

Vantaggi principali:

Protezione avanzata – Application Security Manager (ASM) offre protezione per le tecnologie emergenti, identificando e respingendo gli attacchi xml, javascript, flash, ftp e di evasione di dati.

Disponibilità garantita – BIG-IP Application Security Module dispone della certificazione ICSA e identifica, isola e blocca attacchi sofisticati senza interferire con le transazioni delle applicazioni autorizzate.

Prestazioni e scalabilità straordinarie – ASM è il firewall per applicazioni Web più veloce sul mercato, con prestazioni almeno triple rispetto alla concorrenza. Grazie al nuovo livello di integrazione con TMOS, ASM migliora la distribuzione delle applicazioni tramite compressione, caching e ottimizzazioni TCP.

Difesa in tempo reale – Diversamente dai metodi di ispezione firme tradizionali, ASM adotta un modello euristico bidirezionale che assicura protezione contro intere classi di minacce basate su HTTP e HTTPS (sia note che sconosciute), anziché limitarsi a contrastare un elenco di attacchi conosciuti. Questa soluzione opera in ambienti di produzione dinamici e operativi.

Controllo dettagliato – Con ASM, l'ispezione di firme e modelli può essere implementata facoltativamente in base alle necessità per aumentare le difese di sistemi IPS e firewall e attraverso la prevenzione degli attacchi su protocolli di rete esterni a questi sistemi. Il potente meccanismo di apprendimento e ottimizzazione adattivo riduce l'onere amministrativo di definizione dei criteri.

Informazioni dettagliate di tipo statistico e legal – ASM può registrare una grande quantità di informazioni sulle transazioni e sugli eventi delle applicazioni, preziose per l'analisi del funzionamento delle applicazioni oltre che per il riconoscimento e il contrasto delle attività non autorizzate.

Protezione immediata – ASM, basato sull'architettura TMOS di BIG-IP, si integra facilmente con l'infrastruttura Web delle aziende. Dopo l'installazione, il meccanismo di apprendimento automatico del modulo definisce in modo rapido e accurato criteri di protezione basati sui requisiti specifici delle applicazioni da proteggere, riducendo drasticamente gli oneri della gestione dei criteri e della configurazione manuale.

BIG-IP Application Security Manager™

Protezione delle applicazioni di nuova generazione

BIG-IP Application Security Manager (ASM) rappresenta la migliore soluzione completa per la protezione e l'application delivery in un'unica piattaforma.

Proteggendo il livello applicazioni da attacchi sia specifici che generici, ASM assicura costantemente l'efficienza e la disponibilità delle applicazioni.

Rappresenta inoltre una soluzione solida e completa che riduce il "box clutter", abbatta i costi di gestione e manutenzione e offre un nuovo livello di protezione preventiva delle applicazioni assicurando al contempo prestazioni eccezionali.

Protezione completa e integrata per la distribuzione delle applicazioni

Con la tendenza sempre crescente alla migrazione delle applicazioni sul Web, quantità sempre maggiori di dati riservati dei clienti vengono esposte a nuovi rischi che la maggior parte dei sistemi di protezione non è in grado di arginare. BIG-IP Application Security Manager riduce considerevolmente le minacce che incombono su dati, proprietà intellettuale e applicazioni Web, proteggendo il patrimonio e l'immagine delle organizzazioni e offrendo al contempo ulteriori vantaggi.

Protezione preventiva contro il furto di identità

ASM assicura la massima protezione delle informazioni personali (numeri di carte di credito, conti bancari e così via), controllando l'accesso a tali informazioni durante ogni richiesta/risposta HTTP.

