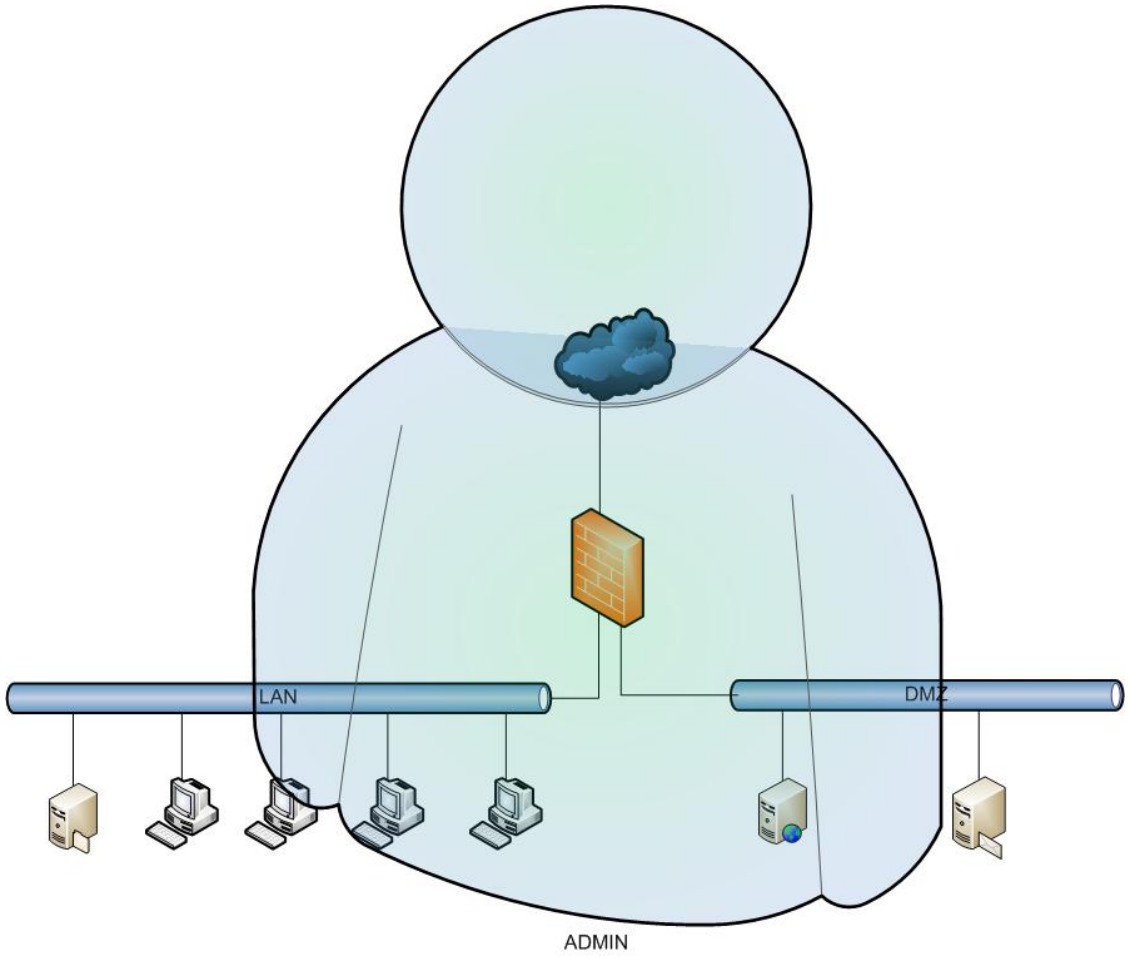
Open Source Tools for Network Access Control

