Deploying Avaya IP Office™ Platform SSL VPN Services

Issue 7
April 2023

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 che potrebbero includere le informazioni sul prodotto, 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 a questa 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 di nessuna 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 di vendita. Sono, inoltre, disponibili a clienti e altre parti 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. Nota: acquistando il prodotto 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 e non da Avaya.

Per “**Servizio ospitato**” si intende l'abbonamento a un servizio ospitato 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 DEL SOFTWARE DISPONIBILI SUL SITO WEB DI AVAYA ALL'INDIRIZZO HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO AL LINK “TERMINI DI LICENZA DEL SOFTWARE AVAYA (prodotti Avaya)”, O SU UN SITO INDICATO SUCCESSIVAMENTE DA AVAYA, SONO APPLICABILI A CHIUNQUE ABBIA SCARICATO, UTILIZZATO E/O INSTALLATO PROGRAMMI SOFTWARE AVAYA, ACQUISTATI PRESSO AVAYA INC., QUALSIASI AFFILIATO AVAYA O UN PARTNER DI CANALE AVAYA AUTORIZZATO (OVE NE RICORRA IL CASO), IN BASE A UN CONTRATTO COMMERCIALE CON AVAYA O CON UN PARTNER DI CANALE AVAYA. SALVO DIVERSAMENTE CONCORDATO DA AVAYA PER ISCRITTO, AVAYA NON ESTENDE TALE LICENZA SE IL SOFTWARE NON È STATO REPERITO DA AVAYA, DA SUOI AFFILIATI O DA UN PARTNER DI CANALE AVAYA. AVAYA SI RISERVA IL DIRITTO DI INTENTARE UN'AZIONE LEGALE CONTRO CHIUNQUE UTILIZZI O VENDA IL SOFTWARE SENZA LICENZA. INSTALLANDO, SCARICANDO O UTILIZZANDO IL SOFTWARE, O AUTORIZZANDO ALTRI A FARLO, SI ACCETTANO, PER SE STESSI E PER L'ENTITÀ PER LA QUALE SIA STA INSTALLANDO, SCARICANDO O UTILIZZANDO IL SOFTWARE (DI SEGUITO “UTENTE” E “UTENTE FINALE”), TALI TERMINI E CONDIZIONI E SI CREA UN CONTRATTO VINCOLANTE CON AVAYA INC. O CON IL RELATIVO AFFILIATO AVAYA (AVAYA). O LA CONSOCIATA AVAYA APPLICABILE (“AVAYA”).

Avaya concede all'Utente una licenza secondo i termini dei tipi di licenza descritti di seguito, ad eccezione del software Heritage Nortel, il cui ambito di licenza è descritto in dettaglio di seguito. Se la documentazione dell'ordine non identifica in maniera esplicita un tipo di licenza, la licenza applicabile sarà una licenza di sistema designata come riportato nella sezione Licenza di sistema designata (DS). Il numero applicabile di licenze e di unità di capacità per le quali la licenza viene concessa è pari a uno (1), eccetto nei casi in cui venga specificato un numero diverso di licenze o di unità di capacità nella documentazione o in altri materiali a disposizione dell'Utente. Il termine “Software” indica programmi di computer in codice oggetto forniti da Avaya o da un Partner di canale Avaya sia come prodotti autonomi, preinstallati su prodotti hardware che come eventuali upgrade, aggiornamenti, patch, correzioni di errori o versioni modificate degli stessi. “Processore designato” indica un singolo dispositivo di elaborazione indipendente. Per “Server” si intende una serie di processori designati che ospita un'applicazione software accessibile da svariati utenti. Per “Istanza” si intende una singola copia del Software in esecuzione in un determinato momento: (i) su una macchina fisica; (ii) su una macchina virtuale (“VM”) con software installato o su un'installazione analoga.

Tipi di licenza

Licenza per sistema designato (DS, Designated System). L'utente finale può installare e utilizzare ciascuna copia o un'Istanza del Software esclusivamente: 1) sul numero massimo di Processori designati indicato nell'ordine o 2) sul numero massimo di Istanze del Software indicato nell'ordine, nella Documentazione o dietro autorizzazione scritta da parte di Avaya. Avayapuò richiedere che i Processori designati siano identificati, nell'ordine, dal tipo, dal numero di serie, dalla chiave funzione, dall'Istanza, dalla posizione o da altre designazioni specifiche oppure che siano forniti dall'Utente finale ad Avaya attraverso mezzi elettronici stabiliti da Avaya specificatamente per questo scopo.

Licenza per utenti simultanei (CU, Concurrent User). L'utente finale può installare e utilizzare il software su più processori designati o su uno o più server a condizione che in qualsiasi momento solo il numero di unità cui è stata concessa la licenza acceda al software e lo utilizzi, secondo quanto indicato nell'ordine o nella Documentazione, oppure dietro autorizzazione scritta da

parte di Avaya. Per “Unità” si intende l'unità su cui Avaya, a propria insindacabile discrezione, basa il prezzo delle licenze; può corrispondere, a titolo esemplificativo, a un agente, una porta o un utente, un account di posta elettronica o di casella vocale a nome di una persona o di un ruolo aziendale (ad esempio, webmaster o servizio di assistenza) o una voce di directory del database amministrativo utilizzato dal Software e che consente all'utente di interagire con il Software. Le unità possono essere collegate a uno specifico Server identificato o a un'Istanza del Software.

Licenza cluster (CL). L'utente finale può installare e utilizzare ogni copia o un'istanza del software solo sul numero di cluster indicato nell'ordine o nella Documentazione, dietro autorizzazione scritta da parte di Avaya o su un (1) cluster predefinito se non indicato.

Licenza enterprise (EN). L'utente finale può installare e utilizzare ciascuna copia o un'Istanza del Software esclusivamente per l'utilizzo a livello aziendale di un numero illimitato di Istanze del Software, secondo quanto indicato nell'ordine o nella Documentazione o dietro autorizzazione scritta da parte di Avaya.

Licenza per utenti identificati (NU, Named User). L'Utente finale può: (i) installare e utilizzare ciascuna copia o Istanza del Software su un singolo Processore designato o Server per ciascun Utente identificato autorizzato (definito di seguito) o (ii) installare e utilizzare ciascuna copia o Istanza del Software su un Server a condizione che solo gli Utenti identificati autorizzati abbiano accesso al Software e lo utilizzino secondo quanto indicato nell'ordine o nella Documentazione, oppure dietro autorizzazione scritta da parte di Avaya. “Utente identificato” indica un utente o dispositivo che è stato espressamente autorizzato da Avaya ad accedere al Software e a utilizzarlo. A esclusiva discrezione di Avaya, un “Utente identificato” può essere, a titolo esemplificativo, designato per nome, funzione aziendale (ad esempio, webmaster o servizio di assistenza), account di posta elettronica o di posta vocale a nome di una persona o di una funzione aziendale oppure voce della directory del database amministrativo utilizzato dal Software che permette a un utente di interagire con il Software.

Licenza a strappo (SR, Shrinkwrap License). L'Utente finale può installare e utilizzare il Software in base ai termini e alle condizioni dei contratti di licenza pertinenti, ad esempio “a strappo” o “di accettazione tramite clic” (le cosiddette licenze clickthrough) in dotazione o relative al Software (quale la “Licenza a strappo”), secondo quanto indicato nell'ordine o nella Documentazione, oppure dietro autorizzazione scritta da parte di Avaya.

Licenza di transazione. L'utente finale può utilizzare il software per il numero massimo di Transazioni specificato entro un periodo di tempo definito e secondo quanto indicato nell'ordine o nella Documentazione, oppure dietro autorizzazione scritta da parte di Avaya. Per "Transazione" si intende l'unità su cui Avaya, a sua discrezione esclusiva, basa i prezzi della relativa licenza e può essere misurata, senza limitazioni, a seconda dell'utilizzo, dell'accesso, dell'interazione (tra client/server o cliente/organizzazione) o delle operazioni del software entro un periodo di tempo definito (ad es. ora, giorno, mese). Alcuni esempi di Transazioni includono, a titolo esemplificativo, tutti i messaggi di saluto riprodotti/messaggi di attesa abilitati, tutte le promozioni personalizzate (in qualsiasi canale), tutte le operazioni di richiamata, tutti gli agenti live o le sessioni di chat Web e tutte le chiamate instradate o reindirizzate (in qualsiasi canale). L'Utente finale non può superare il numero di Transazioni senza un previo consenso da parte di Avaya e il conseguente pagamento di un onere aggiuntivo.

Software Heritage Nortel

“Heritage Nortel Software” significa che il software è stato acquistato da Avaya come parte del suo acquisto di Nortel Enterprise Solutions nel dicembre 2009. Il Software Heritage Nortel, è il software contenuto nell'elenco dei prodotti di Heritage Nortel alla pagina http://support.avaya.com/LicenseInfo (selezionare il collegamento “Heritage Nortel Products”) o su un sito indicato successivamente da Avaya. Per il software Heritage Nortel, Avaya concede al Cliente una licenza d'uso di tale Software, la quale viene fornita in virtù del presente documento esclusivamente per il livello di attivazione o di utilizzo autorizzato, al solo scopo specificato nella Documentazione e solo per l'incorporamento o l'esecuzione in apparecchiature Avaya o la comunicazione con le stesse. Le tariffe per il software Heritage Nortel possono essere applicate in base al livello di attivazione o utilizzo autorizzato specificato in un ordine o una fattura.

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 e/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

Per “Componenti di terzi” si intendono alcuni programmi software o parti incluse nel Software o nel Servizio ospitato, che potrebbero contenere software (incluso software open source) distribuito in conformità ad accordi con terzi (“Componenti di terzi”), contenenti termini relativi ai diritti d'uso di alcune parti del Software (“Termini di terze parti”). Come richiesto, le informazioni sul codice sorgente distribuito del sistema operativo Linux (pertinente ai prodotti che includono tale codice), nonché i dettagli di identificazione dei titolari di copyright relativi ai Componenti di terzi e ai relativi Termini applicabili sono disponibili nei prodotti, nella Documentazione o sul sito Web Avaya al seguente indirizzo: https://support.avaya.com/Copyright oppure su un sito indicato successivamente da Avaya. I termini di licenza del software open source forniti come Termini di terzi sono conformi ai diritti di licenza concessi nei presenti Termini di licenza del Software e possono contenere diritti aggiuntivi a vantaggio dell'Utente, come la modifica e la distribuzione del software open source. I Termini di terzi hanno la precedenza sui presenti Termini di licenza del Software esclusivamente per quanto riguarda i Componenti di terzi applicabili nella misura in cui i presenti Termini di licenza del Software impongono all'Utente restrizioni maggiori rispetto ai Termini di terzi applicabili.

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 I PARTNER DI CANALE AVAYA CHE OSPITANO PRODOTTI O SERVIZI AVAYA, SI APPLICA QUANTO SEGUE. IL PRODOTTO O IL SERVIZIO OSPITATO POTREBBE UTILIZZARE COMPONENTI DI TERZI SOGGETTI AI TERMINI DI QUESTI ULTIMI, PERTANTO IL FORNITORE DEL SERVIZIO DEVE OTTENERE IN MANIERA AUTONOMA UNA LICENZA DIRETTAMENTE DAL FORNITORE TERZO. I PARTNER DI CANALE AVAYA CHE OSPITANO SERVIZI AVAYA DEVONO ESSERE AUTORIZZATI DA AVAYA PER ISCRITTO E, SE TALI PRODOTTI OSPITATI UTILIZZANO O INCORPORANO DETERMINATI SOFTWARE DI TERZI, COMPRESI A TITOLO ESEMPLIFICATIVO SOFTWARE O CODEC

MICROSOFT, IL PARTNER DI CANALE AVAYA DEVE OTTENERE IN MANIERA AUTONOMA QUALSIASI CONTRATTO DI LICENZA APPLICABILE A SPESE DEL MEDESIMO PARTNER DI CANALE AVAYA, DIRETTAMENTE DAL RELATIVO FORNITORE TERZO.

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 tariffaria e si necessita di assistenza o supporto tecnico, chiamare il Centro di assistenza tecnica per l'intervento contro le frodi tariffarie al numero dedicato +1-800-643-2353 per gli Stati Uniti e il Canada. Per ulteriori numeri di telefono di assistenza, visitare il sito Web dell'assistenza Avaya all'indirizzo https://support.avaya.com o un sito indicato successivamente da 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 l'uso di tali marchi senza previo consenso scritto di Avaya o di tali terzi eventuali proprietari 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 registrato di Avaya Inc.

Tutti i marchi di fabbrica non Avaya appartengono ai rispettivi titolari.

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

Contents

Capitolo 1: Modifiche al documento dall'ultima pubblicazione

A questo documento per IP Office versione 9.1 sono state apportate le seguenti modifiche.

Software Development Kit (SDK)

Per facilitare la configurazione del servizio SSL VPN da parte dei partner, sono disponibili due SDK. Tali kit vengono illustrati in Configurazione di un servizio SSL VPN mediante SDK alla pagina 52.

Procedura guidata per la configurazione rapida di AVG

La procedura guidata per la configurazione rapida di AVG è stata aggiornata. Vedere Appendice A Esempio relativo alla procedura guidata per la configurazione rapida di AVG alla pagina 92.

Capitolo 2: Informazioni sul servizio SSL VPN

La soluzione di accesso remoto SSL VPN di IP Office consente di configurare in modo rapido e semplice un accesso remoto protetto con velocità di banda larga. La soluzione è progettata per offrire ad Avaya e ai suoi partner un accesso remoto affidabile in grado di migliorare la fornitura dei servizi, riducendo al contempo i costi associati alla fornitura di servizi in loco. La soluzione consente ad aziende partner di qualsiasi dimensione di creare un'infrastruttura in grado di automatizzare la gestione e la manutenzione dei sistemi IP Office.

Servizi forniti da SSL VPN

Il servizio SSL VPN fornisce il tunneling protetto tra l'hardware Avaya IP Office installato nel sito del cliente e un Avaya VPN Gateway (AVG) remoto. Questo tunnel protetto consente al personale dell'assistenza di offrire servizi di gestione remota ai clienti, tra cui gestione degli errori, monitoraggio e amministrazione. Inoltre, conferisce agli amministratori la capacità di:

- inoltrare il traffico sul servizio SSL VPN mediante instradamenti statici e di split tunneling;
- monitorare IP Office in remoto sul servizio SSL VPN connesso a un server AVG mediante System Status Application (SSA) o SysMonitor;
- gestire sistemi IP Office in remoto mediante Avaya IP Office Manager o IP Office Manager for Server Edition;
- ricevere trap SNMP, voci Syslog e allarmi SMTP via e-mail da IP Office su un servizio SSL VPN connesso a un server AVG;
- abilitare e disabilitare il tunnel mediante Manager o IP Office Manager for Server Edition;
- abilitare e disabilitare il tunnel mediante codici funzione, assistente automatico o amministrazione basata su gruppi;
- eseguire più istanze del servizio SSL VPN contemporaneamente.

Collegamenti correlati

Opzioni di distribuzione alla pagina 10
Modalità operative alla pagina 10
Architettura di sistema alla pagina 13
Limitazioni e requisiti di sistema alla pagina 16
Documentazione correlata alla pagina 17

Opzioni di distribuzione

Servizi di supporto remoto Avaya

La soluzione SSL VPN è parte integrante di IP Office Support Services (IPOSS), che consente ad Avaya di fornire servizi di primissimo livello per quel che riguarda la risoluzione dei problemi e il supporto tecnico in remoto. La possibilità di stabilire una connessione SSL VPN con Avaya è semplificata notevolmente dalla funzione automatica di On-Boarding. Il processo di On-Boarding include l'estrazione dall'inventario, la registrazione in GRT per creare il record della base installata e la registrazione tecnica per la connettività remota ad Avaya.

Per ulteriori informazioni sulla soluzione di manutenzione IPOSS, accedere alla pagina dei servizi di supporto IP Office nel portale delle vendite di Avaya.

Servizi di supporto remoto forniti da partner Avaya

Oltre alla soluzione IPOSS, i partner possono sfruttare il client SSL VPN insieme alla soluzione gateway VPN (AVG) di Avaya per creare un'infrastruttura SSL VPN personalizzata. Questo documento contiene informazioni e procedure utili per i partner Avaya che desiderano creare la propria soluzione SSL VPN per l'accesso remoto, come parte dell'assistenza alla manutenzione che offrono ai propri clienti.

La soluzione SSL VPN configurata dai partner è supportata su Standard Edition e sui sistemi Server Edition IP Office.

Collegamenti correlati

Informazioni sul servizio SSL VPN alla pagina 9

Modalità operative

Modalità operative

Il servizio SSL VPN è supportato sull'hardware IP500v2. Il modulo di controllo IP500 non è supportato.

Il servizio SSL VPN è supportato su sistemi operativi IP Office nelle modalità riportate di seguito. La modalità Branch non è supportata.

- IP Office Standard Edition (modalità Essential, Advanced e Preferred)
- Server Edition
  - Server Edition Primario
  - Server Edition Secondario
- Sistema di espansione Server Edition
  - Sistema di espansione Server Edition (V2), un sistema di espansione IP500v2
  - Sistema di espansione Server Edition (L), un sistema di espansione Linux
- Basic Edition

Nota:

Basic Edition è supportato solo su distribuzioni che utilizzano Avaya IP Office Support Services (IPOSS). Basic Edition non è supportato con un servizio SSL VPN distribuito per servizi di supporto dei partner Avaya.

Funzioni supportate

Le funzionalità disponibili dipendono dalla modalità operativa in uso. In questa sezione vengono fornite informazioni generali sulle funzionalità SSL VPN e vengono elencate le funzioni disponibili in ogni modalità.

Funzioni supportate	Modalità operativa			
	Standard Edition	Server Edition	Sistema di espansione Server Edition	Basic Edition
Connettività				
Connessione SSL VPN costante a un server AVG	✔	✔	✔	✔
Instradamenti di split tunneling	✔	✔	✔	✔
Instradamenti statici	✔	✔	✔	✔
Esecuzione di più istanze del servizio SSL VPN contemporaneamente.	✔	✔	✔	✔
Accesso ai dispositivi LAN (NAPT)	✔	✔	✔	—
Gestione degli errori				
Generazione di trap SNMP	✔	✔	✔	✔
Generazione di voci Syslog	✔	✔	✔	—
Generazione di notifiche e-mail per allarmi	✔	✔	✔	—
Generazione di allarmi di test	✔	✔	✔	✔
Monitoraggio e amministrazione				
Gestione remota mediante Manager o IP Office Manager for Server Edition	✔	✔	✔	✔

Table continues…

Funzioni supportate	Modalità operativa			
	Standard Edition	Server Edition	Sistema di espansione Server Edition	Basic Edition
Monitoraggio remoto mediante System Status Application	✔	✔	✔	✔
Monitoraggio remoto mediante SysMonitor	✔	✔	✔	✔
Abilitazione e disabilitazione del servizio SSL VPN mediante codici funzione	✔	✔	✔	—
Abilitazione e disabilitazione del servizio SSL VPN mediante menu basati su gruppi	—	—	—	✔
Abilitazione e disabilitazione del servizio SSL VPN mediante Manager o IP Office Manager for Server Edition	✔	✔	✔	—
Abilitazione e disabilitazione del servizio SSL VPN mediante assistente automatico	✔	✔	✔	—
Abilitazione e disabilitazione del servizio SSL VPN mediante tasti programmabili nei telefoni da tavolo Avaya	✔	✔	✔	✔
Upgrade remoto di IP Office a nuove versioni	✔	✔	✔	✔

Strumenti di monitoraggio e amministrazione

Se il servizio SSL VPN è connesso, è possibile gestire e monitorare il sistema IP Office in remoto attraverso il tunnel.

Per gestire, eseguire l'upgrade e configurare il sistema IP in remoto, è possibile utilizzare gli strumenti seguenti:

- IP Office Manager: un'applicazione amministrativa che consente di configurare impostazioni di sistema per sistemi IP Office Essential Edition.
  - IP Office Manager for Server Edition: all'avvio di IP Office Manager è possibile scegliere di aprire una configurazione con la modalità IP Office Manager for Server Edition, che consente di amministrare i server e le espansioni di sistema Server Edition.
- IP Office Basic Edition - Web Manager: uno strumento basato su browser che consente di configurare impostazioni di sistema per IP Office.

Per monitorare il sistema IP Office in remoto, è possibile utilizzare gli strumenti seguenti:

- System Status Application (SSA): System Status Application è uno strumento di diagnostica che consente di monitorare lo stato dei sistemi IP Office. SSA segnala eventi in tempo reale e cronologici, nonché dati sullo stato e sulla configurazione.
- SysMonitor: l'applicazione SysMonitor visualizza informazioni operative sul sistema IP Office. Consente di acquisire le informazioni nei file di registro per l'analisi.

Collegamenti correlati

Informazioni sul servizio SSL VPN alla pagina 9

Architettura di sistema

Il servizio SSL VPN fornisce il tunneling protetto tra l'hardware IP Office installato nel sito di un cliente e un'istanza di Avaya VPN Gateway (AVG) installata nel sito del provider del servizio. Le informazioni contenute in questa sezione consentono di comprendere l'architettura di rete utilizzata dal servizio SSL VPN.

Schede di interfaccia di rete

Avaya consiglia di distribuire il server di AVG in una configurazione con due interfacce di rete. un'interfaccia gestisce il traffico privato tra SSL VPN e la rete Intranet protetta. Questa connessione consente l'accesso del servizio SSL VPN alle risorse interne, nonché la configurazione e la gestione del sistema IP Office da una stazione di gestione. La seconda interfaccia gestisce invece il traffico in entrata e in uscita da Internet.

Instradamento

Nel sito del provider del servizio è possibile configurare l'instradamento aziendale tra AVG e la relativa rete privata. Nel sito del cliente è possibile posizionare ogni sistema IP Office nel lato privato di un router aziendale. Il router aziendale non richiede modifiche al configurazione per il funzionamento del servizio SSL VPN.

IP Office inoltra i dati a AVG sul servizio SSL VPN mediante instradamenti di split tunneling o statici. Per inviare il traffico tramite il tunnel SSL VPN, è necessario utilizzare una delle opzioni seguenti:

- Consentire a IP Office l'installazione dinamica di installare instradamenti di split tunneling quando il servizio SSL VPN si connette ad AVG e di rimuoverli alla disconnessione

- configurare un instradamento statico in IP Office Manager

Split tunneling:

In fase di installazione e configurazione di AVG, è possibile aggiungere subnet di reti divise oppure ospitare indirizzi per un gruppo. Il sistema IP Office riceve le informazioni di instradamento per il tunnel in modo dinamico quando il servizio SSL VPN si connette ad AVG. Gli instradamenti delle reti divise verranno rimossi alla disconnessione del servizio SSL VPN service da AVG.

Per informazioni sulla configurazione dello split tunneling in AVG mediante Net Direct, vedere *Avaya VPN Gateway Administration Guide* (Guida all'amministrazione di Avaya VPN Gateway) (NN46120-105) e *Avaya VPN Gateway BBI Application Guide* (Guida all'applicazione BBI di Avaya VPN Gateway (NN46120-102). Per informazioni sulla configurazione dello split tunneling mediante l'interfaccia della riga di comando, vedere *CLI Application Guide* (Guida all'applicazione CLI) (NN46120-101).

Instradamenti statici:

In alternativa allo split tunneling, è possibile configurare un instradamento statico direttamente nel sistema IP Office. In fase di configurazione di un instradamento statico, il sistema utilizza le informazioni dell'instradamento IP configurate in Manager per determinare la destinazione per il traffico inoltrato. È necessario definire il servizio SSL VPN come destinazione.

Utilizzare un instradamento statico nei seguenti casi:

- Gli instradamenti dello split tunneling non sono annunciati da AVG ed è necessario inviare traffico tramite il tunnel
- Il servizio SSL VPN non è connesso ad AVG e si desidera accodare il traffico da inoltrare tramite il tunnel al ripristino della connessione. In questo caso, IP Office accoda temporaneamente un numero ridotto di pacchetti che attivano la connessione se SSL VPN è in servizio, ma disconnesso

È possibile configurare più instradamenti statici nel sistema IP Office.

Autenticazione

Ogni sistema IP Office è in grado di supportare più tunnel SSL VPN. A ogni istanza di un servizio SSL VPN viene assegnato un indirizzo IP statico privato univoco. Quando ci si connette al servizio SSL VPN, AVG autentica il sistema IP Office. Nel caso di un numero ridotto di sistemi IP Office, è possibile utilizzare il database locale di Avaya VPN Gateway (AVG) per creare i dati utente necessari per l'autenticazione. Per distribuzioni più grandi, si consiglia di utilizzare un server RADIUS per l'autenticazione.

Accesso agli agenti di servizio

Gli agenti di servizio posizionati nel sito del provider del servizio possono connettersi a qualsiasi sistema IP Office che dispone di una connessione SSL VPN in servizio ad AVG. Possono monitorare e gestire il sistema IP Office in remoto contattando l'indirizzo IP del tunnel SSL VPN e possono accedere agli indirizzi IP di più servizi SSL VPN contemporaneamente.

AVG verifica che i tunnel SSL VPN non possano comunicare tra loro. Non è necessario configurare ulteriori impostazioni per verificare che i tunnel rimangano protetti e indipendenti.

Gestione degli errori

Un server di gestione degli errori è un componente facoltativo nel servizio SSL VPN. Posizionare un server di gestione degli errori nel sito del provider del servizio e utilizzare il servizio SSL

VPN per inviare errori di sistema al server. È possibile impostare filtri eventi per determinare quali errori verranno segnalati. È ad esempio possibile impostare filtri per segnalare qualsiasi evento correlato al funzionamento del sistema IP Office, nonché segnalare errori specifici per il funzionamento del servizio SSL VPN.

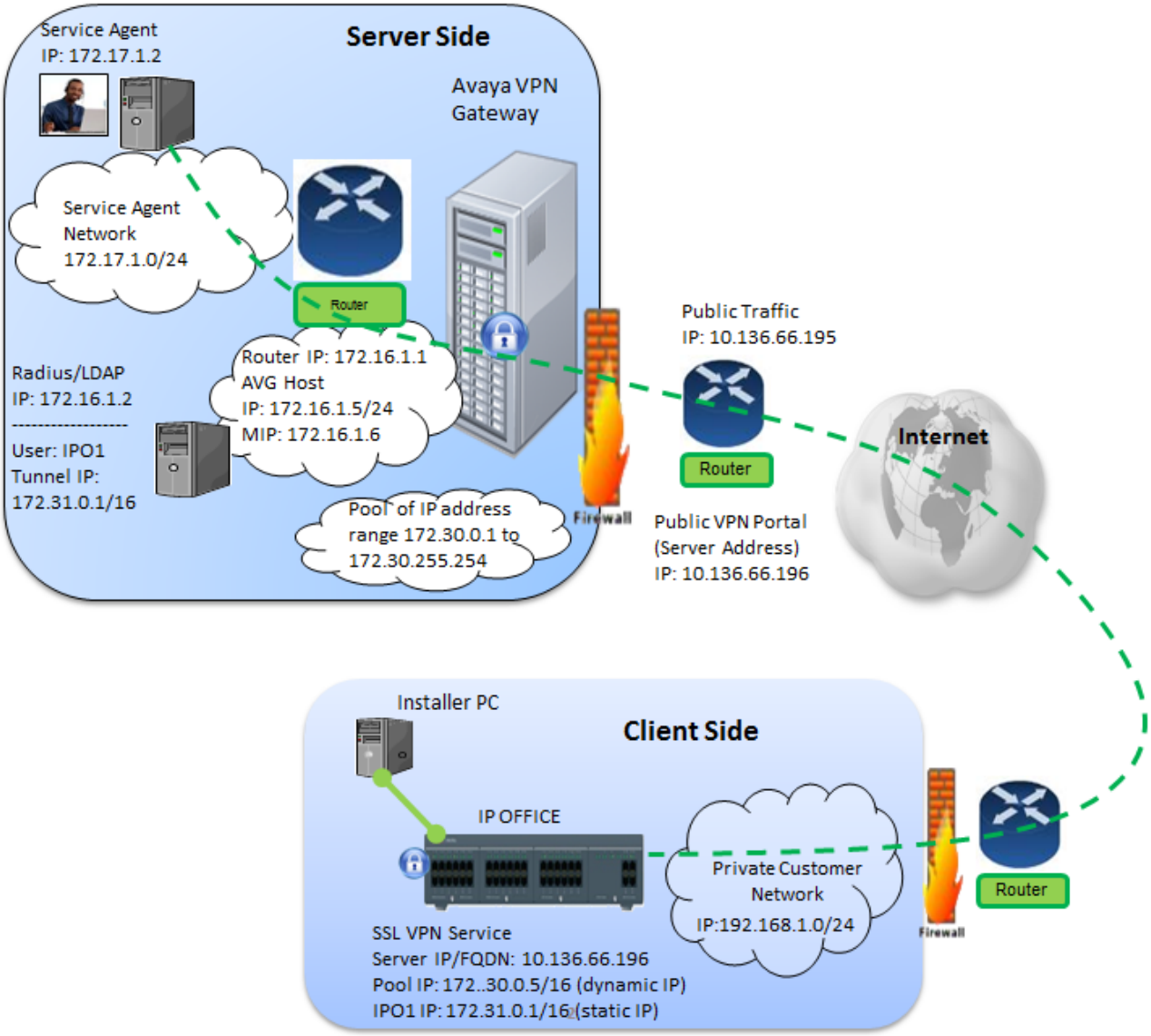
È consigliabile impostare il nome account del servizio SSL VPN in modo che corrisponda al nome ID dispositivo dell'agente SNMP. L'ID dispositivo dell'agente SNMP è configurato in IP Office Manager nel modulo **Sistema**, all'interno di **Eventi di sistema**, **Configurazione**.

Attraversamento del firewall

Il servizio SSL VPN funziona in modo trasparente attraverso il firewall. Non è necessario configurare il router aziendale per consentire il servizio SSL VPN se è già stato configurato per il traffico HTTPS. Il servizio SSL VPN utilizza la stessa porta di destinazione per il traffico TCP.

Esempio di architettura

Nel diagramma indicato di seguito viene illustrato un esempio dell'architettura utilizzata dal servizio SSL VPN.



Collegamenti correlati

Informazioni sul servizio SSL VPN alla pagina 9

Limitazioni e requisiti di sistema

Requisiti

Larghezza di banda:

Verificare che la larghezza di banda di caricamento sia pari ad almeno 90 kB/s (720 kb/s), con latenza non superiore a 150 ms (round trip). Questa specifica garantisce che Avaya Global Services possa fornire supporto remoto tramite il servizio SSL VPN.

Autenticazione:

- Nel caso di un numero ridotto di sistemi IP Office, è possibile utilizzare il database locale di Avaya VPN Gateway (AVG) per creare i dati utente necessari per l'autenticazione.
- Per distribuzioni più grandi, utilizzare un server RADIUS. È consigliabile utilizzare Avaya Identity Engines Ignition Server come server RADIUS.
- Il sistema IP Office utilizza certificati digitali per verificare l'identità di AVG all'estremità del tunnel SSL VPN. È necessario configurare certificati in AVG e installare i certificati X.509 necessari nell'archivio dei certificati di IP Office.

