Solutii enterprise pentru securitatea retelelor

Adrian Dumitrescu

Q-East Software

adrian.dumitrescu@qeast.ro

Tehnologiile Dell pentru securitate fara limite

Dell Software: Leader in securitatea retelei, managementul identitatilor si controlul accesului

- Securitate Email
- Securitate Endpoint-uri
- Management de Identitati si Control Acces
- Securizarea Accesului la Distanta
- Gestiune Endpoint-uri
- Securitatea Retelei

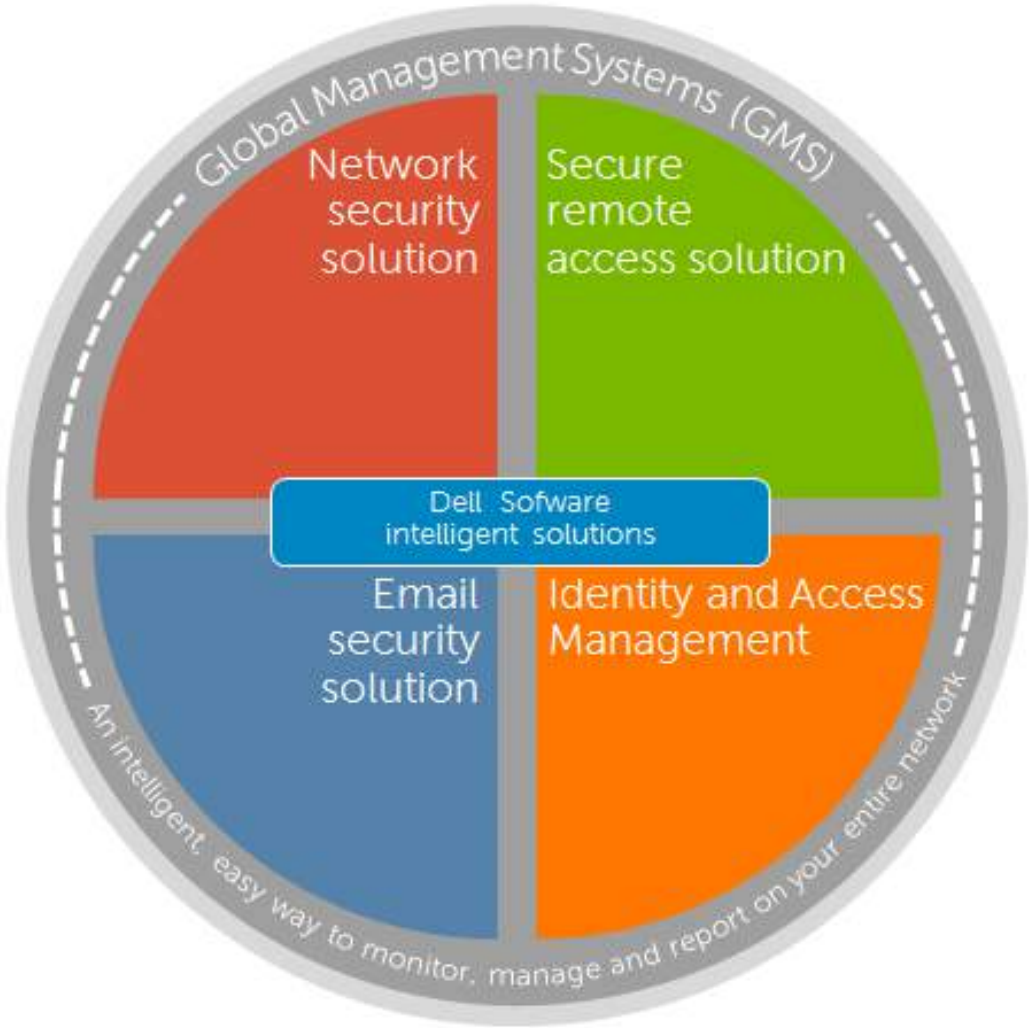
Dell Connected Security

Dell Software este ferm dedicata furnizarii de solutii IT end-to-end ce simplifica managementul organizatiilor IT. Aceasta include protectia continua a datelor, aplicatiilor, sistemelor si retelelor

Solutii de securitate pentru nevoile de business

- Inteligenta, controlul si vizualizarea aplicatiilor
- Clean VPN
- Implementari “clean wireless”
- Scenarii de disaster recovery
- Retele distribuite
- Securitate dinamica
- Solutii mobile
- Protectia retelei
- Access securizat la distanta
- Gestionarea unificata a amenintarilor
- VoIP
- Virtualizare

Solutiile de Securitate Dell SonicWall



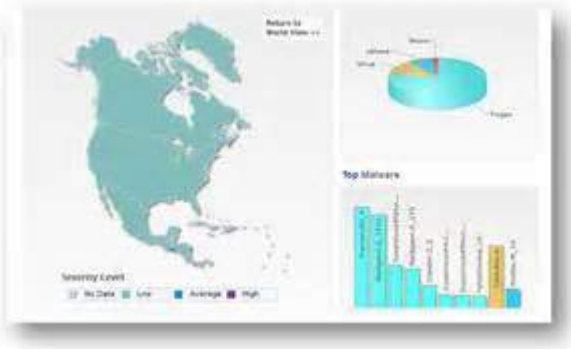
Q-EAST SOFTWARE
Smart Systems Management

