

UNIFIED THREAT

5 appliances op de proef gesteld

Een firewall beschermt u tegen inbraken van hackers op uw netwerk, maar dat is al lang niet meer voldoende. Er komt immers een ware lawine van rommel uw bedrijfsnetwerk binnen via uw internetaansluiting: virussen, parasieten, spam, porno, noem maar op. Een Unified Threat Management- of geïntegreerde beveiligingsappliance beschermt u tegen al die bedreigingen vanuit één enkel toestel. We onderzochten er vijf. JOHAN ZWIEKHORST

Een UTM-appliance bevat een bundeling van veiligheidsgebonden functies. Voordat wij een toestel een UTM-appliance noemen, moet het minstens zowel een firewall als inhoudsinspectie bevatten. Bij voorkeur kan het toestel nog meer: inbraakdetectie en -preventie (IDS/IPS), antimalware, antiphishing, noem maar op. Een toestel met alleen firewall-functionaliteit noemen we dan ook een firewall-appliance.

We onderzochten vijf UTM-appliances: Check Point UTM-1, Fortinet FortiGate 300A, IBM ISS Proventia MX3006, NetASQ F200 en SecPoint Protector P1000-250. Met behulp van

poorten: int, ext, dmz en sync/lan. Het model 1050 dat wij kregen heeft daarnaast nog eens vier netwerkpoorten in een Gigabit-switch ingebouwd en er zijn ook USB-aansluitingen. Check Point levert namelijk een USB-sleutel mee waarmee u zo'n appliance erg snel weer in de fabrieksinstellingen kunt zetten: gewoon een kwestie van sleutel erin en de appliance starten. Het beheer loopt uiteraard via een webinterface en Check Point koos daarvoor een niet-standaard poort.

Beheer en beveiliging

De eerste keer krijgt u een installatie-wizard. Die laat u toe alle netwerk-aansluitingen te configureren en u

aanklikt, schuift die open in subrubrieken. Als er een andere rubriek open stond, gaat die terug dicht. U kunt dus maar één rubriek tegelijk open hebben. De vier hoofdruubrieken zijn: Informatie, Netwerk, Appliance en Productconfiguratie. Onder Informatie vindt u het welkomstschermbild en een statusoverzicht. Netwerk bevat logischerwijze de configuratie van de netwerkpoorten met bijbehorende instellingen voor routing, DNS en hostnaam. De rubriek Appliance omvat instellingen voor datum en tijd, back-up en restore, upgrade- en beeldkopiebeheer, onderhoud (diensten of de hele appliance stoppen of starten), diagnose, beheerwebserver (poort en toegang), appliancebeheerders, web- en SSH-clients, en beheerbeveiliging (loginrestricties en timeouts). Productconfiguratie staat in voor het licentiebeheer, en de toegang voor het GUI-beheer voor gebruikers en beheerders, het downloaden van de SmartConsole-beheerapplicatie en het starten van het SmartPortal. Dat laatste is een webuitbreiding voor SmartCenter om externe toegang voor bepaalde beveiligingsinstellingen mogelijk te maken. UTM-1 bevat licenties voor UTM-1 zelf, voor SmartPortal, voor SmartCenter en voor de Eventia-rapportagemodule. Voor het eigenlijke beveiligingsbeheer gebruikt u dus de SmartConsole en met name SmartDashboard. Die is erg veelzijdig en te ingewikkeld om hier te bespreken, maar er zit alles in om policy's en daarbij horende regels te maken, te bekijken en te bewaken op een zeer overzichtelijke manier.

De Check Point UTM-1 is in essentie een firewall op steroïden. U definieert policypakketten en voor elk

De Fortinet FortiGate 300A is een erg fraaie, goed uitgewerkte en gebruiksvriendelijke appliance

de IBM ISS Internet Scanner hebben we een scan uitgevoerd van zo'n 128 beveiligingsrisico's voor elk van de appliances en het goede nieuws is, dat ze allemaal perfect scoorden en geen enkele informatie vrijgaven over het binnennetwerk. Zo hoort het!

Check Point UTM-1

De bescheiden naamgegeven UTM-1 appliance van het Israëlische Check Point is in lichtgrijs uitgevoerd met op het voorpaneeltje een lichtblauw Check Point-logo. Hoewel alle productinformatie die we kregen voor het model 2050 is, leverde Check Point ons het model 1050. Qua firmware zijn al die modellen identiek, het verschil zit 'm in de prestaties die ze kunnen leveren. De basisfunctionaliteit werkt via vier vaste netwerk-

kiest ook het beheertype: lokaal of centraal. Overigens kunt u met één voor lokaal beheer ingestelde UTM-1 andere UTM-1's centraal beheren. Als u met Windows werkt, krijgt u ook de gelegenheid een SmartConsole-beheerapplicatie te downloaden en te installeren. Daarna kunt u de appliance beheren via die applicatie of via de webinterface. Die laatste geeft u echter geen beheer over de beveiligingsfunctionaliteit van de appliance, alleen over de appliance en zijn werking zelf.

