Documentazione

GoToAssist® CORPORATE

Documentazione sulla sicurezza Citrix GoToAssist Corporate

GoToAssist Corporate fornisce solide misure di protezione dei dati da estremità a estremità, contro gli attacchi sia passivi che attivi alla riservatezza, l'integrità e la disponibilità.

CITRIX® | online

Sommario

Ambito e utenza

Questa guida è rivolta ai clienti di Citrix® GoToAssist® Corporate e a chiunque sia interessato a comprendere l'impatto di GoToAssist sul rischio e sulla conformità relativi alla protezione dei dati nell'ambiente utilizzato.

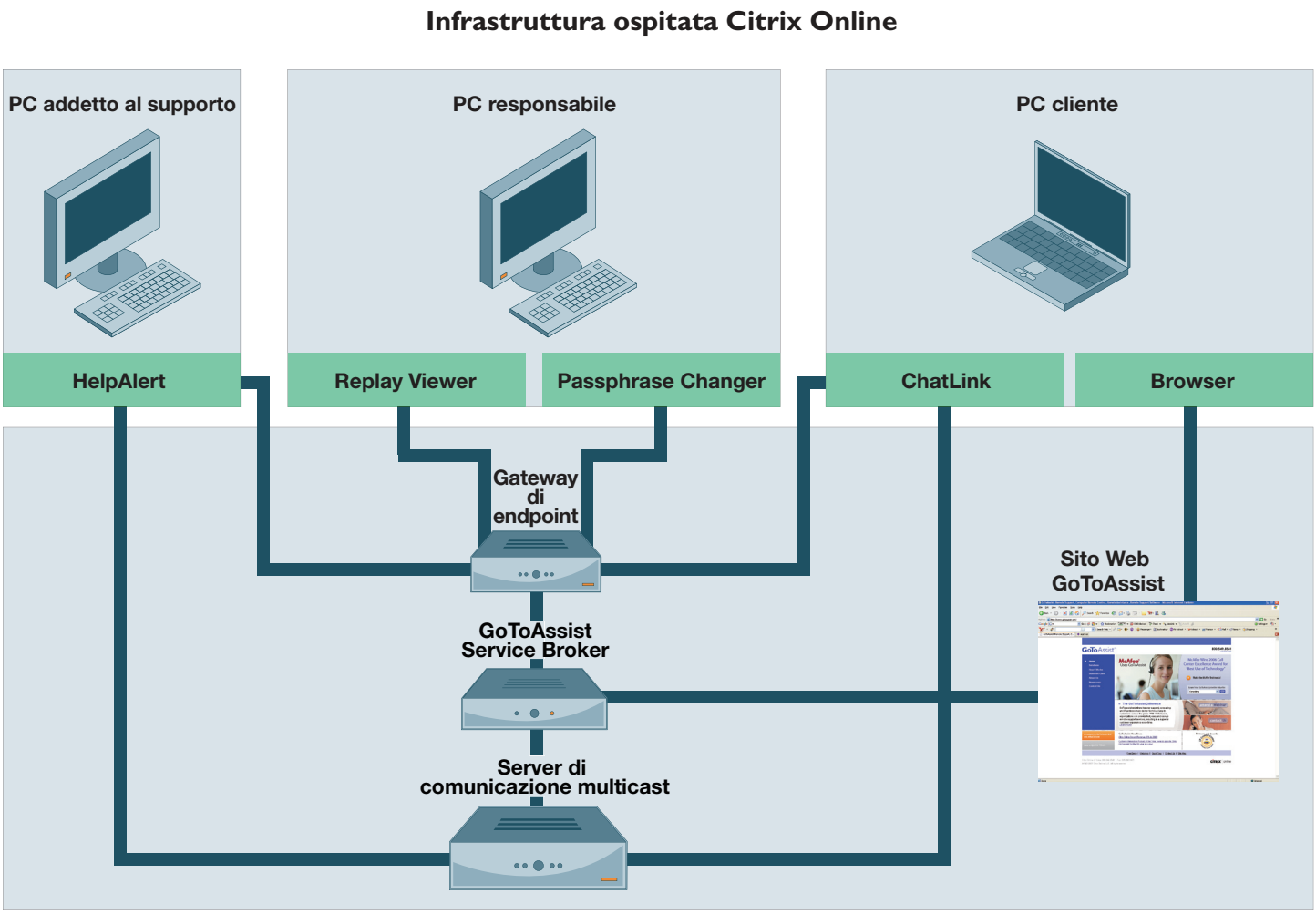
Introduzione

GoToAssist Corporate è un servizio host che fornisce funzionalità di assistenza in remoto ai computer basati su Windows. GoToAssist Corporate consente agli utenti di richiedere assistenza agli addetti al supporto e consente a questi ultimi di visualizzare e controllare, facoltativamente, il PC degli utenti finali in remoto.