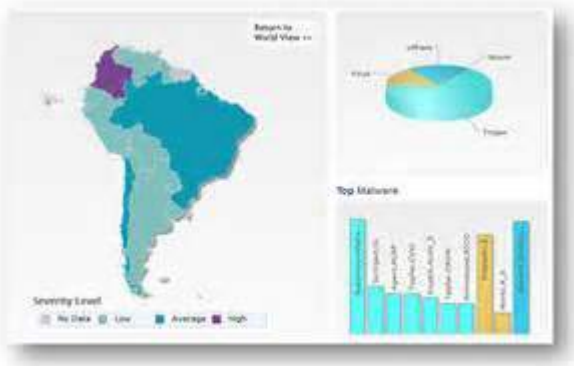
DELL Software

Solutii de securitate pentru nevoile de business

- ✓ Modul dedicat de accelerare WAN
  - ✓ *Reduce traficul inter-office cu pana la 95% prin capabilitati unice de caching la nivel de byte si de fisier*
- ✓ Modul de acces securizat la distanta
  - ✓ *Control granular al accesului SSL VPN si autentificare context-aware*
  - ✓ *Suport pentru Windows, iOS, McOS, Android si Kindle Fire*
- ✓ Solutie dedicata de securitate email
  - ✓ *Tehnici de analiza avansate si acces 24/7 la GRID*
  - ✓ *Ofera aditional criptare si conformitate email*
- ✓ Global Management System
  - ✓ *Dashboard universal si management centralizat*
  - ✓ *Raportare in timp real si istorica*
- ✓ Unelte dedicate de analiza avansata a retelei
  - ✓ *Analizor in timp real pentru traficul pe retea si utilizarea latimii de banda, cu support pentru solutii terte*
  - ✓ *Sistem de raportare avansata in timp real si istoric a activitatii de retea*

Inteligenta si controlul aplicatiilor prin Dell SonicWALL

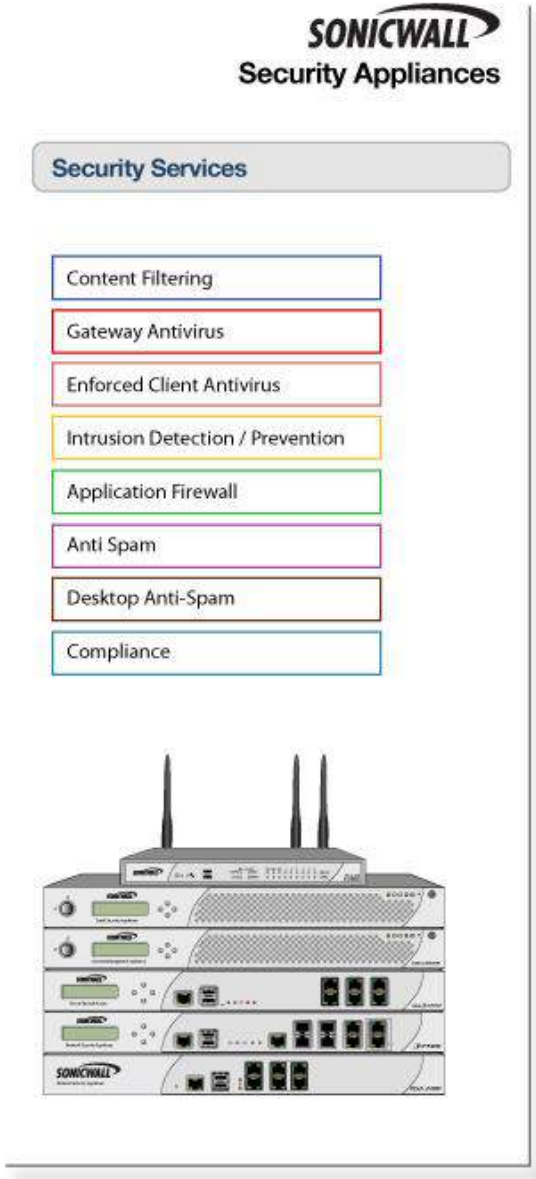




Este **un sistem** care receptioneaza date de la milioane de senzori partajati in reteaua Global Response Intelligent Defense (GRID), proceseaza aceste date si livreaza proactiv contramasuri si actualizari dinamice catre solutiile de securitate instalate la beneficiari.

SonicGRID

Participarea la reteaua globala de raspuns la amenintari



Q-EAST SOFTWARE
Smart Systems Management

DELL Software

SonicWALL in fapte...

- ✓ Peste 15 milioane de semnaturi in cloud
- ✓ Peste 2 milioane de senzori in intreaga lume (al doilea cel mai extins sistem global de reactie si raspuns)
- ✓ Semnaturile sunt generate chiar in momentul primirii unui cod suspect
- ✓ Detectie proactiva

