Acht essentiële firewallregels

De komst van Web 2.0 heeft een stortvloed van nieuwe dreigingen op gang gebracht. De kans is daarom groot dat uw huidige firewall uw bedrijf niet meer voldoende bescherming biedt. Deze checklist is bedoeld om u meer inzicht te geven in de geavanceerde functies van de nieuwe generatie firewalls. U kunt deze lijst ook gebruiken als richtlijn bij het evalueren van firewalloplossingen. Wij vergelijken oudere, verouderde of in technisch opzicht ontoereikende systemen van leveranciers als Cisco en Check Point met de nieuwste McAfee® Firewall Enterprise V8-appliance. Als u binnenkort een grote upgrade wilt uitvoeren, kunt u met behulp van deze lijst zoveel mogelijk voordeel uit uw investering halen.

Regel 1: Een fijnmazige controle vereist inzicht in en handhaving van de interacties van gebruikers en Web 2.0-toepassingen

Het meeste verkeer maakt momenteel gebruik maakt van HTTP (poort 80) en HTTPS (poort 443). U moet daarom in deze protocollen en poorten kunnen kijken om het verkeer zelf, inclusief het versleutelde verkeer, grondig te kunnen inspecteren. Cybercriminelen maken tegenwoordig vaak gebruik van encryptie. Clientaanvallen die gericht zijn op kwetsbare webbrowsers en die gebruik maken van versleutelde verbindingen, kunnen Cisco's firewall ongestoord passeren zonder dat ze ontsleuteld en geïnspecteerd worden. Dit heeft tot gevolg dat netwerken volledig onbeschermd zijn.

Als u controle wilt uitoefenen, moet u kunnen zien welke activiteiten (bijvoorbeeld Skype-activiteiten) er plaatsvinden binnen de context van de persoon die een toepassing gebruikt. Vanuit dit perspectief kunt u regels definiëren die inspelen op de behoeften van uw bedrijf. U doet dit door de gebruiker, de context en de geavanceerde internettoepassingen (die noodzakelijk en geoorloofd zijn) op elkaar af te stemmen. U wilt bijvoorbeeld IRC-chatten toestaan en FTP-activiteiten blokkeren voor het klantenserviceteam van het online serviceportaal. Daarnaast wilt u Yahoo-zoekacties toestaan maar de e-mail- en chattoepassingen van Yahoo blokkeren. En u wilt mogelijk de toegang tot riskante of ongepaste websites blokkeren, tenzij er een zakelijke rechtvaardiging voor een specifieke gebruikerscommunity is. In dat geval moet u het gewenste beleid met een relevante regel kunnen implementeren.

De nieuwste generatie geavanceerde firewalls, zoals de McAfee Firewall Enterprise-appliance, geven u inzicht in uw toepassingsverkeer, met inbegrip van het inkomende en uitgaande versleutelde verkeer. Terwijl Cisco alleen het VoIP-verkeer ontsleutelt (zodat het de firewall kan passeren) inspecteert McAfee daadwerkelijk het SSH-, SFTP- en HTTPS-verkeer op kwaadaardige inhoud. Check Point kan helemaal niet in het versleutelde verkeer kijken.

McAfee biedt u naast toepassingsbeheer ook de mogelijkheid om op gebruikersniveau beleidsregels op inkomende en uitgaande activiteiten toe te passen. Hierdoor kunt u precieze, nauwkeurige toepassingsregels opstellen die goed passen bij uw bedrijf. U kunt deze regels baseren op de bestaande gebruikersgroepen in uw Microsoft Active Directory of LDAP-adreslijst. Deze benadering, die zowel op de toepassing als op de gebruiker is gericht, maakt een fijnmazige controle mogelijk die weinig onderhoud vergt.

Regel 2: Bescherming tegen multivectordreigingen mag geen extra kosten met zich meebrengen

Het ontbreken van diepgaande inspecties en effectieve verdedigingstechnieken in firewalloplossingen heeft met de jaren geleid tot een verscheidenheid van gelaagde of aanvullende beveiligingsmaatregelen. Sommige architecturen dwingen u te kiezen tussen verschillende beveiligingsmogelijkheden. Bij Cisco moet u bijvoorbeeld beslissen of u antivirus of inbraakpreventie op een specifiek systeem wilt activeren. Firewalls van andere leveranciers beschikken vaak niet over geïntegreerde beveiligingsfuncties, met als gevolg dat u aanvullende endpointoplossingen moet kopen.