La presente documentazione si occupa delle funzioni di GoToAssist Corporate sulla protezione dei dati. Si presume che l'utente disponga di una conoscenza di base del prodotto e delle relative funzioni. Ulteriore documentazione su GoToAssist Corporate è disponibile online all'indirizzo www.citrixonline.com oppure tramite un addetto al supporto Citrix Online.

Struttura di implementazione del servizio GoToAssist Corporate

Lo schema seguente offre una panoramica dei principali componenti e percorsi di comunicazione nell'implementazione del servizio GoToAssist Corporate.



Definizioni

HelpAlert: l'eseguibile Win32 disponibile sul computer dell'addetto al supporto del servizio che consente la ricezione e la replica alle richieste in arrivo da parte del cliente.

ChatLink: applicazione endpoint che facilita la comunicazione basata su testo tra un cliente e un addetto al supporto del servizio.

Browser: browser Web standard per Internet, ad esempio Firefox, Internet Explorer e così via.

Replay Viewer: applicazione endpoint che consente ai responsabili dell'azienda, dei team e degli addetti al supporto di riprodurre le sessioni registrate di GoToAssist Corporate. Replay viewer consente di riprodurre la condivisione delle schermate remote e delle schermate locali, le chat e la diagnostica in remoto.

Passphrase Changer: applicazione endpoint che facilita la modifica della passphrase utilizzata per proteggere l'accesso attivato tramite crittografia alle registrazioni delle sessioni.

GoToAssist Web Site: applicazione Web che fornisce l'accesso al sito Web di GoToAssist e ai portali di amministrazione interna ed esterna basata su Web.

GoToAssist Service Broker: applicazione Web che realizza le funzioni di gestione account e servizio, memorizzazione duratura e creazione di report di GoToAssist Corporate.

Server di comunicazione multicast: uno dei tanti server distribuiti a livello globale utilizzati per realizzare un'ampia gamma di servizi di comunicazione unicast e multicast ad alta disponibilità.

Gateway di endpoint: un gateway specifico usato per accedere in modo sicuro a GoToAssist Service Broker da diverse applicazioni endpoint per vari scopi tramite chiamate di procedura in remoto.

Sicurezza delle applicazioni

GoToAssist Corporate fornisce l'accesso a una gamma di risorse e servizi utilizzando un sistema di controllo degli accessi basato su ruoli e abilitato dai vari componenti di implementazione del servizio. Nella tabella di seguito vengono definiti i ruoli e i relativi termini:

Ruoli

Amministratore (o admin)	Il dipendente Citrix Online che crea Gruppi e Portali nel centro di gestione GoToAssist Corporate dell'azienda. Gli amministratori possono creare, modificare ed eliminare gli account, i portali, i responsabili dell'azienda e dei team di GoToAssist Corporate; modificare i dati relativi agli abbonamenti e ai prezzi oltre ad eseguire altre funzioni amministrative.
Società	Cliente di GoToAssist Corporate per il quale vengono configurati i portali.
Responsabile dell'azienda	Un dipendente della società cliente che dispone dell'accesso al relativo centro di gestione GoToAssist Corporate. Autorizzato a modificare account, portali, team e addetti al supporto associati agli account.
Cliente	La persona che richiede assistenza dalla società cliente tramite GoToAssist Corporate.
Gruppo/Team	Insieme di addetti al supporto a cui viene assegnato un portale specifico. Ogni addetto al supporto appartiene a un gruppo o team preciso; ogni gruppo o team viene assegnato a un portale specifico. I gruppi o i team contengono alcune impostazioni predefinite per gli addetti al supporto.
Responsabile di gruppo/ responsabile di team	Un dipendente del cliente autorizzato da un responsabile della società a modificare alcuni aspetti di un team nonché del portale e degli addetti al supporto associati a tale team.
Addetto al supporto	La persona addetta al supporto che risponde alle richieste dei clienti tramite HelpAlert.