pe baza semnaturilor existente

Q-EAST SOFTWARE
Smart Systems Management

DELL Software

SonicWALL NSA Network Security

12 Gbps Inspectie firewall
3 Gbps Inspectie DPI
4 Gbps Inspectie App/IPS
3 Gbps Inspectie malware

5 Gbps trafic VPN
500 interfete VLAN
96 SonicPoint-uri

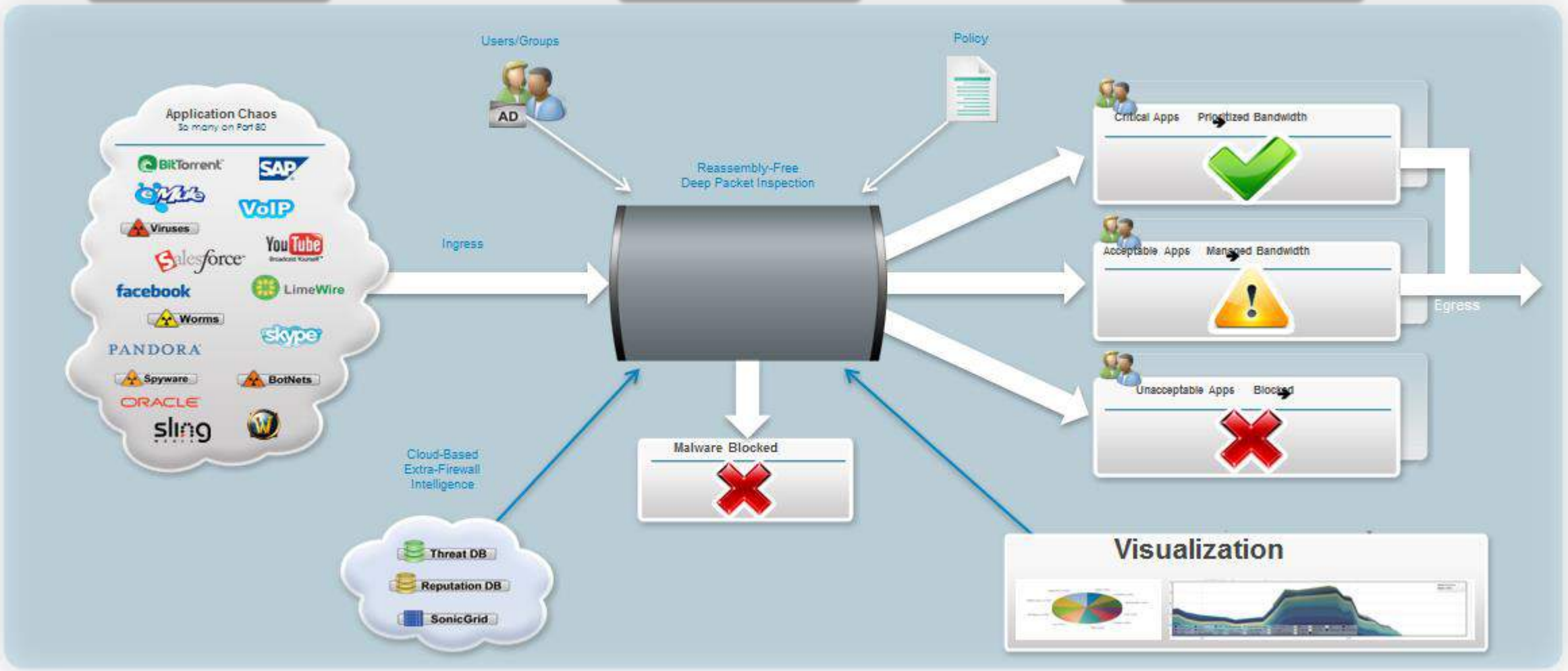
90.000 conexiuni / sec
750.000 conexiuni
4.000 utilizatori SSO
6.000 tunele VPN

