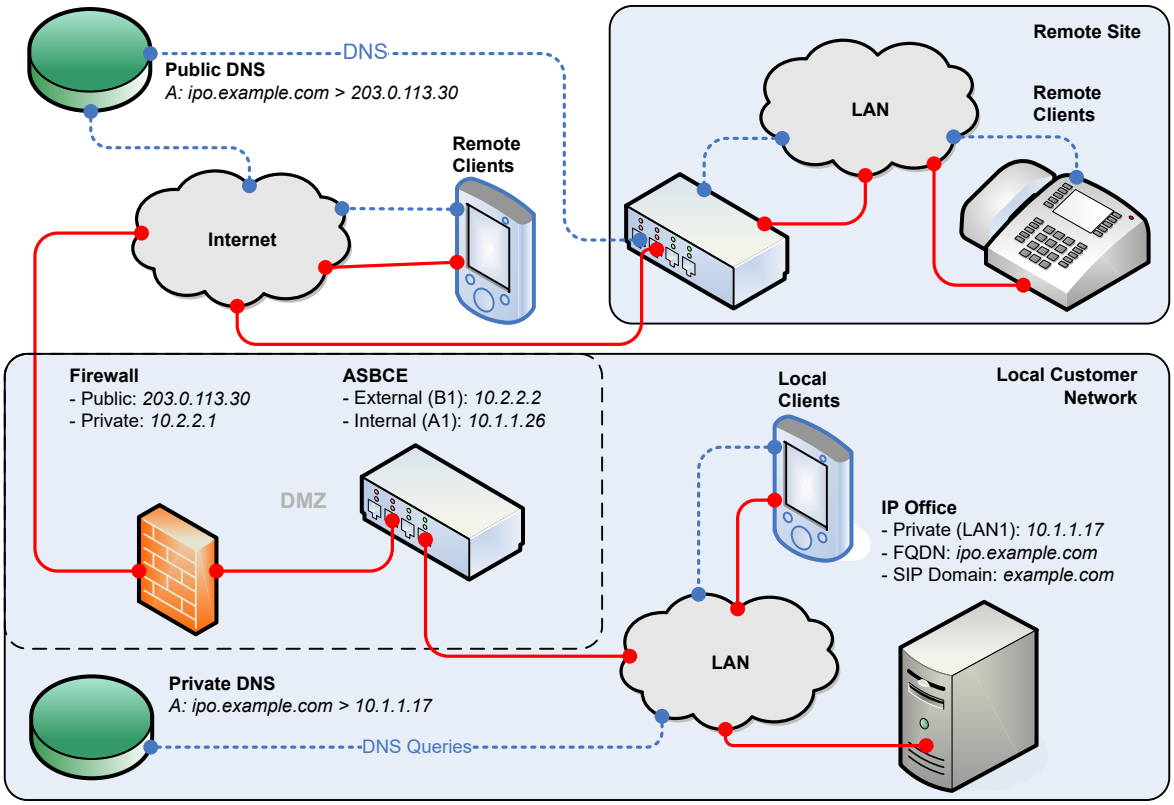
Telefoni da tavolo SIP	Softphone SIP
• Telefoni serie J100 • Telefoni serie K100 (Avaya Vantage™)	• Avaya Workplace Client

Collegamenti correlati

Schema di esempio alla pagina 7
Considerazioni sulla sicurezza alla pagina 9

Schema di esempio

Questo schema mostra lo scenario di esempio utilizzato in questo documento:



- Per questo scenario, gli interni SIP sono telefoni serie J100 e softphone Avaya Workplace Client.
- IP Office è il registrar SIP.
  - Questo esempio utilizza TLS per le connessioni SIP. Ciò richiede la considerazione dei certificati IP Office e la fornitura dei certificati per ASBCE.
- ASBCE dispone di interfacce IP pubbliche e private. Grazie a queste funzioni, funge da gateway per il traffico SIP tra la rete privata del cliente e la rete pubblica Internet.
  - Se utilizzati internamente, i client SIP si connettono direttamente a IP Office.
  - Se utilizzati esternamente, i client SIP si connettono a IP Office tramite ASBCE.
  - ASBCE instrada inoltre le richieste di file utilizzate dagli interni SIP remoti. Ad esempio, le richieste per i file `.txt` e `.xml`.
- La rete del cliente include un firewall tra se stessa e la rete pubblica Internet. Avaya consiglia questa opzione per una maggiore sicurezza.
  - Il firewall inoltra il traffico dagli interni remoti a ASBCE.
- La soluzione DNS del cliente fornisce il DNS diviso. Ovvero:
  - Nella rete privata del cliente, DNS risolve l'FQDN IP Office all'indirizzo IP di IP Office.
  - Sulla rete pubblica Internet, DNS risolve l'FQDN IP Office all'indirizzo IP pubblico del firewall del cliente.

Collegamenti correlati

[Supporto degli interni SIP remoti su IP Office](#) alla pagina 7

Considerazioni sulla sicurezza

Qualsiasi scenario in cui si connette IP Office a una rete pubblica Internet deve includere la considerazione della sicurezza. Le opzioni e i requisiti di sicurezza di IP Office sono descritti nel manuale Avaya IP Office™ Linee guida per la sicurezza di ™ Platform.

In questo caso, la connessione mediante ASBCE rende disponibile una serie di opzioni di sicurezza aggiuntive.

- **Corrispondenza agente utente**

  È possibile configurare le stringhe degli agenti utente che possono connettersi tramite ASBCE. Ciò consente di supportare solo connessioni da applicazioni e dispositivi noti. Consultare Configurazione di un profilo agente utente alla pagina 49.

- **Regole applicazione**

  È possibile utilizzare le regole dell'applicazione per configurare il tipo di media supportato dalle connessioni, il numero massimo di connessioni e il numero massimo di connessioni per interno remoto. Consultare Creazione di una regola dell'applicazione alla pagina 45.

- **Elenchi di blocchi IP/URL**

  È possibile utilizzarli per bloccare gli indirizzi IP o gli URL che non superano ripetutamente la registrazione del nome utente o della password. Consultare Creazione di un elenco di blocchi IP/URI alla pagina 44.

Collegamenti correlati

Supporto degli interni SIP remoti su IP Office alla pagina 7

Capitolo 2: Configurazione di IP Office per interni SIP remoti

Questa sezione fornisce un riepilogo generale della configurazione di IP Office per il supporto della connessione degli interni SIP remoti tramite ASBCE.

Collegamenti correlati

Elenco di controllo per la configurazione di IP Office alla pagina 10
Licenze e sottoscrizioni alla pagina 10
Configurazione VoIP SIP di IP Office alla pagina 11
Impostazione dei dettagli di ASBCE passati agli interni remoti da IP Office alla pagina 12
Aggiunta di ulteriori impostazioni per gli interni remoti alla pagina 14
Aggiunta a whitelist di ASBCE alla pagina 15

Elenco di controllo per la configurazione di IP Office

#	Azione	Collegamenti/Note	✔
1.	Controllare le impostazioni VoIP SIP	Consultare Configurazione VoIP SIP di IP Office alla pagina 11.	
2.	Aggiungere impostazione per interni remoti	Consultare Impostazione dei dettagli di ASBCE passati agli interni remoti da IP Office alla pagina 12.	
3.	Impostare i numeri origine NoUser	Consultare Aggiunta di ulteriori impostazioni per gli interni remoti alla pagina 14.	
4.	Aggiungere alla whitelist ASBCE	Impedire a IP Office di bloccare ASBCE. Consultare Aggiunta a whitelist di ASBCE alla pagina 15.	

Collegamenti correlati

Configurazione di IP Office per interni SIP remoti alla pagina 10

Licenze e sottoscrizioni

IP Office non richiede licenze aggiuntive per supportare il funzionamento con ASBCE. I telefoni e le applicazioni connessi a IP Office mediante ASBCE utilizzano le stesse licenze o sottoscrizioni utilizzate per le operazioni locali.

Collegamenti correlati

Configurazione di IP Office per interni SIP remoti alla pagina 10

Configurazione VoIP SIP di IP Office

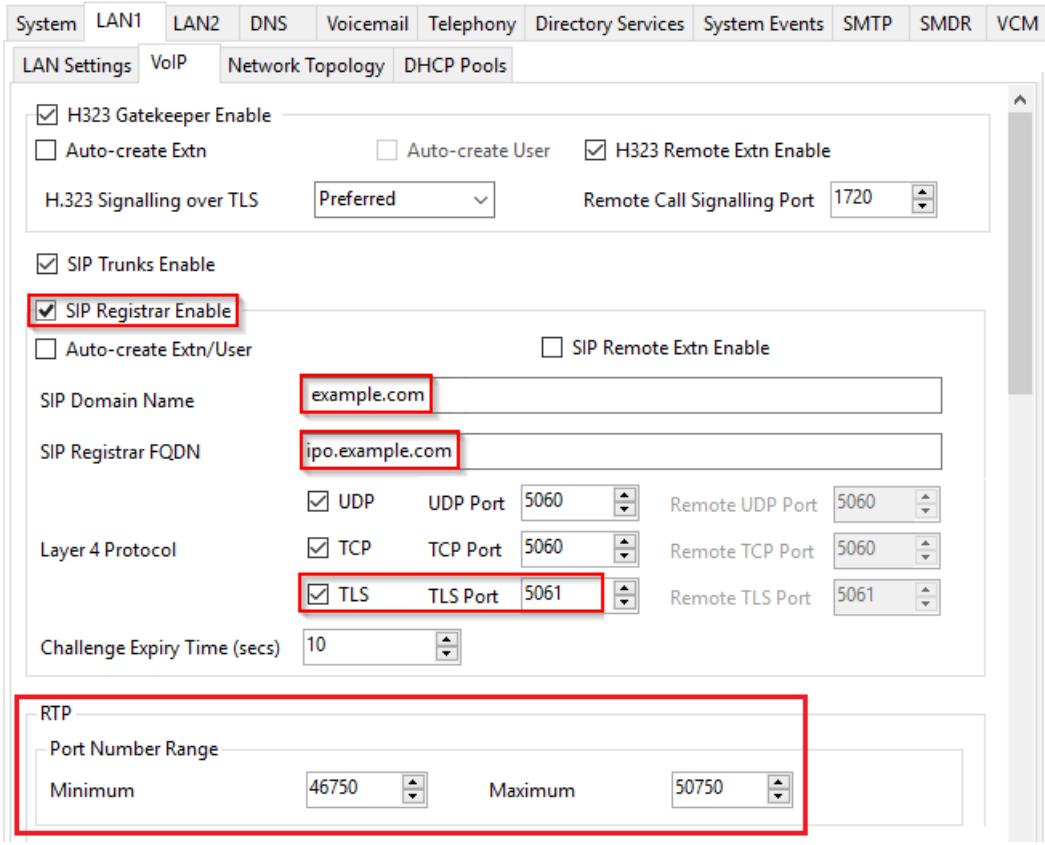
Di seguito è riportata la configurazione di IP Office utilizzata per supportare gli interni SIP nello scenario di esempio. Questa configurazione è la stessa per gli interni SIP locali e remoti.

Importante:

- La modifica di queste impostazioni richiede un riavvio di IP Office.

Procedura

1. Accedere a IP Office utilizzando IP Office Manager o IP Office Web Manager.
2. Selezionare **Sistema** o **Impostazioni di sistema** > **Sistema**.
3. Selezionate il tab **LAN1**.



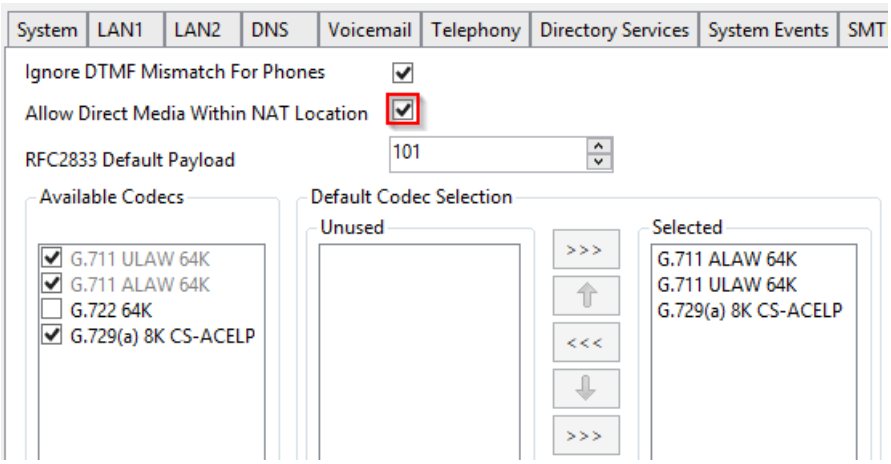
Campo	Descrizione
Abilita registrar SIP	Consente agli interni SIP di registrarsi con IP Office.
Abilita interno remoto SIP	Disabilitata. ASBCE gestisce le connessioni NAT dell'interno remoto.

La tabella continua…

Campo	Descrizione
Nome dominio SIP	Consente di impostare il dominio che i client SIP devono utilizzare per la registrazione.
FQDN registrar SIP	Consente di impostare il nome di dominio completo per l'instradamento delle connessioni SIP a IP Office.
Protocollo livello 4	Consente di impostare i protocolli e le porte di livello 4 su cui IP Office ascolta il traffico degli interni SIP.
Intervallo numeri di porte	Consente di impostare l'intervallo di numeri di porta utilizzato da IP Office per il traffico RTP e RTCP.

4. Selezionare la sottoscheda **VoIP**.

   Attivare la casella di controllo **Consenti Direct Media con posizione NAT**.



   - Abilitando questa opzione, i Direct Media tra i dispositivi risiedono sulla stessa sottorete che si connette a IP Office utilizzando NAT. Per supportare questa funzione tramite , ASBCE richiede una configurazione aggiuntiva affinché ASBCE annulli l'ancoraggio dal media di chiamata, vedere Annullamento dell'ancoraggio dei media di chiamata dal menu ASBCE alla pagina 59.

5. Fare clic su **OK** o **Aggiorna**.
6. Salvare le impostazioni e riavviare il sistema IP Office:
   - Se si utilizza IP Office Manager, salvare le impostazioni e riavviare il sistema
   - Se si utilizza IP Office Web Manager, fare clic su **Salva in IP Office** e riavviare il sistema.

Collegamenti correlati

Configurazione di IP Office per interni SIP remoti alla pagina 10

Impostazione dei dettagli di ASBCE passati agli interni remoti da IP Office

Prima di registrarsi con IP Office, gli interni Avaya richiedono il file `46xxsettings.txt`. Questo file contiene le impostazioni utilizzate dagli interni.

Per gli interni remoti, il file `46xxsettings.txt` generato automaticamente da IP Office deve contenere le informazioni sugli indirizzi che l'interno remoto può utilizzare per connettersi a ASBCE.

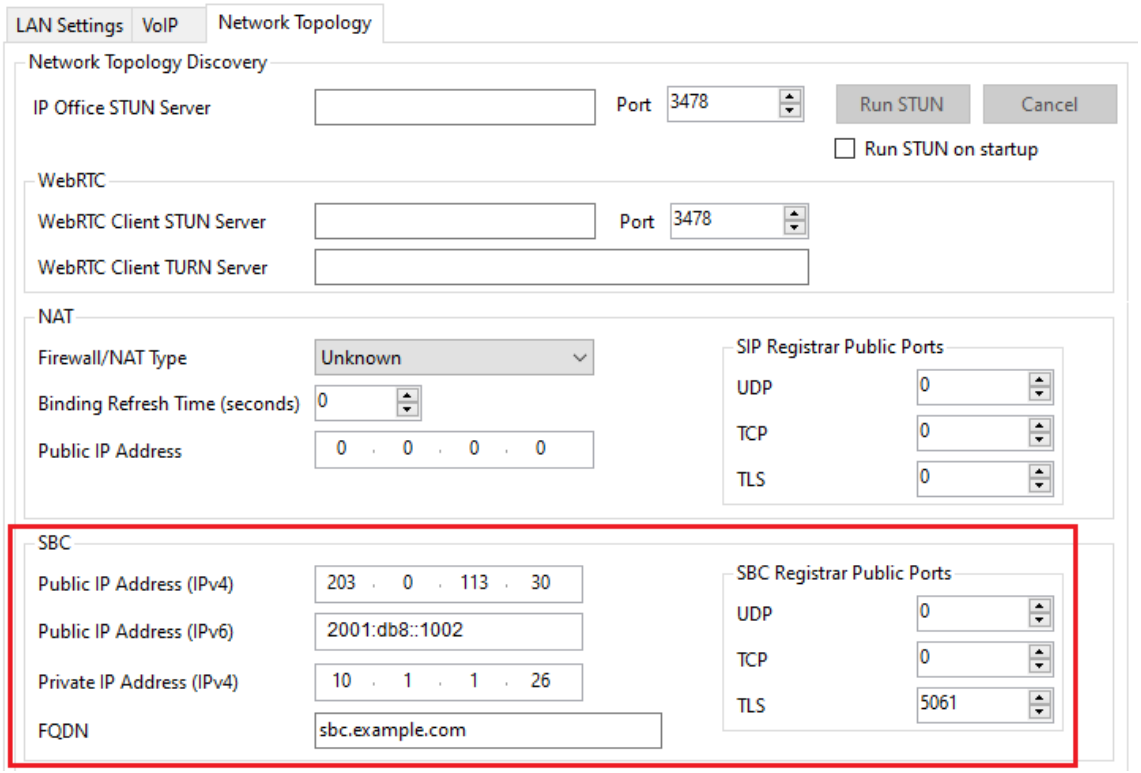
- Gli interni richiedono il file `46xxsettings.txt` quando si registrano per la prima volta con IP Office.
- Dopo aver ricevuto il file `46xxsettings.txt`, per impostazione predefinita gli interni richiedono di nuovo il file ogni 24 ore per applicare eventuali modifiche.
- Gli interni richiedono il file anche ogni volta che si riavviano. È possibile riavviarli in remoto utilizzando SysMonitor o System Status Application.

Importante:

- La modifica di queste impostazioni richiede un riavvio di IP Office.

Procedura

1. Accedere a IP Office utilizzando IP Office Manager o IP Office Web Manager.
2. Selezionare **Sistema** o **Impostazioni di sistema** > **Sistema**.
3. Selezionare la LAN (**LAN1** o **LAN2**) connessa alla stessa rete di ASBCE.
4. Selezionare **Topologia di rete**.
   - Se si utilizza IP Office Web Manager, è possibile modificare queste impostazioni solo in modalità non in linea. Fare clic sull'icona e selezionare **Modalità non in linea**.
5. Nella sezione **SBC**, immettere le seguenti informazioni:



Impostazione	Descrizione
Indirizzo IP pubblico (IPv4)	L'indirizzo IPv4 pubblico per il traffico client SIP in entrata nella rete del cliente. • Si tratta dell'indirizzo IPv4 pubblico di ASBCE o del servizio di accesso a Internet come il firewall del cliente. • Il DNS esterno deve risolvere l'FQDN IP Office a questo indirizzo quando richiesto da un interno remoto IPv4.
Indirizzo IP pubblico (IPv6)	L'indirizzo IPv6 pubblico per il traffico client SIP in entrata nella rete del cliente, come indicato in precedenza. Per maggiori dettagli, consultare Supporto degli interni remoti IPv6 alla pagina 70. • Si tratta dell'indirizzo IPv6 pubblico di ASBCE o del servizio di accesso a Internet come il firewall del cliente. • Il DNS esterno deve risolvere l'FQDN IP Office a questo indirizzo quando richiesto da un interno remoto IPv6.
Indirizzo IP privato (IPv4)	L'indirizzo IPv4 privato/interno di ASBCE. • Il DNS interno deve risolvere **FQDN** indicato di seguito a questo indirizzo.
FQDN	Il nome di dominio completo di ASBCE. Il DNS deve risolvere questo FQDN agli indirizzi IPv6 utilizzati (IPv4 utilizza l'FQDN del registrar SIP IP Office).
Porte pubbliche registrar SIP	Le porte pubbliche (esterne) **UDP**, **TCP** e/o le porte **TLS** che i client SIP esterni devono utilizzare per connettersi a ASBCE.

6. Fare clic su **OK** o **Aggiorna**.
7. Salvare le impostazioni e riavviare il sistema IP Office:
   - Se si utilizza IP Office Manager, salvare le impostazioni e riavviare il sistema
   - Se si utilizza IP Office Web Manager, fare clic su **Salva in IP Office** e riavviare il sistema.

Collegamenti correlati

Configurazione di IP Office per interni SIP remoti alla pagina 10

Aggiunta di ulteriori impostazioni per gli interni remoti

È possibile utilizzare i seguenti numeri origine **NoUser** per impostare valori aggiuntivi nel file `46xxsettings.txt` generato automaticamente che IP Office fornisce agli interni remoti.

Procedura

1. Accedere a IP Office utilizzando IP Office Manager o IP Office Web Manager.
2. Fare clic su **Utente** o **Gestione chiamate** > **Utente**.
3. Individuare le impostazioni per l'utente denominato *NoUser*.
4. Selezionare **Numeri di origini**.
5. Aggiungere i numeri origine *NoUser* aggiuntivi richiesti:
   - **SET_STIMULUS_SBC_REG_INTERVAL=**`<seconds>`

Questo numero origine *NoUser* consente di impostare l'intervallo di registrazione utilizzato dai telefoni serie J100. L'impostazione predefinita è 3600 secondi (1 ora). Quando si supportano i telefoni tramite ASBCE, il valore consigliato è 180 secondi. L'intervallo supportato è compreso tra 180 e 3600 secondi.

- **PUBLIC_HTTP=**`<file server address>`

  Quando si utilizzano le impostazioni **Indirizzo IP server HTTP** e **Reindirizzamento HTTP**, IP Office utilizza questo valore per impostare l'indirizzo del file server pubblico assegnato agli interni remoti.

6. Fare clic su **OK** o **Aggiorna**.
7. Salvare le impostazioni e riavviare il sistema IP Office:
   - Se si utilizza IP Office Manager, salvare le impostazioni e riavviare il sistema
   - Se si utilizza IP Office Web Manager, fare clic su **Salva in IP Office** e riavviare il sistema.

Collegamenti correlati

Configurazione di IP Office per interni SIP remoti alla pagina 10

Aggiunta a whitelist di ASBCE

Con l'interno remoto connesso a IP Office tramite ASBCE, i tentativi di registrazione non corretti possono causare il blocco dell'indirizzo IP ASBCE da parte di IP Office.

Procedura

1. Accedere a IP Office utilizzando IP Office Manager o IP Office Web Manager.
2. Selezionare **Sistema** o **Impostazioni di sistema** > **Sistema**.
3. Selezionare **VoIP** > **Liste di controllo degli accessi**.
4. Aggiungere l'indirizzo IP interno di ASBCE a **Elenco indirizzi abilitati IP**.
5. Fare clic su **OK** o **Aggiorna**.
6. Se si utilizza IP Office Manager, salvare le impostazioni nel sistema IP Office.

Collegamenti correlati

Configurazione di IP Office per interni SIP remoti alla pagina 10

Capitolo 3: Aggiunta di certificati IP Office a ASBCE

Per lo scenario di esempio, IP Office utilizza il certificato autofirmato. In tal caso, ASBCE ha bisogno di:

- Una copia del certificato radice IP Office. Questa è l'autorità di certificazione (CA).
- Un certificato di identità per ASBCE emesso da IP Office.
  - **Per IPv4:** il certificato deve includere l'indirizzo IP Office FQDN (CN o SAN) e IPv4 (SAN).
  - **Per IPv6:** oltre all'indirizzo FQDN e IPv4 di IP Office, il certificato di identità ASBCE deve includere l'indirizzo FQDN e IPv6 ASBCE.

Utilizzo di certificati di terze parti

Se IP Office utilizza certificati emessi da una CA terza, i certificati radice e di identità richiesti per ASBCE devono essere emessi da tale CA. Tuttavia, i principi per i dettagli richiesti nel certificato di identità rimangono gli stessi descritti in questa sezione della documentazione.

Collegamenti correlati

Elenco di controllo certificati ASBCE alla pagina 16
Download del certificato radice di IP Office alla pagina 17
Aggiunta del certificato radice di IP Office a ASBCE alla pagina 18
Generazione di un certificato di identità ASBCE mediante IP Office Web Manager alla pagina 18
Generazione di un certificato di identità ASBCE tramite Web Control (visualizzazione piattaforma) alla pagina 19
Divisione del certificato di identità ASBCE alla pagina 20
Aggiunta del certificato di identità a ASBCE alla pagina 22

Elenco di controllo certificati ASBCE

#	Azione	Collegamenti/Note	✔
1.	Scarica il certificato radice IP Office	Consultare Download del certificato radice di IP Office alla pagina 17.	
2.	Aggiungere il certificato radice a ASBCE	Consultare Aggiunta del certificato radice di IP Office a ASBCE alla pagina 18.	

La tabella continua…

#	Azione	Collegamenti/Note	✔
3.	Generare un certificato di identità per ASBCE	Consultare Generazione di un certificato di identità ASBCE mediante IP Office Web Manager alla pagina 18.	
4.	Dividere il certificato	Estrarre i file separati del certificato e della chiave privata dal certificato di identità. Consultare Divisione del certificato di identità ASBCE alla pagina 20.	
5.	Aggiungere i file a ASBCE	Aggiungere il certificato di identità e i file delle chiavi private a ASBCE Consultare Aggiunta del certificato di identità a ASBCE alla pagina 22.	

Collegamenti correlati

Aggiunta di certificati IP Office a ASBCE alla pagina 16

Download del certificato radice di IP Office

Attenersi alla procedura seguente per scaricare una copia del certificato radice IP Office.

Procedura

1. Accedere a IP Office utilizzando IP Office Web Manager.
   - Per IP500 V2, immettere l'indirizzo di sistema seguito da `:8443/WebMgmtEE/WebManagerment.html`.
   - Per un server basato su Linux, immettere l'indirizzo del sistema seguito da `:7070/WebManagement/WebManagement.html`.
2. Selezionare **Sicurezza** > **Impostazioni di sicurezza**.
3. Se IP Office si trova in una rete multisito, fare clic su accanto a IP Office.
4. Selezionare **Certificati**.
5. In **Store di certificati affidabili**, individuare il certificato radice utilizzato dal sistema IP Office.
6. Fare clic su accanto al certificato.
7. Fare clic su **Sì**.
8. Rinominare il file `IPO_RootCA.crt`.

