

PRAKTIČNI PRIMER (CASE STUDY)



Vzpostavitev redundančnega varnostnega sistema z varovanjem pred okužbami z virusi, nadzorom nad pretokom neprimernih vsebin in zaščito pred SPAM-om, neželjeno pošto na sejmu INTERINFOS 02.

Kazalo

Predgovor	3
Zaščita Internetnih prehodov (gateways)	4
Učinkovita varnostna rešitev	5
Uporaba tehnologije gruč (clustering) za izboljšanje zmogljivosti in dosegljivosti prehodov	5
Gruča protivirusnih rešitev v praksi	6
Vektorska namestitev	6
Namestitev kot Gateway/Proxy	7
Namestitev s razdeljenim pregledovanjem ("Split Gateway")	8
Trend Micro InterScan VirusWall	9
Stonesoft Stonebeat Cluster za Trend Micro InterScan	10
Prednosti	12

Predgovor

V okviru letošnjega sejma INTERINFOS 02 smo sodelovali kot sponzor za varovanje podatkov in kot distributerska hiša varnostnih rešitev in partner podjetij Trend Micro Inc. in Stonesoft Inc., vzpostavili sistem varovanja podatkov.

Danes se sicer veliko organizacij že poskuša zaščiti pred virusi, trojanskimi konji, črvi in drugo škodljivo programsko kodo, vseeno pa vsak dan prihaja do številnih okužb, ki lahko povzročijo ogromno škodo, saj zaščita marsikje ni popolna. Organizacije velikokrat namestijo protivirusno zaščito le na namizne računalnike, kar pa ni dovolj. Podobno situacijo bi dobili, če bi v hiši zaklenili vsa vrata, okna in druga možna vstopna mesta pa bi pustili odprta.

Trend Micro, ki danes ščiti več kot 60% Internetnih prehodov (*gateways*) na svetu, je zaznal potrebo po skalabilni protivirusni rešitvi z veliko dosegljivostjo in je zato pričel sodelovati s podjetjem Stonesoft. Stonesoft je na podlagi svoje zelo uspešne tehnologije gruč (*clustering*), ki jo uporablja v izdelku StoneBeat FullCluster, izdelal StoneBeat SecurityCluster, ki nudi tehnologijo gruč za protivirusne in podobne varnostne rešitve, kot je Trend Micro InterScan VirusWall.

StoneBeat SecurityCluster in Trend Micro InterScan VirusWall skupaj nudita veliko dosegljivo, skalabilno in visoko zmogljivo rešitev za protivirusno pregledovanje in zaščito pred neustreznimi in nezaželenimi internetnimi vsebinami. Ti preizkušeni in tudi že nagrajeni tehnologiji lahko zadovoljita tudi najbolj zahtevna okolja.

Zaščita Internetnih prehodov (*gateways*)

Nekateri virusi, kot je recimo "Love Letter", se lahko razširijo po celem svetu v manj kot eni uri in takrat je čas, ki je potreben za posodobitev protivirusne zaščite na vseh namiznih računalnikih predlog. Tako lahko kljub zaščiti pride do okužbe, ki lahko povzroči veliko škodo. To slabost pa lahko odpravimo z zaščito Internetnih prehodov in prehodov za elektronsko pošto (*Internet and e-mail gateways*), ki se lahko posodobijo v nekaj minutah.

Ker pa prehodi (*gateways*) ponavadi izvajajo poslovno pomembne funkcije, imajo upravitelji sistemov večkrat pomisleke glede implementacije takšnih rešitev. Pred vsem jih skrbi:

- **Stabilnost**

Ali bo protivirusna rešitev delovala brezhibno z ostalo strojno in programsko opremo, požarnimi zidovi in drugimi omrežnimi sistemi?

- **Dosegljivost**

Kako bo protivirusna rešitev vplivala na skalabilnost, vzdrževanje in dosegljivost glavnih funkcij prehoda?

- **Zmogljivost**

Ali bo protivirusna rešitev vplivala na zmogljivost prehoda?

- **Skalabilnost**

Ali bo protivirusna rešitev lahko rasla skupaj s potrebami podjetja? Ali bo to možno izvajati brez prekinitev pomembnih storitev?

Nekatere organizacij lahko te skrbi odpravijo že z manjšimi investicijami, kot so dokup pomnilnika, spremembe nastavitev in podobno, nekatere pa lahko to naredijo s postavitvijo protivirusnih sistemov kot proxy. Veliko pa je takšnih, ki za zadovoljitev svojih trenutnih in bodočih poslovnih zahtev potrebujejo naprednejše rešitve.