Autenticazione

Gli amministratori, i responsabili e gli addetti al supporto di GoToAssist Corporate sono autenticati mediante un nome account e una password forte.

Le password sono regolamentate dai criteri riportati di seguito:

Password forti: una password forte ha una lunghezza da 8 a 32 caratteri e deve contenere almeno tre dei seguenti quattro tipi: maiuscole [A-Z], minuscole [a-z], numeri [0-9] e simboli speciali [~`!@#$%^&*()_-+={}[]|\:;”’<>,.?/]. Le password forti non devono essere uguali al nome di accesso o al nome o cognome reale del titolare dell'account. La forza delle password viene controllata al momento dell'inizializzazione o della modifica.

Periodo di scadenza delle password: è possibile configurare il periodo di validità delle password (minimo: 10 giorni, massimo: 120 giorni, predefinito: 90 giorni). Se il titolare dell'account accede con una password scaduta, è obbligato a modificare la password.

Cronologia password: viene conservata una cronologia delle password. Una password non può essere modificata con una password presente nella cronologia. È possibile configurare la lunghezza della cronologia delle password (minimo: 1, massimo: 5, predefinita: 3).

Blocco account: dopo 3 tentativi di accesso non riusciti, l'account viene messo in uno stato di blocco leggero obbligatorio. Ciò significa che il titolare dell'account non potrà effettuare l'accesso per un periodo di tempo che è possibile configurare (minimo: 5 minuti, massimo: 30 minuti, predefinito: 5 minuti). Scaduto il periodo di blocco, il titolare dell'account è in grado di tentare un nuovo accesso.

È possibile configurare l'applicazione di un blocco rigido come opzione aggiuntiva. Dopo un numero di tentativi di accesso non riusciti, l'account viene messo in uno stato di blocco rigido; tale numero è configurabile. Ciò significa che il titolare dell'account non può effettuare l'accesso finché la password dell'account non viene reimpostata da un altro titolare dell'account con privilegi. Un blocco rigido viene abilitato dopo un numero di tentativi; tale numero è configurabile (minimo: 10, massimo: 50, predefinito: 10).

Protezione del computer e dei dati del cliente

Una parte essenziale della protezione di GoToAssist Corporate è il modello di controllo dell'accesso basato sull'autorizzazione per proteggere l'accesso al computer del cliente e ai dati in esso contenuti.

In primo luogo, tutte le sessioni di GoToAssist Corporate devono essere avviate dal cliente remoto. GoToAssist Corporate non è stato progettato per scenari di assistenza non guidata.

In secondo luogo, al cliente viene sempre richiesta l'autorizzazione prima di avviare ogni condivisione di schermata, controllo remoto o trasferimento dei dati di diagnostica, file o altre informazioni.