Van IRC naar P2P en HTTP

"*Er is een verandering merkbaar in de manier waarop bots worden beheerd. Het beheer verloopt steeds vaker via websites (met behulp van het veelgebruikte HTTP) in plaats van via IRC-kanalen. Deze wijziging is in gang gezet met de komst van exploitpakketten, die voor het merendeel door Russische cybercriminelen worden ontwikkeld. Mpack, ICEPack en Fiesta zijn namen van enkele bekende pakketten. Deze pakketten kunnen software installeren op externe computers en de software vanaf een externe website besturen.*"

"*Hackers hoeven alleen maar spamberichten met koppelingen te verzenden. Slachtoffers die op de koppeling klikken, worden naar een website geleid waar het exploitpakket is geïnstalleerd. Vervolgens kan het exploitpakket bepalen welke exploit moet worden gebruikt, afhankelijk van het land waar het slachtoffer woont en het besturingssysteem, de browser en eventuele meerdere versies van clienttoepassingen die op het systeem aanwezig zijn.*"

—McAfee-dreigingsrapport, vierde kwartaal 2009

Uiteraard genereert elk afzonderlijk product zijn eigen kapitaal- en bedrijfskosten, van aankoop en onderhoud tot afzonderlijke verlengingen van abonnementen. Maar elk afzonderlijk product brengt ook verborgen kosten met zich mee. Check Point activeert bijvoorbeeld een algemene beveiligingsfunctie, zoals signaturen voor inbraakpreventiesystemen, in plaats van beveiliging per regel. Deze werkwijze heeft grote gevolgen voor de prestaties. Sommige gebruikers van Check Point schakelen liever de beveiliging uit dan dat de prestaties worden beïnvloed. Ook komt het voor dat ze bepaalde beveiligingsfuncties door Check Point laten deactiveren bij het bereiken van bepaalde drempelwaarden. En dat terwijl de meeste aanvallen tijdens een piekactiviteit plaatsvinden.

Aanvullende beveiliging wordt vaak door afzonderlijke apparaten op hetzelfde verkeer toegepast, in plaats van in één activiteit geïntegreerd. Deze werkwijze vereist niet alleen extra hardware, maar vertraagt ook de doorvoer.

McAfee heeft een grote stap voorwaarts genomen, zowel op het gebied van functionaliteit als ten aanzien van de kosten, dankzij haar geconsolideerde beveiligingsservices die meerdere beveiligingen samenbrengen in elk vooraf geconfigureerd McAfee Firewall Enterprise V8-systeem. Zonder extra kosten of integratietaken kunt u de volgende beveiligingsfuncties activeren: inbraakpreventie, antimalware, antispyware, URL-filters en wereldwijde reputatiefilters (om riskante sites en bekende spammers te blokkeren). Deze beveiligingen kunnen worden beheerd met behulp van globale toepassingscategorieën of per toepassing, per protocol en per regel. Met een dergelijke flexibele, fijnmazige controle kunt u zelf bepalen hoe de beveiliging het beste kan worden versterkt (misschien voor verkeer naar en van bepaalde regio's) en welke beveiligingsregels moeten worden aangepast. De geïntegreerde inspectie zorgt ervoor dat er zonder vertraging meerdere beveiligingsactiviteiten kunnen worden uitgevoerd. U hoeft dus geen cruciale beveiligingsfuncties uit te schakelen om de prestaties op een acceptabel niveau te houden.

"De sleutel tot het terugdringen van de kosten bestaat uit het drastisch verminderen van het aantal geslaagde aanvallen en gegevensverliezen; met andere woorden, een beter beheer van firewallregels. Door op de juiste wijze te investeren in firewalloplossingen die een betere beveiliging bieden met minder signaturen, moeten organisaties het gemiddelde jaarlijkse gegevensverlies van meer dan een miljoen dollar fors kunnen terugdringen".