Q-EAST SOFTWARE
Smart Systems Management

DELL Software

Propunerea SonicWall: Inteligenta si controlul aplicatiilor

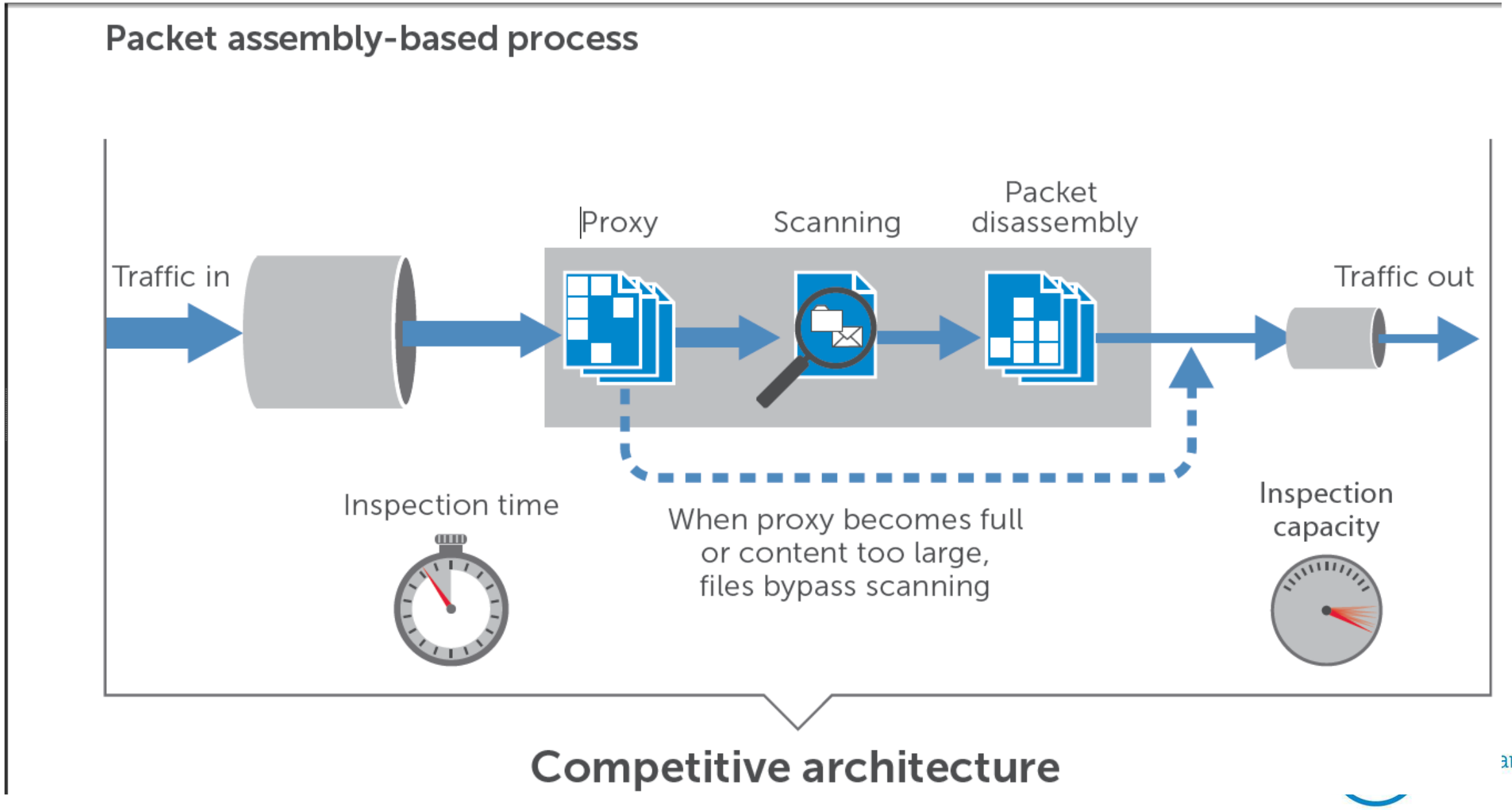
Identificare → Clasificare → Control



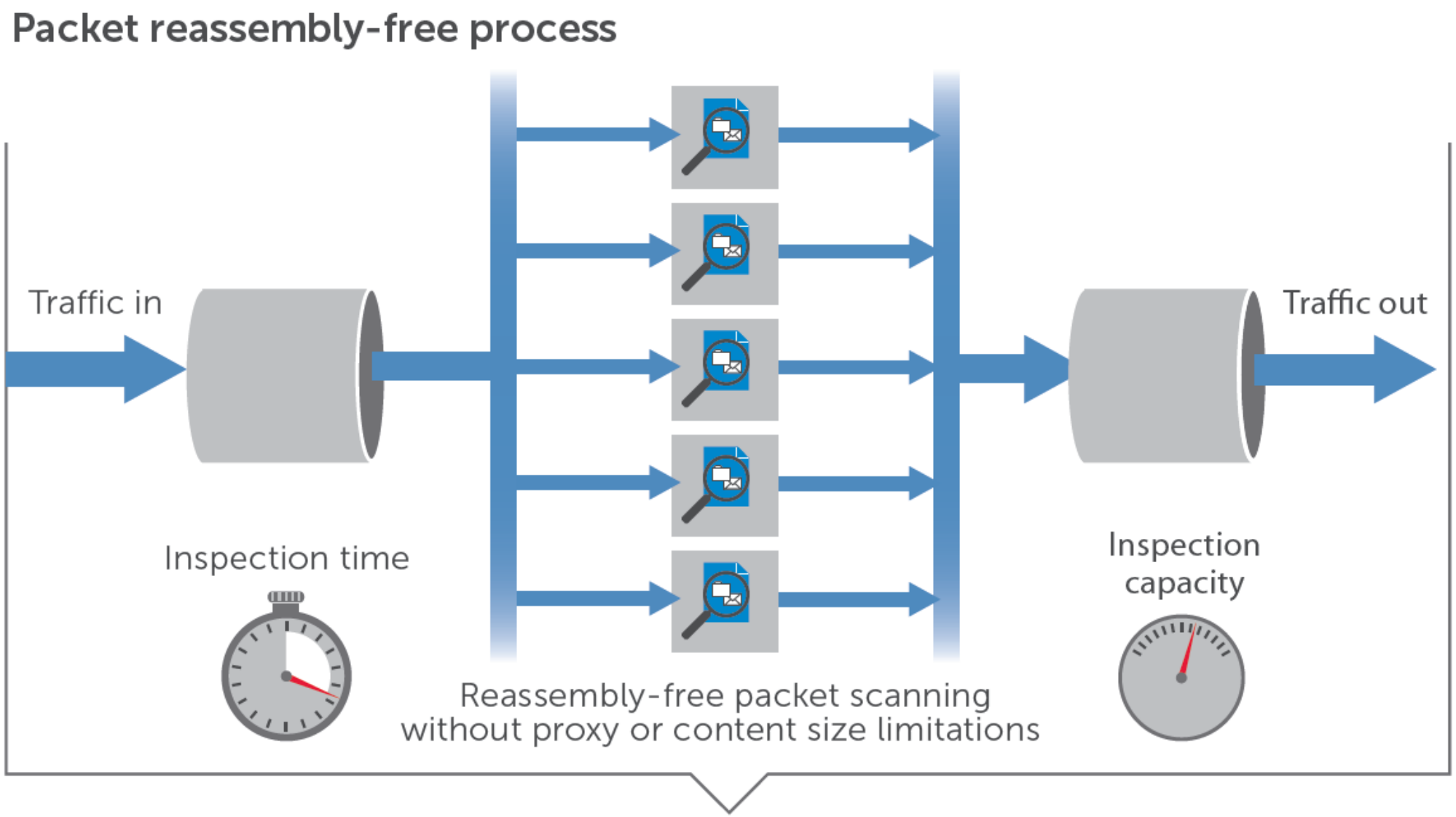
Q-EAST SOFTWARE
Smart Systems Management

