



## AREA CULTURALE IP SECURITY

**Alt alle minacce!**

### **SSL VPN: ACCESSO UNIVERSALE PROTETTO E SEMPLIFICATO PER UTENTI REMOTI**



#### **PANORAMICA**

Le reti VPN (Virtual Private Network) hanno rivoluzionato il modo in cui le filiali e i business partner si collegano a un'organizzazione. Le reti VPN si affidano a un accesso Internet low-cost per realizzare tunnel trusted tra l'ufficio centrale e le filiali o i partner attraverso reti non trusted. IPSec, la tecnologia VPN più utilizzata, è progettato per fornire una robusta protezione ai dati trasferiti tra le due reti. Tuttavia le organizzazioni devono anche risolvere il problema generale dell'accesso remoto protetto per i singoli utenti e non solo per le reti. I dipendenti e i business partner, ad esempio, hanno spesso necessità di accedere alle informazioni in modalità remota, da un'altra rete privata o pubblica, e probabilmente sono essi stessi protetti da firewall o altre apparecchiature di protezione. Le soluzioni IPSec VPN non sono purtroppo adatte all'utilizzo con applicazioni mobili. La maggior parte delle tecnologie IPSec MUVPN (Mobile User VPN) non risultano affidabili per gli utenti fuori sede che hanno necessità di collegarsi alle risorse aziendali e sono protetti da un firewall presso la sede di un cliente o di un partner. Le soluzioni IPSec MUVPN, inoltre, comportano complicazioni dal punto di vista amministrativo ed elevati costi di configurazione e supporto risultanti dall'installazione e dall'aggiornamento del client software che imita la connessione da

rete a rete, per il cui supporto è stata progettata quella specifica tecnologia IPSec.

Le organizzazioni che desiderano risolvere questo problema hanno necessità di un accesso protetto e autenticato per utenti e organizzazioni trusted e la protezione dei dati trasferiti attraverso reti (non trusted) di terze parti. Inoltre, la soluzione ideale deve essere facile da gestire, non essere ostacolata dalle comuni configurazioni dei firewall, offrire supporto completo a tutte le applicazioni e risorse di rete e risultare trasparente per l'utente finale.

WatchGuard Technologies, Inc. ha sviluppato assieme Citrix Systems, Inc. il WatchGuard Firebox® SSL VPN Gateway con Citrix® Secure Access. Questa appliance soddisfa tutti i requisiti elencati e molti altri ancora, oltre a fornire un accesso affidabile, universale e protetto alle risorse di rete con una semplicità di utilizzo senza precedenti, sia per gli amministratori IT sia per gli utenti. A differenza della maggior parte delle soluzioni SSL VPN, Firebox SSL VPN Gateway non richiede speciali connettori o la "webification" per il supporto delle applicazioni. In tal modo consente un risparmio significativo in termini di costi e tempi di amministrazione, assicurando a qualsiasi utente autorizzato un accesso sempre disponibile alle risorse e alle applicazioni di rete specificate.



## AREA CULTURALE IP SECURITY

**Alt alle minacce!**

### **RISOLUZIONE DEI PROBLEMI VPN DI ACCESSO MOBILE**

Le reti VPN sono state create per risolvere il problema relativo a come consentire un accesso remoto protetto su reti non trusted. Nel corso degli anni le organizzazioni hanno sviluppato differenti tipi di soluzioni:

#### **IPSec**

Questo tipo di VPN utilizza una tecnica nota come incapsulamento, che consente ai pacchetti provenienti dalla rete "A" e destinati alla rete "B" di essere incapsulati, crittografati e inviati, pacchetto per pacchetto, a un server trusted della rete "B" dove vengono decodificati e inoltrati alla propria destinazione finale sulla rete "B". Il grande vantaggio offerto dall'incapsulamento consiste nel fatto che attraverso il tunnel sono supportati TUTTI i pacchetti provenienti da TUTTE le applicazioni, senza alcuna modifica. Per le applicazioni mobili, le soluzioni IPSec VPN si affidano a un thick client (client convenzionale) per inizializzare e gestire il tunnel.

#### **Inconvenienti delle soluzioni VPN IPSec mobili**

1. Le soluzioni thick client risultano onerose per l'organizzazione in termini di supporto necessario per agevolare gli utenti finali nelle attività di installazione, manutenzione e risoluzione dei problemi, con conseguenti complicazioni ed elevati costi a carico dell'organizzazione.
2. La maggior parte dei firewall attuali utilizza NAT (Network Address Translation) per gestire il proprio spazio indirizzi IP. NAT si affida alla riscrittura, pacchetto per pacchetto,

degli indirizzi IP di origine e di destinazione in modo da consentire la comunicazione tra computer che utilizzano indirizzi IP privati e pubblici. Dal momento che il codice NAT modifica il traffico del tunnel, i pacchetti trasmessi spesso non superano la convalida a destinazione e vengono eliminati. Nella maggior parte dei casi, NAT impedisce l'utilizzo casuale delle reti IPSec MUVPN da parte di persone che desiderano collegarsi a una rete privata da un'organizzazione diversa. Questa situazione lascia molti dipendenti nell'impossibilità di accedere alla propria rete aziendale quando si trovano nella sede di un'altra organizzazione, limitando così l'accesso alle informazioni a eccezione di quando si trovano in un ambiente con un livello inferiore di restrizioni.