Standard PCI (Payment Card Industry) di protezione dei dati

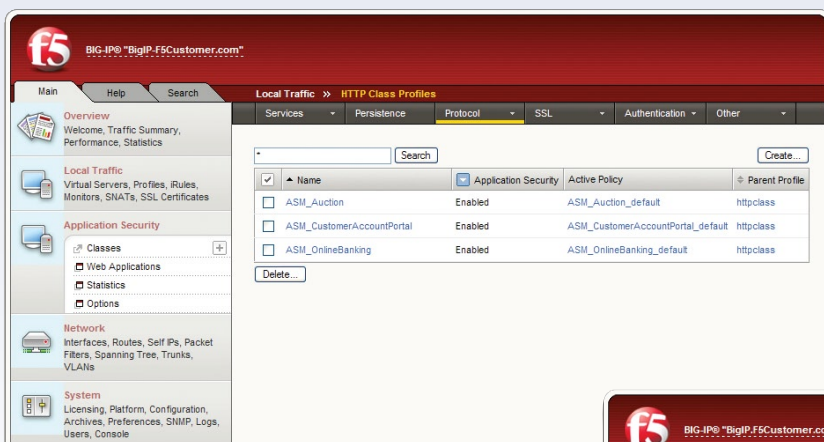
La conformità alle direttive PCI per la protezione dei dati può essere facilitata dall'adozione di una soluzione integrata per la protezione e la distribuzione delle applicazioni. ASM costituisce un'alternativa flessibile e meno costosa alle revisioni annuali del codice.

Costi inferiori per lo sviluppo delle applicazioni

In mancanza di un contesto adeguatamente protetto, gli sviluppatori sono costretti a escludere ogni possibile problema di protezione inserendo nel codice delle proprie applicazioni tutte le contromisure necessarie. Alcune vulnerabilità possono essere individuate dagli scanner di applicazioni, ma la revisione rigorosa e la riscrittura del codice restano sempre necessarie. Con ASM, gli sviluppatori possono concentrarsi sul deployment rapido delle nuove applicazioni e funzionalità, consapevoli che il proprio codice verrà eseguito entro un solido perimetro di protezione.

Riduzione dei costi di risoluzione dei problemi

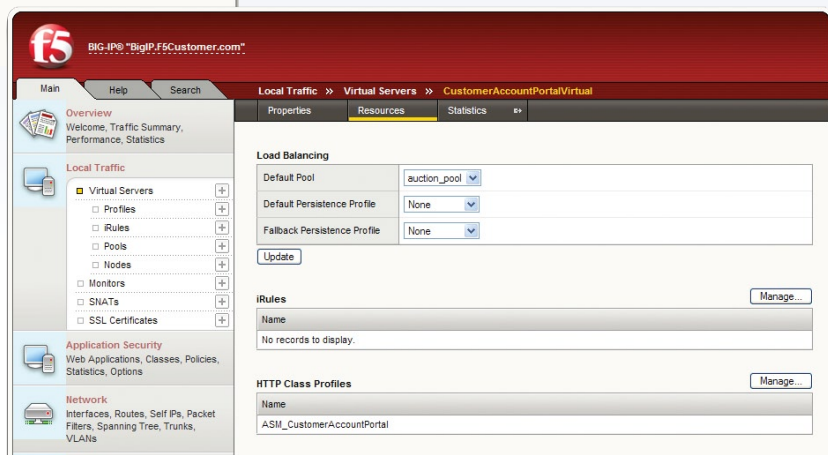
Oltre al costo degli attacchi in sé, le aziende sostengono costi notevoli per far fronte agli attacchi e riparare i danni. Il problema non riguarda solo il reparto IT, ma può coinvolgere le sfere delle pubbliche relazioni e dell'immagine dell'azienda, sollevare problemi legali ed esporre a costi di adeguamento. ASM blocca gli attacchi prima che possano provocare alcun danno.



Grazie all'interfaccia grafica del BIG-IP, specificare quali applicazioni web sono autorizzate diventa facile.

Potete definire la politica di sicurezza per molte applicazioni, per un'applicazione intera o solo per una sezione di un'applicazione individuale.

Definite ed applicate una politica di sicurezza positiva completa sull'integralità del traffico su un Virtual Server



Rendimento dell'investimento facilmente quantificabile

La combinazione della protezione delle applicazioni Web con il sistema di gestione del traffico applicativo di BIG-IP consente di ridurre i tempi di deployment, semplificare la progettazione dell'infrastruttura e ridurre i costi complessivi imputabili alla protezione, ai danni provocati dagli attacchi e alle relative contromisure.