Učinkovita varnostna rešitev

Resnično učinkovita rešitev za protivirusno zaščito Internetnega prehoda mora biti vedno aktivna, posodobljena in imeti polno zmogljivost brez prekinjanja drugih pomembnih storitev. "VirusWall" mora biti stabilen in delovati transparentno.

Mrežne aplikacije in storitve morajo v današnjih organizacijah biti vedno na voljo in čeprav današnje najboljše protivirusne rešitve podpirajo to potrebo z visoko zmogljivostjo, skalabilnostjo in preprostim upravljanjem, se lahko kmalu zgodi, da bodo tudi te zaradi kompleksnosti in rasti omrežij kmalu nezadovoljive.

Uporaba tehnologije gruč (*clustering*) za izboljšanje zmogljivosti in dosegljivosti prehodov

Dosegljivost, skalabilnost in preprostost upravljanje, ki jo lahko dosežemo z enim varnostnim prehodom ni neskončna. Tudi z nadgradnjo strojne opreme pridemo do točke, ko je prekinjanje pomembnih storitev na prehodu neizogibno. Zato je nujna uporaba tehnologije gruč, s katero ustvarimo t.i. "VirusWall Cluster".

1. VirusWall Cluster z uporabo odvečnosti (*redundancy*) nudi zavidljivo visoko kvaliteto in veliko dosegljivost storitev in sicer z odstranitvijo ene-točke-odpovedi (*single-point-of-failure*). Z uporabo tehnologije StoneSoft StoneBeat pa nudi tudi pravo dinamično razporejanje bremena med računalniki v gruči in s tem optimizirano uporabo računalniških sredstev.

2. Rešitev VirusWall Cluster je skalabilna - nudi preprosto in transparentno možnost dodajanja strežnikov v gručo in s tem izpolnitev potreb rastočih organizacij ali nenadnega povečanja prometa.

3. Rešitve, ki uporabljajo tehnologijo gruč, so zelo ekonomične, saj omogočajo, da upravitelji sistema povečajo zmogljivost sistema kar z običajnimi PC računalniki, namesto z velikimi investicijami v drage in ozko specializirane sisteme.

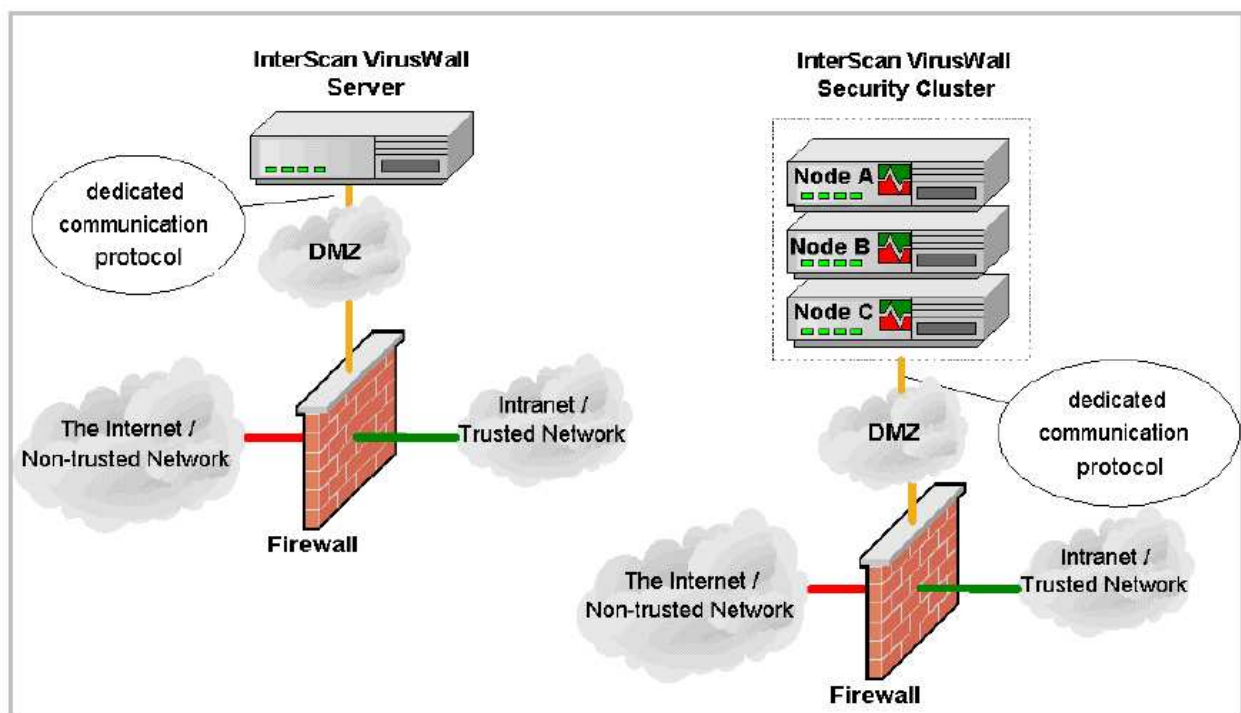
Pomembno pa si je zapomniti, da splošne rešitve za uporabo tehnologije gruč z izboljšanjem dosegljivosti ustvarijo tudi nove težave. Zato je pomembno, da za ta namen izberemo takšno rešitev, ki je namenjena nadzoru vsebin. StoneSoft SecurityCluster je za ta namen edina skalabilna rešitev z veliko dosegljivostjo.