3. Le soluzioni IPSec MUVPN non consentono l'accesso protetto a una rete privata da computer pubblici, quali ad esempio i computer dei chioschi multimediali. I computer presenti nei chioschi non consentono di caricare e configurare il client IPSec necessario per il funzionamento della rete VPN per utenti mobili.

#### **SSL VPN**

La soluzione SSL (Secure Socket Layer) VPN è stata inizialmente sviluppata per risolvere il problema di fornire un accesso protetto a server Web (ad esempio nei siti di



## AREA CULTURALE IP SECURITY

**Alt alle minacce!**

e-commerce) nelle situazioni in cui non è opportuno installare e mantenere un thick client. È inoltre possibile utilizzare SSL VPN per risolvere i problemi associati alle soluzioni IPsec VPN, fornendo in tal modo l'accesso protetto necessario per collaboratori remoti e business partner attraverso reti non compatibili con IPsec. Tuttavia SSL presenta specifici problemi di utilizzo.

Le soluzioni SSL VPN si affidano a connessioni HTTPS per fornire l'accesso a portali Web a un numero limitato di applicazioni Web. Le appliance SSL VPN (definite talvolta concentratori) eseguono questa operazione attraverso l'analisi e la ricostruzione in tempo reale dell'applicazione Web mentre vengono eseguite le richieste.

Ricostruendo i percorsi di navigazione, il concentratore riproduce correttamente la funzionalità dell'applicazione Web senza richiedere un thick client per l'accesso. Dal momento che le soluzioni SSL VPN forniscono una modalità priva di client per accedere ad applicazioni all'interno della rete di un'azienda o di un'organizzazione (il browser Web è il client), consentono di eliminare o ridurre i problemi di amministrazione e i costi elevati per il supporto di client IPsec VPN. Il limite di questo approccio è rappresentato dalla compatibilità con le sole applicazioni Web: in confronto a IPsec MUVPN, l'utilità di questa soluzione è fortemente penalizzata.

### **Applicazioni client/server e soluzioni SSL VPN**

Sebbene le soluzioni SSL VPN funzionino principalmente con applicazioni basate sul Web, alcuni fornitori di reti SSL VPN hanno sviluppato connettori personalizzati per il supporto di un numero limitato di

applicazioni client/server. I connettori personalizzati distribuiti da fornitori di soluzioni SSL VPN sono normalmente destinati ad applicazioni provviste di un client standard (non personalizzabile) quale Microsoft® Outlook®. Dal momento che il client Outlook 2000 Service Pack 3 (SP3) è lo stesso per tutte le organizzazioni, per i fornitori di soluzioni SSL VPN risulta conveniente sviluppare un connettore personalizzato per questa applicazione che potranno rivendere ai clienti come componente aggiuntivo. Per le applicazioni dotate di un client standardizzato (come Outlook), la soluzione con connettore personalizzato utilizza il client residente sul PC degli utenti e crea uno schema di mappatura protocolli che invia al proxy gli scambi di dati tra client e server. Questo schema di mappatura protocolli è specifico per la versione del client software e richiede al reparto IT l'adeguamento dell'ambiente di rete e di ogni computer laptop perché sia compatibile con il proxy e ignori l'applicazione. Questa soluzione fornisce all'applicazione il medesimo livello generale di connettività di IPsec ma penalizza le prestazioni e impone un onere in termini di gestione equivalente o superiore a quello di una soluzione IPsec. Altre comuni applicazioni business, quali ad esempio strumenti SFA (Sales Force Automation), sistemi CRM (Customer Relationship Management) e applicazioni ERP (Enterprise Resource Planning), oltre alle applicazioni di società quali Siebel, Oracle, Remedy, Clarify e SAP, non forniscono client standard. I client per queste applicazioni sono personalizzabili in base alle esigenze dei singoli clienti. Un'implementazione Siebel presso la società A sarà molto diversa dall'implementazione Siebel presso la società B o presso qualsiasi



## AREA CULTURALE IP SECURITY

## Alt alle minacce!

altra società. Per applicazioni personalizzate in base alle esigenze di una specifica organizzazione, il fornitore della soluzione SSL VPN può utilizzare il proprio team di servizi professionali per creare un connettore personalizzato o eseguire la "webification" del prodotto. Dal momento che le applicazioni sono personalizzate in base alle esigenze di una specifica organizzazione, anche la "webification" o la creazione di un connettore personalizzato deve essere specifica per ogni cliente. I costi per questo tipo di programmazione personalizzata sono notevolmente elevati.