Check Point koos voor de beheerinterface pastelkleuren met lichtblauwe, lichtgele en grijzige tinten. Uiterst links is er een hoofdmenu met uitklapbare rubrieken die elk een leuk en duidelijk pictogram hebben (maar ook tekst). Als u een rubriek

MANAGEMENT

reglement definieert u de bijbehorende regels voor alle soorten van netwerk- objecten, -groepen en -structuren met acties voor een of meerdere diensten tegelijk. Daarbij kunt u rekening houden met VPN-verkeer, en QoS-regels aanmaken en opleggen. Naast de bijzonder uitgebreide firewallfunctionaliteit kunt u regels aanmaken voor SmartDefense en voor inhoudsinspectie. SmartDefense is de verzamelnaam voor alles wat maar met aanvallen en hun signaturen te maken heeft: zowel antivirus als antiparasiet en antihacker voor alle mogelijke protocols en applicaties, maar ook IPS. De inhoudsinspectie controleert welbepaalde protocols/applicaties (standaard SMTP, POP3, FTP en HTTP) op malware. U kunt daar bijkomende instellingen voor opgeven. Een echt inhoudsfilter waarbij data uitgesloten of toegelaten worden op inhoud (buiten de aanvalspatronende- tectie) zit echter niet in deze UTM-1.

Praktijk

Check Point biedt een bijzonder veel- zijdige en erg krachtige UTM-appliance. Buiten antimalware zit er geen echt inhoudsfilter in, maar al de rest doet hij wel en zonder dat we er iets op aan te merken hebben. Hiermee kunt u zeer ingewikkelde structuren opzetten die toch overzichtelijk ge-

houden worden via slimme object- kaarten met bijbehorend navigator. Als netwerkbeveiliging voor u zwaar- der weegt dan inhoudsbeveiliging (buiten malware), is deze appliance zeker uw overweging waard.

Fortinet FortiGate

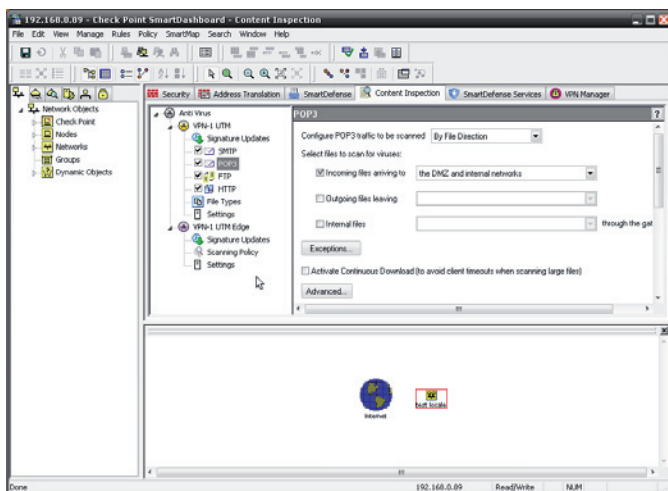
De FortiGate 300A van Fortinet is een compact één-rekeenhoud hoog toestel in smaakvol grijs met een zwart front. Fortinet zorgde voor een vrij stille ventilator: die begint wel wat luider, maar gaat na een tijdje veel stiller draaien. De firmware werkt met modules waarvoor u een licentie moet aanschaffen. De appliance kan als router of als transparante brug werken. Er zijn zes netwerk- aansluitingen waarvan de allereerste standaard voorzien is als een poort voor het interne netwerk, en de vierde als een DMZ-aansluiting. De geboden UTM-functionaliteit is erg volledig en omvat ook web- en e-mailsecurity. Een echte alles-in-één dus.

Beheer en beveiliging

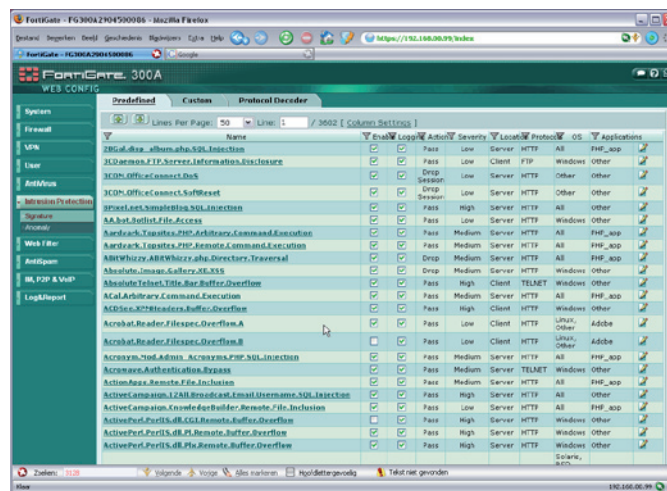
U kunt elk FortiGate-apparaat behe- ren via een webinterface die alleen bereikbaar is in het interne netwerk. Mocht u een groot aantal FortiGate appliances in uw bedrijf hebben of willen, dan heeft Fortinet ook nog een FortiManager: dat is een centraal

beheersysteem voor grote aantallen FortiGate-appliances. De webinterface ziet er eenvoudig uit en blijkt ook zo te zijn in het bedienen ervan. Aan de linker kant ziet u de basisfuncties van de security appliance en door ze aan te klikken splitst u ze uit in hun onderdelen. Elk aangeklikt onderdeel laat zijn configuratie in het rechterdeel van het scherm zien. Vaak is dat dan zelf ook weer in een aantal tabbladen onderverdeeld. Alle onderverdelingen zitten logisch in elkaar en de bediening van de diverse dialoogschermen is zo eenvoudig dat u ermee uit de voeten zou moeten kunnen zelfs als u vrijwel geen ervar- ring heeft met firewalls en dergelijke toestellen.