Gruča protivirusnih rešitev v praksi

V praksi srečamo 3 različne pristope k postavitvi protivirusne gruče: vektorska namestitev, "Gateway/Proxy" namestitev in "Split Gateway" namestitev.

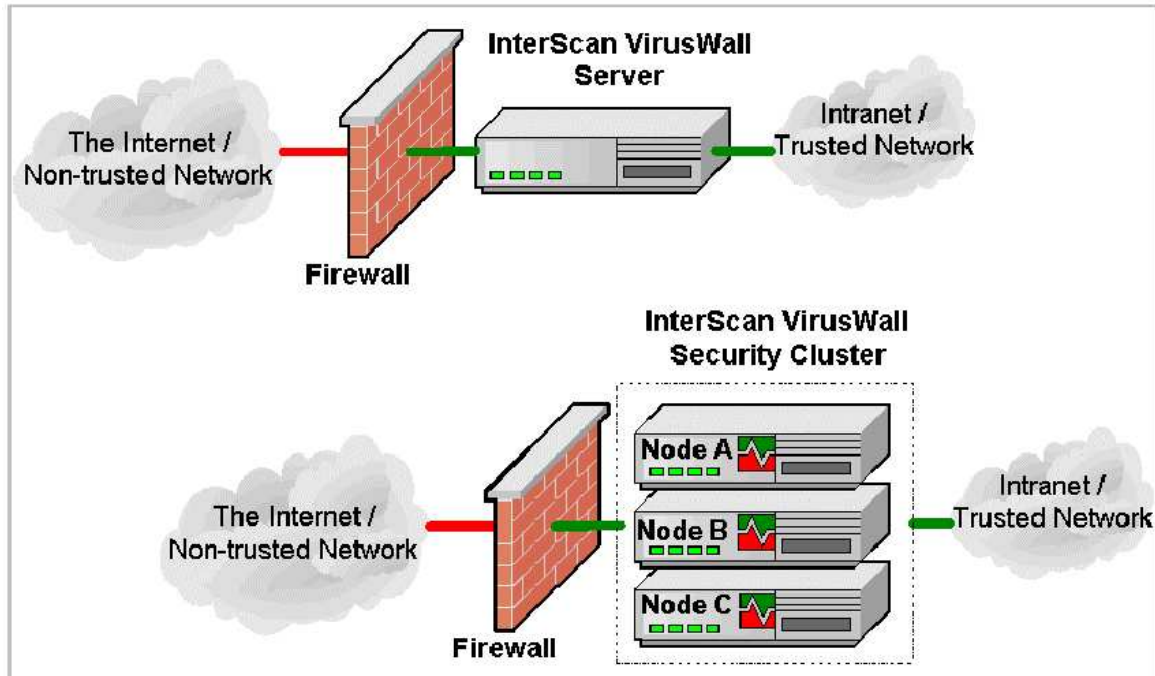
Vektorska namestitev

V tipični vektorski namestitvi postavimo strežnik(e) s protivirusno zaščito v DMZ, takoj za požarni zid. V tej namestitvi požarni zid pošlje vso sumljivo vsebino in programsko kodo na pregled k temu strežniku, ta pa jo po pregledu pošlje dalje. Za komunikacijo med požarnim zidom in pregledovalnim strežnikom potrebujemo poseben komunikacijski protokol.



