

VPN SSL e VPN IPSec a confronto

White Paper



Questo documento contiene informazioni sulle VPN basate su IPSec e quelle basate su SSL. In particolare:

- Le principali differenze
- I loro pro e contro
- La tecnologia più adatta alle esigenze di ognuno

Distributore ufficiale per l'Italia: Horus Informatica

Tel: (+39) 02 33510135

Fax commerciale: (+39) 02 33510199

Email: commerciale@horus.it



www.horus.it

Introduzione

Le reti private virtuali o Virtual Private Network (VPN) consentono alle aziende di espandere le possibilità di accesso alle reti interne a dipendenti esterni e partner su reti internet pubbliche standard. La ragione principale per cui furono create le VPN era l'elevatissimo costo per linee in leasing. Un'azienda doveva avere un collegamento fisicamente chiuso tra i propri partner e i dipendenti remoti, o attraverso un server di accesso remoto (o RAS, Remote Access Server) con collegamento dialup verso la rete aziendale, o affittando frazioni di connessioni T1 tra gli uffici remoti e i partner.

Cos'è una VPN, in realtà?

Una VPN è una tecnologia che consente ai client (i dipendenti) e ai partner di sfruttare i normali provider di accesso pubblici (ISP) e le linee ad alta velocità per accedere a reti private chiuse. Un comune fraintendimento è che le VPN siano sempre soluzioni basate su IPSec. Di fatto, esistono molti protocolli di codifica e sicurezza che offrono le funzionalità di una VPN. SSL è solo uno di questi.

Che cos'è un protocollo di codifica o sicurezza?

I protocolli di sicurezza e di codifica sono protocolli di trasmissione utilizzati per trasmettere in maniera sicura dati ad elevato valore. La codifica, che è al cuore di qualsiasi protocollo di sicurezza, offre tre vantaggi fondamentali rispetto al 'testo in chiaro' o ai dati non codificati:

Riservatezza dei dati

- ovvero la capacità di nascondere i dati trasmessi;

Autenticità e integrità dei dati

- l'algoritmo matematico di codifica permette ai protocolli di sicurezza di garantire che i dati non siano stati modificati o danneggiati durante la trasmissione;

Nessun rifiuto

- un'altra caratteristica dell'algoritmo di codifica è la possibilità di provare che un evento si è verificato

Cos'è l'IPSec?

L'IPSec, o Internet Protocol Security, il protocollo di sicurezza più comunemente associato con una VPN, è un protocollo di codifica che garantisce la trasmissione sicura dei dati codificati presso il Network Layer, su una rete pubblica come internet. Due utenti che desiderano creare un tunnel IPSec devono prima di tutto stabilire una modalità standard per comunicare. Poiché l'IPSec supporta diverse modalità operative, entrambe le parti devono innanzitutto decidere sulla policy di sicurezza e la modalità da utilizzare, a quali algoritmi di codifica e quale metodologia di autenticazione ricorrere nella comunicazione.

Nell'IPSec, una volta che il tunnel IPSec è stato attivato, tutti i protocolli del network layer tra due parti in comunicazione sono codificati. TCP, UDP, SNMP, HTTP, POP, AIM, KaZaa etc., sono tutti codificati, indipendentemente dalla sicurezza e codifica già esistenti (o non esistenti).

Aspetti e problemi dell'IPSec

Poiché l'IPSec si localizza presso il network layer, non solo il traffico di rete viene codificato, ma tutti gli utenti dispongono dell'accesso alle risorse aziendali come se fossero fisicamente presenti in ufficio e collegati alla LAN. Si può decidere se consentire o negare l'accesso alla rete ai partner e ai dipendenti che operano temporaneamente da remoto. Potrebbe essere necessario garantire la sicurezza del traffico solo in una piccola porzione della rete, evitando di codificare tutto quello che passa tra client remoto e rete aziendale.

Aspetto 1: software del client

L'IPSec richiede un software per client dedicato, che in molti casi sostituisce o complementa i sistemi client dello stack TCP/IP. In molti sistemi ciò introduce rischi di compatibilità con altri sistemi software e rischi di accesso da parte di trojan, in particolare se il software client viene scaricato dal web e non installato dal personale tecnico. Per come l'IPSec è stato creato e per la carenza di conformità con lo standard, praticamente tutte le soluzioni IPSec sono proprietarie e non compatibili con le altre.