Fortinet gebruikt een eigen antimalware-engine en uiteraard zorgt het systeem voor volautomatische frequente updates van die malware-handtekeningen, maar ook van de andere signatuurdatabases voor de ingebouwde IDS/IPS en updates voor het spamfilter. Alle beveiligingen activeert u via een firewallreglement of policy. De beveiligingsinstellingen lopen via een beschermingsprofiel dat u kunt wijzigen. Het is mogelijk overrides te definiëren voor beheer- ders of managers. Voor de verschil- lende ingebouwde inhoudsfilters



Instellen van inhoudsinspectie voor POP3 vanuit Check Points SmartDashboard.



Configuratie van Fortinets IPS.

Tabel 1. De functionaliteit in punten uitgedrukt.

TEST & FUNCTIONALITEIT

Merck	Punten	Omschrijving	CheckPoint, UTM-1 2050, SmartDefense AVE	Fortinet, FortiGate 300A, Fortinet AVE	IBM ISS, Proventia MX3006, ISS VPS AVE	NetASQ, F200, ClamAV AVE	SecPoint, Protector P1000-250, SecPoint AVE
Algemeen							
Gratis updates eerste jaar na aanschaf?	1	=Ja	1	0	0	0	1
Appliance hardware							
CPU kloksnelheid (MHz)	1	per 500 MHz	7	4	5	1	5
Totale capaciteit geïnstalleerd geheugen (MB)	1	per 128 MB	16	4	0	1	8
Totale capaciteit van alle geïnstalleerde harde schijven (GB)	1	per 10 GB	8	0	4	4	20
Aantal geïnstalleerde netwerkkaarten	1	per NIC	8	6	6	4	4
Fast Ethernet WAN?	1	=Ja	1	1	1	1	1
Standaard Gigabit Ethernet-ondersteuning?	1	=Ja	1	1	0	0	1
Appliance software							
Ingebouwde DHCP server?	1	=Ja	1	1	1	1	0
DNS server?	2	=Ja	0	0	0	0	2
DNS relay?	2	=Ja	2	2	0	2	0
FTP server?	2	=Ja	0	0	0	0	0
Routerfunctionaliteit (met NAT)?	2	=Ja	2	2	2	2	0
Webserver? (niet webbeheerinterface!)	2	=Ja	0	0	0	0	0
POP3 server?	2	=Ja	0	0	0	0	2
SMTP server?	3	=Ja	0	0	0	0	3
SMTP relay?	2	=Ja	2	2	0	2	2
IMAP4 server?	2	=Ja	0	0	0	0	0
IMAP4 relay?	2	=Ja	0	2	0	0	0
NNTP server?	1	=Ja	0	0	0	0	0
Network time server?	1	=Ja	0	0	0	0	0
HTTP Proxy/Webcache?	2	=Ja	0	2	0	2	0
HTTP Proxy Relay?	2	=Ja	2	2	0	2	0
VPN-ondersteuning?	2	=Ja	2	2	2	2	0
Cryptografie (bitlengte sleutel; 0=geen)	1	per 64 bits	4	4	4	4	64
Scoreberekening							
Totaal aantal punten	115	max.	57	35	25	28	113
Algemeen	100	max.	50	30	22	24	98
Beveiligingsengine + database							
Verwerkingscapaciteit (x1000 scanobjecten/uur)	1	per 5k; 5p = 00	5	5	5	5	0
Netwerkpakketverwerkingsnelheid (pakketten/seconde)	1	per 100k	0	0	0	0	0
Limiet van gelijktijdige TCP-verbindingen	1	per 1M	2	0	0	0	0
Aantal mogelijke beveiligingscategorieën	1	per 50; 10p=00	0	2	1	1	1
Onderverdeling in subcategorieën mogelijk?	1	=Ja	0	1	0	0	1
Zelf categorieën definiëren?	2	=Ja	0	2	0	0	0
Aantal miljoenen scanobjecten (patronen, adressen, sites of URL's) in database	1	per M; 10p = 00	10	32	75	10	10
Bijwerkingsfrequentie (D=dagelijks, W=wekelijks, M=maandelijks, O=ander ritme)	1	=M; +1p=W; +1p=D	0	0	0	3	3
Volautomatische bijwerking?	2	=Ja	2	2	2	2	2
Aanvullende bijwerking?	1	=Ja	1	1	1	1	1
Alle voorgedefinieerde objecten in database geverifieerd?	1	=Ja	1	1	1	1	1
Gebruik eigen (externe) databaseserver mogelijk van meerdere producenten?	1	=Ja	1	0	0	0	1
Scoreberekening							
Totaal aantal punten	90	max.	22	46	85	23	20
Beveiligingsengine + database	100	max.	24	51	94	26	22
Antivirusmaatregelen							
Ingebouwde virusscanner?	5	=Ja	5	5	5	5	5
Indien ingebouwd, welke antivirusengine?	1	=Ja	1	1	1	0	1
Externe virusscanner?	2	=Ja	0	0	0	2	0
Aantal virusscanners van derden ondersteund?	1	per 1; 10p = 00	0	0	0	10	3
Indien beperkte ondersteuning voor derden, geef opsomming?	1	per 1	0	0	0	1	3
Scoreberekening							
Totaal aantal punten	20	max.	6	6	6	18	12
Antivirusmaatregelen	100	max.	30	30	30	90	60
Inhoudelijke, netwerk- of sessiecontrole							
Spamfilter?	5	=Ja	0	5	5	5	5
Basissleutelwoorden?	1	=Ja	0	1	1	1	1
Complexe sleutels?	2	=Ja	0	2	0	2	2
Contextgevoelige herkenning?	5	=Ja	0	5	5	5	5
Bestandsextentiesleutels?	1	=Ja	1	1	1	0	1
Bestandsextensies koppelen aan categorie?	2	=Ja	0	0	0	0	2
Herkenning bestandstypes ingebed in andere bestanden?	5	=Ja	5	5	5	0	5
Recuratief algoritme voor inbeddingen?	2	=Ja	2	2	2	0	0
Beeldanalyse?	10	=Ja	10	10	0	10	10