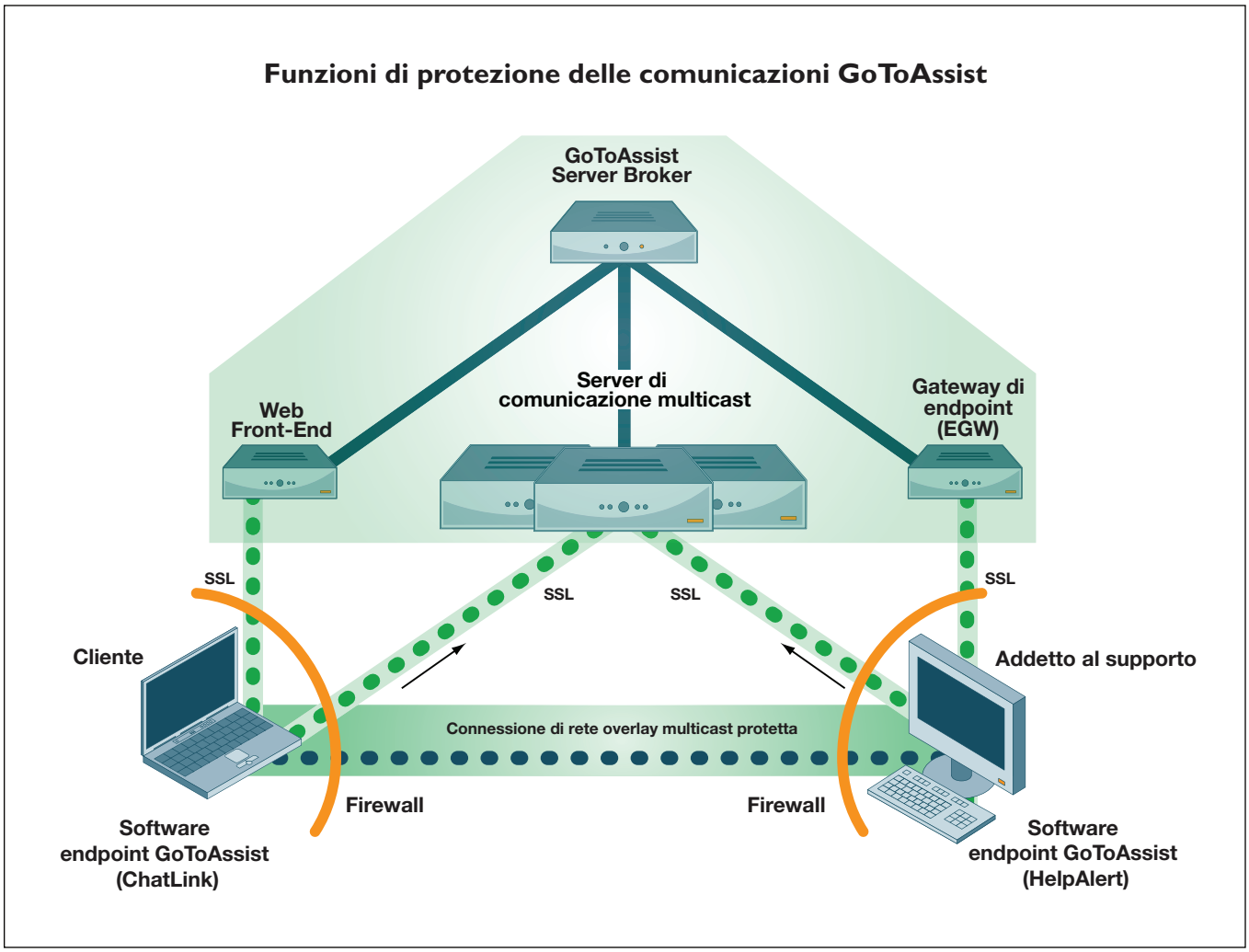
Se il controllo remoto e la condivisione di schermata vengono autorizzati, il cliente può vedere le operazioni che vengono svolte dall'addetto al supporto. Inoltre, il cliente può facilmente riprendere il controllo o terminare la sessione in qualsiasi momento.

I controlli di protezione locale sul computer del cliente non vengono mai annullati; il cliente o l'addetto al supporto deve sempre fornire le credenziali di autenticazione di Windows o dell'applicazione.

Infine, la condivisione di schermata e la sessione di chat possono essere registrate e riprodotte in modo facoltativo per un riesame successivo grazie alla registrazione di tutte le attività di connessione.

Funzioni di protezione delle comunicazioni

La comunicazione tra i partecipanti ad una sessione di GoToAssist Corporate avviene tramite uno stack di rete overlay multicast ubicato logicamente sopra lo stack TCP/IP convenzionale all'interno di ogni computer dell'utente. La rete è formata da un insieme di server MCS (Multicast Communication Servers) attivati da Citrix Online. La struttura delle comunicazioni viene riassunta nella figura di seguito.



I partecipanti alla sessione di GoToAssist Corporate (endpoint) comunicano con i server di comunicazione e i gateway dell'infrastruttura Citrix Online tramite connessioni TCP/IP in uscita sulle porte 8200, 443 e 80. Poiché GoToAssist Corporate è un servizio host basato sul Web, i partecipanti possono essere ubicati ovunque nella rete Internet, in un ufficio remoto, a casa, in un business center o collegati alla rete di un'altra azienda.

L'accesso al servizio GoToAssist Corporate in qualsiasi momento e da ogni luogo offre il massimo della flessibilità e connettività. Tuttavia, per mantenere la riservatezza e l'integrità delle comunicazioni aziendali private, GoToAssist Corporate incorpora anche solide funzioni di protezione delle comunicazioni.

Riservatezza e integrità delle comunicazioni

GoToAssist Corporate fornisce vere misure di protezione dei dati da "estremità a estremità", contro gli attacchi sia passivi che attivi alla riservatezza, l'integrità e la disponibilità. Tutte le connessioni GoToAssist Corporate sono crittografate da "estremità a estremità" e accessibili solo dai partecipanti alla sessione di assistenza autorizzati.