Passi successivi

- Accedere a Aggiunta del certificato radice di IP Office a ASBCE alla pagina 18.

Collegamenti correlati

Aggiunta di certificati IP Office a ASBCE alla pagina 16

Aggiunta del certificato radice di IP Office a ASBCE

Attenersi alla procedura seguente per caricare la copia del certificato radice IP Office in ASBCE.

Prerequisiti

- Scaricare il certificato radice IP Office. Consultare Download del certificato radice di IP Office alla pagina 17.

Procedura

1. Accedere a **Gestione TLS** > **Certificati**.
2. Fare clic su **Installa**.
3. Impostare **Tipo** su **Certificato CA**.
4. Immettere un nome descrittivo per il certificato.
5. Attivare **Consenti certificato/chiave debole**.
6. Fare clic su **Scegli file** e selezionare il file `IPO_RootCA.crt`.
7. Fare clic su **Carica**. Il menu visualizza un avviso che indica che si tratta di un certificato autofirmato.
8. Fare clic su **Procedi**. Il menu visualizza il certificato.
9. Fare clic su **Installa**.
10. Fare clic su **Fine**.

Passi successivi

- Utilizzare IP Office per creare un certificato di identità per ASBCE:
  - Per i sistemi di sottoscrizione, vedere Generazione di un certificato di identità ASBCE mediante IP Office Web Manager alla pagina 18.
  - Per altri sistemi, vedere Generazione di un certificato di identità ASBCE tramite Web Control (visualizzazione piattaforma) alla pagina 19.

Collegamenti correlati

Aggiunta di certificati IP Office a ASBCE alla pagina 16

Generazione di un certificato di identità ASBCE mediante IP Office Web Manager

Questo processo genera un certificato di identità per ASBCE utilizzando IP Office Web Manager.

- Questo processo è destinato ai sistemi IP Office in modalità sottoscrizione che utilizzano la **gestione automatica dei certificati** . Per altri sistemi, vedere Generazione di un certificato di identità ASBCE tramite Web Control (visualizzazione piattaforma) alla pagina 19.

Procedura

1. Accedere al sistema utilizzando IP Office Web Manager.
   - Per IP500 V2, immettere l'indirizzo di sistema seguito da `:8443/WebMgmtEE/WebManagerment.html`.
   - Per un server basato su Linux, immettere l'indirizzo del sistema seguito da `:7070/WebManagement/WebManagement.html`.
2. Selezionare **Sicurezza** > **Impostazioni di sicurezza**.
3. Se IP Office si trova in una rete multisito, fare clic su accanto a IP Office.
4. Selezionare **Certificati**.
5. Fare clic su **Rigenera**.
6. Selezionare **Crea certificato per un altro computer**.
7. In **Nome oggetto**, immettere l'FQDN di ASBCE.
8. In **Nomi alternativi oggetto**, immettere eventuali valori aggiuntivi per altri server e servizi a cui ASBCE deve connettersi.
   - **Per IPv4:** il certificato deve includere l'indirizzo IP Office FQDN e IPv4.
   - **Per IPv6:** oltre all'indirizzo FQDN e IPv4 di IP Office, il certificato di identità ASBCE deve includere l'indirizzo FQDN e IPv6 ASBCE.
   - Utilizzare valori separati da virgole per le voci richieste *DNS:<FQDN>* e *IP:<IP address>*.
   - Se si utilizzano FQDN diversi per il dominio XMPP Avaya one-X® Portal, immettere tutti gli FQDN come elenco separato da virgole di voci DNS.
9. Fare clic su **OK**. Attendere fino a un minuto mentre IP Office genera il certificato.
10. Quando richiesto, impostare una password di crittografia per il certificato di identità e fare clic su **Sì**.
11. Il browser richiederà di scaricare e salvare il file del certificato.
12. Rinominare il file scaricato in `SBCE_ID.p12`.

Passi successivi

- Consultare Divisione del certificato di identità ASBCE alla pagina 20.

Collegamenti correlati

Aggiunta di certificati IP Office a ASBCE alla pagina 16

Generazione di un certificato di identità ASBCE tramite Web Control (visualizzazione piattaforma)

Questo processo genera un certificato di identità per ASBCE utilizzando i menu di Web Control del server IP Office.

Procedura

1. Accedere ai menu Web Control di IP Office:
   - Da IP Office Web Manager, selezionare il server primario. Fare clic su ☰ e selezionare **Visualizzazione piattaforma**.
   - Scorrere fino a `https://<IP Office IP address>:7071` e accedere.
2. Selezionare la scheda **Impostazioni** e scorrere verso il basso fino a **Certificati**.
3. Selezionare **Crea certificato per un altro computer**.
4. Immettere i seguenti dati:
5. In **IP computer** immettere l'indirizzo IP esterno di ASBCE.
6. In **Password** immettere una password per codificare il certificato e la chiave.
7. In **Nome oggetto**, immettere l'FQDN di ASBCE.
8. In **Nomi alternativi oggetto**, immettere eventuali valori aggiuntivi per altri server e servizi a cui ASBCE deve connettersi.
   - **Per IPv4:** il certificato deve includere l'indirizzo IP Office FQDN e IPv4.
   - **Per IPv6:** oltre all'indirizzo FQDN e IPv4 di IP Office, il certificato di identità ASBCE deve includere l'indirizzo FQDN e IPv6 ASBCE.
   - Utilizzare valori separati da virgole per le voci richieste *DNS:<FQDN>* e *IP:<IP address>*.
   - Se si utilizzano FQDN diversi per il dominio XMPP Avaya one-X® Portal, immettere tutti gli FQDN come elenco separato da virgole di voci DNS.
9. Fare clic su **Rigenera**.
10. Fare clic sul collegamento nella finestra popup e salvare il file.
11. Rinominare il file scaricato in `SBCE_ID.p12`.

Passi successivi

- Consultare Divisione del certificato di identità ASBCE alla pagina 20.

Collegamenti correlati

Aggiunta di certificati IP Office a ASBCE alla pagina 16

Divisione del certificato di identità ASBCE

Il certificato di identità creato per ASBCE da IP Office è un singolo file. Contiene sia il certificato che la chiave privata. Per la configurazione di ASBCE, è necessario suddividere il certificato di identità in file separati di certificati e chiavi private.

Prerequisiti

- Utilizzare IP Office per creare un certificato di identità per ASBCE:
  - Per i sistemi di sottoscrizione, vedere Generazione di un certificato di identità ASBCE mediante IP Office Web Manager alla pagina 18.

- Per altri sistemi, vedere Generazione di un certificato di identità ASBCE tramite Web Control (visualizzazione piattaforma) alla pagina 19.

Procedura

1. Utilizzando WinSCP, connettersi all'indirizzo IP di gestione di ASBCE utilizzando la porta 222 e l'accesso ipcs.
2. Copiare il certificato di identità IP Office creato per ASBCE (`SBCE_ID.p12`) nella directory ASBCE **`/home/ipcs`**.
3. SSH all'IP di gestione di ASBCE utilizzando la porta 222 e l'accesso ipcs.
4. Immettere il comando **su root** o **su -root** e digitare la password radice di ASBCE.
5. Immettere i seguenti comandi. Il comando da utilizzare dipende dal fatto che sia stato generato il certificato utilizzando IP Office Web Manager o i menu Web Control (visualizzazione piattaforma).

   Nota:

   - Quando viene richiesta una password o una passphrase PEM, immettere la password specificata durante la generazione del certificato di identità per ASBCE.
   - Se la password include caratteri speciali, devono essere preceduti da `\` quando si inseriscono nella riga di comando. Ad esempio, nella riga di comando, immettere `@` nella password come `\@`.

   - **Certificato Web Control di IP Office:**

     Attenersi alla seguente procedura con un certificato generato utilizzando i menu di Web Control IP Office.

     ```
     openssl pkcs12 -in SBCE_ID.p12 -out SBCE_ID.crt -nokeys -clcerts
     openssl pkcs12 -in SBCE_ID.p12 -out SBCE_ID.key -nocerts
     ```

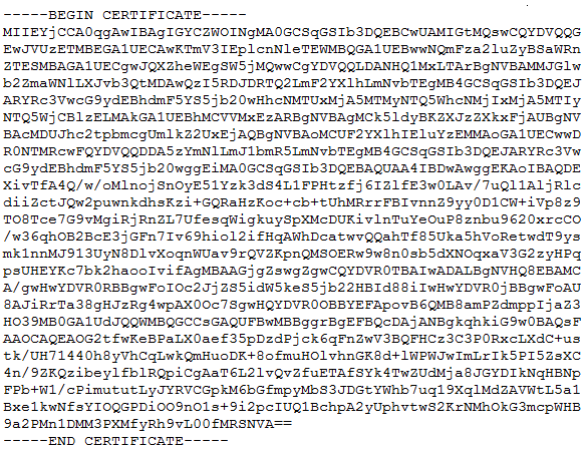
   - **Certificato Web Manager di IP Office:**

     Attenersi alla seguente procedura con un certificato generato utilizzando IP Office Web Manager.

     ```
     openssl enc -base64 -d -in SBCE_ID.p12 -out SBCE_ID_BIN.p12 -A
     openssl pkcs12 -in SBCE_ID_BIN.p12 -out SBCE_ID.crt -nokeys -clcerts
     openssl pkcs12 -in SBCE_ID_BIN.p12 -out SBCE_ID.key -nocerts
     ```

6. Copiare i nuovi file `SBCE_ID.crt` e `SBCE_ID.key` da ASBCE al PC
7. Il file `SBCE_ID.crt` contiene ancora il certificato CA radice IP Office, la chiave privata e il certificato ID ASBCE. Per poter importare il file in ASBCE, è necessario rimuovere il certificato CA e la chiave privata dal file.
   a. Aprire `SBCE_ID.crt` in WordPad sul PC.

b. Rimuovere tutte le righe tranne quelle che si trovano tra la prima riga **BEGIN CERTIFICATE** e **END CERTIFICATE**. Ad esempio:



Passi successivi

- Accedere a Aggiunta del certificato di identità a ASBCE alla pagina 22.

Collegamenti correlati

Aggiunta di certificati IP Office a ASBCE alla pagina 16

Aggiunta del certificato di identità a ASBCE

Attenersi alla procedura seguente per caricare il certificato di identità in ASBCE.

Prerequisiti

- Divisione del certificato di identità ASBCE alla pagina 20

Procedura

1. Accedere a **Gestione TLS** > **Certificati**.
2. Fare clic su **Installa**.
3. In **Tipo**, selezionare **Certificato**.
4. Immettere un nome descrittivo per il certificato.
5. Fare clic su **Scegli file** e selezionare il file `SBCE_ID.crt`.
6. Selezionare **Carica file chiave**.
7. Fare clic su **Scegli file** e selezionare il file `SBCE_ID.key`.
8. Fare clic su **Carica**. Il menu visualizza il certificato.
9. Fare clic su **Installa**.
10. Fare clic su **Fine**.
11. Tramite SSH, accedere all'indirizzo IP di gestione di ASBCE utilizzando la porta 222 e l'accesso ipcs.
    a. Immettere `su root` o `su -root` e la password radice ASBCE.

b. Immettere i seguenti comandi, sostituendo `********` con la password impostata durante la generazione del certificato di identità:

```
cd /usr/local/ipcs/cert/key
enc_key SBCE_ID.key ********
```

- È necessario aggiungere `\` prima dei caratteri speciali nella password. Ad esempio, per immettere `@`, digitare `\@`.

Collegamenti correlati

Aggiunta di certificati IP Office a ASBCE alla pagina 16

Capitolo 4: Configurazione ASBCE per interni SIP remoti

Questa sezione esamina la configurazione di ASBCE per instradare le chiamate SIP tra gli interni remoti e IP Office.

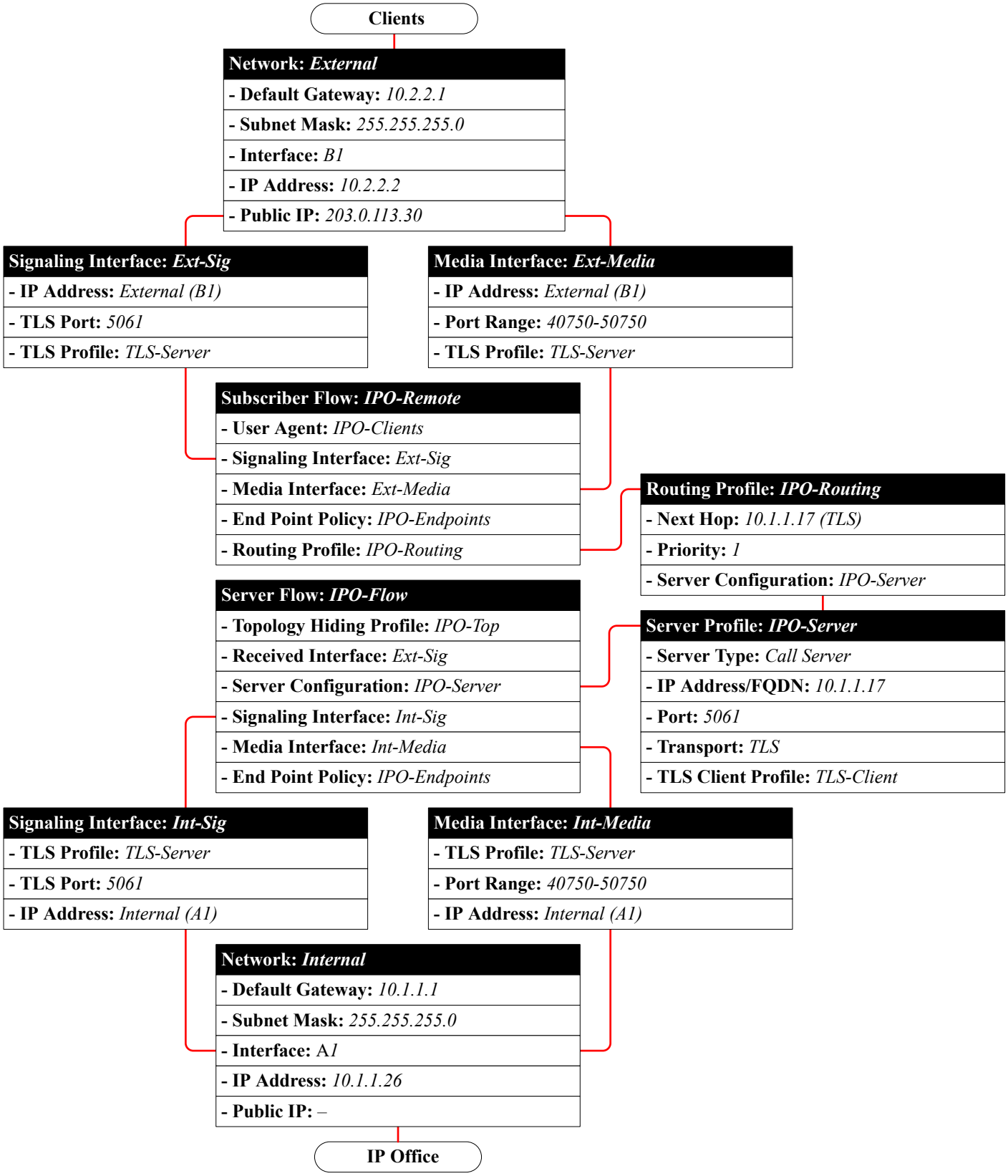
- **Supporto IPv6:** per informazioni dettagliate sul supporto degli interni remoti IPv6, vedere Supporto degli interni remoti IPv6 alla pagina 70.
  - **Se sono supportati solo gli interni remoti IPv6:** seguire la procedura di configurazione descritta in questa sezione per IPv4, ma sostituire gli indirizzi IPv4 esterni con gli indirizzi IPv6, ove applicabile.
  - **Se sono supportati gli interni remoti IPv4 e IPv6:** è necessario eseguire ulteriori passaggi di configurazione dopo aver completato la configurazione IPv4. Consultare Elenco di controllo per la configurazione degli interni remoti IPv4 e IPv6 combinati alla pagina 74.

Collegamenti correlati

Aggiunta di proxy inversi per le richieste di file alla pagina 54

Riepilogo flusso chiamate ASBCE

Questa immagine riepiloga i componenti di configurazione ASBCE utilizzati per la connessione tra gli interni remoti IPv4 e IP Office.



Collegamenti correlati

[Configurazione ASBCE per interni SIP remoti](#) alla pagina 24

Clona / Aggiungi

Importante:

Diversi processi in questo documento indicano di creare nuovi elementi clonando un modello esistente invece di aggiungere una nuova voce. Ovvero, fare clic su **Clona** invece di **Aggiungi**.

- È necessario utilizzare **Clona** quando indicato in un processo ed è necessario clonare il profilo esistente indicato nelle istruzioni.
- Utilizzando **Aggiungi** verrà creata una nuova voce con impostazioni predefinite diverse da quelle del clone previsto. Ciò causerà un funzionamento errato.

Collegamenti correlati

Configurazione ASBCE per interni SIP remoti alla pagina 24

Elenco di controllo per la configurazione di ASBCE

#	Azione	Collegamenti/Note	✔
1.	Configurazione inoltro porta firewall	Instradare il traffico esterno dai client a ASBCE. Consultare Configurazione firewall alla pagina 29.	
2.	Configurazione dell'interfaccia di rete esterna ASBCE	Impostare gli indirizzi IP esterni utilizzati da ASBCE. Consultare Configurazione dell'interfaccia esterna ASBCE alla pagina 29.	
3.	Configurare l'interfaccia di rete interna ASBCE.	Impostare gli indirizzi IP interni utilizzati da ASBCE. Consultare Configurazione dell'interfaccia interna ASBCE alla pagina 31.	
4.	Creazione di un profilo client TLS	Ciò imposta le impostazioni TLS utilizzate da ASBCE quando si connette a IP Office. Consultare Creazione di un profilo client TLS alla pagina 32.	
5.	Creazione di un profilo server TLS	Ciò imposta le impostazioni TLS utilizzate da ASBCE quando i client e IP Office si connettono ad esso. Consultare Creazione di un profilo server TLS alla pagina 34.	
6.	Creazione di un'interfaccia multimediale SIP interna	Definire le porte e gli indirizzi su cui ASBCE ascolta i contenuti multimediali SIP da IP Office. Consultare Creazione di un'interfaccia di segnalazione interna alla pagina 37.	
7.	Creazione di un'interfaccia multimediale SIP esterna	Definire le porte e gli indirizzi su cui ASBCE ascolta i supporti SIP per gli interni remoti. Consultare Creazione dell'interfaccia di segnalazione esterna alla pagina 38.	

La tabella continua…

#	Azione	Collegamenti/Note	✔
8.	Creazione di un'interfaccia di segnalazione SIP interna	Definire le porte e gli indirizzi su cui ASBCE ascolta la segnalazione di chiamata SIP da IP Office. Consultare Creazione di un'interfaccia di segnalazione interna alla pagina 37.	
9.	Creazione di un'interfaccia di segnalazione SIP esterna	Definire le porte e gli indirizzi su cui ASBCE ascolta la segnalazione di chiamata SIP dagli interni remoti. Consultare Creazione dell'interfaccia di segnalazione esterna alla pagina 38.	
10.	Creazione di un profilo server	Consultare Creazione di un profilo server ASBCE per IP Office alla pagina 39.	
11.	Creazione di instradamento server	Consultare Creazione di un profilo di instradamento del server alla pagina 41.	
12.	Configurazione topologia nascosta	Definire le conversioni delle informazioni dell'intestazione SIP che ASBCE deve effettuare. Consultare Creazione di un criterio di topologia nascosta ASBCE alla pagina 43.	
13.	Creazione di un elenco di blocchi IP/URL.	Impostare i tipi di contenuti multimediali supportati e il numero massimo di connessioni. Consultare Creazione di un elenco di blocchi IP/URI alla pagina 44.	
14.	Creazione di una regola dell'applicazione	Impostare il tipo e il numero di connessioni multimediali supportate. Consultare Creazione di una regola dell'applicazione alla pagina 45.	
15.	Creazione di una regola multimediale	Consultare Creazione di una regola multimediale alla pagina 46.	
16.	Creazione di un criterio endpoint	Un criterio endpoint raggruppa le regole dell'applicazione e dei media. Consultare Creazione di un gruppo di criteri endpoint alla pagina 48.	
17.	Aggiunta di un profilo agente utente	Definire i valori UA per gli interni remoti di cui ASBCE deve consentire la connessione. Consultare Configurazione di un profilo agente utente alla pagina 49.	
18.	Creazione di un flusso di abbonati	Consultare Creazione del flusso degli abbonati alla pagina 51.	
19.	Creazione di un flusso server	Consultare Creazione di un flusso server alla pagina 53.	
20.	Aggiungere un proxy inverso per Avaya Workplace Client	Instradare le richieste di file di impostazioni da parte dei client a IP Office. Consultare Aggiunta di proxy inversi per le richieste di file alla pagina 54.	

Collegamenti correlati

Configurazione ASBCE per interni SIP remoti alla pagina 24

Configurazione firewall

È necessario configurare l'apparecchiatura di rete del cliente sull'edge della rete per instradare il traffico dell'interno remoto esterno a ASBCE. Il processo effettivo varia a seconda della rete e dell'apparecchiatura del cliente. Di seguito sono riportate solo le linee guida.

Procedura

1. Attivare solo **NAT livello 3**.
2. Disattivare tutte le funzionalità SIP note come ALG.
3. Inoltrare le seguenti porte all'indirizzo IP dell'interfaccia B1 di ASBCE.
   - **Per Avaya Workplace Client e i telefoni serie J100:**

Protocollo di trasporto/applicazione		Porta	Utilizzo
tcp	tls	5061	Connessione SIP TLS per la registrazione.
	http	80	Richieste di file generali e sicure da telefoni e client se **Usa porte telefono preferito** non è abilitato su IP Office.
	https	443	
	http	8411	Richieste di file generali e sicure da telefoni e client se **Usa porte telefono preferito** è abilitato su IP Office.
	https	411	
udp	rtp	40750 to 50750	L'intervallo di porte utilizzato per il traffico RTP (Call Media) e RTCP (Call Control).
	rtcp		

Passi successivi

- Accedere a Configurazione dell'interfaccia esterna ASBCE alla pagina 29.

Collegamenti correlati

Configurazione ASBCE per interni SIP remoti alla pagina 24

Configurazione dell'interfaccia esterna ASBCE

Aggiungere dettagli per la rete del cliente tra il firewall del cliente e ASBCE.

- **Supporto IPv4/IPv6 doppio:** per supportare gli interni remoti IPv4 e IPv6, è necessario creare voci separate per IPv4 e IPv6:
  - **Indirizzo IP** per ognuno deve utilizzare il rispettivo indirizzo IPv4 o IPv6 *B1*.

Importante:

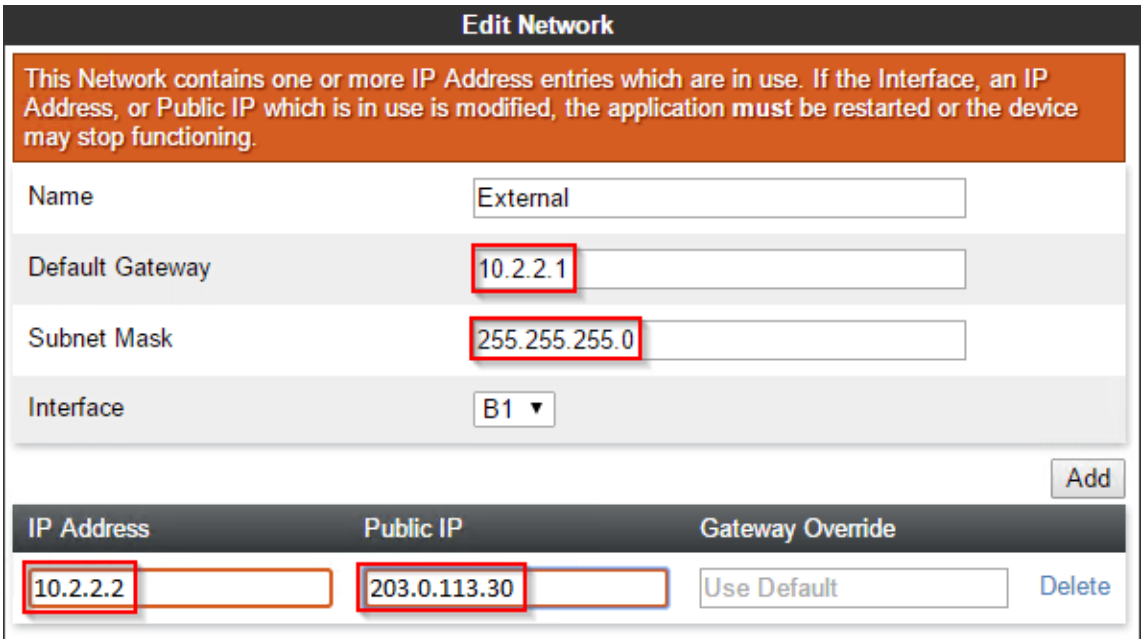
- Questo processo richiede il riavvio di ASBCE. Questa operazione terminerà tutte le connessioni correnti che utilizzano ASBCE.

Prerequisiti

- Configurazione firewall alla pagina 29

Procedura

1. Accedere a **Impostazioni specifiche del dispositivo** > **Gestione rete**.
2. Selezionare la scheda **Reti** e fare clic su **Aggiungi**.
3. Immettere i seguenti dati:



Campo	Descrizione
Nome	Utilizzare questo nome in altri menu per selezionare la rete.
Gateway predefinito	L'indirizzo IP interno dell'apparecchiatura che instrada il traffico tra la rete del cliente e l'Internet pubblico. Per lo scenario di esempio, questo è l'indirizzo interno del firewall.
Subnet mask	Maschera IP per la rete **Gateway predefinito**.
Interfaccia	Selezionare l'interfaccia pubblica di ASBCE.

4. Fare clic su **Aggiungi** e immettere un indirizzo IP utilizzato da ASBCE su questa interfaccia di rete.

Campo	Descrizione
Indirizzo IP	Immettere l'indirizzo IP dell'interfaccia ASBCE connessa al firewall.
IP pubblico	Immettere l'indirizzo IP pubblico del firewall. Deve corrispondere all'indirizzo IP a cui DNS indirizza l'interno remoto quando esegue la ricerca DNS del nome di dominio completo IP Office.