kunt u zelf zoektermen definiëren, URL's of IP-adressen blokkeren, ActiveX, Java en andere scripten en cookies filteren. Fortinet heeft ook eigen filterdiensten waar de appliance gebruik van kan maken (zoals een FortiGuard webfilterdienst) en die dan volledig op afstand beheerd worden. Elk te controleren object wordt voorgelegd aan zo'n filterdienst en die geeft dan een 'OK' of 'niet OK' terug. Dit werkt op basis van objectcategorieën en u kunt van elke categorie aangeven of ze gewenst is of niet.

Praktijk

Dit is een erg fraaie, goed uitgewerkte en gebruiksvriendelijke appliance. De webfilter blijkt niet erg waterdicht te zijn en moet nog verbeterd worden. De andere beveiligingsmaatregelen zijn goed bruikbaar, al moeten we vermelden dat we de spamfilter van deze appliance niet getest hebben.

IBM ISS Proventia MX3006

De Proventia MX3006 van IBM's beveiligingsdivisie Internet Security Systems is een kleine compacte UTM-appliance, maar hij kan toch wat grotere netwerken aan (tot vijfhonderd gebruikers). Hij heeft alle netwerkaansluitingen vooraan en wel zes stuks. Het juiste aantal is afhankelijk van het MX-model. Het model 3006 heeft zes aansluitingen.

Zoals de overgrote meerderheid gebruikt ook ISS een webinterface voor het beheer. Alleen vereist die Java 1.5; de modernere Java 1.6 blijkt problemen op te leveren. De eerste keer verschijnt er een installatie-wizard. Die helpt u door de eerste instellingen heen en laat u ook kiezen tussen twee mogelijke werkmodi: router en transparant. Bij transparant werken alle beveiligingen ook nog, maar fungeert de appliance als een brug: u hoeft dan geen IP-adressen aan de poorten toe te wijzen, behalve één beheeradres. In routermodus definieert u een extern en een intern IP-adres, eventueel een DMZ en nog andere interne netwerken. In dat geval moeten al die poorten een IP-adres en bijhorende routing hebben.

Beheer en beveiliging

U doet het dagelijkse beheer van de appliance via het beheeradres bij transparant gebruik, of via het IP-adres van de interne poort(en) bij

Merk	Punten	Omschrijving	Checkpoint, UTM-1 2050, SmartDefense AVE	Fortinet, FortiGate 300A, Fortinet AVE	IBM ISS, Proventia MX3006, ISS VPS AVE	NetASQ, F200, ClamAV AVE	SecPoint, Protector P1000-250, SecPoint AVE
Actieve antivandaalbewaking?	1	=Ja	1	1	1	1	0
Bewaken van beheerderacties?	1	=Ja	1	1	0	1	1
Censuuruitschakeling door wachtwoord voor beheerders?	1	=Ja	1	1	0	0	0
Automatische koppeling van scanobjecten aan ip-adres(sen)?	5	=Ja	5	0	0	5	5
Uitsluiting van afzenders of sites?	2	=Ja	2	2	2	2	2
Annotatie van uitgaande e-mails?	2	=Ja	0	2	2	0	2
Regels op detailniveau (gebruiker/postbus/site)?	1	=Ja	0	1	0	1	1
Regels op groepeeniveau?	1	=Ja	0	1	0	1	0
Globale regels?	1	=Ja	0	1	1	1	1
Ingebouwde decodering van HTML of XML?	1	=Ja	0	1	1	1	1
Bayesiaanse (zelflerende) filter?	5	=Ja	0	0	0	0	5
Aanroepen andere filters?	2	=Ja	0	2	0	0	2
Meervoudige externe filteroperaties serialiseren?	1	=Ja	1	0	0	0	1
Uitpakken of decoderen van berichttekst of bijlagen vóór de filteranalyse?	1	=Ja	1	1	1	1	1
Interne zwarte lijst van adressen?	2	=Ja	2	2	2	2	2
Interne witte lijst van adressen?	2	=Ja	2	2	2	2	2
Raadplegen van externe zwarte-lijstservers?	5	=Ja	5	5	0	5	5
Aanpasbare lijst van externe zwarte-lijstservers?	5	=Ja	5	5	0	5	0
Voorgeconfigureerde zwarte lijst?	2	=Ja	0	2	0	2	2
IP- / pakketfilter?	1	=Ja	1	1	1	1	0
Applicatieproxy?	1	=Ja	1	1	1	1	0
Meerlagenarchitectuur?	1	=Ja	1	1	1	0	1
Maximum aantal sensoren/detectoren? (00=onbeperkt)	1	per 100; 00=20	20	20	20	0	20
Functionaliteit vanaf welke OSI-netwerklaag? (1-7)	2	per 1	12	2	2	2	14
Centrale distributie van sensoren/detectoren?	2	=Ja	2	2	2	0	2
Analyse van alle populaire applicatieprotocollen?	1	=Ja	1	1	1	1	1
Protocoldecodering?	1	=Ja	1	1	1	1	1
Bewaken van geslaagde/mislukte logins?	1	=Ja	1	1	0	1	1
Detectie van pakketgebaseerde aanvallen op netwerkniveau?	1	=Ja	1	1	1	1	1
Detectie van alle soorten poortenscans, ook 'stealth'?	1	=Ja	1	1	1	1	1
Wedersamenstelling van gefragmenteerde pakketten?	2	=Ja	2	2	2	2	2
Weerstand tegen bekende IDS-ontwikkelingstechnieken?	1	=Ja	0	1	1	1	1
Automatische herconfiguratie firewalls?	1	=Ja	1	1	1	1	0
Preventie-advies bij inbraakwaarschuwing?	2	=Ja	2	0	2	2	0
Expliciete ondersteuning voor lokaas?	1	=Ja	0	0	1	0	0
Scoreberekening							
Totaal aantal punten	115	max.	94	100	69	72	110
Inhoudelijke, netwerk- of sessiecontrole	100	max.	82	87	60	63	96
Beheer							
Beheer op afstand via webbrowser?	2	=Ja	2	2	2	0	2
Beheer op afstand via MMC of speciale software?	1	=Ja	1	1	1	1	0
Afdwingbare beperkingen op volume?	1	=Ja	1	0	0	1	1
Afdwingbare beperkingen op tijd?	1	=Ja	1	0	0	1	0
Waarschuw beheerder bij probleem via e-mail of pop-up?	2	=Ja	2	2	2	2	2
Geautomatiseerd uitvoeren van bepaalde regels of beperkingen?	1	=Ja	1	1	0	1	0
Samenwerking en uitwisseling regels met andere beveiligingsproducten?	1	=Ja	1	0	0	0	0
Scoreberekening							
Totaal aantal punten	9	max.	9	6	5	6	5
Beheer	100	max.	100	67	56	67	56
Rapportering							
Rapportgeneratie - hoeveel ingebouwde soorten?	1	per 5	0	60	4	3	0
Zelf rapporten definiëren?	2	=Ja	2	2	0	2	0
Rapportering via e-mail?	1	=Ja	1	1	0	1	0
Rapportering via webserver?	2	=Ja	2	2	0	0	0
Automatische rapportpublicatie?	1	=Ja	1	1	0	1	0
Grafiekgeneratie?	1	=Ja	1	1	0	1	1
Tabelgeneratie?	1	=Ja	1	1	0	1	1
Rapporten exporteren naar andere formaten?	1	=Ja	1	1	0	1	1
Scoreberekening							
Totaal aantal punten	70	max.	9	69	4	10	3
Rapportering	100	max.	13	99	6	14	4