I dati della condivisione di schermata, i dati di controllo tastiera/mouse e le informazioni di testo delle chat non sono mai esposti in un formato non crittografato mentre risiedono temporaneamente nei server di comunicazione Citrix Online o durante la trasmissione attraverso reti pubbliche o private.

Quando la registrazione è disattivata, la chiave di sessione GoToAssist Corporate non viene mantenuta sui server Citrix Online in alcun formato. Pertanto, l'accesso non autorizzato a un server non consente di rivelare la chiave per i flussi crittografati eventualmente acquisiti dall'intruso.

Quando la registrazione è attivata, i dati relativi alle chat e alla condivisione e visualizzazione di schermata vengono memorizzati in un formato crittografato. Anche la chiave di sessione viene memorizzata, ma è protetta mediante la crittografia con chiave pubblica/privata RSA a 1024 bit. Una chiave pubblica specifica per portale viene usata per crittografare la chiave di sessione prima della memorizzazione. Per la riproduzione sono necessari tre elementi: la registrazione della sessione, la chiave di sessione crittografata e la chiave privata del portale.

I controlli della protezione delle comunicazioni basati su una solida crittografia sono implementati a due layer: il "layer TCP" e il "layer MPSL" (Multicast Packet Security Layer).

Protezione layer TCP

I protocolli SSL (Secure Sockets Layer) e TLS (Transport Layer Security) di standard IETF, sono usati per proteggere tutte le comunicazioni tra endpoint. Per fornire la massima protezione contro le intercettazioni, le modifiche o le riproduzioni non autorizzate, la sola suite di cifre SSL per connessioni TCP non da sito Web è quella RSA a 1024 bit con AES-CBS a 128 bit e HMAC-SHA1. Tuttavia, per la massima compatibilità con quasi tutti i browser Web su tutti i desktop degli utenti, il sito Web di GoToAssist supporta le connessioni in entrata tramite le suite di cifre SSL principalmente supportate. Per la protezione stessa dei clienti, Citrix Online consiglia di configurare i browser per l'uso di un una solida crittografia come impostazione predefinita qualora possibile e di installare sempre le patch di protezione del browser e sistema operativo più recenti.

Quando vengono stabilite le connessioni SSL/TLS al sito Web di GoToAssist e tra i componenti di GoToAssist Corporate, i server Citrix Online si autenticano automaticamente sui client mediante i certificati di chiave pubblica VeriSign/Thawte. Per una maggiore protezione contro gli attacchi all'infrastruttura, viene usata l'autenticazione reciproca basata su certificato per tutti i collegamenti da server a server (ad esempio, da MCS a MCS, da MCS a Broker). Queste forti misure di autenticazione impediscono ai potenziali pirati di fingersi server dell'infrastruttura o di inserirsi nelle comunicazioni della sessione di assistenza.

Layer MPSL

Funzioni aggiuntive forniscono una protezione completa da "estremità a estremità" per i dati di pacchetti multicast, indipendentemente da quanto fornito da SSL/TLS. Nello specifico, tutti i dati delle sessioni multicast sono protetti dalla crittografia da "estremità a estremità" e da meccanismi di integrità che impediscono a chiunque disponga dell'accesso ai nostri server di comunicazione (sia friendly che hostile) di intercettare le sessioni di GoToAssist Corporate o di manomettere i dati senza rilevamento. Questo livello di riservatezza e integrità delle comunicazioni è specifico di GoToAssist Corporate. Le comunicazioni aziendali non sono mai visibili a terze parti, inclusi sia gli utenti che non sono invitati a una determinata sessione di assistenza, sia Citrix Online stesso.

La creazione di una chiave MPSL viene effettuata utilizzando l'accordo sulle chiavi autenticate SRP-6 basato su chiave pubblica, mediante un modulo a 1024 bit per stabilire una chiave di crittografia principale (vedere http://srp.stanford.edu/design.html). Tale chiave viene quindi usata per la distribuzione della chiave simmetrica di gruppo mediante l'algoritmo per chiave di crittografia principale AES, IETF RFC 3394. Tutto il materiale relativo alla chiave viene creato tramite un generatore di numeri pseudo-casuali, conforme a FIPS, nel quale vengono inseriti dati entropici raccolti durante il runtime da più sorgenti sul computer host. La creazione di una chiave solida e dinamica e i metodi di scambio offrono una forte protezione contro ogni tentativo di indovinare la chiave.