### **Applicazioni Web e soluzioni SSL VPN**

Molti fornitori di soluzioni SFA, CRM e ERP forniscono un'interfaccia Web nativa e sembrano preferire presentarla agli utenti remoti, ignorando le limitazioni delle reti SSL VPN menzionate in precedenza. SSL VPN è essenzialmente una tecnologia proxy e come tale deve analizzare e riscrivere i link allo scopo di consentire l'accesso alle applicazioni Web interne. Questo significa che SSL VPN è compatibile solo con componenti Web che possono venire letti e riscritti al momento, quando viene richiesto. Le applet Java, ActiveX, Flash e altri diffusi componenti Web sono costituiti da codice binario eseguibile e pertanto non possono essere riscritti. Purtroppo, molte delle interfacce Web standard offerte da fornitori di sistemi SFA, CRM ed ERP contengono questo tipo di strutture che impediscono l'accesso attraverso una rete SSL VPN. Inoltre per quanto riguarda le applicazioni Web che *possono* essere utilizzate con SSL VPN, si verifica una significativa riduzione delle prestazioni a causa dell'impegnativo processo di elaborazione: analisi della pagina Web, identificazione degli URL,

riscrittura e mappatura dei percorsi di navigazione su URL accessibili esternamente e quindi ricostruzione delle pagine Web per l'utente finale.

### **INCONVENIENTI DELLE SOLUZIONI SSL VPN STANDARD**

1. **Voci DNS separate** – Durante la connessione a una risorsa interna, il client PC ricerca un indirizzo IP o un nome di server che non può essere visto all'esterno del firewall (SSL VPN non fornisce un accesso trasparente come IPsec VPN), pertanto l'amministratore IT deve configurare voci DNS separate sull'host oppure su un server DNS. Ad esempio, un client Outlook è normalmente configurato per ricercare il server Exchange in base al nome. Questo server viene facilmente raggiunto e connesso in base al nome se il PC si trova all'interno della rete. Tuttavia, per un client esterno, non è possibile risolvere il nome DNS del server in quanto generalmente non è disponibile una voce DNS pubblicata esternamente relativa ai server interni. Anche se la voce fosse stata pubblicata dal server DNS pubblico dell'azienda, il client non sarebbe in grado di trovare una route per il server privato poiché, nella maggior parte dei casi, il server Exchange utilizza un indirizzo IP privato o non instradabile. I fornitori di soluzioni SSL VPN risolvono questo problema richiedendo all'amministratore IT la configurazione di voci DNS separate che instradano verso il server Exchange il PC, qualora si trovi sulla rete principale. In caso contrario, tuttavia, viene instradato sull'indirizzo di loopback SSL VPN in esecuzione nel PC (questa operazione viene eseguita specificando un indirizzo di loopback come 127.0.0.1 come indirizzo IP



## AREA CULTURALE IP SECURITY

## Alt alle minacce!

del server Exchange). In alternativa, alcuni fornitori di soluzioni SSL VPN evitano i connettori di loopback, puntando direttamente verso il server SSL VPN PC esterni alla rete privata, tuttavia anche questa operazione richiede una voce DNS separata (principalmente per eseguire la risoluzione dei PC esterni alla rete nel server SSL VPN pubblico). Ogni PC che utilizza la soluzione SSL VPN per accedere all'applicazione dovrà modificare il nome server nel client per puntare alla nuova voce DNS separata (al momento della configurazione di SSL VPN) o al connettore dell'applicazione, parte integrante del server SSL VPN.

**2. Prestazioni delle applicazioni** - Quando un client PC accede all'applicazione server attraverso una rete SSL VPN, le prestazioni dell'applicazione vengono significativamente penalizzate. Questa situazione è dovuta alle conversioni di protocollo che devono essere eseguite tra il client PC e il client SSL VPN e quindi tra il server SSL VPN e l'applicazione. Naturalmente, le conversioni opposte dei protocolli devono avvenire nel viaggio di ritorno dei dati, dall'applicazione al client dell'applicazione.

