

McAfee Desktop Firewall 8.0

Proaktiv beskyttelse og styring af netværksklienter

følge ISCA-laboratorierne er der over 200 nye alvorlige trusler hver måned, som skal lægges til de mere end 72.500 trusler, vi kender i dag. Ud over de "traditionelle" virustrusler ser vi nu et stigende antal orm på internettet, udsendelser af masse-mails, angreb, der blokerer for adgang til tjenester, trojanske heste, trojanske heste med fjernadgang, zombier, hackere og sårbarheder i operativsystemerne. Disse trusler er ikke blot potentielt mere destruktive, de spredes også hurtigere. Mens det tidligere tog uger eller måneder at sprede en computervirus, kan eksempelvis SQLSlammer udnytte virksomhedernes netværk og internettet og opnå global udbredelse på minutter.

Integreret klientsikkerhed

Lavere ejeromkostninger

McAfee® Desktop Firewall™ og McAfee VirusScan™ Enterprise og ePolicy Orchestrator™ kan integreres og yde virusbeskyttelse med global administration og rapportering. Den integrerede klientsikkerhed sikrer problemløs interoperabilitet, fuldstændig beskyttelse mod virus, hackere og ondsindede trusler, forhindrer datatyveri og reducerer ejeromkostningerne.

Firewall med filtrering af pakker

Stopper og dæmper op for nye trusler, som virusbeskyttelsen ikke klarer alene

McAfee Desktop Firewall er en firewall på pakkeniveau, der kan filtrere al ind- og udgående netværkstrafik. Desktop Firewall anvender regler defineret af administratoren og opbygger automatisk regler, der blokerer for eller tillader netværkstrafik. Vha. pakkefiltreringen kan Desktop Firewall forhindre, at klienterne bliver vært for et angreb eller modtager uautoriseret trafik, der kan være et fjendtligt angreb. Den kan f.eks. proaktivt forhindre spredning via netværket – en teknik, der blev benyttet af hovedparten af de største trusler i 2002. Desktop Firewall understøtter flere netværksprotokoller, herunder over 120 IP-baserede protokoller. Desuden kan administratoren oprette regler for ikke-IP-protokoller, herunder WiFi (802.11x), NetBEUI, IPX og AppleTalk. Mange protokolregler øger sikkerheden på netværket, fordi de kan filtrere et bredere spektrum af netværkstrafikken.

Firewall til programlaget

Kontrollerer programmer med adgang til netværket

McAfee Desktop Firewall er en firewall på programniveau, der kan filtrere alle programmer, der genererer netværkstrafik. Administratorerne kan forhindre misbrug og øge sikkerheden ved at kontrollere de porte og protokoller, der benyttes af programmer, der er tillid til.

Overvågning af programmer

Blokerer for uautoriserede programmer og sikrer et kontrolleret driftsmiljøet (COE – Common Operating Environment)

Desktop Firewall omfatter programovervågning, der gør det muligt at kontrollere og overvåge programmer ved at forhindre uautoriserede programmer i at køre eller koble sig på andre programmer. Programreglerne kan konfigureres manuelt eller opbygges automatisk og låses, så de ikke kan ændres. Regler for oprettelse af programmer forhindrer, at der køres uautoriserede programmer. Et eksempel herpå er, når legitimt software, f.eks. onlinemeddelelser, udgør en sikkerhedsrisiko, fordi det har adgang til netværket, og trusler som f.eks. trojanske heste, orm, trojanske heste med fjernadgang eller spyware-programmer, der medfører skader på systemet, nedgang i produktiviteten og tabt fortjeneste. Med programreglerne kan administratoren kontrollere driftsmiljøet og forhindre, at brugeren installerer eller kører software, der ikke er godkendt, og derved udgør en yderligere risiko for sikkerheden. Afsløring af programmer, der hægter sig på andre programmer, forhindrer avancerede angreb, f.eks. kapring af browseren.

Signaturbaseret afsløring af indtrængen

Beskytter mod kendte teknikker til angreb på netværket

Intrusion Detection er en Desktop Firewall, der kan afsløre adfærd i den legale netværkstrafik, eller programaktivitet, der tyder på et angreb på klienten. Den er baseret på regler defineret i en McAfee Security-signaturfil. IDS-signaturer kan opdateres automatisk eller manuelt for at sikre, at Desktop Firewall også kan beskytte mod de angreb, der dukker op i fremtiden. Hvis Desktop Firewall identificerer et ind- eller udgående angreb, kan den blokere for indtrængen, give besked og logge hændelsen. Ved at registrere indtrængen kan Desktop Firewall beskytte klienterne mod angreb og forhindre, at de bruges til at angribe andre. Desktop Firewall kan forhindre mange almindelige angrebsmetoder, f.eks. IP Spoofing, Ping Flood, SYN Flood m.m.

Quarantine Mode

Forhindrer, at ikke-sikre klienter opretter forbindelse til netværket

I Quarantine Mode undersøges Desktop Firewall af ePolicy Orchestrator, inden klienten får fuld forbindelse til netværket. Hvis klienten er forældet eller kører med gamle regler, begrænses netværksadgangen. Desktop Firewall- og VirusScan Enterprise-regler, softwareopdateringer og DAT-filer kan derefter bringes på plads og klienten frigives fra karantæne. Quarantine Mode beskytter netværket mod forældede antivirusprogrammer og regler samt forældet Desktop Firewall-software, der gør klienterne sårbare over for angreb. Ved at anbringe klienterne i karantæne, indtil de er opdateret, begrænses risikoen på netværket, fordi potentielt farlig trafik ikke kommer ud på netværket.

