

# BITDEFENDER SECURITY FOR ISA SERVERS

## GATEWAY-URILE DE INTERNET – PRIMA LINIE DE APĂRARE

Astăzi organizațiile asigură acces la Internet pentru majoritatea angajaților. Din acest punct de vedere, serviciile proxy online vă pot ajuta să administrați utilizarea lățimii de bandă în mod corespunzător și să consolidați traficul stocând date temporar pe serverul local. Accesarea Internetului pentru a găsi informații de orice natură crește exponențial traficul web și expune, în egală măsură, rețeaua dumneavoastră informatică posibilității de a contracta viruși. Tocmai din această cauză, companiile ce își instalează gateway-uri de Internet, precum Microsoft® Internet Security and Acceleration (ISA) Server întrevăd mari beneficii de pe urma unor timpi de răspuns reduși și funcției de bază a firewall-urilor ce asigură protecție în lupta cu virușii.

## GATEWAY-URILE DE ACCES LA INTERNET TREBUIE PROTEJATE !

Chiar dacă organizațiile ce implementează gateway-uri de acces la Internet beneficiază de pe urma nivelului suplimentar de protecție oferit de firewall-uri, protecția furnizată de acestea rămâne limitată, în mare parte din cauza regulilor statice ale firewall-ului și lipsei de vizibilitate a pachetelor ce trec prin gateway. Protecția împotriva codurilor periculoase ce pot penetra rețeaua informatică a unei companii prin intermediul aplicațiilor nemonitorizate sau din cauza lipsei unei inspecții riguroase la nivelul conținutului ce traversează rețeaua devine esențială. Ignorarea aspectului securității informatice poate avea consecințe grave precum pierderea de timp, bani, și resurse IT.

Serviciile online pot aduce cu sine diverse amenințări, inclusiv:

- Accesarea de site-uri web sau descărcarea unor fișiere infectate cu programe malware
- Descărcarea de atașamente mail infectate utilizând servicii de poștă electronică
- Descărcarea sau încărcarea de fișiere infectate utilizând fluxul FTP
- Infectarea prin intermediul unităților de rețea mapate

Gateway-urile sunt, de asemenea, un punct central de limitare a conținutului online ce vine dinspre exterior către organizație. Acestea pot ajuta companiile să implementeze politici de securitate privind fluxul de date din interior, dar și din interior către exteriorul organizației, reguli respectate și aplicate de către toți utilizatorii rețelei. Pentru a optimiza protecția și a mări durata de viață a serverelor ISA active, fără a le afecta nivelul de performanță și timpul de răspuns în momentul efectuării unor operațiuni critice pentru organizație, adoptarea unor măsuri suplimentare de securitate a datelor este strict necesară.

## ASIGURAȚI-VĂ GATEWAY-URILE DE INTERNET CU BITDEFENDER

BitDefender Security for ISA Servers permite organizațiilor să-și protejeze serverele de tip Microsoft® ISA prin blocarea anumitor pagini web, scanarea fișierelor descărcate și a atașamentelor e-mail primite de la anumite servicii de e-mail. Companiile își pot impune astfel politicile de securitate mai ușor în rândul angajaților. În același timp, acestea pot menține controlul asupra datelor confidențiale prevenind scurgerea informațiilor în exterior.



BitDefender Security for ISA Servers scanează traficul WEB și FTP din interiorul și către exteriorul companiei și aplică un set de reguli de scanare și filtrare ce pot fi configurate centralizat, cu ajutorul unui server.

## PRINCIPALELE CARACTERISTICI ȘI BENEFICII

- Tehnologie recunoscută și premiată internațional de detectare, trimitere în carantină și dezinfectare a virușilor.
- Reducerea perioadei în care rețeaua nu funcționează și creșterea eficienței operaționale
- Reducerea amenințărilor privind siguranța, a costurilor legate de administrarea și supravegherea rețelei IT și creșterea productivității
- Tehnologie ce reduce nivelul de solicitare a browser-ului online prin verificarea fișierelor de mari dimensiuni din aproape în aproape
- Filtrarea site-urilor web și a serverelor FTP pe bază de cuvinte cheie, cu ajutorul unor liste albe (obiecte legitime) sau negre (obiecte nelegitime) ușor de administrat
- Scanarea fluxului de fișiere pentru a se asigura o protecție antimalware în timp real și pentru reducerea riscului propagării virușilor în rețea
- Integritate în sistemul de reguli Firewall ale Microsoft și stocare în cache pe web prin intermediul ISAPI (Virus Scanning Interface) a Microsoft pentru optimizarea și accelerarea procesului de scanare
- Raportarea activității virușilor și realizarea unor statistici despre sesiunile de scanare și traficul de date online
- Posibilitatea de a configura o serie de acțiuni, precum alertarea utilizatorului prin intermediul poștei electronice, în funcție de specificul evenimentelor petrecute sau executarea altor acțiuni
- Posibilitatea de a susține implementările ISA Servers configurate ca un grup, destinate echilibrării fluxului de date
- Asigură configurarea de la distanță, de pe orice stație de lucru din organizație, prin intermediul consolei de management centralizat

## TEHNOLOGII BITDEFENDER:

**b-have** Toate produsele BitDefender conțin B-HAVE. Aceasta este o tehnologie în curs de brevetare ce analizează comportamentul codurilor potențial periculoase într-un mediu virtual. B-HAVE elimină răspunsurile fals pozitive și crește simțitor rata de detecție a programelor malware noi sau necunoscute.

