Il firewall Clavister a Ferrara

- Dal 2006 utilizzavamo il software Clavister CorePlus, che gira su pc commodity, in configurazione HA (2 pc con un collegamento dedicato tra loro per la sincronizzazione) e senza feature aggiuntive;
- Nel 2013 Clavister ha cessato la versione per hardware reale ed introdotto quella per VM Vmware (Clavister Cos);
- Contemporaneamente ha anche cambiato le opzioni di licenza: base (solo aggiornamenti) o con tutte le funzionalita' avanzate;
- Queste ultime consistono di: antivirus, Web Content Filtering (WCF) e Intrusion Detection & Prevention (IDP).

Si e' optato per una coppia di macchine ed una di licenze avanzate, con manutenzione triennale.

Virtualizzazione

La virtualizzazione impone qualche vincolo in piu':

- le interfacce virtuali sono collegate da switch virtuali, entrambi vanno configurati correttamente se si utilizzano funzionalita' di bridging, vlan;
- l' hypervisor ha un suo indirizzo e deve poter essere raggiungibile;
- I mac address delle VM debbono essere scelti in un range statico;
- la sincronizzazione dei due firewall utilizza un protocollo proprietario (e un poco particolare).

Feature avanzate:

- **Antivirus**: si tratta di Kaspersky SafeStream e puo' essere applicato solo ai pacchetti SMTP, POP3, FTP e HTTP;

- **Web Content Filtering**: le URL delle pagine richieste dall' utente vengono inviate a Clavister, che le confronta con un elenco restituendo la categoria di appartenenza. In questo modo il firewall puo' “filtrare per categorie”.
  Problemi:
  - privacy;
  - e' necessario poter raggiungere i server di Clavister perche' il filtraggio funzioni...;
  - l' appartenenza ad una categoria e' una scelta di Clavister, non del gestore, anche se ci sono black e white list;
  - dipende anche da quanti siti ha censito Clavister;

IDP

- L' idp consiste di un elenco di segnature relative a varie vulnerabilita', le segnature vengono utilizzate per effettuare match di pacchetti a livello di singolo protocollo applicativo. Percio' occorre specificare comunque un insieme di regole composte da sorgente/destinazione, porte UDP/TCP e vulnerabilita' da cercare.
- Occorre che l' elenco delle segnature sia aggiornato;
- occorre che le regole siano specificate;
- non c'e' una analisi dei comportamenti anomali;
- l' elenco delle vulnerabilita' e' presente alla URL: https://forums.clavister.com/securityportal/advisories/

Considerazioni finali

Pro:

- ridottissimo consumo di risorse
- packet firewall performante
- soluzione economica
- qualche feature insolita (p.es. pcap, proxy arp, link-based routing, server load balancing)

Contro:

- Le funzionalita' avanzate debbono essere configurate esplicitamente, non sono “plug-and-play”;
- non ci sono alcuni aspetti solitamente associati ai firewall NG: deep packet inspection, anomalies detection, SSL decryption, etc
- il ridotto consumo di risorse impone qualche limite ai parametri di funzionamento