—IDC, *The State of Today's Firewall Management Challenges* (De actuele status van firewallbeheerproblemen), juni 2009

Regel 3: Beheer mag seconden duren, geen minuten

Een firewallbeheerder heeft doorgaans zijn handen wel vol aan het beheer van beleidsregels en beveiligingsfuncties. Als een bedrijf verschillende systemen en meerdere beheerders heeft, is het niet alleen moeilijk om goede regels op te stellen maar ook om deze regels te onderhouden. Bij Cisco moeten gebruikers bijvoorbeeld firewall- en NAT-regels (Network Address Translation) in afzonderlijke vensters configureren. Elke afzonderlijke stap betekent extra werk en een grotere kans op vergissingen. Als er meerdere beheerders zijn, neemt de complexiteit toe en is de kans groter dat regels elkaar overlappen, met als gevolg tragere prestaties en regels die nooit actief worden. Het toevoegen van meer beheermogelijkheden voor toepassingen en gebruikers leidt tot extra opties, meer beslissingen en in principe veel meer werk.

McAfee maakt in plaats daarvan gebruik van een "één-regel-weergave" waarin alle informatie wordt weergeven die u nodig hebt om snel en eenvoudig nauwkeurige regels op te stellen. In het verkeer van en naar poort 80 of 443 kunt u bijvoorbeeld beperkingen op specifieke functies invoegen, McAfee TrustedSource™-reputatieservices toevoegen of locatiefilters activeren. Elke regel kan aan een specifieke gebruikersgroep worden gekoppeld.

Al deze opties worden weergegeven in één venster. Elke regel kan met slechts enkele muisklikken worden geactiveerd, zodat u snel en eenvoudig van de beschikbare mogelijkheden gebruik kunt maken. In het venster voor regelinteracties kunt u vervolgens een voorbeeld van de regels bekijken om conflicten of overlappingen op te sporen. Aangezien onze firewalloplossing een natuurlijke werkstroom ondersteunt, kunt u de volgorde controleren en de details van elke hele regel in één venster bekijken. Als u meer informatie over het gebruik nodig hebt of problemen wilt oplossen, kunt u met onze visualisatie de activiteit per gebruiker, toepassing en dreiging weergeven en rechtstreeks naar de juiste regels navigeren om deze aan te passen.

Regel 4: Een realtime risicoanalyse moet alle dreigingsvectoren omvatten en intern worden ontwikkeld

Naast de hoge kosten en de trage prestaties vormt de inferieure bescherming ook een belangrijk nadeel van afzonderlijke beveiligingsoplossingen. Elk programma houdt vast aan zijn beperkte kijk op het probleem, zonder te leren van andere systemen die nieuwe dreigingen en zero-day kwetsbaarheden aan het licht brengen. Cybercriminelen maken momenteel op grote schaal misbruik van deze geïsoleerde

programma's met behulp van slimme dreigingen die uit meerdere fasen bestaan en van meerdere vectoren gebruik maken. Conficker, operatie Aurora en Mariposa bedienen zich alle drie van meerdere ingangen. Deze geraffineerde en complexe aanvallen kunnen niet meer worden tegengehouden door reactieve, op signaturen gebaseerde oplossingen die gericht zijn op één vector. Signatuurtechnologieën behouden hun waarde (vraag het onze onderzoekers maar, zij zullen u vertellen dat oude wormen nooit doodgaan, maar alleen van vorm veranderen) maar zijn niet langer de enige vorm van bescherming.

Waarom schieten signaturen tekort? Signaturen documenteren bekende dreigingen pas nadat deze zijn gevalideerd. Het verspreiden en installeren van signaturen kan ertoe leiden dat de aankondiging van een probleem enkele dagen (of langer) wordt uitgesteld. Veel leveranciers hebben een licentie op beveiligingen van derden, waardoor de ontvangst veel vertraging oploopt. Check Point maakt gebruik van technologieën van Kaspersky, Websense en Commtouch. Als u Cisco gebruikt, ontvangt u een wekelijkse antivirusupdate via Trend Micro. Dit betekent dat het wel een week kan duren voordat u beschermd bent tegen nieuwe dreigingen. Het is algemeen bekend dat de kwaliteit van signaturen per leverancier grote verschillen vertoont. De kwaliteit wordt beperkt door het aantal onderzoekers en het onderzoeksbereik van de betreffende leverancier (of de leverancier van de leverancier). Al deze verschillende activiteiten leiden tot een inefficiënte beveiliging, die door middel van abonnementskosten bij u in rekening wordt gebracht, terwijl u ook nog eens met een gat in de beveiliging zit.