5. Se sono supportati sia gli interni remoti IPv4 che IPv6, ripetere la procedura per creare le voci IPv6.

Passi successivi

- Accedere a Configurazione dell'interfaccia interna ASBCE alla pagina 31.

Collegamenti correlati

Configurazione ASBCE per interni SIP remoti alla pagina 24

Configurazione dell'interfaccia interna ASBCE

Aggiungere dettagli per la rete del cliente tra ASBCE e IP Office.

- **Supporto IPv4/IPv6 doppio:** è possibile utilizzare la stessa voce per gli interni remoti IPv4 e IPv6.

Importante:

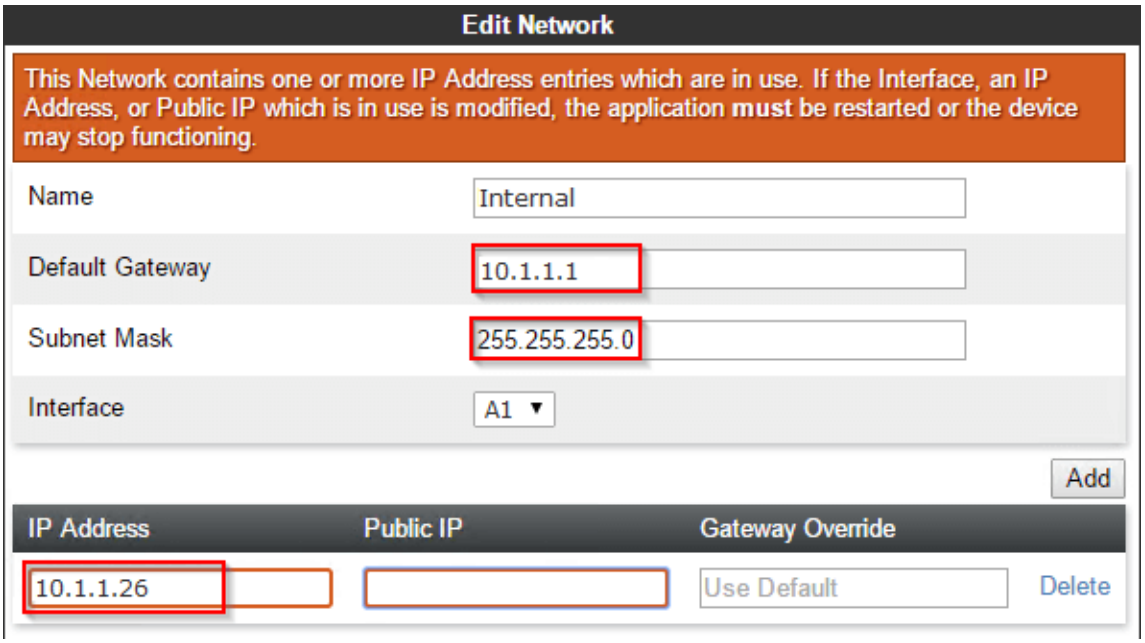
- Questo processo richiede il riavvio di ASBCE. Questa operazione terminerà tutte le connessioni correnti che utilizzano ASBCE.

Prerequisiti

- Configurazione dell'interfaccia esterna ASBCE alla pagina 29

Procedura

1. Accedere a **Impostazioni specifiche del dispositivo** > **Gestione rete**.
2. Selezionare la scheda **Reti** e fare clic su **Aggiungi**.
3. Immettere i seguenti dati:



Campo	Descrizione
Nome	Utilizzare questo nome in altri menu per selezionare la rete.
Gateway predefinito	L'indirizzo IP e il gateway predefinito per il traffico all'interno della rete del cliente.
Subnet mask	
Interfaccia	Selezionare l'interfaccia privata di ASBCE.

4. Fare clic su **Aggiungi** e immettere un indirizzo IP utilizzato da ASBCE su questa interfaccia di rete.

Campo	Descrizione
Indirizzo IP	Immettere l'indirizzo IP dell'interfaccia ASBCE connessa alla rete del cliente. Questo è l'indirizzo IP dell'interfaccia A1.

5. Accedere a **Gestione del sistema** e fare clic su **Riavvia applicazione**.

Passi successivi

- Accedere a Creazione di un profilo client TLS alla pagina 32.

Collegamenti correlati

Configurazione ASBCE per interni SIP remoti alla pagina 24

Creazione di un profilo client TLS

Per le connessioni TLS da ASBCE, agisce come client TLS. Ad esempio, per le connessioni a IP Office e ai client esterni. Il profilo del client TLS utilizzato per ciascuna connessione definisce i certificati utilizzati e le altre impostazioni TLS.

- **Supporto IPv4/IPv6 doppio:** è possibile utilizzare la stessa voce per gli interni remoti IPv4 e IPv6.

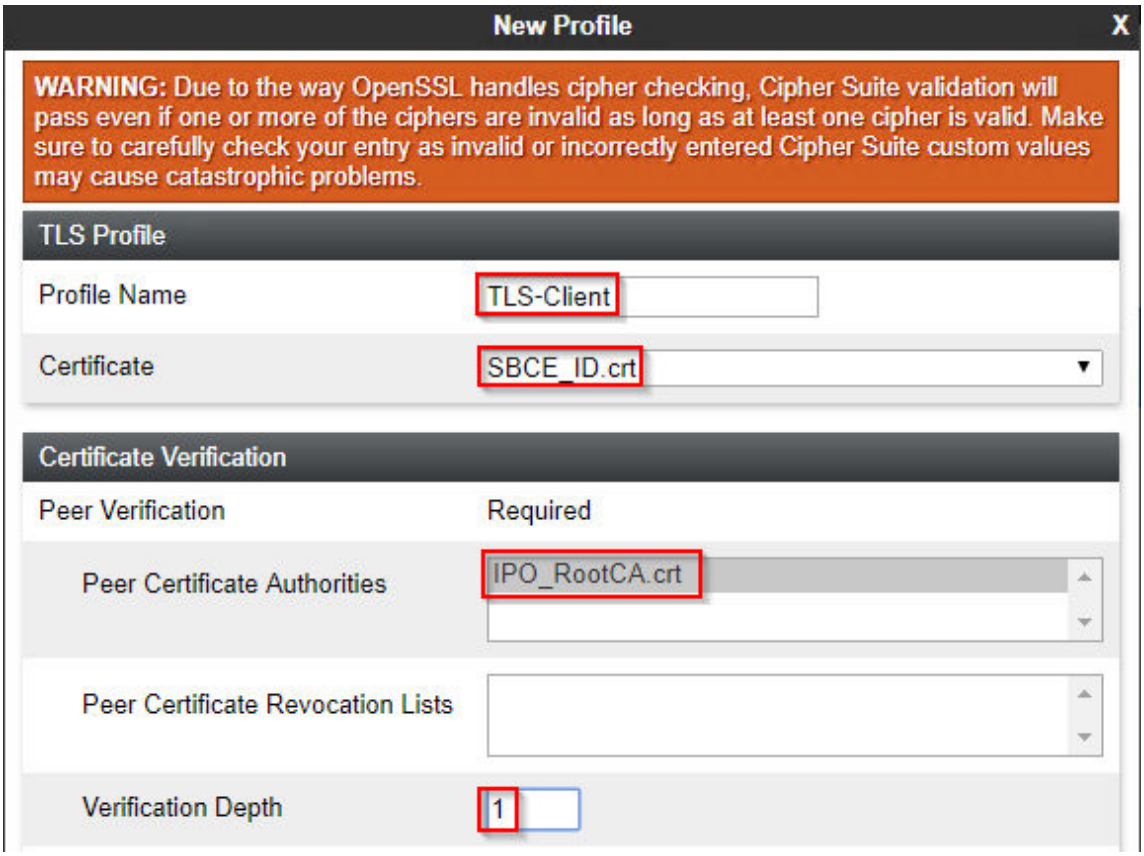
Prerequisiti

- Configurazione dell'interfaccia interna ASBCE alla pagina 31.

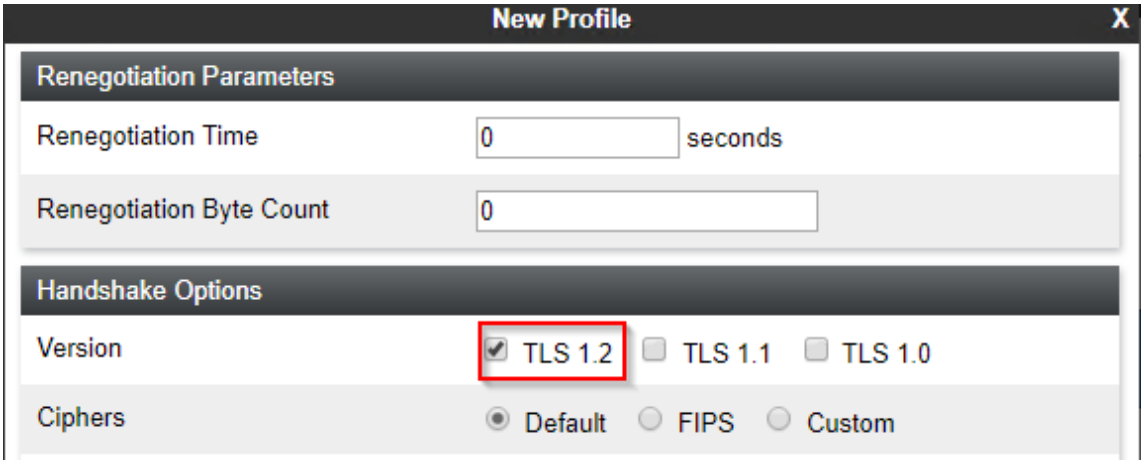
Procedura

1. Selezionare **Gestione TLS** > **Profili client**.

2. Fare clic su **Aggiungi**.



3. Immettere un nome. È quindi possibile utilizzare questa opzione per selezionare il criterio in altri menu.
4. In **Certificato**, selezionare il certificato di identità creato per ASBCE.
5. In **Autorità di certificazione peer**, selezionare il certificato radice utilizzato per creare il certificato di identità. Per lo scenario di esempio, questo è il file `IPO_RootCA.crt` caricato in ASBCE.
6. In **Profondità di verifica**, immettere **1**.
7. Fare clic su **Avanti**.



8. Attivare **TLS 1.2**.
9. Fare clic su **Fine**.

Passi successivi

- Accedere a Creazione di un profilo server TLS alla pagina 34.

Collegamenti correlati

Configurazione ASBCE per interni SIP remoti alla pagina 24

Creazione di un profilo server TLS

Per le connessioni TLS a ASBCE, agisce come server TLS. Ad esempio, per le connessioni da IP Office e da client esterni. Il profilo del client TLS utilizzato per ciascuna connessione definisce i certificati utilizzati e le altre impostazioni TLS.

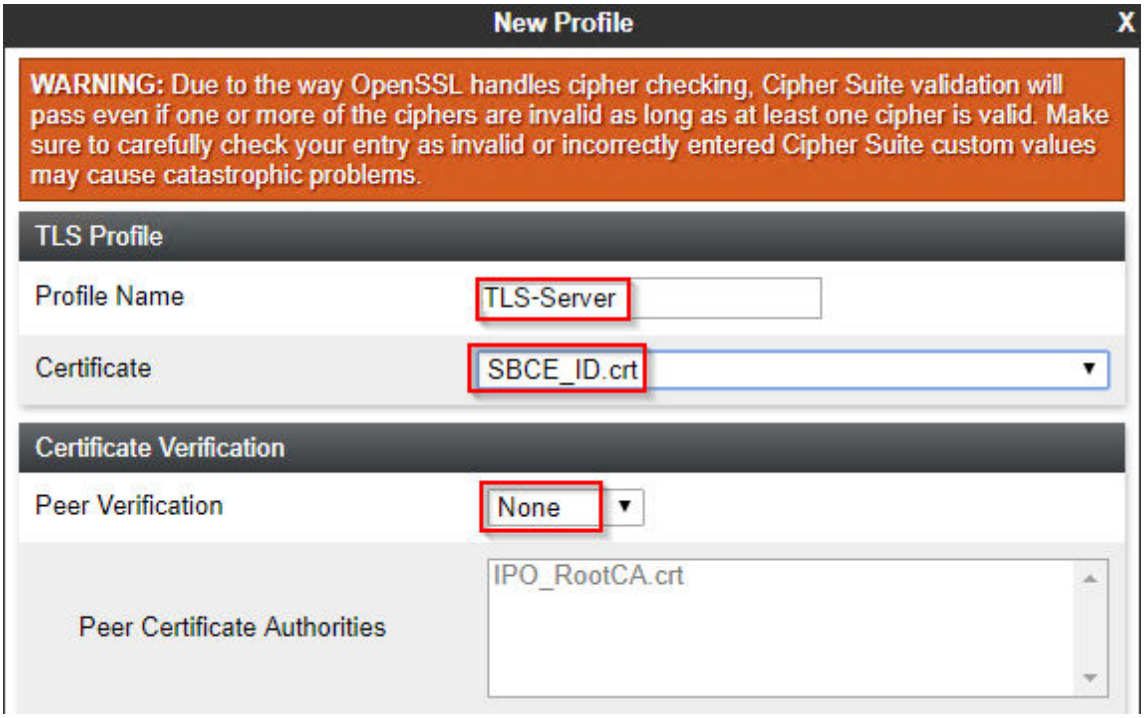
- **Supporto IPv4/IPv6 doppio:** è possibile utilizzare la stessa voce per gli interni remoti IPv4 e IPv6.

Prerequisiti

- Creazione di un profilo client TLS alla pagina 32.

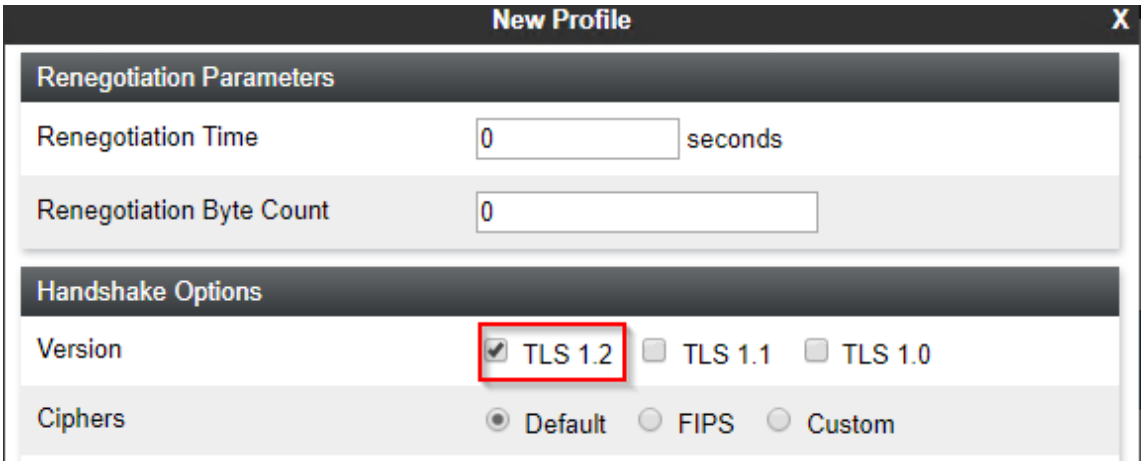
Procedura

1. Selezionare **Gestione TLS** > **Profili client**.
2. Fare clic su **Aggiungi**.



3. Immettere un nome. È quindi possibile utilizzare questa opzione per selezionare il criterio in altri menu.

4. In **Certificato**, selezionare il certificato di identità creato per ASBCE.
5. In **Autorità di certificazione peer**, selezionare **Nessuno**.
6. Fare clic su **Avanti**.



7. Attivare **TLS 1.2**.
8. Fare clic su **Fine**.

Passi successivi

- Accedere a Creazione di un'interfaccia multimediale interna alla pagina 35.

Collegamenti correlati

Configurazione ASBCE per interni SIP remoti alla pagina 24

Creazione di un'interfaccia multimediale interna

È necessario creare un'interfaccia multimediale interna. ASBCE la utilizza per ascoltare i contenuti multimediali delle chiamate SIP da IP Office.

- **Supporto IPv4/IPv6 doppio:** è possibile utilizzare la stessa voce per gli interni remoti IPv4 e IPv6.

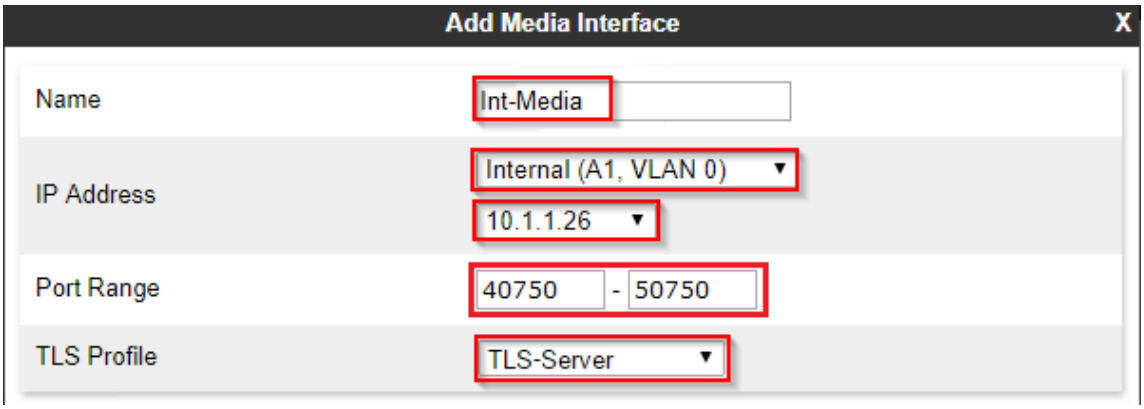
Prerequisiti

- Creazione di un profilo client TLS alla pagina 32.

Procedura

1. Selezionare **Impostazioni specifiche del dispositivo** > **Interfaccia multimediale**.

2. Fare clic su **Aggiungi**.



3. Immettere un nome. È quindi possibile utilizzare questa opzione per selezionare il criterio in altri menu.
4. Selezionare l'interfaccia interna di ASBCE.
5. Per **Profilo TLS**, selezionare il profilo del server TLS creato per il traffico verso ASBCE.
6. Fare clic su **Fine**.

Passi successivi

- Accedere a Creazione di un'interfaccia multimediale esterna alla pagina 36.

Collegamenti correlati

Configurazione ASBCE per interni SIP remoti alla pagina 24

Creazione di un'interfaccia multimediale esterna

È necessario creare un'interfaccia multimediale esterna. ASBCE utilizza questa opzione per ascoltare i contenuti multimediali delle chiamate SIP dagli interni remoti.

- **Supporto IPv4/IPv6 doppio:** per supportare gli interni remoti IPv4 e IPv6, è necessario creare voci separate per IPv4 e IPv6:
  - **Indirizzo IP** per ognuno deve utilizzare il rispettivo indirizzo IPv4 o IPv6 *B1*.

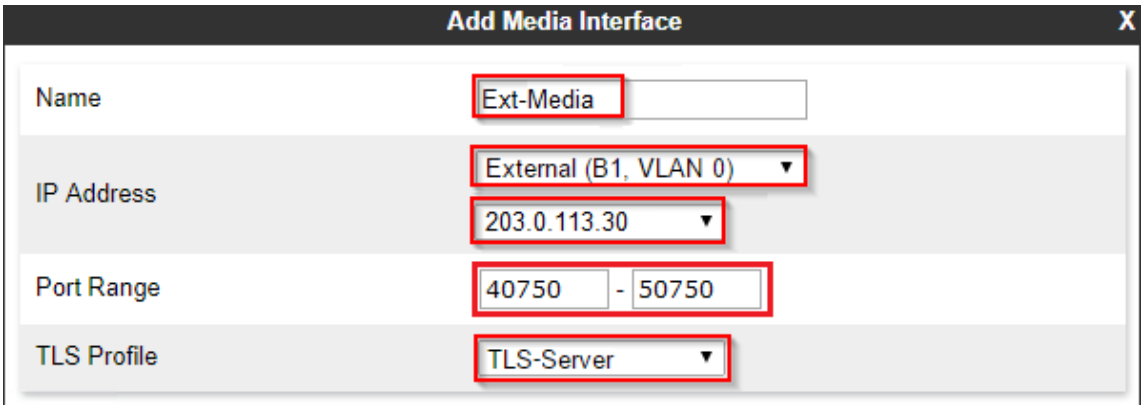
Prerequisiti

- Creazione di un'interfaccia multimediale interna alla pagina 35.

Procedura

1. Accedere a **Impostazioni specifiche del dispositivo** > **Interfaccia multimediale**.

2. Fare clic su **Aggiungi**.



3. Immettere un nome. È quindi possibile utilizzare questa opzione per selezionare il criterio in altri menu.
4. Selezionare l'interfaccia esterna e l'indirizzo IP di ASBCE.
5. Per **Profilo TLS**, selezionare il profilo del server TLS creato per il traffico verso ASBCE.
6. Fare clic su **Fine**.
7. Se sono supportati sia gli interni remoti IPv4 che IPv6, ripetere la procedura per creare le voci IPv6.

Passi successivi

- Accedere a Creazione di un'interfaccia di segnalazione interna alla pagina 37.

Collegamenti correlati

Configurazione ASBCE per interni SIP remoti alla pagina 24

Creazione di un'interfaccia di segnalazione interna

È necessario creare un'interfaccia di segnalazione interna. ASBCE la utilizza per ascoltare la segnalazione di chiamata SIP da IP Office.

- **Supporto IPv4/IPv6 doppio:** è possibile utilizzare la stessa voce per gli interni remoti IPv4 e IPv6.

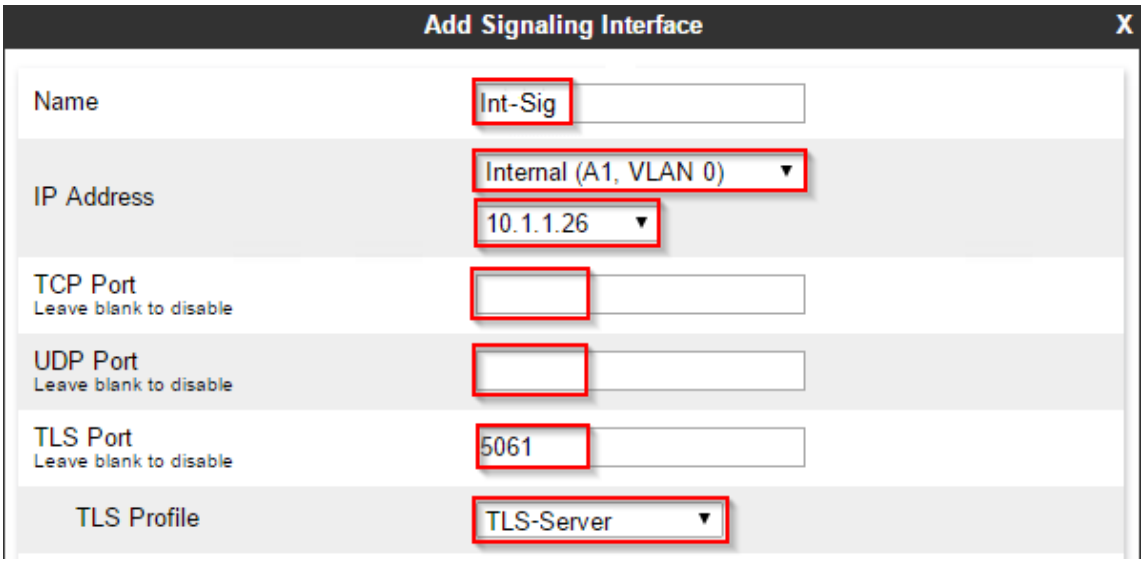
Prerequisiti

- Creazione di un'interfaccia multimediale esterna alla pagina 36.

Procedura

1. Selezionare **Impostazioni specifiche del dispositivo** > **Interfaccia di segnalazione**.

2. Fare clic su **Aggiungi**.



3. Immettere un nome. È quindi possibile utilizzare questa opzione per selezionare il criterio in altri menu.
4. Scegliere *A1* dall'elenco a discesa **Indirizzo IP**.
5. Lasciare **Porta TCP** vuoto per disattivare TCP.
6. Lasciare **Porta UDP** vuoto per disattivare UDP.
7. Impostare **Porta TLS** in modo che corrisponda alla porta TLS IP Office.
8. Per **Profilo TLS**, selezionare il profilo del server TLS creato per il traffico verso ASBCE.
9. Fare clic su **Fine**.

Passi successivi

- Accedere a Creazione dell'interfaccia di segnalazione esterna alla pagina 38.

Collegamenti correlati

Configurazione ASBCE per interni SIP remoti alla pagina 24

Creazione dell'interfaccia di segnalazione esterna

È necessario creare un'interfaccia di segnalazione esterna. ASBCE la utilizza per ascoltare i messaggi di registrazione SIP dagli interni remoti.

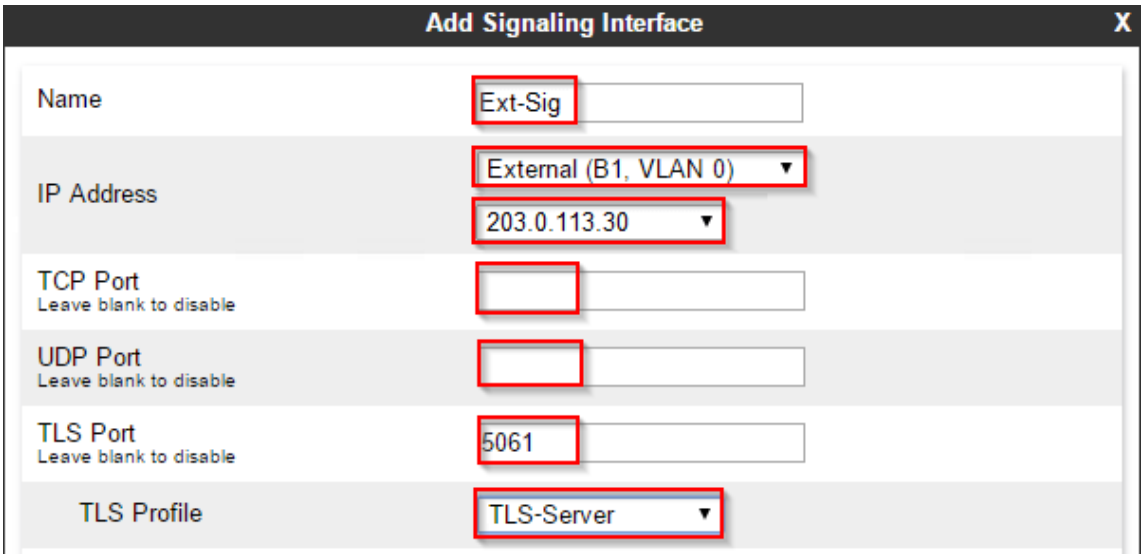
- **Supporto IPv4/IPv6 doppio:** per supportare gli interni remoti IPv4 e IPv6, è necessario creare voci separate per IPv4 e IPv6:
  - **Indirizzo IP** per ognuno deve utilizzare il rispettivo indirizzo IPv4 o IPv6 *B1*.