Ad esempio, un client Outlook utilizza normalmente un protocollo MAPI per comunicare con un server Exchange. Quando viene introdotta una tecnologia SSL VPN, il client Outlook comunica ancora tramite MAPI con il client SSL VPN. Il client SSL VPN converte questi dati in un protocollo personalizzato che utilizza per comunicare con il server SSL VPN. Il server SSL VPN deve quindi convertire questo protocollo personalizzato in un protocollo MAPI, previsto dal server Exchange. Nel viaggio di ritorno dei dati, dal server Exchange al client Outlook, si verifica

nuovamente questo insieme di conversioni di protocollo, in senso contrario.

**3. Aggiornamenti delle applicazioni** - La maggior parte degli aggiornamenti di un'applicazione richiedono un corrispondente aggiornamento delle soluzioni SSL VPN, poiché queste ultime sono sensibili alle modifiche dei protocolli di comunicazione client/server. Quando l'aggiornamento di un'applicazione apporta una modifica nella modalità di comunicazione dell'applicazione stessa, la rete SSL VPN che fornisce accesso agli utenti remoti deve adeguarsi a questo cambiamento.

Tornando all'esempio di Outlook, se un'organizzazione esegue l'aggiornamento del server Exchange dalla versione 5.5 alla versione 2000, il protocollo MAPI utilizzato tra il client Outlook e il server Exchange viene modificato. Dal momento che il client e il server SSL VPN convertono questo specifico protocollo MAPI nel protocollo SSL VPN proprietario, sarà necessario aggiornare la corrispondente conversione di protocollo del server SSL VPN. Inoltre, se il protocollo MAPI tra Outlook e il server Exchange viene modificato durante l'aggiornamento del Service Pack (ad esempio da SP3 a SP4); sarà necessario aggiornare anche la soluzione SSL VPN.

**4. Tempi di implementazione lunghi e costi elevati** - La "webification" è un servizio professionale che consente di fornire l'accesso browser a un'applicazione client/server perché sia accessibile attraverso una rete SSL VPN. Un'organizzazione che fornisce servizi professionali SSL VPN crea un controllo ActiveX, un'applet Java o una rappresentazione HTML dell'applicazione che viene eseguita nel browser Web del PC.



## AREA CULTURALE IP SECURITY

**Alt alle minacce!**

Questo processo richiede l'implementazione di un servizio Web in grado di convertire il protocollo e i dati del server dell'applicazione in un front-end compatibile con il Web.

Se la "webification" come servizio professionale richiede dieci giorni a un costo di 2000 dollari al giorno, il totale sarà di 20.000 dollari, oltre al costo del prodotto e ai costi di trasporto e spese accessorie.

**5. Modifiche dell'interfaccia utente** - I dipendenti si abituano alle interfacce utente esistenti. È molto probabile che lo sviluppo di interfacce browser non intuitive per applicazioni native trasformerà l'aspetto dell'applicazione. Una situazione del genere può richiedere alle organizzazioni tempi significativamente elevati per riabituare gli utenti insoddisfatti all'utilizzo dell'applicazione.

**6. Funzionalità inibita del protocollo (ad esempio SMB)** - Proprio come un'interfaccia non intuitiva può influire negativamente sull'efficienza di un dipendente che utilizza un'applicazione sottoposta a "webification", la medesima situazione può verificarsi con alcune delle conversioni del protocollo di base incluse in una soluzione SSL VPN.

Un esempio di questa situazione è il protocollo SMB (Server Message Block). Se un utente si trova alla propria scrivania, le unità di rete mappate sono disponibili per l'accesso o il salvataggio di file anche da applicazioni quali Microsoft Word, Microsoft PowerPoint, Microsoft Excel, ecc.

Costringere un utente remoto che utilizza una rete SSL VPN a utilizzare un protocollo di condivisione file sottoposto a "webification" diminuisce l'efficienza di tale utente, in special modo se non si tratta di un *power user*.

**7. Il traffico in tempo reale (voce o video) non è supportato** - Le soluzioni SSL VPN non sono in grado di supportare il traffico vocale o video in tempo reale, ovvero gli utenti non possono usufruire di servizi di telefonia software sui propri PC o di sessioni video di formazione in tempo reale.

**8. Le modalità chiosco possono lasciare file temporanei e cookie** - Una rete SSL VPN utilizzata tramite chioschi multimediali esegue uno script di pulizia al termine della sessione, per eliminare i file temporanei eventualmente aperti nella posta elettronica e per eliminare i cookie presenti.

Il problema di questo approccio è che il processo può non essere completato, qualora si verifichi un errore del browser durante la sessione. Se il browser subisce un arresto anomalo durante la sessione, lo script di pulizia non verrà eseguito e tutte le informazioni proprietarie aperte durante la sessione verranno memorizzate nel chiosco.

