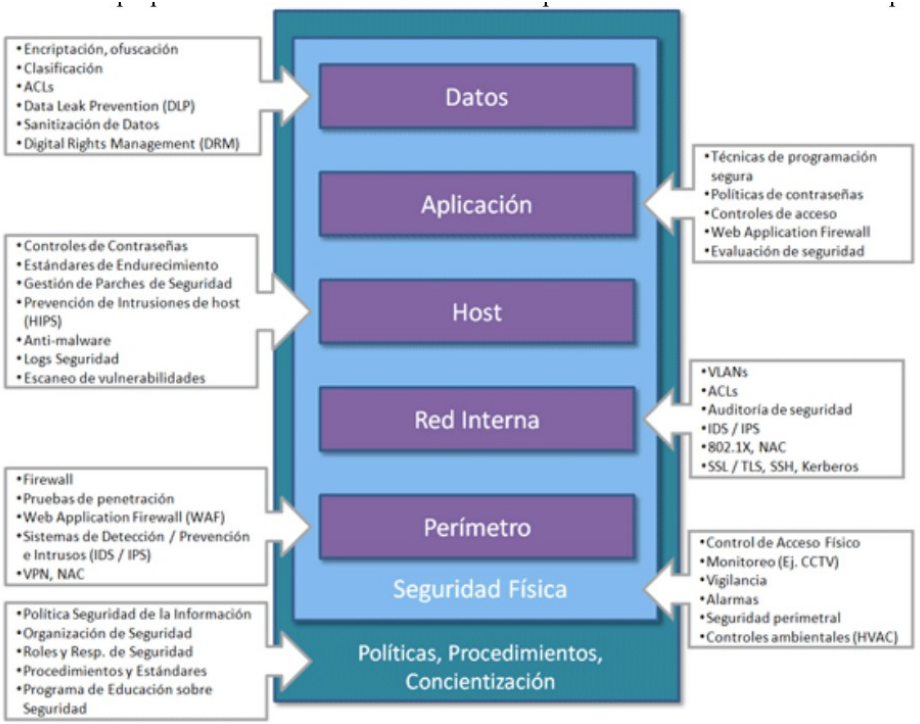
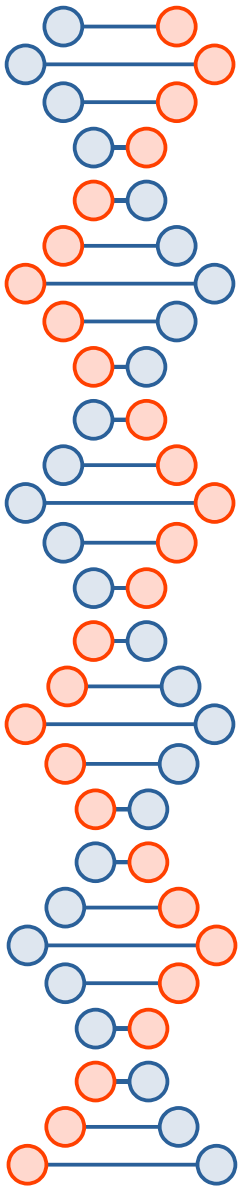
Firewalls e Arquitecturas de Rede

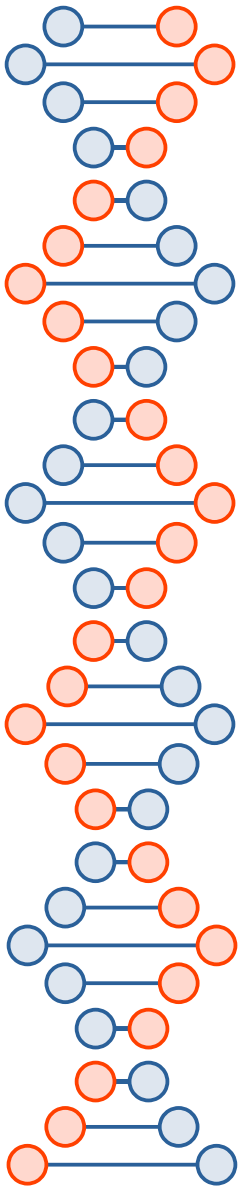
- Os firewalls forman parte das arquitecturas de **defensa en profundidade**, encargándose principalmente de filtrar (permitir ou denegar) o tráfico de datos dende ou hacia a rede protexida.