Licenze:

Il servizio SSL VPN non richiede una chiave di licenza.

Limitazioni

Small Community Network:

In caso di implementazione di sistemi IP Office in reti di tipo Small Community Network (SCN), è possibile configurare un servizio SSL VPN tra specifici nodi nella rete SCN e in AVG. Non è possibile utilizzare la connessione SSL VPN per accedere in remoto ad altri nodi nella topologia SCN: il servizio SSL VPN comunica solo con il sistema IP Office che corrisponde all'endpoint. È necessario configurare un servizio SSL VPN per ogni nodo nella rete SCN a cui si desidera accedere in remoto.

Certificati:

È possibile archiviare fino a 25 certificati nell'archivio dei certificati attendibili di IP Office.

Versione HTTP:

Se si utilizza un browser con una versione HTTP più recente della 1.1, è possibile che la connessione a un dispositivo utilizzando il servizio NAPT di SSL VPN non riesca. Nel caso di problemi di connessione a un dispositivo LAN, modificare le impostazioni del browser in modo da utilizzare HTTP versione 1.1.

Collegamenti correlati

Informazioni sul servizio SSL VPN alla pagina 9

Documentazione correlata

Per installare, configurare e amministrare la soluzione SSL VPN, è necessario fare riferimento alla documentazione per il sistema Avaya IP Office, Avaya VPN Gateway (AVG) e Avaya Identity Engines Ignition Server. È inoltre necessario fare riferimento alla documentazione resa disponibile da altri fornitori di supporto all'hardware e al software utilizzati nell'infrastruttura di rete.

Per il supporto della soluzione SSL VPN, disporre della documentazione Avaya indicata di seguito.

Avaya VPN Gatewaydocumentazione

- *Avaya VMware Getting Started Guide - Avaya VPN Gateway* (Guida introduttiva di Avaya VMWare per Avaya VPN Gateway) (NN46120-302)

- *Avaya VPN Gateway User Guide* (Guida per l'utente di Avaya VPN Gateway) (NN46120-104)
- *Avaya VPN Gateway Administration Guide* (Guida all'amministrazione di Avaya VPN Gateway) (NN46120-105)
- *Avaya VPN Gateway BBI Application Guide* (Guida all'applicazione BBI di Avaya VPN Gateway) (NN46120-102)
- *Avaya VPN Gateway CLI Application Guide* (Guida all'applicazione CLI di Avaya VPN Gateway) (NN46120-101)

Documentazione di Avaya IP Office

- *Avaya IP Office Basic Edition – Web Manager*
- *Avaya IP Office Manager*
- *Amministrazione di Voicemail Pro*
- *Installazione di Embedded Voicemail*

Documentazione di Avaya Identity Engines Ignition Server

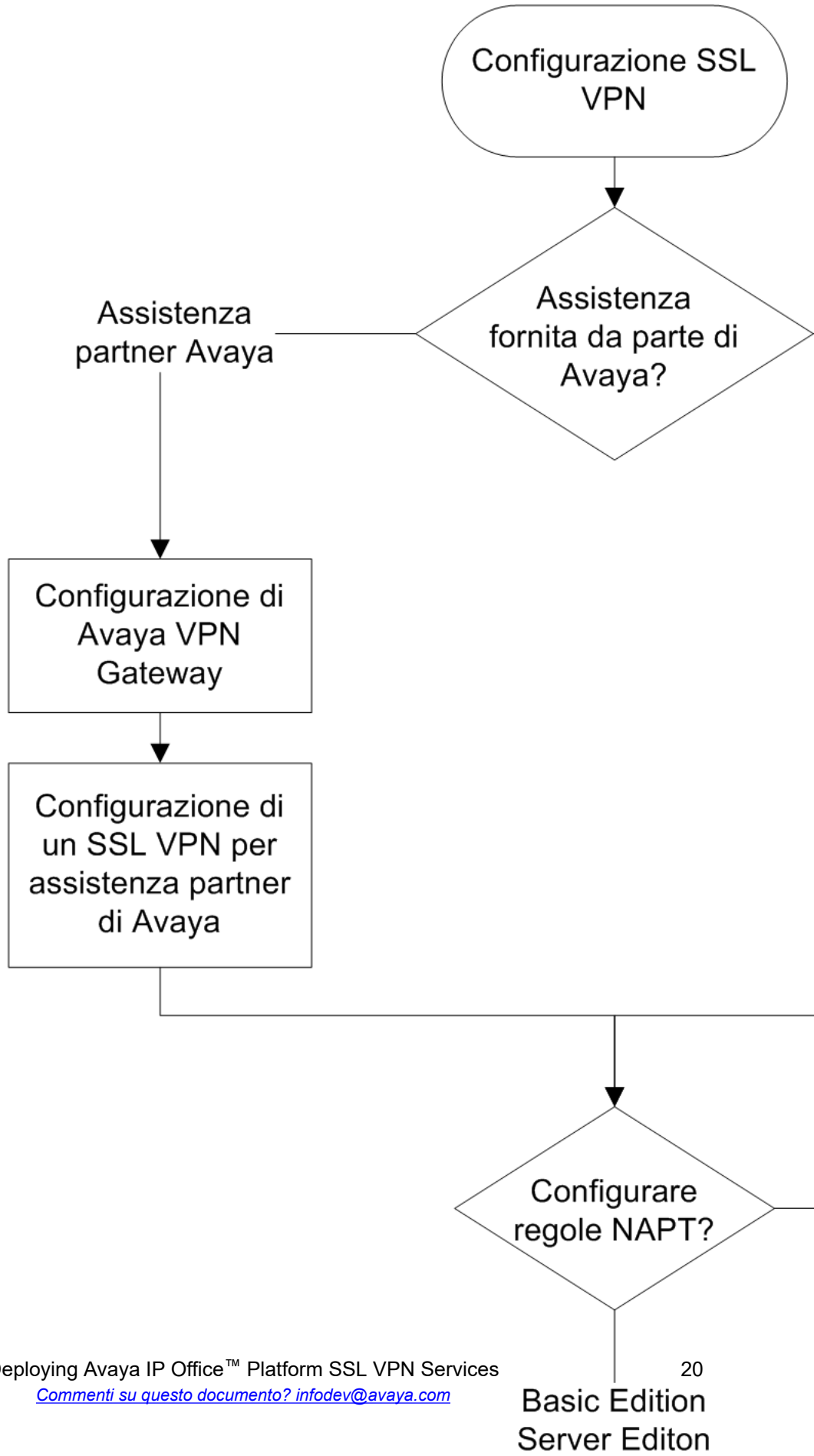
- *Avaya Identity Engines Ignition Server — Configuration Guide* (Guida alla configurazione di Avaya Identity Engines Ignition Server) (NN47280-500)

Collegamenti correlati

Informazioni sul servizio SSL VPN alla pagina 9

Capitolo 3: Flusso di lavoro per configurare un servizio SSL VPN

Il flusso di lavoro nelle pagine seguenti mostra la sequenza di attività da svolgere per configurare un servizio SSL VPN.


Configurazione SSL VPN
Assistenza fornita da parte di Avaya?
Assistenza partner Avaya
Configurazione di Avaya VPN Gateway
Configurazione di un SSL VPN per assistenza partner di Avaya
Configurare regole NAPT?
Basic Edition
Server Editon

Navigazione

- Configurazione di alla pagina 22
- Configurazione di un SSL VPN per assistenza di Avaya alla pagina 36
- Configurazione di un SSL VPN per assistenza partner di Avaya alla pagina 39
- Regole NAPT (Network Address and Port Translation) alla pagina 59
- Verifica della connessione tra e alla pagina 61

Capitolo 4: Configurazione di Avaya VPN Gateway

Per fornire servizi di supporto mediante la soluzione SSL VPN, i partner Avaya devono configurare Avaya VPN Gateway (AVG)

In questa sezione vengono fornite informazioni sulle attività che è necessario completare in caso di installazione e configurazione di AVG per supportare una connessione SSL VPN con un sistema IP Office.

Prima di configurare il sistema IP Office per un servizio SSL VPN, è necessario configurare l'infrastruttura a cui si connette il servizio. Questa sezione descrive la configurazione dell'interoperabilità tra AVG e un sistema IP Office. Per completare queste attività, è necessario fare riferimento alla documentazione per AVG, nonché alla documentazione resa disponibile da altri fornitori per il supporto dell'hardware e dell'software utilizzati nell'infrastruttura di rete.

In questo capitolo sono descritte le attività principali per distribuire Avaya VPN Gateway. Questi sono consigli generali. I dettagli esatti per la distribuzione possono variare a seconda dell'ambiente specifico del partner aziendale.

Collegamenti correlati

Pianificazione iniziale e configurazione alla pagina 22
Avaya VPN GatewayFlusso delle attività di configurazione alla pagina 23
Configurazione AVG di base alla pagina 25
Abilitazione dei servizi di accesso remoto alla pagina 26
Esecuzione della procedura guidata Net Direct alla pagina 26
Modifica dell'AVG predefinito per il servizio SSL VPN alla pagina 27
Configurazione dell'autenticazione locale alla pagina 29
Configurazione dell'autenticazione RADIUS alla pagina 30
Attributi di configurazione del server RADIUS alla pagina 32

Pianificazione iniziale e configurazione

Ambiente virtualizzato

Il client SSL VPN richiede che Avaya VPN Gateway (AVG) sia installato in un ambiente virtualizzato come server gateway VPN. Come ambienti virtuali sono supportati solo i server ESX

ed ESXi. I modelli di AVG sono tre: 3050–VM, 3070–VM e 3090–VM. Per le specifiche hardware di ogni modello, vedere *VMware Getting Started Guide, Avaya VPN Gateway* (Guida introduttiva di VMWare per Avaya VPN Gateway) (NN46120-302). È possibile scaricare la documentazione completa di AVG da http://support.avaya.com.

Ulteriori informazioni sui server VMware ESXi sono disponibile in http://www.vmware.com.

Configurazione con due schede di interfaccia di rete

Installare Avaya VPN Gateway (AVG) implementando una configurazione con due schede di interfaccia di rete (NIC), di cui deve essere dotato il server AVG. Assegnare un indirizzo IP statico a ogni NIC.

- La prima interfaccia gestisce il traffico privato ed è utilizzata come interfaccia di gestione.
- La seconda interfaccia gestisce l'accesso a Internet e il tunneling SSL VPN.

Software AVG

Sono due le opzioni per distribuire il software AVG.

- Distribuzione di dispositivi virtuali AVG
- CD-ROM di autoinstallazione

Per informazioni e procedure di installazione di AVG, vedere *VMware Getting Started Guide, Avaya VPN Gateway* (Guida introduttiva di VMWare per Avaya VPN Gateway) (NN46120-302).

PC dell'agente del servizio

Installare il PC dell'agente del servizio sulla rete privata e impostare il gateway predefinito sull'indirizzo IP dell'host Avaya VPN Gateway (AVG).

Dal PC dell'agente del servizio è possibile effettuare quanto segue:

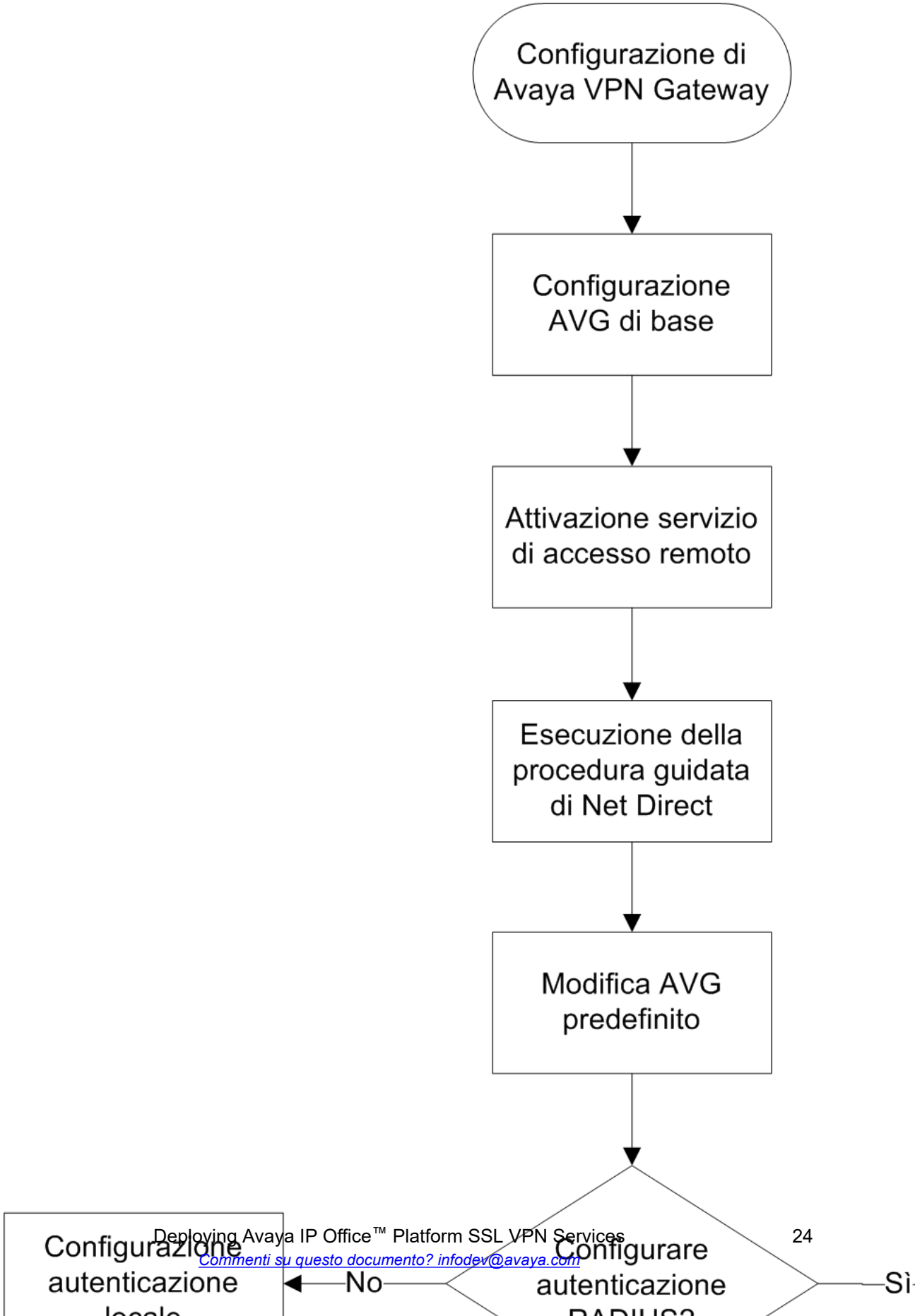
- Utilizzare l'IP dell'interfaccia di gestione per avviare un'interfaccia BBI (Browser Based Interface) o CLI (Command Line Interface) di gestione per configurare e monitorare AVG.
- Utilizzare l'indirizzo IP del tunneling SSL VPN IP per gestire e monitorare in remoto i sistemi IP Office.

Collegamenti correlati

Configurazione di Avaya VPN Gateway alla pagina 22

Avaya VPN GatewayFlusso delle attività di configurazione

Il flusso di attività seguente mostra la sequenza delle procedure da eseguire per configurare AVG.


Configurazione di Avaya VPN Gateway
Configurazione AVG di base
Attivazione servizio di accesso remoto
Esecuzione della procedura guidata di Net Direct
Modifica AVG predefinito
Configurare autenticazione
No
Sì
Configurazione autenticazione

Navigazione

Collegamenti correlati

Configurazione di Avaya VPN Gateway alla pagina 22

Configurazione AVG di base

Configurazione di AVG dal PC dell'agente del servizio

Quando si avvia per la prima volta VPN Gateway, viene visualizzato il menu **Configurazione**. Questo menu contiene il comando CLI **nuovo**. Questa è una configurazione guidata iniziale basata su CLI molto intuitiva per AVG che fornisce le impostazioni predefinite per stabilire rapidamente connessioni SSL da IP Office. È utile per la configurazione iniziale e i test. Inoltre, è il metodo più rapido per eseguire la configurazione iniziale di AVG. Successivamente, è possibile utilizzare l'interfaccia di gestione BBI per apportare le modifiche consigliate per la connettività del servizio SSL VPN. Per ulteriori informazioni, vedere *User Guide Avaya VPN Gateway* (Guida utente di Avaya VPN Gateway) (NN46120-104).

Dopo aver eseguito il comando "nuovo" per eseguire la configurazione rapida, vengono create le seguenti impostazioni:

- Un VPN. Di solito si definisce un VPN per accedere a una Intranet, a sue parti o a una Extranet.
- Un server SSL virtuale del tipo di portale. Viene assegnato un indirizzo IP del portale, al quale l'utente remoto deve connettersi per accedere al portale. Se si sceglie di utilizzare la funzione VPN senza un commutatore di applicazioni, il server del portale viene impostato in modalità autonoma (standalone).
- Un certificato di prova viene installato e mappato al server del portale.
- Il metodo di autenticazione è impostato sul database locale ed è configurato un utente di prova. Questo utente appartiene a un gruppo chiamato `trusted`, le cui regole di accesso consentono di accedere a tutte le reti, i servizi e i percorsi.
- Uno o più nomi di dominio vengono aggiunti all'elenco di ricerca DNS, in odo che l'utente remoto possa immettere un nome breve nei vari campi degli indirizzi del portale (ad esempio, "interno" invece di "interno.esempio.com" se esempio.com 'viene aggiunto all'elenco di ricerca).

- Se si sceglie di abilitare il reindirizzamento da HTTP a HTTPS, viene creato un ulteriori server di tipo HTTP per reindirizzare le richieste effettuate con HTTP a HTTPS, poiché il server del portale richiede una connessione SSL.

Una stampa delle impostazioni di configurazione esempio per il file di registro Configurazione rapida è disponibile nell'Appendice A: esempio di file di registro di configurazione rapida AVG alla pagina 92.

Collegamenti correlati

Configurazione di Avaya VPN Gateway alla pagina 22

Abilitazione dei servizi di accesso remoto

Oltre a usare la console VM locale per configurare il VPN, l'amministratore deve anche gestirlo utilizzando una sessione TELNET o SSH o mediante l'interfaccia BBI. Per consentire la configurazione remota del gateway VPN, è necessario abilitare i servizi di accesso remoto.

Eseguire questa procedura mediante l'interfaccia CLI. Consultare i seguenti documenti di AVG:

- *Command Reference Avaya VPN Gateway (Riferimento per i comandi di Avaya VPN Gateway)*
- *CLI Application Guide (Guida all'applicazione CLI di Avaya VPN Gateway)*

Procedura

1. Accedere a AVG.
2. Immettere i seguenti comandi.

```
/cfg/sys/adm/.
        telnet on
        ssh on
/cfg/sys/adm/https/.
        cert 1
        ena true
/cfg/sys/adm/http/.
        ena true
apply
```

Collegamenti correlati

Configurazione di Avaya VPN Gateway alla pagina 22

Esecuzione della procedura guidata Net Direct

La procedura guidata Net Direct consente di creare nel portale un collegamento che consente di scaricare e avviare una versione semplificata di Avaya VPN Client, ovvero il client Net Direct. Eseguire la procedura guidata Net Direct dall'interfaccia di gestione BBI. Vedere *Avaya VPN Gateway BBI Application Guide* (Guida all'applicazione BBI di Avaya VPN Gateway).

Procedura

1. Accedere all'interfaccia BBI di AVG.

   Selezionare **Wizards** (Procedure guidate) nel riquadro di navigazione di sinistra.
2. Fare clic su **Net Direct Wizard** (Procedura guidata Net Direct).
3. Nella pagina **Net Direct settings for the selected VPN** (Impostazioni Net Direct per il VPN selezionato), selezionare il pulsante di opzione **Enable Net Direct for this VPN** (Abilita Net Direct per questo VPN).
4. Nella pagina **Default IP Pool Settings** (Impostazioni del pool IP predefinito):
   - Per **Default IPPool** (Pool IP predefinito), selezionare **Local_pool**.
   - Immettere l'indirizzo IP più basso e quello più alto per l'intervallo del pool.

Collegamenti correlati

Configurazione di Avaya VPN Gateway alla pagina 22

Modifica dell'AVG predefinito per il servizio SSL VPN

Dopo aver eseguito la configurazione rapida e la configurazione guidata per Net Direct, è necessario modificare la configurazione predefinita in modo che supporti una connessione SSL VPN con un sistema IP Office.

Eseguire questa procedura mediante l'interfaccia BBI basata sul browser di AVG. Vedere *Avaya VPN Gateway BBI Application Guide* (Guida all'applicazione BBI di Avaya VPN Gateway).

Questa procedura è duplicata in Appendice B: Modifica dell'AVG predefinito per il servizio SSL VPN (con schermate) alla pagina 97. Questa versione della procedura include alcune schermate dell'interfaccia utente.

Prerequisiti

Assicurarsi che il gateway predefinito configurato in AVG soddisfi le richieste ICMP. Se il gateway predefinito non risponde alle richieste ICMP, AVG non può fornire i servizi VPN.

Procedura

1. Accedere all'interfaccia BBI di AVG come amministratore.
2. Nel riquadro di navigazione di sinistra, selezionare la scheda **Config** (Configurazione), quindi **VPN Gateway** > **VPN1** > **IP Pool** (Pool IP).
3. Il VPN predefinito della configurazione di base di AVG potrebbe già contenere un pool locale. In caso contrario, è necessario aggiungerne uno al VPN predefinito. Nella pagina **Add new IP Address Pool** (Aggiungi nuovo pool di indirizzi IP), aggiungere un pool locale al VPN predefinito.

4. Nella pagina **Modify IP Address Pool** (Modifica pool di indirizzi IP), verificare che i valori nei campi **Lower IP** (IP più basso) e **Upper IP** (IP più alto) corrispondano a quelli impostati con la configurazione guidata di Net Direct.
5. Nella pagina **IP Pool (Pool IP)** > **Network Attributes Settings (Impostazioni attributi di rete)**, selezionare la scheda **Network Attributes** (Attributi di rete) e immettere i valori per la rete in uso.
6. Nella pagina **IP Pool** (Pool IP), impostare **Default IP Pool** (Pool IP predefinito) sul pool locale creato nel passo 3.
7. Nella pagina **Net Direct Client Access Settings** (Impostazioni di accesso al client Net Direct), verificare le impostazioni create dalla configurazione guidata di Net Direct.
   - Assicurarsi che **Idle Check** (Controllo inattività) sia impostato su **off** (disattivato).
   - Assicurarsi che sia impostato il banner Net Direct.
8. Impostare il collegamento del portale per avviare il client Net Direct. Nella pagina **Portal Linkset Configuration** (Configurazione set di collegamenti del portale), selezionare la scheda **Portal Link** (Collegamento portale). Nel campo **Link Type** (Tipo di collegamento), selezionare **Net Direct**.
9. Nella pagina **Networks for Split Tunnels** (Reti per split tunneling):
   - impostare **Split Tunnel Mode** (Modalità split tunneling) su **enabled** (abilitata);
   - impostare gli instradamenti di split tunneling in modo da raggiungere l'agente del servizio sulla rete privata
10. Per VPN1, accedere alla pagina dei gruppi e selezionare **Group1** (Gruppo 1). Nella pagina **Modify a Group** (Modifica un gruppo), impostare il pool di IP su quello locale creato al punto 3.
11. Accedere alla pagina **VPN1** > **Group1 (Gruppo 1)** > **Access Lists (Elenchi di accesso)**. Nella pagina **Firewall Access List** (Elenco di accesso al firewall), creare una regola di accesso, qualora non sia già stata creata per impostazione predefinita.
12. Accedere alla pagina **VPN1** > **SSL**. Nella pagina **Server Settings** (Impostazioni server), alla sezione **SSL Settings** (Impostazioni SSL) impostare **Ciphers** (Cifrature) su **AES256-SHA** per avere una codifica molto sicura.
13. Accedere alla pagina **VPN1** > **Authorization (Autorizzazione)** > **Services (Servizi)**. Rimuovere tutti i servizi impostati nella configurazione predefinita, poiché non sono richiesti dal servizio SSL VPN.
14. Accedere alla pagina **VPN1** > **Authorization (Autorizzazione)** > **Networks (Reti)**. Impostare la subnet della rete di autorizzazione alla quale viene fatto riferimento in una delle regole di accesso impostata in **VPN1** > **Group1 (Gruppo 1)** > **Access Lists (Elenchi di accesso)**.

Nota:

I controlli delle impostazioni del servizio SSL VPN effettuano il tunneling della comunicazione intermedia. La comunicazione viene attivata solo specificando un

elenco numero autorizzati delle reti "intranet". La comunicazione del client Inter-VPN è bloccata per impostazione predefinita.

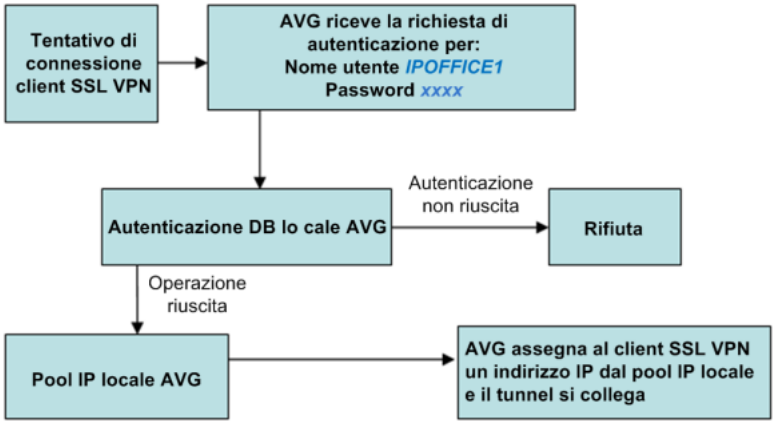
15. Accedere alla pagina **VPN1** > **General Settings (Impostazioni generali)** > **Session (Sessione)**. Impostare **Session Idle Time** (Tempo di inattività sessione) su 2 minuti.

Collegamenti correlati

[Configurazione di Avaya VPN Gateway](#) alla pagina 22

Configurazione dell'autenticazione locale

Nel caso di un numero ridotto di sistemi IP Office, è possibile utilizzare il database locale di Avaya VPN Gateway (AVG) per creare i dati utente necessari per l'autenticazione. In questo modo è possibile configurare rapidamente l'autenticazione se non sono disponibili server di autenticazione RADIUS esterni. Configurare un pool di IP per assegnare in modo dinamico gli indirizzi IP agli utenti locali. L'immagine in basso mostra il flusso di autenticazione del client SSL VPN e la modalità di allocazione degli indirizzi del pool IP.



Questa procedura descrive i passi manuali per configurare l'autenticazione locale. In alternativa, è possibile configurare l'autenticazione utilizzando la procedura guidata di autenticazione di AVG.

Procedura

1. Per **VPN1**, accedere alla pagina **IP Pool Configuration** (Configurazione pool IP) e aggiungere un pool di IP locale.
2. Accedere a **VPN1** > **IP Pool (Pool IP)** > **Add/Modify (Aggiungi/modifica)**. Impostare l'intervallo dinamico del pool di IP immettendo i valori nei campi **Lower IP** (IP più basso) e **Upper IP** (IP più alto).
3. Accedere a **VPN1** > **IP Pool (Pool IP)** > **Network Attribute (Attributo di rete)**. Impostare il valore per **Client Netmask** (Maschera di rete client).
4. Nella pagina **Add a Group** (Aggiungi un gruppo), aggiungere un nuovo gruppo al VPN1.

5. Accedere a **VPN1** > **<nome_gruppo>** > **Modify Group (Modifica gruppo)**. Selezionare la scheda **General** (Generale) e assegnare un pool locale a gruppo selezionandolo nel campo **IP Pool** (Pool IP).
6. Selezionare la scheda **Access Lists** (Elenchi di accesso) e specificare l'elenco di accesso per il gruppo di utenti locale.
7. Selezionare la scheda **Linksets** (Set di collegamenti) e assegnare i set di collegamenti.
8. Modificare le impostazioni di autenticazione VPN. Nella pagina **Authentication Servers** (Server di autenticazione), aggiungere un nuovo server di autenticazione.
9. Accedere a **VPN1** > **<nome_server_autenticazione>** > **Add/Modify Users (Aggiungi/modifica utenti)** e aggiungere gli utenti al gruppo.
10. Modificare il server di autenticazione e specificare il valore per **Authentication Order** (Ordine di autenticazione).

Collegamenti correlati

Configurazione di Avaya VPN Gateway alla pagina 22

Configurazione dell'autenticazione RADIUS

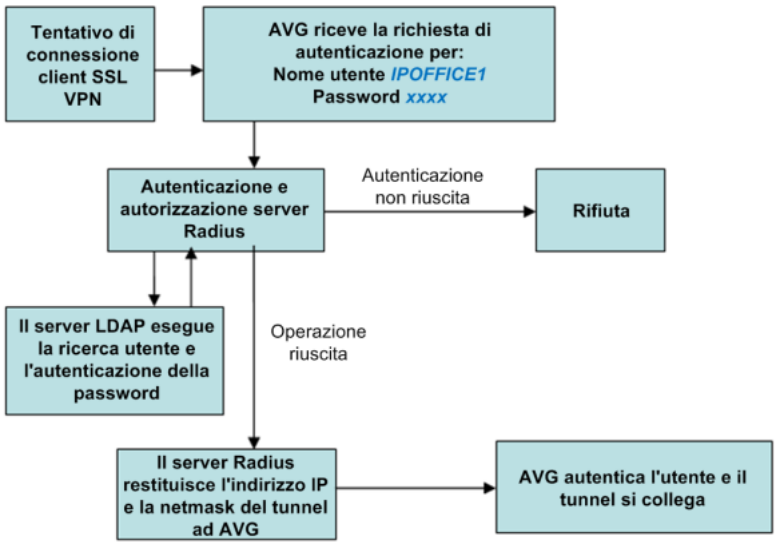
Il vantaggio maggiore dell'autenticazione RADIUS è che al servizio SSL VPN viene sempre assegnato lo stesso indirizzo IP per il tunneling.

Per configurare l'autenticazione RADIUS, è necessario installare un server RADIUS. Avaya consiglia di utilizzare Avaya Identity Engine per un server RADIUS. Per informazioni e modalità di scaricamento del software, accedere a http://support.avaya.com.

Le informazioni di autenticazione del protocollo RADIUS, ad esempio dati dell'account utente e informazioni di tunneling SSL VPN come indirizzo IP e maschera di rete, devono essere memorizzate in un database. Sono disponibili due opzioni:

- Utilizzare il database locale di Identity Engine per memorizzare le informazioni utente e fornire i servizi di ricerca e autenticazione e autorizzazione. Questa opzione è ideale nel caso di un numero ridotto di utenti. Identity Engine dispone di un numero limitato di utenti. Consultare la documentazione per conoscere il valore esatto.
- Utilizzare un server LDAP per memorizzare le credenziali utente e le informazioni di tunneling SSL VPN per i servizi di ricerca e autenticazione. Questa opzione è ideale per scenari di distribuzione con un ampio numero di utenti.