Prerequisiti

- Creazione di un'interfaccia di segnalazione interna alla pagina 37.

Procedura

1. Selezionare **Impostazioni specifiche del dispositivo** > **Interfaccia di segnalazione**.
2. Fare clic su **Aggiungi**.



3. Immettere un nome. È quindi possibile utilizzare questa opzione per selezionare il criterio in altri menu.
4. Scegliere *B1* dall'elenco a discesa **Indirizzo IP**.
5. Lasciare **Porta TCP** vuoto per disattivare TCP.
6. Lasciare **Porta UDP** vuoto per disattivare UDP.
7. Impostare **Porta TLS** in modo che corrisponda alla porta TLS IP Office.
8. Per **Profilo TLS**, selezionare il profilo del server TLS creato per il traffico verso ASBCE.
9. Fare clic su **Fine**.
10. Se sono supportati sia gli interni remoti IPv4 che IPv6, ripetere la procedura per creare le voci IPv6.

Passi successivi

- Accedere a Creazione di un profilo server ASBCE per IP Office alla pagina 39.

Collegamenti correlati

Configurazione ASBCE per interni SIP remoti alla pagina 24

Creazione di un profilo server ASBCE per IP Office

È necessario creare un profilo server su ASBCE che corrisponda alla configurazione di IP Office, vedere Configurazione VoIP SIP di IP Office alla pagina 11.

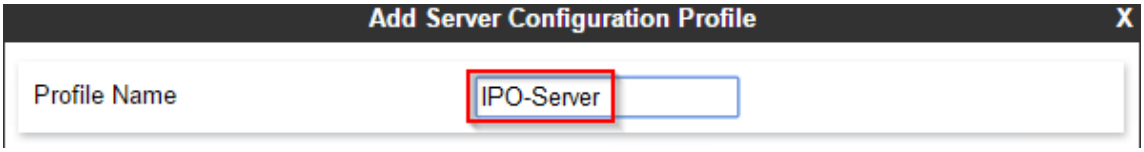
- **Supporto IPv4/IPv6 doppio:** è possibile utilizzare la stessa voce per gli interni remoti IPv4 e IPv6.

Prerequisiti

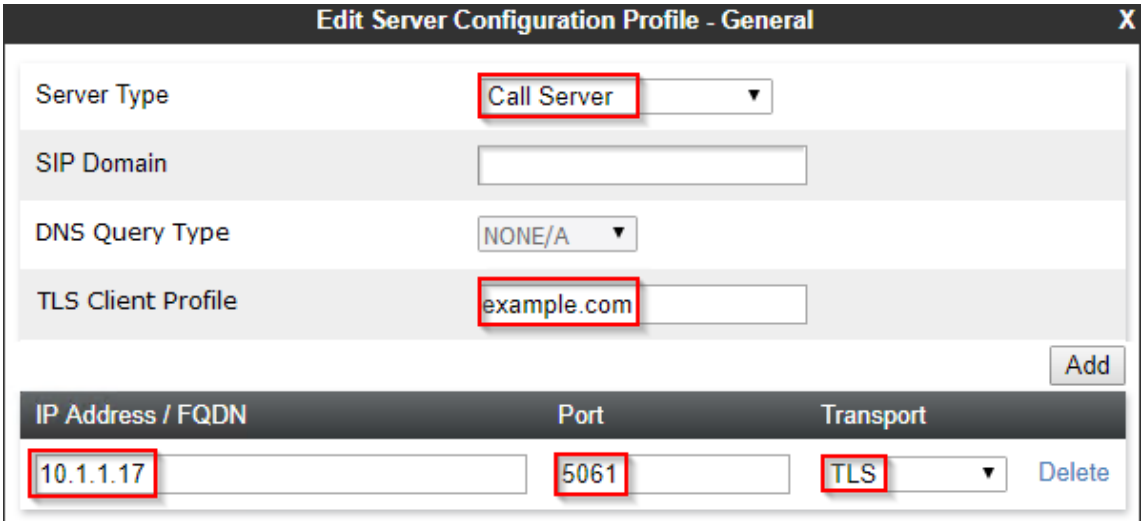
- Creazione di un'interfaccia di segnalazione interna alla pagina 37.

Procedura

1. Selezionare **Profili globali** > **Configurazione server**.
2. Fare clic su **Aggiungi**.
3. Immettere un nome. È quindi possibile utilizzare questa opzione per selezionare il criterio in altri menu.

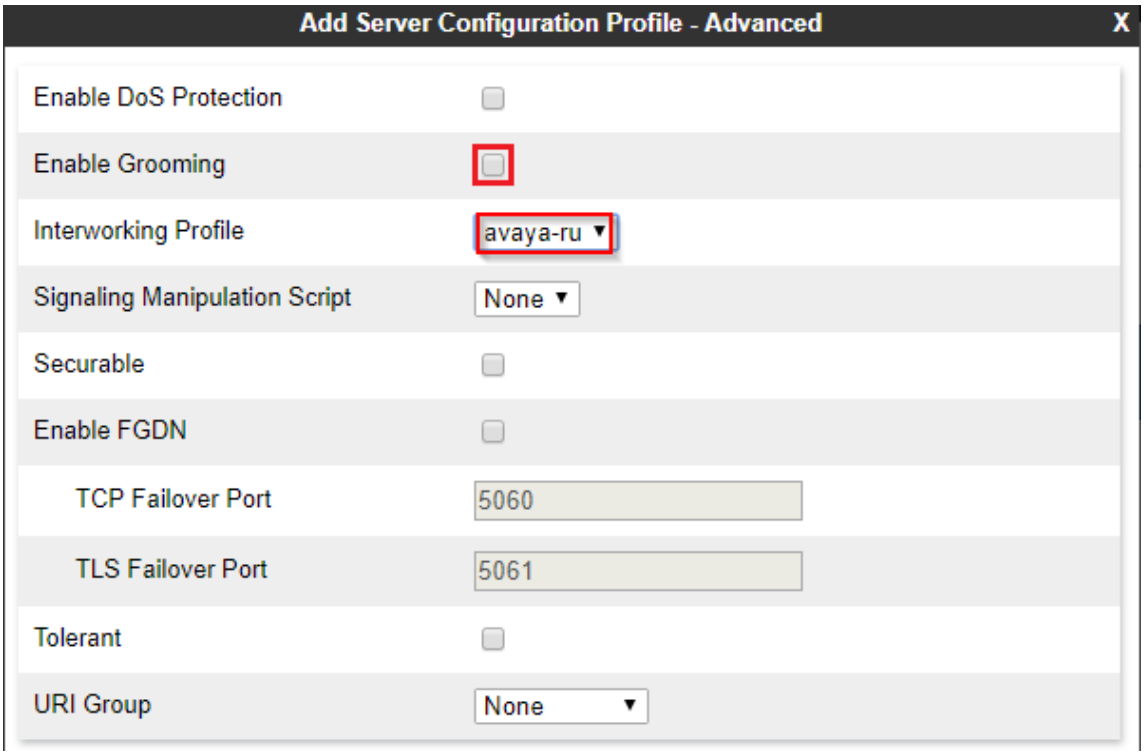


4. Fare clic su **Avanti**.



   a. Per **Tipo di server** selezionare **Server delle chiamate**.
   b. Impostare **Dominio SIP** in modo che corrisponda a quello utilizzato da IP Office per la registrazione SIP.
   c. Per **Profilo client TLS** selezionare il profilo client TLS creato.
   d. Fare clic su **Aggiungi** e immettere i dettagli per le connessioni SIP della porta di livello 4 impostate nella configurazione di IP Office.
      - Impostare **Indirizzo IP/FQDN** su un indirizzo IP di IP Office.
      - Impostare **Porta** e **Trasporto** in modo che corrispondano alle impostazioni IP Office.
   e. Fare clic su **Avanti**.
5. Fare clic su **Avanti** per saltare le impostazioni di **Autenticazione**.
6. Fare clic su **Avanti** per saltare le impostazioni **Heartbeat**.

7. Regolare le impostazioni avanzate come segue:



   a. Deselezionare la casella di controllo **Abilita grooming**.
   b. Impostare **Profilo di interoperabilità** su *avaya-ru*.

8. Fare clic su **Fine**.

Passi successivi

- Accedere a Creazione di un profilo di instradamento del server alla pagina 41.

Collegamenti correlati

Configurazione ASBCE per interni SIP remoti alla pagina 24

Creazione di un profilo di instradamento del server

ASBCE utilizza un profilo di instradamento del server per instradare il traffico in entrata corrispondente al server o ai server appropriati. In questo caso, è necessario creare un profilo che instrada il traffico a IP Office.

- **Supporto IPv4/IPv6 doppio:** è possibile utilizzare la stessa voce per gli interni remoti IPv4 e IPv6.

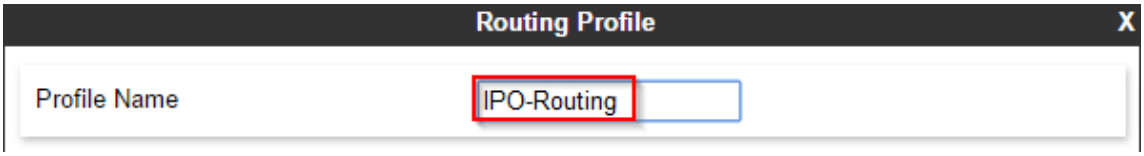
Prerequisiti

- Creazione di un profilo server ASBCE per IP Office alla pagina 39.

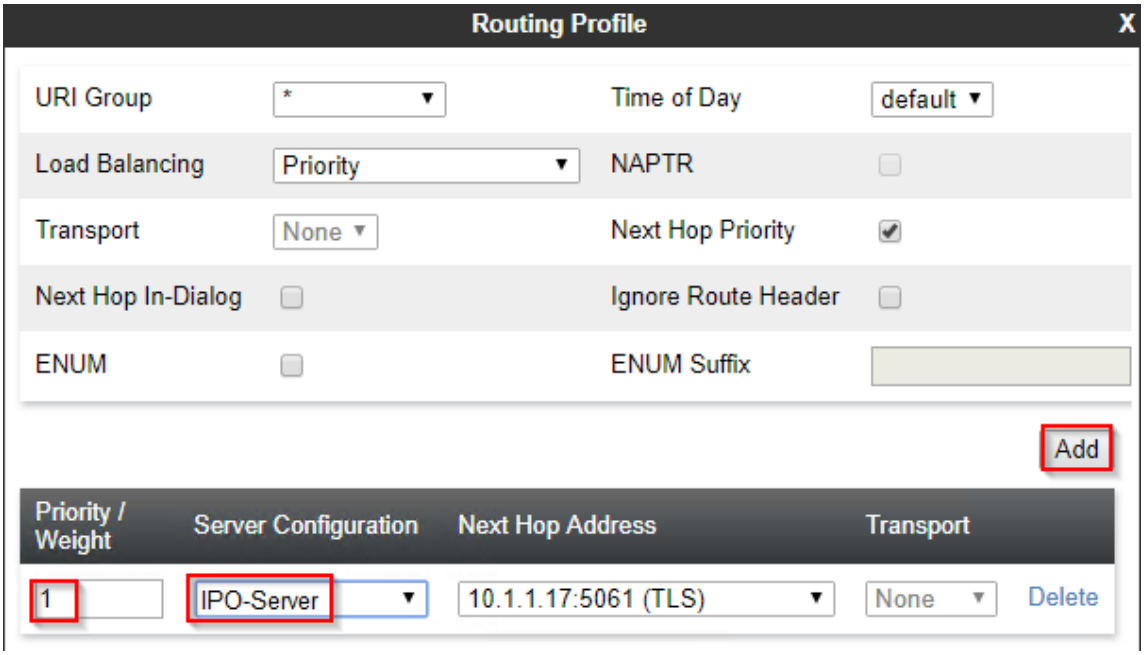
Procedura

1. Selezionare **Profili globali** > **Instradamento**.

2. Fare clic su **Aggiungi**.
3. Immettere un nome. È quindi possibile utilizzare questa opzione per selezionare il criterio in altri menu.



4. Fare clic su **Avanti**.



5. Fare clic su **Aggiungi**.
6. Impostare **Priorità** su 1.
7. Impostare **Configurazione del server** sul profilo server creato per IP Office.
8. In **Indirizzo hop successivo**, selezionare l'indirizzo IP di IP Office.
9. Fare clic su **Fine**.

Passi successivi

- Accedere a Creazione di un criterio di topologia nascosta ASBCE alla pagina 43.

Collegamenti correlati

Configurazione ASBCE per interni SIP remoti alla pagina 24

Creazione di un criterio di topologia nascosta ASBCE

ASBCE può utilizzare l'impostazione di topologia nascosta per rimuovere o sostituire i valori nei messaggi SIP. Ad esempio, sostituire un indirizzo IP in un'intestazione SIP con un nome di dominio completo richiesto.

- **Supporto IPv4/IPv6 doppio:** è possibile utilizzare la stessa voce per gli interni remoti IPv4 e IPv6.

Prerequisiti

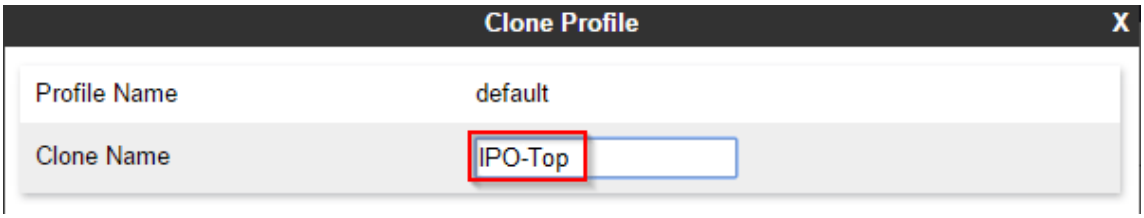
- Creazione di un profilo di instradamento del server alla pagina 41.

Procedura

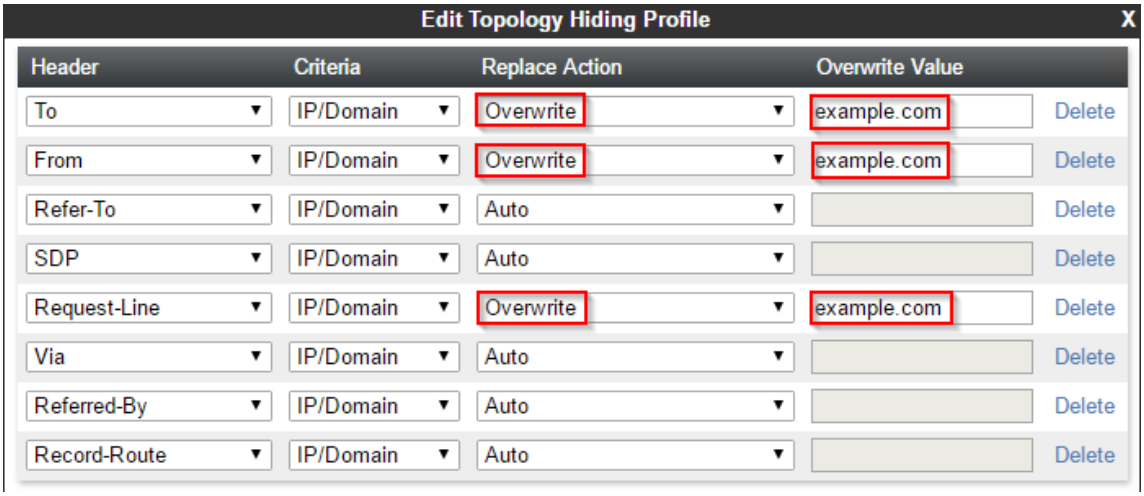
1. Selezionare **Profili globali** > **Nascondi topologia**.
2. Selezionare il profilo predefinito e fare clic su **Clona**.

   Importante:

   - È necessario utilizzare **Clona** e il profilo o il criterio indicato. L'utilizzo di **Aggiungi** creerà un nuovo profilo o criterio con diverse impostazioni predefinite.
3. Immettere un nome. È quindi possibile utilizzare questa opzione per selezionare il criterio in altri menu.



4. Fare clic su **Fine**.
5. Selezionare il nuovo profilo e fare clic su **Modifica**.



6. Per i campi **A**, **Da**, **Riferimento a**, **SDP** e **Linea di richiesta**:
   a. Impostare **Sostituisci azione** su **Sovrascrivi**.
   b. Immettere il dominio IP Office come **Sovrascrivi valore**.

7. Fare clic su **Fine**.

Passi successivi

- Accedere a Creazione di un elenco di blocchi IP/URI alla pagina 44.

Collegamenti correlati

Configurazione ASBCE per interni SIP remoti alla pagina 24

Creazione di un elenco di blocchi IP/URI

È possibile utilizzare un elenco di blocchi per avere gli indirizzi IP e gli URI di blocco ASBCE che sono l'origine delle richieste di registrazione non riuscite. È quindi possibile aggiungere l'elenco di blocchi a qualsiasi flusso di abbonati e invertire i proxy creati.

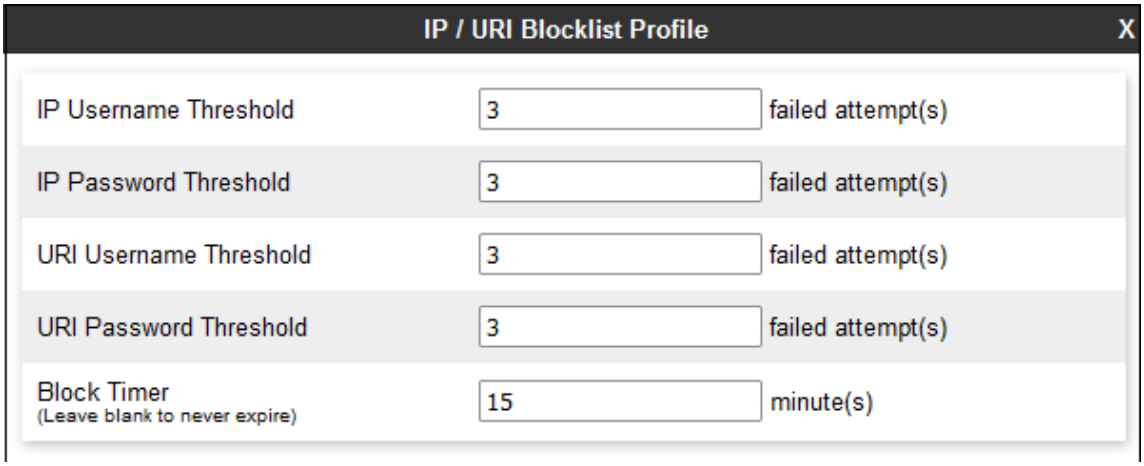
- **Supporto IPv4/IPv6 doppio:** è possibile utilizzare la stessa voce per gli interni remoti IPv4 e IPv6.

Prerequisiti

- Creazione di un criterio di topologia nascosta ASBCE alla pagina 43.

Procedura

1. Selezionare **Criteri di dominio** > **Profilo elenco di blocchi IP/URI**.
2. Fare clic su **Aggiungi**.



3. Immettere un nome. È quindi possibile utilizzare questa opzione per selezionare il criterio in altri menu.
4. Impostare il numero di tentativi di nome e password non riusciti consentiti.
5. Impostare la durata del blocco di un indirizzo IP o URI dopo aver superato uno qualsiasi dei limiti impostati.
6. Fare clic su **Fine**.

Passi successivi

- Passare al Creazione di una regola dell'applicazione alla pagina 45.

Collegamenti correlati

Configurazione ASBCE per interni SIP remoti alla pagina 24

Creazione di una regola dell'applicazione

È possibile utilizzare una regola dell'applicazione per limitare il tipo di connessioni multimediali consentite da ASBCE. Può anche impostare il numero massimo di tali connessioni e il numero massimo di connessioni per interno remoto.

- **Supporto IPv4/IPv6 doppio:** è possibile utilizzare la stessa voce per gli interni remoti IPv4 e IPv6.

Prerequisiti

- Creazione di un elenco di blocchi IP/URI alla pagina 44.

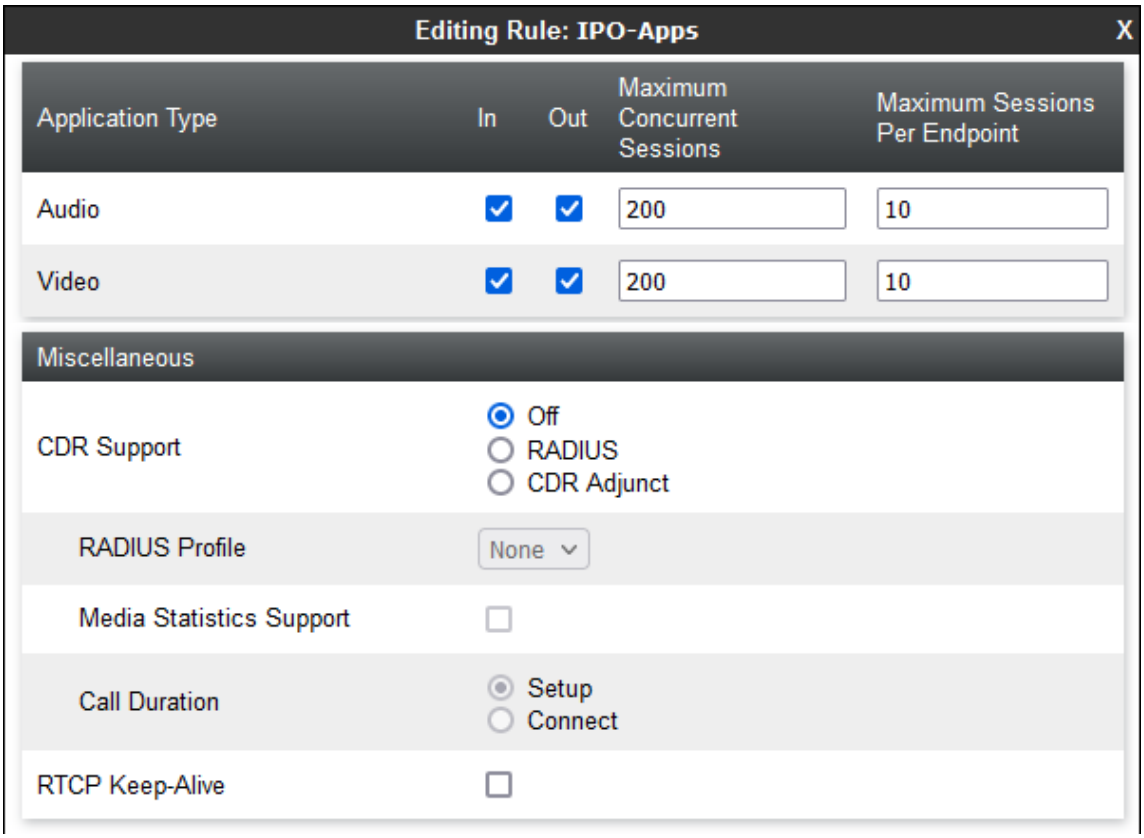
Procedura

1. Selezionare **Criteri di dominio** > **Regole applicazione**.
2. Selezionare il criterio *default-low* e fare clic su **Clona**.

   Importante:

   - È necessario utilizzare **Clona** e il profilo o il criterio indicato. L'utilizzo di **Aggiungi** creerà un nuovo profilo o criterio con diverse impostazioni predefinite.
3. Immettere un nome. È quindi possibile utilizzare questa opzione per selezionare il criterio in altri menu.
4. Fare clic su **Fine**.
5. Selezionare il nuovo criterio e fare clic su **Modifica**.

6. Selezionare se consentire **Audio** e/o **Video**.



7. Per ciascuna delle opzioni precedenti, impostare **Numero massimo di sessioni simultanee** e **Numero massimo di sessioni per endpoint**.
8. Fare clic su **Fine**.

Passi successivi

- Passare al Creazione di una regola multimediale alla pagina 46.

Collegamenti correlati

Configurazione ASBCE per interni SIP remoti alla pagina 24

Creazione di una regola multimediale

È possibile utilizzare una regola multimediale per definire varie impostazioni multimediali.

- **Supporto IPv4/IPv6 doppio:** è possibile utilizzare la stessa voce per gli interni remoti IPv4 e IPv6.

Prerequisiti

- Creazione di una regola dell'applicazione alla pagina 45.