**9. I tempi di installazione possono venire rappresentati in maniera inaccurata** - I fornitori di soluzioni SSL VPN vantano una significativa riduzione della quantità di tempo necessaria per installare una soluzione SSL VPN rispetto alle soluzioni IPsec. Questa affermazione, tuttavia, presuppone che il fornitore della soluzione SSL VPN non debba eseguire alcun intervento di personalizzazione o erogare servizi professionali. Persino quando si utilizzano connettori personalizzati, si verificano problemi con le voci DNS separate che aumentano i tempi di installazione sia dell'applicazione che del client.

La "webification" di un'applicazione incrementa ulteriormente i tempi richiesti per



## AREA CULTURALE IP SECURITY

## Alt alle minacce!

l'installazione. In altre parole, questa grande riduzione dei tempi di installazione si ottiene quando la soluzione SSL VPN può essere installata senza apportare modifiche all'applicazione o al client o senza dover erogare servizi professionali.

### Riepilogo delle soluzioni SSL VPN

Le soluzioni SSL VPN funzionano dalla maggior parte dei computer, anche se protetti da svariate configurazioni di firewall. Presentano tuttavia alcuni inconvenienti:

1. SSL VPN non rappresenta una soluzione completa per l'accesso remoto. È compatibile solo con determinati tipi di applicazioni Web e non con applicazioni Web avanzate che utilizzano tecnologie a oggetti binari come applet Java e controlli ActiveX. Non sono compatibili con applicazioni client/server in assenza di connettori personalizzati o costose "webification".
2. Le soluzioni SSL VPN sono lente a causa del numero limitato di applicazioni client/server supportate.
3. Le soluzioni SSL VPN risultano lente per le applicazioni Web; la logica dal lato server richiede l'analisi e la riscrittura delle applicazioni Web.
4. Le soluzioni SSL VPN non consentono l'utilizzo di applicazioni peer-to-peer o in tempo reale, dove due applicazioni devono aprire reciprocamente connessioni IP separate per stabilire percorsi dei dati, allo scopo di consentire il funzionamento del protocollo peer-to-peer o anche del protocollo client/server.

5. Le soluzioni SSL VPN forniscono un accesso "innaturale" ad applicazioni limitate, invece di un accesso simile a quello sperimentato dagli utenti dalla propria scrivania.

Chiaramente, la tecnologia di accesso remoto SSL VPN non è quindi in grado di soddisfare tutte le esigenze di accesso remoto.

### Le tecnologie prevalenti non sono all'altezza della situazione

La tecnologia IPsec è in grado di incapsulare in pratica qualsiasi tipo di traffico e di inoltrarlo all'host di destinazione, offrendo all'utente l'illusione di trovarsi nella rete principale. Tuttavia, l'installazione e la manutenzione risultano complicate e costose e questa tecnologia è notoriamente inaffidabile quando è necessario passare attraverso firewall e dispositivi NAT e persino attraverso alcune reti ISP. D'altro canto, SSL attraversa con tranquillità la maggior parte degli ambienti di rete affidandosi all'ubiquità dell'accesso Web e in numerosi casi non richiede alcuna installazione dal lato client, in quanto la maggior parte degli utenti dispone già di un browser Web. Poiché si affida a una tecnologia Web, tuttavia, SSL presenta anche una serie di importanti limitazioni. Le prestazioni rappresentano un problema, a causa della necessità di riscrivere al momento i siti Web e non è possibile convertire applicazioni Web che utilizzano tecnologie binarie come Java e Microsoft ActiveX®. Le applicazioni client/server come Microsoft Outlook, implementazioni CRM e i database devono venire sottoposte a "webification" o disporre di connettori personalizzati appositamente scritti, per poter funzionare sulla rete SSL VPN. Tutto questo



## AREA CULTURALE IP SECURITY

## Alt alle minacce!

implica un notevole costo per l'organizzazione.

È quindi necessaria una soluzione che combini i punti di forza di ciascuna soluzione evitandone allo stesso tempo i punti deboli. Numerose organizzazioni rispondono a questa sfida utilizzando entrambe le tecnologie laddove esse risultano più appropriate, ma questo approccio richiede infrastrutture parallele e maggiori costi di supporto e non consente comunque un accesso uniforme in tutte le circostanze.

### **LA SOLUZIONE WATCHGUARD®: I VANTAGGI DI IPSEC E SSL SENZA GLI SVANTAGGI**

WatchGuard® Firebox® SSL Core™ VPN Gateway utilizza la tecnologia Citrix® Secure Access che, sebbene basata sulla tecnologia SSL VPN, combina tutti i vantaggi di IPsec in termini di connettività di rete con la capacità offerta da SSL VPN di ottenere l'accesso dalla maggior parte delle reti, indipendentemente dalla configurazione NAT o del firewall.