Il layer MPSL protegge ulteriormente i dati dei pacchetti multicast da intercettazioni mediante crittografia AES a 128 bit in modalità contatore. I dati di testo semplice vengono compressi prima della crittografia utilizzando tecniche proprietarie, ad alte prestazioni, per ottimizzare la larghezza di banda. La protezione dell'integrità dei dati viene compiuta includendo un valore di controllo dell'integrità generato con l'algoritmo HMAC-SHA-1. Poiché GoToAssist Corporate usa misure di crittografia potenti e standard nel settore, i clienti possono riporre piena fiducia nella protezione dei dati delle sessioni di assistenza multicast contro divulgazioni non autorizzate o modifiche non rilevate.

Inoltre, non vi sono costi aggiuntivi né deterioramento delle prestazioni o usura associati a queste fondamentali funzioni di protezione delle comunicazioni. La protezione dei dati basata su standard e a prestazioni elevate è una funzione "integrata" in ogni sessione di GoToAssist Corporate.

Punti chiave

- La crittografia AES a 128 bit è utilizzata per la riservatezza delle sessioni.
- La chiave della sessione iniziale è scelta casualmente da Broker, quindi viene inoltrata agli endpoint tramite canali autenticati e crittografati.
- Gli endpoint negoziano successivamente una chiave di sessione finale tra di loro.
- La chiave di sessione finale non è conosciuta da Broker.
- I server di comunicazione inoltrano soltanto i pacchetti crittografati e non dispongono della chiave di crittografia delle sessioni.
- La struttura di GoToAssist Corporate riduce al minimo il rischio di esposizione dei dati delle sessioni mentre ottimizza la capacità di collegare agenti a chi richiede assistenza.

Compatibilità di firewall e proxy

Come altri prodotti Citrix Online, GoToAssist Corporate integra la logica di gestione delle connessioni e il rilevamento dei proxy che consente di automatizzare l'installazione di software, evitare la necessità di riconfigurare reti complesse e ottimizzare la produttività degli utenti. I firewall e i proxy già presenti nella rete in uso non richiedono in genere alcuna configurazione particolare per abilitare l'uso di GoToAssist Corporate.

Quando viene avviato, il software dell'endpoint di GoToAssist Corporate tenta di contattare il broker del servizio GoToAssist tramite il gateway dell'endpoint (EGW) avviando una o più connessioni TCP protette da SSL in uscita, sulle porte 8200, 443 e/o 80. La connessione che risponde per prima viene utilizzata, mentre le altre vengono annullate. Tale connessione fornisce la base per partecipare a tutte le sessioni di assistenza future abilitando la comunicazione tra i server ospitati e il desktop dell'utente.

Quando un utente prova a partecipare ad una sessione di assistenza, il software dell'endpoint di GoToAssist Corporate stabilisce una o più connessioni aggiuntive ai server di comunicazione Citrix Online, usando di nuovo connessioni TCP protette da SSL sulle porte 8200, 443 e/o 80. Tali connessioni trasportano i dati della sessione di assistenza durante una sessione attiva.

Inoltre, per ottimizzare la connettività, il software dell'endpoint avvia una o più connessioni TCP di breve durata sulle porte 8200, 443 e/o 80 non protette da SSL. Queste "esplorazioni" di rete non contengono informazioni sensibili o sfruttabili e non espongono a rischi di divulgazione i dati importanti.

Un elenco completo di intervalli degli indirizzi IP usati da Citrix Online è disponibile nella pagina Web www.citrixonline.com/iprange.

Regolando automaticamente le condizioni della rete locale soltanto tramite connessioni in uscita e scegliendo una porta già aperta nella maggior parte di firewall e proxy, GoToAssist Corporate fornisce un livello elevato di compatibilità con le misure di protezione di rete esistenti. A differenza di altri prodotti, GoToAssist Corporate non richiede alle aziende di disattivare i controlli di protezione del perimetro di rete esistenti per consentire la comunicazione delle sessioni di assistenza online. Tali funzioni ottimizzano la compatibilità e la sicurezza della rete complessiva.