Sicurezza e usabilità per ambienti di rete BYOD

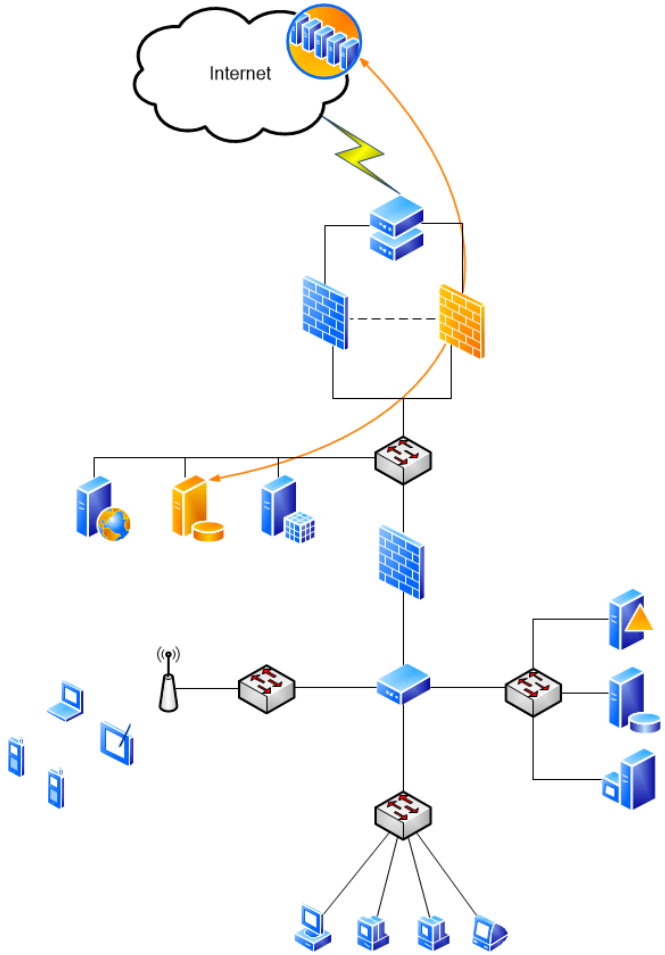
Esempio di rete (tradizionale)



Esempio di rete (tradizionale)

- Layout ben definito
- Numero di end point ben definito
- Architetture hardware e software omogenee
- L'amministratore controllava TUTTO
  - Hardware di rete
  - Sistemi operativi
  - AV/Patch Management
  - Software installati

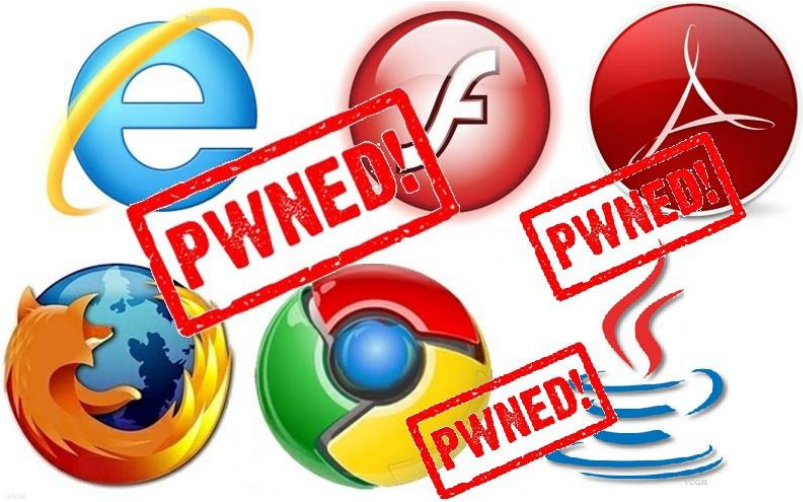
Esempio di rete (BYOD)



Esempio di rete (BYOD)

- Layout definito solo a livello macroscopico
- Numero di end point variabile
- Architetture hardware e software eterogenee
- L'amministratore controlla SOLO LA RETE
  - Nessun controllo sugli end point degli utenti
  - Sistemi AV sconosciuti / patch management assente
  - Potenziale accesso da parte di sistemi ostili

Le Conseguenze



Conseguenze (2)

Admin Tribute

Admin Tribute

Dove?