Protezione completa contro i rischi esterni

BIG-IP Application Security Manager rappresenta una tecnologia di protezione leader per il filtraggio sicuro del traffico applicativo gestito dalla solida piattaforma di BIG-IP. Il risultato finale è una soluzione completa, flessibile e di facile gestione per la protezione delle applicazioni Web.

Vantaggi offerti da Application Security Manager:

- Protezione euristica bidirezionale da attacchi specifici:
- Apprendimento adattivo e motore di ottimizzazione
 - Criteri di protezione standard preconfigurati e testati
 - Manipolazione di input non convalidato
 - Controllo delle violazioni di accesso (forceful browsing)
 - Overflow del buffer
 - Cross-site scripting
 - Attacchi intrusivi nel codice SQL/sistema operativo
 - Cookie poisoning
 - Invio di richieste HTTP non valide

I filtri basati sul riconoscimento selettivo delle firme offrono protezione globale dai seguenti attacchi:

- Attacchi Denial of Service automatici
- Worm e vulnerabilità noti
- Richieste di tipi di file e oggetti soggetti a limitazioni
- Altri exploit noti

Cloaking:

- Prevenzione dall'identificazione di sistema operativo e server Web
- Occultamento dei messaggi di errore HTTP agli utenti
- Rimozione dei messaggi di errore delle applicazioni dalle pagine inviate agli utenti
- Prevenzione della perdita di codice server

Ulteriori servizi per la protezione della rete:

- Acceleratore SSL
- Filtro IP/porta
- Proxy inverso
- Gestione di chiavi e failover
- Terminazione SSL e riesecuzione della crittografia verso i server Web

Funzionalità di protezione avanzata:

- Firewall XML
- Protezione FTP
- Protezione da attacchi di evasione di dati

Prestazioni e flessibilità di TMOS

Il nucleo funzionale di ASM è costituito da TMOS, un'architettura intelligente, modulare e scalabile che consente l'adattamento rapido ai problemi futuri delle aziende e la semplificazione delle attività di gestione. TMOS migliora tutte le funzioni eseguite su ASM, assicurando chiarezza, flessibilità e controllo e facilitando la protezione intelligente delle applicazioni Web.

- Elimina la necessità del compromesso tra efficienza operativa e protezione olistica
- Contribuisce alla riduzione del "box clutter"
- Consente una protezione solida ed economicamente conveniente
- Include criteri preconfigurati e testati per applicazioni standard quali Microsoft SharePoint, OWA, Oracle e SAP
- Offre un modello di protezione centralizzato e bidirezionale che si adatta al variare dei rischi
- Prevede un sistema di aggiornamento semplice per il presente e il futuro

Proxy applicazioni veloce di TMOS

TMOS consente di utilizzare BIG-IP come un proxy completo per il traffico in transito destinato ai o proveniente dai server del data center. Questa capacità permette a BIG-IP di "comprendere" il contenuto delle applicazioni e di prendere decisioni basate su regole complesse associate a un'applicazione specifica. È inoltre in grado di modificare in modo intelligente il contenuto in base alle esigenze per aumentare il grado di protezione e assolvere a compiti che avrebbero altrimenti richiesto una modifica dell'applicazione stessa.

Motore di ispezione universale

TMOS incorpora una nuova versione del motore di ispezione universale di F5 per un controllo senza precedenti sulla gestione in tempo reale del traffico applicativo all'interno della transazione o del flusso dell'applicazione. BIG-IP è il punto di controllo chiave che consente di risolvere diversi problemi della distribuzione di applicazioni alla velocità della rete.

Manipolazione dell'input e manomissione dei parametri

Il flusso delle applicazioni Web attuali cambia in base all'input degli utenti. Fino al momento in cui lascia il computer dell'utente, l'input può essere manomesso dall'utente stesso o da malware eventualmente presente sul client. Se l'input non viene convalidato prima dell'utilizzo, il flusso dell'applicazione può essere alterato in qualsiasi momento. ASM offre protezione da questo tipo di attacchi convalidando tutti i parametri accessibili e nascosti in base allo stato dell'utente e alle informazioni sul flusso dell'applicazione.