Funzioni di protezione del sistema degli endpoint

Il software della sessione di assistenza deve essere compatibile con un'ampia gamma di ambienti desktop e creare nello stesso tempo un endpoint sicuro sul desktop di ogni utente. GoToAssist Corporate consente tutto ciò grazie all'uso di eseguibili scaricabili dal Web che utilizzano solide misure di crittografia.

Software endpoint firmato

Il software dell'endpoint client di GoToAssist Corporate è un eseguibile Win32 che viene scaricato sui computer degli utenti. Un applet Java firmato digitalmente viene usato per mediare il download e verificare l'integrità del software dell'endpoint di GoToAssist Corporate dai server Citrix Online. Ciò consente di proteggere l'utente dall'installazione accidentale di trojan o altri malware interpretati come software di GoToAssist Corporate.

Il software dell'endpoint è composto da diversi eseguibili Win32 e da librerie collegate in modo dinamico. Citrix Online esegue rigorosi controlli di qualità e procedure di gestione della configurazione durante lo sviluppo e l'implementazione per garantire la sicurezza del software. Il software dell'endpoint non espone interfacce di rete disponibili esternamente e non può essere utilizzato da malware o virus per sfruttare o infettare i sistemi remoti. Questo protegge gli altri desktop che partecipano alle sessioni di assistenza dalle infezioni tramite un host infetto e usato da altri utenti.

Implementazione di un sottosistema di crittografia

Tutte le funzioni di crittografia e i protocolli di protezione impiegati dal software dell'endpoint client di GoToAssist Corporate vengono implementati utilizzando le librerie all'avanguardia Certicom Security Builder® Crypto™ e Certicom Security Builder® SSL™ che garantiscono sicurezza ed elevate prestazioni (vedere www.certicom.com per ulteriori informazioni).

L'uso delle librerie di crittografia è limitato all'applicazione endpoint di GoToAssist Corporate; nessun API esterno è esposto all'accesso da parte di altri software in esecuzione sul desktop. Tutti gli algoritmi di crittografia e integrità, dimensione delle chiavi e altri parametri dei criteri di crittografia sono codificati staticamente durante la compilazione dell'applicazione. Le impostazioni di crittografia non sono configurabili da parte dell'utente finale, pertanto è impossibile che gli utenti possano compromettere la protezione delle sessioni di GoToAssist Corporate tramite configurazioni non corrette accidentali o intenzionali. Una società che utilizza GoToAssist Corporate può essere sicura che lo stesso livello di sicurezza delle sessioni di assistenza online è presente su tutti gli endpoint che vi partecipano, indipendentemente dall'utente che possiede o utilizza ciascun desktop.

Funzioni di protezione dell'infrastruttura ospitata

Citrix Online fornisce GoToAssist Corporate usando un modello ASP (Application Service Provider) progettato appositamente per garantire un funzionamento solido e sicuro durante l'integrazione senza interruzioni con la rete e l'infrastruttura di protezione già esistenti in un'azienda.

Infrastruttura scalabile e affidabile

L'architettura del servizio globale Citrix Online è stata progettata per offrire il massimo delle prestazioni, dell'affidabilità e della scalabilità. Il servizio GoToAssist Corporate è controllato tramite server ad elevata capacità, standard nel settore e apparecchiature di rete dotate delle più recenti patch di protezione. Router e switch ridondanti sono integrati nell'architettura per garantire che non vi sia mai alcun punto di errore. Cluster di server e sistemi di backup garantiscono un flusso senza interruzioni dei processi applicativi, anche nel caso di carichi pesanti o problemi di sistema. Per ottenere prestazioni ottimali, il carico del broker di GoToAssist bilancia le sessioni client/server attraverso i server di comunicazione distribuiti geograficamente.

Sicurezza fisica

Tutti i server Web, di applicazione, di comunicazione e database GoToAssist Corporate sono alloggiati in centri dati in co-location sicuri. L'accesso fisico ai server è strettamente riservato e continuamente controllato. Tutte le risorse dispongono di alimentazione ridondante e controlli dell'ambiente.

Sicurezza delle rete

Citrix Online utilizza firewall, router e controlli di accesso basati su VPN per proteggere le reti di servizio privato e i server back-end. La sicurezza dell'infrastruttura è continuamente controllata e vengono effettuati regolarmente test di vulnerabilità dallo staff di sicurezza interna e da revisori esterni di terze parti.