McAfee® Desktop Firewall™ 8.0

Proaktiv beskyttelse og styring af netværksklienter

Central administration

Global håndhævelse af regler

Desktop Firewall fås i to udgaver: en enkeltstående løsning, der er ideel til mindre virksomheder eller brugere med behov for at styre deres egne regler, samt en McAfee ePolicy Orchestrator-løsning til den større virksomhed. Med integreret i McAfee ePolicy Orchestrator kan Desktop Firewall administreres centralt fra en enkelt konsol. ePolicy Orchestrator kan installere og indstille regler for Desktop Firewall og jævnlige udsende produktopdateringer og ændringer af regler. I kraft af den centraliserede administration i ePolicy Orchestrator kan administratorerne spare penge, tid og båndbredde, fordi det kun er nødvendigt med én konsol til administration af ikke bare Desktop Firewall, men også vurdering af virusbeskyttelsen og sårbarheden over for virus på virksomhedsplan. Håndhævelsen af reglerne sikrer, at Desktop Firewall-klienterne ikke ændres, eller at der manipuleres med deres indstillinger.

Grafisk rapportering

Global synlighed

ePolicy Orchestrator har effektive grafiske rapporteringsfaciliteter, der omfatter hele virksomheden, herunder standard eller brugerdefinerede rapporteringsskabeloner. Der er standardskabeloner for: Al indtrængen, mål for og kilde til indtrængen, angrebsmålenes top-10, top-10 blandt indtrængere samt oversigt over indtrængen baseret på type, år, måned eller uge. Med rapporterne kan administratorerne udarbejde detaljerede analyser af angreb og indtrængen på netværket og finde ud af, hvorfra de stammer. Desuden giver ePolicy Orchestrator administratorerne mulighed for at afsløre problemer og handle hurtigt, når problemer med netværkssikkerheden skal løses.

Learn Mode

Dynamisk opbygning af Desktop Firewall-regler

Desktop Firewall får automatisk oplysninger om ind- og udgående netværkstrafik og programaktivitet. I Learn Mode beder Desktop Firewall brugerne eller administratorerne om at tillade eller afvise såvel program- som netværksaktivitet. Med Learn Mode kan en administrator hurtigt opbygge brugerdefinerede regler uden at hindre, at den lovlige klientaktivitet fungerer, hvilket er ideelt i nyinstallationer.

Auto-Learn og Audit Mode

Forenklet installation i virksomheden og opbygning af regler

Desktop Firewall kan automatisk få oplysninger om aktivitet, uden at brugeren behøver tillade eller afvise regler. Administratorerne kan foretage en regelrevison af Desktop Firewall og få vist de regler, der er oprettet. Reglerne kan derefter ændres, låses og distribueres til andre klienter som et standardregelsæt. Administratorerne kan desuden hurtigt opbygge brugerdefinerede regler, der kan overføres til resten af virksomheden, hvilket forenkler udbredelsen.

VPN-kompatibilitet

Fungerer sammen med løsninger fra andre leverandører

Desktop Firewall er designet med henblik på at styrke VPN-beskyttelsen (Virtual Private Network) og er testet og kører sammen med det mest populære VPN-klientsoftware, herunder Checkpoint, Cisco, Nortel og Microsoft®.

Kompatibiliteten sikrer, at organisationens nuværende VPN-klienter fungerer sammen med Desktop Firewall.

Expert Services

Maksimering af investeringen i sikkerhed

Den øgede afhængighed af informationsteknologien og de hastige "fremskridt" inden for angrebsteknikkerne betyder, at vurdering af sikkerheden, udbredelse af sikkerhedsteknologier og indførelse af sikkerhedsregler, der fungerer, i dag er af

vital betydning for, at virksomhederne kan få succes. Network Associates Expert Services har til formål at yde ekspertassistance inden for alle faser af administrationen af sikkerhedsprogrammet – fra design og vurdering til udbredelse af teknologien og akut indsats. Som leverandør af netværksoptimering og sikkerhedstjenester ved ingen bedre end os, at tilgængelighed er et forretningsmål, der har lige så stor betydning for virksomhedens succes som sikkerheden. Derfor kan vi levere løsninger, der skaber balance mellem effektiv netværksdrift og sikker kontrol. Slutresultatet er sikkerhedsforanstaltninger, der arbejder for organisationen snarere end at hæmme den.

Systemkrav

Bemærk: Systemkravene i det følgende er generelle systemkrav og kan variere afhængigt af driftsmiljøet.

- En Intel® Pentium 166 MHz processor eller hurtigere
- Minimum 64 MB RAM
- Minimum 32 MB ledig plads på harddisken
- Et af følgende operativsystemer:
 - Microsoft Windows® 98 SE (Second Edition)
 - Microsoft Windows NT Workstation 4.0 med Service Pack 6 eller nyere
 - Microsoft Windows NT Server 4.0 med Service Pack 6 eller nyere
 - Microsoft Windows 2000 Professional med Service Pack 2
 - Microsoft Windows 2000 Server med Service Pack 2
 - Microsoft Windows 2000 Advanced Server med Service Pack 2
 - Microsoft Windows ME (Millennium Edition)
 - Microsoft Windows XP Home Edition
 - Microsoft Windows XP Professional

Alle produkter fra Network Associates® har vores PrimeSupport®-program og Network Associates Laboratories i ryggen. Prime Support-service, der er skræddersyet til din virksomheds behov, tilbyder vigtigt produktkendskab samt hurtige og pålidelige tekniske løsninger, der kan holde systemerne kørende. Network Associates Laboratories, verdens førende inden for informationssystemer og sikkerhed, er din garanti for vedvarende udvikling og forbedring af alle vores teknologier.

3965 Freedom Circle | Santa Clara, CA 95054 | 800.764.3337 main

networkassociates.com



YOUR NETWORK. OUR BUSINESS.