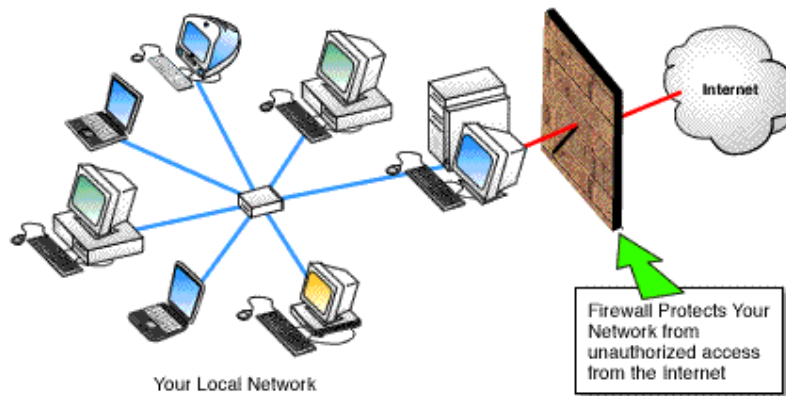


Wat is een firewall

Een firewall is een gateway die het verkeer regelt tussen verkeersstromen en netwerken, vaak tussen een intern bedrijfsnetwerk en het Internet. Firewalls kunnen tevens zorgen voor veilige gateway diensten tussen intern netwerk.

Bijvoorbeeld, een militaire installatie heeft 2 netwerken, één voor niet-geclassificeerde data, algemene verbinding en een ander netwerk die verbinding maakt met strategisch afweer systeem.

Een zeer betrouwbare firewall moet aanwezig zijn om er zeker van te zijn dat alleen bevoegde gebruikers toegang hebben tot het beveiligde netwerk. In sommige gevallen, is geen verbinding hebben nog het meest veilige beleid.



Kastelen en de verdediging ervan worden vaak gebruikt als een analogie in het beschrijven van firewalls. Een kasteel is ontworpen om de mensen die binnen in het kasteel zijn te beschermen tegen bestormingen van buitenaf. Er is in de omtrek van een kasteel een beveiligingssysteem dat dreigingen zo ver als mogelijk moet weghouden (door middel van muren, een gracht enz.). De poort van het kasteel is het "choke point" waardoor de mensen en bevoorrading het kasteel in of uit gaan. Het is het meest beveiligde, maar ook het meest kwetsbare gedeelte van het kasteel.

Een firewall is een "choke point" voor interne netwerken die verkeersstromen tussen netwerken actief controleert en regelt. In het geval van een proxy firewall, zal het verkeer nooit direct tussen de netwerken bewegen.

In plaats daarvan, deelt de proxy verzonden en ontvangen pakketjes opnieuw in.

Geen enkele interne host is direct toegankelijk vanuit het externe netwerk en geen enkele externe host is direct toegankelijk via een interne host. Denk aan de mensen in het kasteel.

Tijdens een aanval kunnen zij de voorkeur geven om binnenin het kasteel te verblijven en proxy agenten hun zaken aan de buitenkant aan te pakken.

Een deel van het ontwerp van een veilig Internet netwerk verbinding is ervoor om te creëren wat een "demilitarized zone" of DMZ heet. Dat is een netwerk dat bestaat uit het beveiligde en niet beveiligde netwerk.

De DMZ is beveiligd door een grenzend beveiligingssysteem, dat te vergelijken is met de buitenmuren en de gracht van het kasteel. Denk maar eens aan een marktplein in een kasteel.

In de middeleeuwen was het aan lokale mensen en handelaren meestal toegestaan om het kasteel relatief makkelijk binnen te komen, zodat ze goederen konden leveren of ophalen.

's Avonds waren de poorten gesloten en werden goederen naar het kasteel gebracht. Meestal na grondige inspectie.

Aan de poort stonden gedurende de hele dag bewakers om alle mensen die binnenkwamen te controleren. Als men op de hoogte was van hooligans (vandalen) die naar het kasteel kwamen dan werden ze onmiddellijk de andere kant op gewezen.

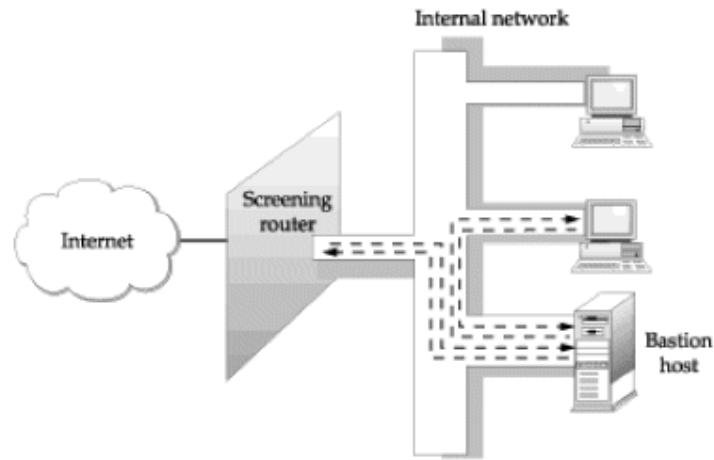
De DMZ tussen de beveiligde en niet beveiligde netwerken volgt deze analogie.