Riservatezza dei clienti

La fiducia degli utenti rappresenta una priorità e per questo Citrix Online si è impegnata a rispettare la loro riservatezza. Un collegamento a una copia dell'informativa attuale sulla riservatezza di Citrix GoToAssist Corporate è disponibile sul sito Web del servizio all'indirizzo www.citrixonline.com.

Conformità in ambienti regolamentati

Per la serie completa dei controlli di protezione delle comunicazioni e dell'applicazione, tra cui il modello di protezione basato su autorizzazione da parte del cliente, GoToAssist Corporate può essere utilizzato in modo sicuro per fornire assistenza a computer e applicazioni in ambienti soggetti a normative HIPAA, Gramm-Leach-Bliley Act o Sarbanes-Oxley, in cui è necessario utilizzare solidi controlli sulla riservatezza e l'integrità dei dati.

Citrix Online consiglia alle aziende di esaminare attentamente tutte le funzioni di protezione standard e configurabili di GoToAssist Corporate nel contesto specifico degli ambienti utilizzati, del tipo di utenti e dei requisiti dei criteri, per stabilire quali funzioni devono essere abilitate e per ottimizzarne la configurazione. In alcuni casi, è consigliabile comunicare agli utenti ulteriori linee guida sull'utilizzo per garantire che vengano soddisfatti tutti gli obiettivi di protezione di chiunque è interessato al prodotto. Il team del servizio professionale Citrix Online può fornire materiale aggiuntivo relativo alle pratiche ottimali per l'implementazione e l'utilizzo di GoToAssist Corporate.

Conclusione

L'interfaccia e la serie di funzioni intuitive e sicure di GoToAssist Corporate ne fanno la soluzione più efficace per condurre sessioni di assistenza online. Grazie a GoToAssist Corporate, i professionisti addetti al supporto, alla consulenza e ai servizi IT possono offrire rapidamente e in modo semplice assistenza tecnica ai clienti in tutto il mondo.

Oltre a tutto ciò, l'architettura del servizio host di Citrix Online supporta in modo trasparente la collaborazione multipoint fornendo un ambiente sicuro e affidabile. Come descritto nella presente documentazione, GoToAssist Corporate promuove la facilità d'uso e la flessibilità senza compromettere l'integrità, la riservatezza o la gestione delle risorse IT o delle comunicazioni aziendali.

Appendice: Conformità agli standard di sicurezza

GoToAssist Corporate è conforme agli standard del settore e del governo degli Stati Uniti descritti di seguito relativi agli algoritmi di crittografia e ai protocolli di sicurezza:

- Protocollo TLS/SSL, versione 1.0 IETF RFC 2246
- AES (Advanced Encryption Standard), FIPS 197
- (Implementazione convalidata FIPS, Certificato NIST N.175)
- Suite di cifre AES per TLS, IETF RFC 3268
- Algoritmo per chiave di crittografia principale AES, IETF RFC 3394
- RSA, PKCS N.1
- SHA-1, FIPS 180-1 (Implementazione convalidata FIPS, Certificato NIST N.89)
- HMAC-SHA-1, IETF RFC 2104
- MD5, IETF RFC 1321
- Generazione di numeri pseudo-casuali, ANSI X9.62 e FIPS 140-2

Citrix Online

Divisione Citrix Online

Informazioni sul prodotto:
www.citrixonline.com

Informazioni sulle vendite:
Italy@citrixonline.com
Telefono: +353 (0) 867 953 521

Informazioni sui supporti:
pr@citrixonline.com
Telefono: +441 49 454 1715

www.citrixonline.com

Per ulteriori informazioni su Citrix GoToAssist Corporate, visitare www.citrixonline.com

Informazioni su Citrix Online

Citrix Online fornisce soluzioni online sicure e di facile utilizzo che consentono di lavorare ovunque e con chiunque. Sia che utilizzino GoToMyPC® per accedere e lavorare su computer remoti, GoToAssist® per assistere i clienti o GoToMeeting® per svolgere meeting e Webinar online, i nostri clienti (oltre 35.000 aziende e centinaia di migliaia di singoli utenti) riescono ad aumentare la produttività, ridurre i costi relativi agli spostamenti e migliorare le vendite, la formazione e i servizi a livello globale. Divisione di Citrix Systems, Inc. (Nasdaq: CTXS), la società ha sede a Santa Barbara, California (USA). Per ulteriori informazioni, visitare il sito Web all'indirizzo: www.citrixonline.com o chiamare il numero 805-690-6400.

18191/11.17.08/PDF