Beveiligingsfunctie	McAfee Labs™
Malwaredetectie	Detecteert 50.000 nieuwe malwaresamples per dag
Internetfilters	Circa 35 miljoen sites gecategoriseerd voor filtering
Spam/phishing	Analyseert 20 miljard query's per maand
Netwerk IPS	Circa 300 miljoen IPS-aanvallen geanalyseerd per maand; 100 miljoen query's op IP/poort-reputaties per maand
Internetreputatie	Zes jaar gegevens; omvat nu 80 miljoen websites
IP-adresreputatie	Zeven jaar gegevens
Bestandsreputatie	Twintig jaar gegevens

Afbeelding 1: omvang en ervaring zijn van groot belang bij wereldwijde dreigingsinformatie

Gehackte inhoud en onbekende zero-day dreigingen vormen momenteel een groot risico voor bedrijven. Als een dreiging niet bevestigd is, moeten programma's het risico zelf beoordelen op basis van gedrag, reputatie, bronadres, doeladres en de inhoud zelf (inclusief verborgen inhoud die is ontsleuteld en van versluieringslagen is ontdaan). Hoe meer gegevenspunten en dreigingsvectoren waaruit u informatie kunt putten, des te nauwkeuriger en sneller uw evaluatie tot stand komt. Als de analyse direct plaatsvindt - in real time - geeft dit de beste kans op vroegtijdige bescherming tegen bekende dreigingen. Dit brede perspectief is mogelijk de belangrijkste reden om te kiezen voor een leverancier die het totaalbeeld observeert en analyseert, zonder cruciale delen aan kleinere spelers uit te besteden.

De McAfee Firewall Enterprise-appliance biedt u proactieve bescherming met behulp van wereldwijde dreigingsinformatie die in real time wordt bezorgd. Meer dan 100 miljoen sensoren en automatische technieken correleren dreigingen van 15 verschillende vectoren op het gebied van hosts, netwerken, internet, e-mail en gegevensverlies. Wij vergelijken tevens nieuwe inhoud en activiteiten met een gedragsdatabase voor berichten en communicatie, die onder andere informatie bevat over reputaties, hoeveelheden en trends op het gebied van e-mail, internetverkeer en malware. Dankzij dit uitgebreide, onderling verbonden systeem, dat in een tijdsbestek van meer dan 20 jaar is opgebouwd, kunnen wij risico's herkennen en u bescherming bieden nog voordat een specifieke dreiging het officiële signatuurproces heeft doorlopen. Andere leveranciers kiezen één protocol of dreigingsvector en werken met reputaties die zich beperken tot één element, bijvoorbeeld spamberichten. McAfee werkt daarentegen met alle protocollen en dreigingstrends om een zo compleet mogelijk beeld te creëren en de meest effectieve bescherming te bieden.

Regel 5: Uw firewall mag u niet kwetsbaarder maken

Exploitcocktails bestaan uit een verzameling malware die gericht is op elke potentiële zwakheid in elk systeem. Uw beveiligingsproducten moeten u helpen met het oplossen van dit probleem, in plaats van zelf kwetsbaarheden te huisvesten of als katalysator voor noodpatches te fungeren. Telkens wanneer u een patch moet installeren, loopt u het risico dat u het verkeer ontwricht of de stabiliteit van het systeem in gevaar brengt.

De McAfee Firewall Enterprise-appliance is gebaseerd op het robuuste McAfee SecureOS®-platform dat zo'n twintig jaar geleden voor de Amerikaanse geheime dienst werd ontwikkeld. Deze appliance kan bogen op een ongeëvenaarde CERT-geschiedenis, met nul kwetsbaarheden in onze SecureOS, nul gegevenslekken en nul noodpatches.