Namestitev kot Gateway/Proxy

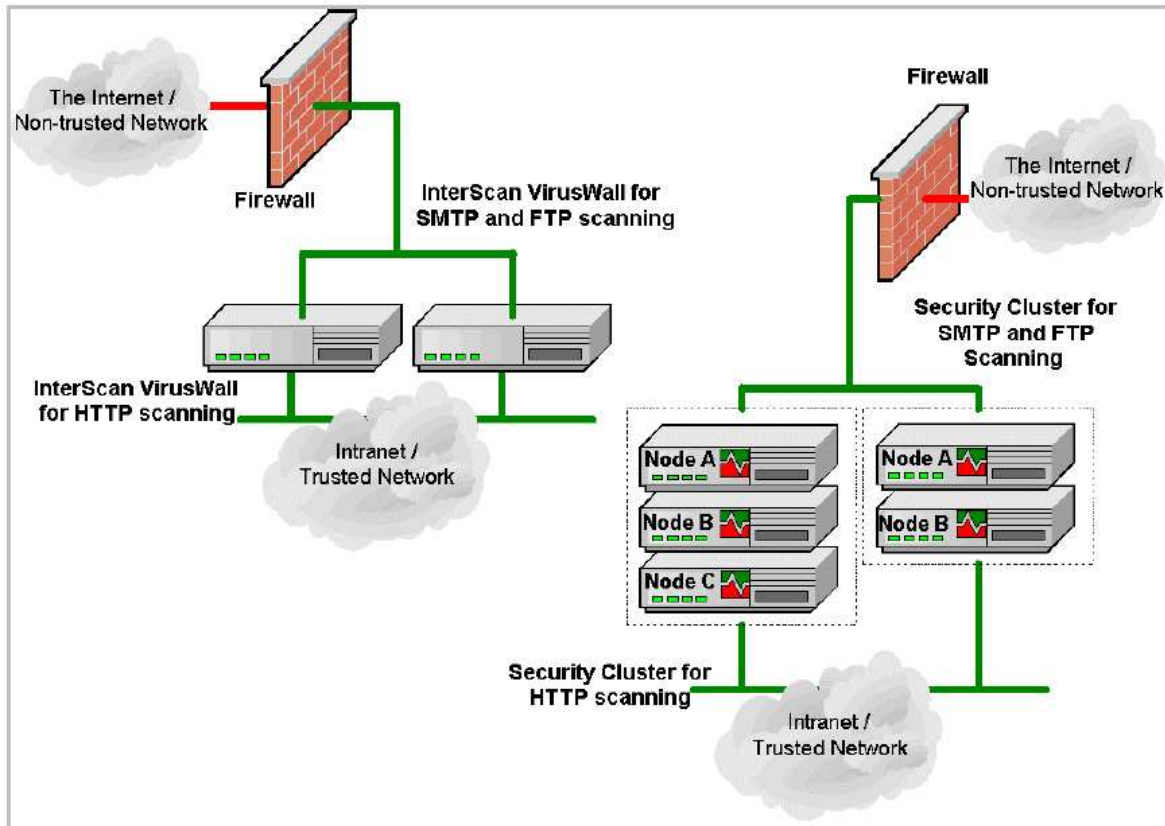
V topologiji te namestitve postavimo pregledovalni strežnik med požarni zid in lokalno omrežje. Ta postavitev je sicer preprosta, vendar ima v primeru samostojnega pregledovalnega strežnika (brez gruč) kar nekaj slabosti. Protivirusno pregledovalni proces zelo obremeni procesor in zato lahko samostojen protivirusni strežnik močno upočasni ves omrežni promet. V primeru izpada takšnega strežnika, pa bo brez povezave ostalo celotno omrežje.



Z uporabo StoneBeat SecurityClusterja pa ta postavitev ni več problematična, saj odpravi enotočko-odpovedi in težavo preobremenjenosti procesorja. Pravzaprav postane ta namestitev zelo privlačna, saj ne potrebuje dodatnih protokolov za komunikacijo med požarnim zidom in protivirusnim strežnikom.

Namestitev s razdeljenim pregledovanjem ("Split Gateway")

Velike organizacije z zelo intenzivnim omrežnim prometom pogosto razdelijo opravila oziroma naloge varnostnih strežnikov. Na primer, za pregledovanje SMTP in FTP prometa zadolžimo enega, za HTTP promet pa drug strežnik. Takšna postavitev lahko izboljša zmogljivost in do neke mere tudi dosegljivost sistema (če izpade strežnik za HTTP pregledovanje, SMTP in FTP promet še vedno delujeta). Za pravo veliko dosegljivost in boljšo zmogljivost in varnost pa moramo tudi v tej namestitvi uporabiti tehnologijo gruč.