DELL Software

Arhitectura clasica



Arhitectura scalabila



DELL Software

Capabilitati Next Generation Firewall

- ✓Stateful Packet Inspection
- ✓Secure Remote Access (VPN)
- ✓Access Control Rules
- ✓In-line, bump-in-the-wire
- ✓*Intrusion Prevention w/ Anti-Evasion*
- ✓*Anti-Malware*
- ✓*Application Intelligence*
- ✓*Integrates with Active Directory*
- ✓*SSL Decryption*

Q-EAST SOFTWARE
Smart Systems Management

DELL Software

SonicWALL NSA Network Security

Dual Band /
Dual Rado

Perimetru radio

Accelerare WAN

Standard 802.11 a/b/g/n
8 AP-uri virtuale
m-In / m-Out
SSL VPN

Wireless IDS
Wireless Guest
Autentificare Hotspot
Filtrare MAC

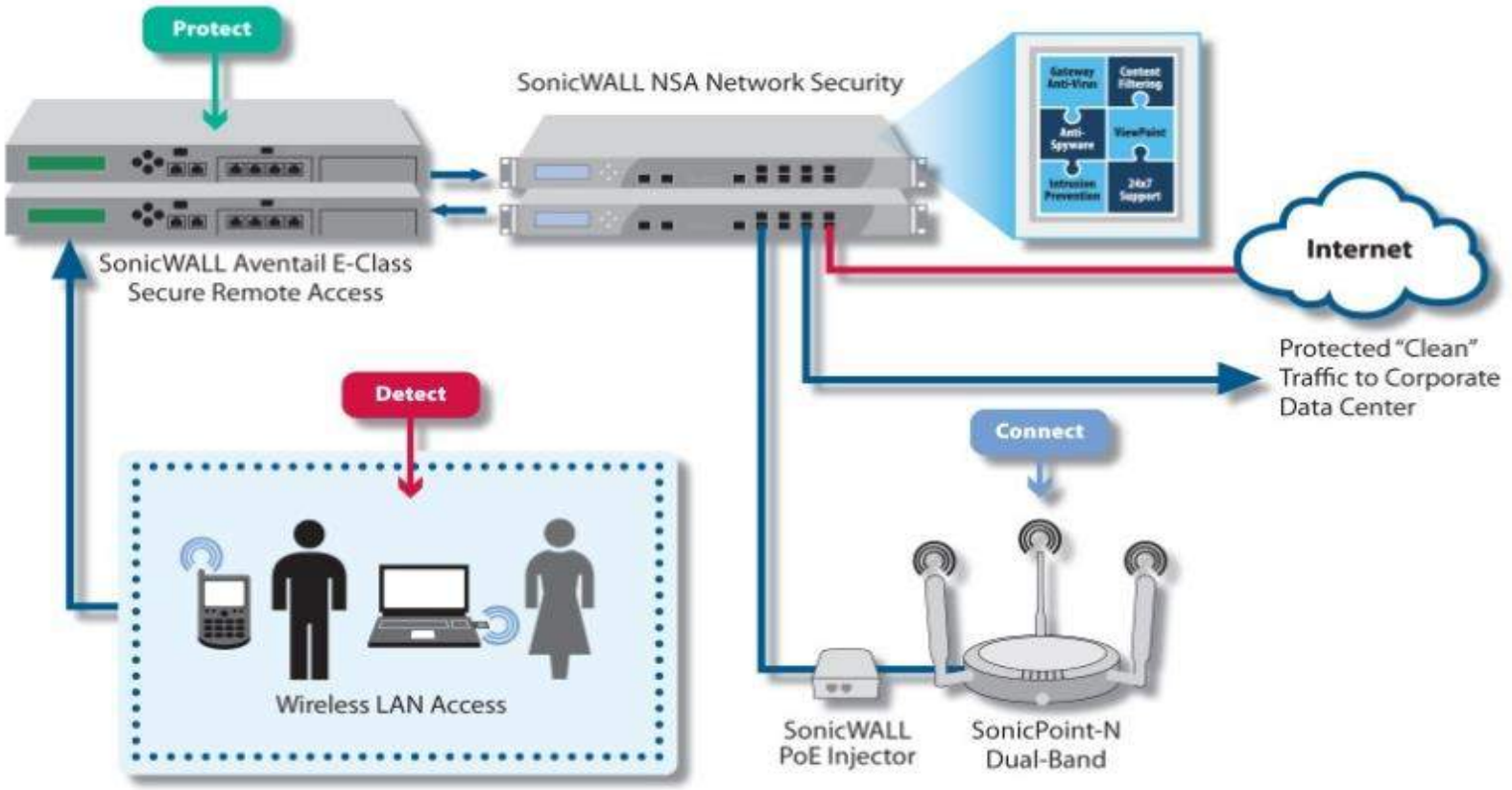
2.000 utilizatori
10.000 conexiuni
Byte caching
Accelerare WFS
Compresie date