## ACTUALIZĂRI AUTOMATE

BitDefender Security for ISA Servers asigură actualizări inteligente din oră în oră cu noile definiții ale virusilor. Astfel, BitDefender Security for<sup>®</sup> ISA Servers pentru Microsoft poate fi actualizat de la distanță în mod constant, protejând rețeaua dumneavoastră de cele mai recente amenințări informatice.

## PROTECȚIE RIGUROASĂ

BitDefender Security for ISA Servers este parte integrantă a unei game complete de soluții ce oferă protecție întregii dumneavoastră rețele informatice, de la nivel de gateway, până la stațiile de lucru. Tehnologia proactivă BitDefender, compatibilă cu un număr mare de sisteme de operare, detectează și oprește virusii, programele spyware, programele de tip adware și troienii ce pot amenința integritatea rețelei dumneavoastră informatice.

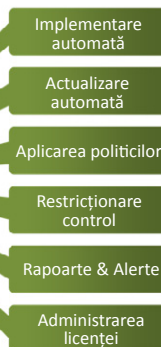
## CERINȚE DE SISTEM

- Windows Server 2003 + SP1, Windows Server 2003 R2
- Windows Server 2008, Windows Server 2008 R2
- Microsoft ISA Server 2000/2004/2006 Standard Edition
- Microsoft ISA Server 2004/2006 Enterprise Edition
- Internet Explorer 6.0 sau mai recent

### Protecție proactivă



### Management centralizat



BitDefender Security for ISA Servers oferă tehnologii premiate de detecție a virusilor și funcții de management și de raportare, pentru ca transferul de informații din interiorul organizației să se desfășoare în siguranță

## NIVELURI MULTIPLE DE SCANARE ȘI FILTRARE

Premiatele motoare de scanare BitDefender au fost recunoscute de organisme internaționale de certificare precum ICSA Labs, Virus Bulletin sau West Coast Labs pentru capacitatea lor de a oferi protecție împotriva programelor malware. Acestea furnizează multiple modalități de scanare și filtrare a conținutului, astfel că detectează codurile periculoase și protejează datele confidențiale;

**Trafic web (HTTP)** Motorul de scanare detectează virusii și alte programe periculoase în timp real, la accesarea unor site-uri web, a serviciilor de poștă electronică sau a altor aplicații online.

**Scanarea FTP Upload/Download** detectează virusii și programe malware în timp real, de fiecare dată când un utilizator descarcă sau încarcă fișiere folosind protocolul de transfer fișiere (FTP).

**Filtrarea de conținut** - Filtrarea de conținut permite detectarea informațiilor predefinite, cum ar fi informații despre cartea dumneavoastră de credit, numărul de cont, nume de rapoarte, bazele de date ale clienților etc. și împiedică scurgerea acestora în afara mediului organizațional. Filtrarea de conținut este flexibilă și se aplică în funcție de anumite adrese web și servere FTP cunoscute ca fiind nelegitime, cuvinte cheie sau mărirea conținutului.

**Listele Albe și Listele Negre** sunt folosite pentru blocarea paginilor web cu conținut neadecvat, pe baza cuvintelor cheie sau a stocării adreselor web cunoscute ca fiind sigure.

**Politicile de folosire** permit aplicarea de restricții flexibile la nivelul rețelei unei organizații, pe baza unor protocoale, a tipurilor de conținut accesat sau a adreselor IP.

## PROTECȚIE ATÂT ÎN INTERIORUL REȚELEI, CÂT ȘI ÎMPOTRIVA AMENINȚĂRILOR EXTERIOARE

- Tehnologie recunoscută și premiată internațional de detectare, trimitere în carantină și dezinfectare a virusilor.
- Integrare în sistemul de reguli Firewall ale Microsoft și stocare în cache pe web prin intermediul ISAPI (Virus Scanning Interface) Microsoft pentru optimizarea și accelerarea procesului de scanare
- Scanarea fișierelor și a conținutului web pentru o protecție în timp real, care să împiedice propagarea programelor periculoase în rețea
- Filtrarea site-urilor web și a serverelor FTP pe bază de cuvinte cheie, cu ajutorul unor liste albe (obiecte legitime) sau negre (obiecte nelegitime) ușor de administrat

## OPTIMIZARE, MANAGEMENT ȘI RAPORTARE

- Reduce volumul de muncă necesar administrării prin activarea funcției de management centralizat al notificărilor odată cu integrarea alertelor BitDefender în Modulul de alerte al Serverului ISA
- Permite implementările ISA Server cu configurare de tip array, destinate folosirii în mediile cu volume mari de trafic pentru echilibrarea fluxului de date din rețea
- Tehnologie de scanare și verificare a fișierelor de mari dimensiuni din aproape în aproape
- Raportarea activității virusilor și realizarea unor statistici despre sesiunile de scanare și traficul de date online
- Posibilitatea de a configura o serie de acțiuni, precum alertarea utilizatorului prin intermediul poștei electronice, în funcție de specificul evenimentelor petrecute sau executarea altor acțiuni