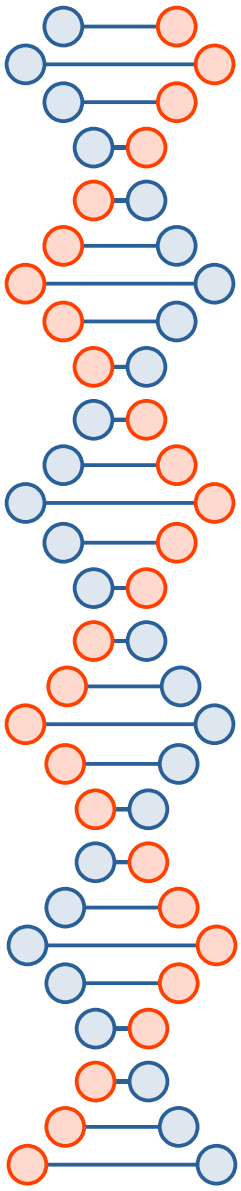
Conceptos Xerais

- Un firewall é un dispositivo formado por un ou varios equipos que se sitúan entre a rede a protexer e a rede exterior encargado de analizar todos os paquetes de datos que transitan entre ambas as dúas redes e filtrar os que non deben ser reenviados de acordo aos criterios establecidos.
- O análise dos paquetes se realiza en función de:
  - A procedencia
  - O destino
  - O protocolo
  - O Contido
- Mediante un firewall podemos illar as aplicacións, servizos e máquinas da rede interna do tráfico entrante non desexado e limitar ou cortar o acceso dos equipos da rede interna aos servizos ofertados en redes externas.
- Os firewalls tamén se utilizan para establecer varios ámbitos de uso na mesma organización.



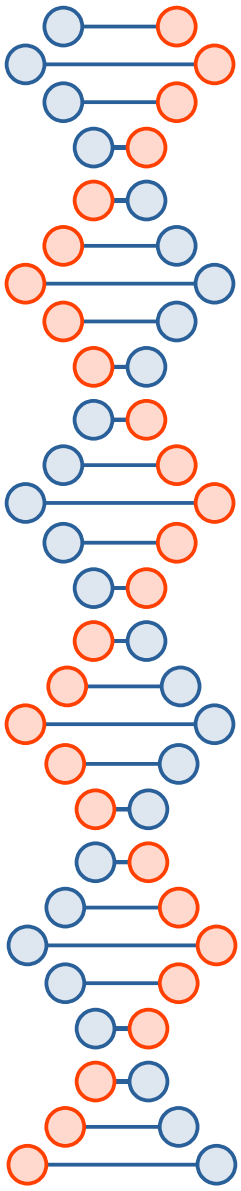
As Regras do Firewall

- As políticas de control de acceso establecidas nun firewall se indican mediante regras (rules) creando conxuntos de regras (rulesets). Cada regra identifica un determinado tipo de paquete e a acción a realizar.
- A configuración dun firewall consiste na creación do ruleset apropiado para as políticas de acceso que desexamos implantar



