SONICWALL™

Più sicurezza sul web per gli studenti delle scuole primarie e secondarie

Le best practice per controllare l'accesso a Internet dalle reti delle scuole elementari

Abstract

L'accesso a contenuti web inappropriati, pericolosi e illegali espone a rischi gli istituti scolastici primari e secondari. Un servizio di filtraggio dei contenuti efficace permette alle scuole primarie e secondarie e ai distretti scolastici di proteggere le proprie reti, aumentare la produttività degli utenti e rispettare le direttive federali impedendo l'accesso a contenuti web discutibili, non produttivi e non sicuri.

Background

Gli istituti e i distretti scolastici hanno la responsabilità di proteggere gli studenti da contenuti web inappropriati e dannosi. Gli istituti primari e secondari si assumono rischi notevoli nel fornire a studenti, docenti o altri collaboratori dei computer, messi a disposizione dai responsabili IT, con cui accedere a Internet anche al di fuori del perimetro del firewall, all'interno del quale vigono precise policy di utilizzo del web. Ciò è particolarmente vero nel momento in cui quelle connessioni vengono utilizzate per accedere a siti contenenti informazioni, immagini o video inopportuni, pericolosi o illeciti. Questi siti possono essere infettati da malware che potrebbero essere scaricati inavvertitamente e utilizzati per rubare informazioni riservate.

Per ricevere i fondi federali del programma E-Rate, inoltre, le scuole e le biblioteche negli Stati Uniti sono tenute per legge a installare un sistema di filtraggio dei contenuti conforme ai criteri del Children's Internet Protection Act (CIPA). Fornendo a studenti, docenti e personale scolastico un accesso non controllato al web si possono creare situazioni di navigazione improduttiva in Internet, con enormi perdite di produttività e larghezza di banda, per non parlare poi delle possibili responsabilità giuridiche.

Per le scuole primarie e secondarie serve quindi una potente soluzione per la protezione e la produttività, in grado di applicare un filtraggio completo dei contenuti. Le migliori pratiche per una soluzione completa di filtraggio dei contenuti prevedono le seguenti funzionalità:

- Controllo granulare delle policy
- Filtraggio dei contenuti all'interno del perimetro di sicurezza della rete
- Filtraggio dei contenuti oltre il perimetro di sicurezza della rete

Controllo granulare delle policy

Un sistema efficace di content filtering offre una vasta gamma di categorie prestabilite e consente di definire e applicare categorie di

Le best practice richiedono un controllo delle policy e un filtraggio dei contenuti a livello granulare sia all'interno che all'esterno del perimetro di sicurezza della rete.

filtraggio personalizzate quando necessario. Dovrebbe permettere di creare un controllo delle policy per consentire o bloccare singoli URL, domini o IP e di applicare tale controllo a singoli utenti o a gruppi. Il database di filtraggio dei contenuti dovrebbe esaminare in tempo reale milioni di IP, URL e domini di tutto il mondo e confrontare le valutazioni con le policy impostate localmente, riducendo al minimo i falsi positivi.

Per aumentare la sicurezza e la produttività di studenti, docenti e personale scolastico, un servizio di filtraggio dei contenuti dovrebbe consentire l'aggiunta di funzioni di controllo per affinare le policy in modo da limitare l'accesso in base alla data e all'ora del giorno. Ciò permette di applicare regole di filtraggio dei contenuti a siti web ritenuti inappropriati o non produttivi durante l'orario scolastico e lavorativo, ad esempio siti per lo shopping online e quelli che trasmettono eventi sportivi. I siti di questo genere, oltre a influire negativamente sulla produttività e a fungere da vettori per attacchi più ampi provenienti dalla rete globale, consumano larghezza di banda e riducono le prestazioni di rete.

Un sistema di filtraggio granulare dei contenuti dovrebbe essere in grado di creare un elenco di indirizzi IP e URL consentiti all'interno di categorie di contenuti altrimenti interdette. CNN Student News, ad esempio, è un portale di video news concepito ad hoc per i ragazzi delle scuole medie e superiori. Con una soluzione di filtraggio granulare dei contenuti si potrebbe autorizzare il personale scolastico e gli insegnanti a guardare qualsiasi programma sulla CNN, mentre agli studenti potrebbe essere consentito solo l'accesso a CNN Student News e agli altri siti web in streaming espressamente consentiti dalla scuola. Le richieste di accesso a CNN.com da parte degli studenti potrebbero essere reindirizzate automaticamente a CNN Student News.