Dove?

Scuole

- Computer portatili degli insegnanti
- Tablet / ebook degli strudenti
- Smartphone con accesso ad internet

PMI

- Computer portatili dei dipendenti
- Smartphone
- Tablet
- Dispositivi degli ospiti che necessitano di accedere ad internet

Possibili soluzioni?

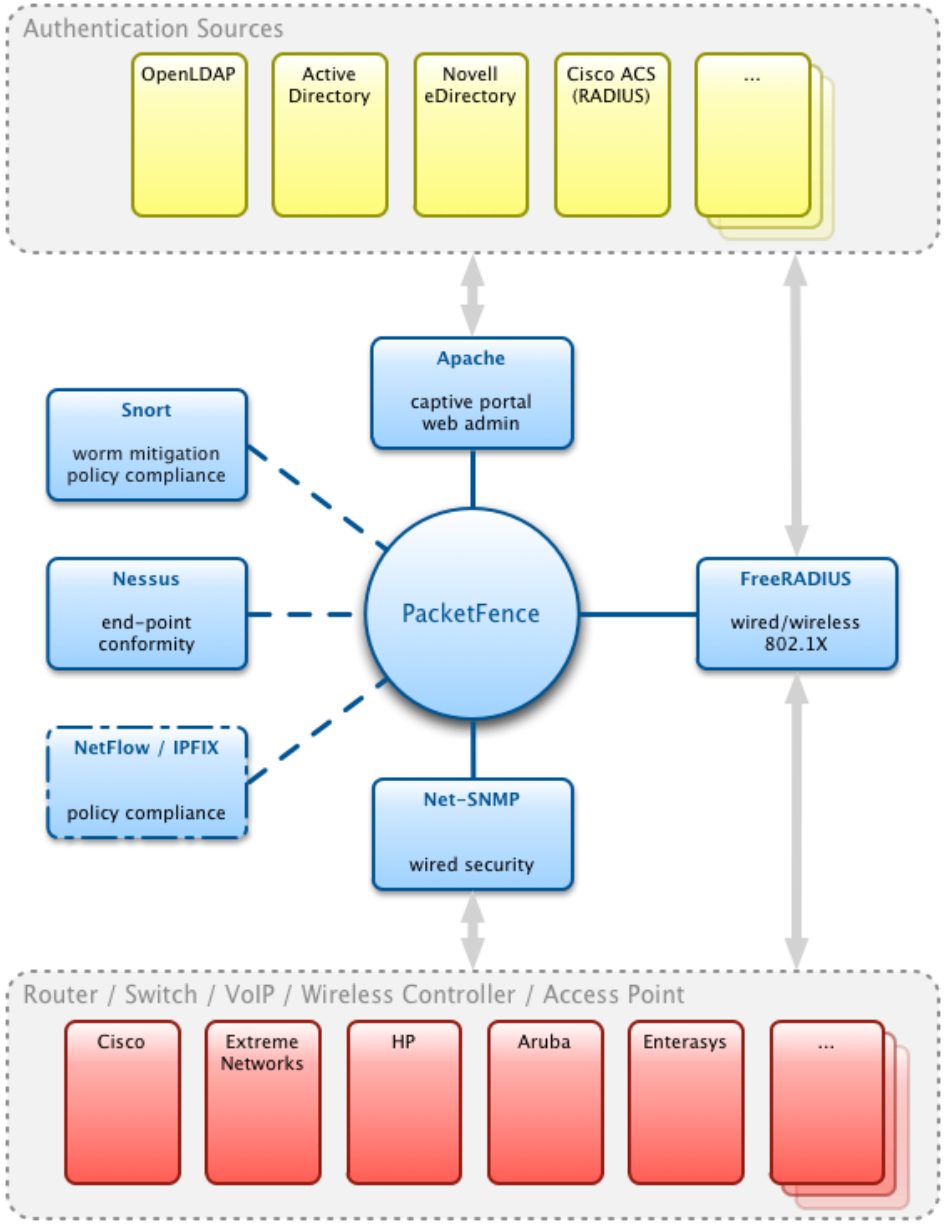
Agire in modo intelligente a livello di rete per sopperire alla mancanza di controllo sugli end point.