Internetgebruikers kunnen vrijuit de DMZ binnengaan om naar de publieke Web servers te gaan, maar routers schermen het toegangspunt af om ongewenst verkeer te filteren.

Ongewenst verkeer zoals stromen verkeer die hackers versturen, die daarmee proberen werkzaamheden te ontwrichten. Op hetzelfde moment is het interne privé netwerk beveiligd door zeer goede veiligheids firewall.

Binnen de kasteelmuren wisten ze het staande te houden

een zwaar verstevigd bouwwerk dat de laatste verdediging tegen aanvallers was.



Interessant was dat het kasteel beproefd was stand te houden voor een aanval, totdat er een kanon aan te pas kwam.

In de 16e eeuw overmeesterden Essex en Cromwell vele kastelen in Ierland met weinig krijgsmacht. Ze bliezen eenvoudig de borstwering van de top van de kasteelmuur af om zo de mensen in het kasteel onverdedigbaar te maken en vervolgens de muren met een ladder beklimmen.

Welk soortgelijk wapen zal onze netwerkverdediging tegenkomen?

Firewalls zijn behoorlijk geraffineerd geworden in de loop der jaren, maar ze zijn geen alles-in-één beveiligingsoplossing. Firewalls zijn een middel van beveiligings gereedschap beschikbaar voor beheerders. Merk het volgende op:

Een firewall kan uitgerust zijn met verschillende onderdelen, waaronder een router, een gateway server en een authentiek (authentication) server

Firewalls controleren binnenkomende en uitgaande verkeerstromen. Een firewall kan pakketten filteren, omleiden, opnieuw in pakken en verwijderen.

Verkeer kan gefiltreerd worden gebaseerd op hun bron en bestemmings IP adres, bron en bestemming TCP poort nummers, bits instellingen in de TCP rubriek, enzovoort.

In het geval van het gebruik van een proxy firewall, is de firewall het eindpunt van de inkomende en uitgaande connectie.

Het kan uitgebreide beveiliging en geldigverklaringen scannen tijdens het werken.

De proxy draait veilig, niet onderbroken met een bug-free versie van protocols en software.

Firewalls kunnen het veiligheidsbeleid van een organisatie versterken door middel van filteren van uitgaand verkeer van interne gebruikers om er zeker van te zijn dat ze zich aan het beleid houden.

Hoogwaardige logs, toezicht en inbraak detectie zijn nu een onderdeel van de meeste commerciële firewalls.

RFC 2979, "Behavior of and Requirements for Internet Firewalls," (oktober 2000) ("gedrag van Internet firewalls en de benodigdheden ervoor,") beschrijft andere firewall eigenschappen.

Hackers en andere aanvallers worden steeds slimmer, agressiever en het worden er ook steeds meer. In 2000 kondigde China aan dat ze niet konden meekomen met de Verenigde Staten qua militaire krachten, en dreigde met een "cyber" oorlog met de Verenigde Staten.

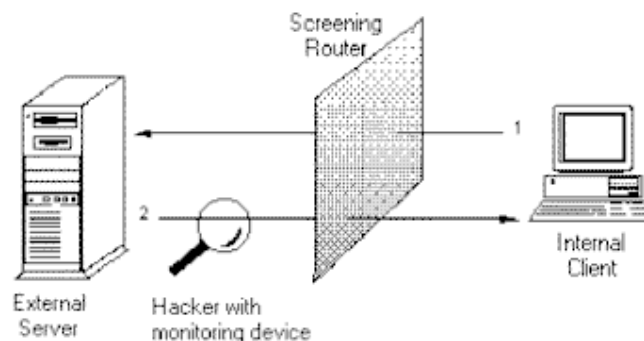
Computersystemen van de Verenigde Staten liggen onder een constante aanval door geraffineerde en ongeraffineerde aanvallers.

Hoeveel onbetrapte indringers zitten in deze systemen?

Bijvoorbeeld, een aanvaller zet van tevoren een aanval via een virus in een e-mail op, om zogeheten "zombie" programma's op honderden of misschien wel duizenden computers van onschuldige Internetgebruikers te zetten, velen in uw eigen netwerk.

De programma's zijn ingesteld om op specifieke tijden andere systemen aan te vallen.