Per un'installazione con server LDAP, la documentazione di Avaya Identity Engine per server RADIUS contiene le opzioni per configurare i server LDAP di vari produttori. L'autenticazione RADIUS mediante server LDAP è descritta nella figura in basso. La configurazione con server RADIUS descritta in questa procedura non richiede un server LDAP.



Questa procedura descrive i passi manuali per configurare l'autenticazione RADIUS. In alternativa, è possibile configurare l'autenticazione utilizzando la procedura guidata di autenticazione di AVG.

Questa procedura è duplicata nell'Appendice C: Configurazione autenticazione RADIUS (con schermate) alla pagina 103. Questa versione della procedura include alcune schermate dell'interfaccia utente.

Procedura

1. Accedere all'interfaccia BBI di AVG come amministratore.
2. Nella pagina **IP Pool Configuration** (Configurazione pool IP), aggiungere un nuovo pool di indirizzi IP per l'autenticazione RADIUS.
3. Nella pagina **IP Pool** (Pool IP), impostare **Default IP Pool** (Pool IP predefinito) sul pool di indirizzi IP per l'autenticazione RADIUS creato nel passo 2.
4. Modificare il VPN. Nella pagina **Authentication Servers (Server di autenticazione)** > **Add New Authentication Server (Aggiungi nuovo server di autenticazione)**, compilare i campi per il server RADIUS.
5. Configurare le impostazioni del server di autenticazione RADIUS. L'ID produttore 1872 è associato ad Alteon e identifica AVG. Selezionare la scheda **Settings** (Impostazioni) e compilare i seguenti campi.
   - **ID produttore: 1872**
   - **Tipo di produttore: 1**
   - **Timeout: 10**
   - **ID produttore per ID VPN: 1872**
   - **Tipo di produttore per ID VPN: 3**
6. Configurare gli attributi di rete RADIUS. Selezionare la scheda **Network Attributes** (Attributi di rete) e compilare i seguenti campi.

Impostazioni ID produttore	Impostazioni tipo di produttore
Indirizzo IP client: 1872	Indirizzo IP client: 4
Maschera di rete client: 1872	Maschera di rete client: 5
Server NBNS primario: 1872	Server NBNS primario: 6
Server NBNS secondario: 1872	Server NBNS secondario: 7
Server DNS primario: 1872	Server DNS primario: 8

7. Configurare gli attributi di filtro. Selezionare la scheda Attributi di filtro e compilare i seguenti campi.
   - **Attributo di filtro RADIUS: disabilitato**
   - **ID produttore per attributo di filtro: 9**
   - **Tipo di produttore per attributo di filtro: 1**
8. Specificare l'indirizzo del server RADIUS. Selezionare la scheda **Servers** (Server) nella pagina **RADIUS Servers** (Server RADIUS).
9. Fare clic su **Add** (Aggiungi) e immettere nella pagina **Modify RADIUS Server** (Modifica server RADIUS) l'indirizzo IP del server RADIUS e il segreto condiviso.
10. Selezionare la scheda **Authentication Order** (Ordine di autenticazione) e specificare l'ordine desiderato per i metodi di autenticazione.

Collegamenti correlati

Configurazione di Avaya VPN Gateway alla pagina 22

Attributi di configurazione del server RADIUS

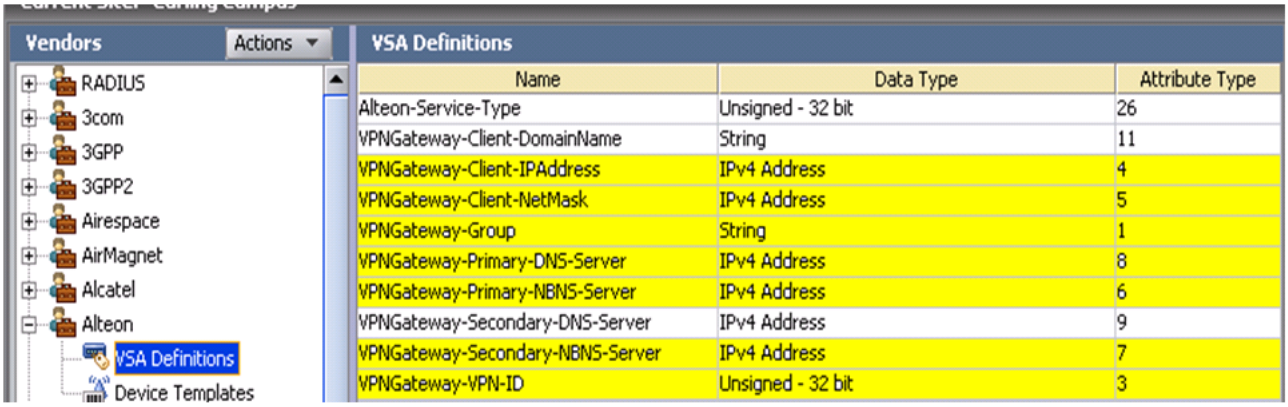
Il servizio SSL VPN richiede un server RADIUS. È consigliabile utilizzare Avaya Identity Engines Ignition Server come server RADIUS.

In fase di connessione del servizio SSL VPN, Avaya VPN Gateway (AVG) autentica il sistema IP Office inviando una query a un server RADIUS esterno. In questa sezione vengono elencati gli attributi che è necessario configurare nel server RADIUS.

Mappatura degli attributi del server RADIUS

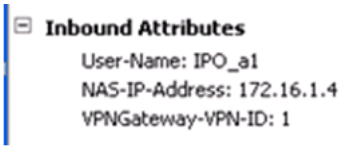
L'elenco riportato di seguito contiene i nomi degli attributi RADIUS specifici dei produttori oltre ai tipi di dati associati e ai codici di tipo di produttore Alteon (AVG).

Gli esempi seguenti sono stati ottenuti utilizzando un server RADIUS Avaya Identity Engines. Gli attributi evidenziati sono stati configurati come **Attributi di rete** e **Impostazioni** nella configurazione del server RADIUS AVG.



Name	Data Type	Attribute Type
Alteon-Service-Type	Unsigned - 32 bit	26
VPNGateway-Client-DomainName	String	11
VPNGateway-Client-IPAddress	IPv4 Address	4
VPNGateway-Client-NetMask	IPv4 Address	5
VPNGateway-Group	String	1
VPNGateway-Primary-DNS-Server	IPv4 Address	8
VPNGateway-Primary-NBNS-Server	IPv4 Address	6
VPNGateway-Secondary-DNS-Server	IPv4 Address	9
VPNGateway-Secondary-NBNS-Server	IPv4 Address	7
VPNGateway-VPN-ID	Unsigned - 32 bit	3

• Di seguito sono indicati gli attributi in entrata provenienti da AVG e diretti al server RADIUS durante una richiesta di autenticazione.



Gli attributi RADIUS inviati da AVG sono i seguenti:

- NAS-IP-Address (attributo RADIUS generico) è l'indirizzo IP di AVG.
- User-Name (attributo RADIUS generico) è il nome dell'account utente.
- VPNGateway-VPN-ID è un attributo Alteon.

Il server RADIUS IDEngine ha una mappatura predefinita di attributi interni per gli attributi RADIUS più comuni, indicati nella tabella in basso. Le righe evidenziate corrispondono agli attributi RADIUS contenuti nella richiesta in alto.

Inbound Attributes

Name	Vendor	Attribute Mapping
Inbound-Digest-Auth-Param	RADIUS	Digest-Auth-Param
Inbound-Digest-Domain	RADIUS	Digest-Domain
Inbound-Digest-Method	RADIUS	Digest-Method
Inbound-Digest-Nonce-Count	RADIUS	Digest-Nonce-Count
Inbound-Digest-Opaque	RADIUS	Digest-Opaque
Inbound-Digest-Qop	RADIUS	Digest-Qop
Inbound-Digest-Realm	RADIUS	Digest-Realm
Inbound-Digest-SIP-AOR	RADIUS	Digest-SIP-AOR
Inbound-Digest-URI	RADIUS	Digest-URI
Inbound-Digest-Username	RADIUS	Digest-Username
Inbound-Framed-Compression	RADIUS	Framed-Compression
Inbound-Framed-Interface-Id	RADIUS	Framed-Interface-Id
Inbound-Framed-IP-Address	RADIUS	Framed-IP-Address
Inbound-Framed-IP-Netmask	RADIUS	Framed-IP-Netmask
Inbound-Framed-MTU	RADIUS	Framed-MTU
Inbound-Framed-Pool	RADIUS	Framed-Pool
Inbound-Framed-Protocol	RADIUS	Framed-Protocol
Inbound-Login-IP-Host	RADIUS	Login-IP-Host
Inbound-NAS-Identifier	RADIUS	NAS-Identifier
Inbound-NAS-IP-Address	RADIUS	NAS-IP-Address
Inbound-NAS-Port	RADIUS	NAS-Port
Inbound-NAS-Port-Id	RADIUS	NAS-Port-Id
Inbound-NAS-Port-Type	RADIUS	NAS-Port-Type
Inbound-Port-Limit	RADIUS	Port-Limit
Inbound-Service-Type	RADIUS	Service-Type
Inbound-Tunnel-Client-Auth-Id	RADIUS	Tunnel-Client-Auth-Id
Inbound-Tunnel-Client-Endpoint	RADIUS	Tunnel-Client-Endpoint
Inbound-Tunnel-Medium-Type	RADIUS	Tunnel-Medium-Type
Inbound-Tunnel-Preference	RADIUS	Tunnel-Preference
Inbound-Tunnel-Private-Group-Id	RADIUS	Tunnel-Private-Group-Id
Inbound-Tunnel-Server-Auth-Id	RADIUS	Tunnel-Server-Auth-Id
Inbound-Tunnel-Server-Endpoint	RADIUS	Tunnel-Server-Endpoint
Inbound-Tunnel-Type	RADIUS	Tunnel-Type
Inbound-User-Name	RADIUS	User-Name

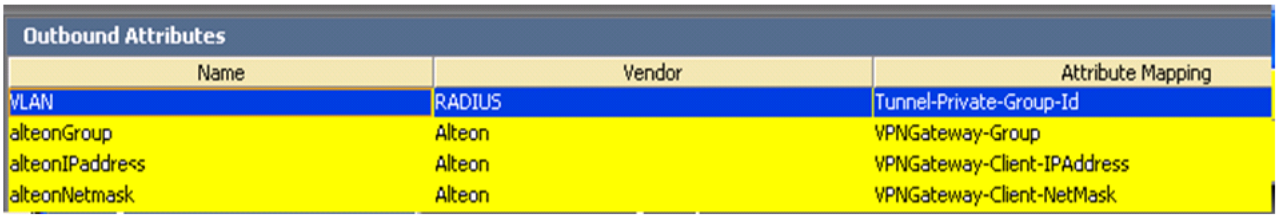
I server RADIUS valutano gli attributi in entrata mediante regole di autorizzazione. La regola può utilizzare un attributo in entrata per controllare una condizione specifica o può restituire l'attributo in entrata in una risposta RADIUS come valore in uscita. Se un attributo in entrata inviato da AVG deve essere valutato, ma non fa parte del set predefinito del server RADIUS, deve essere definito come nuovo attributo in entrata nel server RADIUS. Per esempi delle regole di autenticazione vedere *IDEngine Administration* (Amministrazione di IDEngine).

• Di seguito sono riportati gli attributi in uscita inviati da AVG al server RADIUS durante l'autenticazione:

Outbound Attributes

alteonNetmask (VPNGateway-Client-NetMask): 255.255.0.0
alteonGroup (VPNGateway-Group): IPoffice
alteonIPaddress (VPNGateway-Client-IPAddress): 10.1.0.1

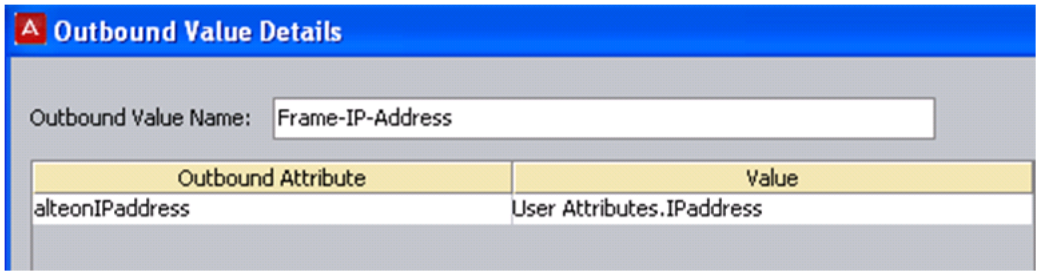
Gli attributi in uscita sono i campi di dati utilizzati dal server RADIUS per trasportare i dati di provisioning a VPN Gateway. Gli attributi in uscita sono attributi di protocollo RADIUS generici o specifici dei produttori. Come nel caso degli attributi in entrata, quelli in uscita devono essere creati qualora non facciano parte del set predefinito del server RADIUS. Nell'esempio in alto, i tra attributi in uscita Alteon (specifici per AVG) “alteonGroup”, “alteonIPaddress” e “alteonNetmask” devono essere creati nel server RADIUS, come descritto nell'esempio in basso.



Outbound Attributes

Name	Vendor	Attribute Mapping
VLAN	RADIUS	Tunnel-Private-Group-Id
alteonGroup	Alteon	VPNGateway-Group
alteonIPaddress	Alteon	VPNGateway-Client-IPAddress
alteonNetmask	Alteon	VPNGateway-Client-NetMask

Gli attributi in uscita possono essere impostati su valori statici o essere mappati ad attributi utente nel database locale del server RADIUS o in un repository LDAP. Di seguito è riportato un esempio di valore di attributo in uscita mappato a un attributo utente di database:



Outbound Value Details

Outbound Value Name: Frame-IP-Address

Outbound Attribute	Value
alteonIPaddress	User Attributes.IPaddress

I valori in uscita sono associati a regole di autenticazione e sono inviati a VPN Gateway come attributi RADIUS al momento della valutazione della regola. Se la regola viene accettata (“Allow”), i valori in uscita vengono utilizzati per impostare varie caratteristiche della sessione dell'utente. Se la regola non viene accettata (“Deny”), i valori in uscita restituiti vengono usati, di solito, per fornire informazioni sulla causa del rifiuto. Per ulteriori informazioni, consultare la documentazione di IDEngine.

Collegamenti correlati

Configurazione di Avaya VPN Gateway alla pagina 22

Capitolo 5: Configurazione di un servizio SSL VPN per il supporto Avaya

Questa sezione fornisce informazioni sul processo di configurazione per IP Office nel caso in cui il fornitore del servizio sia Avaya. È possibile configurare automaticamente il servizio SSL VPN utilizzando il processo di On-Boarding.

È possibile configurare più istanze del servizio SSL VPN ed eseguirle contemporaneamente.

Prerequisiti

In caso di configurazione di un servizio SSL VPN, l'indirizzo del gateway VPN può essere un nome di dominio completo (FQDN). Per risolvere indirizzi FQDN, è necessario configurare il server DNS. Configurare le impostazioni DSN nel modulo **Sistema** di IP Office Manager, all'interno di **DNS**.

Collegamenti correlati

Configurazione di un servizio SSL VPN mediante un file di On-Boarding alla pagina 36
Utilizzo del file di On-Boarding per modificare un servizio esistente alla pagina 37

Configurazione di un servizio SSL VPN mediante un file di On-Boarding

Il file XML di On-Boarding viene reso disponibile da Avaya. Contiene le impostazioni necessarie per stabilire un tunnel protetto tra IP Office e un server AVG. In fase di importazione del file XML di On-Boarding, vengono applicate le impostazioni e viene installato uno o più certificati TLS.

Se si configura il servizio SSL VPN in un nuovo sistema, generare in primo luogo un file inventario del sistema IP Office. In fase di registrazione del sistema IP Office, il file di inventario generato verrà caricato in GRT e i dati di inventario verranno popolati nel database Avaya Customer Support (ACS). Una volta abilitato il supporto remoto, sarà possibile scaricare il file XML di On-Boarding dal sito Web GRT e caricarlo nel sistema IP Office.

Il processo di On-Boarding configura quanto segue:

- Configurazione del servizio SSL VPN
- Codici funzione per abilitare e disabilitare il servizio SSL VPN
- Trap di allarmi SNMP

- Uno o più certificati TLS nell'archivio dei certificati attendibili di IP Office

Eseguire questa procedura utilizzando il client IP Office Web Manager di Avaya.

Avvertenza:

Il processo di On-Boarding crea automaticamente un servizio SSL VPN nella configurazione del sistema quando il file di On-Boarding viene caricato nel sistema. Fare attenzione a non eliminare o modificare questo servizio se non espressamente indicato da Avaya.

Prerequisiti

Prima di iniziare, è necessario disporre dei codici hardware e della descrizione di catalogo del sistema IP Office. Ad esempio, "IP OFFICE 500 VERSION 2 CONTROL UNIT TAA" rappresentano il codice hardware e la descrizione di catalogo.

Procedura

1. Selezionare **Strumenti > On-Boarding**.

   Verrà visualizzata la finestra di dialogo On-Boarding.
2. Se il codice hardware per il sistema IP Office termina con le lettere TAA, selezionare la casella di controllo accanto al prompt **Si sta utilizzando un hardware serie TAA?**
3. Fare clic su **Ottieni file archivio** per generare un inventario del sistema IP Office.
4. Fare clic su **Registra IP Office**.

   Verrà visualizzato il sito GRT in un browser.
5. Accedere al sito Web e immettere i dati richiesti per il sistema IP Office.
6. Selezionare **Remote Support** (Supporto remoto) per il sistema IP Office.
7. Fare clic su **Download** e salvare il file di On-Boarding.
8. Passare al percorso in cui è stato salvato il file di On-Boarding e fare clic su **Carica**.

   Verrà visualizzato un messaggio di conferma dell'installazione del file di On-Boarding.

Collegamenti correlati

Configurazione di un servizio SSL VPN per il supporto Avaya alla pagina 36

Utilizzo del file di On-Boarding per modificare un servizio esistente

È possibile utilizzare il file di On-Boarding per configurare il servizio SSL VPN. Il file di On-Boarding contiene le impostazioni necessarie per stabilire un tunnel protetto tra IP Office e un server AVG. Attenersi alla procedura indicata di seguito se si è già configurato il servizio SSL VPN in un sistema IP Office e si necessita di aggiornare o modificare la configurazione SSL VPN.

Eseguire questa procedura nell'interfaccia di Avaya IP Office Web Manager.

Prerequisiti

Prima di iniziare, è necessario disporre dei codici hardware e della descrizione di catalogo del sistema IP Office. Ad esempio, "IP OFFICE 500 VERSION 2 CONTROL UNIT TAA" rappresentano il codice hardware e la descrizione di catalogo.

Procedura

1. Selezionare **Strumenti > On-Boarding**.

   Verrà visualizzata la finestra di dialogo On-Boarding.

2. Questa fase è opzionale. Per generare un inventario del sistema IP Office, attenersi alla procedura seguente:

   - Se il codice hardware per il sistema IP Office termina con le lettere TAA, selezionare la casella di controllo accanto al prompt **Si sta utilizzando un hardware serie TAA?**
   - Fare clic su **Ottieni file archivio**.

3. Fare clic su **Modifica**.

   Verrà visualizzato il sito Web Avaya in un browser.

4. Accedere al sito Web.

   Verrà visualizzata la pagina di connettività remota e gestione password di IP Office.

5. Fare clic su **Existing IP Office SSL VPN Remote Connectivity** (Connettività remota SSL VPN IP Office esistente).

6. Selezionare **Regenerate on-boarding file (existing properties)** (Rigenera file On-Boarding (proprietà esistente)).

7. Immettere il nome del servizio e il nome dell'account SSL VPN nei campi appropriati.

8. Fare clic su **Submit** (Invia).

9. Selezionare se si desidera ricevere il file di On-Boarding aggiornato tramite posta elettronica oppure scaricare il file aggiornato e seguire i prompt visualizzati.

10. Una volta scaricato o ricevuto il file di On-Boarding aggiornato, salvarlo nel sistema locale.

11. Passare al percorso in cui è stato salvato il file di On-Boarding e fare clic su **Carica** nell'interfaccia di Web Manager.

    Verrà visualizzato un messaggio di conferma dell'installazione del file di On-Boarding.

Collegamenti correlati

Configurazione di un servizio SSL VPN per il supporto Avaya alla pagina 36

Capitolo 6: Configurazione di un servizio SSL VPN per il supporto di partner Avaya

I fornitori di servizi di terze parti possono utilizzare Avaya VPN Gateway per fornire il supporto remoto ai clienti tramite la tecnologia SSL VPN di IP Office.

Per il supporto di fornitori terzi del servizio, il servizio SSL VPN può essere configurato manualmente utilizzando l'applicazione Manager. È possibile configurare un sistema con modalità Standard o Server Edition. La configurazione manuale non è supportata in modalità Basic Edition.

È possibile configurare più istanze del servizio SSL VPN ed eseguirle contemporaneamente.

Prerequisiti

In caso di configurazione di un servizio SSL VPN, l'indirizzo del gateway VPN può essere un nome di dominio completo (FQDN). Per risolvere indirizzi FQDN, è necessario configurare il server DNS. Configurare le impostazioni DNS nel modulo **Sistema** di IP Office Manager, all'interno di **DNS**.

Procedure di configurazione di un servizio SSL VPN per il supporto di partner Avaya

L'elenco seguente mostra la sequenza di procedure da eseguire per configurare un servizio SSL VPN per il supporto di partner.

- Configurazione del servizio SSL VPN alla pagina 40
- Installazione di un certificato alla pagina 42
- Configurazione di codici funzione alla pagina 43
- Configurazione di notifiche di allarme alla pagina 47
- Configurazione di un instradamento statico alla pagina 51
- Verifica della connessione con alla pagina 61
- Invio di un allarme di test alla pagina 63

Collegamenti correlati

Configurazione del servizio SSL VPN alla pagina 40
Installazione di un certificato alla pagina 42
Configurazione di codici funzione alla pagina 43
Configurazione di notifiche di allarme alla pagina 47
Configurazione di un instradamento statico alla pagina 51

Configurazione del servizio SSL VPN

Attenersi alla procedura indicata di seguito per configurare il servizio SSL VPN.

Eseguire questa procedura nell'interfaccia di Manager. In caso di configurazione di un sistema Server Edition, utilizzare la modalità IP Office Manager for Server Edition.

Prerequisiti

È necessario conoscere il valore delle seguenti variabili di configurazione.

Tabella 1: Scheda Servizio

Variabile	Descrizione
Nome del servizio	Immettere un nome per il nuovo servizio SSL VPN.
Nome account	Immettere il nome account del servizio SSL VPN. Il nome account viene utilizzato per l'autenticazione del servizio SSL VPN durante la connessione ad AVG. **Sistemi Server Edition:** In caso di configurazione di un sistema Server Edition, è consigliabile configurare lo stesso nome per l'account del servizio SSL VPN è l'ID dispositivo dell'agente SNMP. Se queste impostazioni corrispondono, il personale del supporto tecnico può utilizzare queste informazioni per identificare l'indirizzo del tunnel SSL VPN. È possibile configurare un solo ID dispositivo dell'agente SNMP per sistema. Se si configurano più istanze del servizio SSL VPN, scegliere uno dei nomi account del servizio SSL VPN che corrisponda all'ID dispositivo dell'agente SNMP in base alle esigenze di supporto tecnico remoto. È inoltre possibile visualizzare l'ID dispositivo selezionando **Rete** dall'elenco di navigazione e scegliendo un sistema Server Edition. Verrà visualizzato un riepilogo delle impostazioni per il sistema selezionato.
Password account	Immettere la password per l'account del servizio SSL VPN.
Conferma password	Confermare la password per l'account del servizio SSL VPN.
Indirizzo server	Immettere l'indirizzo del gateway VPN. Può trattarsi di un indirizzo FQDN o IPv4.
Tipo di server	Selezionare AVG.
Numero porta server	Selezionare un numero di porta. Il numero di porta predefinito è 443.

Tabella 2: Scheda Sessione

Variabile	Descrizione
Protocollo trasferimento dati preferito	Selezionare TCP. Si tratta del protocollo utilizzato dal servizio SSL VPN per il trasporto di dati. Se si seleziona UDP come protocollo durante la configurazione della connessione, UDP verrà visualizzato in questo campo, ma il servizio SSL VPN tornerà a utilizzare il protocollo TCP.
Intervallo di Heartbeat	Immettere la lunghezza dell'intervallo tra i messaggi heartbeat in secondi. Il valore predefinito è 30 secondi.
Nuovi tentativi Heartbeat	Immettere il numero di messaggi heartbeat non riconosciuti inviati da IP Office a AVG prima di determinare che AVG non risponde. Se viene raggiunto il numero di messaggi heartbeat consecutivi senza essere riconosciuti da AVG, IP Office termina la connessione. L'impostazione predefinita è 4.
Intervallo di riconnessione in caso di guasto	Intervallo di attesa prima che il servizio SSL VPN tenti di ristabilire una connessione con AVG. L'intervallo inizia quando il tunnel SSL VPN è operativo ed effettua un tentativo non riuscito di connessione ad AVG oppure quando viene persa la connessione con AVG. L'impostazione predefinita è 60 secondi.

Procedura

1. Nell'elenco di navigazione fare clic con il pulsante destro del mouse su **Servizio**.
2. Scegliere **Nuovo** > **Servizio SSL VPN**.
3. Nella scheda **Servizio** configurare le impostazioni elencate nella tabella di seguito.
4. Selezionare la scheda **Sessione** e configurare le impostazioni elencate nella tabella di seguito.
5. Selezionare la scheda **Fallback** e scegliere una delle opzioni seguenti:
   - Per abilitare il servizio e stabilire una connessione SSL VPN, verificare che l'opzione **In fallback** sia deselezionata
   - Per configurare il servizio senza stabilire una connessione SSL VPN, selezionare l'opzione **In fallback**
6. Fare clic su **OK**.
7. Per salvare la configurazione, fare clic sull'icona **Salva**.

Collegamenti correlati

Configurazione di un servizio SSL VPN per il supporto di partner Avaya alla pagina 39

Installazione di un certificato

Il servizio SSL VPN utilizza certificati digitali per verificare l'identità dei dispositivi a ogni estremità del tunnel SSL VPN. In questa procedura viene descritto come installare un certificato nell'archivio dei certificati attendibili di IP Office.

Managercontiene un'opzione di menu che consente di ripristinare le impostazioni di protezione predefinite in IP Office. Se si ripristinano le impostazioni di protezione predefinite e il servizio SSL VPN non effettua la riconnessione a AVG dopo qualche minuto, è necessario aggiungere nuovamente il certificato nell'archivio certificati attendibili.

Analogamente, l'applicazione Security Manager consente di eliminare il certificato dall'archivio dei certificati attendibili. Se si elimina il certificato tramite Security Manager e il servizio SSL VPN è già stato collegato ad AVG, il servizio SSL VPN si disconnette alla successiva rinegoziazione della chiave segreta tramite il tunnel. Tale rinegoziazione ha luogo ogni otto ore per impostazione predefinita e può verificarsi a diversi intervalli a seconda delle impostazioni configurate in AVG. Se il servizio SSL VPN si disconnette durante la rinegoziazione o se l'utente disattiva il servizio prima che si verifichi la successiva rinegoziazione, non sarà possibile attivare nuovamente il servizio SSL VPN fino a quando non verrà installato il certificato richiesto nell'archivio dei certificati attendibili.

Prerequisiti

È necessario installare un tipo di certificato tra quelli indicati di seguito.

- Il certificato AVG autofirmato del portale VPN al quale il servizio SSL VPN di IP Office si collega
- Il certificato dell'autorità di certificazione che ha firmato il certificato AVG

Procedura

1. Selezionare **File > Avanzate > Impostazioni di sicurezza**.

   Verrà visualizzata una finestra di dialogo contenente l'elenco dei sistemi IP Office.
2. Fare clic sulla casella di controllo per selezionare il sistema IP Office in cui si desidera installare il certificato.
3. Fare clic su **OK**.

   Verrà visualizzata una finestra di dialogo.
4. Nel campo **Nome utente servizio**, immettere il nome utente dell'amministratore IP Office.
5. Nel campo **Password utente servizio** immettere la password dell'amministratore IP Office.
6. Fare clic su **OK**.

   Le credenziali vengono accettate.
7. Nel riquadro di navigazione selezionare **Sicurezza > Sistema** e selezionare il nome della configurazione.
8. Nella scheda **Certificati** fare clic su **Aggiungi**.

Verrà visualizzata una finestra di dialogo in cui si richiede di selezionare un'origine per il certificato.

9. Selezionare **Incolla dagli Appunti** e fare clic su **OK**.

   Verrà visualizzata una finestra di dialogo per acquisire il testo del certificato.

10. Copiare il certificato e incollare il testo nella finestra aperta. È necessario includere le righe `-----BEGIN CERTIFICATE-----` e `-----END CERTIFICATE-----`.

11. Fare clic su **OK**.

    Il nome del certificato verrà visualizzato nell'elenco Certificati installati.

Collegamenti correlati

Configurazione di un servizio SSL VPN per il supporto di partner Avaya alla pagina 39

Configurazione di codici funzione

Il sistema IP Office consente di configurare codici funzione. Questi codici funzione attivano un'azione specifica quando vengono digitati su un deskphone connesso al sistema IP Office. Per informazioni sulla programmazione dei pulsanti del telefono con codici funzione, vedere la documentazione di IP Office Manager.

È possibile configurare codici funzione e utilizzarli per abilitare e disabilitare il servizio SSL VPN. In caso di utilizzo dei codici funzione per abilitare o disabilitare il servizio SSL VPN, il servizio rimane con provisioning eseguito nel sistema. I codici funzione mettono il tunnel in stato di servizio o di fallback.

Il sistema IP Office include un gruppo di funzioni predefinite accessibili tramite codici funzione. È possibile utilizzare le funzioni predefinite indicate di seguito per creare codici funzione che abilitano o disabilitano il servizio SSL VPN:

- Cancella servizio notte per gruppo di ricerca: abilita il servizio SSL VPN
- Imposta servizio notte per gruppo di ricerca: disabilita il servizio SSL VPN

Questi codici funzione sono disponibili per uso interno ed è necessario comporli da un telefono collegato al sistema IP Office. Se si desidera utilizzare i codici funzione da un telefono esterno, è possibile configurare un assistente automatico. L'assistente automatico consente di effettuare le composizioni nel sistema IP Office da un numero di telefono esterno e attivare i codici funzione mediante un sistema di menu.