#### **Un'analisi delle esigenze**

Un utente finale può indicare le proprie esigenze nel modo seguente: "Un accesso in maniera sicura a ogni risorsa protetta da qualsiasi luogo". È una richiesta davvero impegnativa. Nel caso in cui l'utente mobile utilizzi un computer preso in prestito o si trovi in un chiosco multimediale, la soluzione VPN non deve dipendere dalla possibilità di installare software nel computer, poiché l'utente potrebbe non averne l'autorizzazione. Quando la sessione è completata, la soluzione non può lasciare tracce della presenza o delle attività dell'utente finale che potrebbero essere rilevate da estranei. Un amministratore di

rete potrebbe inoltre richiedere che gli utenti possano accedere alle risorse solo il numero di volte necessario. Il reparto amministrativo potrebbe richiedere che la distribuzione o la manutenzione della soluzione non risultino economicamente onerose. In breve, gli utenti mobili richiedono un mezzo protetto, affidabile, flessibile ed economico per accedere alla rete quando si trovano fuori sede.

### **CLIENT DI ACCESSO PROTETTO: ACCESSO UNIVERSALE SEMPLIFICATO**

WatchGuard Firebox SSL VPN Gateway controlla le connessioni tra gli utenti finali fuori sede e la rete principale. Il traffico di rete diretto verso la rete principale viene incapsulato in SSL dal client Citrix® Secure Access, un client leggero scaricato automaticamente nel browser dell'utente finale dopo l'autenticazione. Poiché il traffico è incapsulato, non sono necessari "webification" o connettori personalizzati per supportare l'accesso completo alla rete. Inoltre il traffico è di tipo SSL, quindi non può essere danneggiato da dispositivi NAT o da altre misure che disturbano le connessioni IPsec. Le funzioni di autenticazione e il meccanismo di distribuzione del client Citrix® Secure Access sono disponibili sul sito Web protetto esterno di Firebox SSL VPN Gateway.

#### **Definizione del tunnel protetto**

Il completamento della sequenza di autenticazione stabilisce un tunnel protetto su HTTPS (porta 443 o qualsiasi altra porta configurata sul gateway) utilizzando SSL. Dopo avere stabilito il tunnel, il gateway invia al client Citrix® Secure Access le informazioni di configurazione che



## AREA CULTURALE IP SECURITY

**Alt alle minacce!**

descrivono le reti raggiungibili attraverso la connessione protetta.

### **Tunneling del traffico di indirizzi privati di destinazione su SSL**

Dopo l'autenticazione e un'appropriata configurazione, tutto il traffico di rete o solo il traffico di rete destinato alle reti esterne al gateway, viene acquisito e reindirizzato nel tunnel protetto fino all'interfaccia pubblica del gateway (questa opzione è definita "split tunneling" ed è configurabile sul gateway). Tutti i pacchetti IP, indipendentemente dal protocollo, vengono acquisiti in questo modo e trasmessi sulla connessione protetta analogamente a quanto avviene con un client IPsec. Tuttavia, dal momento che i routing di rete non vengono annunciati sul computer client, i worm non sono in grado di utilizzare questo tunnel per propagarsi dal computer client alla rete aziendale. Questa funzionalità fornisce la cosiddetta "in office experience" della soluzione

### **WatchGuard Firebox SSL VPN**

Chiusura del tunnel protetto e rigenerazione dei pacchetti sulla rete privata Firebox SSL termina il tunnel SSL e accetta qualsiasi pacchetto in entrata destinato alla rete privata. Se il traffico soddisfa i criteri di controllo dell'accesso e di autorizzazione, viene innanzitutto riscritto (le intestazioni IP vengono ricreate per essere visualizzate dall'intervallo di indirizzi IP della rete privata di Firebox SSL oppure dall'IP privato assegnato al client) e quindi trasferito alla rete privata. Per le connessioni di circuito, il gateway aggiorna una tabella NAT di mappatura porte, in modo che sia possibile far corrispondere le connessioni e inviare nuovamente i pacchetti attraverso il tunnel al client con i numeri di porta corretti in modo

tale che siano in grado di raggiungere l'applicazione corretta.

### **CLIENT DI ACCESSO PROTETTO: PROTEZIONE AFFIDABILE**

#### **Funzionalità "always-on" configurabile**

Quando il laptop o il PC è disconnesso dalla rete, il client Citrix® Secure Access continua a essere eseguito in memoria. Questa funzionalità "always-on" (sempre attivo) fornisce all'utente vantaggi quali la riconnessione automatica (la connessione VPN viene ripristinata automaticamente al ritorno della connessione di rete), connettività in voce remota, controllo remoto dei PC da parte del reparto IT e così via. Questa modalità fornisce un mezzo potente per assicurare sempre la protezione su reti 802.11 senza la necessità di distribuire e gestire un ambiente WEP o WPA/PSK. Questa funzionalità non è attualmente disponibile in soluzioni IPsec o SSL VPN.