Procedura

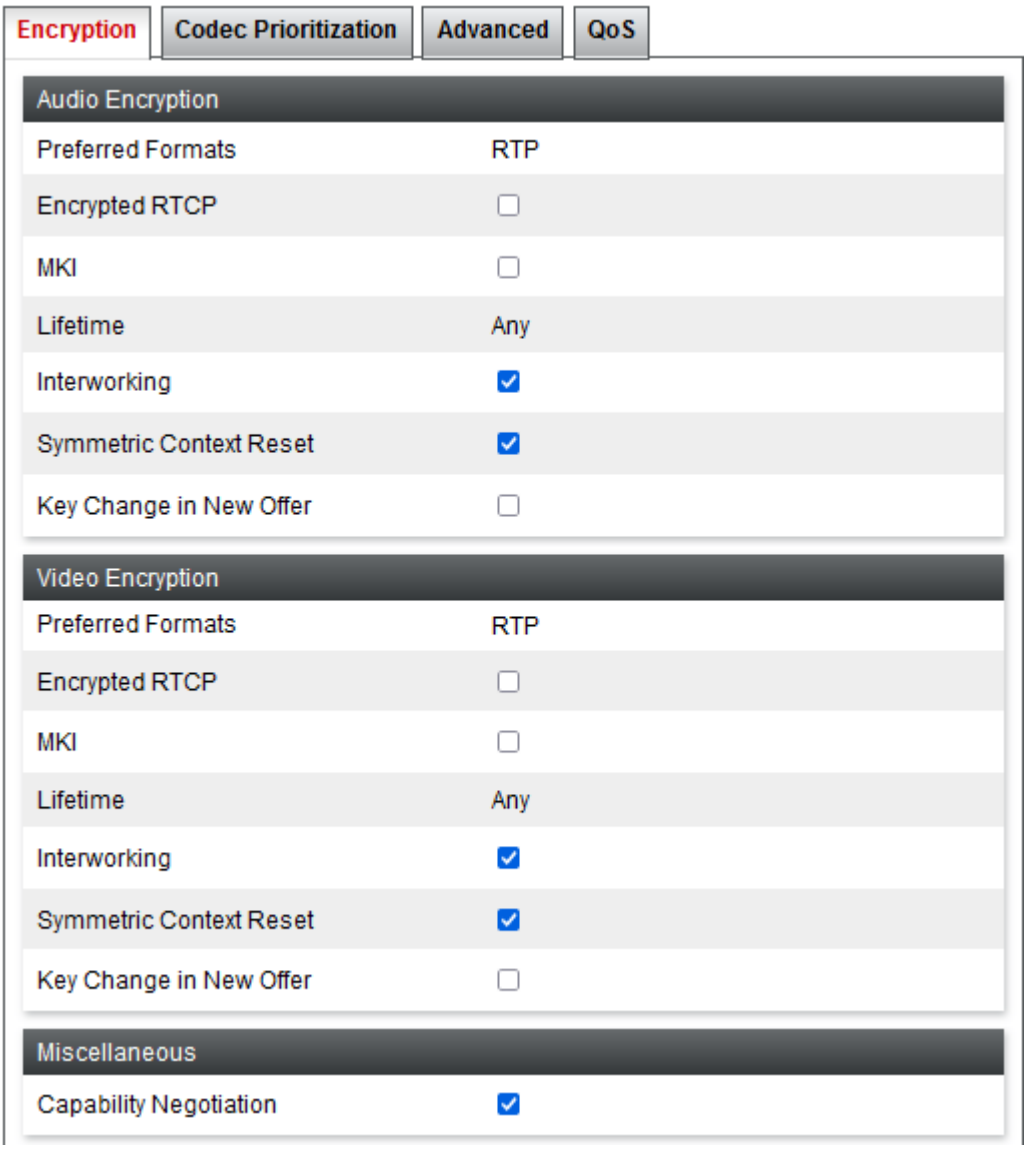
1. Selezionare **Criteri di dominio** > **Regole multimediali**.

2. Selezionare il criterio *avaya-low-med-enc* e fare clic su **Clona**.

   Importante:

   - È necessario utilizzare **Clona** e il profilo o il criterio indicato. L'utilizzo di **Aggiungi** creerà un nuovo profilo o criterio con diverse impostazioni predefinite.

3. Immettere un nome. È quindi possibile utilizzare questa opzione per selezionare il criterio in altri menu.
4. Fare clic su **Fine**.
5. Selezionare il nuovo criterio e fare clic su **Modifica**.
6. Per le opzioni **Crittografia audio** e **Crittografia video**, impostare **Formati preferiti** su *RTP*.



   - Se si utilizza SRTP, impostare i valori **Formati preferiti** e **RTCP crittografato** in modo che corrispondano alle impostazioni di **Sicurezza VoIP** impostate in IP Office.

7. Verificare che l'impostazione **Opzioni avanzate** > **ANAT abilitato** non sia selezionata.

8. Fare clic su **Fine**.

Passi successivi

- Passare al Creazione di un gruppo di criteri endpoint alla pagina 48.

Collegamenti correlati

Configurazione ASBCE per interni SIP remoti alla pagina 24

Creazione di un gruppo di criteri endpoint

Un criterio endpoint raggruppa regole come le regole dei media e delle applicazioni. Dopo aver creato un criterio endpoint, è possibile associarlo ai flussi dell'abbonato e del server creati.

- **Supporto IPv4/IPv6 doppio:** è possibile utilizzare la stessa voce per gli interni remoti IPv4 e IPv6.

Prerequisiti

- Creazione di una regola multimediale alla pagina 46.

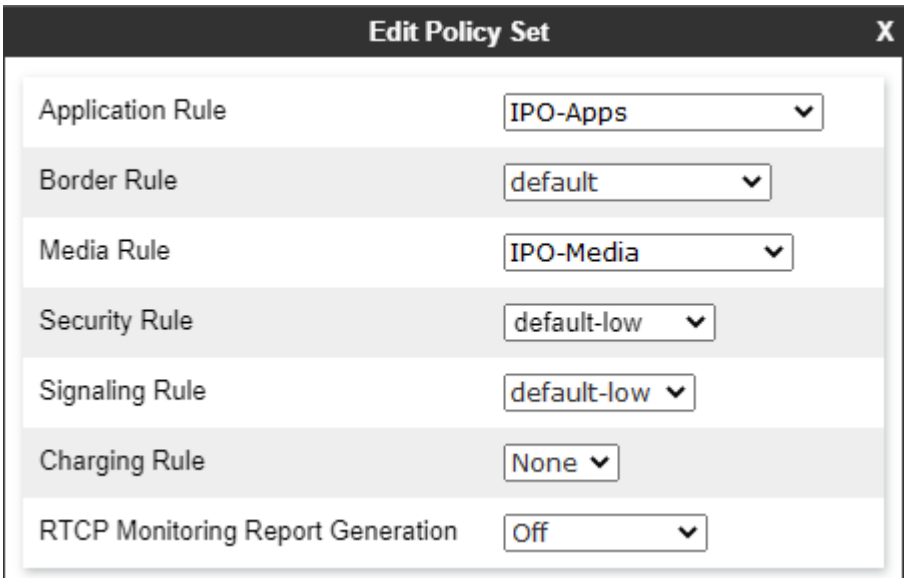
Procedura

1. Selezionare **Criteri di dominio** > **Gruppi di criteri endpoint**.
2. Selezionare il criterio *default-low* e fare clic su **Clona**.

   Importante:

   - È necessario utilizzare **Clona** e il profilo o il criterio indicato. L'utilizzo di **Aggiungi** creerà un nuovo profilo o criterio con diverse impostazioni predefinite.
3. Immettere un nome. È quindi possibile utilizzare questa opzione per selezionare il criterio in altri menu.
4. Fare clic su **Fine**.
5. Selezionare il nuovo criterio e fare clic su **Modifica**.

6. In **Regola applicazione**, selezionare le regole dell'applicazione e dei media create per gli interni remoti.



7. In **Regola multimediale**, selezionare la regola dei media creata.
8. Fare clic su **Fine**.

Passi successivi

- Passare al Configurazione di un profilo agente utente alla pagina 49.

Collegamenti correlati

Configurazione ASBCE per interni SIP remoti alla pagina 24

Configurazione di un profilo agente utente

È possibile utilizzare **Agenti utente** per limitare la connessione di ASBCE ai client e ai telefoni che inviano una stringa corrispondente *User Agent* (*UA*). In caso contrario, qualsiasi telefono o client può connettersi.

- **Supporto IPv4/IPv6 doppio:** è possibile utilizzare la stessa voce per gli interni remoti IPv4 e IPv6.

Di seguito sono riportate stringhe *UA* di esempio inviate dai client Avaya.

Telefono o client Avaya	Agente utente
Telefoni Avaya serie 9600	*Avaya one-X Deskphone*
Avaya J159	*Avaya J159 IP Phone 4.0.10.3.2*
Avaya Workplace Client - Android	*Avaya Communicator Android/3.35.2 (FA-RELEASE80-BUILD.18; Pixel 8 Pro)*

La tabella continua…

Telefono o client Avaya	Agente utente
Avaya Workplace Client - Windows	*Avaya Communicator/3.0 (3.33.0.96.6; Avaya SDK; Microsoft Windows NT 10.0.19045.0)*

- Come mostrato negli esempi precedenti, la stringa *UA* può variare a seconda della versione del software e/o della piattaforma.
- È possibile visualizzare *UA* inviato da un determinato telefono o softphone in SysMonitor dopo aver registrato il telefono o il client.

La corrispondenza UA utilizza una corrispondenza della stringa a un'espressione regolare (regex). Di seguito sono riportati esempi di stringhe regex:

Espressione regolare	Descrizione
`Avaya.*`	Corrisponde a qualsiasi *UA* che inizia con *Avaya*. *.* corrisponde a qualsiasi carattere. *.** corrisponde a un numero qualsiasi di caratteri.
`Avaya J1.*`	Corrisponde alla stringa *UA* di qualsiasi telefono serie J100.
`Avaya (J1|Communicator).*`	Corrisponde alla stringa *UA* dei telefoni serie J100 e Avaya Workplace Client. Le parentesi *( )* racchiudono le potenziali corrispondenze, ciascuna delle quali è separata da un carattere |.
`Avaya Communicator\/3\.0 \(3\.33.*`	Corrisponde alla stringa *UA* solo della versione Windows 3.33 di Avaya Workplace Client. L'espressione regex utilizza \ come prefisso dei caratteri che altrimenti verrebbero trattati come comandi regex. Ad esempio *.* corrisponde a qualsiasi carattere mentre *\.* corrisponde solo a un carattere letterale *.*.

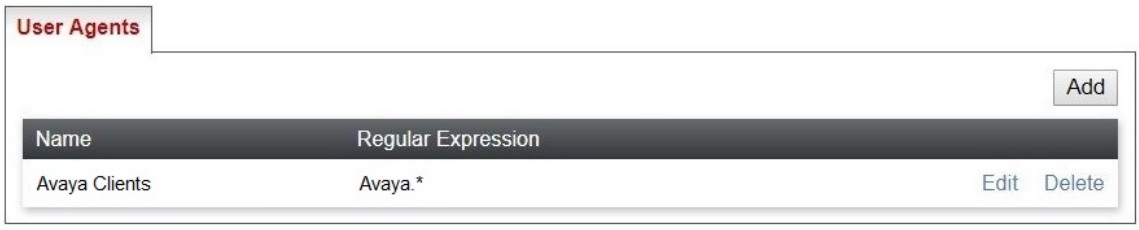
Per ulteriori informazioni sulla creazione di stringhe regex, vedere https://learn.microsoft.com/en-us/dotnet/standard/base-types/regular-expression-language-quick-reference e https://regex101.com.

Prerequisiti

- Creazione di un criterio di topologia nascosta ASBCE alla pagina 43.

Procedura

1. Selezionare **Gestione del sistema** > **Parametri globali** > **Agenti utente**.
2. Fare clic su **Aggiungi**.



3. Immettere un nome. È quindi possibile utilizzare questa opzione per selezionare il criterio in altri menu.
4. Immettere l'espressione regolare per la stringa o le stringhe dell'agente utente che si desidera abbinare.
5. Fare clic su **Fine**.

Passi successivi

- Accedere a Creazione del flusso degli abbonati alla pagina 51.

Collegamenti correlati

Configurazione ASBCE per interni SIP remoti alla pagina 24

Creazione del flusso degli abbonati

ASBCE utilizza un flusso di abbonati per gestire le connessioni in entrata dagli interni remoti.

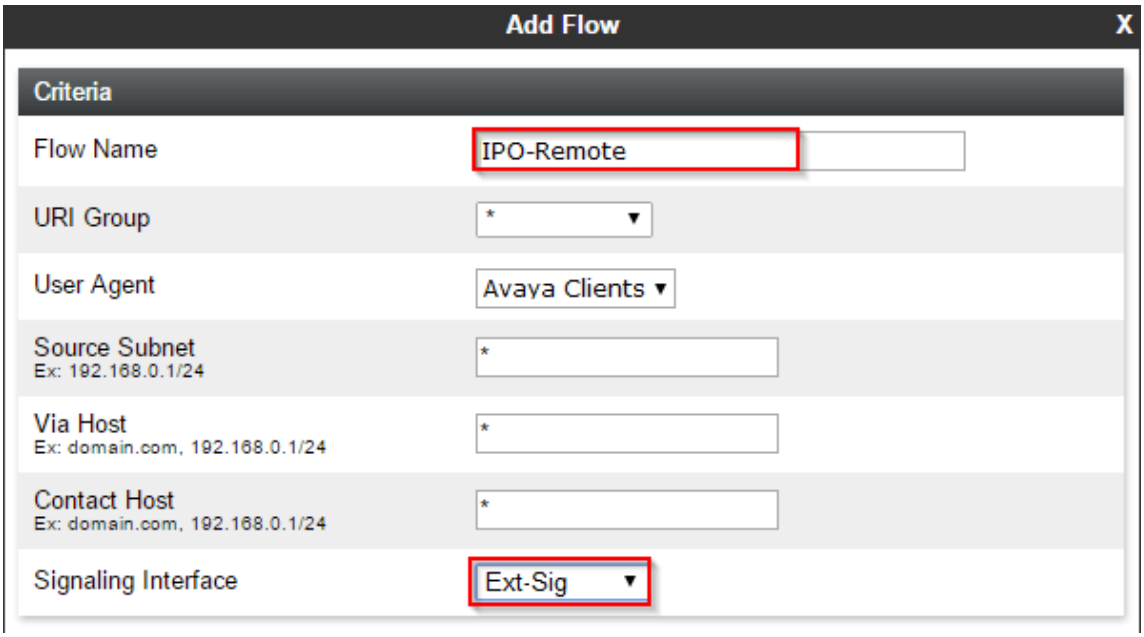
- **Supporto IPv4/IPv6 doppio:** per supportare gli interni remoti IPv4 e IPv6, è necessario creare voci separate per IPv4 e IPv6:
  - Le interfacce **Interfaccia di segnalazione** e **Interfaccia multimediale** per ognuno devono utilizzare le rispettive interfacce IPv4 o IPv6 esterne.

Prerequisiti

- Configurazione di un profilo agente utente alla pagina 49.

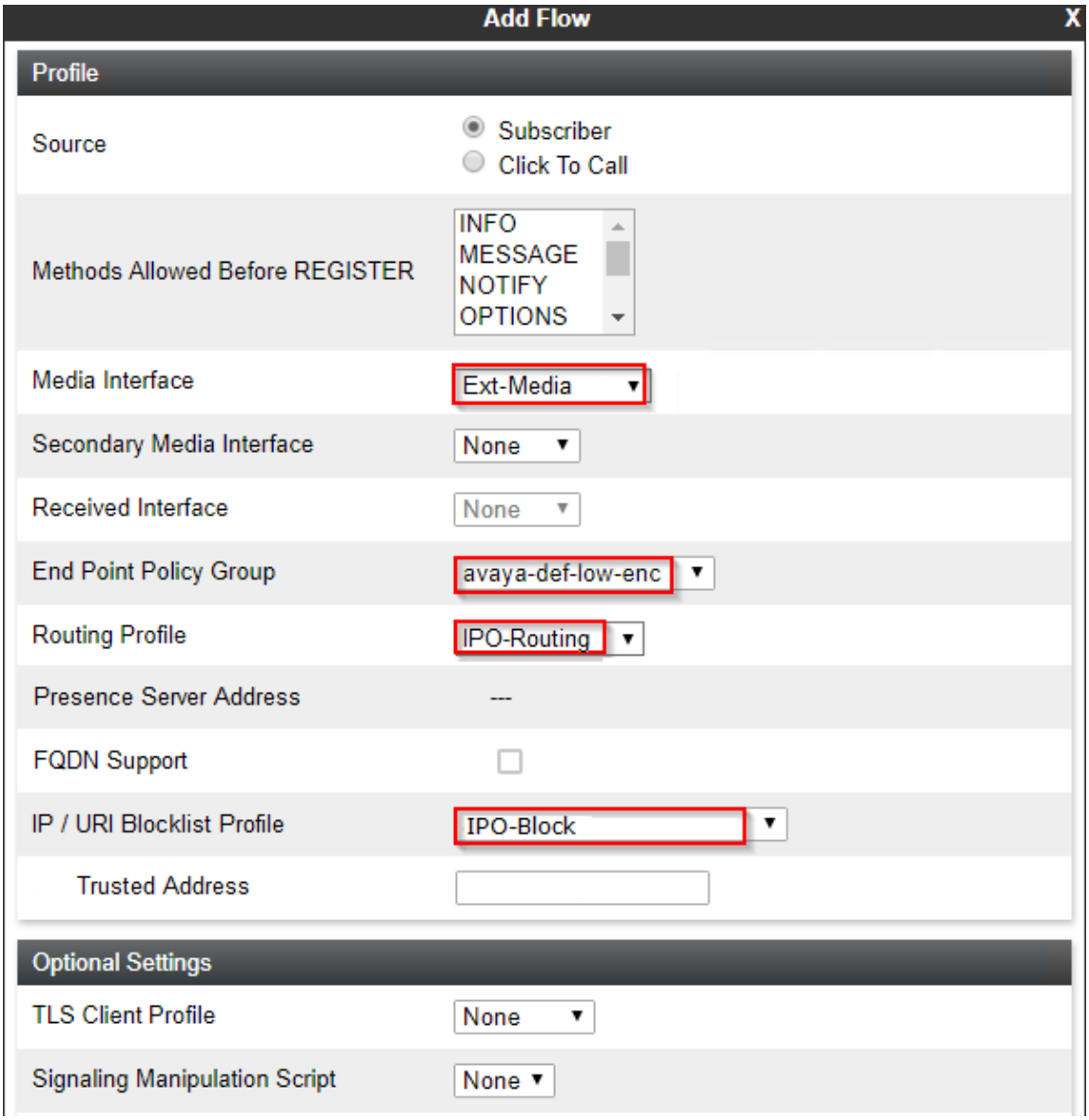
Procedura

1. Selezionare **Impostazioni specifiche del dispositivo** > **Flussi endpoint**.
2. Selezionare la scheda **Flussi dell'abbonato** e fare clic su **Aggiungi**.



   a. Immettere un nome. È quindi possibile utilizzare questa opzione per selezionare il criterio in altri menu.
   b. Se necessario, selezionare il profilo **Agente utente** creato in modo che corrisponda all'UA dei client a cui è consentito utilizzare il flusso degli abbonati.
   c. Selezionare l'esterno **Interfaccia di segnalazione** creato per gli interni remoti.

3. Fare clic su **Avanti**.



   a. In **Interfaccia multimediale**, selezionare l'interfaccia multimediale esterna creata per gli interni remoti.
   b. In **Gruppo di criteri endpoint**, selezionare *avaya-def-low-enc*.
   c. In **Profilo di instradamento**, selezionare il profilo di instradamento del server creato per IP Office.
   d. Se è stato creato un profilo elenco blocchi, selezionarlo utilizzando l'elenco a discesa **Profilo elenco di blocchi IP/URI**.

4. Fare clic su **Fine**.
5. Se sono supportati sia gli interni remoti IPv4 che IPv6, ripetere la procedura per creare le voci IPv6.

Passi successivi

- Accedere a Creazione di un flusso server alla pagina 53.

Collegamenti correlati

Configurazione ASBCE per interni SIP remoti alla pagina 24

Creazione di un flusso server

ASBCE utilizza un flusso server per gestire le connessioni in entrata dal server IP Office.

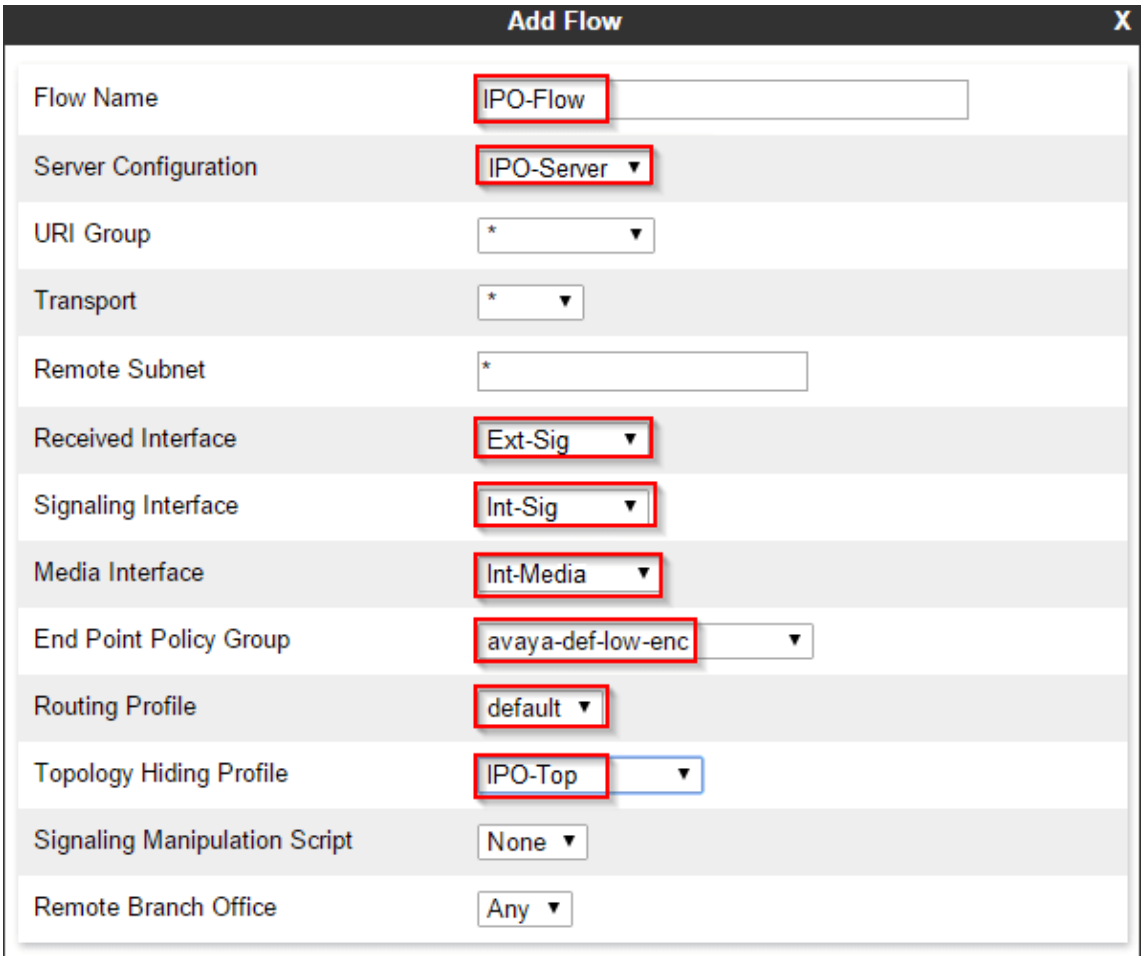
- **Supporto IPv4/IPv6 doppio:** per supportare gli interni remoti IPv4 e IPv6, è necessario creare voci separate per IPv4 e IPv6:
  - **Interfaccia ricevuta** per ogni flusso di server deve utilizzare la rispettiva interfaccia di segnalazione esterna IPv4 o IPv6.

Prerequisiti

- Creazione del flusso degli abbonati alla pagina 51.

Procedura

1. Selezionare **Impostazioni specifiche del dispositivo** > **Flussi endpoint**.
2. Selezionare la scheda **Flussi del server** e fare clic su **Aggiungi**.



a. In **Nome del flusso**, immettere un nome descrittivo.

b. In **Configurazione del server**, selezionare il profilo del server creato per il server IP Office.
c. In **Interfaccia ricevuta**, selezionare l'interfaccia di segnalazione esterna creata per gli interni remoti.
d. In **Interfaccia di segnalazione**, selezionare l'interfaccia di segnalazione interna creata per gli interni remoti.
e. In **Interfaccia multimediale**, selezionare l'interfaccia multimediale interna creata per gli interni remoti.
f. In **Gruppo di criteri endpoint**, selezionare *avaya-def-low-enc*.
g. In **Profilo di instradamento**, selezionare *default*.
h. In **Profilo nascondi topologia**, selezionare il profilo nascosto della topologia creato per gli interni remoti IP Office.

3. Fare clic su **Fine**.
4. Se sono supportati sia gli interni remoti IPv4 che IPv6, ripetere la procedura per creare le voci IPv6.

Passi successivi

- Accedere a Aggiunta di proxy inversi per le richieste di file alla pagina 54.

Collegamenti correlati

Configurazione ASBCE per interni SIP remoti alla pagina 24

Aggiunta di proxy inversi per le richieste di file

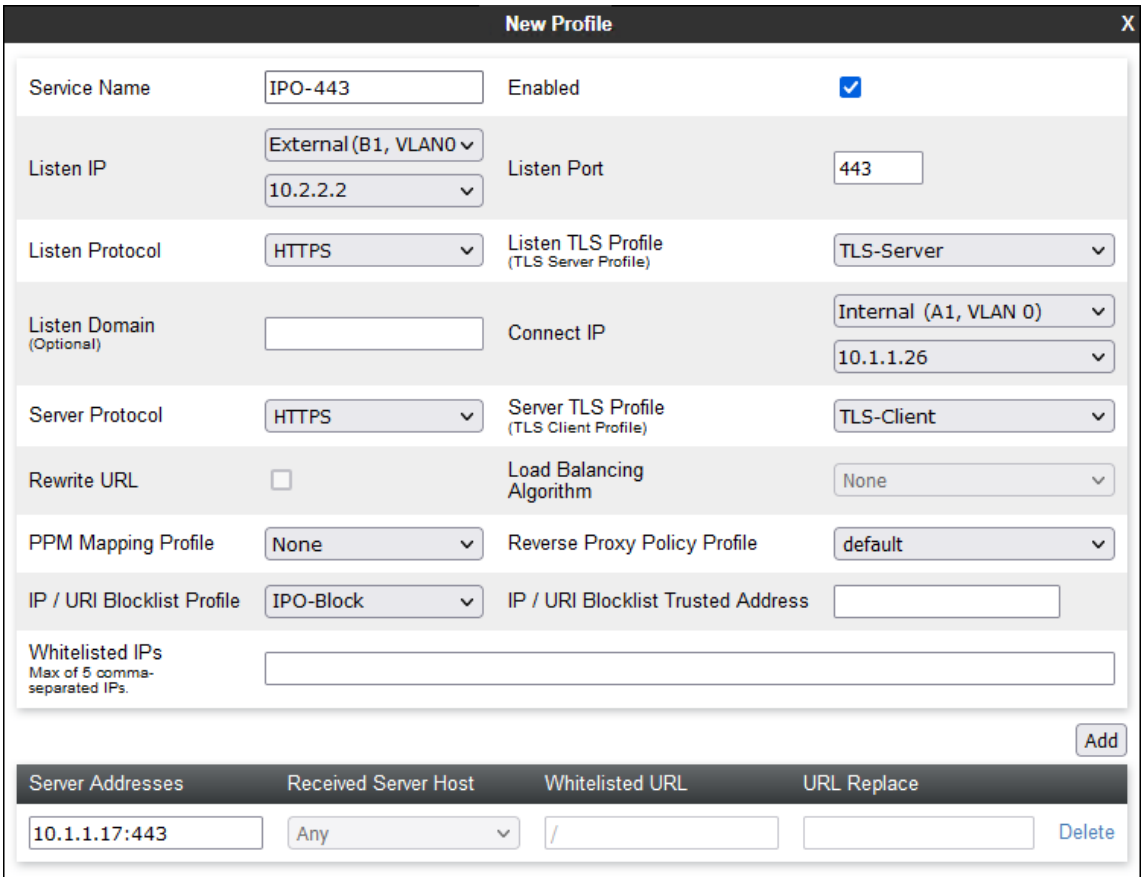
Di seguito è riportato un esempio di creazione di proxy inversi per gli interni remoti. Ciò consente agli interni remoti di richiedere file da IP Office. Ad esempio, richiedere file `46xxsettings.txt` e `46xxspecials.txt`.