Trend Micro InterScan VirusWall

Trend Micro InterScan VirusWall je strežniški izdelek, ki združuje upravljanje pretoka podatkov in protivirusno zaščito na internetnem prehodu. Sestavljen je iz dveh delov: VirusWall (protivirusno pregledovanje SMTP, FTP in HTTP prometa) in opsijski dodatek eManager, ki skrbi za zaščito pred neustreznimi in nezaželenimi vsebinami v elektronskih sporočilih ter upravlja njihovo dostavljanje.

InterScan VirusWall skrbi za odkrivanje in odstranjevanje virusov in druge škodljive programske kode v Internetnem prometu (SMTP, FTP in HTTP). Za pregledovanje uporablja lastno, zelo hitro tehnologijo proxy in je tako lahko neodvisen od požarnega zidu. Za optimizacijo zmogljivosti InterScan VirusWall inteligentno pregleduje le tisti promet, ki bi lahko prenašal škodljivo programsko kodo.

InterScan eManager je orodje, ki upraviteljem sistemov omogoča ustavljanje elektronskih sporočil z neustrezno in nezaželeno vsebino ter upravljanje dostave velikih elektronskih sporočil. eManager je sestavljen iz filtra za nezaželeno elektronsko pošto (*spam*), filtra za vsebino in upravitelja elektronske pošte.

InterScan VirusWall je bil načrtovan posebej za okolja z veliko količino prometa in je stabilna varnostna rešitev z minimalnim vplivom na zmogljivost sistema. S transparentnim ustavljanjem virusov in druge škodljive programske kode, kot tudi z razporejanjem bremena storitev za optimizacijo omrežja in okolja elektronske pošte, je to rešitev, ki bo sigurno povečala produktivno organizacije.

Stonesoft StoneBeat Cluster za Trend Micro InterScan

StoneBeat SecurityCluster - *The Scalable High Availability Solution for Security Servers* je programska rešitev, ki je bila razvita za izgradnjo vedno dostopnih sistemov varnostnih strežnikov. Zgrajena je na enaki, preverjeni tehnologiji gruč kot StoneBeat FullCluster for FireWall-1.

Celotna SecurityCluster gruča je, ne glede na število posameznih strežnikov v njej, na zunaj vidna kot en sam, visoko zmogljiv strežnik, ki je vedno dosegljiv.

Promet vedno najprej prispe do vseh strežnikov v gruči z uporabo multicasta, vendar bo pakete obdelal le en strežnik, saj bo filter za porazdeljevanje bremena drugim strežnikom povedal, da naj te pakete preprosto ignorirajo. S to metodologijo dosežemo maksimalno propustnost, saj bi bilo usmerjanje paketov k posameznim strežnikom v gruči dosti bolj zamudno opravilo.

Popolna transparentnost

Ni potrebe po spreminjanju drugih omrežnih komponent, saj lahko gruča prevzame že obstoječi IP in MAC naslov. Prav tako so vse nastavitve gruče, kot je dodajanje ali odstranjevanje strežnika, popolnoma nevidne za druge omrežne komponente in uporabnike. Enako velja za razporejanje bremena in preklon na drug strežnik v primeru napake (*fail-over*).