Q-EAST SOFTWARE
Smart Systems Management

DELL Software

Arhitectura de securitate SonicWALL

Wireless, firewall de ultima generatie, acces securizat la distanta, toate avand in centru puternice capabilitati UTM



Detect **SonicWALL Aventail's Endpoint Control** continually detects the identity and security state of the end device

Protect **SonicWALL Aventail Unified Policy** enforces devices access control, ensuring users access only to authorized applications

Connect **SonicWALL Aventail Smart Access and Smart Tunneling** ensure easy, secure user access to all network resources

Comprehensive Gateway Security Suite includes gateway anti-virus, gateway anti-spyware, intrusion prevention, content filtering and 24x7 support.

Secure wireless zone with Reassembly-free Deep Packet Inspection scanning

Q-EAST SOFTV
Smart Systems Mana

10 Lucruri pe care un firewall ar trebui sa le faca

ZECE lucruri pe care un sistem de securitate ar trebui sa le faca

#1: Controlul aplicatiilor permise in retea

#2: Gestionarea latimii de banda pentru aplicatii critice

#3: Blocarea aplicatiilor peer-to-peer

#4: Blocarea componentelor neproductive ale aplicatiilor

#5: Vizualizarea traficului produs de aplicatii

#6: Gestionarea latimii de banda pentru un grup anume de utilizatori

#7: Blocarea virusilor la intrarea in retea

#8: Identificarea conexiunilor dupa tara

#9: Prevenirea scurgerilor de date prin email si web mail

#10: Gestionarea latimii de banda pentru streamingul audio si video

#1: Controlul aplicatiilor permise in retea

Vizualizarea aplicatiilor permite administratorilor sa determine ce versiuni de aplicatii sunt folosite inainte de a crea o politica de control

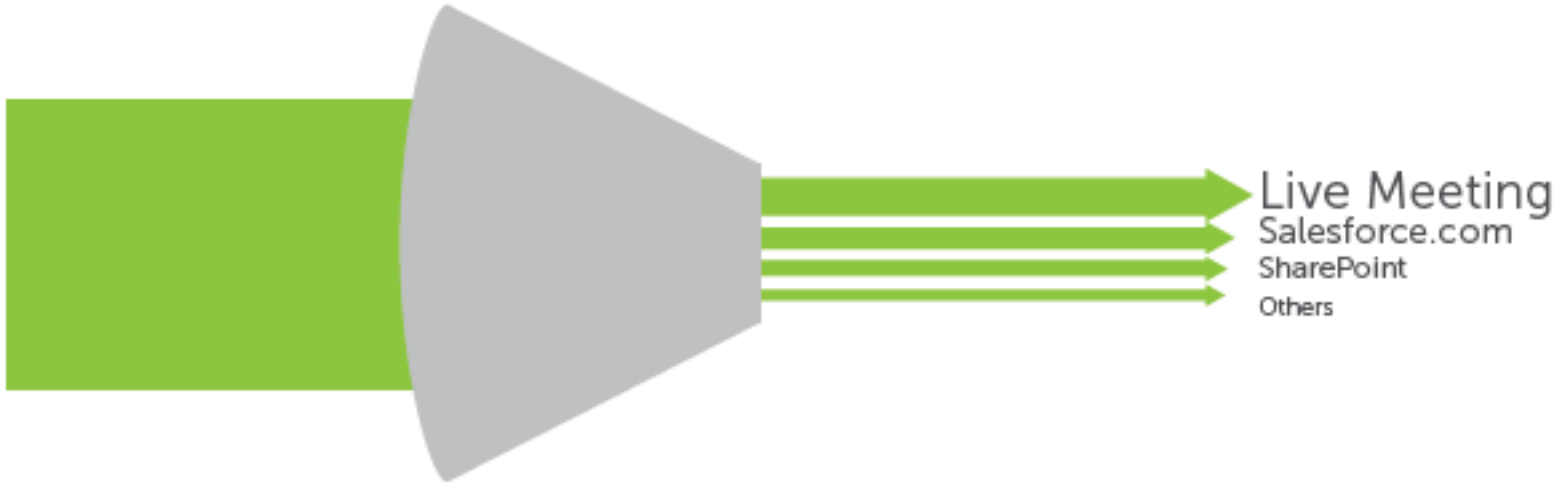
De exemplu, un utilizator care lanseaza IE6 sau IE7 va fi redirectionat automat catre pagina de download IE8

#2: Gestionarea latimii de banda pentru aplicatii critice

Prioritatea aplicatiilor poate fi bazata

pe timp, sau un alt criteriu impus de

business



De exemplu, aplicatiile contabile vor avea prioritate de acces
la inceputul si sfarsitul de trimestru

#3: Blocarea aplicatiilor peer-to-peer

Baza de date de semnaturi este actualizata permanent cu noi aplicatii si versiuni de aplicatii P2P

De exemplu, o noua versiune de BitTorrent va putea fi blocata automat, fara nici o interventie a administratorilor