#### **Protezione endpoint integrata**

La protezione endpoint integrata consente di monitorare continuamente e in tempo reale componenti quali file, checksum e controlli del Registro di sistema oltre a indicare se l'endpoint è un asset aziendale autorizzato. L'accesso alla rete aziendale viene consentito solo se il criterio di protezione per il computer client viene soddisfatto e continua a esserlo durante la sessione SSL VPN. Per fornire questa funzionalità, le implementazioni concorrenti si affidano a prodotti di terze parti, con ulteriori costi aggiuntivi e impegnative attività di integrazione. Nelle poche soluzioni SSL VPN in grado di eseguire controlli limitati integrati nel prodotto, il controllo viene eseguito una sola volta e solo durante l'accesso al proprio



## AREA CULTURALE IP SECURITY

**Alt alle minacce!**

portale di applicazioni sottoposte a "webification". Endpoint Assurance è incluso in WatchGuard Firebox SSL VPN Gateway.

### **Blocco trasversale worm**

Dal momento che le informazioni di routing di rete non vengono propagate nel computer client dalla rete attraverso il tunnel SSL VPN, i worm non sono in grado di utilizzare il tunnel SSL VPN per passare dal computer client alla rete aziendale, pertanto viene assicurata una maggiore protezione.

### **Controllo remoto**

Il controllo remoto integrato elimina i tempi e le spese associati ad applicazioni di terze parti quali Microsoft NetMeeting®, Virtual Network Computing o costoso software di videoconferenza Web per accedere, valutare e riparare i computer remoti. Oltre a fornire agli amministratori IT e di rete opzioni potenziate per la risoluzione dei problemi, il controllo remoto può essere utilizzato dai dipendenti come strumento di collaborazione immediata. I dipendenti possono quindi condividere la maggior parte delle applicazioni desktop semplicemente facendo clic con il tasto destro del mouse sull'icona di Firebox SSL Secure Access e selezionando la persona con la quale desiderano collaborare.

### **Funzionamento attraverso proxy e firewall NAT**

Il tunnel di Firebox SSL VPN Gateway viene stabilito utilizzando HTTPS, HTTPS con proxy o SOCKS. In questo modo diventa compatibile con il firewall e consente ai computer di accedere in maniera affidabile alle reti private dalla rete protetta da firewall di un'altra organizzazione, senza richiedere la riconfigurazione della rete o del client.

### **Algoritmi di crittografia**

Il tunnel di Firebox SSL VPN Gateway è crittografato con SSL/TLS. Interi flussi di dati vengono crittografati, incluse le informazioni di intestazione come l'intestazione IP. Il Firebox SSL VPN Gateway supporta la crittografia a 196 bit, oltre ai valori di bit superiori o inferiori impostati nel certificato. Inoltre il Firebox SSL VPN Gateway supporta tutte le codifiche OpenSSL: CAST, CAST5, DES, Triple-DES, IDEA, RC2, RC4, RC5, SSL v3 e TLS v1.

### **Gestione di protocolli bidirezionali**

Il protocollo FTP e molte applicazioni vocali in tempo reale richiedono che il client stabilisca una connessione con il server che a sua volta crea una connessione con il client. Per queste applicazioni, il client Citrix® Secure

Access è in grado di fornire all'applicazione locale un indirizzo IP privato che WatchGuard Firebox SSL VPN Gateway utilizzerà sulla rete interna per gestire le comunicazioni bidirezionali tra il client e il server.

### **Prestazioni e traffico in tempo reale**

Molte applicazioni, ad esempio quelle vocali e video, sono in tempo reale, pertanto sono implementate tramite UDP. Con queste applicazioni, è più importante inoltrare i pacchetti in tempo reale che assicurarsi che tutti i pacchetti siano inoltrati. Tuttavia, con qualsiasi tecnologia di tunneling su TCP, non è possibile soddisfare questi requisiti di prestazioni in tempo reale.

WatchGuard Firebox SSL VPN Gateway risolve questo problema instradando i pacchetti UDP nel tunnel protetto in forma di pacchetti IP personalizzati che non



## AREA CULTURALE IP SECURITY

## Alt alle minacce!

richiedono riconoscimenti TCP. Anche se i pacchetti si perdono nella rete, non vi è alcun tentativo da parte delle applicazioni client o server di rigenerarli, pertanto le prestazioni in tempo reale (analogamente a UDP) sono raggiunte attraverso un tunnel protetto basato su TCP.