Controllo delle violazioni di accesso/deep linking (forceful browsing)

Benché le applicazioni Web siano disponibili al pubblico, non tutte le parti devono essere accessibili a tutti. Attacchi di esplorazione URL, ad esempio tramite la modifica del percorso e dei nomi di directory contenuti nell'URL, o l'apertura di aree private ai crawler (attacchi tramite Google), sono attacchi molto comuni contro l'architettura di un'applicazione. Gli utenti che conoscono bene l'applicazione possono spesso indovinare o scoprire dove puntare il proprio browser o anche modificare i diritti di accesso in chiaro contenuti in un cookie per ottenere l'accesso a percorsi vietati conosciuti.

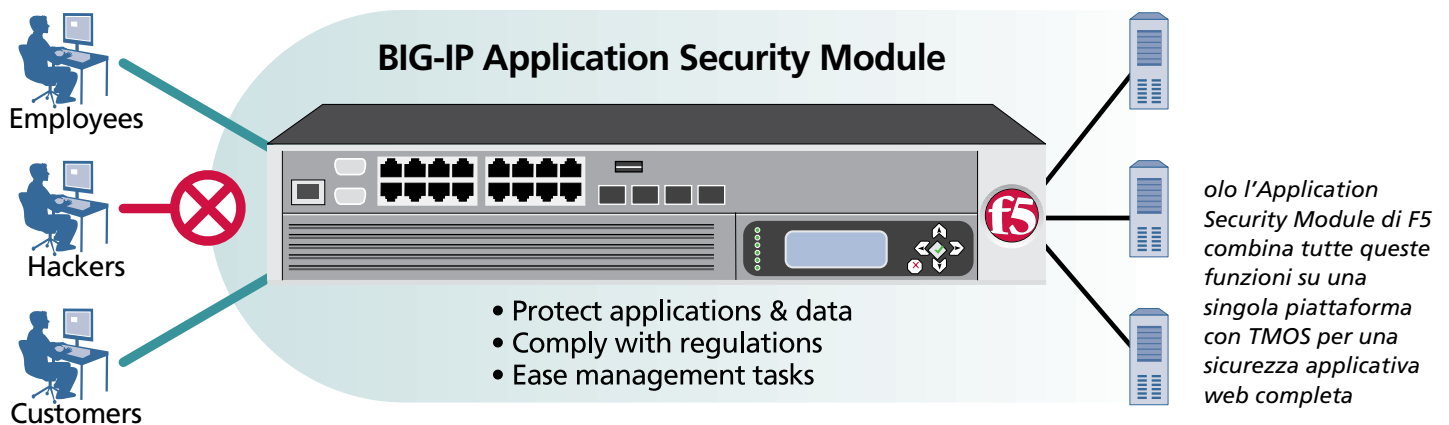
ASM offre protezione contro questo genere di violazioni grazie alla completa comprensione dell'interazione dell'utente con l'applicazione Web e alla solida consapevolezza dello stato e del contesto dell'utente durante una sessione.

Difesa in tempo reale

Avvalendosi di un modello di protezione positivo, ASM consente solo il traffico conosciuto e accettabile anziché limitarsi ad analizzare e bloccare gli attacchi contenenti firme note. I dispositivi che si affidano a un elenco di firme di attacchi conosciuti non possono offrire protezione contro gli attacchi mirati in cui un malintenzionato si adopera per cercare le vulnerabilità specifiche di una determinata applicazione. L'hardware dedicato e il software in attesa di brevetto di BIG-IP e Application Security Module rilevano e fronteggiano exploit sconosciuti in tempo reale, offrendo protezione accurata e complementare ai firewall e ai dispositivi IDS esistenti, che non sono in grado di arginare i rischi propagati tramite HTTP e HTTPS.

Cloaking/proxy inverso

ASM nasconde l'infrastruttura Web affinché i pirati informatici non possano scoprire quali server sono in esecuzione nella rete. Rimuove dalle intestazioni dei messaggi le informazioni che identificano il sistema operativo e il server Web (stringhe di versione, messaggi e firme), nasconde tutti i messaggi di errore HTTP agli utenti, rimuove i messaggi di errore dell'applicazione dalle pagine inviate agli utenti e controlla che il codice server e i commenti HTML privati non vengano inseriti nelle pagine Web pubbliche. Fungendo da proxy inverso, ASM offre accelerazione e terminazione SSL, riesecuzione della crittografia verso i server Web, gestione delle chiavi SSL, bilanciamento del carico e gestione del failover.