Network Access Control (NAC)

Una soluzione per definire e implementare policy che rendano sicuro e controllabile l'accesso alle risorse di una rete da parte dei dispositivi collegati.

Come si implementa

- User Authentication
- End Point Identification & Fingerprinting
- Policy Enforcement
- End Point Compliance
- Web Content Filtering
- Intelligent & adaptive real time network device reconfiguration

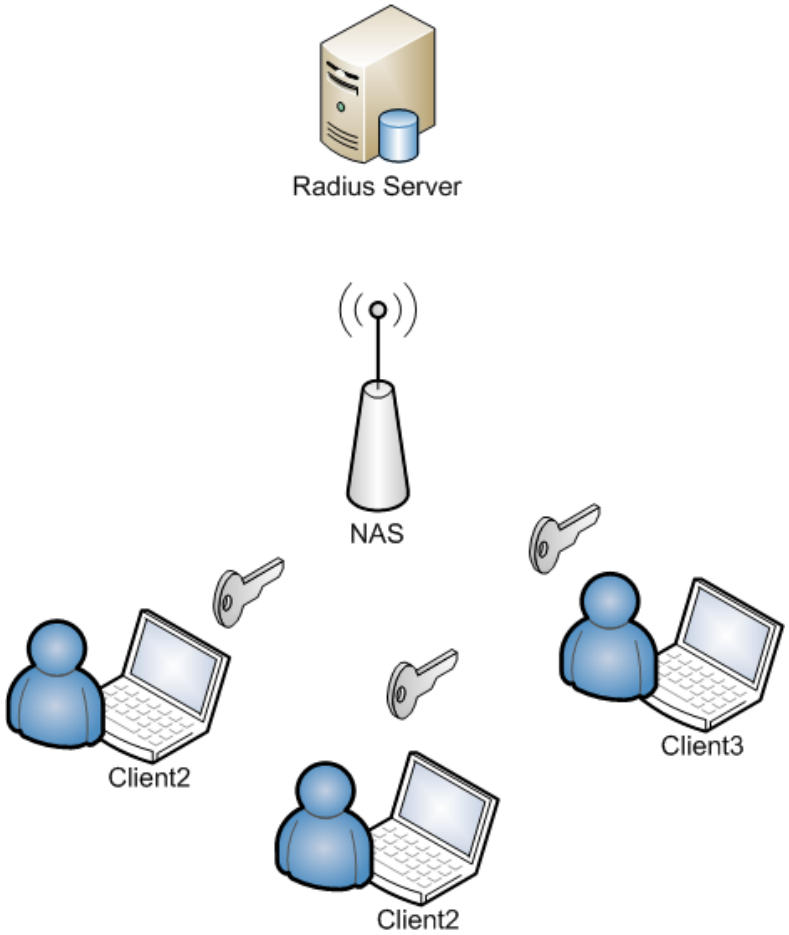

Authentication Sources
OpenLDAP
Active Directory
Novell eDirectory
Cisco ACS (RADIUS)
...
Apache
captive portal
web admin
Snort
worm mitigation
policy compliance
Nessus
end-point
conformity
NetFlow / IPFIX
policy compliance
PacketFence
FreeRADIUS
wired/wireless
802.1X
Net-SNMP
wired security
Router / Switch / VoIP / Wireless Controller / Access Point
Cisco
Extreme Networks
HP
Aruba
Enterasys
...