Regel 6: Bestaande regels moeten worden overgezet, in plaats van nieuwe te maken

Het ontwikkelen en onderhouden van firewallregels is het duurste aspect van een firewall. Als u overweegt een migratie uit te voeren, moet u kunnen rekenen op automatische migratieprogramma's en specifieke services die uw oude regels in uw nieuwe omgeving importeren.

McAfee biedt Forbes Global 2000-bedrijven en overheidsorganisaties al jaren ondersteuning bij het migreren van hun bestaande regels naar onze eenvoudige, gecentraliseerde regelomgeving. Ons programma voor het migreren van regels verplaatst 90 procent van alle configuratiegegevens, met inbegrip van objectgegevens, services en bestaande regelsets. U kunt uw configuratie ook stroomlijnen door objecten of services uit te sluiten die momenteel niet door de regelset worden gebruikt.

Ons gespecialiseerde serviceteam voor netwerkbeveiliging beschikt over handige programma's om u door het migratieproces te loodsen. Met behulp van deze programma's kunnen beleidsregels van Cisco PIX-, Cisco ASA- en Check Point-firewalls moeiteloos worden overgezet. Binnenkort komen er ook programma's voor Juniper- en Fortinet-oplossingen beschikbaar.

Regel 7: Integratie en flexibiliteit is een vereiste, tot en met de ondersteuning

Wilt u de rol van integreerder spelen of tijdelijke oplossingen voor slecht ontworpen en beperkte producten bedenken? U kunt uw tijd vast wel beter gebruiken. Tegenwoordig is elk bedrijf gedistribueerd en elk netwerk uniek. Dit zijn de ongeschreven regels van het spel dat beveiliging heet. Slimme leveranciers kennen deze regels en zorgen ervoor dat u snel en eenvoudig een goede beveiliging kunt implementeren. Bovendien bieden ze u altijd en overal ondersteuning, 24 uur per dag, 7 dagen per week, 365 dagen per jaar.

De firewalloplossingen van McAfee zijn verkrijgbaar in een grote verscheidenheid van betaalbare, robuuste configuraties, die zowel geschikt zijn voor bijkantoren als voor veeleisende ondernemingen die behoefte hebben aan een doorvoercapaciteit van 12 Gbps. U kunt kiezen uit de volgende drie mogelijkheden: een speciaal vervaardigde appliance, een multifirewall-appliance met 4, 8, 16 of 32 firewalls in een klein 2U-chassis of een virtuele firewall-appliance voor VMware ESX. Wij bieden tevens McAfee Firewall Enterprise for Riverbed (die kan worden geïnstalleerd op verschillende modellen Riverbed Steelhead-appliances die op het Riverbed Services Platform draaien) plus zeer robuuste appliances die bestand zijn tegen ruwe omgevingen. Dit zijn hulpmiddelen waar u echt mee kunt werken.

Al deze flexibiliteit wordt geleverd tegen een betaalbare prijs. In tegenstelling tot Cisco betaalt u bij McAfee niet voor een lappendeken van appliances en beveiligingsmodules. In tegenstelling tot Check Point betaalt u bij McAfee niet voor complexiteit en de noodzaak om meerdere blade-opties te configureren die hardware van andere leveranciers moeten worden gezet.

Aangezien centraal beheer de kern is van efficiëntie (en compliancerapportage) kunt u appliances voor zeer grote bedrijven combineren met mkb-systemen binnen dezelfde beheeromgeving. Tot de taken van het meegeleverde McAfee Firewall Reporter behoren de centrale bewaking van meerdere systemen en het verzamelen en analyseren van logboekgegevens die afkomstig zijn van meerdere apparaten. U kunt kiezen uit meer dan 500 gratis rapportsjablonen; er is dus vast een sjabloon bij dat precies bij uw bedrijf en richtlijnen past.

Voor vragen of ondersteuning kunt u terecht bij ons supportteam van firewalltechnici, dat 24 uur per dag, 7 dagen per week voor u klaar staat. De reactietijden zijn kort: enkele minuten, in plaats van enkele uren. Wij schakelen 's nachts de telefoon niet uit en helpen niet alleen gebruikers uit één werelddeel; onze klanten, ons onderzoek en onze support omvatten de hele wereld.