Collegamenti correlati

Configurazione di un servizio SSL VPN per il supporto di partner Avaya alla pagina 39
Configurazione di un codice funzione per abilitare il servizio SSL VPN alla pagina 44
Configurazione di un codice funzione per disabilitare il servizio SSL VPN alla pagina 44
Configurazione di un assistente automatico alla pagina 45

Configurazione di un codice funzione per abilitare il servizio SSL VPN

Attenersi alla procedura indicata di seguito per configurare un codice funzione che abilita il servizio SSL VPN quando viene composto da un deskphone collegato al sistema IP Office.

Procedura

1. Nell'elenco di navigazione selezionare **Cod funz**.

   Verrà visualizzato l'elenco dei codici funzione predefiniti.

2. Fare clic con il pulsante destro del mouse e scegliere **Nuovo**.

   Verrà visualizzata la scheda Codice funzione.

3. Nel campo **Codice** immettere ***775*x*1**, dove *x* rappresenta un'istanza del servizio SSL VPN compreso tra 1 e 9. Se ad esempio sono configurate due istanze del servizio SSL VPN e vengono configurati i codici funzione per la prima istanza, immettere ***77511**.

   Nota:

   È possibile assegnare numeri diversi al codice funzione. Per semplicità, è consigliabile utilizzare *775, che rappresenta *SSL su una tastiera.

4. Nell'elenco **Funzione** selezionare **Cancella servizio notte per gruppo di ricerca**.

5. Nel campo **Numero telefonico** immettere il nome del servizio SSL VPN tra virgolette. Se ad esempio il nome del servizio è Service1, immettere "`Service1`".

   Utilizzare il nome del servizio SSL VPN immesso in fase di creazione del servizio SSL VPN. Consultare Configurazione del servizio SSL VPN alla pagina 40 per informazioni su questa impostazione.

6. Fare clic su **OK**.

7. Per salvare le modifiche alla configurazione, fare clic sull'icona **Salva**.

Collegamenti correlati

Configurazione di codici funzione alla pagina 43

Configurazione di un codice funzione per disabilitare il servizio SSL VPN

Attenersi alla procedura indicata di seguito per configurare un codice funzione che disabilita il servizio SSL VPN quando viene composto da un deskphone collegato al sistema IP Office.

Procedura

1. Nell'elenco di navigazione selezionare **Cod funz**.

   Verrà visualizzato l'elenco dei codici funzione predefiniti.

2. Fare clic con il pulsante destro del mouse e scegliere **Nuovo**.

Verrà visualizzata la scheda Codice funzione.

3. Nel campo **Codice** immettere ***775*x*0**, dove *x* rappresenta un'istanza del servizio SSL VPN compreso tra 1 e 9. Se ad esempio sono configurate due istanze del servizio SSL VPN e vengono configurati i codici funzione per la prima istanza, immettere ***77510**.

   Nota:

   È possibile assegnare numeri diversi al codice funzione. Per semplicità, è consigliabile utilizzare *775, che rappresenta *SSL su una tastiera.

4. Nell'elenco **Funzione** selezionare **Imposta servizio notte per gruppo di ricerca**.
5. Nel campo **Numero telefonico** immettere il nome del servizio SSL VPN tra virgolette. Se ad esempio il nome del servizio è Service1, immettere "`Service1`".

   Utilizzare il nome del servizio SSL VPN immesso in fase di creazione del servizio SSL VPN. Consultare Configurazione del servizio SSL VPN alla pagina 40 per informazioni su questa impostazione.

6. Fare clic su **OK**.
7. Per salvare le modifiche alla configurazione, fare clic sull'icona **Salva**.

Collegamenti correlati

Configurazione di codici funzione alla pagina 43

Configurazione di un assistente automatico

Per configurare un assistente automatico, attenersi alla procedura indicata di seguito. L'assistente automatico consente di accedere al sistema IP Office da un numero di telefono interno o esterno e utilizzare un sistema di menu per abilitare o disabilitare il servizio SSL VPN.

Prerequisiti

È necessario configurare codici funzione. Consultare Configurazione di codici funzione alla pagina 43.

In caso di utilizzo di Avaya Voicemail Pro, è necessario configurare un modulo per il trasferimento assistito prima di eseguire questa procedura. Per ulteriori informazioni, vedere *Amministrazione di Voicemail Pro* (15–601063).

Informazioni su questa attività

In questa procedura verrà creato un assistente automatico, a cui verranno mappate le chiamate in entrata. In questo esempio vengono utilizzati 0 per abilitare il servizio SSL VPN e 1 per disabilitarlo, ma è possibile assegnare queste funzioni a qualsiasi tasto sulla tastiera.

Procedura

1. Selezionare una delle seguenti opzioni:
   - In caso di utilizzo di Embedded Voicemail, selezionare **Assistente automatico** nell'elenco di navigazione.
   - In caso di utilizzo di Voicemail Pro, seguire la procedura a partire dalla fase 12 alla pagina 46.

2. Fare clic con il pulsante destro del mouse e scegliere **Nuovo**.
3. Nel campo **Nome** immettere il nome dell'assistente automatico.
4. Selezionare la scheda **Azioni**.
5. Selezionare la voce per il tasto **0** e fare clic sul pulsante **Modifica**.
6. Nell'elenco **Azioni** selezionare una delle seguenti opzioni:
   - Selezionare **Trasferimento normale**.
   - Selezionare **Trasferisci**.
7. Nell'elenco **Destinazione** digitare il codice funzione configurato per abilitare il servizio e fare clic su **OK**.
8. Selezionare la voce per il tasto **1** e fare clic sul pulsante **Modifica**.
9. Nell'elenco **Azioni** selezionare una delle seguenti opzioni:
   - Selezionare **Trasferimento normale**.
   - Selezionare **Trasferisci**.
10. Nell'elenco **Destinazione** digitare il codice funzione configurato per disabilitare il servizio e fare clic su **OK**.
11. Per salvare le modifiche alla configurazione, fare clic sull'icona **Salva**.
12. Nell'elenco di navigazione selezionare **Instradamento chiamate in entrata**.
13. Nella scheda **Standard** impostare il campo **Capacità portante** su **Qualsiasi voce**.
14. Nell'elenco **ID gruppo linee** selezionare la linea che si desidera utilizzare per abilitare e disabilitare il servizio SSL VPN.
15. Selezionare la scheda **Destinazione**.
16. È possibile scegliere tre le seguenti opzioni:
    - In caso di utilizzo di Embedded Voicemail, selezionare l'assistente automatico configurato dall'elenco **Destinazione**.
    - In caso di utilizzo di Voicemail Pro, digitare `VM:<nome>` nell'elenco **Destinazione**, dove `<nome>` è il nome del modulo Voicemail Pro.
17. Fare clic su **OK**.
18. Per salvare le modifiche alla configurazione, fare clic sull'icona **Salva**.

Passi successivi

È possibile registrare i prompt per l'assistente automatico. Per ulteriori informazioni sulla registrazione dei prompt, vedere la documentazione relativa al sistema di posta vocale in uso. In caso di utilizzo di Embedded Voicemail, vedere *Installazione di Embedded Voicemail*. In caso di utilizzo di Voicemail Pro, vedere *Amministrazione di Voicemail Pro*.

Collegamenti correlati

Configurazione di codici funzione alla pagina 43

Configurazione di notifiche di allarme

È possibile configurare la gestione degli errori per il servizio SSL VPN. Se si sceglie di configurarla, è possibile impostare filtri per determinare i tipi di eventi di cui ricevere notifica. È ad esempio possibile ricevere notifiche sugli errori correlati al servizio SSL VPN oppure al sistema IP Office.

Se si configura la gestione degli errori, è necessario definire destinazioni per gli allarmi in cui verranno segnalati gli errori di sistema. Per la segnalazione degli allarmi è possibile configurare le destinazioni seguenti:

- Trap SNMP segnalate in una rete LAN locale oppure in un server remoto
- Notifiche tramite e-mail segnalate a un server SMTP in una rete LAN locale oppure in un server SMTP remoto
- Voci Syslog segnalate in una rete LAN locale oppure in un server remoto

Le destinazioni degli allarmi che è possibile configurare variano a seconda della modalità operativa in uso. Nella tabella indicata di seguito vengono elencate le destinazioni degli allarmi supportate in ogni modalità.

Destinazione allarme	**Modalità operativa**			
	Essential Edition	**IP Office Server Edition**	**Sistema di espansione Server Edition**	**Basic Edition**
Trap SNMP				
SNMP in una rete LAN locale	✔	✔	✔	✔
SNMP su un servizio SSL VPN	✔	✔	✔	✔
Notifiche tramite e-mail				
Server SMTP in una rete LAN locale	✔	✔	✔	—
Server SMTP su un tunnel SSL VPN	✔	✔	✔	—
Voci Syslog				
Server Syslog in una rete LAN locale	✔	✔	✔	—
Server Syslog su un tunnel SSL VPN	✔	✔	✔	—

Collegamenti correlati

[Configurazione di un servizio SSL VPN per il supporto di partner Avaya](#) alla pagina 39
[Configurazione di destinazioni di trap SNMP](#) alla pagina 48

Configurazione di notifiche di allarmi tramite e-mail alla pagina 49
Configurazione di voci Syslog alla pagina 50

Configurazione di destinazioni di trap SNMP

Attenersi alla procedura indicata di seguito per segnalare errori di sistema come trap SNMP. È possibile impostare filtri per determinare i tipi di eventi che generano trap SNMP. È ad esempio possibile generare trap SNMP per errori relativi al servizio SSL VPN o al sistema IP Office.

Prerequisiti

In fase di definizione di un indirizzo IP di destinazione per un evento di errore, il sistema utilizza una tabella di instradamenti IP per determinare l'interfaccia da utilizzare per l'invio dell'evento di errore. La destinazione deve essere un indirizzo IPv4 affinché la trap SNMP venga instradata in modo corretto al server di gestione degli errori.

È necessario configurare un listener di trap nel computer di destinazione in cui vengono segnalate le trap SNMP.

Procedura

1. Nell'elenco di navigazione fare clic su **Sistema** e selezionare la scheda **Eventi di sistema**.

   Manager visualizza una scheda **Configurazione** e una scheda **Allarmi**.
2. Nella scheda **Configurazione** selezionare l'opzione **SNMP abilitato**.
3. Nel campo **Comunità** immettere `public`.
4. Nella scheda **Allarmi** fare clic su **Aggiungi**.
5. Selezionare **Trap** e immettere un indirizzo di destinazione per le trap SNMP nel campo **Indirizzo IP**. .
6. Immettere un numero di porta o utilizzare il numero di porta predefinito (162).
7. Nel campo **Comunità** immettere `public`.
8. Nell'elenco **Eventi** scegliere il filtro eventi:
   - Selezionare **Servizio** per generare trap SNMP per errori relativi al servizio SSL VPN.
   - Selezionare qualsiasi evento correlato al funzionamento del sistema IP Office per cui si desidera generare trap SNMP. Per informazioni su queste opzioni, vedere *IP Office Manager*.
9. Fare clic su **OK** per chiudere la finestra di dialogo.
10. Fare clic su **OK** nella scheda Allarmi.
11. Per salvare le modifiche alla configurazione, fare clic sull'icona **Salva**.

Collegamenti correlati

Configurazione di notifiche di allarme alla pagina 47

Configurazione di notifiche di allarmi tramite e-mail

Attenersi alla procedura indicata di seguito per ricevere notifiche tramite e-mail nel caso in cui si verifichino errori. È possibile impostare filtri per determinare i tipi di eventi di cui ricevere notifica. È ad esempio possibile ricevere notifiche sugli errori correlati al servizio SSL VPN oppure al sistema IP Office.

Prerequisiti

È necessario configurare un server di posta elettronica SMTP nel computer utilizzato per la gestione degli errori. È inoltre necessario configurare un client di posta elettronica nel computer in cui si desidera ricevere le notifiche tramite e-mail.

In fase di definizione di un indirizzo di destinazione per un evento di errore, il sistema utilizza una tabella di instradamenti IP per determinare l'interfaccia da utilizzare per l'invio dell'evento di errore. La destinazione deve essere un indirizzo IPv4 affinché la notifica venga instradata in modo corretto al server di gestione degli errori.

Procedura

1. Nell'elenco di navigazione fare clic su **Sistema** e selezionare la scheda **Eventi di sistema**.

   Manager visualizza una scheda **Configurazione** e una scheda **Allarmi**.
2. Nella scheda **Allarmi** fare clic su **Aggiungi**.
3. Selezionare l'opzione **Posta elettronica** e immettere l'indirizzo a cui si desidera ricevere le notifiche tramite e-mail nel campo **Posta elettronica**.
4. Nell'elenco **Eventi** scegliere il filtro eventi:
   - Selezionare **Servizio** per ricevere notifiche su errori correlati al servizio SSL VPN.
   - Selezionare qualsiasi evento correlato al funzionamento del sistema IP Office su cui si desidera ricevere notifiche. Per informazioni su queste opzioni, vedere *IP Office Manager*.
5. Fare clic su **OK** per chiudere la finestra di dialogo.
6. Fare clic su **OK** nella scheda Allarmi.
7. Selezionare la scheda **SMTP**.
8. Nel campo **Indirizzo IP** immettere l'indirizzo IP del server SMTP.
9. Nel campo **Porta** immettere il numero di porta del server SMTP.
10. Nel campo **Invia e-mail dall'indirizzo** immettere l'indirizzo e-mail utilizzato dal sistema IP Office per inviare le notifiche tramite e-mail.
11. Selezionare **Il server richiede autenticazione**.
12. Nei campi **Nome utente** e **Password** immettere le credenziali necessarie per accedere al server SMTP.
13. Fare clic su **OK**.
14. Per salvare le modifiche alla configurazione, fare clic sull'icona **Salva**.

Collegamenti correlati

Configurazione di notifiche di allarme alla pagina 47

Configurazione di voci Syslog

Attenersi alla procedura indicata di seguito per segnalare errori di sistema come voci Syslog. È possibile impostare i filtri per definire i tipi di eventi segnalati. È ad esempio possibile segnalare errori correlati al servizio SSL VPN oppure al sistema IP Office.

Prerequisiti

È necessario configurare un client Syslog nel server in cui si desidera segnalare gli errori di sistema.

In fase di definizione di un indirizzo IP di destinazione per un evento di errore, il sistema utilizza una tabella di instradamenti IP per determinare l'interfaccia da utilizzare per l'invio dell'evento di errore. La destinazione deve essere un indirizzo IPv4 affinché la notifica venga instradata in modo corretto al server di gestione degli errori.

Procedura

1. Nell'elenco di navigazione fare clic su **Sistema** e selezionare la scheda **Eventi di sistema**.

   Manager visualizza una scheda **Configurazione** e una scheda **Allarmi**.
2. Nella scheda **Allarmi** fare clic su **Aggiungi**.
3. Selezionare l'opzione **Syslog** e immettere l'indirizzo IP del server in cui è configurato il client Syslog nel campo **Indirizzo IP**.
4. Immettere il numero di porta del server in cui è configurato il client Syslog nel campo **Porta**.
5. Nell'elenco **Eventi** scegliere il filtro eventi:
   - Selezionare **Servizio** per segnalare errori correlati al servizio SSL VPN.
   - Selezionare qualsiasi evento correlato al funzionamento del sistema IP Office su cui si desidera ricevere notifiche. Per informazioni su queste opzioni, vedere *IP Office Manager*.
6. Fare clic su **OK** per chiudere la finestra di dialogo.
7. Fare clic su **OK** nella scheda **Allarmi**.
8. Per salvare le modifiche alla configurazione, fare clic sull'icona **Salva**.

Collegamenti correlati

Configurazione di notifiche di allarme alla pagina 47

Configurazione di un instradamento statico

In fase di configurazione di instradamenti di split tunneling in AVG, il sistema IP Office acquisisce le informazioni di instradamento per il tunnel in modo dinamico quando il servizio SSL VPN service si connette ad AVG. È tuttavia possibile configurare un instradamento statico. In questa sezione vengono fornite informazioni che consentono di determinare se è opportuno configurare un instradamento statico e viene descritta la relativa procedura.

In fase di configurazione di un instradamento statico, il sistema utilizza le informazioni dell'instradamento IP configurate in Manager per determinare la destinazione per il traffico inoltrato. È possibile definire il servizio SSL VPN come destinazione.

Utilizzare un instradamento statico nei seguenti casi:

- Gli instradamenti dello split tunneling non sono annunciati da AVG ed è necessario inviare traffico tramite il tunnel
- Il servizio SSL VPN non è connesso ad AVG e si desidera accodare il traffico da inoltrare tramite il tunnel al ripristino della connessione

Prerequisiti

Prima di iniziare, è necessario disporre delle informazioni seguenti:

- Indirizzo della subnet remota. Si tratta della subnet situata nella rete privata in cui è installato AVG
- Subnet mask applicata all'indirizzo della subnet
- Nome del servizio SSL VPN che si desidera utilizzare per inviare traffico alla subnet remota

Procedura

1. Nell'elenco di navigazione selezionare **Instradamento IP**.
2. Fare clic con il pulsante destro del mouse e scegliere **Nuovo**.
3. Nel campo **Indirizzo IP** immettere l'indirizzo della subnet remota situata nel sito in cui è installato AVG.
4. Nel campo **Subnet mask** immettere la subnet mask applicata alla subnet remota.
5. Nel campo **Indirizzo IP gateway** verificare l'indirizzo IP del gateway sia impostato su 0.0.0.0.
6. Nell'elenco **Destinazione** selezionare il nome del servizio SSL VPN.

Collegamenti correlati

Configurazione di un servizio SSL VPN per il supporto di partner Avaya alla pagina 39

Capitolo 7: Configurazione di un servizio SSL VPN di un partner Avaya tramite un SDK

I fornitori di servizi di terze parti possono utilizzare Avaya VPN Gateway per fornire il supporto remoto ai clienti tramite la tecnologia SSL VPN di IP Office.

Per il supporto dei fornitori di servizi di terze parti, l'SSL VPN può essere configurato tramite un kit di sviluppo di software (SDK). L'SDK è progettato per consentire ai partner di configurare AVG automatizzando alcuni o tutti gli aspetti della registrazione di IP Office e del processo di On-Boarding. Il processo automatizzato sostituisce le procedure utilizzate per la configurazione manuale.

Server SDK

Sono disponibili due SDK di On-Boarding.

- SDK di On-Boarding
- SDK di On-Boarding rapido

SDK di On-Boarding:

Per ogni nuova installazione di IP Office, l'SDK di On-Boarding viene eseguito sul server Web del partner per generare il file xml di On-Boarding caricato su IP Office tramite Web Manager. Questo processo consente di configurare il tunnel SSL VPN dal la piattaforma IP Office del cliente a quella AVG del partner.

SDK di On-Boarding rapido:

L'SDK di On-Boarding rapido può essere eseguito in modalità offline, senza una connessione a Internet. Quando si esegue l'SDK, IP Office viene registrato immediatamente, quindi raccoglie tutti i file del processo di On-Boarding rilevanti e li registra in un file zip. A questo punto, il tunnel SSL VPN cerca di connettersi ad AVG ma non riesce ad eseguire il processo di autenticazione. Quando il partner elabora il contenuto del file zip per creare le credenziali SSL VPN del sito del cliente associato, AVG accetta la definizione del tunnel SSL VPN.

Codici funzione

IP Office supporta più istanze del servizio SSL VPN. Ciò significa che possono esserci due servizi SSL VPN concorrenti e attivamente collegati, uno per la piattaforma AVG del supporto Avaya e uno per quella AVG del partner. Quando due servizi SSL VPN sono configurati su IP Office, Avaya suggerisce le convenzioni di denominazione e numerazione dei codici funzione elencate di seguito

per il servizio SSL VPN del supporto Avaya e il servizio SSL VPN del partner. Le convenzioni sono basate su:

- Le cifre 775 = SSL su una tastiera di selezione telefonica.
- Il quarto valore numerico 1 o 2 si riferisce all'istanza del servizio.
- Per il quinto valore numerico, valgono le seguenti regole: 1=attivato e 0=disattivato.

Servizio SSL-VPN di supporto Avaya:

- Nome del servizio: AVAYA_SUPPORT
- Codice funzione per l'attivazione del servizio AVAYA_SUPPORT: 77511
- Codice funzione per la disattivazione del servizio AVAYA_SUPPORT: 77510

Servizio SSL VPN del partner:

- Nome del servizio: BP_SUPPORT
- Codice funzione per l'attivazione del servizio BP_SUPPORT: 77521
- Codice funzione per la disattivazione del servizio BP_SUPPORT: 77520

Prerequisiti

- Sul computer sul quale viene eseguito l'SDK deve essere installato Java 1.6 o versione successiva.
- L'indirizzo IP del tunnel non deve essere compreso tra 172.22.0.0 e 172.25.255.255. Questo intervallo di indirizzi è riservato al supporto Avaya.

Collegamenti correlati

Download dell'SDK alla pagina 53
Download del file di inventario di IP Office alla pagina 53
Utilizzo dell'SDK di On-Boarding alla pagina 54
Utilizzo dell'SDK di On-Boarding rapido alla pagina 57

Download dell'SDK

È possibile scaricare l'SDK di On-Boarding e l'SDK di On-Boarding rapido dal sito Web Avaya DevConnect all'indirizzo http://www.devconnectprogram.com/

Collegamenti correlati

Configurazione di un servizio SSL VPN di un partner Avaya tramite un SDK alla pagina 52

Download del file di inventario di IP Office

Questa procedura offre il metodo manuale per il download del file di inventario di IP Office tramite Web Manager. L'SDK di On-Boarding rapido offre strumenti per automatizzare il download

senza l'utilizzo di Web Manager. Per informazioni, vedere la documentazione inclusa con l'SDK di On-Boarding rapido.

Procedura

1. Accedere a Web Manager. In un browser Web immettere l'indirizzo IP del sistema IP Office nel formato `http://<ip_address>/index.html`.

   Viene visualizzata la pagina dell'indice per il server.
2. Fare clic su **IP Office Web Manager**.
3. Nella finestra di accesso immettere il nome utente e la password e fare clic su **Accesso**.
4. Nella pagina della soluzione fare clic sul menu del server a destra del server e selezionare **On-boarding**.
5. Nella pagina di On-Boarding, fare clic su **Ottieni file archivio**.

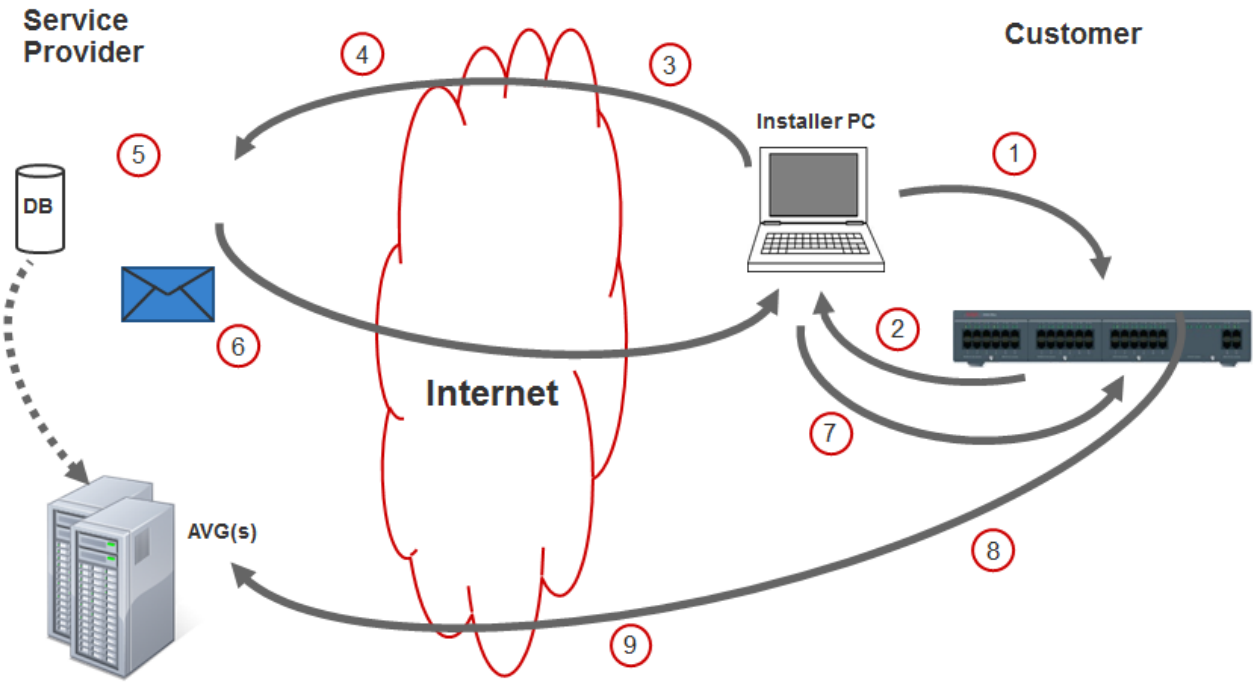
   Il file di inventario viene scaricato sul PC dell'installatore.

Collegamenti correlati

Configurazione di un servizio SSL VPN di un partner Avaya tramite un SDK alla pagina 52

Utilizzo dell'SDK di On-Boarding

Processo di configurazione del servizio SSL VPN tramite l'SDK di On-Boarding



1	Configurare le seguenti impostazioni di IP Office: • ID di sistema • Licenze • Interfacce LAN • Server DNS
2	Sul sito del cliente scaricare il file di inventario XML da IP Office nel PC dell'installatore.
3	Caricare il file di inventario sul sito del partner.
4	Memorizzare le credenziali SSL VPN nel database.
5	Eseguire l'SDK di On-Boarding.
6	Inviare via e-mail o caricare il file xml di On-Boarding sul PC dell'installatore.
7	Caricare il file xml di On-Boarding su IP Office.
8	Il servizio SSL VPN consente di connettersi ad AVG.
9	Utilizzare SSA per verificare la connettività SSL VPN.

Collegamenti correlati

Configurazione di un servizio SSL VPN di un partner Avaya tramite un SDK alla pagina 52
Memorizzazione delle credenziali SSL VPN nel database AVG alla pagina 55
Esecuzione dell'SDK di On-Boarding alla pagina 55
Caricamento del file di On-Boarding e verifica di SSL VPN alla pagina 56

Memorizzazione delle credenziali SSL VPN nel database AVG

Se si utilizza il database AVG locale, aggiungere le credenziali nell'interfaccia di configurazione di AVG.

Se si utilizza un database LDAP o RADIUS, utilizzare l'interfaccia appropriata per aggiungere le credenziali nel database.

Collegamenti correlati

Utilizzo dell'SDK di On-Boarding alla pagina 54

Esecuzione dell'SDK di On-Boarding

Sono disponibili due modi per eseguire l'SDK.

- Richiamare il wrapper della riga del comando relativa allo script del batch DOS di On-Boarding con i parametri e i nomi file di input/output rilevanti.
- Utilizzare le API JAVA pubblicate.

Per informazioni, fare riferimento alla guida dello sviluppatore dell'SDK inclusa nel file zip dell'SDK.

L'output dell'SDK è il file xml di On-Boarding. Trasferire il file sul PC dell'installatore sul sito del cliente.

Collegamenti correlati

Utilizzo dell'SDK di On-Boarding alla pagina 54

Caricamento del file di On-Boarding e verifica di SSL VPN

Procedura

1. Accedere a Web Manager. In un browser Web immettere l'indirizzo IP del sistema IP Office nel formato `http://<ip_address>/index.html`.

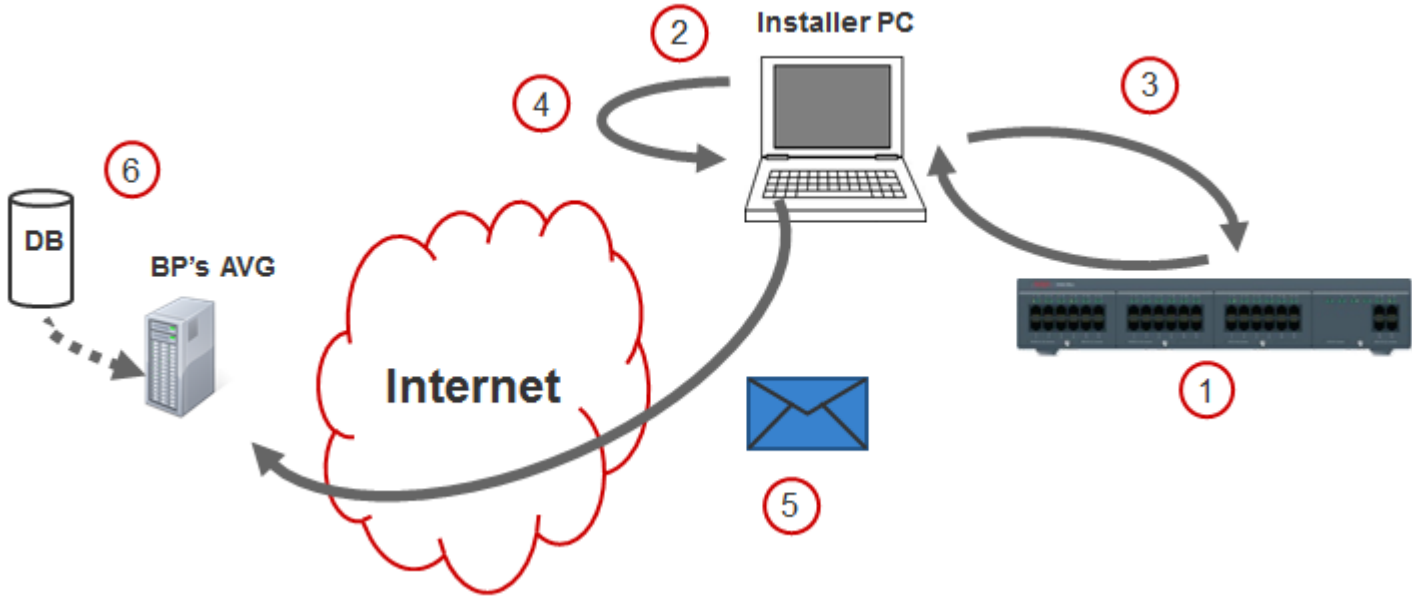
   Viene visualizzata la pagina dell'indice per il server.
2. Fare clic su **IP Office Web Manager**.
3. Nella finestra di accesso immettere il nome utente e la password e fare clic su **Accesso**.
4. Nella pagina della soluzione fare clic sul menu del server a destra del server e selezionare **On-boarding**.
5. Nella pagina di On-Boarding, nel riquadro numero 3, fare clic su **Sfoglia** e accedere alla posizione del file xml di On-Boarding.
6. Fare clic su **Carica**.
7. Verificare la connettività di SSL VPN tramite l'applicazione SSA.