routergebruik. Vervolgens kunt u via https bij de Java-webinterface voor de eigenlijke configuratie. De interface is helder en duidelijk en maakt gebruik van een uitklapbare hoofdmenuboom uiterst links met een zestal rubrieken. De 'home'-pagina toont statusinformatie. De rest is eigenlijk zelfverklarend.

De pagina voor 'firewall' is waarschijnlijk de meest ingewikkelde omdat er het grootste aantal subtabs aanwezig is, maar ISS is er toch in geslaagd om de eigenlijke informatiepanelen erg eenvoudig en overzichtelijk te houden. Voor alle beveiligingspolicy's kiest u bijvoorbeeld eerst voor welk bereik de policy bedoeld is (zoals intern, dmz of voor de appliance zelf). Daarna toont het systeem een venster 'inbound' en een venster 'outbound' waarin de regels te zien zijn voor inkomend en uitgaand verkeer. Elke regel geeft op wat toegestaan of verboden is voor welk netwerk, welk protocol, welke zenders en welke bestemmingen (zowel adressen als poorten). Als u een regel wil bewerken of toevoegen, krijgt u een pop-upvenster met de dialoog die u nodig heeft om de regel samen te stellen. ISS hield ook dit zeer eenvoudig en biedt afrolkeuzemenuutjes overal waar dat mogelijk is. Het is op deze manier zelden of nooit nodig de documentatie te raadplegen.

Heel interessant is dat de inbraakpreventie protocollen herkent en dus niet aparte regels voor iedere niet-standaard TCP- of UDP-poort moet hebben zoals het geval is voor veel andere appliances op de markt. Een bekende trojan wordt dus herkend als hij via de normale HTTP-poort 80 het netwerk binnenkomt, maar ook als dat zou gebeuren via bijvoorbeeld poort 9000. De appliance maakt trouwens volautomatisch zogenaamde 'dynamische regels' aan om een gedetecteerde aanval af te weren. Zo zal het systeem na detectie van een trojan die bijvoorbeeld poort 7777 gebruikt het verkeer van en naar uw netwerk via die poort voor een half uur volledig blokkeren via zo'n dynamische regel. Uiteraard kunt u dit verhinderen als u dat niet wilt. In de webinterface kunt u te allen tijde de op het moment geldende dynamische regels bekijken en desgewenst verwijderen. De ingebouwde antivirusmo-

dule is van Sophos, maar ISS heeft er een eigen engine rondom gebouwd en noemt dat geheel 'ISS Virus Prevention System'. De virusupdates zijn wel volledig die van Sophos, maar de appliance haalt ze van de site van ISS. Dat geeft ISS de gelegenheid om alle beveiligingsupdates in één keer door te sturen, dus ook inbraakpatronen. Standaard staat de machine ingesteld om één keer per dag te gaan kijken naar nieuwe updates. Daarbij hoort ook updates van de IPS-signaturen en de categorie- en URL-lijsten voor de ingebouwde webfilter.