De echte aanvaller kan niet geïdentificeerd worden omdat de aanvallen vanuit onschuldige gebruikers over het gehele Internet komen. Het gehele Internet kan een wapen worden dat gericht is op uw privé-netwerk.



Vanwege deze dreigingen, zijn firewalls nu nodig in bijna iedere computer die verbinding maakt met het Internet, vooral voor de computers van "altijd-aan" diensten, zoals DSL en kabel (CATV) verbindingen. Een typische thuisinstallatie is om een netwerkverbinding te maken tussen een ouder z'n computer en een kind z'n computer, om zo één DSL of kabel verbinding met het Internet te delen.

Sinds de verbinding altijd aan is, heeft het altijd hetzelfde IP adres dat als een vlag op het Internet staat. Hackers zullen uiteindelijk het IP adres vinden en zullen terug komen om systemen na te kijken en te verstoren. Firewalls zijn ontworpen om deze systemen te beschermen gedurende het minimaliseren van complex installatie procedures.

Firewall Terminologie

Een standaard firewall terminologie helpt het verwijderen van de verwarring van omliggend firewall technologie. RFC 2647, "Merkteken Terminologie voor Firewall Prestatie," (augustus 1999) is een document dat probeert deze terminologie vast te stellen.

(De meest belangrijke termen die het beschrijven staan hier weergegeven).

U wordt verwezen naar de RFC voor een meer complete omschrijving.

De volgende lijst is geordend voor duidelijkheid en is herschreven om de leesbaarheid te bevorderen.

Firewall » Een apparaat of een groep apparaten die een toegang controle beleid toepassen tussen netwerken.

Firewalls verbinden beveiligde en niet beveiligde netwerken, of ondersteunen tri-homing, welke een DMZ netwerk toelaat.

Beveiligd netwerk » Netwerksegment of netwerksegmenten waarbij toegang wordt gecontroleerd. Beveiligde netwerken worden soms "interne netwerken" genoemd, maar RFC 2647 zegt dat de term niet toepasselijk is omdat firewalls zich meer en meer ontplooiën binnen een organisatie, waar alle segmenten per definitie intern zijn.

Niet beveiligd netwerk » Een netwerksegment of netwerksegmenten waarbij toegang niet wordt gecontroleerd door een firewall.

Demilitarized zone (DMZ) » Een netwerksegment of netwerksegmenten die tussen de beveiligde en niet beveiligde netwerken zitten

De DMZ mag geen verbinding maken met het beveiligde netwerk op welke manier dan ook.

De DMZ mag ook een afweer systeem bevatten. Bijvoorbeeld, de DMZ kan gemaakt zijn om het erop te laten lijken dat het een onderdeel van het beveiligde netwerk is, om op deze manier hackers in de val te lokken en hun activiteiten vast te leggen om zo te proberen de bron te vinden.

Dual-homed firewall » Een firewall met twee interfaces, één in het beveiligde netwerk en één voor het niet beveiligde netwerk.

Tri-homed firewall » Een tri-homed firewall verbindt drie netwerk segmenten met verschillende netwerk adressen. Natuurlijk zijn dit beveiligde, DMZ, en niet beveiligde segmenten.

Proxy » een aanvraag voor een verbinding bij een host. Een proxy zit tussen een beveiligd en niet beveiligd netwerk.

Denk aan een quarantainegebied waar mensen binnen in zitten die een telefoon gebruiken om mensen buiten dat gebied te bellen.

Het leidt alle externe verbindingen naar de proxy om deze te beëindigen in de proxy.

Dit beëindigt de IP routing tussen de netwerken effectief. De proxy zet de berichten in nieuwe pakketten die toegestaan zijn in het interne netwerk. De proxy stopt ook het interne verkeer dat richting het Internet gaat en pakt het in nieuwe pakketten met de bron IP adres van de proxy, niet de interne host. Het belangrijkste is dat de proxy het verkeer inspecteert en filtert. Een regel die van tevoren bepaald is, is welk verkeer doorgelaten moet worden en welk geblokkeerd moet worden.

Er zijn twee soorten proxies: application proxies en circuit proxies

Zoals kortweg omschreven.

Network address translation (NAT) » een methode van archiveren die min of meer privé gereserveerd IP adres naar een meer openbaar IP adres verandert.

De NAT werd eerst beschreven als een methode om IPv4 adressen te behouden en te verwijzen naar een specifiek blok van IP adressen dat nooit herkent of door routers gezien zou worden op het Internet.

Het laat organisaties toe om hun eigen interne IP adressen schema te gebruiken. Een NAT systeem vertaalt tussen interne en externe adressen, en is meestal gecombineerd met proxy service. NAT systemen zijn toepassingen in firewalls om het privé adres schema zoals in de RFC 1918 te ondersteunen.