Collegamenti correlati

Utilizzo dell'SDK di On-Boarding alla pagina 54

Utilizzo dell'SDK di On-Boarding rapido

Processo di configurazione del servizio SSL VPN tramite l'SDK di On-Boarding rapido



1	Configurare le seguenti impostazioni di IP Office. • ID di sistema • Licenze • Interfacce LAN • Server DNS
2	Eseguire dell'SDK di On-Boarding rapido.
3	L'SDK di On-Boarding rapido consente di scambiare file con IP Office.
4	L'SDK di On-Boarding rapido consente di creare un file zip contenente tutti i file richiesti per l'On-Boarding. Ripetere i passaggi 1–3 per tutti i sistemi IP Office.
5	Trasferire in sicurezza i file zip sul sito del partner. Ad esempio, utilizzare un servizio di hosting dei file o un servizio di memorizzazione cloud per trasferire il file.
6	Elaborare tutti i file di On-Boarding per creare il tunnel SSL VPN.

Collegamenti correlati

Configurazione di un servizio SSL VPN di un partner Avaya tramite un SDK alla pagina 52
Esecuzione dell'SDK di On-Boarding rapido alla pagina 58
Elaborazione dei file zip dell'SDK di On-Boarding rapido alla pagina 58

Esecuzione dell'SDK di On-Boarding rapido

Questa procedura fornisce informazioni sull'interfaccia utente predefinita della riga di comando. È disponibile anche un'API JAVA per facilitare la creazione di un'interfaccia utente alternativa. L'interfaccia predefinita della riga di comando raccoglie i dati utilizzati per creare il file delle proprietà come input all'API JAVA.

Ad esempio, un'applicazione per dispositivi mobili potrebbe essere creata con un modulo per raccogliere i dati necessari. Quindi, sarà necessario richiamare l'API JAVA che contatta IP Office per completare il processo di registrazione e creare il file zip risultante.

Procedura

1. Modificare il file `default_parameters.txt`.
2. Eseguire il file `sslvpnOnboardingExpress.bat` dell'SDK di On-Boarding rapido utilizzando i parametri di comando appropriati.

   L'SDK di On-Boarding rapido consente di creare un file zip contenente i file richiesti per configurare il servizio SSL VPN per IP Office. Il file zip viene memorizzato nella cartella `sslvpn_OUTPUT`.

Passi successivi

Trasferire in sicurezza i file zip sul sito del partner. Ad esempio, utilizzare un servizio di hosting dei file o un servizio di memorizzazione cloud per trasferire il file.

Collegamenti correlati

Utilizzo dell'SDK di On-Boarding rapido alla pagina 57

Elaborazione dei file zip dell'SDK di On-Boarding rapido

Una volta che il file zip generato dall'SDK è stato trasferito al sito del partner, le credenziali del tunnel SSL VPN per l'installazione del cliente vengono configurate in AVG, Radius o LDAP. Una volta completata la procedura, il tunnel SSL VPN effettuerà la connessione ad AVG.

Se si utilizza un servizio di archiviazione dei file cloud condiviso, l'elaborazione del file zip sul sito del partner può essere effettuata in pochi secondi. Ciò consente all'installatore di avviare SSA immediatamente dopo aver eseguito lo script di On-Boarding rapido per verificare il funzionamento della connettività del tunnel SSL VPN.

Collegamenti correlati

Utilizzo dell'SDK di On-Boarding rapido alla pagina 57

Capitolo 8: Regole NAPT (Network Address and Port Translation)

Utilizzare un servizio SSL VPN e le regole NAPT (Network Address and Port Translation) per stabilire sessione di comunicazione remota con dispositivi LAN come un modulo UCM di IP Office. Per connettersi a un dispositivo LAN sulla rete privata di IP Office, il fornitore del servizio di supporto deve avviare un'applicazione di comunicazione su un PC situato nella sede del fornitore del servizio remoto, quindi specificare i seguenti parametri di configurazione per la sessione:

- Indirizzo IP di un tunnel SSL VPN
- Numero di porta esterna per il dispositivo LAN

IP Office utilizza le regole NAPT per mappare l'indirizzo IP del tunnel e il numero di porta esterna con l'indirizzo IP e il numero di porta corretti nella rete privata.

Collegamenti correlati

[Configurazione delle regole NAPT](#) alla pagina 59
[Eliminazione di una regola NAPT](#) alla pagina 60

Configurazione delle regole NAPT

Eseguire questa procedura nell'interfaccia di Manager. È possibile configurare fino a 64 regole.

Quando si configura una regola NAPT, è necessario selezionare un tipo di applicazione. Sono disponibili le seguenti opzioni di applicazione:

- Personalizzato
- VMPro
- one-X Portal
- SSH
- TELNET
- RDP (Remote Desktop Protocol)
- Web Control

È possibile utilizzare l'impostazione **Personalizzata** per configurare una regola NAPT per un nuovo tipo di applicazione. È possibile anche utilizzare l'impostazione **Personalizzata** con un **Numero porta esterna** modificato per aprire due sessioni di comunicazione contemporanee

utilizzando la stessa applicazione per connettersi allo stesso dispositivo LAN. Ad esempio, per abilitare due sessioni SSH contemporanee sullo stesso indirizzo IP, le due regole NAPT potrebbero essere simili a quelle riportate di seguito.

Applicazione	Protocollo	Numero di porta esterna	Indirizzo IP interno	Numero di porta interna
SSH	TCP	22	192.168.40.1	22
Personalizzato	TCP	221	192.168.40.1	22

Procedura

1. Nell'elenco di navigazione selezionare **Servizio**.
2. Nell'elenco **Servizio**, selezionare il servizio SSL VPN in cui si desidera configurare le regole NAPT.
3. Nel riquadro dei dettagli per il servizio, selezionare la scheda **NAPT**.
4. In **Applicazione**, aprire l'elenco a discesa e selezionare un tipo di applicazione.

   Nel campo **Protocollo** e nei campi **Numero porta** vengono inseriti automaticamente i valori predefiniti.
5. (Facoltativo) Se si desidera configurare un'applicazione **Personalizzata**, modificare il campo **Numero porta esterna**.
6. Ripetere i passi 4 e 5 per configurare altre regole.

Collegamenti correlati

Regole NAPT (Network Address and Port Translation) alla pagina 59

Eliminazione di una regola NAPT

Procedura

Per eliminare una regola NAPT, utilizzare la colonna vuota a sinistra della tabella. Fare clic con il pulsante destro del mouse nella cella vuota accanto alla regola da eliminare e selezionare l'icona di eliminazione.

Collegamenti correlati

Regole NAPT (Network Address and Port Translation) alla pagina 59

Capitolo 9: Verifica della connessione tra IP Office e AVG

Attenersi alle procedure in questa sezione per eseguire il test della connessione tra il sistema IP Office e AVG.

Collegamenti correlati

[Verifica della connessione con SysMonitor](#) alla pagina 61
[Verifica della distribuzione SSL VPN di AVG mediante System Status Application](#) alla pagina 62
[Verifica della connessione mediante l'interfaccia BBI di AVG](#) alla pagina 62
[Invio di un allarme di test](#) alla pagina 63

Verifica della connessione con SysMonitor

È possibile utilizzare System Status Application (SSA) per verificare che il tunnel SSL VPN sia in servizio. Avviare SSA e verificare che siano elencate le impostazioni di configurazione del tunnel.

È possibile attenersi alla procedura descritta di seguito per utilizzare SysMonitor al fine di verificare la connessione SSL VPN tra il sistema IP Office e AVG.

Procedura

1. Selezionare **Start > Programmi > IP Office > Monitor**.

   L'applicazione SysMonitor si connette al server IP Office e visualizza un registro del sistema.

2. Selezionare le opzioni **Filters > Trace** (Filtri > Traccia) e fare clic sulla scheda **VPN**.
3. Nell'area SSL VPN verificare che **Session** (Sessione) e **Session State** (Stato sessione) siano abilitati. Fare clic su **OK**.

   Nel registro di SysMonitor viene elencata l'attività del servizio SSL VPN sotto il nome configurato per il servizio.

4. Individuare il nome del servizio e controllare le informazioni seguenti:

Modifica dello stato della sessione	In caso di abilitazione del servizio SSL VPN, lo stato della sessione attraversa le fasi indicate di seguito: • risoluzione del nome del dominio • avvio della sessione • connessione dell'indirizzo IP di IP Office all'indirizzo IP del gateway VPN Se IP Office non è in grado di risolvere il nome del dominio, verrà visualizzato il messaggio di errore seguente: "DNS failed to resolve host name <x.x.x> and reached MAX retries. Restart session" (DNS: impossibile risolvere il nome host <x.x.x>. È stato raggiunto il numero massimo di nuovi tentativi. Riavviare la sessione).

Collegamenti correlati

Verifica della connessione tra IP Office e AVG alla pagina 61

Verifica della distribuzione SSL VPN di AVG mediante System Status Application

Effettuare le operazioni seguenti per eseguire il test della distribuzione SSL di AVG.

1. Avviare IP Office System Status Application (SSA) e verificare che il tunnel SSL VPN sia **In servizio** e che sia visualizzato l'**Indirizzo IP tunnel**.
2. Eseguire il ping di IP Office in remoto. Dal computer dell'agente del servizio, avviare una finestra dei comandi ed eseguire un comando di a ping utilizzando l'indirizzo IP del tunnel. Il ping dovrebbe riuscire.

Collegamenti correlati

Verifica della connessione tra IP Office e AVG alla pagina 61

Verifica della connessione mediante l'interfaccia BBI di AVG

Procedura

1. Accedere all'interfaccia BBI di AVG.
2. Espandere **Monitor** nel riquadro di navigazione di sinistra.

3. All'interno di **Monitor**, selezionare **Utenti**.
4. La colonna **IP origine** contiene quanto segue:
   - L'indirizzo IP di IP Office.
   - L'indirizzo IP del tunnel SSL VPN assegnato all'utente locale.

Collegamenti correlati

Verifica della connessione tra IP Office e AVG alla pagina 61

Invio di un allarme di test

Attenersi alla procedura indicata di seguito per inviare un allarme di test da System Status Application (SSA). Utilizzare l'allarme di test per generare un evento di errore.

Prerequisiti

È necessario definire una destinazione di allarme. In fase di definizione di un indirizzo IP di destinazione per l'evento di errore, il sistema utilizza una tabella di instradamenti IP per determinare l'interfaccia da utilizzare per l'invio dell'evento di errore.

Procedura

1. Avviare SSA mediante uno dei seguenti metodi:
   - Avviare SSA dal DVD IP Office.
   - Selezionare **Start > Programmi > IP Office > System Status**.
   - In Manager o IP Office Manager for Server Edition selezionare **File > Avanzate > System Status**.
2. Selezionare **Allarmi > Servizio** nell'elenco di navigazione.
3. Fare clic sul pulsante **Prova allarme**.

   La tabella visualizza i risultati del test:

Valore	Descrizione
Ultima data dell'errore	Data e ora in cui si è verificato l'allarme.
Occorrenze	Numero di volte in cui si è verificato l'errore dall'ultimo riavvio dell'unità di controllo o dall'ultima cancellazione dell'allarme.
Descrizione errore	Gli allarmi di test visualizzano il messaggio "L'operatore ha avviato l'allarme di test".

   Se si è configurata una destinazione di allarme per una trap SNMP, l'allarme di test genererà le informazioni seguenti:

```
Enterprise: ipoGenTraps
Bindings (8)
Binding #1: ipoGTEventStdSeverity.0 *** (int32) major(4)
Binding #2: ipoGTEventDateTime.0 *** (octets)
```

```
Binding #3: ipoGTEventDevID.0 *** (octets)
Binding #4: sysDescr.0 *** (octets)
Binding #5: ipoGTEventReason.0 *** (int32) testAlarm(39)
Binding #6: ipoGTEventData.0 *** (octets)
Binding #7: ipoGTEventAlarmDescription.0 *** (octets) Operator initiated test
alarm - do not process
Binding #8: ipoGTEventAlarmRemedialAction.0 *** (octets) (zero-length)
```

Collegamenti correlati

Verifica della connessione tra IP Office e AVG alla pagina 61

Capitolo 10: Monitoraggio e gestione del sistema IP Office

Se il servizio SSL VPN è connesso, è possibile monitorare il sistema IP Office in remoto attraverso il tunnel. È inoltre possibile gestire il sistema IP Office ed eseguirne l'upgrade in remoto. Il servizio SSL VPN consente di utilizzare applicazioni thick client e basate su Web come se fossero direttamente connesse a un'interfaccia LAN locale. In questa sezione vengono fornite informazioni sulle applicazioni supportate e su come utilizzarle.

Strumenti di monitoraggio

Per monitorare il sistema IP Office in remoto, è possibile utilizzare gli strumenti seguenti:

- System Status Application (SSA): System Status Application è uno strumento di diagnostica che consente di monitorare lo stato dei sistemi IP Office. SSA segnala eventi in tempo reale e cronologici, nonché dati sullo stato e sulla configurazione.
- SysMonitor: l'applicazione SysMonitor visualizza informazioni operative sul sistema IP Office. Consente di acquisire le informazioni nei file di registro per l'analisi.

Strumenti di gestione

Per gestire, eseguire l'upgrade e configurare il sistema IP Office in remoto, è possibile utilizzare gli strumenti seguenti:

- IP Office Manager: un'applicazione amministrativa che consente di configurare impostazioni di sistema per sistemi IP Office Essential Edition.
  - IP Office Manager for Server Edition: all'avvio di IP Office Manager è possibile scegliere di aprire una configurazione con la modalità IP Office Manager for Server Edition, che consente di amministrare i server e le espansioni di sistema Server Edition.
- IP Office Basic Edition - Web Manager: uno strumento basato su browser che consente di configurare impostazioni di sistema per IP Office.

Segnalazione di errori

È possibile utilizzare il servizio SSL VPN per inviare errori di sistema a un server di gestione degli errori remoto situato nel sito del fornitore del servizio in cui è installato AVG. È possibile impostare filtri eventi per determinare quali errori verranno segnalati e configurare le destinazioni a cui verranno inviati gli errori.

Per informazioni sulla segnalazione di errori, consultare Configurazione di notifiche di allarme alla pagina 47

Modalità operative

Gli strumenti che è possibile utilizzare per monitorare e gestire il sistema IP Office in remoto variano a seconda della modalità operativa in uso. Nella tabella indicata di seguito vengono elencati gli strumenti supportati in ogni modalità.

Strumenti	Modalità operativa			
	Essential Edition	IP Office Server Edition	Sistema di espansione Server Edition	Basic Edition
SSA	✔	✔	✔	✔
SysMonitor	✔	✔	✔	✔
Manager(semplificato)	—	—	—	✔
Manager (standard) e IP Office Manager for Server Edition	✔	✔	✔	—
Web Manager	—	—	—	✔
Segnalazione di errori	✔	✔	✔	✔

Collegamenti correlati

Monitoraggio di IP Office in remoto con SSA alla pagina 66
Monitoraggio di IP Office in remoto con SysMonitor alla pagina 67
Monitoraggio in remoto di dispositivi LAN mediante il tunnel SSL VPN alla pagina 68
Configurazione di IP Office in remoto con Web Manager alla pagina 68
Configurazione di IP Office in remoto con Manager alla pagina 69
Configurazione in remoto dei sistemi Server Edition tramite IP Office Manager for Server Edition alla pagina 70
Configurazione in remoto dei sistemi Server Edition tramite Web Control alla pagina 71

Monitoraggio di IP Office in remoto con SSA

Attenersi alla procedura indicata di seguito per connettere System Status Application (SSA) a IP Office attraverso il tunnel SSL VPN.

Prerequisiti

Il tunnel SSL VPN deve essere in servizio ed è necessario disporre delle seguenti informazioni:

- indirizzo IP del tunnel SSL VPN

- nome utente dell'account amministratore IP Office
- password dell'account amministratore IP Office

Procedura

1. Avviare SSA mediante uno dei seguenti metodi:
   - Avviare SSA dal DVD IP Office.
   - Selezionare **Start > Programmi > IP Office > System Status**.
   - In Manager o IP Office Manager for Server Edition selezionare **File > Avanzate > System Status**.
2. Nel campo **Indirizzo IP unità di controllo** immettere l'indirizzo IP del tunnel SSL VPN.
3. Nel campo **Nome utente** immettere il nome utente dell'account amministratore IP Office.
4. Nel campo **Password** immettere la password dell'account amministratore IP Office
5. Fare clic su **Accesso**.

Collegamenti correlati

Monitoraggio e gestione del sistema IP Office alla pagina 65

Monitoraggio di IP Office in remoto con SysMonitor

Attenersi alla procedura indicata di seguito per connettere l'applicazione SysMonitor a IP Office attraverso il tunnel SSL VPN.

Prerequisiti

Il tunnel SSL VPN deve essere in servizio ed è necessario disporre delle seguenti informazioni:

- Indirizzo IP del tunnel SSL VPN
- Password dell'account amministratore IP Office

Procedura

1. Selezionare **Start > Programmi > IP Office > Monitor**.
2. Fare clic sull'icona **Select Unit** (Unità selezione).

   Verrà visualizzata una finestra di dialogo.
3. Nel campo **Indirizzo IP unità di controllo** immettere l'indirizzo IP del tunnel SSL VPN.
4. Nel campo **Password** immettere la password dell'account amministratore IP Office.
5. Fare clic sul pulsante Sfoglia accanto al campo **Trace Log Settings Filename** (Nome file impostazioni registro di traccia) e passare al percorso in cui si desidera salvare il registro di traccia, quindi fare clic su **Open** (Apri).
6. Fare clic su **OK**.

Collegamenti correlati

Monitoraggio e gestione del sistema IP Office alla pagina 65

Monitoraggio in remoto di dispositivi LAN mediante il tunnel SSL VPN

Attenersi alla procedura indicata di seguito per connettersi a un dispositivo LAN nella rete di IP Office mediante il tunnel SSL VPN utilizzando il NAPT (Network Address and Port Translation). Per connettersi a un dispositivo LAN, utilizzare un'applicazione di comunicazione per la quale sia configurata la regola NAPT. Per informazioni sulla configurazione delle regole NAPT, consultare Regole di traduzione degli indirizzi di rete e delle porte (NAPT) alla pagina 59.

Prerequisiti

Il tunnel SSL VPN deve essere in servizio ed è necessario disporre delle seguenti informazioni:

- Indirizzo IP del tunnel SSL VPN
- Numero di porta esterna configurata nella regola NAPT per il dispositivo LAN al quale ci si connette

Procedura

1. Aprire l'applicazione di comunicazione utilizzata per connettersi a un dispositivo LAN mediante il tunnel SSL VPN.
2. Stabilire una sessione di comunicazione utilizzando l'indirizzo IP del tunnel SSL VPN e il numero di porta esterna per il dispositivo LAN.

Collegamenti correlati

Monitoraggio e gestione del sistema IP Office alla pagina 65

Configurazione di IP Office in remoto con Web Manager

Attenersi alla procedura indicata di seguito per connettere l'applicazione Web Manager a IP Office attraverso il tunnel SSL VPN.

Per informazioni su come utilizzare l'applicazione Web Manager per configurare il sistema IP Office, vedere *Avaya IP Office Basic Edition - Web Manager.*

Prerequisiti

Il tunnel SSL VPN deve essere in servizio ed è necessario disporre delle seguenti informazioni:

- Indirizzo IP del tunnel SSL VPN
- Nome dell'account amministratore IP Office
- Password dell'account amministratore IP Office

Procedura

1. In un browser immettere l'indirizzo IP per la gestione Web nel formato seguente: `https://10.0.0.1:8443/webmanagement/WebManagement.html`, dove *10.0.0.1* è l'indirizzo IP del tunnel SSL VPN.

   Se il browser risponde con un avviso di sicurezza, seguire le impostazioni di menu visualizzate per procedere con la connessione.
2. Una volta visualizzato il menu di accesso, immettere il nome utente e la password per l'amministrazione del sistema.
3. Fare clic su **Accesso**.

   Verrà visualizzata la home page per la gestione Web del sistema.

Collegamenti correlati

Monitoraggio e gestione del sistema IP Office alla pagina 65

Configurazione di IP Office in remoto con Manager

È possibile utilizzare Manager per amministrare in remoto il sistema IP Office attraverso il tunnel SSL VPN. Se si utilizza Manager attraverso il tunnel SSL VPN, non è supportata l'individuazione automatica dei sistemi IP Office. È necessario configurare l'indirizzo IP del sistema a cui si desidera connettersi. Attenersi alla procedura indicata di seguito per connettere l'applicazione Manager a IP Office attraverso il tunnel SSL VPN.

Per informazioni su come configurare Manager e come utilizzarlo per amministrare un sistema IP Office, vedere *Avaya IP Office Manager*.

Prerequisiti

Il tunnel SSL VPN deve essere in servizio ed è necessario disporre delle seguenti informazioni:

- Indirizzo IP del tunnel SSL VPN
- Nome dell'account amministratore IP Office
- Password dell'account amministratore IP Office

Procedura

1. Selezionare **Start > Programmi > IP Office > Manager**.
2. Fare clic sull'icona **Apri configurazione da IP Office**.

   Verrà visualizzata la finestra di dialogo Seleziona IP Office.
3. Immettere l'indirizzo IP del tunnel SSL VPN nel campo **Indirizzo trasmissione/unità** e fare clic su **Aggiorna**.
4. Selezionare il sistema IP Office che si desidera configurare e fare clic su **OK**.

   Verrà visualizzata la finestra di dialogo Accesso utente del servizio di configurazione.

5. Immettere il nome utente per l'account amministratore di IP Office nel campo **Nome utente servizio** e immettere la password per l'account amministratore di IP Office nel campo **Password utente servizio**. Fare clic su **OK**.

Collegamenti correlati

Monitoraggio e gestione del sistema IP Office alla pagina 65

Configurazione in remoto dei sistemi Server Edition tramite IP Office Manager for Server Edition

È possibile utilizzare IP Office Manager for Server Edition per amministrare in remoto i sistemi indicati di seguito attraverso il tunnel SSL VPN:

- Server Edition Primario
- Server Edition Secondario
- Sistema di espansione Server Edition

Prerequisiti

Il tunnel SSL VPN deve essere in servizio ed è necessario disporre delle seguenti informazioni:

- Indirizzo IP del tunnel SSL VPN
- Nome dell'account amministratore IP Office Manager for Server Edition
- Password dell'account amministratore IP Office Manager for Server Edition

Informazioni su questa attività

Per configurare in remoto i sistemi Server Edition, è necessario configurare un servizio SSL VPN tra AVG e il Server Edition Primario. Sarà quindi possibile apportare modifiche alla configurazione dei sistemi Server Edition connessi al server primario. È in primo luogo necessario configurare un servizio SSL VPN tra ogni sistema Server Edition e AVG.

Attenersi alla procedura indicata di seguito per connettere IP Office Manager for Server Edition a un Server Edition Primario attraverso il tunnel SSL VPN.

Per informazioni su come utilizzare IP Office Manager for Server Edition, vedere *Avaya IP Office Manager*.

Procedura

1. Selezionare **Start > Programmi > IP Office > Manager**.
2. Selezionare **File > Preferenze**.
3. Selezionare **Utilizza accesso remoto per Multi-Site** e fare clic su **OK**.
4. Fare clic sull'icona **Apri configurazione da IP Office**.

   Verrà visualizzata la finestra di dialogo Seleziona IP Office.
5. Immettere l'indirizzo IP del tunnel SSL VPN nel campo **Indirizzo trasmissione/unità** e fare clic su **Aggiorna**.

6. Selezionare il sistema Server Edition che si desidera configurare.

   Se si seleziona il sistema Server Edition, verrà visualizzata l'opzione Apri con Server Edition, abilitata per impostazione predefinita.

7. Se ci si connette a un Server Edition Primario e si desidera apportare modifiche di configurazione ai sistemi Server Edition a esso connessi, selezionare **Usa accesso remoto**. Se ci si connette direttamente al sistema Server Edition che si desidera configurare, non è necessario selezionare questa opzione.

8. Fare clic su **OK**.

   Verrà visualizzata la finestra di dialogo Accesso utente del servizio di configurazione.

9. Immettere il nome utente per l'account amministratore di IP Office Manager for Server Edition nel campo **Nome utente servizio** e immettere la password per l'account amministratore di IP Office Manager for Server Edition nel campo **Password utente servizio**. Fare clic su **OK**.

10. Nell'elenco di navigazione selezionare **Rete**.

    Verrà visualizzata la schermata di riepilogo. In una tabella nella parte inferiore della schermata vengono elencati tutti i sistemi Server Edition.

11. Selezionare il sistema Server Edition che si desidera configurare.

    La schermata Riepilogo visualizzerà le informazioni di configurazione per il sistema selezionato.

Collegamenti correlati

Monitoraggio e gestione del sistema IP Office alla pagina 65

Configurazione in remoto dei sistemi Server Edition tramite Web Control

È possibile utilizzare l'interfaccia Web Control per avviare IP Office Manager for Server Edition e amministrare sistemi Server Edition in remoto attraverso il tunnel SSL VPN.

È possibile utilizzare IP Office Manager for Server Edition per amministrare in remoto i sistemi indicati di seguito attraverso il tunnel SSL VPN:

- Server Edition Primario
- Server Edition Secondario
- Sistema di espansione Server Edition

Prerequisiti

Il tunnel SSL VPN deve essere in servizio ed è necessario disporre delle seguenti informazioni:

- Indirizzo IP del tunnel SSL VPN

- Nome dell'account amministratore Web Control
- Password dell'account amministratore Web Control

Informazioni su questa attività

Per configurare in remoto i sistemi Server Edition, è necessario configurare un servizio SSL VPN tra AVG e il Server Edition Primario. Sarà quindi possibile apportare modifiche alla configurazione dei sistemi Server Edition connessi al server primario. È in primo luogo necessario configurare un servizio SSL VPN tra ogni sistema Server Edition e AVG.

Attenersi alla seguente procedura per avviare IP Office Manager for Server Edition attraverso l'interfaccia di Web Control e utilizzarlo per la connessione a un Server Edition Primario attraverso il tunnel SSL VPN.

Per informazioni su come utilizzare IP Office Manager for Server Edition, vedere *Avaya IP Office Manager*.

Procedura

1. Aprire un browser e immettere `https://<indirizzo IP>:7070`, dove *<indirizzo IP>* è l'indirizzo del tunnel SSL VPN configurato per il Server Edition Primario.
2. Immettere le credenziali di amministratore nei campi **Accesso** e **Password** e fare clic su **Accesso**.

   Verrà visualizzata la schermata Home, contenente i server e i sistemi di espansione Server Edition.
3. Fare clic su **Manager**.

   Verrà visualizzata la schermata di riepilogo di IP Office Manager for Server Edition.
4. Selezionare **File > Chiudi** per chiudere la configurazione.
5. Selezionare **File > Preferenze**.
6. Selezionare **Utilizza accesso remoto per Multi-Site** e fare clic su **OK**.
7. Fare clic sull'icona **Apri configurazione da IP Office**.

   Verrà visualizzata la finestra di dialogo Seleziona IP Office.
8. Immettere l'indirizzo IP del tunnel SSL VPN nel campo **Indirizzo trasmissione/unità** e fare clic su **Aggiorna**.
9. Selezionare il server Server Edition.

   Se si seleziona il sistema Server Edition, verrà visualizzata l'opzione Apri con Server Edition, abilitata per impostazione predefinita.
10. Selezionare **Usa accesso remoto** e fare clic su **OK**.

    Verrà visualizzata la finestra di dialogo Accesso utente del servizio di configurazione.
11. Immettere il nome utente per l'account amministratore di IP Office Manager for Server Edition nel campo **Nome utente servizio** e immettere la password per l'account amministratore di IP Office Manager for Server Edition nel campo **Password utente servizio**. Fare clic su **OK**.

Verrà visualizzata la schermata di riepilogo di IP Office Manager for Server Edition.

12. Nella tabella nella parte inferiore della schermata selezionare il Server Edition Primario.
13. Nell'elenco **Apri. . .** nel lato destro della schermata fare clic su **Configurazione**.

    Verrà visualizzata una struttura di navigazione per il sistema.
14. Dopo aver configurato il sistema selezionato e salvato le modifiche, selezionare **Rete** dall'elenco di navigazione per tornare alla schermata **Riepilogo**.
15. Per configurare altri sistemi Server Edition connessi al server Server Edition Primario, selezionare il sistema dalla tabella nella parte inferiore della schermata Riepilogo.

    La schermata Riepilogo visualizzerà le informazioni di configurazione per il sistema selezionato.

Collegamenti correlati

Monitoraggio e gestione del sistema IP Office alla pagina 65

Capitolo 10: Upgrade di IP Office in remoto

È possibile utilizzare il tunnel SSL VPN per eseguire l'upgrade del sistema IP Office dal sito del fornitore del servizio. Questa funzione è disponibile quando si esegue l'upgrade di un sistema 8.1 a una versione software superiore.

Se si utilizza Manager attraverso il tunnel SSL VPN, non è supportata l'individuazione automatica dei sistemi IP Office.

Eseguire questa procedura nel sito nel fornitore del servizio, utilizzando l'interfaccia di Manager installata nel server dell'agente del servizio. In caso di configurazione di un sistema Server Edition, utilizzare la modalità IP Office Manager for Server Edition.

Prerequisiti

Nel sito del fornitore del servizio è necessario installare il DVD IP Office Admin contenente la nuova versione software nel PC dell'agente del servizio.

Il tunnel SSL VPN deve essere in servizio ed è necessario disporre delle seguenti informazioni:

- indirizzo IP del tunnel SSL VPN

Procedura

1. Selezionare **File > Preferenze > Individuazione**.
2. Nel campo **Criteri di ricerca IP** immettere l'indirizzo IP del tunnel SSL VPN e fare clic su **OK**.
3. Selezionare **File > Avanzate > Aggiornamento**.

   Verrà visualizzato l'Aggiornamento guidato.

   Nota:

   Se viene visualizzata una finestra di dialogo contenente la richiesta di aprire un file di configurazione, fare clic su Annulla e procedere con questa fase. Non è necessario aprire un file di configurazione prima di eseguire un upgrade.
4. Nel campo **Indirizzo trasmissione/unità** immettere l'indirizzo IP del tunnel SSL VPN e fare clic su **Aggiorna**.

   Non immettere un indirizzo di trasmissione. Gli indirizzi di trasmissione non sono supportati per gli upgrade remoti su una connessione SSL VPN.
5. Fare clic su una casella di controllo per selezionare il sistema di cui si desidera eseguire l'upgrade e fare clic su **Aggiornamento**.

Una volta completato l'upgrade, verrà eseguito il riavvio di IP Office e il servizio SSL VPN si riconnetterà automaticamente.

Capitolo 11: Monitoraggio del servizio SSL VPN

Oltre al sistema IP Office, è possibile monitorare il tunnel SSL VPN. In questa sezione vengono fornite informazioni sugli strumenti di monitoraggio disponibili per il servizio SSL VPN e su come utilizzarli.