Voor de IPS steunt ISS niet alleen op aanvalspatronsingaturen, maar ook en vooral op kwetsbaarheidsingaturen. In plaats van te proberen de aanval te identificeren, bekijkt de inbraakpreventie van ISS de acties die hij onderneemt op protocolniveau en vergelijkt die met een database van kwetsbaarheden. Is er een overeenkomst, dan wordt de actie geblokkeerd. Het grote voordeel van dit systeem is, dat er een

Windows. Ook herkent het pogingen om spyware, adware of bepaalde andere soorten malware op uw netwerk te krijgen.

De webfilter is niet denderend. Hij kent voornamelijk foute Amerikaanse sites, maar veel Europese niet. De beveiliging is bovendien gemakkelijk omzeilbaar door via de Google cache te werken of door (indien mogelijk) een externe proxyserver te definiëren in uw browser.

Praktijk

Deze MX3006 van IBM ISS werkt over het algemeen goed en heeft een gebruiksvriendelijke beheerinterface, al zijn we niet zo gelukkig met de nogal specifieke Java-vereisten. De beveiliging is adequaat, maar er zijn gebieden die IBM ISS nog zou kunnen verbeteren.

NetASQ F200

De UTM-appliances van het Franse NetASQ draaien in feite allemaal dezelfde firmware en hebben hetzelfde

wall- en IPS-prestaties van zo'n 192 Mbps en VPN-prestaties van 32 Mbps met maximaal 65.000 gelijktijdige TCP-verbindingen. Met maxima van duizend VPN-tunnels en 2048 filterregels moet deze F200 al heel wat werk kunnen verzetten. Het toestel heeft een bijzonder in het oog springend ontwerp: het is matzwart met vooraan een witte streep waarvan het middendeel rood oplicht als de appliance aan staat. Alle aansluitingen zitten achteraan. De F200 heeft vier netwerkpoorten. De eerste daarvan is standaard voor het externe netwerk bedoeld, en de tweede voor het interne. Wel even uitkijken dus, want dat betekent onder meer dat voor het beheer die tweede aangesloten moet zijn! Bij de eerste setup is dat geen probleem omdat dan alle poorten beheer toestaan, maar als u hem uit het rek haalt omdat er een probleem is opgetreden of zo, dan moet u daar dus wel aan denken. In tegenstelling tot alle andere toestellen in deze test beheert u deze UTM niet via een webinterface, maar via een speciaal beheerprogramma. Dat is de NetASQ Unified Manager en die draait helaas alleen onder Windows.

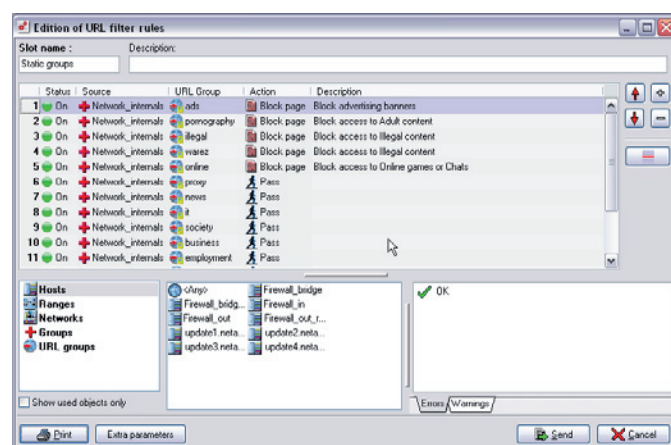
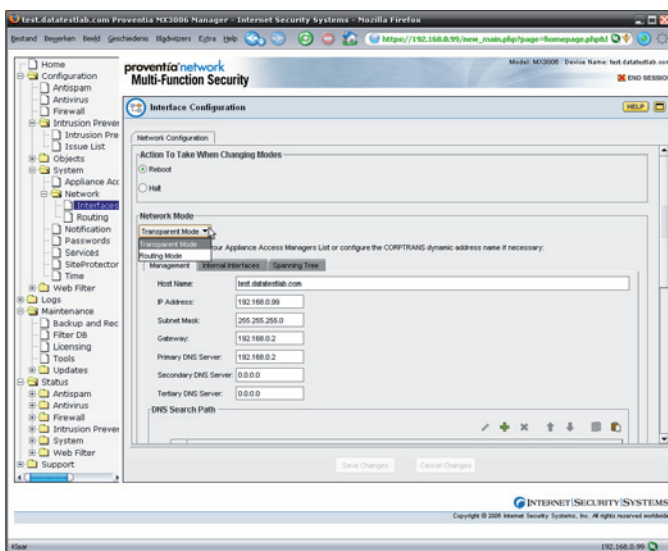
De NetASQ UTM F200 demonstreert duidelijk dat alle heil inzake beveiliging zeker niet van over de oceaan hoeft te komen

signatuurverdeling kan gebeuren zodra een kwetsbaarheid ontdekt of gepubliceerd wordt, zelfs voordat er voor de betrokken applicatie een patch uitgebracht is en voordat er aanvallers bekend geraakt zijn. De inbraakpreventie van ISS kan zelfs rekening houden met pogingen om misbruik te maken van 'buffer overflow'-bugs in

beheer, alleen hun hardwareprestaties verschillen. De UTM-productreeks loopt van het allerkleinste model F25 voor MKB's tot de machtige F550 die hetzelfde werk tegen een continue doorvoersnelheid van 2 Gbps kan leveren. De F200 is het laagste van drie middenmootmodellen. Het is bedoeld voor iets grotere MKB's en levert fire-

Beheer en beveiliging

De beheersuite Unified Manager heeft naast de eigenlijke beheerapplicatie ook nog een bewaakprogramma ('Realtime Monitor') en een rapportage-applicatie ('Event Reporter'). De beheerapplicatie opent met een standaard pull-downmenubalk zoals u die in alle Windows-applicaties ziet: File, Firewall, Maintenance, Ap-



Webfilterreglement NetASQ.