In alcuni casi, l'IPSec viene eseguito su un'appliance hardware della rete. Queste soluzioni comportano spesso l'esigenza di avere lo stesso hardware ai due estremi della comunicazione. Inoltre, le stesse questioni di compatibilità relative ai software dei client si possono ritrovare negli hardware dotati di IPSec.

I client IPSec sono legati a un laptop specifico o a un sistema desktop. Ciò limita la mobilità degli utenti, che non possono collegarsi alla VPN senza che un client IPSec venga prima caricato sul sistema client utilizzato per accedere alla rete. Dalle sale di attesa degli aeroporti, ad esempio, risulta impossibile collegarsi.

Aspetto 2: supporto tecnico

Le soluzioni IPSec hanno bisogno di un fortissimo supporto tecnico sia per l'implementazione che per la manutenzione di lungo termine.

Le aziende più grandi hanno spesso personale dedicato all'assistenza e rivolto a supportare i dipendenti che operano da remoto tramite IPSec.

Aspetto 3: limitazioni della piattaforma

I client IPSec funzionano di solito solo su macchine windows. Esistono pochissime implementazioni dell'IPSec su altre piattaforme PC come Mac, Linux, Solaris, ecc.

Cos'è l'SSL e in cosa è diverso?

L'SSL, o Secure Sockets Layer, è un protocollo a livello di applicazione più comunemente utilizzato per rendere sicure le comunicazioni web via internet. L'SSL utilizza la codifica e l'autenticazione in maniera analoga all'IPSec. In origine, il protocollo SSL codificava il traffico tra due applicazioni che volevano interagire l'una con l'altra ma che non codificavano il traffico tra un host e l'altro. Oggi, grazie ai progressi della tecnologia, le VPN SSL possono essere utilizzate per codificare tutto il traffico tra client e server con VPN SSL in maniera simile alla codifica dei client IPSec, ma senza l'utilizzo di un client. Qualsiasi software sul lato client necessario a supportare la codifica del network layer viene scaricato istantaneamente mediante tecnologia ActiveX o Java dopo che l'utente è stato debitamente autenticato e autorizzato. Si tratta di una tecnologia trasparente, che permette la gestione e il controllo centralizzati, poiché i client 'light' sono di tipo intelligente e gestiti tramite il gateway di controllo centralizzato degli accessi. Ciò porta il supporto del client oltre le applicazioni 'SSL aware', verso altre applicazioni, come i web browser (ad es. Internet Explorer e Netscape) o client di posta elettronica (ad es. Outlook ed Eudora) che utilizzano qualsiasi protocollo IP-based (ad es. TCP, UDP, ICMP ecc.) per sfruttare una vasta gamma di applicazioni alternative, quali navigazione web o videoconferenza, su un meccanismo di tunneling ovunque presente.

Perché utilizzare un proxy SSL?

Esistono molte motivazioni per utilizzare un server proxy anziché stabilire una comunicazione diretta tra client e una risorsa dotata di SSL. La più evidente è il rendimento.

Motivazione 1: maggior rendimento

L'SSL è un protocollo di per sé molto veloce; tuttavia, come ogni altro protocollo di codifica, vi sono alcuni calcoli estremamente onerosi per la CPU che devono essere effettuati prima che venga stabilita una sessione sicura. Un esempio è l'algoritmo RSA, che viene utilizzato nell'ambito dell'SSL per negoziare le chiavi tra client e server. Nel processo di negoziazione, il server deve decodificare e verificare una firma digitale: entrambe sono operazioni che impegnano molto il processore. La maggior parte dei server web moderni, ad esempio, può accettare solo 75 nuove connessioni SSL al secondo e per ognuna di queste deve essere effettuata un'operazione RSA di decodifica e verifica. Se il sistema dovesse accettare più di 75 connessioni al secondo, l'utilizzazione della CPU supererebbe di gran lunga il consentito e il server non risponderebbe più alle richieste di rete.

Al fine di incrementare la capacità del server, i proxy SSL possono comprendere un acceleratore SSL, il quale è molto simile al co-processore dei PC 486SX/DX. L'acceleratore SSL effettua le operazioni di calcolo più onerose precedentemente affidate alla CPU del server e le elabora tramite un processore ad hoc. Il server, che prima era in grado di effettuare un massimo di 75 sessioni RSA al secondo, può gestire ora più di 800 sessioni al secondo.