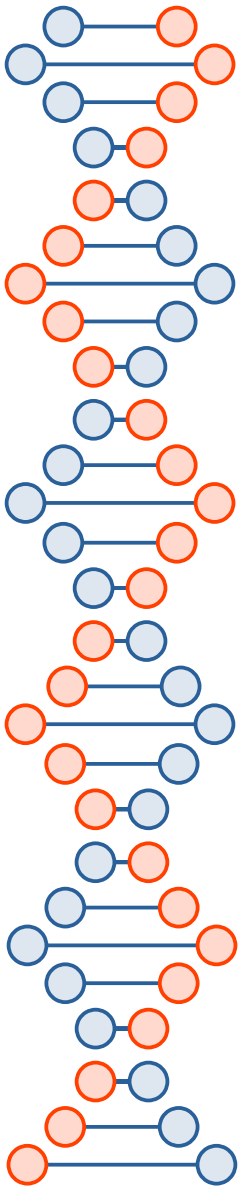
Tipos de Firewall

- Segundo o ámbito de aplicación
  - Firewall de Rede
  - Firewall de Host ou de Sistema
- Segundo o nivel de rede sobre o que traballan
  - Firewalls de Nivel de Rede: Analizan os valores dos datagramas IP, segmentos TCP e datagramas UDP. Os firewalls deste nivel son capaces de facer NAT. Podemos distinguir dous subtipos:
    - Filtrado sen estado: Se analiza cada paquete de xeito independente sin ter en conta o estado das conexións a nivel de transporte.
    - Filtrado con estado: Se pode ter en conta o estado do paquete para realizar o filtrado utilizando unha táboa de estado e permitindo distinguir os paquetes dunha mesma conexión en función do seu estado (inicio de conexión, pertencente a unha conexión...)
  - Firewalls de Nivel de Aplicación: Traballan no nivel de aplicación funcionando realmente como proxys entre a rede segura e a rede insegura. Exemplos de firewall de aplicacion son os WAF (Web Application Firewall), ou proxys de propósito xeral como Squid ou HAProxy.



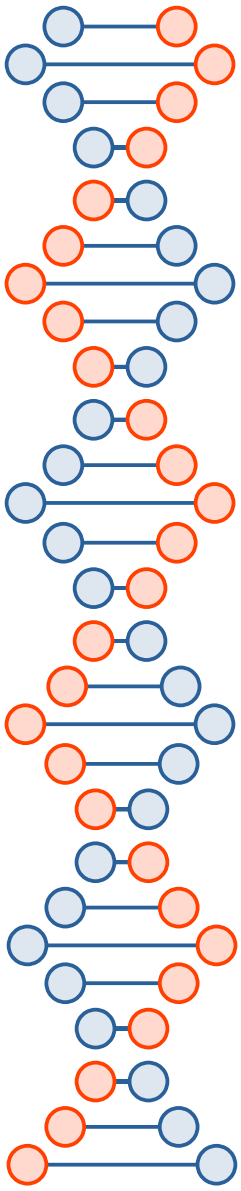
Arquitecturas de Rede I

- Router-Firewall: A organización sae a Internet a través dun router que se encarga tamén do análise e filtrado do tráfico. É común no ámbito SOHO (Small Office – Home Office) onde non se ofrecen servizos de internet ou estes son moi básicos.
  - As posibilidades dos firewall dos router son moi limitadas
  - A función de filtraxe sobrecarga a capacidade de procesamento do router o que pode reducir a velocidade do tráfico
  - Si o router é comprometido queda exposta toda a organización
- Host bastión: Todo o tráfico do router se redirixe a unha máquina denominada “host bastión” que está especialmente asegurada e realiza as funcións de filtraxe . Tamén é común no ámbito SOHO
- DMZ ou Zona Desmilitarizada: Se define unha zona especial da rede que será accesible dende o exterior separada da rede da organización. A rede da organización en ningún caso podería ser accedida dende equipos situados fora da mesma.
  - Os servidores da DMZ non deberían poder iniciar conexións co exterior.
  - Si necesitamos distintos graos de protección podemos facer un deseño multi-DMZ empregando varios firewalls, isto nos permite colocar na DMZ interna os equipos que queremos facer accesibles dende a DMZ externa sen comprometer toda a rede.
  - Tamén podemos aillar os distintos equipos da DMZ utilizando VLAN de modo que o compromiso dun equipo non afecte ao resto.