EINDSCORES

MerkModel of Type	CheckPoint, UTM-12050, Smart Defense AVE	Fortinet, FortiGate 300A, Fortinet AVE	IBM ISS, Proventia MX3006, ISS VPS AVE	NetASQ, F200, ClamAV AVE	SecPoint, Protector P1000-250, SecPoint AVE	
Commerciële Informatie						
Berekende maandgebruiksprijs (euro/licentie-eenheid/maand) voor 250 eenheden	258,33	137,17	92,41	50,2	100	
Adviesprijs Appliance, euro ex. BTW	\$15.500	8230	5490	2999	6000	
Adviesprijs Gebruikerslicentie, euro ex. BTW, voor 250 eenheden (gebruikers/postbussen/...)	0	0	2723	640	0	
BEOORDELING (max. 100)	Weging					
Algemeen	15%	50	30	22	24	98
Beveiligingsengine + Database	17%	24	51	94	26	22
Antivirusmaatregelen	17%	30	30	30	90	60
Inhoudelijke, Netwerk- Of Sessiecontrole	17%	82	87	60	63	96
Beheer	17%	100	67	56	67	56
Rapportering	17%	13	99	6	14	4
Prestatiescore	70%	50	61	45	48	55
Prijsscore	15%	18	34	51	93	47
Gebruikskosten	15%	19	36	54	100	50
Prijs-prestatiescore		41	53	47	63	53

Tabel 2. De prestaties! De prijsscore hebben we berekend door de vermelde prijzen te vergelijken met een 'ideale' gebruikspreis van 50 euro per eenheid per maand en een 'ideale' toestelprijs van 2800 euro. De foutmarge bedraagt 2 punten.

plications, Options en Help. Onder het File-menu logt u uit of kiest u andere appliances om te beheren (die kunt u in een appliance-telefoonboek opslaan zodat u ze gemakkelijk kunt oproepen). Het Firewall-menu geeft u licentiebeheer, systeemconfiguratie, beheerwachtwoordinstellingen, hoge beschikbaarheid, en veilige configuratie. Bij deze laatste optie wordt de hele configuratie

tje voor staat, kunt u uitsplitsen in enkele subrubrieken.

Bij het opgeven van filterregels kunt u tien filterslots per policy definiëren, elk met hun eigen regels, tijdstellingen en prioriteit. Bij de IPS-configuratie kunt u alle mogelijke acties en responses bekijken en zo nodig wijzigen. De stateful inspectie van netwerkpakketten hoort hier ook bij. Het inhoudsfilter verzorgt

We begrijpen niet goed waarom SecPoint geen gewone firewallfunctionaliteit aan deze UTM toegevoegd heeft

versleuteld weggeschreven op een USB-sleutel. Die moet dan wel altijd in de UTM-appliance steken als die gestart wordt. Onder 'Maintenance' (onderhoud) kunt u uw beheerinstellingen back-uppen of herstellen, de firmware controleren en updaten, of de appliance herstarten of afsluiten. Het Applicatie-menu laat u het bewaak- of rapportageprogramma starten. Onder Opties kunt u enkele voorkeuringstellingen vastleggen voor het werken met de appliance. Het belangrijkste voor uw dagelijkse beheer vindt u onder deze menubalk: de rest van het applicatievenster is verdeeld in twee panelen. Een smaller menu-paneel links met aanklikbare UTM-menurubrieken en rechts daarvan een breder paneel dat een statusoverzicht bevat. Rubrieken waar een plusteken-

antispam, antivirus en URL-filtering. Het antispamgedeelte gebruikt zwartelijstservers op internet en eigen zwarte en witte lijsten. De instelmogelijkheden zijn eerder beperkt en we hebben deze antispamfunctie niet expliciet getest. De MFiltro 300 losse mail security appliance van NetASQ hebben we wél getest en die bleek uitstekend. De antivirusfunctie werkt samen met de proxyserverfuncties en controleert dus alles wat de appliance catcht ook op malware. Standaard is dat het geval voor pop3, smtp en nntp. Voor websurfen kunt u dat ook aanzetten, maar dat vertraagt de surfervaring natuurlijk nogal. Standaard gebruikt NetASQ ClamAV als antivirusmodule, maar mits een bijkomende licentie kunt u ook kiezen voor Kaspersky. De URL-filter werkt met

categorieën en raadpleegt daarvoor een NetASQ url-databaseserver. Er is een voorziening in de beheerinterface ingebouwd om een alternatieve URL-filterdatabase te raadplegen, maar die was tijdens onze test nog niet actief.