FreeRADIUS

- Servizio di AAA (Authentication Authorization and Accounting)
- Utilizzato per l'autenticazione degli utenti su reti wireless (ma anche cablate)
- WPA/WPA2 Enterprise
- 802.1X
- Layer 2 Security

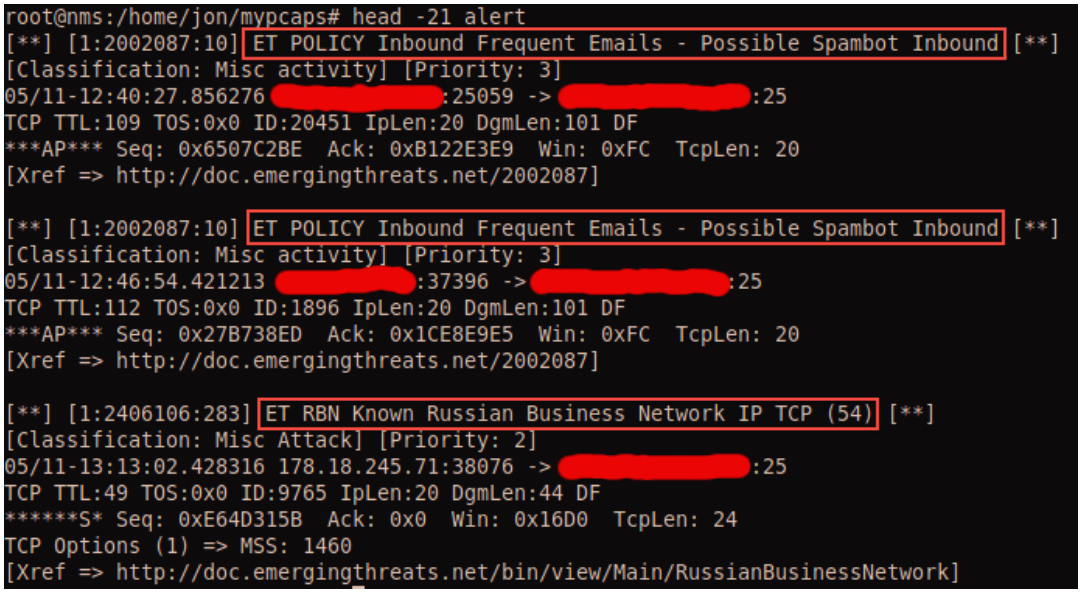
FreeRADIUS

- Il client invia le proprie credenziali di accesso al NAS
- Il NAS trasmette le credenziali al server RADIUS
- Il server RADIUS verifica eventuali criteri di restrizione (check) aggiuntivi
  - Orario di accesso
  - Appartenenza ad un gruppo
  - …
- Il server RADIUS conferma/nega l'accesso comunicando al NAS eventuali policy da forzare al client
  - Limiti di banda
  - VLAN di appartenenza
  - IP/Netmask/gateway