Per monitorare il servizio SSL VPN, è possibile utilizzare gli strumenti seguenti:

- System Status Application (SSA): System Status Application è uno strumento di diagnostica che consente di monitorare lo stato del tunnel SSL VPN. SSA segnala eventi in tempo reale e cronologici.
- SysMonitor: l'applicazione SysMonitor visualizza informazioni operative sul tunnel SSL VPN. Consente di acquisire le informazioni nei file di registro per l'analisi. Utilizzare questo strumento per acquisire informazioni solo quando richieste dal personale di supporto tecnico.
- Segnalazione degli errori: il servizio SSL VPN genera errori per i propri componenti quando si verificano problemi. È possibile impostare filtri eventi in modo da ricevere notifiche nel caso in cui si verifichino errori, nonché configurare la destinazione a cui verranno inviate le notifiche. Per informazioni su come impostare filtri eventi e configurare destinazioni di allarmi, vedere Configurazione di notifiche di allarme alla pagina 47.

Collegamenti correlati

Visualizzazione dello stato del tunnel alla pagina 76
Monitoraggio degli allarmi con SSA alla pagina 79
Risoluzione dei problemi relativi al servizio SSL VPN alla pagina 81

Visualizzazione dello stato del tunnel

Attenersi alla procedura indicata di seguito per visualizzare lo stato del tunnel SSL VPN con System Status Application (SSA).

Procedura

1. Avviare SSA mediante uno dei seguenti metodi:
   - Avviare SSA dal DVD IP Office.
   - Selezionare **Start > Programmi > IP Office > System Status**.

- In Manager selezionare **File > Avanzate > System Status**.

2. Selezionare **Reti IP > SSL VPN** dall'elenco di navigazione.

   Verrà visualizzata una tabella di riepilogo contenente informazioni su ogni servizio SSL VPN configurato.

3. Per visualizzare le informazioni dettagliate su uno specifico servizio SSL VPN, evidenziare il servizio SSL VPN e fare clic su **Seleziona**.

   Verrà visualizzata una tabella dettagliata contenente le informazioni di stato sul servizio SSL VPN selezionato.

Collegamenti correlati

Monitoraggio del servizio SSL VPN alla pagina 76
Descrizioni dei campi di Stato tunnel: tabella di riepilogo alla pagina 77
Descrizione dei campi Stato tunnel: tabella dei dettagli alla pagina 78

Descrizioni dei campi di Stato tunnel: tabella di riepilogo

System Status Application (SSA) visualizza le informazioni di riepilogo seguenti per il servizio SSL VPN:

Valore	Descrizione
Nome	Nome del servizio SSL VPN configurato in IP Office.
Stato servizio	Indica se SSL VPN è in servizio o in fallback.
Ora dell'ultima connessione	Indicatore di data e ora dell'ultima connessione.
Ora dell'ultima disconnessione	Indicatore di data e ora dell'ultima disconnessione.
Indirizzo IP tunnel	Indirizzo IP del tunnel SSL VPN.
Heartbeat complessivi persi	Conteggio cumulativo dei segnali heartbeat persi. Il conteggio viene riportato a 0 al riavvio di IP Office oppure in caso di deprovisioning del servizio SSL VPN in Manager.
Keep-alive complessivi persi	I keep-alive vengono utilizzati per le connessioni UDP. UDP non è supportato per il servizio SSL VPN. Il valore è 0.
Endpoint TCP locale	Indirizzo IP TCP e numero di porta di IP Office.
Endpoint TCP remoto	Si tratta dell'indirizzo pubblico e del numero di porta di AVG. VIP di AVG.
Endpoint UDP locale	UDP non è supportato per il servizio SSL VPN. Il valore è 0.
Endpoint UDP remoto	UDP non è supportato per il servizio SSL VPN. Il valore è 0.

Collegamenti correlati

Visualizzazione dello stato del tunnel alla pagina 76

Descrizione dei campi Stato tunnel: tabella dei dettagli

System Status Application (SSA) visualizza i dettagli seguenti per il servizio SSL VPN:

Valore	Descrizione
Nome del servizio	Nome del servizio configurato in IP Office.
Stato servizio	Indica se SSL VPN è in servizio o in fallback.
Nome account	Nome account del servizio SSL VPN. Il nome account viene utilizzato per l'autenticazione del servizio SSL VPN durante la connessione ad AVG.
Indirizzo server	Indirizzo del server gateway VPN nel sito del fornitore del servizio. L'indirizzo visualizzato può essere un indirizzo IPv4 o un indirizzo FQDN.
Tipo di server	Il servizio SSL VPN è supportato da Avaya VPN Gateway. Il tipo di server è AVG.
Protocollo	Il protocollo utilizzato dal servizio SSL VPN per il trasporto dati è TCP. Se si seleziona UDP come protocollo durante la configurazione della connessione, UDP verrà visualizzato in questo campo, ma il servizio SSL VPN tornerà a utilizzare il protocollo TCP.
Ora dell'ultima connessione	Indicatore di data e ora dell'ultima connessione.
Ora dell'ultima disconnessione	Indicatore di data e ora dell'ultima disconnessione.
Indirizzo IP tunnel	Indirizzo IP del tunnel SSL VPN.
Maschera di subnet del tunnel	Maschera di subnet del tunnel SSL VPN.
Indirizzo gateway del tunnel	Indirizzo IP del gateway predefinito IP di IP Office.
Dominio del tunnel	Indirizzo del dominio del tunnel.
Indirizzo TCP locale	Indirizzo IP TCP di IP Office.
Porta TCP locale	Porta TCP di IP Office. Il numero di porta è dinamico.
Indirizzo TCP remoto	Indirizzo IP TCP del server AVG.
Porta TCP remota	Porta TCP del server AVG. Il numero di porta predefinito è 443.
Indirizzo UDP locale	UDP non è supportato per il servizio SSL VPN. Il valore è 0.
Porta UDP locale	UDP non è supportato per il servizio SSL VPN. Il valore è 0.
Indirizzo UDP remoto	UDP non è supportato per il servizio SSL VPN. Il valore è 0.
Porta UDP remota	UDP non è supportato per il servizio SSL VPN. Il valore è 0.

Table continues…

Valore	Descrizione
Indirizzo DNS primario	Indirizzo del server DNS primario configurato in AVG. L'indirizzo viene fornito a scopo informativo e non viene utilizzato da IP Office.
Indirizzo DNS secondario	Indirizzo del server DNS secondario configurato in AVG. L'indirizzo viene fornito a scopo informativo e non viene utilizzato da IP Office.
Indirizzo WINS primario	WINS primario configurato in AVG. L'indirizzo viene fornito a scopo informativo e non viene utilizzato da IP Office.
Indirizzo WINS secondario	WINS secondario configurato in AVG. L'indirizzo viene fornito a scopo informativo e non viene utilizzato da IP Office.
Heartbeat complessivi persi	Conteggio cumulativo dei segnali heartbeat persi. Il conteggio viene riportato a 0 al riavvio di IP Office oppure in caso di deprovisioning del servizio SSL VPN in Manager.
Keep-alive complessivi persi	I keep-alive vengono utilizzati per le connessioni UDP. UDP non è supportato per il servizio SSL VPN. Il valore è 0.

Collegamenti correlati

Visualizzazione dello stato del tunnel alla pagina 76

Monitoraggio degli allarmi con SSA

Attenersi alla procedura indicata di seguito per visualizzare gli errori di sistema relativi al servizio SSL VPN segnalati in System Status Application (SSA).

Procedura

1. Avviare SSA mediante uno dei seguenti metodi:
   - Avviare SSA dal DVD IP Office.
   - Selezionare **Start > Programmi > IP Office > System Status**.
   - In Manager selezionare **File > Avanzate > System Status**.
2. Selezionare **Allarmi > Servizio** nell'elenco di navigazione.

   Verrà visualizzata una tabella contenente gli errori di sistema. Gli errori di sistema correlati al servizio SSL VPN sono identificati dal nome del servizio.

Collegamenti correlati

Monitoraggio del servizio SSL VPN alla pagina 76
Descrizioni degli allarmi SSA alla pagina 80

Descrizioni degli allarmi SSA

Gli errori di sistema indicati di seguito sono correlati al servizio SSL VPN e vengono segnalati in System Status Application (SSA).

Nome	Descrizione
Ultima data dell'errore	Data e ora in cui si è verificato l'allarme.
Occorrenze	Numero di volte in cui si è verificato l'errore dall'ultimo riavvio dell'unità di controllo o dall'ultima cancellazione dell'allarme.
Descrizione errore	Gli allarmi correlati al servizio SSL VPN visualizzano i messaggi di errore indicati di seguito, seguiti dal nome del servizio SSL VPN: • SSL VPN fuori servizio per manutenzione programmata • SSL VPN fuori servizio per server non raggiungibile o errore della rete • SSL VPN fuori servizio per errore di negoziazione della sessione TLS • SSL VPN fuori servizio per errore di rinegoziazione della chiave della sessione TLS • SSL VPN fuori servizio per mancanza di risorse in IP Office • SSL VPN fuori servizio per errore interno di IP Office • SSL VPN fuori servizio per troppi messaggi heartbeat persi • SSL VPN fuori servizio per FQDN server non risolto • SSL VPN fuori servizio per indirizzo IP duplicato rilevato in un'altra interfaccia IP Office • SSL VPN fuori servizio per errore di autenticazione • SSL VPN fuori servizio per errore del protocollo SOCKS • SSL VPN fuori servizio per errore riportato dal server

Collegamenti correlati

Monitoraggio degli allarmi con SSA alla pagina 79

Risoluzione dei problemi relativi al servizio SSL VPN

È possibile utilizzare le informazioni acquisite da SysMonitor per risolvere problemi di connettività. SysMonitor acquisisce informazioni che consentono di risolvere problemi nel caso in cui il servizio SSL VPN non si connetta ad AVG e System Status Application (SSA) non fornisca informazioni sufficienti a identificare la causa principale dell'errore.

Attenersi alla procedura indicata di seguito per acquisire informazioni solo quando richieste dal personale di supporto tecnico.

Procedura

1. Selezionare **Start > Programmi > IP Office > Monitor**.

   L'applicazione SysMonitor si connette al server IP Office e visualizza un registro del sistema.

2. Selezionare le opzioni **Filters > Trace** (Filtri > Traccia) e fare clic sulla scheda **VPN**.
3. Nell'area SSL VPN selezionare i filtri specificati dal supporto tecnico.
4. Fare clic su **OK**

   Nel registro di SysMonitor viene elencata l'attività del servizio SSL VPN sotto il nome configurato per il servizio.

Collegamenti correlati

Monitoraggio del servizio SSL VPN alla pagina 76
Descrizioni di output di SysMonitor alla pagina 81

Descrizioni di output di SysMonitor

Nella tabella seguente vengono elencati i filtri che è possibile selezionare in SysMonitor e vengono descritti gli output generati da ogni filtro. Queste informazioni sono destinate al personale di supporto tecnico per la risoluzione dei problemi relativi al servizio SSL VPN.

Nome	Descrizione
Configuration (Configurazione)	Visualizza informazioni sulla data di aggiunta, modifica o eliminazione del servizio SSL VPN.
Session (Sessione)	Visualizza informazioni sullo stato del servizio SSL VPN, ad esempio se il tunnel è in servizio o in fallback oppure sta tentando la connessione. Se il servizio SSL VPN è connesso, vengono mostrati i parametri del tunnel SSL VPN negoziati con AVG.
SessionState (StatoSessione)	Visualizza informazioni sullo stato quando si verifica un evento. Gli stati definiti sono: Idle, Connecting, Connected, Disconnecting, WaitingToStart, e NeedsRestart.

Table continues…

Nome	Descrizione
Fsm	Utilizzato per le connessioni UDP. UDP non è supportato per il servizio SSL VPN. Non viene generato alcun output.
Socks (Sock)	Visualizza gli eventi dello stack SOCKS attivati per mezzo di messaggi di segnalazione.
SocksState (StatoSock)	Visualizza gli stati interni dello stack SOCKS se vengono elaborati messaggi di segnalazione SOCKS5.
Heartbeat	Visualizza informazioni relative all'invio e alla ricezione di messaggi heartbeat.
Keepalive (Keep-alive)	Utilizzato per le connessioni UDP. UDP non è supportato per il servizio SSL VPN. Non viene generato alcun output.
SignalingPktRx (RicPaccSegnalazione)	Visualizza un flusso di byte di pacchetti di segnalazione SOCKS ricevuti da AVG.
SignalingPktTx (TrasmPaccSegnalazione)	Visualizza un flusso di byte di pacchetti di segnalazione SOCKS inviati a AVG.
DataPktRx (RicPaccDati)	Visualizza un sottoinsieme del datagramma, a partire dal pacchetto dati ricevuto dal tunnel SSL VPN da AVG e passato al sistema IP Office.
DataPktTx (TrasmPaccDati)	Visualizza un sottoinsieme del datagramma, a partire dal pacchetto dati inviato dall'interfaccia del tunnel SSL VPN ad AVG.
TunnelInterface (InterfacciaTunnel)	Visualizza informazioni sulle interazioni tra l'interfaccia del tunnel SSL VPN e lo stack IP di IP Office.
TunnelRoutes (InstradamentiTunnel)	Visualizza informazioni sugli instradamenti di split tunneling installati e rimossi dalla tabella degli instradamenti di IP Office.

Collegamenti correlati

Risoluzione dei problemi relativi al servizio SSL VPN alla pagina 81

Capitolo 12: Manutenzione del servizio SSL VPN

In questa sezione vengono descritte le attività eseguite regolarmente dopo aver configurato e connesso il servizio SSL VPN.

Utilizzare le informazioni in questa sezione per eseguire le attività di manutenzione seguenti:

- Trasferimento del tunnel fuori servizio e ripristino in servizio
- Modifica della password per l'account SSL VPN

Collegamenti correlati

Abilitazione e disabilitazione del servizio alla pagina 83
Reimpostazione della password alla pagina 89

Abilitazione e disabilitazione del servizio

Dopo aver configurato il servizio SSL VPN, sarà possibile utilizzare le interfacce indicate di seguito per abilitare o disabilitare il tunnel.

- Manager
- System Status Application(SSA)
- Codici funzione composti su telefoni da tavolo Avaya
- Tasti programmabili sui telefoni da tavolo Avaya supportati
- Assistente automatico configurato nei sistemi Embedded Voicemail o Voicemail Pro
- Amministrazione basata su gruppi nei telefoni da tavolo Avaya supportati

I metodi disponibili variano in base alla modalità operativa in uso.

Nella tabella indicata di seguito vengono elencati i metodi supportati in ogni modalità operativa.

Metodo	Modalità operativa			
	Essential Edition	IP Office Server Edition	Sistema di espansione Server Edition	Basic Edition
Manager	✔	✔	✔	—
SSA	✔	✔	✔	—
Codici funzione composti su telefoni da tavolo Avaya	✔	✔	✔	—
Tasti programmabili sui telefoni da tavolo Avaya supportati	✔	✔	✔	—
Assistente automatico in sistemi Embedded Voicemail o Voicemail Pro	✔	✔	✔	—
Amministrazione basata su gruppi	—	—	—	✔

Collegamenti correlati

Manutenzione del servizio SSL VPN alla pagina 83
Abilitazione del servizio con Manager alla pagina 84
Disabilitazione del servizio con Manager alla pagina 85
Abilitazione del servizio con SSA alla pagina 85
Disabilitazione del servizio con SSA alla pagina 86
Abilitazione del servizio con un codice funzione alla pagina 86
Disabilitazione del servizio con un codice funzione alla pagina 87
Abilitazione e disabilitazione del servizio mediante amministrazione basata su gruppi alla pagina 87
Abilitazione e disabilitazione del servizio con tasti programmabili alla pagina 88

Abilitazione del servizio con Manager

Attenersi alla procedura indicata di seguito per abilitare il servizio SSL VPN dall'interfaccia di Manager. In caso di configurazione di un sistema Server Edition, utilizzare la modalità IP Office Manager for Server Edition.

Prima di iniziare, lo stato del servizio SSL VPN deve essere In fallback.

Procedura

1. Nell'elenco di navigazione fare clic con il pulsante destro del mouse su **Servizio**.

   L'elenco verrà espanso per visualizzare i servizi configurati nel sistema.
2. Selezionare il servizio SSL VPN che si desidera abilitare.
3. Selezionare la scheda **Fallback** e deselezionare l'opzione **In fallback**.
4. Fare clic su **OK**.
5. Per salvare la configurazione, fare clic sull'icona **Salva**.

Collegamenti correlati

Abilitazione e disabilitazione del servizio alla pagina 83

Disabilitazione del servizio con Manager

Attenersi alla procedura indicata di seguito per disabilitare il servizio SSL VPN dall'interfaccia di Manager. In caso di configurazione di un sistema Server Edition, utilizzare la modalità IP Office Manager for Server Edition.

Prima di iniziare, lo stato del servizio SSL VPN deve essere In servizio.

Procedura

1. Nell'elenco di navigazione fare clic con il pulsante destro del mouse su **Servizio**.

   L'elenco verrà espanso per visualizzare i servizi configurati nel sistema.
2. Selezionare il servizio SSL VPN che si desidera disabilitare.
3. Selezionare la scheda **Fallback** e l'opzione **In fallback**.
4. Fare clic su **OK**.
5. Per salvare la configurazione, fare clic sull'icona **Salva**.

Collegamenti correlati

Abilitazione e disabilitazione del servizio alla pagina 83

Abilitazione del servizio con SSA

Attenersi alla procedura indicata di seguito per abilitare il servizio SSL VPN da System Status Application (SSA) . Prima di iniziare, lo stato del servizio SSL VPN deve essere In fallback.

Procedura

1. Avviare SSA mediante uno dei seguenti metodi:
   - Avviare SSA dal DVD IP Office.
   - Selezionare **Start > Programmi > IP Office > System Status**.
   - In Manager selezionare **File > Avanzate > System Status**.
2. Selezionare **Reti IP > SSL VPN** dall'elenco di navigazione.

3. Selezionare il servizio SSL VPN che si desidera abilitare dall'elenco.
4. Fare clic sul pulsante **Imposta in servizio**.

   Lo stato passa a In servizio.

Collegamenti correlati

Abilitazione e disabilitazione del servizio alla pagina 83

Disabilitazione del servizio con SSA

Attenersi alla procedura indicata di seguito per disabilitare il servizio SSL VPN da System Status Application (SSA) . Prima di iniziare, lo stato del servizio SSL VPN deve essere In servizio.

Procedura

1. Avviare SSA mediante uno dei seguenti metodi:
   - Avviare SSA dal DVD IP Office.
   - Selezionare **Start > Programmi > IP Office > System Status**.
   - In Manager o IP Office Manager for Server Edition selezionare **File > Avanzate > System Status**.
2. Selezionare **Reti IP > SSL VPN** dall'elenco di navigazione.
3. Selezionare il servizio SSL VPN che si desidera abilitare dall'elenco.
4. Fare clic sul pulsante **Imposta in fallback**.

   Verrà visualizzata una finestra di dialogo di conferma.
5. Fare clic su **Sì**.

   Verrà generato un allarme per confermare la disabilitazione del servizio SSL VPN.
6. Per visualizzare l'allarme, selezionare **Allarmi > Servizio** dall'elenco di navigazione.

   L'allarme visualizzerà il messaggio seguente: "SSL VPN fuori servizio per manutenzione programmata", seguito dal nome del servizio.

Collegamenti correlati

Abilitazione e disabilitazione del servizio alla pagina 83

Abilitazione del servizio con un codice funzione

Attenersi alla procedura indicata di seguito per abilitare il servizio SSL VPN componendo un codice funzione da un telefono da tavolo. Prima di iniziare, lo stato del servizio SSL VPN deve essere In fallback.

Prerequisiti

Questa funzione è disponibile solo se l'amministratore del sistema ha configurato codici funzione nel sistema IP Office. Per ulteriori informazioni, consultare Configurazione di codici funzione alla pagina 43. Prima di iniziare, è necessario conoscere il numero configurato dall'amministratore del sistema nel codice funzione per identificare il servizio SSL VPN.

Procedura

Da un telefono da tavolo collegato al sistema IP Office, immettere ***775x1**, dove *x* rappresenta un'istanza del servizio SSL VPN compreso tra 1 e 9. Se ad esempio l'amministratore del sistema ha configurato il codice funzione in modo che **1** identifichi il servizio SSL VPN, immettere ***77511**.

La connessione SSL VPN è in servizio.

Collegamenti correlati

Abilitazione e disabilitazione del servizio alla pagina 83

Disabilitazione del servizio con un codice funzione

Attenersi alla procedura indicata di seguito per disabilitare il servizio SSL VPN componendo un codice funzione da un telefono da tavolo. Prima di iniziare, lo stato del servizio SSL VPN deve essere In servizio.

Prerequisiti

Questa funzione è disponibile solo se l'amministratore del sistema ha configurato codici funzione nel sistema IP Office. Per ulteriori informazioni, consultare Configurazione di codici funzione alla pagina 43. Prima di iniziare, è necessario conoscere il numero configurato dall'amministratore del sistema nel codice funzione per identificare il servizio SSL VPN.

Procedura

Da un telefono da tavolo collegato al sistema IP Office, immettere ***775x0**, dove *x* rappresenta un'istanza del servizio SSL VPN compreso tra 1 e 9. Se ad esempio l'amministratore del sistema ha configurato il codice funzione in modo che **1** identifichi il servizio SSL VPN, immettere ***77510**.

La connessione SSL VPN è in fallback.

Collegamenti correlati

Abilitazione e disabilitazione del servizio alla pagina 83

Abilitazione e disabilitazione del servizio mediante amministrazione basata su gruppi

In alcuni modelli di telefoni Avaya è possibile utilizzare softkey per abilitare e disabilitare il servizio SSL VPN. In questa sezione vengono fornite informazioni su questa funzione e sui telefoni supportati.

Prerequisiti

Prima che questa funzione sia disponibile, è necessario configurare diritti di telefono del sistema per l'utente. Per informazioni su come impostare diritti di telefono del sistema, vedere *IP Office Manager*.

I telefoni devono essere collegati in una delle prime due porte della prima scheda nella piattaforma IP500 V2.

Informazioni su questa attività

È possibile utilizzare softkey per abilitare o disabilitare il servizio SSL VPN nei telefoni Avaya seguenti:

- Telefoni da tavolo ETR 18D e ETR 34D
- Telefono da tavolo digitale 1416
- Telefono da tavolo digitale 1408
- Telefoni da tavolo digitali 9504
- Telefoni da tavolo digitali 9508
- Telefoni da tavolo digitali T7316 e 7316E
- Telefoni da tavolo digitali M7310 e M7324

Nella procedura indicata di seguito viene fornita una guida generale per accedere alla funzione SSL VPN in questi telefoni. Per informazioni dettagliate sulle opzioni di menu, fare riferimento alla guida per l'utente relativa al telefono in uso.

Procedura

1. I menu in cui è necessario spostarsi per accedere alla funzione SSL VPN variano a seconda del modello di telefono in uso. Per accedere alla funzione SSL VPN, utilizzare uno dei metodi seguenti:
   - Selezionare **Ammin. > Amministrazione sistema > Parametri di sistema** e scorrere fino al servizio SSL VPN.
   - Selezionare **Ammin. > Funzione** e scorrere fino al servizio SSL VPN.
   - Selezionare **Ammin.** e premere **#775** per accedere al menu SSL VPN.
2. Premere il softkey appropriato per abilitare o disabilitare il servizio.

Collegamenti correlati

Abilitazione e disabilitazione del servizio alla pagina 83

Abilitazione e disabilitazione del servizio con tasti programmabili

Alcuni modelli di telefoni Avaya dispongono di tasti programmabili. È possibile utilizzare questi tasti come scorciatoie per non dover immettere un codice funzione o spostarsi all'interno dei menu nell'interfaccia utente al fine di attivare una funzione. L'amministratore del sistema può configurare un tasto programmabile che consente di abilitare e disabilitare il servizio SSL VPN.

Se l'amministratore di sistema ha configurato un tasto programmabile sul telefono per il servizio SSL VPN, verrà visualizzata un'etichetta accanto al tasto programmato sul telefono.

Premere il tasto per abilitare (in servizio) e disabilitare (in fallback) il servizio SSL VPN.

Lo stato del servizio SSL VPN verrà visualizzato accanto al tasto sul telefono. Il modo in cui viene visualizzato lo stato varia in base al modello del telefono. Ad esempio, alcuni telefoni visualizzano un'icona, altri utilizzano LED per indicare lo stato di una funzione. Se l'icona è visualizzata o il LED è illuminato, il servizio SSL VPN è abilitato.

Se si preme il tasto per disabilitare il servizio SSL VPN, l'icona non sarà più visibile e il LED si spegnerà.

Collegamenti correlati

Abilitazione e disabilitazione del servizio alla pagina 83

Reimpostazione della password

In questa sezione vengono descritti i metodi che è possibile utilizzare per reimpostare la password per il servizio SSL VPN.

Sono disponibili due metodi per reimpostare la password del servizio SSL VPN.

- È possibile modificare la password nel file di On-Boarding e reimportarla.
- È possibile modificare la password mediante Manager.

Per entrambi i metodi è inoltre necessario modificare la password configurata per il servizio SSL VPN nel server RADIUS.

Collegamenti correlati

Manutenzione del servizio SSL VPN alla pagina 83
Reimpostazione della password mediante un file di On-Boarding alla pagina 89
Reimpostazione della password con Manager alla pagina 90

Reimpostazione della password mediante un file di On-Boarding

Attenersi alla procedura indicata di seguito se si è già configurato il servizio SSL VPN in un sistema IP Office e si necessita di modificare il servizio SSL VPN.

Eseguire questa procedura nell'interfaccia di Avaya IP Office Web Manager nel sito del cliente.

Prerequisiti

Prima di iniziare, è necessario disporre delle informazioni seguenti:

- nome del servizio SSL VPN
- nome account utilizzato per l'autenticazione del servizio SSL VPN durante la connessione ad AVG.

È possibile utilizzare System Status Application (SSA) per cercare il nome del servizio SSL VPN e il nome account. Per ulteriori informazioni, vedere Visualizzazione dello stato del tunnel alla pagina 76.

È inoltre necessario reimpostare la password per il servizio SSL VPN nel server RADIUS.

Procedura

1. Selezionare **Strumenti > On-Boarding**.

   Verrà visualizzata la finestra di dialogo On-Boarding.

2. Fare clic su **Modifica**.

   Verrà visualizzato il sito Web Avaya in un browser.

3. Accedere al sito Web.

   Verrà visualizzata la pagina di connettività remota e gestione password di IP Office.

4. Fare clic su **Existing IP Office SSL VPN Remote Connectivity** (Connettività remota SSL VPN IP Office esistente).

5. Selezionare **Password Reset** (Reimpostazione password).

   Verrà visualizzato il nome del servizio SSL VPN predefinito.

6. Verificare che il nome del servizio visualizzato corrisponda al nome del servizio SSL VPN per cui si desidera reimpostare la password. Se il nome del servizio predefinito non corrisponde, immettere il nome del servizio.

7. Immettere il nome account SSL VPN.

8. Fare clic su **Submit** (Invia).

9. Selezionare se si desidera ricevere il file di On-Boarding aggiornato tramite posta elettronica oppure scaricare il file aggiornato e seguire i prompt visualizzati.

10. Una volta scaricato o ricevuto il file di On-Boarding aggiornato, salvarlo nel sistema locale.

11. Passare al percorso in cui è stato salvato il file di On-Boarding e fare clic su **Carica** nell'interfaccia di Web Manager.

    Verrà visualizzato un messaggio di conferma dell'installazione del file di On-Boarding.

Passi successivi

Dopo aver reimpostato la password, confermare l'avvenuta riconnessione del servizio SSL VPN a AVG seguendo la procedura in Visualizzazione dello stato del tunnel alla pagina 76.

Collegamenti correlati

Reimpostazione della password alla pagina 89

Reimpostazione della password con Manager

Attenersi alla procedura indicata di seguito per modificare la password per il servizio SSL VPN. Eseguire questa procedura nell'interfaccia di Manager nel sito del cliente. In caso di configurazione di un sistema Server Edition, utilizzare la modalità IP Office Manager for Server Edition.

Prerequisiti

È inoltre necessario reimpostare la password per il servizio SSL VPN nel server RADIUS.

Procedura

1. Nell'elenco di navigazione selezionare **Servizio**.
2. Selezionare il nome del servizio SSL VPN.

3. Selezionare la scheda **Sessione** e immettere la nuova password per l'account del servizio SSL VPN nel campo **Password account**.
4. Reimmettere la password nel campo **Conferma password**.
5. Fare clic su **OK**.
6. Per salvare la configurazione, fare clic sull'icona **Salva**.

Collegamenti correlati

Reimpostazione della password alla pagina 89

Capitolo 13: Appendice A: Esempio relativo alla procedura guidata per la configurazione rapida di AVG

Per avviare la procedura guidata, avviare una nuova immagine AVG. Nella console una volta visualizzato il prompt `localhost login:`, accedere con nome utente "admin" e password "admin". Viene visualizzato il menu della procedura guidata. Selezionare `new` e seguire le istruzioni visualizzate.