Praktijk

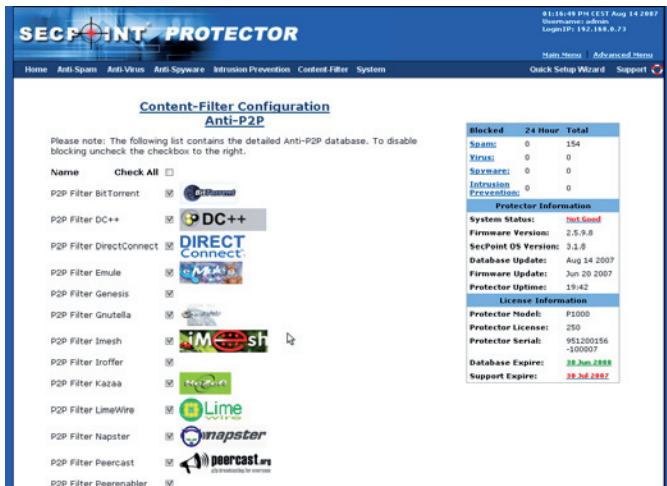
Deze NetASQ UTM F200 demonstreert duidelijk dat alle heil inzake beveiliging zeker niet van over de oceaan hoeft te komen. Deze Franse UTM-appliance werkt prima en biedt een gebruikersvriendelijke en veelzijdige Windows-beheerapplicatie. Bovendien is ze nog erg aantrekkelijk geprijsd ook!

SecPoint Protector P1000-250

Ook in Denemarken maakt men beveiligingsappliances en SecPoint komt daar vandaan. De Protector P1000 (de toevoeging -250 slaat op het aantal aangekochte gebruikerslicenties) is uitgevoerd in blauw en heeft vier netwerkpoorten. Helemaal links is er een lcd-paneeltje met bijbehorende bedieningstoetsen, maar in principe hoeft u dat zelden of nooit te gebruiken. De eerste netwerkpoort 'A' heeft een vast IP-adres 10.10.10.100 en zo kunt u dus altijd aan de beheerinterface, ook al weet u niet op welk IP-adres de appliance is ingesteld. De andere netwerkpoorten kunt u naar behoefte indelen. Een verrassing is, dat SecPoint een eigen antimalware-engine gebruikt. Het is echter mogelijk een alternatieve engine te laten gebruiken: u kunt kiezen uit ClamAV, Kaspersky of Norman.

Beheer en beveiliging

De webinterface van de SecPoint Protector zit vrij eenvoudig in elkaar. Bovenaan is er een balk met de hoofdmenurubrieken voor het dagelijks beheer: Home, Antispam, Antivirus, Antispyware, IPS, inhoudsfilter, systeem. Helemaal rechts bovenaan kunt u kiezen tussen dit hoofdmenu en een 'geavanceerd menu' met systeeminstellingen en activiteiten die bedoeld zijn voor het beheer van de appliance zelf. Onder Antivirus en Antispyware kunt u eigenlijk alleen 'aan of uit' kiezen (bij Antispyware kunt u individuele controles uitschakelen), maar normaal zult u dat allemaal aan laten staan. De hoofd-rubrieken vallen uiteen in 'pull-down'-menu's met soms uitgebreide opties,



Configuratie inhoudsfilter SecPoint.

maar vaak is het niet meer dan opties aan of uit zetten. Een kind kan bij wijze van spreken de was doen.

De SecPoint Protector heeft naast antispam ook volledige antimalware-onderschepping voor zowat alle protocollen aan boord en inhoudsfilters voor post en webverkeer. Veel van de beveiligingsopties zijn eigenlijk niet door uzelf instelbaar, buiten dan dat u ze kunt aan- of uitzetten. Dat maakt het beheer eigenlijk erg eenvoudig. Gewoon aanzetten en het werkt. Eigenaardig genoeg zijn er geen gewone firewallregels te vinden. De reden daarvoor is, dat deze UTM zich specialiseert in inhoudsfiltering. Als u specifieke firewallregels wilt kunnen instellen, zult u een aparte firewall moeten gebruiken. Er zitten natuurlijk wel firewallfuncties in, maar die hangen samen met de inhoudsfilters en de IPS. U kunt bijvoorbeeld niet zelf een DMZ definiëren en andere werkzones.

Praktijk

We begrijpen niet goed waarom SecPoint geen gewone firewallfunctionaliteit aan deze UTM toegevoegd heeft. Dat zou niet meer gekost hebben en de inzetbaarheid van deze appliance enorm hebben doen toenemen. De inhoudsfilters werken voorbeeldig en het spamfilter is zelfs uitstekend. In een afzonderlijke spamfiltertest scoorde deze spamfilter zelfs beter dan de absolute koning aller spamfilters, namelijk IronPort!

Deze test is tot stand gekomen op verzoek van het vakblad Infosecurity en staat los van de beurs Infosecurity.nl. VNU Exhibitions is dan ook niet aansprakelijk voor de inhoud.

CONCLUSIES

De in onze ogen meest indrukwekkende UTM-appliances in deze test zijn in volgorde de Fortinet FortiGate 300A, de SecPoint Protector P1000 en de Check Point UTM-1 2050. Houden we ook rekening met de prijs, dan gaat de titel van beste koop naar het Franse product NetASQ F200 en de tweede plaats wordt dan gedeeld door Fortinet en SecPoint.

TRULY
REVOLUTIONARY



Real Time Classificatie Van internet sites

Boek vandaag nog
een online demonstratie!

Maak kennis met
de Bloxx Tru-View
Technologie en zie
de toekomst van
webfiltering tijdens
Infosecurity 2007
op standnummer C098.

+31 (0)70 320 5009
info@bloxx-europe.com
www.bloxx.com



BEVOLGTONABVA
TRULY
REVOLUTIONARY