Regel 8: Integratie is een voorwaarde voor optimale beveiliging

We hebben de besparingen en eenvoud van meerdere beveiligingsfuncties in één firewall uitgebreid besproken. Maar omdat de firewall slechts één onderdeel van uw beveiligings- en IT-beheer is, moet u ook zoeken naar eenvoud achter de firewall. Hoe zit het met uw andere netwerkbeveiligingsproducten, herstelprogramma's, beveiligingsinformatiebeheer en gerelateerde werkstromen? En hoe staan de zaken met betrekking tot endpointbeveiliging, preventie van gegevensverlies en risicobeheer? Hoe beter uw systemen met elkaar communiceren, des te eenvoudiger uw taken worden. En wij zijn gespecialiseerd in de onderlinge communicatie tussen beveiligingsoplossingen.

McAfee is de grootste gespecialiseerde leverancier van beveiligingsproducten. Onze firewall is geïmplementeerd bij meer dan 15.000 klanten en communiceert met een groot aantal andere netwerkbeveiligingsfuncties, zoals internetgateways, e-mailgateways, netwerktoegangsbeheer, gedragsanalyses van netwerkgebruikers, netwerkdreigingsreacties en inbraakpreventiesystemen. Wij zijn een reeds lang bestaande en erkende leider op het gebied van onder andere endpointbeveiliging, beveiliging van mobiele gegevens en cloudbeveiliging. De producten uit onze uitgebreide portfolio zijn met elkaar verbonden via het open, gecentraliseerde McAfee ePolicy Orchestrator® (McAfee ePO™)-beheerplatform. U profiteert dus van operationele voordelen met elke bescherming die u implementeert. Daarnaast zijn meer dan 90 McAfee Security Innovation Alliance-partners met het McAfee ePO-beheerplatform verbonden, zodat de besparingen en eenvoud worden uitgebreid naar andere beveiligings- en IT-activiteiten.

Web 2.0 is de naam van een nieuw spel. Zorg dat u zich aan de spelregels houdt.

Als u overweegt een migratie uit te voeren naar een meer geavanceerde bescherming, kunt u met behulp van deze regels controleren of uw nieuwe firewall geschikt is voor de huidige geavanceerde hardnekkige dreigingen en complexe Web 2.0-toepassingen:

1. Een fijnmazige controle vereist inzicht in en handhaving van de interacties van gebruikers en Web 2.0-toepassingen.
2. Bescherming tegen multivectordreigingen mag geen extra kosten met zich meebrengen.
3. Beheer mag seconden duren, geen minuten.
4. Een realtime risicoanalyse moet alle dreigingsvectoren omvatten en intern worden ontwikkeld.
5. Uw firewall mag u niet kwetsbaarder maken.
6. Bestaande regels moeten worden overgezet, in plaats van nieuwe te maken.
7. Integratie en flexibiliteit is een vereiste, tot en met de ondersteuning.
8. Integratie is een voorwaarde voor optimale beveiliging.

Met de McAfee Firewall Enterprise-appliance kunt u het poort- en protocolbeheer vervangen door effectieve en nauwkeurige bescherming. Uw organisatie profiteert van een betere toegang tot Web 2.0-toepassingen en wordt beveiligd door identiteits- en toepassingsgericht beheer, wereldwijde dreigingsinformatie en meerdere beveiligingsservices. Al deze elementen werken als een hecht team samen om uw organisatie bescherming te bieden.

Wij zorgen ervoor dat een migratie soepel verloopt, met behulp van ons proefprogramma op een virtuele firewall, onze migratieprogramma's en onze gerichte professionele services. Maak een eind aan blinde vlekken en bescherm uw bedrijf tegen de huidige geavanceerde hardnekkige dreigingen, zonder verplichte patchdagen en met minder tijd en moeite. Ga voor meer informatie naar www.mcafee.com/nl en maak een proefrit met onze V8 op www.mcafee.com/virtualtestdrive.

McAfee International BV
Gatwickstraat 25, Postbus 58326
1043 GL Amsterdam
The Netherlands
+ 31 (0)20 5863800
www.mcafee.com/nl

8816brf_nts_nextgen-firewall_0310