#4: Blocarea componentelor neproductive ale aplicatiilor

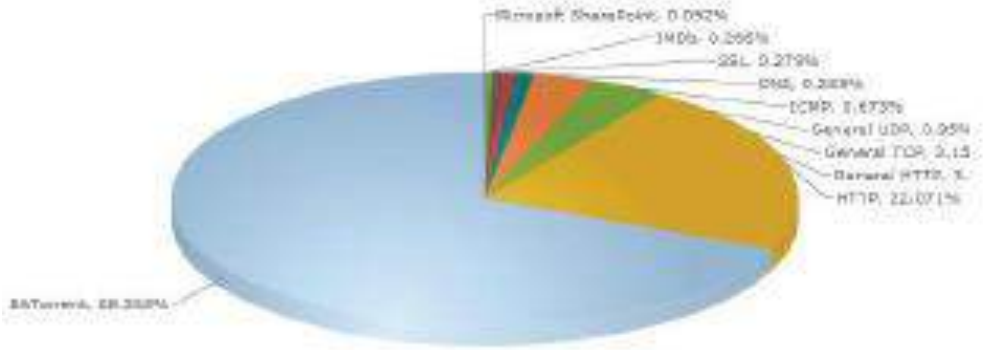
Devine astfel posibila controlarea modului cum sunt folosite aplicatiile web in folosul organizatiei, in locul interzicerii lor complete.

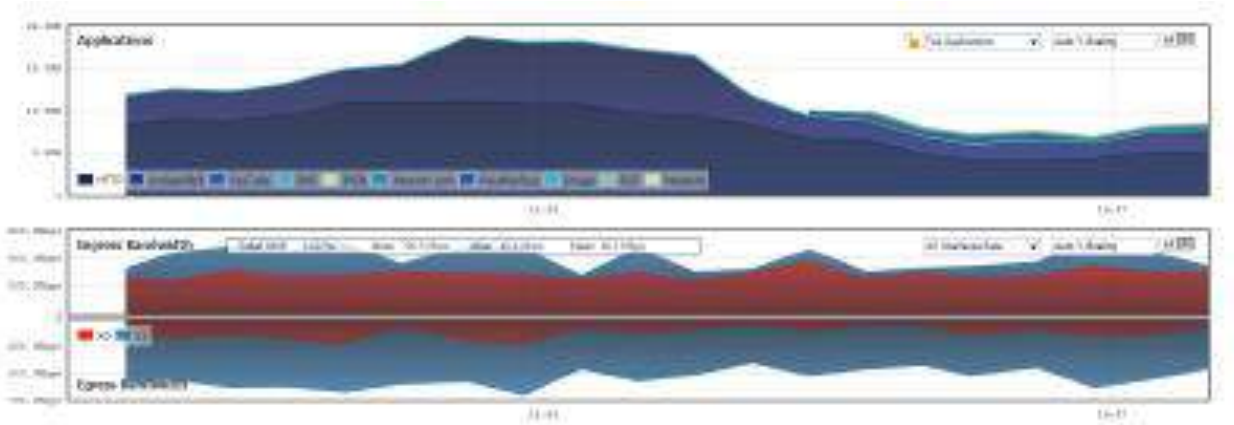
De exemplu, poate fi util accesul departamentului de Relatii Publice la Facebook, dar fara ca utilizatorii sa poata accesa jocurile.

#5: Vizualizarea traficului produs de aplicatii

Graficele representative furnizeaza administratorilor

raspuns instantaneu la fluxurile de traffic al retelei

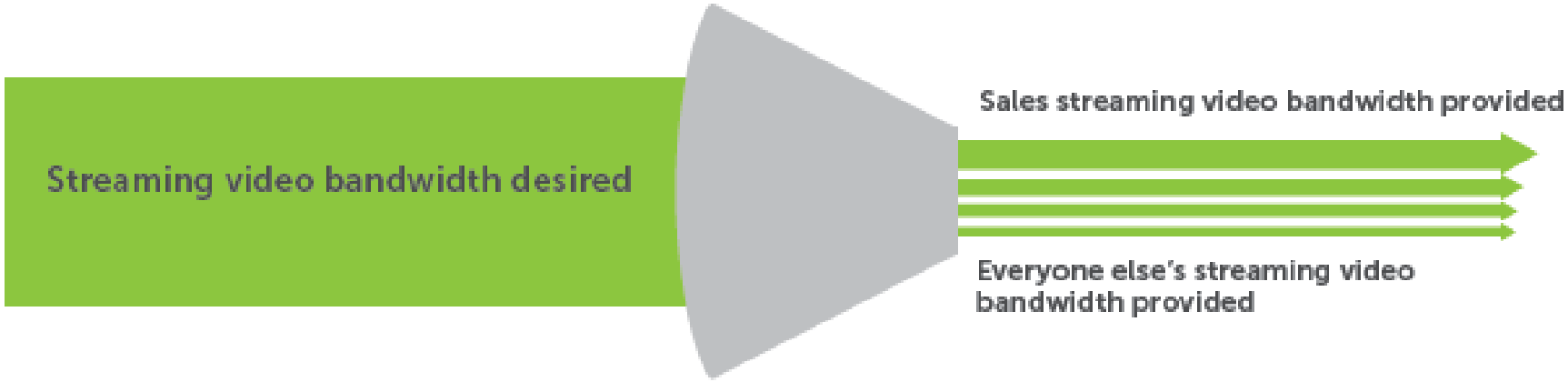




Se poate raspunde astfel la intrebari esentiale relative la sanatatea retelei: Ce se intampla in retea? Cine consuma latimea de banda? De ce este reteaua lenta? Etc.