Le porte e il protocollo richiesti dipendono dai requisiti del tipo di interno remoto.

- Per impostazione predefinita, per la connessione iniziale a IP Office per richiedere il file `46xxsettings.txt`, gli interni utilizzano `http` o `https`. IP Office utilizza rispettivamente la porta `80` e la porta `443`.
- Le impostazioni di `46xxsettings.txt` indicano all'interno remoto quali porte e protocolli utilizzare per le connessioni future.
- Se **Sistema** > **Sistema** > **Usa porte telefono preferito** è abilitato, `46xxsettings.txt` indica ai telefoni e ai client di utilizzare la porta `8411` per HTTP e la porta `411` per le richieste di file HTTPS e tali porte sono abilitate su IP Office.
  - Se l'opzione **Usa porte telefono preferito** è attivata, IP Office consente comunque le connessioni sulla porta `80` e sulla porta `443`. IP Office richiede ciò per la connessione iniziale e per i client legacy.
- **Supporto IPv4/IPv6 doppio:** per supportare gli interni remoti IPv4 e IPv6, è necessario creare voci separate per IPv4 e IPv6. Ciascuna di esse utilizza le rispettive interfacce esterne IPv4 e IPv6.

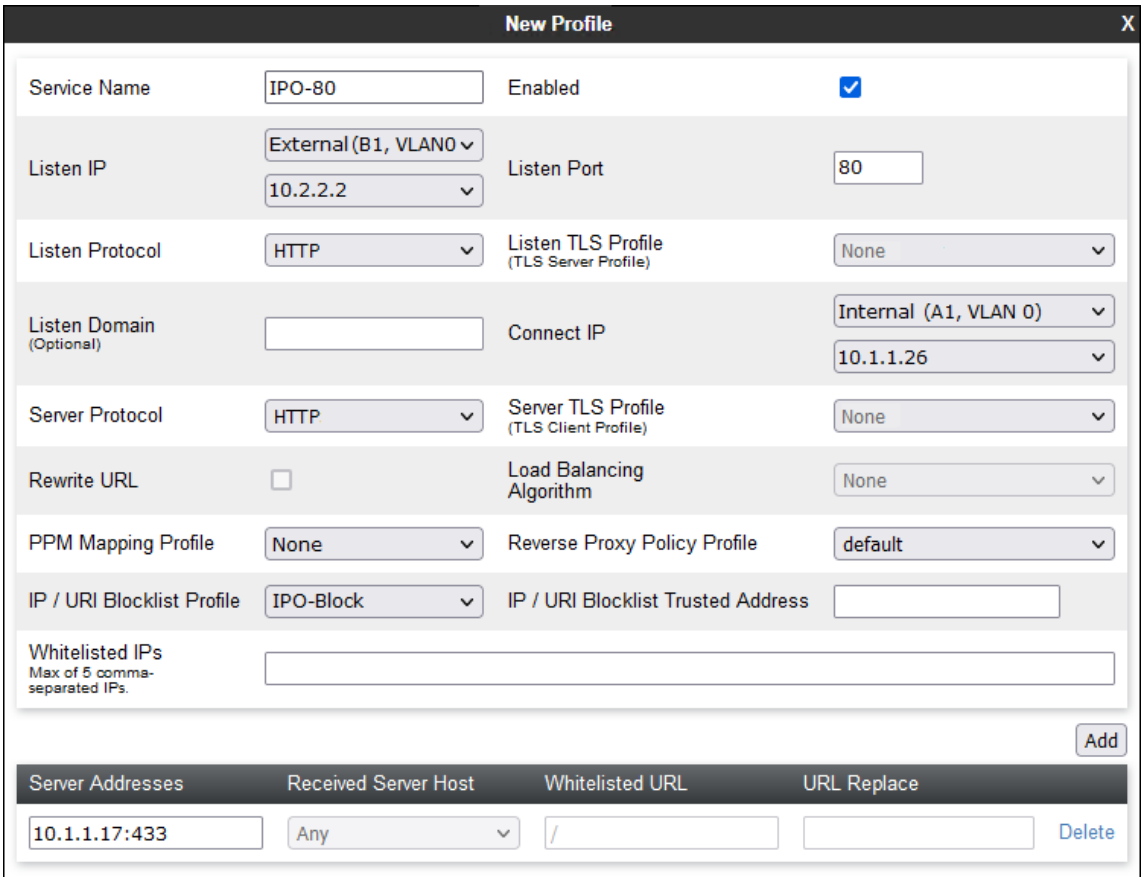
Procedura

1. Selezionare **Impostazioni specifiche del dispositivo** > **Servizi DMZ** > **Servizi relè**.
2. Selezionare la scheda **Proxy inverso** e fare clic su **Aggiungi**.



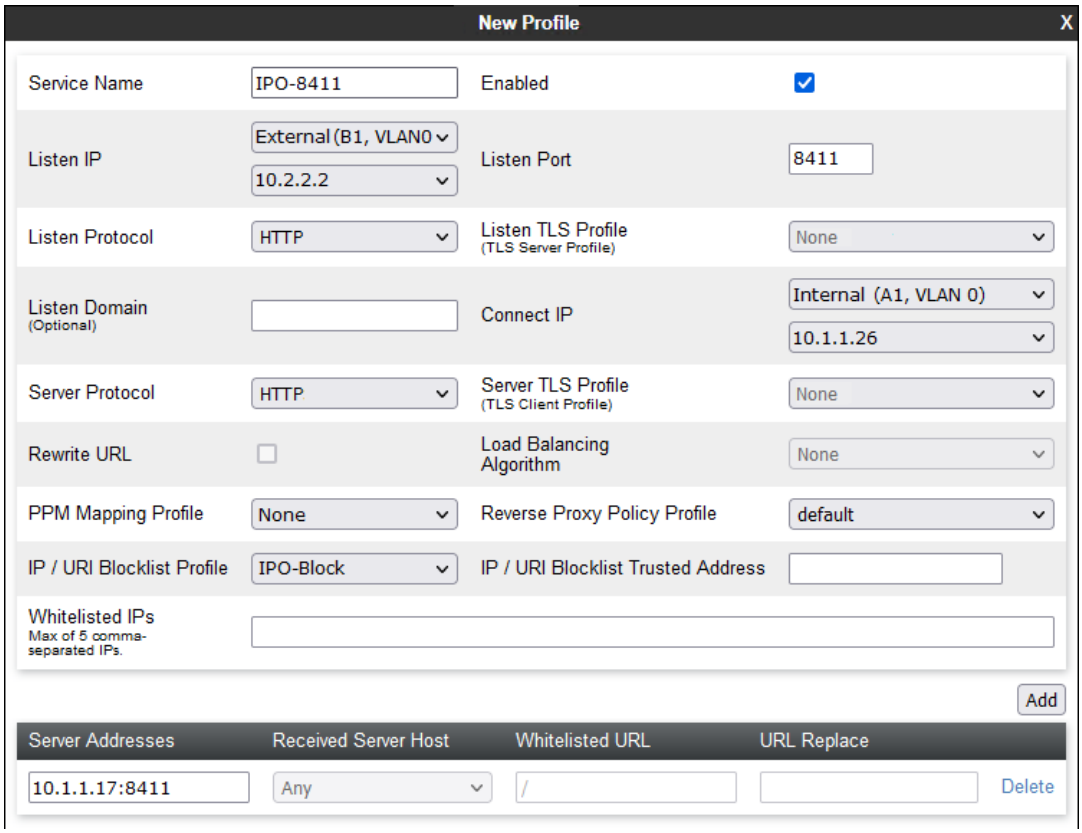
   a. In **Nome servizio** immettere un nome descrittivo per il proxy inverso.
   b. In **IP ascolto**, selezionare l'interfaccia esterna *B1* e l'indirizzo IP.
   c. Impostare **Porta di ascolto** su `443`.
   d. Impostare **Protocollo ascolto** su **HTTPS**.
   e. In **Profilo TLS ascolto**, selezionare il profilo del server TLS.
   f. In **IP di connessione**, selezionare l'interfaccia interna *A1* e l'indirizzo IP.
   g. In **Protocollo del server**, selezionare **HTTPS**.
   h. In **Profilo TLS server**, selezionare il profilo del client TLS.
   i. Se è stato creato un elenco di blocchi, selezionarlo utilizzando l'elenco a discesa **Profilo elenco di blocchi IP/URI**.
   j. Fare clic su **Aggiungi**:
   k. Per **Indirizzo del server**, immettere l'indirizzo IP di IP Office seguito da `:443`.
3. Fare clic su **Fine**.

4. Ripetere la procedura per aggiungere un proxy per le richieste di file HTTP `80` della porta. Questo proxy non utilizza profili TLS.

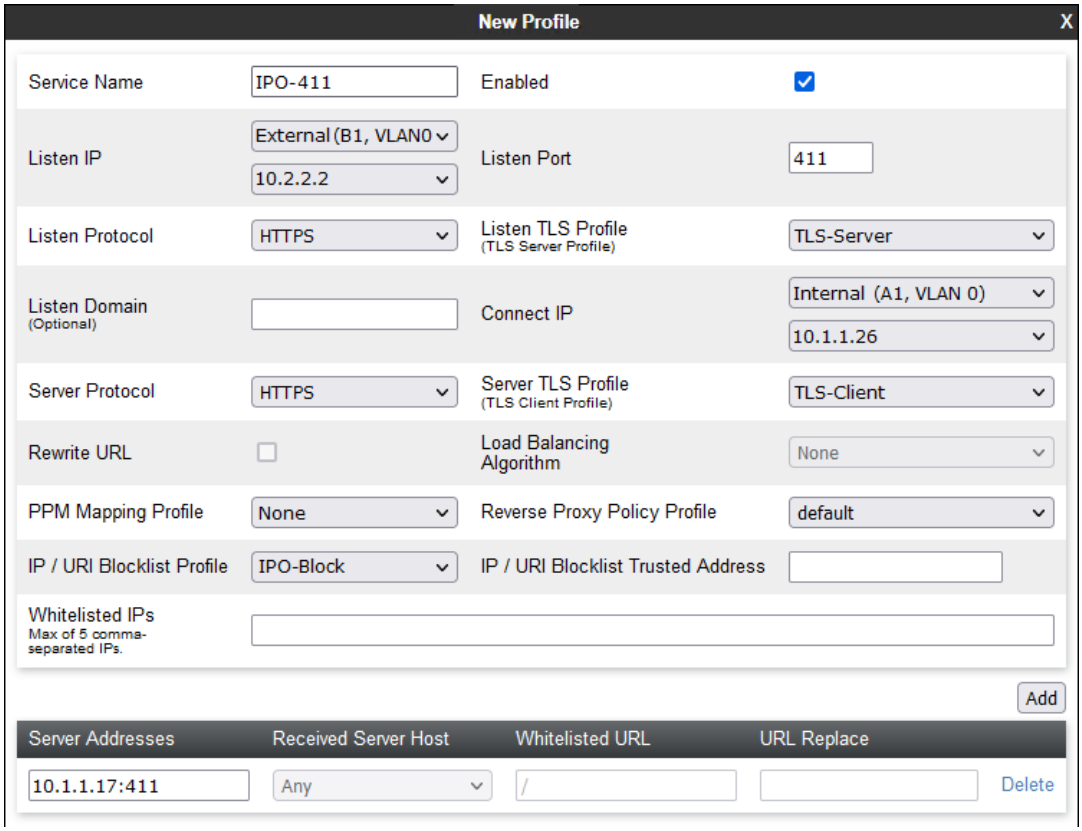


5. Fare clic su **Fine**.

6. Se **Usa porte telefono preferito** è abilitato su IP Office:
   a. Aggiungere un proxy inverso per HTTP sulla porta `8411`.



b. Aggiungere un proxy inverso per HTTPS sulla porta `411`.



7. Se sono supportati sia gli interni remoti IPv4 che IPv6, ripetere la procedura per creare le voci IPv6.

Collegamenti correlati

Configurazione ASBCE per interni SIP remoti alla pagina 24

Capitolo 5: Annullamento dell'ancoraggio dei media di chiamata dal menu ASBCE

ASBCE normalmente rimane parte di tutte le chiamate instradate. Tutti i media di chiamata e le segnalazioni di chiamata rimangono ancorati a ASBCE, pertanto richiedono larghezza di banda ed elaborazione da ASBCE.

Negli scenari in cui le reti coinvolte supportano l'instradamento diretto tra tutti gli interlocutori della chiamata, è possibile annullare l'ancoraggio dei media di chiamata da ASBCE. L'annullamento dell'ancoraggio riduce la larghezza di banda e le risorse richieste da ASBCE. ASBCE continua a gestire la segnalazione di chiamata.

- Per gli interni remoti sulla stessa sottorete remota, l'annullamento dell'ancoraggio di ASBCE abilita i media diretti tra gli interni remoti su tale sottorete.
- L'ancoraggio si può annullare anche in altri scenari. Ad esempio, tra interni remoti su due sottoreti separate. Per ulteriori informazioni, vedere https://documentation.avaya.com/bundle/GUID-416B16B1-7DB4-4C01-A966-3E62EFEA4D43/page/Media_Unanchoring_scenarios.html.

L'annullamento dell'ancoraggio utilizza i seguenti elementi di configurazione aggiuntivi ASBCE:

- **Flusso sessione**

  Un flusso di sessione definisce una coppia di intervalli di indirizzi di rete e quale criterio di sessione ASBCE deve applicare al traffico tra tali reti. Per i media diretti in un sito remoto, l'intervallo di indirizzi dei siti è impostato per entrambe le reti nel flusso della sessione.

- **Criterio di sessione**

  Un criterio di sessione imposta il modo in cui ASBCE deve trattare i media di chiamata. È possibile utilizzare lo stesso criterio di sessione per diversi flussi di sessione.

Collegamenti correlati

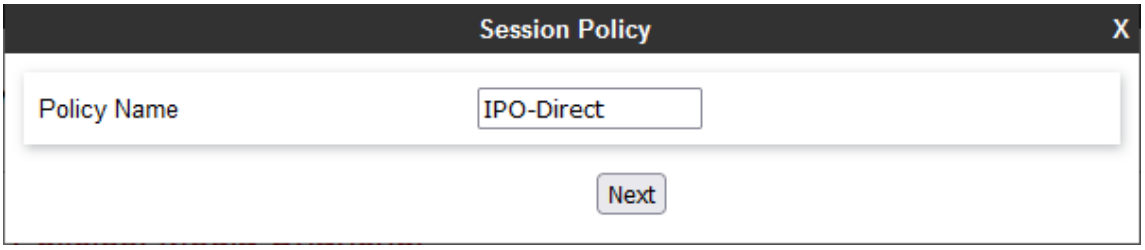
Creazione di un criterio di sessione per un sito remoto alla pagina 59
Creazione di un flusso di sessione per il sito remoto alla pagina 61

Creazione di un criterio di sessione per un sito remoto

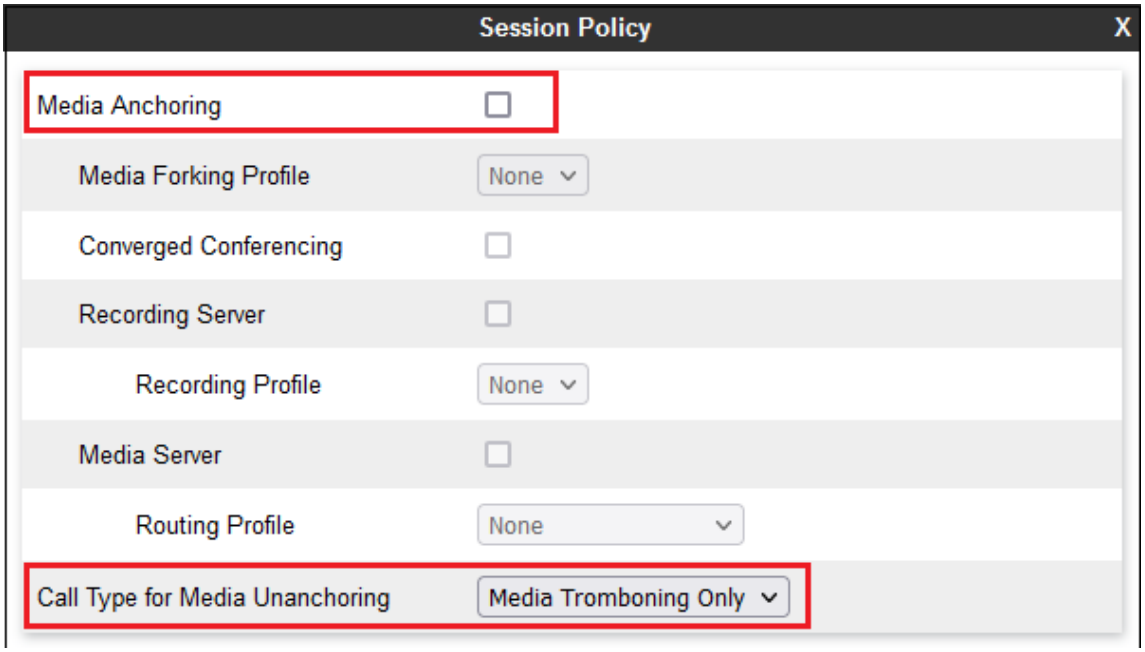
Un criterio di sessione imposta il modo in cui ASBCE deve trattare il traffico tra i siti abbinato da qualsiasi flusso di sessione che utilizza il criterio. È possibile utilizzare lo stesso criterio per più flussi di sessione. Ovvero, per più siti remoti.

Procedura

1. Selezionare **Criteri di dominio** > **Criteri di sessione**.
2. Fare clic su **Aggiungi**.
3. Immettere un nome. È quindi possibile utilizzare questa opzione per selezionare il criterio in altri menu.



4. Fare clic su **Avanti**.



5. Deselezionare **Ancoraggio multimediale**.
6. Impostare **Tipo di chiamata per l'annullamento dell'ancoraggio multimediale** su **Solo tromboning multimediale**.
7. Fare clic su **Fine**.

Passi successivi

- Accedere a Creazione di un flusso di sessione per il sito remoto alla pagina 61.

Collegamenti correlati

Annullamento dell'ancoraggio dei media di chiamata dal menu ASBCE alla pagina 59

Creazione di un flusso di sessione per il sito remoto

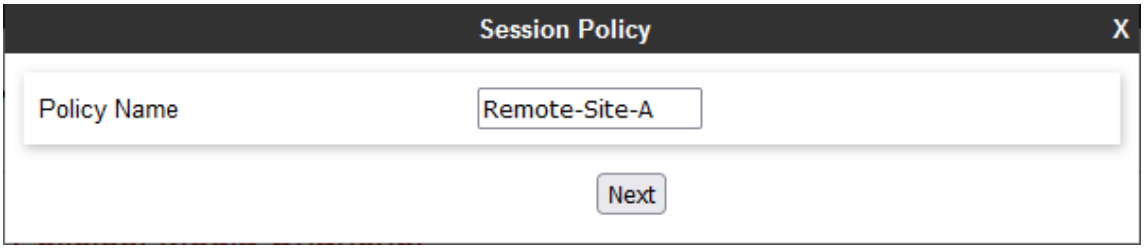
Un flusso di sessione definisce gli intervalli di indirizzi tra i quali ASBCE deve applicare un criterio di sessione. Per una sottorete remota, gli intervalli di indirizzi su entrambi i lati sono gli stessi.

Prerequisiti

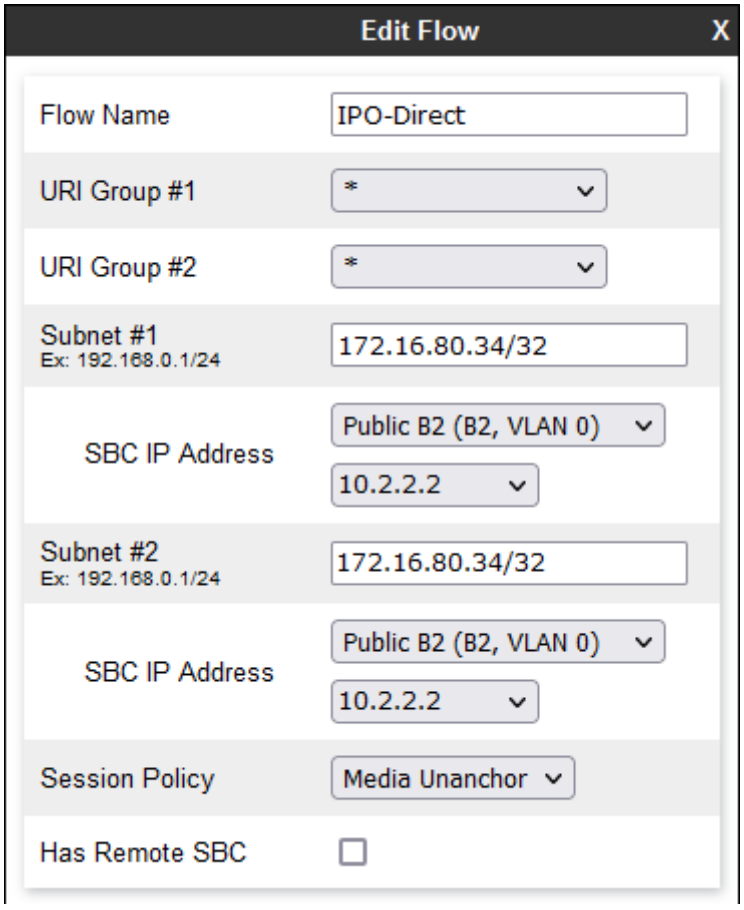
- Creazione di un criterio di sessione per un sito remoto alla pagina 59.

Procedura

1. Selezionare **Rete e flussi** > **Flussi di sessione**.
2. Fare clic su **Aggiungi**.
3. Immettere un nome. È quindi possibile utilizzare questa opzione per selezionare il criterio in altri menu.



4. Fare clic su **Avanti**.



5. Per **Sottorete n. 1** impostare l'intervallo di indirizzi IP utilizzati dagli interni remoti nel sito remoto. Impostare **Indirizzo IP SBC** sull'interfaccia esterna di ASBCE.
6. Impostare gli stessi valori per **Sottorete n. 2**.
7. Per **Criteri di sessione**, selezionare il criterio di sessione creato.
8. Fare clic su **Fine**.

Collegamenti correlati

Annullamento dell'ancoraggio dei media di chiamata dal menu ASBCE alla pagina 59

Capitolo 6: Supporto di Avaya Workplace Client come interno remoto

Questa sezione fornisce note sul funzionamento di Avaya Workplace Client quando utilizzato come interno SIP remoto per IP Office.

Collegamenti correlati

[Registrazione SIP Avaya Workplace Client](#) alla pagina 63
[Controllo delle impostazioni remote](#) alla pagina 64

Registrazione SIP Avaya Workplace Client

1. Gli utenti possono utilizzare i seguenti metodi per registrare Avaya Workplace Client all'avvio:
   - **Registrazione diretta:**

     L'utente immette l'indirizzo IP Office nel modulo `https://<IPOffice_FQDN>/46xxsettings.txt` quando `://<IPOffice_FQDN>/` è l'FQDN del registrar SIP configurato su IP Office.

     - Per gli interni remoti, il DNS pubblico risolve l'FQDN all'indirizzo IP pubblico del firewall di rete del cliente.
     - Per IPv6, l'utente deve utilizzare `https://<SBC_FQDN>/46xxsettings.txt` dove <SBC_FQDN> è l'FQDN di ASBCE.
   - **Registrazione indirizzo basata su e-mail:**

     L'utente immette il proprio indirizzo e-mail. Il client contatta Avaya Spaces, dove il profilo configurato per il dominio e-mail del cliente fornisce l'indirizzo FQDN del sistema IP Office.

     - Questo metodo di registrazione non è supportato per gli interni remoti IPV6.
   - **Accesso SSO**

     Questo metodo di accesso utilizza le stesse informazioni del profilo Avaya Spaces utilizzate per la registrazione tramite e-mail di cui sopra.

     - Questo metodo di registrazione non è supportato per gli interni remoti IPV6.

2. Dopo aver ricevuto un file `46xxsettings.txt` da IP Office, Avaya Workplace Client invia una query DNS per l'indirizzo IP dell'FQDN fornito in **SIP_CONTROLLER_LIST** nel file `46xxsettings.txt`.
   - Per gli interni remoti, i valori utilizzati nel file `46xxsettings.txt` generato automaticamente vengono impostati dalle impostazioni della **Sistema** > **LAN1** > **Topologia della rete** > **SBC** nella configurazione di IP Office.
3. Il client tenta quindi di registrarsi come interno SIP utilizzando l'indirizzo IP restituito dal server DNS. Per un interno remoto, ovvero l'indirizzo IP pubblico del cliente per il firewall di rete o ASBCE.

Collegamenti correlati

Supporto di Avaya Workplace Client come interno remoto alla pagina 63

Controllo delle impostazioni remote

Utilizzando un PC remoto, è possibile visualizzare e controllare le impostazioni fornite agli interni remoti.