Filtraggio dei contenuti all'interno del perimetro di sicurezza della rete

In genere i servizi di filtraggio dei contenuti vengono eseguiti su un firewall. Affinché i contenuti vengano filtrati occorre che lo studente o il collaboratore sia connesso a Internet attraverso il firewall. A questo proposito, il fatto che il dispositivo sia personale o fornito dall'ufficio informatico dell'istituto scolastico è irrilevante. Il controllo dei contenuti web viene svolto a livello del gateway di rete dal servizio di filtraggio dei contenuti del firewall. Ciò vale anche nel caso in cui i dispositivi al di fuori della struttura scolastica si colleghino prima alla rete tramite VPN e poi a Internet mediante il firewall di rete. Tuttavia questo non è sufficiente per filtrare i contenuti nei dispositivi come smartphone e tablet, usati a casa o fuori dalla scuola, che si connettono direttamente a Internet dall'esterno del perimetro di sicurezza della rete.

Filtraggio dei contenuti oltre il perimetro di sicurezza della rete

Dal momento che sempre più istituti scolastici forniscono dispositivi abilitati a connettersi al web, la possibilità di filtrare i contenuti oltre il perimetro assume un'importanza decisiva. Molti studenti hanno tablet, laptop e smartphone che possono portare con sé al di fuori del perimetro di sicurezza della rete. Se la scuola fornisce questi dispositivi senza dotarli di alcuna forma di filtraggio dei contenuti, possono emergere dei problemi.

Ad esempio è possibile definire delle policy per far sì che ogni accesso a Internet da un dispositivo in roaming sia instradato tramite VPN attraverso il firewall e sottoposto alla sua policy di filtraggio dei contenuti. Questo tuttavia potrebbe incidere negativamente sulla larghezza di banda disponibile e sulla performance del firewall. Un modo per incrementare le prestazioni consiste nel memorizzare le valutazioni precedenti nella cache locale del firewall.

Per i dispositivi che oltrepassano il perimetro, un'opzione ancora migliore sarebbe un client di filtraggio dei contenuti residente sul dispositivo e con accesso a un database basato sul cloud. In questo modo il dispositivo potrebbe accedere a Internet in qualunque momento e luogo nel pieno rispetto delle policy di filtraggio dei contenuti.

Conclusioni

Quando si parla di filtraggio dei contenuti web, l'obiettivo primario è la salvaguardia degli studenti. Negli Stati Uniti è inoltre fondamentale rispettare le direttive federali come il CIPA per poter accedere ai fondi federali del programma E-Rate. Gli istituti scolastici devono adottare tutte le misure idonee a impedire l'accesso a siti web inappropriati o pericolosi da parte degli studenti in aula o di collaboratori negli uffici amministrativi.

Per scoprire come attuare queste best practice di filtraggio dei contenuti nell'ambiente di sicurezza di rete delle vostre scuole primarie e secondarie, consultate il foglio dati di SonicWall Content Filtering Service.

Informazioni su SonicWall

Da oltre 25 anni SonicWall è il partner di fiducia nel campo della sicurezza. Dalla sicurezza della rete alla protezione degli accessi fino alla sicurezza dell'email, SonicWall ha costantemente ampliato la sua gamma di prodotti consentendo alle organizzazioni di fare innovazione, accelerare e crescere. Con oltre un milione di dispositivi di sicurezza in quasi 200 paesi e aree del mondo, SonicWall permette ai suoi clienti di guardare al futuro con fiducia.
www.sonicwall.com

Per qualsiasi domanda sul possibile utilizzo di questo materiale, contattare:

SonicWall
5455 Great America Parkway,
Santa Clara, CA 95054
www.sonicwall.com

Consulta il nostro sito Web per informazioni sulle sedi regionali e internazionali.