Ci si potrebbe chiedere perché si ha bisogno di un proxy SSL se il server ha un acceleratore SSL. Ma in realtà quello che ci si deve chiedere è: quanti dei server posseduti potrebbero aver bisogno di un'accelerazione SSL? Si dispone delle risorse per acquistare acceleratori SSL per ognuno di questi server? Il vantaggio di un proxy SSL è che si può utilizzare lo stesso acceleratore SSL per molti server?

Grazie ad Array SP (Security Proxy) di Array Networks, ad esempio, si possono avviare 800 connessioni SSL al secondo dai client che accedono alle risorse, mantenendo una sola connessione SSL attiva tra il proxy ed il server di back-end. Si noti che l'Array SP è in grado di avviare un numero ridotto di collegamenti SSL verso il back-end, mentre gestisce fino a 800 sessioni al secondo di Array SP. Il chiaro vantaggio è che il server web non viene mai sovraccaricato a causa di richieste di collegamento SSL.

Motivazione 2: autenticazione

Un'ulteriore aspetto del protocollo SSL tradizionale è la mancanza di metodi di autenticazione impiegati. L'SSL comprende l'autenticazione crittografica sia per il server che per il client, ma tutta la sicurezza si basa sul concetto che la chiave crittografica del client è stata tenuta sicura. Se la chiave fosse stata compromessa o non vigilata, non si potrebbe più fare affidamento sul client. Potrebbe essere necessario aggiungere ulteriori metodi di autenticazione all'SSL per garantire che l'utente o il client sia effettivamente chi dice di essere.

Un proxy SSL, tuttavia, prevede l'autenticazione forte dei client prima ancora che questi si colleghino alle risorse back-end. I proxy SSL garantiscono metodi di autenticazione ancora più forti di quanto una risorsa back-end potrebbe supportare come caratteristica nativa. Molti server web oggi non supportano metodi di autenticazioni nativi diversi dall'SSL.

Perché utilizzare un proxy SSL su VPN IPSec?

Non è richiesto software o hardware dal lato client

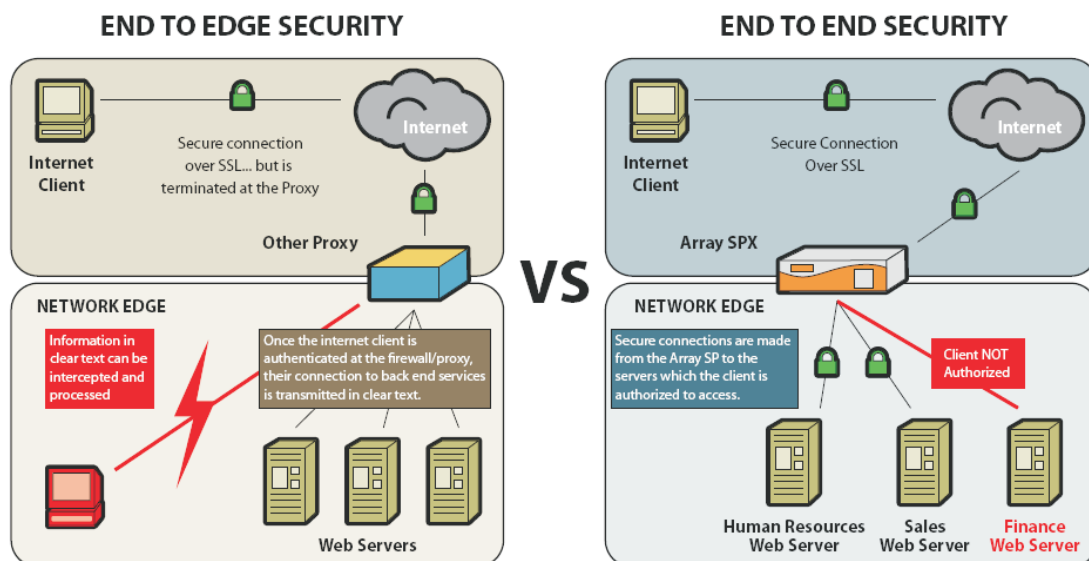
Un vantaggio chiave di un proxy SSL è che non deve essere caricato né distribuito alcun software per client tra i client stessi. I proxy SSL possono utilizzare browser web client e-mail standard che sono già abilitati all'utilizzo dell'SSL.