Application proxy » Een proxy service die gestart en gestopt wordt na aanleiding van een aanvraag van een client, in plaats van een statische proxy service (die altijd gestart is).

De toepassing proxy vervuld alle diensten van een proxy, maar voor specifieke toepassingen

Ter contrast, een basis proxy voert algemene pakketfiltering uit. De toepassing proxy verwerkt alleen pakketverwante toepassingen die het ondersteunt. Wanneer een code niet is geïnstalleerd voor een toepassing, worden de inkomende pakketten geweigerd. Pakketten worden alleen toegelaten als er een verbinding is gemaakt, bij die pakketten wordt gekeken of ze bevoegdheid hebben.

Circuit proxy » Een proxy die statisch bepaald welk verkeer door gelaten wordt.

De circuit proxy is een speciale functie uitgevoerd door application proxies, meestal om de proxyverbinding tussen interne gebruikers en externe hosts te ondersteunen.

De pakketten worden doorgestuurd zonder dat ze gefiltreerd wordt en omdat pakketjes van vertrouwde interne gebruikers afkomstig zijn, en op weg zijn naar het externe netwerk.

Hoe dan ook, pakketten die terug komen als reactie op deze pakketten worden volledig nagekeken door de proxy toepassing diensten.

Policy/beleid » Een bepaald document dat weet wat geaccepteerd moet worden in beveiligde, DMZ, en niet beveiligde netwerken.

Rule set » Alle regels over toegangscontrole, welk pakket wordt doorgestuurd en welk wordt geblokkeerd.

Toegelaten verkeer » pakketten die doorgegeven worden op grond van de regels.

Illegaal verkeer » Pakketten die geblokkeerd worden ten gevolge van de regels.

Geweigerd verkeer » Pakketten die geblokkeerd worden ten gevolge van de regels.

Authenticatie » Het proces van het verifiëren dat een gebruiker die een network-bron aanvraagt, is wie hij of zij claimt te zijn. De partij die geauthenticeerd wordt kan een computer zijn of een gebruiker, dus authenticatie kan o.a. plaats vinden op basis van IP-adres, TCP of UDP poortnummers, wachtwoorden, en andere vormen van identificatie, zoals bijvoorbeeld biometrische identificatie.

Security association » de reeks van beveiligingsinformatie verwant aan een gegeven netwerk verbinding of reeks van verbindingen. Deze omschrijving geeft de relatie aan tussen het beleid en de verbindingen. Associatie kan voorkomen tijdens het verbinding maken, en ze kunnen ook herhalen of verzakken tijdens een verbinding.

Pakket filtering » het proces van het controleren van de toegang door pakketten te onderzoeken gebaseerd op de inhoud van de headers. Header informatie, zoals IP adres of TCP poort nummer worden onderzocht om te kijken of deze doorgestuurd moeten worden, of zouden moeten worden geweigerd, gebaseerd op een aantal regels.

Stateful packet filtering » het proces van het doorlaten of blokkeren van "verkeerd gebaseerd" op de "state table" die wordt bijgehouden door de firewall. Wanneer stateful filtering wordt gebruikt, worden pakketjes alleen doorgestuurd als ze toebehoren aan een verbinding die al tot stand is gekomen en die wordt bijgehouden in de state table.

Logging » het vastleggen of een gebruiker verbinding heeft geprobeerd te maken met de firewall. Alle aanvragen worden op volgorde gelogd, zoals toegelaten, illegaal of geblokkeerd verkeer. Een inbraak-detectie-systeem houdt actief toezicht op de toegangspunten om hackers en hun aanvallen tegen te houden.

SOCKS is een circuit-level proxy firewall service die TCP/IP hosts van een veilig kanaal probeert te voorzien, typisch een web cliënt op een intern bedrijfs netwerk die zich met een buitenstaande web server wil verbinden (op het Internet, op het netwerk van een andere organisatie, of op een ander gedeelte van het intranet). SOCKS levert firewall services, zo ook doorlichting, management, fouttolerantie, en andere karaktereigenschappen. De meeste firewalls voeren authenticatie uit om de identiteit van de gebruiker of processen te verifiëren.

RADIUS wordt vaak gebruikt als authenticatie-service. Het is dezelfde authenticatie-service die wordt gebruikt bij netwerkverbindingen via de telefoon bij bedrijfsnetwerken en Internet-service-providers (ISP). Op basis van gebruikersnaam kan met specifieke gebruikers wel toelaten en anderen niet. Moderne firewalls ondersteunen ook VPN's, die een veilige tunnel tussen een firewall en een gebruiker op afstand voorziet op het Internet.

De firewall authenticeert de gebruiker, codeert alle data, en verzekert data-integriteit door het gebruik van digitale handtekeningstechnologie.