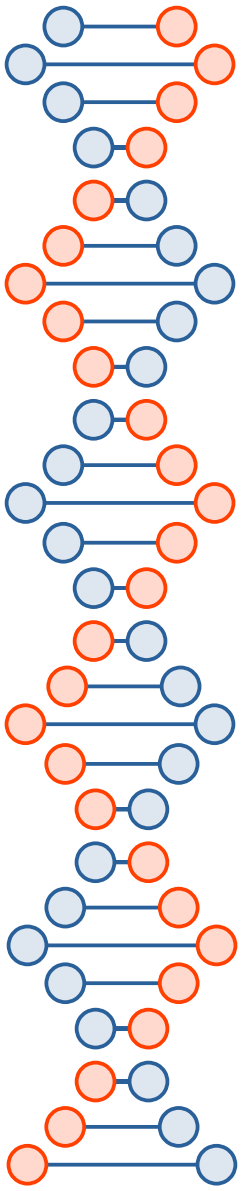
Arquitecturas de Rede II

- Sempre debemos ter en conta que:
  - Non existen tecnoloxías infalibles
  - Poden existir erros de configuración
  - As veces e necesario debilitar a seguridade en pro da funcionalidade
  - E completamente seguro que nalgún momento algunha parte da nosa infraestrutura se vexa comprometida
- Debido aos puntos anteriores debemos establecer múltiples capas de seguridade e non confiar nos firewalls como o único dispositivo para garantir a seguridade. Os principios a seguir na configuración son:
  - Principio do minimo privilexio
  - Adecuación de necesidades e risco
  - Aseguramento do control de acceso
  - Separación dos servizos
  - KISS (Keep It Simple, Stupid)
  - Escalabilidade
  - Redundancia
  - Complementaridade tecnolóxica



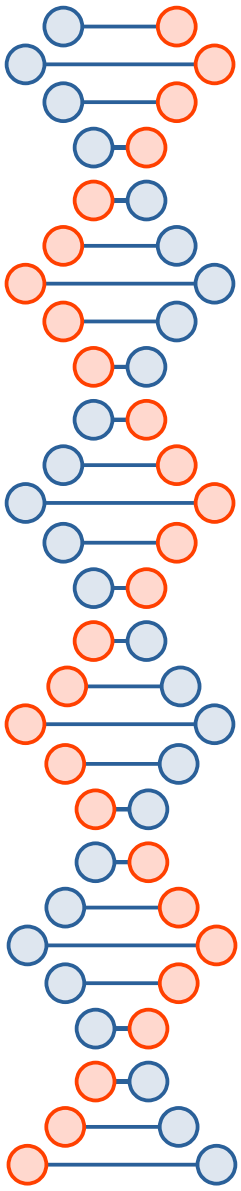
Software vs Appliance (Dispositivo Adicado)

- Ventaxas dos Appliance:
  - Máis simples de instalar e configurar xa que dispoñen de asistentes e interfaces específicamente deseñados.
  - Están optimizados a nivel de hardware para realizar a súa función
- Ventaxas do Software:
  - Precisan dun investimento inferior
  - Son moito máis flexibles no seu uso
- Os sistemas encargados de xestionar a seguridade das redes se denominan UTM (unified threat management).



NAT (Network Address Translation)

- O NAT consiste en alterar a dirección IP do paquete (orixe ou destino), o porto de destino ou ambas cousas.
  - NAT básico: Se modifica únicamente a IP. Pode ser SNAT si modificamos a dirección de orixe do paquete ou DNAT si modificamos a dirección destino
  - NAPT / PAT: Se modifica tamén o porto TCP ou UDP de destino.
- Esta traducción pode facerse de xeito estático ou dinámico. No NAT dinámico se dispón dun pool de direccións que se van asignando sobre demanda de xeito dinámico, mentras que no estático se realiza unha correspondencia fixa.
- O “Masquerading” e un tipo de NAT no que se traduce a dirección de orixe do paquete saínte pola dirección IP da interface pola que se sae. No caso en que a dirección da interface sexa dinámica non é posible facer un SNAT estático normal sendo necesario especificar “masquerading”



Firewalls

- PfSense
  - Pfsense é unha distribución especializada do sistema UNIX FreeBSD para o seu uso como Firewall e Router proporcionando un panel de xestión web simple. Ademáis das fucións básicas de router/firewall nos permite a creación de VPN, facer balanceo de carga, portal cautivo, servidor DNS e DHCP, proxy Squid, Snort, ClamAV..... etc.
- NetFilter
  - NetFilter é a infraestructura de filtrado de paquetes do Kernel Linux. Esta infraestrutura de filtrado é xestionada mediante a utilidade **iptables** ou a mais moderna **nftables**.
- Ufw
  - Ufw é unha aplicación que permite a construcción de firewalls sobre Netfilter de xeito sinxelo. Dispón de utilidades gráficas como **gufw**
- Fwbuilder
  - Fwbuilder non é un firewall. É unha aplicación que nos permite deseñar regras de firewall e exportalas en diversos formatos como iptables/netfilter, freebsd ou para firewalls Cisco.