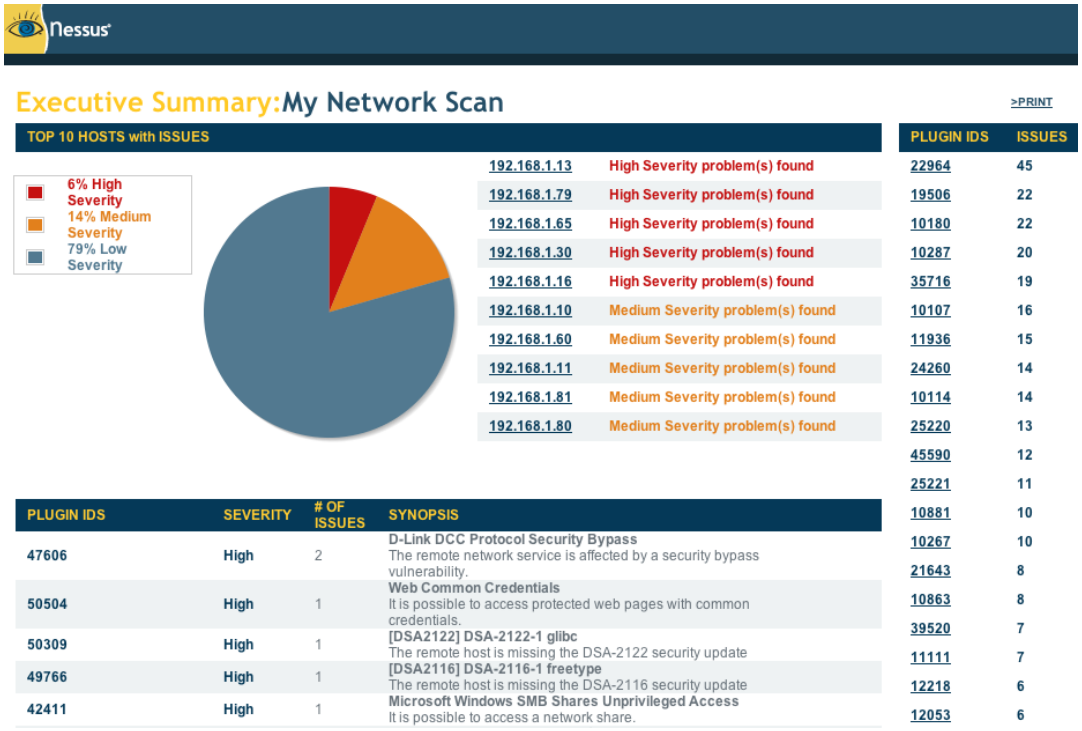
Snort/Suricata

- Intrusion detection system
- Deep Packet Inspection
- Network Traffic analysis
- Anomaly Detection
- Malware Mitigation
- Client Isolation



Nessus/openVAS

- Scansione attiva dei dispositivi connessi in rete
- Identificazione di sistemi non patchati
- Scansione dei servizi e dei relativi livelli di aggiornamento
- Fingerprinting dei dispositivi
  - iOS
  - Windows
  - Mac OS
  - Linux
  - Android
- End Point Conformity
- End Point Isolation



Content Filtering

In molti ambienti, soprattutto quelli scolastici è fondamentale poter discernere sul tipo di contenuto che gli utenti possono andare a consultare anche all'esterno del perimetro della rete locale.

Content Filtering (Requisiti)