Configurare le interfacce AVG

```
Enter port number for the management interface [1-4]: 1
Enter IP address for this machine (on management interface): 172.16.1.5
Enter network mask [255.255.255.0]:
Enter VLAN tag id (or zero for no VLAN) [0]:
Setup a two armed configuration (yes/no) [yes]:
Enter port number for the traffic interface [1-4]: 2
Enter IP address for this machine (on traffic interface): 10.136.66.195
Enter network mask [255.255.255.0]:
Enter VLAN tag id (or zero for no VLAN) [0]:
Enter default gateway IP address (on the traffic interface): 10.136.66.1
Enter the Management IP (MIP) address: 172.16.1.6
Making sure the MIP does not exist...ok
Trying to contact gateway...ok
```

Configurare il certificato autofirmato

```
Enter a timezone or 'UTC' or 'select' [select]: UTC
Enter the current date (YYYY-MM-DD) [2014-11-20]:
Enter the current time (HH:MM:SS) [23:54:18]:
Enter NTP server address (or blank to skip):
Enter DNS server address: 198.152.7.12
   Enabled SSH (allow CLI access).
Enter a password for the "admin" user:
Re-enter to confirm:
Run VPN quick setup wizard [yes]:
Enter VPN Portal IP address: 10.136.66.196
   Using VPN device without an Alteon switch.
   Using empty DNS search list.
   Creating HTTP to HTTPS redirect server.
   Enabling HTTPS BBI on port 443.
Use self-signed certificate (yes/no) [yes]:
!!!The combined length of the following parameters may not exceed 225 bytes!!!
Country Name (2 letter code): ca
State or Province Name (full name): on
Locality Name (eg, city): ottawa
Organization Name (eg, company): smec
Organizational Unit Name (eg, section):
Common Name (eg, your name or your server's hostname): testavg
Email Address:
Subject alternative name (blank or comma separated list of
URI:<uri>, DNS:<fqdn>, IP:<ip-address>, otherName:<string>, email:<email-address
>):
Valid for days [2556 (7 years)]:
Key size (512/1024/2048/4096) [2048]:
```

Opzione 1: Configurare il pool IP locale

```
Use RADIUS authentication server (yes/no) [yes]: no
   Using LOCAL authentication.
Enter Lower IP address in pool range: 172.30.0.1
Enter Upper IP address in pool range: 172.30.255.254
Enter Network mask for the pool range [255.255.255.0]: 255.255.0.0
```

Opzione 2: Configurare il server RADIUS

```
Use RADIUS authentication server (yes/no) [yes]:
Use generic RADIUS server configuration parameters (yes/no) [yes]:
Enter RADIUS server IP address: 172.16.1.2
Enter shared secret:
Re-enter to confirm:
```

Configurare la subnet dell'agente di servizio

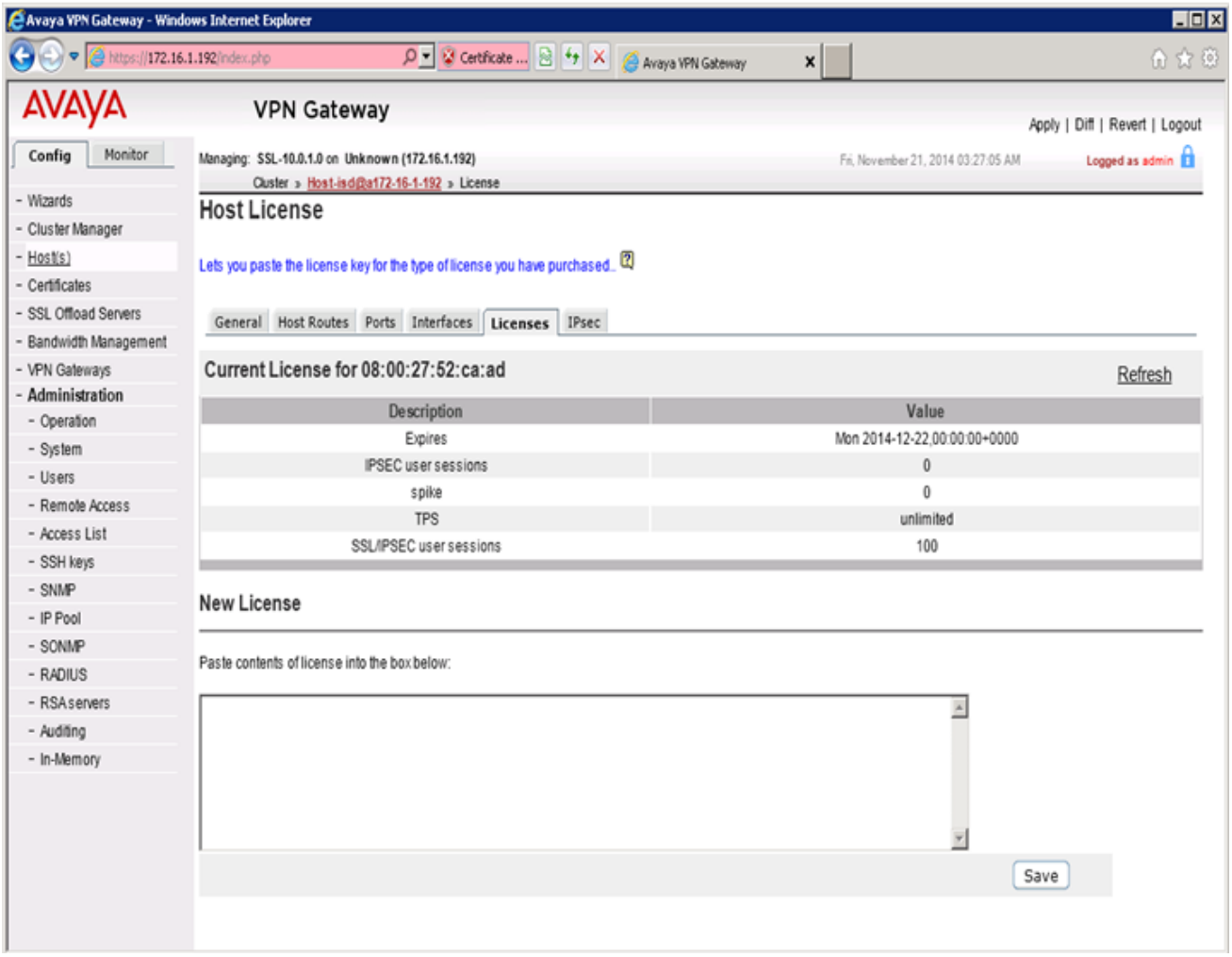
Nota:

Se la subnet dell'agente di servizio si trova sulla stessa subnet dell'interfaccia host di AVG, ad esempio 172.16.1.0 maschera di rete 255.255.255.0, viene visualizzato un prompt per il gateway anche se quest'ultimo non è configurato o utilizzato. Se per la subnet dell'interfaccia host è presente un gateway disponibile, utilizzare l'indirizzo IP del gateway (e.g. 172.16.1.1). In caso contrario, immettere nuovamente l'indirizzo della subnet (ad es. 172.16.1.0).

```
Enter intranet network address: 172.17.1.0
Enter intranet network mask [255.255.255.0]:
Enter intranet gateway: 172.16.1.1
   Enabling network attributes.
   Enabling NetDirect.
   Enabling Split Tunnel Mode.
   Set splittun based on intranet network.
   Added a static route with intranet network.
   Creating empty portal linkset 'base-links'.
   Creating group 'trusted' with secure access.
   Creating network access rule to allow only intranet network for group 'truste
d'.
   Asigning portal linkset 'base-links' to group 'trusted'.
   Creating group 'ipoffice' with secure access.
   Creating network access rule to allow only intranet network for group 'ipoffi
ce'.
   Asigning portal linkset 'base-links' to group 'ipoffice'.
Initializing system.....
```

Aggiunta della licenza SSL VPN

Accedere all'interfaccia AVG per aggiungere una licenza.

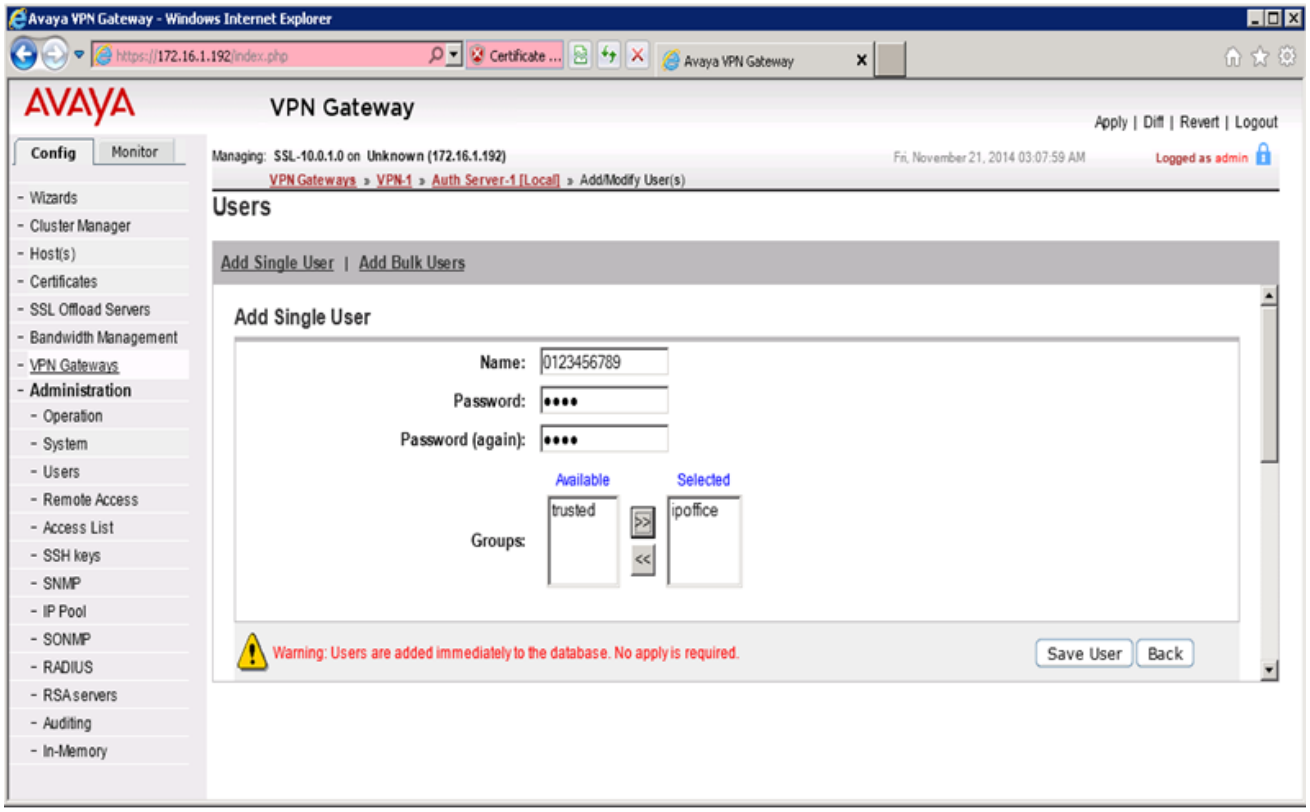


Aggiunta di un utente

A questo punto, la configurazione è terminata.

Se è stata utilizzata l'opzione 1, configurare il pool IP locale. A questo punto, è possibile aggiungere utenti nel database AVG locale. Gli utenti devono far parte del gruppo di **ipoffice**.

Appendice A: Esempio relativo alla procedura guidata per la configurazione rapida di AVG



Capitolo 14: Appendice B: Modifica dell'AVG predefinito per il servizio SSL VPN (con schermate)

Dopo aver eseguito la configurazione rapida e la configurazione guidata per Net Direct, è necessario modificare la configurazione predefinita in modo che supporti una connessione SSL VPN con un sistema IP Office.

Eseguire questa procedura mediante l'interfaccia BBI basata sul browser di AVG. Vedere *Avaya VPN Gateway BBI Application Guide* (Guida all'applicazione BBI di Avaya VPN Gateway).

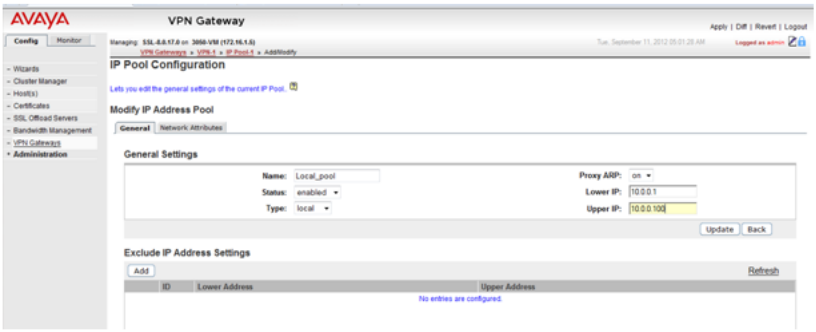
Prerequisiti

Assicurarsi che il gateway predefinito configurato in AVG risponda alle richieste ICMP. Se il gateway predefinito non risponde alle richieste ICMP, AVG non può fornire i servizi VPN.

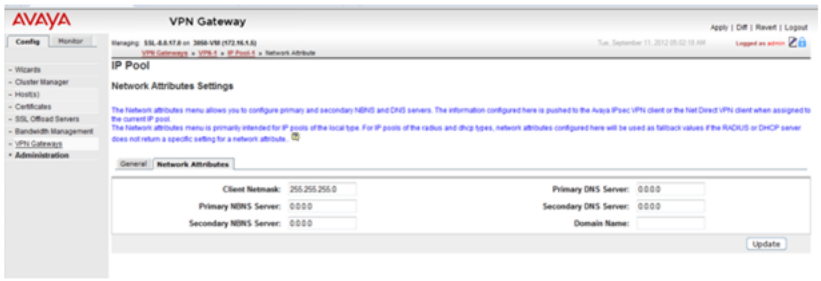
Procedura

1. Accedere all'interfaccia BBI di AVG come amministratore.
2. Nel riquadro di navigazione di sinistra, selezionare la scheda **Config** (Configurazione), quindi **VPN Gateway** > **VPN1** > **IP Pool** (Pool IP).
3. Il VPN predefinito della configurazione di base di AVG potrebbe già contenere un pool locale. In caso contrario, è necessario aggiungerne uno al VPN predefinito. Nella pagina **Add new IP Address Pool** (Aggiungi nuovo pool di indirizzi IP), aggiungere un pool locale al VPN predefinito.

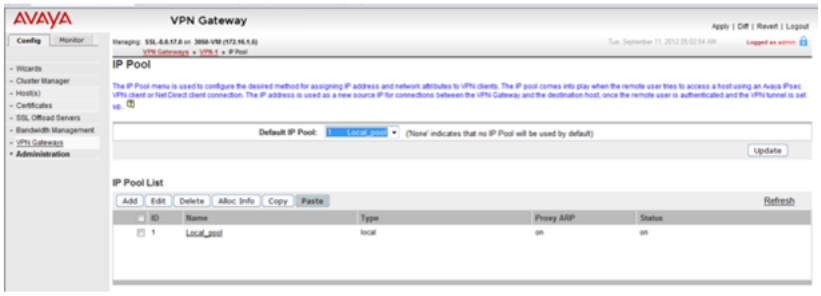
4. Nella pagina **Modify IP Address Pool** (Modifica pool di indirizzi IP), verificare che i valori nei campi **Lower IP** (IP più basso) e **Upper IP** (IP più alto) corrispondano a quelli impostati con la configurazione guidata di Net Direct.



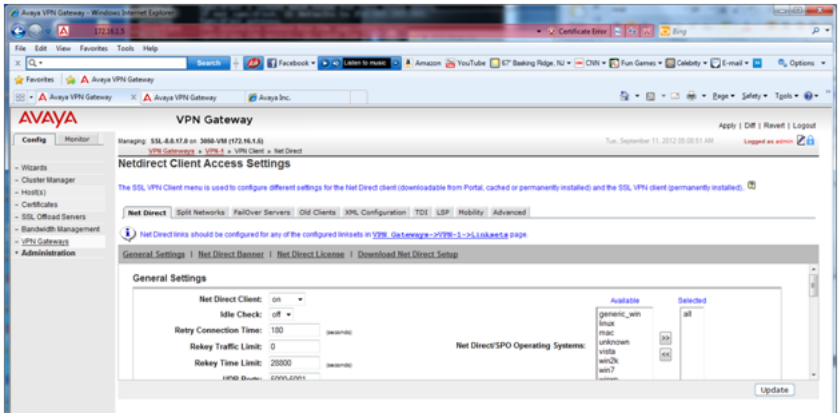
5. Nella pagina **IP Pool (Pool IP)** > **Network Attributes Settings (Impostazioni attributi di rete)**, selezionare la scheda **Network Attributes** (Attributi di rete) e immettere i valori per la rete in uso.



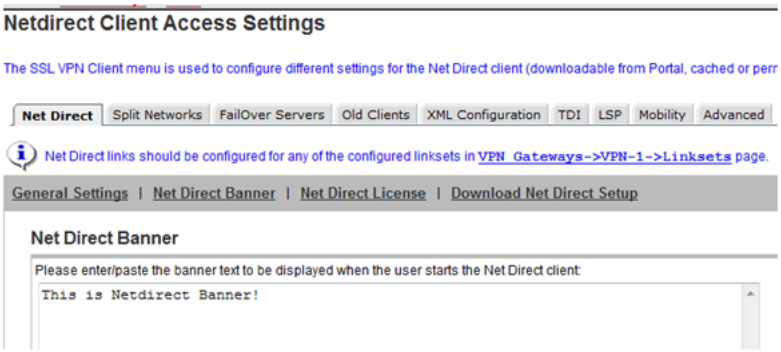
6. Nella pagina **IP Pool** (Pool IP), impostare **Default IP Pool** (Pool IP predefinito) sul pool locale creato nel passo 3.



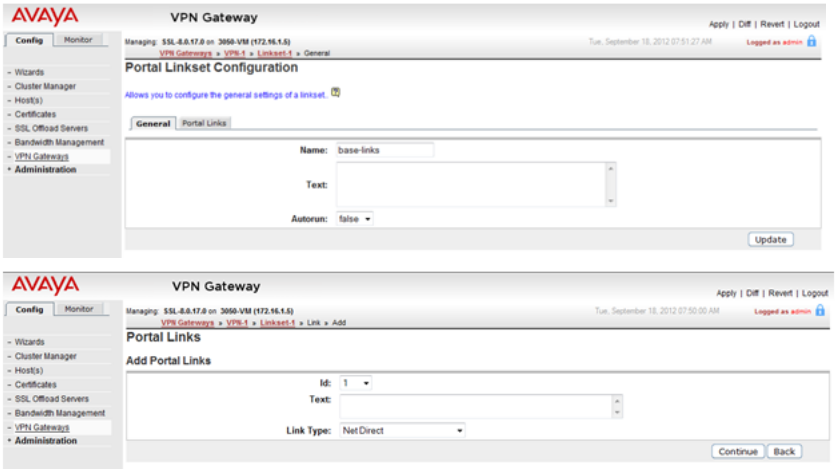
7. Nella pagina **Net Direct Client Access Settings** (Impostazioni di accesso al client Net Direct), verificare le impostazioni create dalla configurazione guidata di Net Direct.
   a. Assicurarsi che **Idle Check** (Controllo inattività) sia impostato su **off** (disattivato).



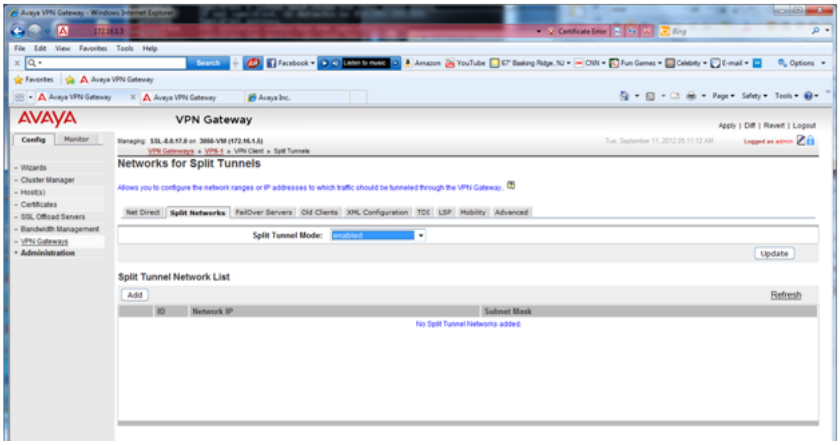
b. Assicurarsi che sia impostato il banner Net Direct.



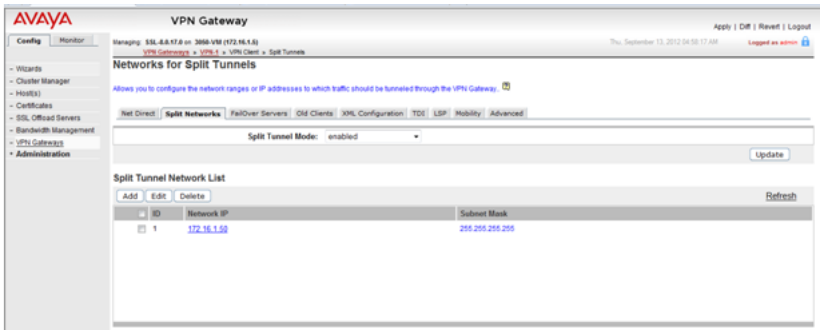
8. Impostare il collegamento del portale per avviare il client Net Direct. Nella pagina **Portal Linkset Configuration** (Configurazione set di collegamenti del portale), selezionare la scheda **Portal Link** (Collegamento portale). Nel campo **Link Type** (Tipo di collegamento), selezionare **Net Direct**.



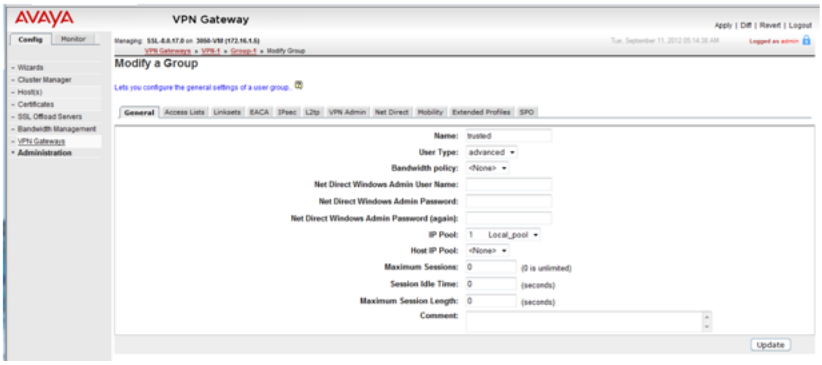
9. Nella pagina **Networks for Split Tunnels** (Reti per split tunneling):
   a. impostare **Split Tunnel Mode** (Modalità split tunneling) su **enabled** (abilitata);



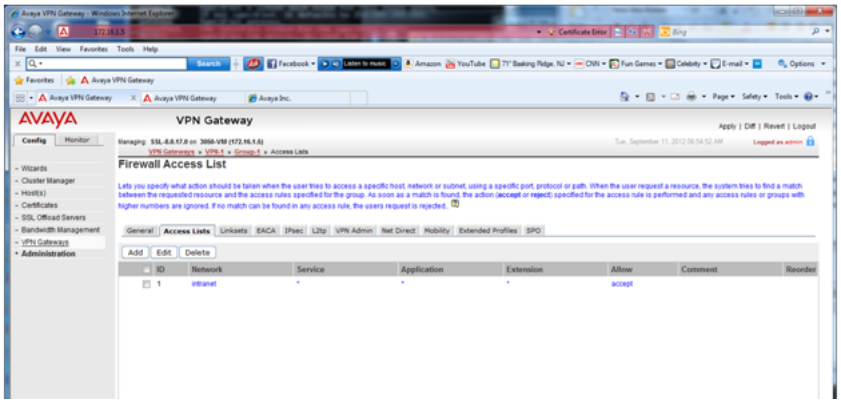
b. impostare gli instradamenti di split tunneling in modo da raggiungere l'agente del servizio sulla rete privata.



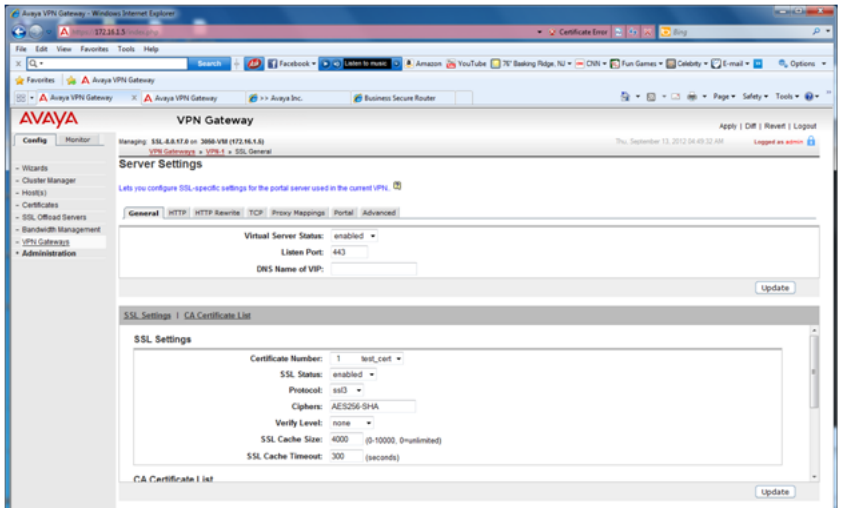
10. Per VPN1, accedere alla pagina dei gruppi e selezionare **Group1** (Gruppo 1). Nella pagina **Modify a Group** (Modifica un gruppo), impostare il pool di IP su quello locale creato al punto 3.



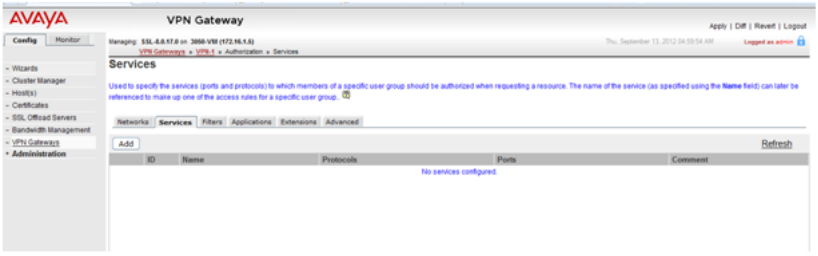
11. Accedere alla pagina **VPN1** > **Group1 (Gruppo 1)** > **Access Lists (Elenchi di accesso)**. Nella pagina **Firewall Access List** (Elenco di accesso al firewall), creare una regola di accesso, qualora non sia già stata creata per impostazione predefinita.



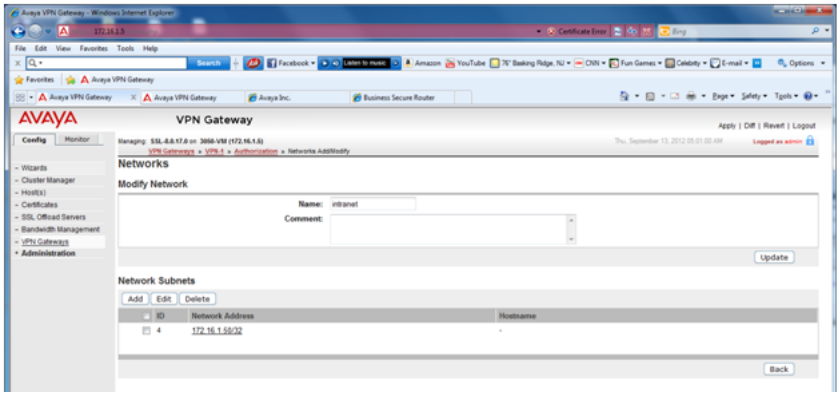
12. Accedere alla pagina **VPN1** > **SSL**. Nella pagina **Server Settings** (Impostazioni server), alla sezione **SSL Settings** (Impostazioni SSL) impostare **Ciphers** (Cifrature) su **AES256-SHA** per avere una codifica molto sicura.



13. Accedere alla pagina **VPN1** > **Authorization (Autorizzazione)** > **Services (Servizi)**. Rimuovere tutti i servizi impostati nella configurazione predefinita, poiché non sono richiesti dal servizio SSL VPN.



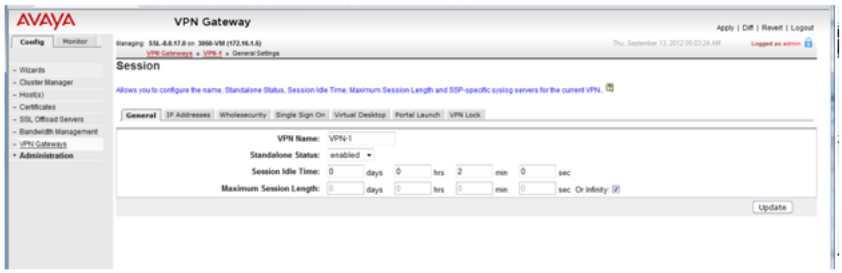
14. Accedere alla pagina **VPN1** > **Authorization (Autorizzazione)** > **Networks (Reti)**. Impostare la subnet della rete di autorizzazione alla quale viene fatto riferimento in una delle regole di accesso impostata in **VPN1** > **Group1 (Gruppo 1)** > **Access Lists (Elenchi di accesso)**.



Nota:

I controlli delle impostazioni del servizio SSL VPN effettuano il tunneling della comunicazione intermedia. La comunicazione viene attivata solo specificando un elenco numero autorizzati delle reti "intranet". La comunicazione del client Inter-VPN è bloccata per impostazione predefinita.

15. Accedere alla pagina **VPN1** > **General Settings (Impostazioni generali)** > **Session (Sessione)**. Impostare **Session Idle Time** (Tempo di inattività sessione) su 2 minuti.



Capitolo 15: Appendice C: configurazione dell'autenticazione RADIUS (con schermate)

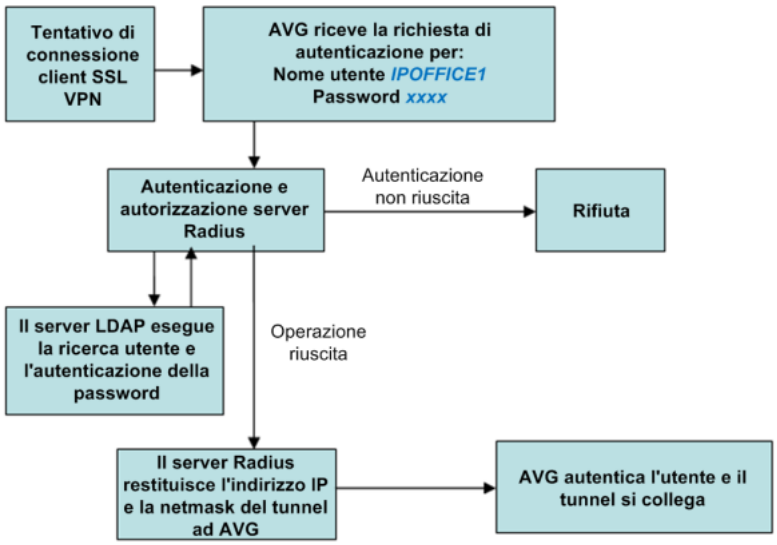
Il vantaggio maggiore dell'autenticazione RADIUS è che al servizio SSL VPN viene sempre assegnato lo stesso indirizzo IP per il tunneling.

Per configurare l'autenticazione RADIUS, è necessario installare un server RADIUS. Avaya consiglia di utilizzare Avaya Identity Engine per un server RADIUS. Per informazioni e modalità di scaricamento del software, accedere a http://support.avaya.com.

Le informazioni di autenticazione del protocollo RADIUS, ad esempio dati dell'account utente e informazioni di tunneling SSL VPN come indirizzo IP e maschera di rete, devono essere memorizzate in un database. Sono disponibili due opzioni:

- Utilizzare il database locale di Identity Engine per memorizzare le informazioni utente e fornire i servizi di ricerca e autenticazione e autorizzazione. Questa opzione è ideale nel caso di un numero ridotto di utenti. Identity Engine dispone di un numero limitato di utenti. Consultare la documentazione per conoscere il valore esatto.
- Utilizzare un server LDAP per memorizzare le credenziali utente e le informazioni di tunneling SSL VPN per i servizi di ricerca e autenticazione. Questa opzione è ideale per scenari di distribuzione con un ampio numero di utenti.

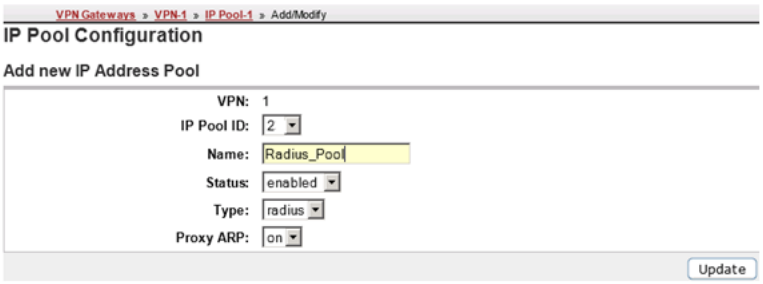
Per un'installazione con server LDAP, la documentazione di Avaya Identity Engine per server RADIUS contiene le opzioni per configurare i server LDAP di vari produttori. L'autenticazione RADIUS mediante server LDAP è descritta nella figura in basso. La configurazione con server RADIUS descritta in questa procedura non richiede un server LDAP.