Ordering Information

Til modulo Application Security Module è disponibile sulle piattaforme BIG-IP 6400, 6800, 8400, and 8800, sia per una singola applicazione che per un numero illimitato di applicazioni con failover. Potete rivolgervi a F5 Italia per ulteriori informazioni.

* 6800 and 6400 platforms shown below.



Physical Specifications



BIG-IP 6800



BIG-IP 6400

Serie 8800

Processore: doppia CPU, dual core (4 processori)

Memoria base: 4 GB

ASIC: Packet Velocity ASIC 10

Porte Gigabit Ethernet in rame: 12 (in rame o fibra)

Porte 10-Gigabit in fibra: 2 (connettori ottici XFP)

TPS SSL include/TPS massime/crittografia di massa: 100/48.000/6 Gbps

Velocità traffico: 10 Gbps – L4; 8 Gbps – L7

Compressione hardware: 6 Gbps

Voltaggio di input:

90-240 VCA +/- 10%

90-132 9 A

180-264 4 A

Serie 8400

Processore: doppia CPU

Memoria base: 2 GB

ASIC: Packet Velocity ASIC 10

Porte Gigabit Ethernet in rame: 12 (in rame o fibra)

Porte 10-Gigabit in fibra: 2 (connettori ottici XFP)

TPS SSL include/TPS massime/crittografia di massa:

100/22.000/2,5 Gbps

Velocità traffico: 10 Gbps

Opzioni hardware disponibili:

Compressione hardware* (2 Gbps)

Elaborazione FIPS** (7.000 TPS e velocità SSL da 1,5 Gbps)

Voltaggio di input:

90-240 VCA +/- 10%

36-72 VCC (facoltativo)

90-132 9 A

180-264 4 A

Serie 6800

Processore: doppia CPU

Memoria base: 2 GB

ASIC: Packet Velocity ASIC 2

Porte Gigabit in rame: 16

Porte Gigabit in fibra (SFP-GBIC Mini): 4 (2 standard, 2 facoltative)

TPS SSL include/TPS massime/crittografia di massa: 100/20.000/2 Gbps

Velocità traffico: 4 Gbps

Opzioni hardware disponibili:

Compressione hardware* (2 Gbps)

Elaborazione FIPS** (7.000 TPS e velocità SSL da 1,5 Gbps)

Voltaggio di input:

90-240 VCA +/- 10%

90-132 9 A

180-264 4 A

Serie 6400

Processore: doppia CPU

Memoria base: 2 GB

ASIC: Packet Velocity ASIC 2

Porte Gigabit in rame: 16

Porte Gigabit in fibra (SFP-GBIC Mini): 4 (2 standard, 2 facoltative)

TPS SSL include/TPS massime/crittografia di massa: 100/15.000/2 Gbps

Velocità traffico: 2 Gbps

Opzioni hardware disponibili:

Compressione hardware* (2 Gbps)

Elaborazione FIPS** (7.000 TPS e velocità SSL da 1,5 Gbps)

Voltaggio di input:

90-240 VCA +/- 10%

36-72 VCC (facoltativo)

90-132 9 A

180-264 4 A



F5 Networks, Inc.
Sede centrale

401 Elliott Avenue West
Seattle, WA 98119
Telefono (206) 272-5555
Numero verde (888) 88BIGIP
Fax (206) 272-5556
www.f5.com
info@f5.com

F5 Networks
Asia Pacifico

Telefono +65-6533-6103
Fax +65-6533-6106
info.asia@f5.com

F5 Networks Ltd.
Europa/Medio Oriente/Africa

Telefono +44 (0) 1932 582 000
Fax +44 (0) 1932 582 001
emeainfo@f5.com

F5 Networks
Giappone

Telefono +81-3-5114-3200
Fax +81-3-5114-3201
info@f5networks.co.jp