### **Soluzione con client di accesso protetto**

WatchGuard Firebox SSL VPN Gateway fornisce accesso remoto protetto alle reti e a tutte le applicazioni di un'organizzazione tramite SSL/TLS. Questa applicazione è adatta a dipendenti che accedono in modalità remota all'organizzazione e per l'accesso Intranet da reti LAN con restrizioni quali reti wireless e siti client. Con WatchGuard Firebox SSL VPN funzionalità quali il roaming "always-on", la protezione integrata endpoint e il controllo remoto sono integrate nel prodotto e non richiedono l'acquisto di prodotti che soddisfino questi requisiti.

### **MODALITÀ CHIOSCO**

La modalità chiosco è progettata per fornire l'accesso a risorse aziendali da computer pubblici, ad esempio i computer di Internet café o di biblioteche, oppure da dispositivi che supportano una Java Virtual Machine.

### **Supporto applicazioni**

Nella modalità chiosco, Firebox SSL fornisce accesso a Citrix ICA, funzionalità di desktop remoto, protocollo SSH, software di emulazione Telnet 3270, server VNC e accesso con un clic a unità di rete condivise. L'accesso può essere controllato in base al gruppo.

### **Acquisizione dell'accesso remoto**

Agli utenti finali sarà sufficiente accedere con il browser a un URL Web protetto per ottenere l'accesso remoto.

Una volta connessi, ai client sono richiesti nome utente e password attraverso HTTP 401 Basic, Digest o NTLM. Firebox SSL autentica quindi queste credenziali con il server di accesso dell'organizzazione (ad esempio Microsoft Active Directory o RADIUS) e, se le credenziali sono corrette, consente all'utente di scegliere una connessione dal proprio computer o da un computer pubblico. Se viene scelta la connessione da un computer pubblico, all'utente viene concesso un accesso limitato alla rete aziendale dell'organizzazione attraverso la modalità chiosco.

### **Funzionamento**

In modalità chiosco, Firebox SSL apre una connessione di tipo VNC (Virtual Network Computing) in una finestra. Firebox SSL invia solo immagini (non dati) attraverso la connessione VPN. Per questo motivo non vi è il rischio di lasciare file temporanei o cookie nel computer pubblico.

- Per computer che eseguono Windows 2000 e versioni successive, la funzionalità chiosco è disponibile attraverso il portale di accesso. Il link al chiosco può essere rimosso dal portale di accesso in base ai diversi.
- Per computer che eseguono JVM 1.4.2 o versioni successive (come computer Macintosh o Windows 95/98), la funzionalità chiosco è disponibile attraverso un'applet Java.
- In Macintosh, il browser supportato è Safari.

### **RIEPILOGO**

Le soluzioni IPsec e SSL VPN presentano vantaggi e svantaggi. Per soddisfare l'esigenza di un accesso remoto, protetto ed



## AREA CULTURALE IP SECURITY

**Alt alle minacce!**

economico per utenti mobili, le organizzazioni necessitano dei vantaggi di entrambi questi tipi di prodotto, senza nessuno degli svantaggi. WatchGuard Firebox SSL VPN Gateway con Citrix® Secure Access fornisce ad aziende e organizzazioni i vantaggi sia di IPsec VPN che di SSL VPN senza i relativi problemi, evitando la necessità di implementare soluzioni IPsec o SSL VPN pure.

Se le soluzioni IPsec VPN forniscono crittografia e accesso a livello di rete e le soluzioni SSL VPN forniscono crittografia e accesso a livello di applicazione, WatchGuard combina le funzionalità di accesso a livello di rete e crittografia a livello di applicazione in una tecnologia ibrida. In questo modo l'esperienza di rete dell'utente finale viene significativamente migliorata e allo stesso tempo vengono drasticamente ridotti i costi generali di manutenzione e di protezione sostenuti dal reparto IT.

WatchGuard Firebox SSL VPN Gateway offre quanto segue:

- Accesso universale protetto e semplificato per tutte le applicazioni, incluse applicazioni in tempo reale e VoIP
- Impareggiabile semplicità di utilizzo
- Protezione affidabile e controllo amministrativo
- I costi complessivi di proprietà più bassi della sua categoria

### **Libertà e produttività**

Le soluzioni IPsec e SSL VPN presentano entrambe vantaggi e svantaggi ma WatchGuard Firebox SSL VPN Gateway con Citrix® Secure Access offre alle organizzazioni solo il meglio di entrambe le soluzioni. Integrando i vantaggi combinati di IPsec e SSL in un unico prodotto di semplice installazione e gestione, Firebox

SSL VPN Gateway facilita il dinamismo dell'azienda con una soluzione di accesso remoto protetto che non richiede assolutamente connettori aggiuntivi o interventi di "webification".

Per ulteriori informazioni sulle soluzioni di protezione WatchGuard, visitare il sito Web [www.watchguard.com](http://www.watchguard.com) oppure rivolgersi ad EDSlan.