Procedura

1. Utilizzare **nslookup** per verificare che DNS risolva l'FQDN per IP Office agli indirizzi IP corretti.

```
C:\ nslookup ipo.example.com
Server:  Unknown
Address: 203.0.113.30
```

2. Utilizzando un browser, richiedere il file `46xxsettings.txt` da IP Office. Ad esempio, immettere `ipo.example.com/46xxsettings.txt`.
3. Controllare l'intervallo di porte visualizzato. Avaya Workplace Client può utilizzare le porte RTP/RTCP nell'intervallo `40750 to 50750`.

```
# SIPXAUTOGENERATEDSETTINGS
IF $SIG_IN_USE SEQ H323 GOTO 96X1AUTOGENERATEDSETTINGS
SET RTP_PORT_LOW 40750
SET RTP_PORT_RANGE 10002
SET TLSSRVRID 1
```

4. Altre impostazioni mostrano i valori utilizzati da Avaya Workplace Client per connettersi ai servizi IP Office:

```
# K1EXAUTOGENERATEDSETTINGS
SET ENABLE_AVAYA_CLOUD_ACCOUNTS 1
SET SIP_CONTROLLER_LIST ipo.example.com:5061;transport=tls
SET CONFERENCE_FACTORY_URI "ConfServer@ipo.example.com"
SET PSTN_VM_NUM "VM.user@ipo.example.com"
SET SETTINGS_FILE URL "https://ipo.example.com:411/46xxsettings.txt"
SET FQDN IP MAP "ipo.example.com=10.1.1.17"
```

5. Per i contatti e i servizi di presenza, verificare se i valori `IPO_PRESENCE_ENABLED` e `IPO_CONTACTS_ENABLED` sono impostati su `1`.

```
# SETTINGSK1EX
SET SSOENABLED 0
SET EWSSSO 0
SET SIPREGPROXYPOLICY "alternate"
SET IPO_PRESENCE_ENABLED 1
SET IPO_CONTACTS_ENABLED 1
SET DND_SAC_LINK 1
SET POUND_KEY_AS_CALL_TRIGGER 0
```

Collegamenti correlati

Supporto di Avaya Workplace Client come interno remoto alla pagina 63

Capitolo 7: Controllo dello stato dell'interno remoto in ASBCE

ASBCE fornisce una serie di menu che visualizzano lo stato delle connessioni e tentano di crearle.

Collegamenti correlati

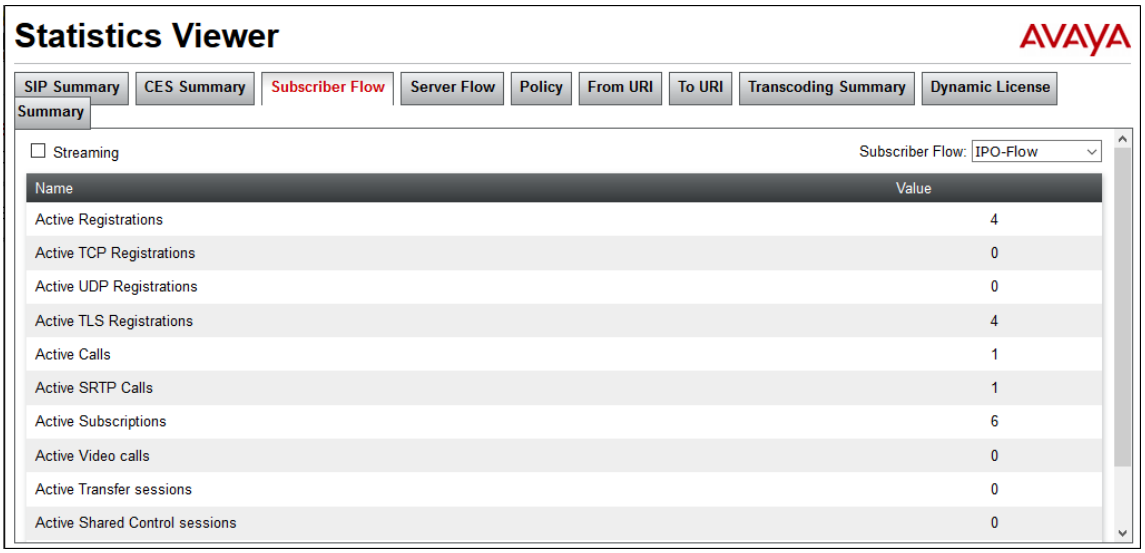
[Visualizzazione delle statistiche SIP di ASBCE](#) alla pagina 66
[Visualizzazione delle statistiche utente di ASBCE](#) alla pagina 67
[Visualizzazione degli incidenti di ASBCE](#) alla pagina 67

Visualizzazione delle statistiche SIP di ASBCE

Visualizzatore statistiche può visualizzare dettagli sul numero di connessioni e chiamate dell'interno remoto.

Procedura

1. Selezionare **Stato** > **Statistiche SIP**.
2. Selezionare **Flusso dell'abbonato** e nel menu a discesa selezionare il flusso creato per gli interni remoti.
3. Il visualizzatore visualizza dettagli quali il numero di registrazioni, il numero di chiamate e così via.



Collegamenti correlati

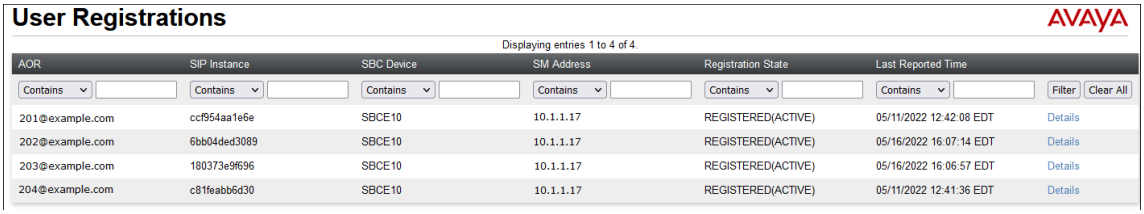
Controllo dello stato dell'interno remoto in ASBCE alla pagina 66

Visualizzazione delle statistiche utente di ASBCE

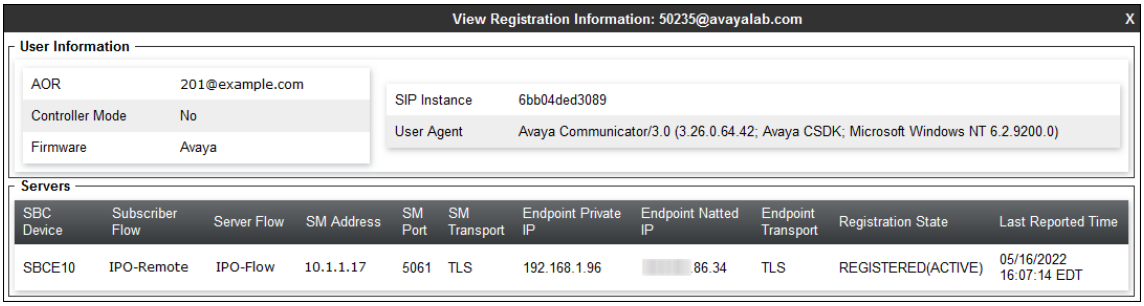
Visualizzatore statistiche può visualizzare i dettagli dei singoli interni remoti.

Procedura

1. Selezionare **Stato** > **Registrazioni utente**.
2. Il visualizzatore visualizza i dettagli dei client SIP registrati tramite ASBCE.



3. Per visualizzare informazioni aggiuntive per un determinato utente, fare clic su **Dettagli**.



Collegamenti correlati

Controllo dello stato dell'interno remoto in ASBCE alla pagina 66

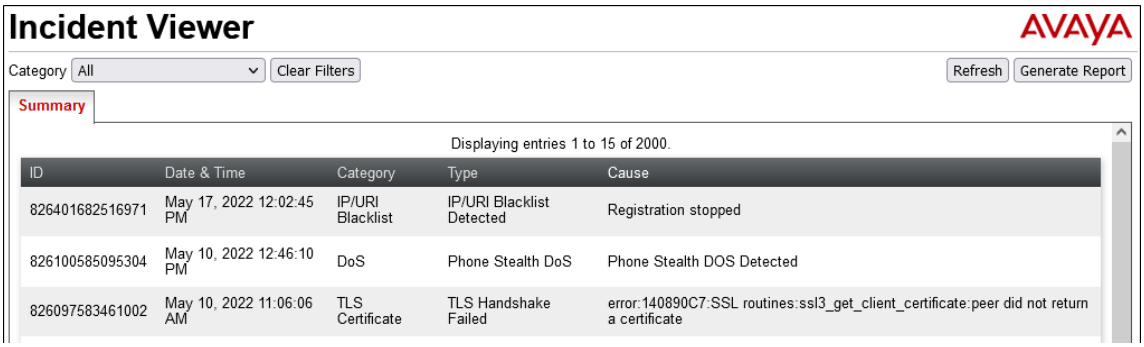
Visualizzazione degli incidenti di ASBCE

ASBCE può visualizzare i dettagli di problemi quali errori di certificazione e problemi di registrazione. Se gli interni remoti riscontrano problemi durante la connessione a IP Office, potrebbe essere visualizzato il motivo del problema su ASBCE.

Procedura

1. Selezionare **Incidenti**.

2. Il visualizzatore visualizza i dettagli degli incidenti.



Collegamenti correlati

Controllo dello stato dell'interno remoto in ASBCE alla pagina 66

Parte 2: Supporto di IPv6

Capitolo 8: Supporto degli interni remoti IPv6

Per la versione IP Office 11.1.3.1 e successive, IP Office supporta gli interni remoti Avaya Workplace Client su iOS e Android utilizzando IPv6.

Collegamenti correlati

[Supporto IPv6 interno remoto](#) alla pagina 70
[Schema interno remoto IPv6](#) alla pagina 71
[Limitazioni dell'interno remoto IPv6](#) alla pagina 71
[Configurazione DNS per supporto interno remoto IPv6](#) alla pagina 72
[Configurazione del certificato per il supporto dell'interno remoto IPv6](#) alla pagina 72
[Configurazione di Avaya Spaces per supporto interno remoto IPv6](#) alla pagina 72
[Elenco di controllo per la configurazione degli interni remoti IPv6](#) alla pagina 73
[Elenco di controllo per la configurazione degli interni remoti IPv4 e IPv6 combinati](#) alla pagina 74

Supporto IPv6 interno remoto

Per IP Office R11.1.3.1 e versioni successive, il cellulare remoto Avaya Workplace Client può utilizzare IPv6.

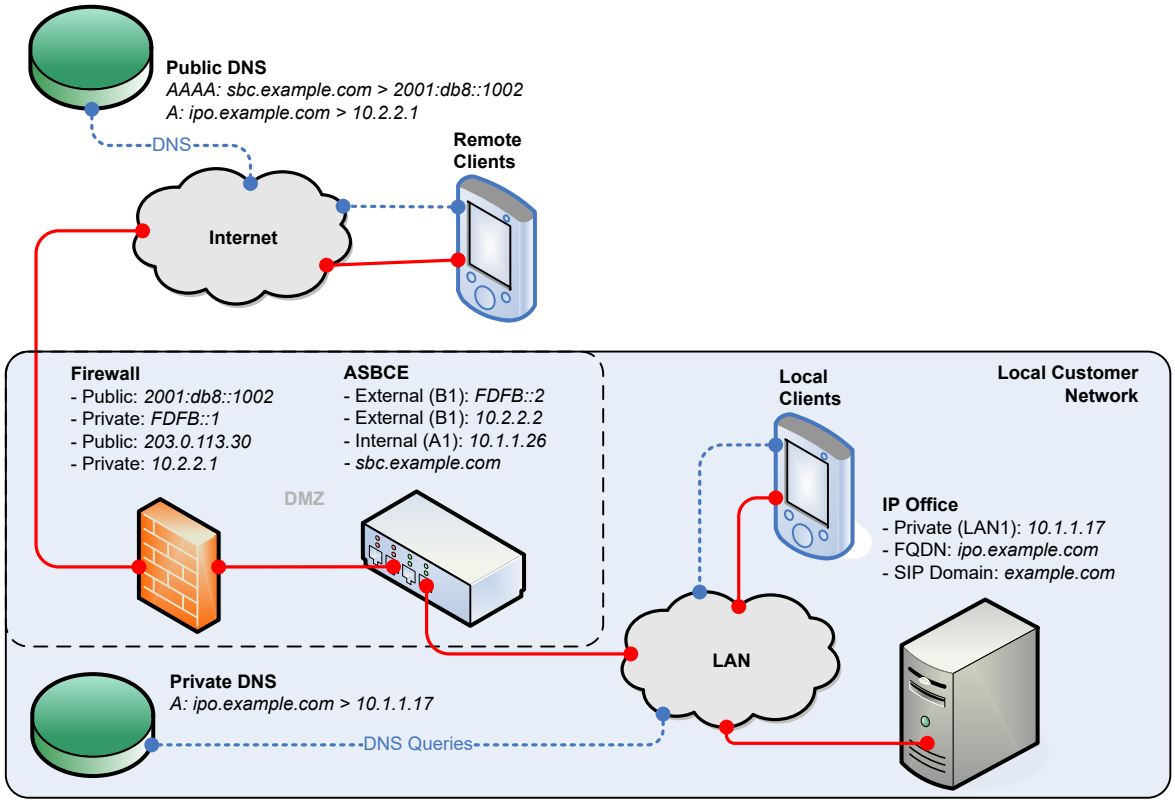
- È possibile configurare IP Office per fornire al cellulare remoto Avaya Workplace Client l'FQDN ASBCE nel file `46xxsettings.txt` generato automaticamente.
- La connessione richiede ASBCE R10.1.2 installato in un'installazione a due stack. ASBCE esegue l'instradamento tra i client IPv6 e IPv4 IP Office.
- Avaya Workplace Client:
  - iOS: Avaya Workplace Client R3.35 e successive.
  - Android: Avaya Workplace Client R3.35.1 e successive.
  - I dispositivi iPad e Vantage non sono inclusi nel supporto IPv6.
- I telefoni e i client SIP sulla rete privata del cliente utilizzano comunque IPv4 per connettersi direttamente a IP Office.
- Se la rete a cui Avaya Workplace Client è connesso supporta sia IPv4 che IPv6, l'impostazione predefinita di Avaya Workplace Client è IPv4.

Collegamenti correlati

[Supporto degli interni remoti IPv6](#) alla pagina 70

Schema interno remoto IPv6

Lo schema seguente è un esempio di supporto degli interni remoti IPv6.



- IP Office fornisce agli interni remoti l'FQDN ASBCE.
- Il DNS pubblico risolve l'FQDN ASBCE all'indirizzo IPv6 pubblico del firewall del cliente.
- Il firewall inoltra le porte utilizzate dagli interni remoti all'interfaccia esterna di ASBCE.
- Il doppio stack ASBCE gestisce l'instradamento tra gli indirizzi IPv6 e IPv4.
- Per gli interni, il DNS privato risolve l'FQDN IP Office all'indirizzo IPv4 del sistema IP Office.

Collegamenti correlati

Supporto degli interni remoti IPv6 alla pagina 70

Limitazioni dell'interno remoto IPv6

- Sebbene esista un firmware per il funzionamento IPv6 del telefono serie J100, devono utilizzare IPv4 per la connessione dell'interno remoto a IP Office.
- Avaya Spaces non supporta IPv6. Pertanto, Avaya Workplace Client che utilizza IPv6 non supporta le funzioni fornite da Avaya Spaces. Ad esempio:
  - Nessuna registrazione del client tramite e-mail o accesso SSO.
  - Nessuna messaggistica istantanea se IP Office è configurato per utilizzare Avaya Spaces come server di messaggistica.

- Se la rete a cui Avaya Workplace Client è connesso supporta sia IPv4 che IPv6, l'impostazione predefinita di Avaya Workplace Client è IPv4.

Collegamenti correlati

Supporto degli interni remoti IPv6 alla pagina 70

Configurazione DNS per supporto interno remoto IPv6

Per supportare IPv6, il DNS deve risolvere l'FQDN ASBCE oltre all'FQDN IP Office:

- Il DNS pubblico per l'FQDN IP Office deve comunque essere risolto in un indirizzo IPv4.
- Il DNS pubblico deve anche risolvere l'FQDN ASBCE in un indirizzo IPv6. A tale scopo, il cliente deve aggiungere i record `AAAA` al servizio DNS pubblico.
- Gli interni locali continuano a connettersi direttamente a IP Office utilizzando gli indirizzi IPv4. Questo problema viene risolto dal DNS privato del cliente.

Collegamenti correlati

Supporto degli interni remoti IPv6 alla pagina 70

Configurazione del certificato per il supporto dell'interno remoto IPv6

Quando si supportano gli interni remoti IPv6, oltre agli indirizzi IP Office FQDN e IPv4, il certificato di identità ASBCE deve includere gli indirizzi FQDN e IPv6 di ASBCE.

- L'FQDN di ASBCE può essere aggiunto come parte del nome comune del certificato (CN) o del nome alternativo dell'oggetto (SAN).
- L'indirizzo IPv6 deve essere aggiunto al SAN.

Collegamenti correlati

Supporto degli interni remoti IPv6 alla pagina 70

Configurazione di Avaya Spaces per supporto interno remoto IPv6

Avaya Spaces non supporta IPv6. Pertanto, Avaya Workplace Client che utilizza IPv6 non supporta le funzioni fornite da Avaya Spaces. Ad esempio:

- Nessuna registrazione del client tramite e-mail o accesso SSO.
- Nessuna messaggistica istantanea se IP Office è configurato per utilizzare Avaya Spaces come server di messaggistica.

Pagina di accesso vuota

Se non si disattiva il supporto SSO, quando si accede agli utenti del client IPv6 viene visualizzata una pagina vuota. Per accedere, è necessario chiudere la pagina vuota e quindi accedere direttamente utilizzando l'indirizzo del file IP Office `46xxsettings.txt`.

- Se si desidera che gli utenti del client IPv4 siano ancora in grado di utilizzare SSO, è necessario indicare agli utenti dell'interno remoto IPv6 di chiudere la pagina vuota e accedere utilizzando l'indirizzo del file IP Office `46xxsettings.txt`.
- In caso contrario, per evitare che la pagina vuota venga avviata all'avvio di Avaya Workplace Client, è necessario aggiungere un file `46xxspecials.txt` con l'impostazione `SET SIPSSO 0` a IP Office. Si noti che questo interesserà tutti gli utenti di Avaya Workplace Client.

```
...
SETTINGSEQNX
SET SIPSSO 0
GOTO GENERALSPECIALS
```

Collegamenti correlati

Supporto degli interni remoti IPv6 alla pagina 70

Elenco di controllo per la configurazione degli interni remoti IPv6

Se si supportano solo gli interni remoti IPv6, seguire la stessa procedura di configurazione utilizzata per IPv4, ma sostituire gli indirizzi IPv4 esterni con indirizzi IPv6, se applicabile. Consultare Configurazione ASBCE per interni SIP remoti alla pagina 24.

#	Azione	Collegamenti/Note	✔
1.	Configurare il supporto DNS pubblico per IPv6	Il DNS deve risolvere l'FQDN ASBCE all'indirizzo IPv6 per il traffico verso ASBCE. Consultare Configurazione DNS per supporto interno remoto IPv6 alla pagina 72.	
2.	Includere l'indirizzo ASBCE FQDN e IPv6 nel certificato di identità ASBCE.	Consultare Configurazione del certificato per il supporto dell'interno remoto IPv6 alla pagina 72.	
3.	Disattivare il supporto Avaya Spaces.	Consultare Configurazione di Avaya Spaces per supporto interno remoto IPv6 alla pagina 72.	
4.	Impostare l'indirizzo IPv6 pubblico per IP Office	È necessario fornire agli interni remoti l'indirizzo IPv6 da utilizzare per la registrazione SIP e le chiamate. Consultare Impostazione dei dettagli di ASBCE passati agli interni remoti da IP Office alla pagina 12.	
5.	Configurazione del flusso di chiamata ASBCE	Seguire lo stesso processo di configurazione ASBCE utilizzato per IPv4, ma utilizzando gli indirizzi IPv6, se necessario. Consultare Elenco di controllo per la configurazione di ASBCE alla pagina 27.	

Collegamenti correlati

Supporto degli interni remoti IPv6 alla pagina 70

Elenco di controllo per la configurazione degli interni remoti IPv4 e IPv6 combinati

Questo elenco di controllo presuppone che sia stata completata la configurazione di ASBCE per supportare gli interni remoti IPv4. Consultare Elenco di controllo per la configurazione di ASBCE alla pagina 27. Le note indicano dove ASBCE richiede una configurazione aggiuntiva per supportare gli interni remoti IPv4 e IPv6.

#	Azione	Collegamenti/Note	✔
1.	Configurare il supporto DNS pubblico per IPv6	Il DNS deve risolvere l'FQDN ASBCE all'indirizzo IPv6 per il traffico verso ASBCE. Consultare Configurazione DNS per supporto interno remoto IPv6 alla pagina 72.	
2.	Includere l'indirizzo ASBCE FQDN e IPv6 nel certificato di identità ASBCE.	L'identità ASBCE deve includere l'indirizzo FQDN e IPv4 IP Office più l'indirizzo FQDN e IPv6 ASBCE. Consultare Configurazione di Avaya Spaces per supporto interno remoto IPv6 alla pagina 72.	
3.	Disattivare il supporto Avaya Spaces.	Avaya Spaces non è supportato con IPv6. Consultare Configurazione di Avaya Spaces per supporto interno remoto IPv6 alla pagina 72.	
4.	Impostare l'indirizzo IPv6 pubblico per IP Office	È necessario fornire agli interni remoti l'indirizzo IPv6 da utilizzare per la registrazione SIP e le chiamate. Consultare Impostazione dei dettagli di ASBCE passati agli interni remoti da IP Office alla pagina 12.	
5.	Configurazione inoltro porta firewall	Aggiungere una nuova voce, come quella IPv4, ma utilizzando gli indirizzi IPv6, se applicabile. Consultare Configurazione firewall alla pagina 29.	
6.	Configurazione dell'interfaccia di rete esterna ASBCE	Aggiungere una nuova voce per l'interfaccia esterna, ma utilizzando gli indirizzi IPv6. Consultare Configurazione dell'interfaccia esterna ASBCE alla pagina 29.	
7.	Configurazione dell'interfaccia di rete interna ASBCE	Utilizzare la voce IPv4 esistente. Consultare Configurazione dell'interfaccia interna ASBCE alla pagina 31.	
8.	Creazione di un profilo client TLS	Utilizzare la voce IPv4 esistente. Consultare Creazione di un profilo client TLS alla pagina 32.	

La tabella continua…

#	Azione	Collegamenti/Note	✔
9.	Creazione di un profilo server TLS	Utilizzare la voce IPv4 esistente. Consultare Creazione di un profilo server TLS alla pagina 34.	
10.	Creazione di un'interfaccia multimediale SIP interna	Utilizzare la voce IPv4 esistente. Consultare Creazione di un'interfaccia multimediale interna alla pagina 35.	
11.	Creazione di un'interfaccia multimediale SIP esterna	Aggiungere una nuova voce, come quella IPv4, ma utilizzando gli indirizzi IPv6, se applicabile. Consultare Creazione di un'interfaccia multimediale esterna alla pagina 36.	
12.	Creazione di un'interfaccia di segnalazione delle chiamate SIP interna	Utilizzare la voce IPv4 esistente. Consultare Creazione di un'interfaccia di segnalazione interna alla pagina 37.	
13.	Creazione di un'interfaccia di segnalazione delle chiamate SIP esterna	Aggiungere una nuova voce, come quella IPv4, ma utilizzando gli indirizzi IPv6, se applicabile. Consultare Creazione dell'interfaccia di segnalazione esterna alla pagina 38.	
14.	Creazione di un profilo server	Utilizzare la voce IPv4 esistente. Consultare Creazione di un profilo server ASBCE per IP Office alla pagina 39.	
15.	Creazione di instradamento server	Utilizzare la voce IPv4 esistente. Consultare Creazione di un profilo di instradamento del server alla pagina 41.	
16.	Configurazione topologia nascosta	Utilizzare la voce IPv4 esistente. Consultare Creazione di un criterio di topologia nascosta ASBCE alla pagina 43.	
17.	Creazione di un elenco di blocchi IP/URL.	Utilizzare la voce IPv4 esistente. Consultare Creazione di un elenco di blocchi IP/URI alla pagina 44.	
18.	Creazione di una regola dell'applicazione	Utilizzare la voce IPv4 esistente. Consultare Creazione di una regola dell'applicazione alla pagina 45.	
19.	Creazione di una regola multimediale	Utilizzare la voce IPv4 esistente. • Assicurarsi che **Opzioni avanzate** > **ANAT abilitato** non sia selezionato. Consultare Creazione di una regola multimediale alla pagina 46.	
20.	Creazione di un criterio endpoint	Utilizzare la voce IPv4 esistente. Consultare Creazione di un gruppo di criteri endpoint alla pagina 48.	

La tabella continua…

#	Azione	Collegamenti/Note	✔
21.	Aggiunta di un profilo agente utente	Utilizzare la voce IPv4 esistente. Consultare Configurazione di un profilo agente utente alla pagina 49.	
22.	Creazione di un flusso di abbonati	Aggiungere una nuova voce, come la voce IPv4: • Impostare le interfacce multimediali e di segnalazione in modo che utilizzino le interfacce IPv6 esterne. Consultare Creazione del flusso degli abbonati alla pagina 51.	
23.	Creazione di un flusso server	Aggiungere una nuova voce, come la voce IPv4: • Impostare l'interfaccia di segnalazione esterna IPv6 come **Interfaccia ricevuta**. Consultare Creazione di un flusso server alla pagina 53.	
24.	Aggiungere un proxy inverso per Avaya Workplace Client	Aggiungere nuovi proxy utilizzando l'interfaccia esterna B1 configurata per gli indirizzi IPv6. Consultare Aggiunta di proxy inversi per le richieste di file alla pagina 54.	

Collegamenti correlati

Supporto degli interni remoti IPv6 alla pagina 70

Parte 3: Resilienza

Capitolo 9: Resilienza di ASBCE e IP Office

IP Office supporta una serie di opzioni di resilienza, tra cui la resilienza per i telefoni SIP e le applicazioni softphone SIP. Per ulteriori informazioni, consultare il manuale IP Office Panoramica della resilienza.