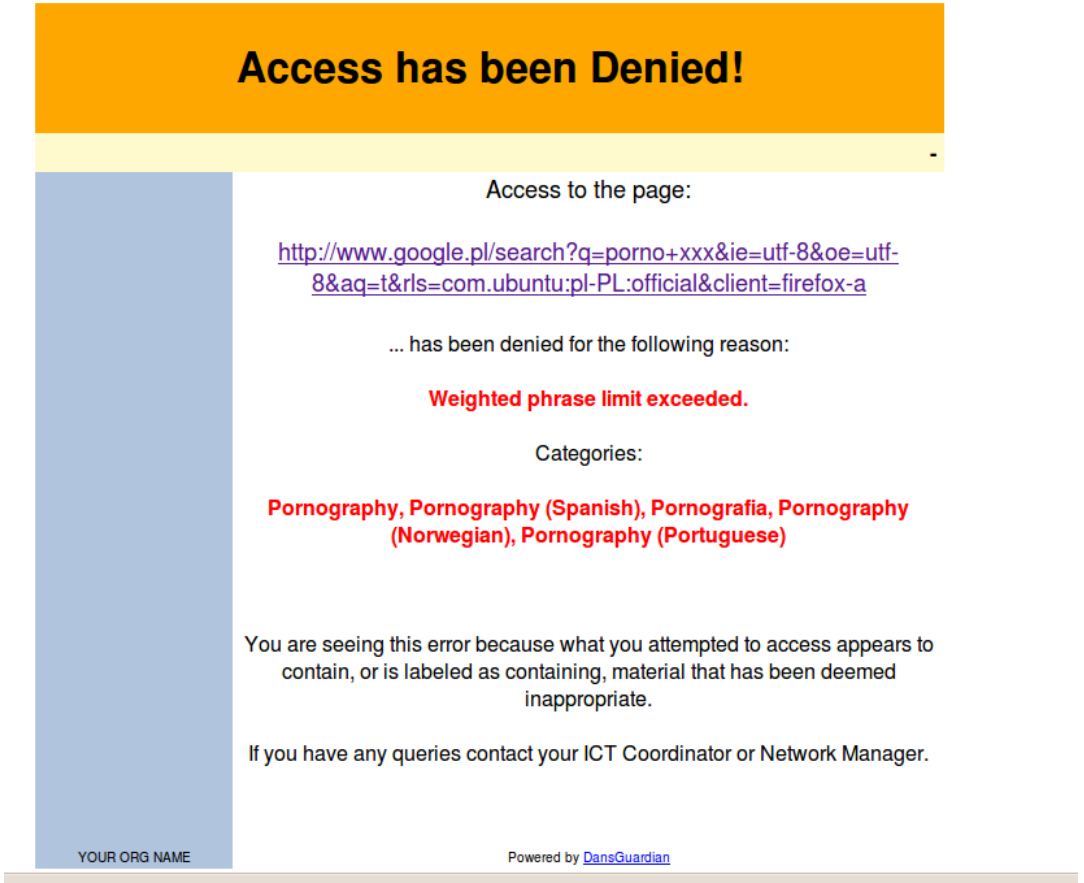
- Possibilità di filtrare il contenuto delle pagine web ed eventualmente bloccare pagine non appropriate
- Differenziazione per utente
  - Studente != Insegnante != Segretario != Dirigente
  - Le informazioni accessibili devono essere filtrate in maniera differente.
- Plug & Play
  - Nessuna configurazione sui client.

Dansguardian: Pro

- Supporta black/white list per domini e url
- Blocco di estensioni
- Blocco di mimetype
- Analisi semantica del contenuto delle pagine (Deep Content Inspection)
- In base al risultato dell'analisi del contenuto CATALOGA la pagina assegnandola ad una specifica categoria.

Dansguardian: Cons

- Necessita di appoggiarsi ad un proxy
- Non è in grado di autenticare in maniera autonoma gli utenti, li può solo categorizzare



Transparent Squid

Pros

- Zero Configuration sui client
- Nessuna possibilità di evasion

Cons

- Qualsiasi proxy in transparent mode non può fare autenticazione

Senza Autenticazione dansguardian non può riconoscere gli utenti e quindi non è possibile applicare filtri personalizzati per utenti/gruppi
Per avere l'autenticazione il proxy va configurato manualmente nel browser

Remember?

Soluzione?

- Si patcha Dansguardian aggiungendo un plugin di autenticazione extra
  - Plugin di autenticazione SQL
  - Legge i dati delle autenticazioni dalla tabella di accounting RADIUS
  - Sviluppato da terze parti facendo fork del codice originale del progetto
  - Possibile perché il software è open source

Concludendo

- Utilizzando strumenti liberi e opensource si possono implementare soluzioni per la gestione di reti molto complesse e articolate senza dover scendere a compromessi.
- Il software open source non rappresenta l'alternativa ma la scelta migliore che si possa fare per la messa in sicurezza dei sistemi e delle reti
- Il free software è flessibile e permette a chiunque di personalizzarlo per far fronte anche alle più particolari delle esigenze
- Il free software è sicuro perché consente sempre di conoscere il modo in cui opera per validarne la genuinità

Questions?

Thanks

Feel *FREE* to contact me:

Francesco Acchiappati

Mobile: 349.1660172

Email: francesco.acchiappati@ethsec.com