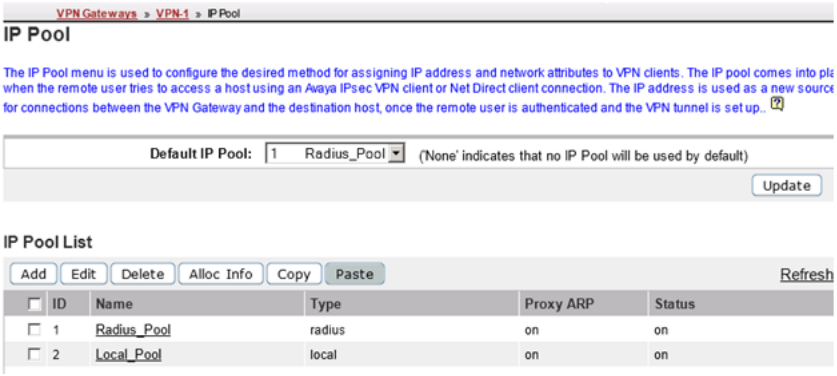
Questa procedura descrive i passi manuali per configurare l'autenticazione RADIUS. In alternativa, è possibile configurare l'autenticazione utilizzando la procedura guidata di autenticazione di AVG.

Procedura

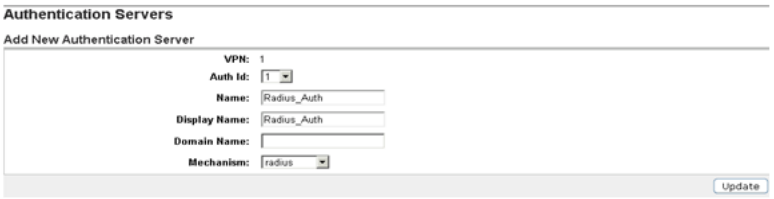
1. Accedere all'interfaccia BBI di AVG come amministratore.
2. Nella pagina **IP Pool Configuration** (Configurazione pool IP), aggiungere un nuovo pool di indirizzi IP per l'autenticazione RADIUS.



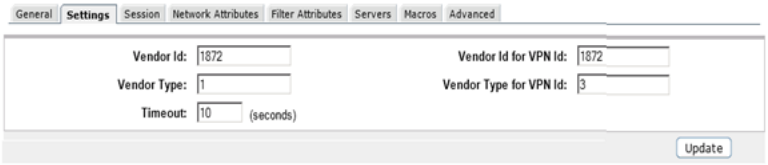
3. Nella pagina **IP Pool** (Pool IP), impostare **Default IP Pool** (Pool IP predefinito) sul pool di indirizzi IP per l'autenticazione RADIUS creato nel passo 2.



4. Modificare il VPN. Nella pagina **Authentication Servers (Server di autenticazione)** > **Add New Authentication Server (Aggiungi nuovo server di autenticazione)**, compilare i campi per il server RADIUS.



5. Configurare le impostazioni del server di autenticazione RADIUS. L'ID produttore 1872 è associato ad Alteon e identifica AVG. Selezionare la scheda **Settings** (Impostazioni) e compilare i seguenti campi.
   - **ID produttore: 1872**
   - **Tipo di produttore: 1**
   - **Timeout: 10**
   - **ID produttore per ID VPN: 1872**
   - **Tipo di produttore per ID VPN: 3**

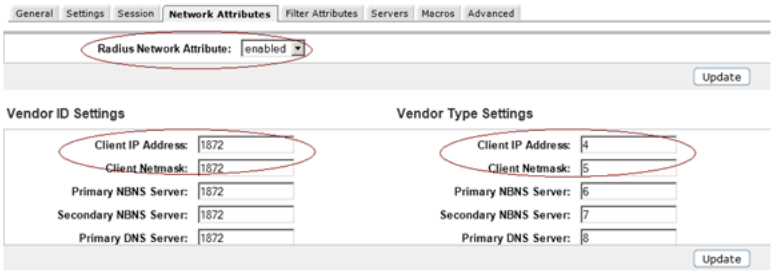


6. Configurare gli attributi di rete RADIUS. Selezionare la scheda **Network Attributes** (Attributi di rete) e compilare i seguenti campi.

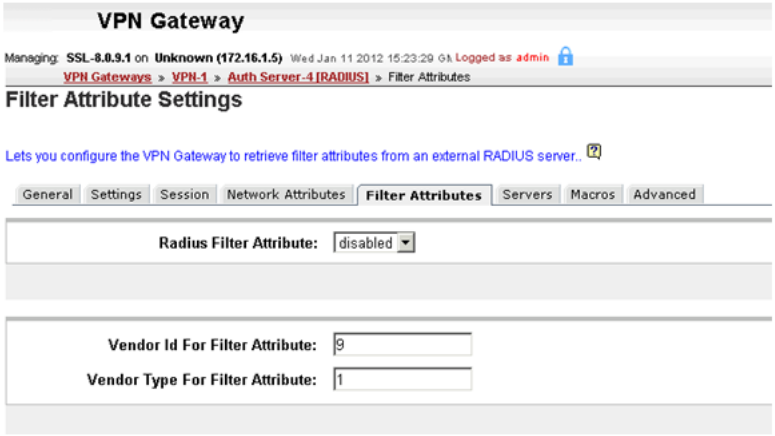
Impostazioni ID produttore	Impostazioni tipo di produttore
Indirizzo IP client: 1872	Indirizzo IP client: 4
Maschera di rete client: 1872	Maschera di rete client: 5
Server NBNS primario: 1872	Server NBNS primario: 6

Table continues…

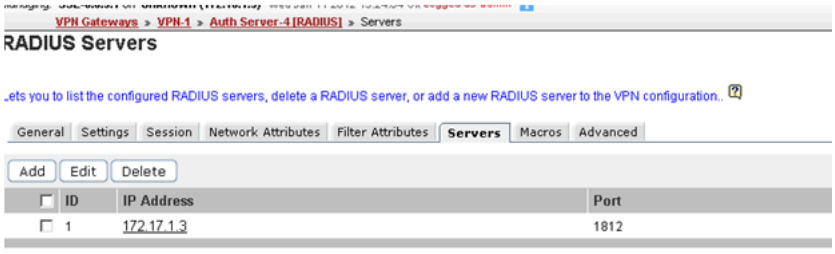
Impostazioni ID produttore	Impostazioni tipo di produttore
Server NBNS secondario: 1872	Server NBNS secondario: 7
Server DNS primario: 1872	Server DNS primario: 8



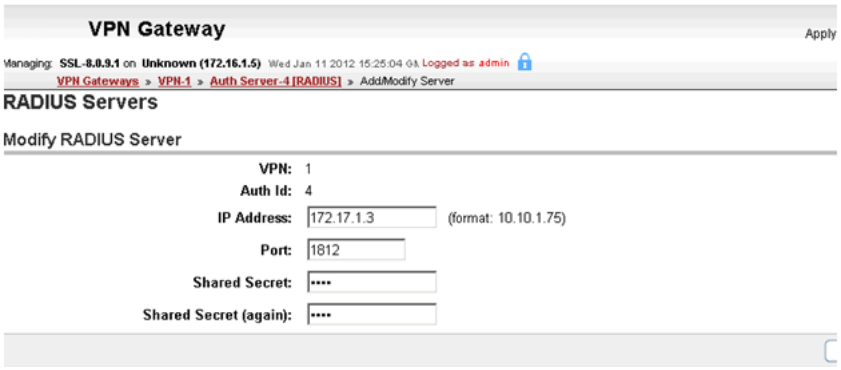
7. Configurare gli attributi di filtro. Selezionare la scheda Attributi di filtro e compilare i seguenti campi.
   - **Attributo di filtro RADIUS: disabilitato**
   - **ID produttore per attributo di filtro: 9**
   - **Tipo di produttore per attributo di filtro: 1**



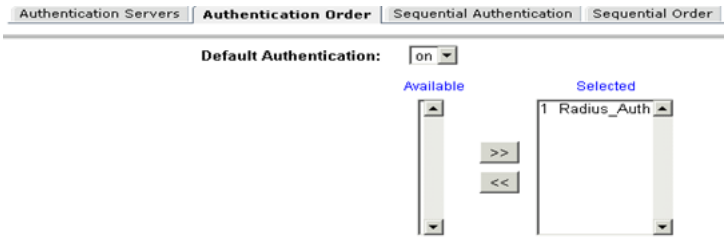
8. Specificare l'indirizzo del server RADIUS. Selezionare la scheda **Servers** (Server) nella pagina **RADIUS Servers** (Server RADIUS).



9. Fare clic su **Add** (Aggiungi) e immettere nella pagina **Modify RADIUS Server** (Modifica server RADIUS) l'indirizzo IP del server RADIUS e il segreto condiviso.



10. Selezionare la scheda **Authentication Order** (Ordine di autenticazione) e specificare l'ordine desiderato per i metodi di autenticazione.



Capitolo 16: Appendice D: impostazioni di configurazione AVG

```
[Main Menu]       info       - Information menu       stats      -
Statistics menu       cfg        - Configuration menu       boot
     - Boot menu       maint      - Maintenance menu       diff
    - Show pending config changes   [global command]       apply
    - Apply pending config changes  [global command]       revert
    - Revert pending config changes [global command]       paste
    - Restore saved config with key [global command]       help
    - Show command help             [global command]       exit
    - Exit  [global command, always available]

>> Main# cfg

------------------------------------------------------------
[Configuration Menu]
      ssl        - SSL offload menu
      cert       - Certificate menu
      vpn        - VPN menu
      test       - Create test vpn, portal and certificate
      quick      - Quick vpn setup wizard
      sys        - System-wide parameter menu
      lang       - Language support
      bwm        - Bandwidth management menu
      log        - logging system menu
      ptcfg      - Backup configuration to TFTP/FTP/SCP/SFTP server
      gtcfg      - Restore configuration from TFTP/FTP/SCP/SFTP server
      dump       - Dump configuration on screen for copy-and-paste

>> Configuration# dump
Dump private/secret keys (yes/no) [no]:
Collecting data, please wait...
/*
/*
/* Alteon iSD SSL
/* Configuration dump taken Tue Sep 18 08:40:50 EDT 2012
/* Hardware Platform: 3050-VM
/* Software Version: 8.0.17.0
/* Uptime:  8 days 3 hours 59 minutes
/* IP Address: 172.16.1.4
/* Hardware Address: 00:0c:29:e0:d8:73
/* Disk space:   config         10110  386513  3 %
  user_content   32832  6015488  1 %

/*
/*
/cfg/.
/cfg/ssl/.
/cfg/ssl/server 1/.
        name "Redirect to VPN 1"
        vips 216.13.56.91
```

```
        standalone off
        port "80 (http)"
        rip 0.0.0.0
        rport 81
        type http
        proxy on
        loopback on
        fastfin off
        ena enabled
/cfg/ssl/server 1/trace/.
/cfg/ssl/server 1/ssl/.
        cert 1
        cachesize 4000
        cachettl 5m
        renegotiate legacy
        protocol ssl3
        verify none
        log none
        verifylog none
        ciphers ALL:-EXPORT:-LOW!ADH
        ena disabled
/cfg/ssl/server 1/tcp/.
        cwrite 15m
        ckeep 15m
        swrite 15m
        sconnect 30s
        csendbuf auto
        crecbuf auto
        ssendbuf auto
        srecbuf 6000
/cfg/ssl/server 1/http/.
        httpsredir on
        redirect on
        downstatus unavailable
        securecookie off
        certcard off
        cookieonce off
        sslheader on
        sslxheader off
        sslsidheader off
        addxfor off
        addvia on
        addxisd off
        addfront off
        addbeassl off
        addbeacli off
        addclicert off
        addnostore off
        nocachehdr off
        compress off
        cmsie on
        rhost off
        maxrcount 40
        maxline 16384
        urlobscure off
        sessionhdr off
/cfg/ssl/server 1/http/redirmap/.
/cfg/ssl/server 1/http/dynheader/.
/cfg/ssl/server 1/http/rewrite/.
        paramtag none
        urldeferattr on
        rewrite off
        ciphers HIGH:MEDIUM
        response iSD
        URI "/cgi-bin/weakcipher"
```

```
/cfg/ssl/server 1/http/auth/.
        mode basic
        realm Xnet
        proxy off
        ena disabled
/cfg/ssl/server 1/dns/.
/cfg/ssl/server 1/adv/.
/cfg/ssl/server 1/adv/pool/.
        timeout 15s
        ena disabled
/cfg/ssl/server 1/adv/traflog/.
        protocol bsd
        sysloghost 0.0.0.0
        udpport 514
        priority info
        facility local4
        ena disabled
/cfg/ssl/server 1/adv/loadbalancing/.
        type all
        persistence none
        metric hash
        health auto
        interval 10s
        grace on
        ena disabled
/cfg/ssl/server 1/adv/loadbalancing/script/.
/cfg/ssl/server 1/adv/loadbalancing/remotessl/.
        protocol ssl3
        ciphers ALL
/cfg/ssl/server 1/adv/loadbalancing/remotessl/verify/.
        verify none
/cfg/ssl/server 1/adv/sslconnect/.
        protocol ssl3
        cachemode on
        ciphers EXP-RC4-MD5:ALL!DH
        ena disabled
/cfg/ssl/server 1/adv/sslconnect/verify/.
        verify none
/cfg/cert 1/.
        name test_cert
        cert
-----BEGIN CERTIFICATE-----
MIIEejCCA+OgAwIBAgIJAODDyCE7V9E3MA0GCSqGSIb3DQEBBAUAMIG/MQswCQYD
VQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5pYTEQMA4GA1UEBxMHVGVzdGluZzEo
MCYGA1UEChMfVGVzdCBJbmMuIDEgMDQ6Mzc6MjEgMjAxMi0wOS0xMDESMBAGA1UE
CxMJdGVzdCBkZXB0MSAwHgYDVQQDExd3d3cuZHVtbXlzc2x0ZXN0aW5nLmNvbTEp
MCcGCSqGSIb3DQEJARYadGVzdGVyQGR1bW15c3NsdGVzdGluZy5jb20wHhcNMTIw
OTEwMDgzNzIyWhcNMTMwOTEwMDgzNzIyWjCBvzELMAkGA1UEBhMCVVMxEzARBgNV
BAgTCkNhbGlmb3JuaWExEDAOBgNVBAcTB1Rlc3RpbmcxKDAmBgNVBAoTH1Rlc3Qg
SW5jLiAxIDA0OjM3OjIxIDIwMTItMDktMTAxEjAQBgNVBAsTCXRlc3QgZGVwdDEg
MB4GA1UEAxMXd3d3LmR1bW15c3NsdGVzdGluZy5jb20xKTAnBgkqhkiG9w0BCQEW
GnRlc3RlckBkdW1teXNzbHRlc3RpbmcuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GN
ADCBiQKBgQCyw80A6VzNwFRpizR9iWJnvZziAgwJZBmI7V2QjtQD+7tMwZA1mNZf
JohYRRS24WGOerGJd3YtAkQHv3yWSo6NiQ5X0Ng8ou4wvg7nlhsqSjeReSn7RUPV
Jl7L45MySiLI5iKWH2j+i1NxLfLbtkqO7+RVAlM3lL4T0Lsjg4RiswIDAQABo4IB
ejCCAXYwDAYDVR0TBAUwAwEB/zARBglghkgBhvhCAQEEBAMCAkQwMgYJYIZIAYb4
QgENBCUWI0FsdGVvbi9Ob3J0ZWwgR2VuZXJhdGVkIENlcnRpZmljYXRlMB0GA1Ud
DgQWBBSGR0w74d4NpcyEeYyLayjiBtRc9DCB9AYDVR0jBIHsMIHpgBSGR0w74d4N
pcyEeYyLayjiBtRc9KGBxaSBwjCBvzELMAkGA1UEBhMCVVMxEzARBgNVBAgTCkNh
bGlmb3JuaWExEDAOBgNVBAcTB1Rlc3RpbmcxKDAmBgNVBAoTH1Rlc3QgSW5jLiAx
IDA0OjM3OjIxIDIwMTItMDktMTAxEjAQBgNVBAsTCXRlc3QgZGVwdDEgMB4GA1UE
AxMXd3d3LmR1bW15c3NsdGVzdGluZy5jb20xKTAnBgkqhkiG9w0BCQEWGnRlc3Rl
ckBkdW1teXNzbHRlc3RpbmcuY29tggkA4MPIITtX0TcwCQYDVR0SBAIwADANBgkq
hkiG9w0BAQQFAAOBgQAMw7vnW4aWgwQZEpjWEYxzRkbAD1+vWYbtdNix9kPtHzWu
e5Fr9c4iuzSHW6cC8natTQc+8iAUNjokBpZ2PT62mENRsNjfj2Ov3/OzXuUYtwkt
```

```
OtOCddd5gM1DL6ovxM4k59VLkDYdn5p0kwknSAGHJyoUjQ3g7XWGAOffJy+Wbw==
-----END CERTIFICATE-----
...
/cfg/cert 1/revoke/.
/cfg/cert 1/revoke/automatic/.
        anonymous false
        interval 1d
        verify off
        ena disabled
/cfg/vpn 1/.
        name VPN-1
        ips 216.13.56.91
        standalone on
        hostippool false
/cfg/vpn 1/aaa/.
        idlettl 2m
        sessionttl infinity
        authorder 1
        defauth on
        defippool 1
/cfg/vpn 1/aaa/tg/.
        ena disabled
        recheck 15m
        action teardown
        details on
        runonce off
        logmode off
        loglevel info
        bypass off
/cfg/vpn 1/aaa/tg/agent/.
        timeout 2s
        minver 0.0.0.0
/cfg/vpn 1/aaa/nap/.
        autorem false
/cfg/vpn 1/aaa/nap/probation/.
        ena false
/cfg/vpn 1/aaa/nap/servers/.
/cfg/vpn 1/aaa/nap/shvs/.
        add 311 128 wshv
        add 40082 0 nshv
/cfg/vpn 1/aaa/nap/wshv/.
        firewall on
        autoupdate on
/cfg/vpn 1/aaa/nap/wshv/virus/.
        enabled false
/cfg/vpn 1/aaa/nap/wshv/spyware/.
        enabled false
/cfg/vpn 1/aaa/nap/wshv/secupdates/.
        enabled false
/cfg/vpn 1/aaa/wholesec/.
        ena false
/cfg/vpn 1/aaa/auth 1/.
        type local
        name local
/cfg/vpn 1/aaa/auth 1/local/.
        pwdage 0
        expirewarn 15
/cfg/vpn 1/aaa/auth 1/adv/.
/cfg/vpn 1/aaa/seqauth/.
        ena false
        copyuser off
        usesecond off
        retries 3
/cfg/vpn 1/aaa/network 1/.
        name intranet
```

```
/cfg/vpn 1/aaa/network 1/subnet 4/.
        net 172.16.1.50
        mask 255.255.255.255
/cfg/vpn 1/aaa/group 1/.
        name trusted
        restrict 0
        usertype advanced
        idlettl 0
        sessionttl 0
        ippool 1
/cfg/vpn 1/aaa/group 1/access 1/.
        network intranet
        service *
        appspec *
        extspec *
        action accept
/cfg/vpn 1/aaa/group 1/linkset/.
        add base-links
/cfg/vpn 1/aaa/group 1/l2tp/.
/cfg/vpn 1/aaa/group 1/ipsec/.
/cfg/vpn 1/aaa/ssodomains/.
/cfg/vpn 1/aaa/ssoheaders/.
/cfg/vpn 1/aaa/radacct/.
        ena false
/cfg/vpn 1/aaa/radacct/servers/.
/cfg/vpn 1/aaa/radacct/vpnattribute/.
        vendorid "1872 (alteon)"
        vendortype 3
/cfg/vpn 1/aaa/adv/.
/cfg/vpn 1/aaa/adv/unmatchgrp/.
        ena disabled
/cfg/vpn 1/server/.
        port "443 (https)"
        loopback on
        fastfin off
        ena enabled
/cfg/vpn 1/server/trace/.
/cfg/vpn 1/server/ssl/.
        cert 1
        cachesize 4000
        cachettl 5m
        renegotiate legacy
        protocol ssl3
        log none
        verifylog none
        ciphers AES256-SHA
        verify none
        ena enabled
/cfg/vpn 1/server/tcp/.
        cwrite 15m
        ckeep 15m
        skeep 2m
        sinterval 1m
        swrite 15m
        sconnect 30s
        csendbuf auto
        crecbuf auto
        ssendbuf auto
        srecbuf 6000
/cfg/vpn 1/server/http/.
        downstatus unavailable
        securecookie on
        certcard off
        cookieonce off
        sslheader off
```

```
        sslxheader off
        sslsidheader off
        addxfor off
        addvia on
        addxisd off
        addclicert off
        addnostore on
        nocachehdr off
        compress off
        allowimage on
        allowdoc off
        allowscript off
        allowica on
        cmsie on
        maxrcount 40
        maxline 16384
        urlobscure off
        sessionhdr off
/cfg/vpn 1/server/http/rewrite/.
        paramtag none
        urldeferattr on
        rewrite off
        ciphers HIGH:MEDIUM
        response iSD
        URI "/cgi-bin/weakcipher"
/cfg/vpn 1/server/proxymap/.
/cfg/vpn 1/server/portal/.
        wipecookies on
        cookiedb on
        resetcookie off
        persistent off
/cfg/vpn 1/server/portal/urlrewrite/.
        rewrite on
        jrewrite on
        cssrewrite on
        gziprewrite on
        ena enabled
/cfg/vpn 1/server/adv/.
/cfg/vpn 1/server/adv/traflog/.
        protocol bsd
        sysloghost 0.0.0.0
        udpport 514
        priority info
        facility local4
        ena disabled
/cfg/vpn 1/server/adv/sslconnect/.
        protocol ssl23
        cachemode on
        ciphers EXP-RC4-MD5:ALL!DH
/cfg/vpn 1/server/adv/sslconnect/verify/.
        verify none
/cfg/vpn 1/l2tp/.
        ena disabled
        cert unset
        authorder mschapv2,pap
        groupmatch true
/cfg/vpn 1/ipsec/.
        ena disabled
        cert unset
        groupmatch true
        groupbind off
/cfg/vpn 1/ipsec/sys/.
/cfg/vpn 1/ipsec/sys/failover/.
        primary 0.0.0.0
        secondary 0.0.0.0
```

```
        tertiary 0.0.0.0
/cfg/vpn 1/ipsec/sys/nat-t/.
        udpport 10001
        portswitch off
        ena false
/cfg/vpn 1/ippool 1/.
        type local
        name Local_pool
        lowerip 10.0.0.1
        upperip 10.0.0.100
        proxyarp on
        ena enabled
/cfg/vpn 1/ippool 1/exclude/.
/cfg/vpn 1/ippool 1/netattr/.
        netmask 255.255.255.0
        primnbns 0.0.0.0
        secnbns 0.0.0.0
        primdns 0.0.0.0
        secdns 0.0.0.0
/cfg/vpn 1/portal/.
        logintext
This is a configurable text.
...
        seclogtext
This is a configurable text.
...
        iconmode fancy
        linktext

...
        linkurl on
        punblock off
        linkcols 2
        linkwidth 100%
        companyname "Avaya Inc."
        smbworkgrp WORKGROUP
        autojre on
        applet on
        wiper on
        rsaauto off
        ieclear on
        citrix off
        clientauth off
        trustsite off
/cfg/vpn 1/portal/colors/.
        color1 #ececec
        color2 #ececec
        color3 #cc0000
        color4 #cc0000
/cfg/vpn 1/portal/content/.
        ena disabled
/cfg/vpn 1/portal/faccess/.
        ena disabled
        ipsecmode native
        contip 0.0.0.0
        portalmsg
From this page you can gain full network access. This
requires that Net Direct is enabled or
that you have either Avaya's IPSEC client (version 4.89 or better)
and/or SSL-VPN (TDI version 1.1 or better) client installed. If the Net Direct
installable client is installed it will be used if Net Direct is enabled.
Note: Your browser must support Java. If not download SUN's
J2SE JRE from
class="white_link" href="javascript:download_jre()">www.java.com.
Remember: You can only access resources on the network as defined by
```

```
your access rights. Contact your network operator if you are
dissatisfied with your current access rights.
...
appletmsg
The quest for full network access has started._The outcome of the quest will be indicated
in the progress bar and console window below.
...
/cfg/vpn 1/portal/lang/.
        setlang en
/cfg/vpn 1/portal/lang/beconv/.
/cfg/vpn 1/portal/whitelist/.
        ena disabled
/cfg/vpn 1/portal/whitelist/domains/.
/cfg/vpn 1/portal/blacklist/.
        ena disabled
/cfg/vpn 1/portal/blacklist/domains/.
/cfg/vpn 1/portal/usertype/.
/cfg/vpn 1/portal/usertype/novice/.
        sysinfo off
/cfg/vpn 1/linkset 1/.
        name base-links
        autorun false
/cfg/vpn 1/linkset 1/link 1/.
        href <netdirect>
        NetdirectFlag off
        type netdirect
/cfg/vpn 1/linkset 1/link 1/netdirect/.
/cfg/vpn 1/vdesktop/.
        ena off
        prelogon off
        always off
        force off
        switch off
        secure off
        persist off
        filesep off
        remdisk off
        print off
        netshare off
        cryptlevel 128
        timeout 5
        conncntrl off
/cfg/vpn 1/vdesktop/mcd/.
        ena disabled
        keylogger off
        scrscrap off
        acntcreate off
/cfg/vpn 1/vdesktop/mcd/vkeyboard/.
        ena disabled
/cfg/vpn 1/sslclient/.
        ippool off
        netdirect on
        caching off
        ndbanner
This is Netdirect Banner!
...
ndlicense
END USER LICENSE AGREEMENT
FOR AVAYA VPN CLIENT
This Software License Agreement ('Agreement') is between you, ('User') and Avaya
Corporation and its subsidiaries and affiliates ('Avaya').  PLEASE READ THE FOLLOWING
CAREFULLY.
BY CLICKING ON THE 'YES' BUTTON OR USING THIS SOFTWARE, YOU ('USER') ARE CONSENTING TO BE
BOUND BY THIS AGREEMENT BETWEEN YOURSELF AND AVAYA.  IF YOU DO NOT AGREE TO BE BOUND BY
THIS AGREEMENT, CLICK 'NO' AND DO NOT USE THIS SOFTWARE.
```

```
LICENSE GRANT: This Agreement shall govern the licensing of Avaya and Avaya licensor's
software and the accompanying user manuals, on line help services, Avaya Web Site and
other instructions (collectively, the 'Software') provided or made available to User.
The Software includes client software, which resides on the computers of User, to access
Sublicensor's networks (the 'Client Software').  The Software provided under this License
is proprietary to Avaya and to third parties from whom Avaya has acquired license
rights.  This Software was licensed in conjunction with the purchase of a 'Avaya VPN
Gateway' or other Avaya VPN device, that will give the User access to the Sublicensor's
purchaser's network and may only be used for this purpose by you.  User is hereby granted
a nonexclusive object code only license to use the Software under the following terms:
- User shall use the Software only in conjunction with the Avaya VPN Gateway or other
Avaya VPN device with which the Software was distributed.
- User may make one copy of the Software only for safekeeping (archives) or backup
purposes.
- User may not modify, translate, adapt, decompile, disassemble, decrypt, extract,
or otherwise reverse engineer or attempt to discover the source code and techniques
incorporated in the Software.  User may not create derivative works based on the Software
or any trade secret or proprietary information of Avaya.
- Title to Software shall not pass to User.
- User shall not provide, or otherwise make available, any Software, in whole or in part,
in any form, to any third party, nor shall User sublicense, rent or lease the Software.
- Upon termination or breach of this Agreement, or in the event that the Avaya device
with which it was distributed is no longer in use, User will immediately cease use of
and destroy all copies of the Software and  return the Software to Avaya or certify as
to such destruction to Avaya that is has been destroyed. Avaya and Third-party owners
from whom Avaya has acquired license rights to material that is incorporated into the
Software shall have the right to enforce the provisions of this Agreement against User.
IN NO EVENT SHALL AVAYA OR ITS  AGENTS, SUPPLIERS, MANUFACTURERS OR DISTRIBUTORS BE
LIABLE FOR ANY DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF
BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION OR DATA, DAMAGES
BASED ON ANY THIRD PARTY CLAIM,  OR, OR ANY OTHER PECUNIARY LOSS ARISING OUT OF THE USE
OR INABILITY TO USE THE SOFTWARE, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY
OF SUCH DAMAGES.  SOME JURISDICTIONS DO NOT ALLOW THESE LIMITATIONS OR EXCLUSIONS AND IN
SUCH EVENT THEY MAY NOT APPLY.
User agrees to comply with all export restrictions regarding the Software, and shall not
export, directly or indirectly, any Software or related technical data or information
without first obtaining any required export licenses or other governmental approvals. THE
SOFTWARE IS PROVIDED 'AS IS' WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS
OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. THE ENTIRE RISK ARISING OUT OF
USE OR PERFORMANCE OF THE SOFTWARE REMAINS WITH USER.  Avaya is not obligated to User
to provide support of any kind for the Software, and in the event it chooses to do
so, such support is subject to the terms of this Agreement.  Some jurisdictions do not
allow exclusion of implied warranties and, in such event, the above exclusions may not
apply. If User is the United States Government, the following paragraph shall apply:
All Software provided hereunder is commercial computer software and commercial computer
software documentation, as applicable, and in the event Software is licensed for or
on behalf of the United States Government, the respective rights to the Software is
governed by Avaya standard commercial license in accordance with U.S. Federal Regulations
at 48 C.F.R. Sections 12.212 (for non-DoD entities) and  48 C.F.R. 227.7202 (for DoD
entities). Software contains trade secrets and copyrighted material and User agrees to
treat the Software as confidential information using a reasonable standard of care.  User
shall not remove or obscure any copyright, patent, trademark, trade secret, or similar
intellectual property or restricted rights notice within or affixed to any Software and
shall reproduce and affix such notices on any backup copy of software. User may terminate
this Agreement at any time.  Avaya may terminate this Agreement if User fails to comply
with any of its terms.  This Agreement is the complete and exclusive agreement between
the parties hereto regarding its subject matter, and shall be governed solely by the laws
of the state of New York, without regard to its rules governing conflicts of law.
...
          oslist all
        udpports 5000-5001
        rekeytraf 0
        rekeytime 8h
        portalbind on
```

```
        idlecheck off
        keepalive 0
        recncttime 3m
        clampmss on
        splittun enabled
        tdiclient off
        lspclient off
        oldclients false
/cfg/vp
```

Index

P

R

S

T

U

V