#6: Gestionarea latimii de banda pentru un grup anume de utilizatori sau pentru un anumit tip de trafic

Multe organizatii au descoperit ca angajatii sunt mai fericiti daca sunt lasati sa aiba acces complet la web, chiar daca a fost redusa latimea de banda pentru site-urile neproductive



De exemplu, departamentul de media poate primi un procent mai mare din latimea de banda, pentru accesarea de continut video, insa numai pana la terminarea programului de lucru

#7: Blocarea virusilor la intrarea in retea

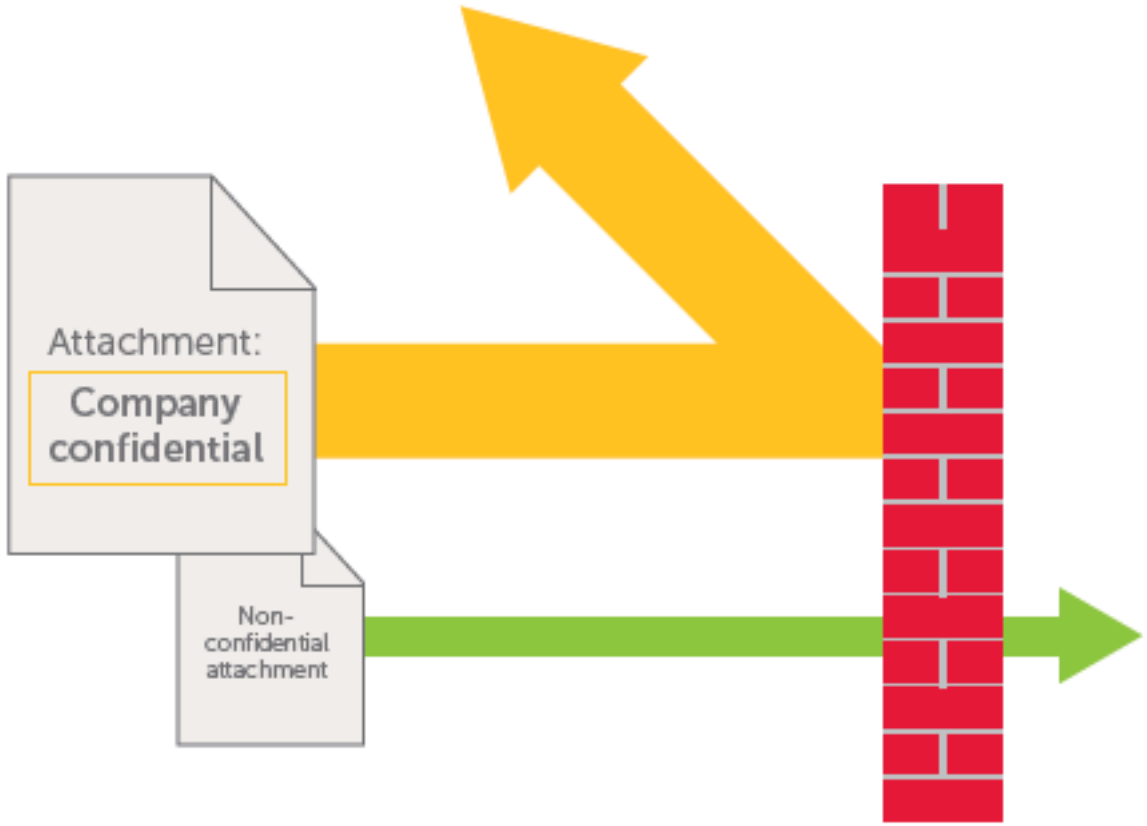
Blocarea virusilor, a spyware-ului si a altor tipuri de malware inainte sa ajunga in retea este critica pentru sanatatea si disponibilitatea componentelor din mediul informatic. Pot fi blocate milioane de amenintari inainte de a deveni un pericol pentru utilizatori, ori de a pune la incercare securitatea endpoint-urilor

#8: Identificarea conexiunilor dupa tara

Inteligenta aplicatiilor poate fi folosita drept o puternica unealta de investigatii pentru a identifica exact ce se intampla in retea, iar apoi modulul de captura a traficului va analiza exact natura conexiunii.

#9: Prevenirea scurgerilor de date prin mail

Este esential pentru orice organizatie sa existe un control asupra ce continut email poate fi trimis in exterior, de catre cine si catre ce destinatie.



De exemplu, pot fi setate politici ca numai personalul de vanzari sa poata trimite oferte, ori nimeni sa nu poata expedia documente marcate “confidential”

#10: Prevenirea scurgerilor de date prin web mail

Aditional controlarii “datelor in miscare” prin sistemul de mail, este necesar ca utilizatorii cu drept de utilizare a serviciilor de mail terte (Gmail, Yahoo etc.) sau FTP sa nu poata folosi aceste canale pentru expedierea de date confidentiale

Va multumim!

adrian.dumitrescu@qeast.ro
www.qeast.ro

livedemo.sonicwall.com
www.sonicwall.com