Questa sezione di questo documento fornisce una panoramica della configurazione aggiuntiva richiesta per aggiungere il supporto della resilienza a una configurazione esistente. I passaggi aggiuntivi principali sono:

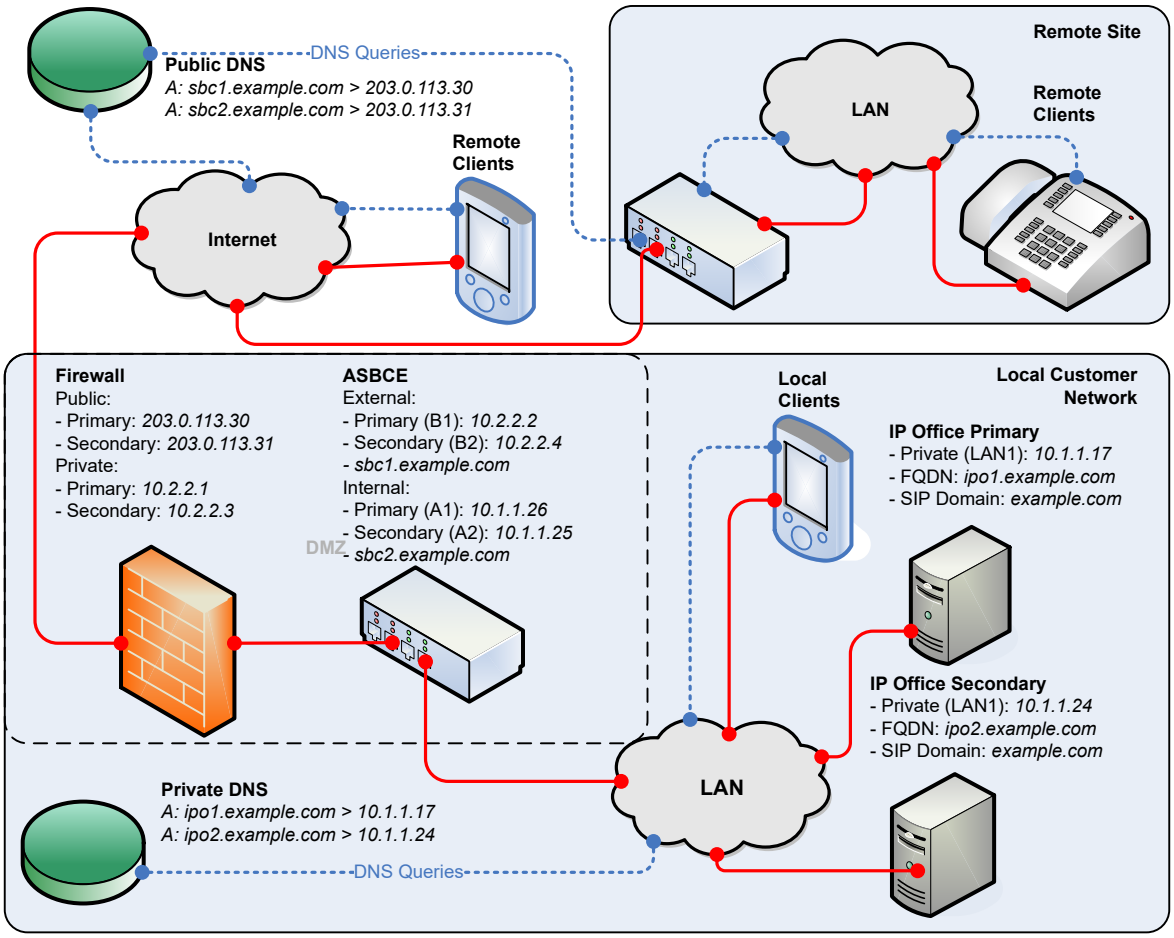
- IP Office non può utilizzare l'indirizzo IP dell'interno remoto per corrispondere a una posizione nella configurazione di IP Office. Pertanto, per utilizzare le impostazioni di posizione nella resilienza, è necessario configurare la posizione nella configurazione dell'interno.

Collegamenti correlati

Esempio di schema di resilienza alla pagina 78
Generazione di un certificato di identità per il server secondario IP Office alla pagina 79
Installazione del certificato di identità secondario IP Office alla pagina 80
Configurazione di IP Office per la resilienza dell'interno remoto alla pagina 81
Configurazione di Avaya one-X Portal alla pagina 81
Configurazione di ASBCE per la resilienza alla pagina 82
Configurazione del DNS per la resilienza alla pagina 82

Esempio di schema di resilienza

Di seguito è riportato uno schema di esempio per una configurazione resiliente.



Per il supporto resiliente degli interni remoti, ASBCE utilizza 2 set di indirizzi IP pubblici/privati:

- ASBCE instrada un set al server primario IP Office e l'altro al server secondario IP Office.
- Questa logica è la stessa indipendentemente dall'installazione di ASBCE: Simplex, HA, due server ASBCE separati o dual-stack.

Collegamenti correlati

[Resilienza di ASBCE e IP Office](#) alla pagina 78

Generazione di un certificato di identità per il server secondario IP Office

Il server secondario IP Office richiede un certificato di identità emesso dal server primario IP Office.

Procedura

1. Accedere ai menu Web Control di IP Office:
   - Da IP Office Web Manager, selezionare il server primario. Fare clic su ☰ e selezionare **Visualizzazione piattaforma**.

- Scorrere fino a `https://<IP Office IP address>:7071` e accedere.

2. Andare alla scheda **Impostazioni** e scorrere verso il basso fino a **Certificati** .
3. Immettere i seguenti dati:

Valore	Descrizione
IP computer	Immettere l'indirizzo IP del server secondario.
Password	Immettere una password per codificare il certificato e la chiave.
Nome oggetto	Immettere l'FQDN del server secondario IP Office.
Nomi alternativi oggetto	Elencare l'FQDN del server secondarioIP Office, il dominio XMPP del server secondario, il dominio SIP e gli indirizzi IP interni ed esterni del server secondario IP Office.

4. Fare clic su **Rigenera** e **Applica**.
5. Nella finestra popup, fare clic sul collegamento per scaricare il certificato.
6. Fare clic su **OK**.
7. Rinominare il file scaricato in `IPOSEC_ID.p12`.

Passi successivi

- Installazione del certificato di identità secondario IP Office alla pagina 80.

Collegamenti correlati

Resilienza di ASBCE e IP Office alla pagina 78

Installazione del certificato di identità secondario IP Office

È necessario aggiungere il certificato di identità creato per il server secondario IP Office.

Prerequisiti

- Generazione di un certificato di identità per il server secondario IP Office alla pagina 79.

Procedura

1. Accedere al sistema utilizzando IP Office Web Manager.
   - Per IP500 V2, immettere l'indirizzo di sistema seguito da `:8443/WebMgmtEE/WebManagerment.html`.
   - Per un server basato su Linux, immettere l'indirizzo del sistema seguito da `:7070/WebManagement/WebManagement.html`.
2. Andare a **Gestione sicurezza** > **Certificati**.
3. Fare clic sull'icona ✎ accanto al server secondario.
4. Fare clic su **Imposta** .
5. Individuare e selezionare il file del certificato di identità.
6. Immettere la password.

7. Fare clic su **Carica**.

Collegamenti correlati

Resilienza di ASBCE e IP Office alla pagina 78

Configurazione di IP Office per la resilienza dell'interno remoto

Oltre alla configurazione standard per la resilienza (vedere IP Office Panoramica della resilienza), è necessario configurare il server secondario IP Office come segue:

- Impostare le impostazioni del registrar SIP, ad eccezione di **FQDN registrar SIP**, sulle stesse impostazioni utilizzate sul server primario IP Office. Ciò include la corrispondenza con **Nome dominio SIP**. Consultare Configurazione VoIP SIP di IP Office alla pagina 11.
- Impostare **FQDN registrar SIP** in modo che corrisponda all'FQDN configurato nel DNS per instradare il traffico SIP al server secondario IP Office.
- Impostare le impostazioni **SBC** che gli interni remoti devono utilizzare per connettersi a ASBCE configurato per instradare le chiamate SIP al server secondario ASBCE. Consultare Impostazione dei dettagli di ASBCE passati agli interni remoti da IP Office alla pagina 12.

Collegamenti correlati

Resilienza di ASBCE e IP Office alla pagina 78

Configurazione di Avaya one-X Portal

È necessario configurare il servizio Avaya one-X Portal con il nome di dominio del server secondario IP Office.

Procedura

1. Accedere ai menu dell'amministratore Avaya one-X Portal:
   - In IP Office Manager, selezionare **Applicazioni** > **one-X Portal** > .
   - Scorrere fino a `https://<portal IP address>:9443/onexportal-admin.html` e accedere come Amministratore.
2. Selezionare **Configurazione** > **Nome dominio host**.
   a. Impostare il **Nome dominio host secondario** sull'FQDN del server secondario Avaya one-X Portal.
   b. Fare clic su **Salva**.
3. Fare clic sull'icona nella parte superiore dei menu per riavviare Avaya one-X Portal.

Collegamenti correlati

Resilienza di ASBCE e IP Office alla pagina 78

Configurazione di ASBCE per la resilienza

I passaggi di configurazione di ASBCE sono simili a quelli per la configurazione di un singolo server. È necessario creare voci aggiuntive, ma utilizzando gli indirizzi IP pubblici e privati del server secondario IP Office.

Collegamenti correlati

Resilienza di ASBCE e IP Office alla pagina 78

Configurazione del DNS per la resilienza

La configurazione del server DNS è simile a quella di un singolo server IP Office. Il DNS richiede record aggiuntivi, l'FQDN dei server secondari IP Office e ASBCE.

Collegamenti correlati

Resilienza di ASBCE e IP Office alla pagina 78

Capitolo 10: Controllo della configurazione della resilienza

È possibile utilizzare i seguenti metodi per controllare le informazioni sulla resilienza fornite da IP Office agli interni remoti.

Collegamenti correlati

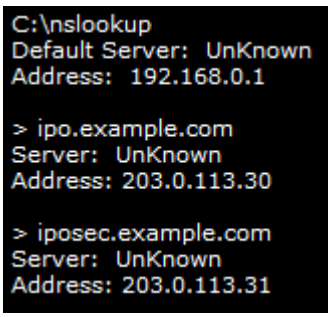
[Controllo dell'instradamento DNS della resilienza](#) alla pagina 83
[Visualizzazione del tracciato ASBCE](#) alla pagina 84
[Controllo delle risposte Avaya one-X Portal](#) alla pagina 85

Controllo dell'instradamento DNS della resilienza

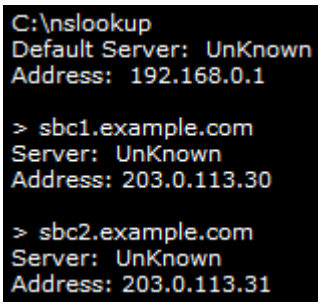
Utilizzando un PC remoto, è possibile verificare che il DNS stia risolvendo correttamente le richieste.

Procedura

1. Utilizzare il comando `nslookup` per verificare che DNS risolva gli FQDN del server primario IP Office e del server secondario IP Office agli indirizzi IP corretti. Ad esempio:



2. Utilizzare il comando `nslookup` per verificare che DNS risolva gli FQDN del server primario e secondario ASBCE.



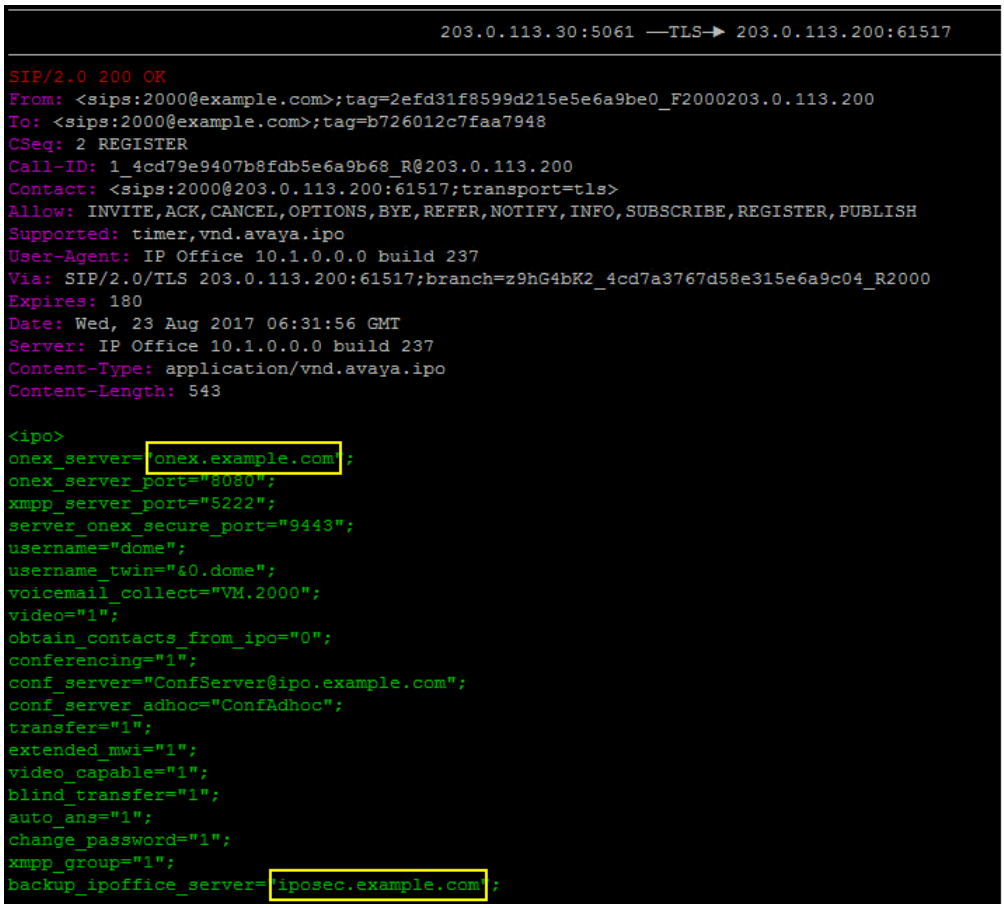
Collegamenti correlati

[Controllo della configurazione della resilienza](#) alla pagina 83

Visualizzazione del tracciato ASBCE

Di seguito è riportato un esempio di sessione traceSBC per la registrazione di un client. Visualizza la risposta SIP di *200 OK* inviata al client.

La risposta contiene una serie di impostazioni di configurazione. Per gli interni remoti, la risposta includerà l'FQDN SBC configurato sul server secondario IP Office.



- **Durante il normale funzionamento:**

  La risposta di *200 OK* mostra i valori *onex_server* e *backup_ipoffice_server* impostati rispettivamente con i server primario e secondario.

- **Durante la resilienza:**

  onex_server contiene l'FQDN del portale secondario e *backup_ipoffice_server* è *0.0.0.0*.

Collegamenti correlati

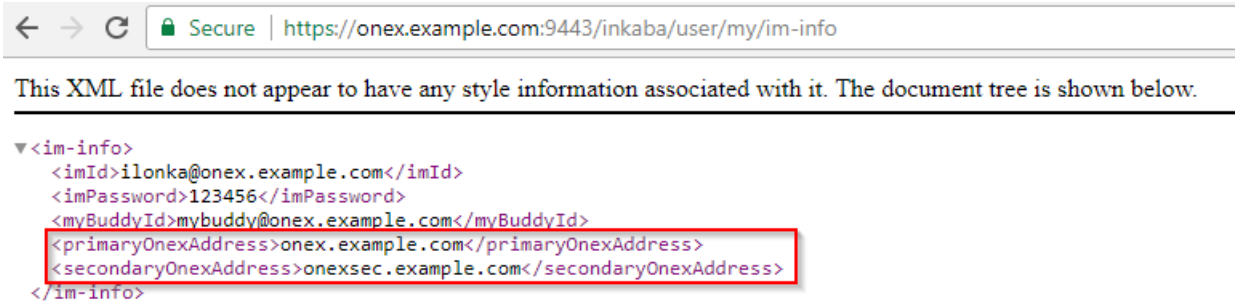
[Controllo della configurazione della resilienza](#) alla pagina 83

Controllo delle risposte Avaya one-X Portal

Quando un client richiede informazioni XMPP dal servizio primario Avaya one-X Portal, la risposta include gli indirizzi del server XMPP primario e secondario.

Procedura

1. Durante il normale funzionamento, tramite un browser, immettere `https://<FQDN>:9443/inkaba/user/my/im-info` dove *<FQDN>* è l'FQDN del servizio primario Avaya one-X Portal.



2. Verificare che la risposta includa gli FQDN dei servizi Avaya one-X Portal primario e secondario.

   a.

   b. La risposta deve includere l'FQDN del server primario IP Office.

3. Tramite un browser, immettere `https://<FQDN>:9443/inkaba/user/my/sip-info` dove *<FQDN>* è l'FQDN del servizio primario Avaya one-X Portal.

4. Se si ripetono i passaggi durante la resilienza, utilizzare l'FQDN del server secondario Avaya one-X Portal.

   - Le informazioni di `im-info` saranno le stesse.
   - Le informazioni di `sip-info` mostreranno l'FQDN del server secondario IP Office.

Collegamenti correlati

Controllo della configurazione della resilienza alla pagina 83

Parte 4: Informazioni aggiuntive

Capitolo 11: Guida e documentazione aggiuntive

Le pagine seguenti forniscono le fonti per ulteriore assistenza.

Collegamenti correlati

Manuali aggiuntivi e guide per l'utente alla pagina 88
Utilizzo della guida alla pagina 88
Ricerca di un business partner Avaya alla pagina 89
Risorse IP Office aggiuntive alla pagina 89
Formazione alla pagina 90

Manuali aggiuntivi e guide per l'utente

Il sito Web Avaya Centro documentazione contiene manuali per l'utente e manuali per i prodotti Avaya, tra cui IP Office.

- Per un elenco dei manuali IP Office e delle guide utente correnti, consultare il documento Avaya IP Office™ Manuali e guide per l'utente di ™ Platform.
- I siti Web Avaya IP Office Knowledge base e Avaya Supporto consentono inoltre di accedere ai manuali tecnici IP Office e alle guide utente.
  - Se possibile, questi siti reindirizzano gli utenti alla versione del documento ospitato da Avaya Centro documentazione.

Per altri tipi di documenti e altre risorse, visitare i vari siti Web Avaya (vedere Risorse IP Office aggiuntive alla pagina 89).

Collegamenti correlati

Guida e documentazione aggiuntive alla pagina 88

Utilizzo della guida

Avaya vende IP Office tramite partner commerciali accreditati. Questi business partner forniscono supporto diretto ai propri clienti e possono segnalano i problemi ad Avaya se necessario.

Se il sistema IP Office attualmente non dispone di un business partner Avaya che fornisce assistenza e manutenzione, è possibile utilizzare lo strumento Avaya Partner Locator per trovare un business partner. Consultare Ricerca di un business partner Avaya alla pagina 89.

Collegamenti correlati

Guida e documentazione aggiuntive alla pagina 88

Ricerca di un business partner Avaya

Se il sistema IP Office attualmente non dispone di un business partner Avaya che fornisce assistenza e manutenzione, è possibile utilizzare lo strumento Avaya Partner Locator per trovarne uno.

Procedura

1. Utilizzando un browser, accedere a Sito Web Avaya presso https://www.avaya.com
2. Selezionare **Partner**, quindi **Trova un partner**.
3. Immettere le informazioni sulla posizione.
4. Per i business partner IP Office, utilizzare il **Filtro**, selezionare **Piccola/media impresa**.

Collegamenti correlati

Guida e documentazione aggiuntive alla pagina 88

Risorse IP Office aggiuntive

Oltre al sito Web della documentazione (vedere Manuali aggiuntivi e guide per l'utente alla pagina 88), è disponibile una gamma di siti Web che forniscono informazioni sui prodotti e i servizi Avaya, tra cui IP Office.

- Sito Web Avaya (https://www.avaya.com)

  Questo è il sito Web ufficiale di Avaya. Dalla home page è possibile accedere ai singoli siti Web di Avaya di varie aree e Paesi.

- **Portale Avaya Sales & Partner** *(*https://sales.avaya.com*)*

  Questo è il Sito Web ufficiale per tutti i business partner di Avaya. Per accedere al sito occorre registrare nome utente e password. Una volta effettuato l'accesso, è possibile personalizzare il portale in modo da visualizzare prodotti specifici e il tipo di informazioni che si desidera visualizzare.

- **Avaya IP Office Knowledge base** *(*https://ipofficekb.avaya.com*)*

  Questo sito fornisce l'accesso a una versione online regolarmente aggiornata delle guide dell'utente e del manuale tecnico IP Office.

- **Avaya Supporto** *(*https://support.avaya.com*)*

  Questo sito fornisce l'accesso al software del prodotto di Avaya, alla documentazione e ad altri servizi per gli addetti all'installazione e alla manutenzione del prodotto di Avaya.

  - **Avaya Forum di supporto** *(*https://support.avaya.com/forums/index.php*)*

    Questo sito fornisce forum di discussione dei problemi dei prodotti.

- **Gruppo utenti internazionale di Avaya** *(*https://www.iuag.org*)*

  Si tratta dell'organizzazione per i clienti di Avaya. Vengono forniti gruppi e forum di discussione.

- **Avaya DevConnect** *(*https://www.devconnectprogram.com/*)*

  Questo sito fornisce dettagli su API e SDK per i prodotti Avaya, incluso IP Office. Il sito fornisce inoltre note sull'applicazione per prodotti non-Avaya di terze parti che interagiscono con IP Office utilizzando tali API e SDK.

- **Avaya Learning** *(*https://www.avaya-learning.com/*)*

  Questo sito fornisce l'accesso ai corsi di formazione e ai programmi di accreditamento per i prodotti di Avaya.

Collegamenti correlati

Guida e documentazione aggiuntive alla pagina 88

Formazione

La formazione e le credenziali di Avaya assicurano che i partner aziendali possiedano le capacità e le competenze necessarie per vendere, implementare e supportare con successo le soluzioni Avaya e superare le aspettative dei clienti. Sono disponibili le seguenti credenziali:

- Avaya Certified Sales Specialist (APSS)
- Avaya Implementation Professional Specialist (AIPS)
- Avaya Certified Support Specialist (ACSS)

Le mappe delle credenziali sono disponibili sul sito Web Avaya Learning.

Collegamenti correlati

Guida e documentazione aggiuntive alla pagina 88

Capitolo 12: Glossario

Di seguito sono riportate le definizioni dei termini utilizzati in questo documento.

Collegamenti correlati

Un record

"Record indirizzo". Record DNS di base che mappa un nome di dominio o FQDN a un indirizzo IPv4. Per gli indirizzi IPv6, DNS utilizza i record `AAAA`.

Collegamenti correlati

Glossario alla pagina 91

Record AAAA

Chiamato anche "Record Quad-A". I servizi DNS utilizzano i record `AAAA` per mappare un nome di dominio o FQDN a un indirizzo IPv6. Sono simili ai record `A` utilizzati per gli indirizzi IPv4.

Collegamenti correlati

Glossario alla pagina 91

ASBCE

"Avaya Session Border Controller for Enterprise". Piattaforma Avaya per la fornitura di servizi SBC per una rete del cliente.

Collegamenti correlati

Glossario alla pagina 91

DNS

"Server dei nomi di dominio". Server o servizio che fornisce informazioni sull'indirizzo IP in risposta a un nome di dominio o a una query FQDN. Ad esempio, quando un'applicazione tenta di connettersi a `www.example.com`, contatta prima il server DNS sulla sua rete. Il server DNS risolve l'indirizzo di testo `www.example.com` all'indirizzo IP numerico richiesto. Il processo prevede che il server DNS controlli i record DNS che detiene e, se necessario, quelli detenuti da altri server DNS nella rete o su Internet.

Collegamenti correlati

Glossario alla pagina 91

Nome di dominio

L'indirizzo di testo utilizzato per identificare una rete di dispositivi. Un server DNS traduce il nome di dominio e i nomi di dominio completamente qualificati in indirizzi IP specifici.

Collegamenti correlati

Glossario alla pagina 91

FQDN

"Nome dominio completo". L'indirizzo di testo completo assegnato a un server, servizio o client specifico all'interno di un dominio.

Collegamenti correlati

Glossario alla pagina 91

IP di gestione

L'indirizzo IP utilizzato per l'accesso dell'amministratore al server ASBCE. Si tratta di un indirizzo diverso da quello utilizzato per le interfacce di traffico di rete interne ed esterne fornite da ASBCE.

Collegamenti correlati

Glossario alla pagina 91

SBC

"Session Border Controller". Un SBC è un dispositivo che controlla la segnalazione e i media delle chiamate SIP tra due reti.

Collegamenti correlati

Glossario alla pagina 91

Suddividi DNS

L'utilizzo di FQDN e server DNS per instradare il traffico all'interno e tra le reti semplifica la manutenzione della rete. Tuttavia, possono verificarsi problemi quando si utilizza l'instradamento FQDN per il traffico di rete interno ed esterno. Può causare l'instradamento esterno del traffico interno ai servizi interni. In questo modo vengono visualizzati i servizi interni e gli indirizzi che devono rimanere nascosti.

Suddividi DNS utilizza un servizio DNS pubblico per il traffico esterno alla rete del cliente e un servizio DNS privato per il traffico interno all'interno della rete del cliente.

I clienti possono configurare il DNS diviso utilizzando un singolo server DNS sul perimetro della rete del cliente o server DNS pubblici e privati separati.

Collegamenti correlati

Glossario alla pagina 91

Record SRV

"Record di servizio". Per i domini che supportano più servizi, ad esempio `www.example.com` o `sip.example.com`, i record DNS `A` potrebbero non essere sufficienti per l'instradamento richiesto. I record DNS `SRV` forniscono la mappatura per servizi specifici in esecuzione all'interno di un dominio.

Collegamenti correlati

Glossario alla pagina 91

XMPP

"Extensible Messaging and Presence Protocol". XMPP è un protocollo standard aperto che consente ai dispositivi di scambiare informazioni su messaggi istantanei, presenza e contatti.

Collegamenti correlati

Glossario alla pagina 91

Indice

M

N

O

P

Q

R

S

T

U

V

W