Interfaccia web facile da utilizzare e supportare

I browser web e i client e-mail dotati di SSL sono di vario tipo e trovano impiego su piattaforme Windows, Macintosh e Linux/UNIX, su PDA e persino cellulari e tutti possono comunicare in maniera sicura tramite SSL. I dipendenti hanno già una discreta familiarità nell'utilizzo ed è minima la necessità di formare l'utente finale.

Sicurezza End-to-End e End-to-Edge a confronto

Uno dei maggiori svantaggi dell'IPSec è che crea semplicemente un tunnel sicuro tra il client e un server VPN periferico. Quando il client richiede l'accesso a una risorsa, viene considerato come parte di quella stessa rete su cui la risorsa risiede tramite IPSec. L'unica connessione sicura è quella tra client e la risorsa aziendale; tutti i dati circolanti nella rete interna sono in chiaro, comprese le password e i dati sensibili.



Con l'SSL, il tunnel sicuro viene creato direttamente dal client alla risorsa cui questo accede. Grazie a una vera sicurezza end-to-end, nessun dato viene inviato in chiaro, né sulla rete interna né in internet. Tutto ciò che viaggia tra il client e la risorsa viene autenticato e codificato in maniera sicura.

Quale tecnologia è più adatta per le mie esigenze

IPSec: trova il suo miglior impiego nella connettività Site-to-Site dove i tunnel sono permanenti, come nel caso di collegamento tra filiali e sedi centrali e in quegli scenari in cui programmi automatici veicolano grandi volumi di traffico in background verso altri programmi automatici.

SSL – Da utilizzare per tutti i casi in cui è previsto un accesso da remoto

	VPN SSL	VPN IPSec
Autenticazione	Token di autenticazione monodirezionale Token di autenticazione bidirezionale Certificati digitali	Autenticazione bidirezionale con token Certificati digitali
Codifica	Codifica forte Basato su browser	Codifica forte Dipende dall'implementazione
Sicurezza globale	Sicurezza tra punti terminali Codifica tra client e risorsa	Da perimetro a client Codifica solo tra client e gateway della VPN
Accessibilità	Accesso in ogni momento e in ogni luogo a una base di utenti ampiamente distribuita	Accesso limitato a una base di utenti limitata e ben definita
Costo	Basso Nessuna esigenza di ulteriori software per client	Elevato E' richiesto un software gestito per client
Installazione	Installazione plug and play Nessuna installazione software o hardware dal lato client	Richiede spesso molto tempo E' richiesto software o hardware dal lato client
Semplicità per l'utente	Molto user-friendly; utilizza browser web familiari Non è richiesto un addestramento specifico per gli utenti	Complesso per utenti non esperti Richiede formazione specifica
Applicazioni supportate	Applicazioni web File Sharing E-mail	Tutti i servizi basati su IP
Utenti	Clienti, partner, dipendenti, utenti remoti, vendor, ecc.	Più adatto per usi aziendali interni
Scalabilità	Facilmente installabile e scalabile	Scalabile sul lato server Difficoltà nella scalabilità dei client

Chi è Array Networks

Fondata nel 2000, Array Networks è uno dei principali provider di soluzioni ad alto rendimento per l'accesso sicuro universale. Array offre linee di prodotti indirizzate al crescente mercato delle VPN SSL e al mercato dell'accelerazione delle applicazioni. Più di 500 clienti tra cui aziende, provider di servizi, organizzazioni governative e verticali nel campo della salute, della finanza e della formazione si affidano ad Array per offrire un accesso sicuro e ottimizzato in ogni momento e da ogni luogo. Array fornisce i prodotti per VPN SSL più veloci e scalabili oggi disponibili sul mercato. La tecnologia di Array è 8 volte più veloce e si adatta 12 volte più velocemente del suo più prossimo competitor. Di conseguenza, nessuna azienda è in grado di fornire soluzioni per VPN SSL ad alto rendimento agli stessi costi. Array è stato riconosciuto da aziende leader come Deloitte, Red Herring e Synergy come leader del mercato e tecnologico. La sede principale di Array è a Milpitas, in California, mentre i suoi uffici vendite sono sparsi in tutto il mondo. La società ha circa 60 rivenditori e value-added reseller nel mondo.

Per ulteriori informazioni, visitare il sito www.arraynetworks.it.

Distributore ufficiale per l'Italia:

Horus Informatica

Tel: (+39) 02 33510135

Fax commerciale: (+39) 02 33510199

Email: commerciale@horus.it



www.horus.it