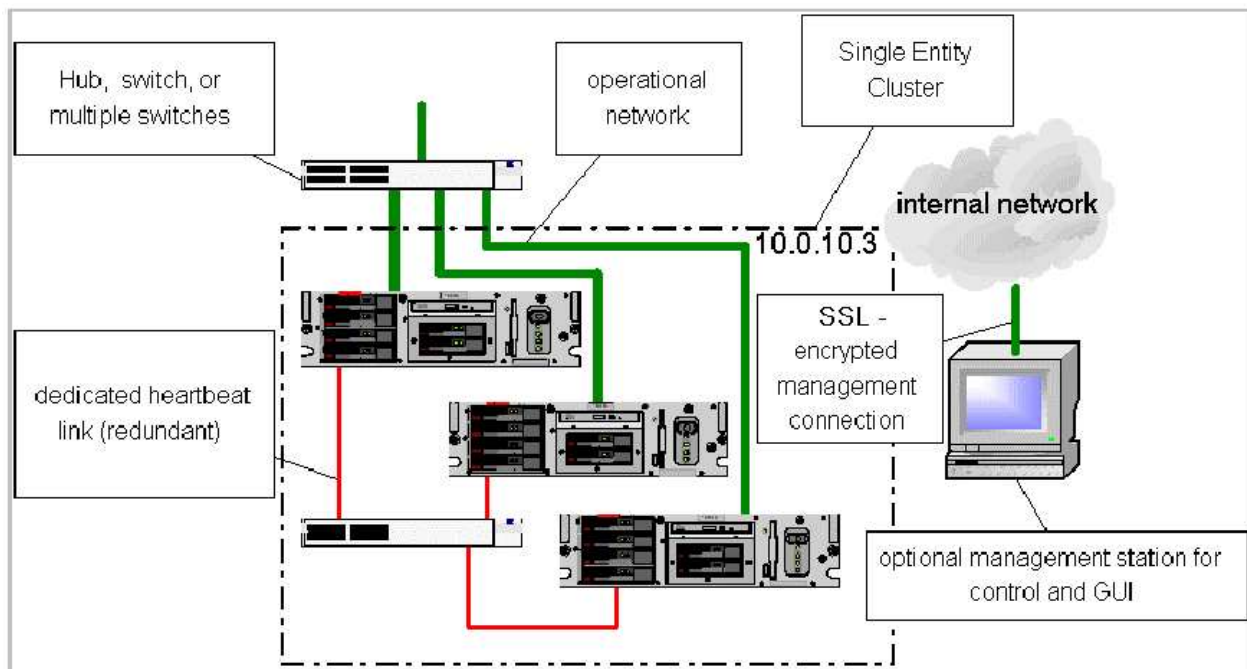
Preprosto upravljanje

Vzdrževanje programske in strojne opreme z posodabljanjem in nadgrajevanjem v delovnem času je rutinsko opravilo. Z vzdrževanjem popolne transparentnosti, lahko za posodabljanje, nadgradnjo ali testiranje iz gruče izklopimo enega ali več strežnikov in jih nato tudi brez težav vrnemo v gručo.

Vsa ta opravila lahko v StoneBeat SecurityCluster izvedemo preko grafičnega uporabniškega vmesnika, ki temelji na Javi ali pa s pisanjem ukazov v ukazno vrstico. Nadzorovan izklop strežnika poskrbi za prenos vseh njegovih transakcij k drugem strežniku pred izklopom.

Napredno odkrivanje napak

Uspešno upravljanje z viri temelji na sistemu povratne informacije zato je zmožnost pravočasnega odkritja programske ali strojne napake ključnega pomena. Tehnologija gruč SoneBeat uporablja stalno notranje opazovanje virov in tako natančno informacijo o dosegljivosti vsakega strežnika v gruči. Alternativno opazovanje od zunaj, ki ga uporablja večina ostalih rešitev, je manj učinkovito, saj je omejeno le na opazovanje odzivov strežnika v gruči na določen vhod.



Prednosti rešitve

StoneBeat SecurityCluster zagotavlja neprekinjeno dosegljivost Trend Micro InterScan VirusWall protivirusnih strežnikov. Tako lahko izrabimo vse prednosti centralizirane protivirusne zaščite na Internetnem prehodu s produktom InterScan VirusWall in brez težav z dosegljivostjo sistema.

Z rešitvijo StoneBeat SecurityCluster zagotovimo, da protivirusni pregledovanje z InterScan VirusWall ne bo nikoli ozko grlo našega omrežja. Dinamično razporejanje bremena z upoštevanjem kapacitete, zasedenosti in količine prostega pomnilnika porazdeli pregledovanje vsebine na vse strežnike v varnostni gruči VirusWall. Tako z razpoložljivimi sredstvi dosežemo maksimalno propustnost.

InterScan VirusWall in StoneBeat SecurityCluster nudita skalabilno protivirusno rešitev, ki za namestitev ne zahteva spreminjanja trenutno topologije omrežja. Prav tako lahko nove pregledovalne strežnike po potrebi brez težav dodajamo v gručo.

S StoneBeat SecurityCluster okrepljena protivirusna zaščita z izdelkom Trend Micro InterScan VirusWall, bo s centraliziranim upravljanjem, avtomatizacijo rutinskih opravil in arhitekturo za veliko dosegljivost močno izboljšala varnost in zmogljivost sistema ter olajšala upravljanje omrežja.