Network Admission Control

(a cura di **Stefano Maccaglia**)

INDICE DELLA PRESENTAZIONE :

1. Il Network Admission Control
2. Perché Admission Control?
3. Il Framework
4. Features
5. Componenti del NAC
6. Architetture

7. Riferimenti bibliografici e sitografici

Il Network Admission Control (NAC)

Perché Admission Control?

1980-1990

Occorrevano settimane o mesi per rispondere ad un incidente di Sicurezza

2000 - 2002

Gli attacchi procedono a ritmi sostenuti. Nel giro di poche ore.

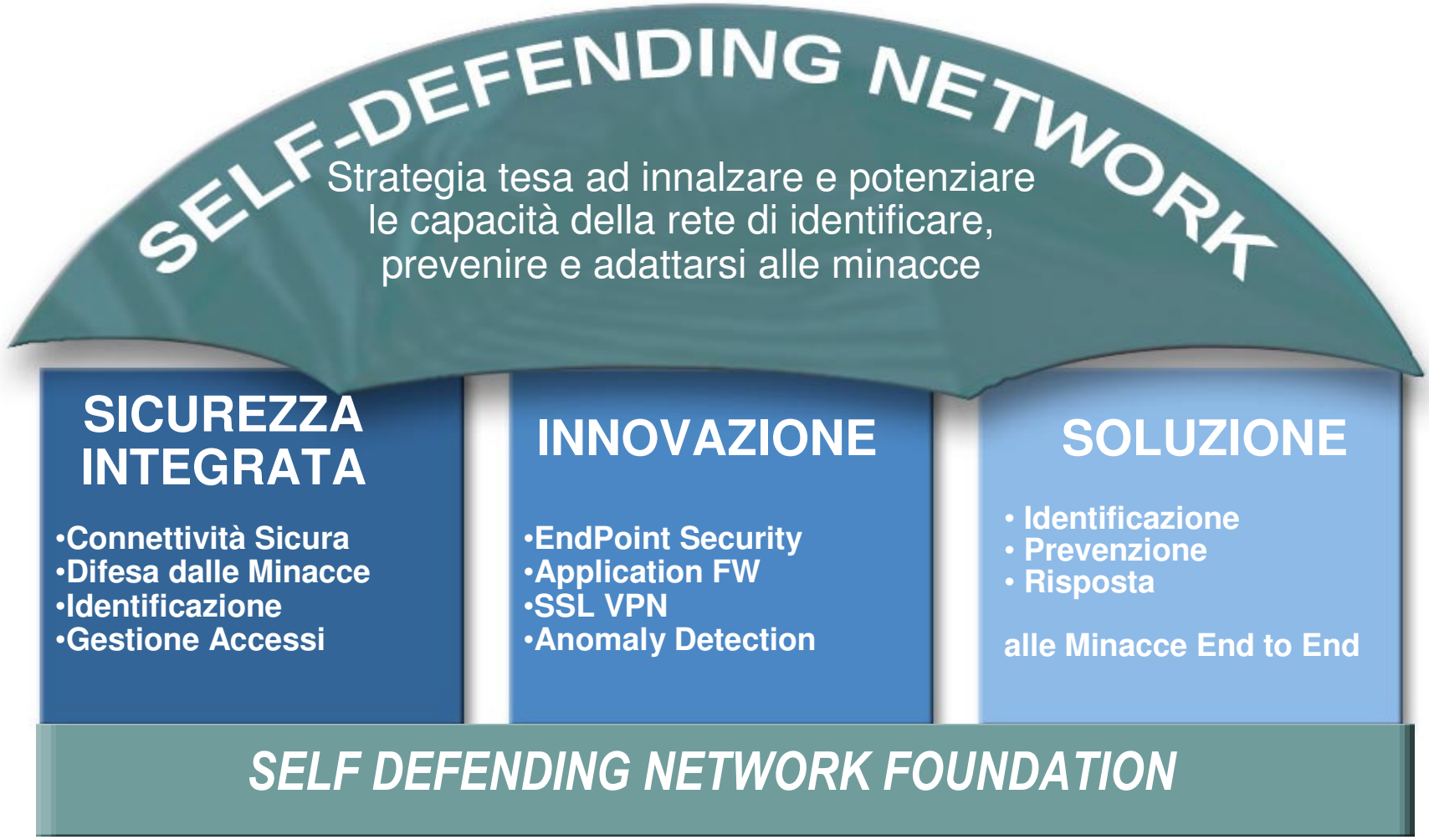
Entra in scena la Sicurezza Strutturata

2003 - Oggi

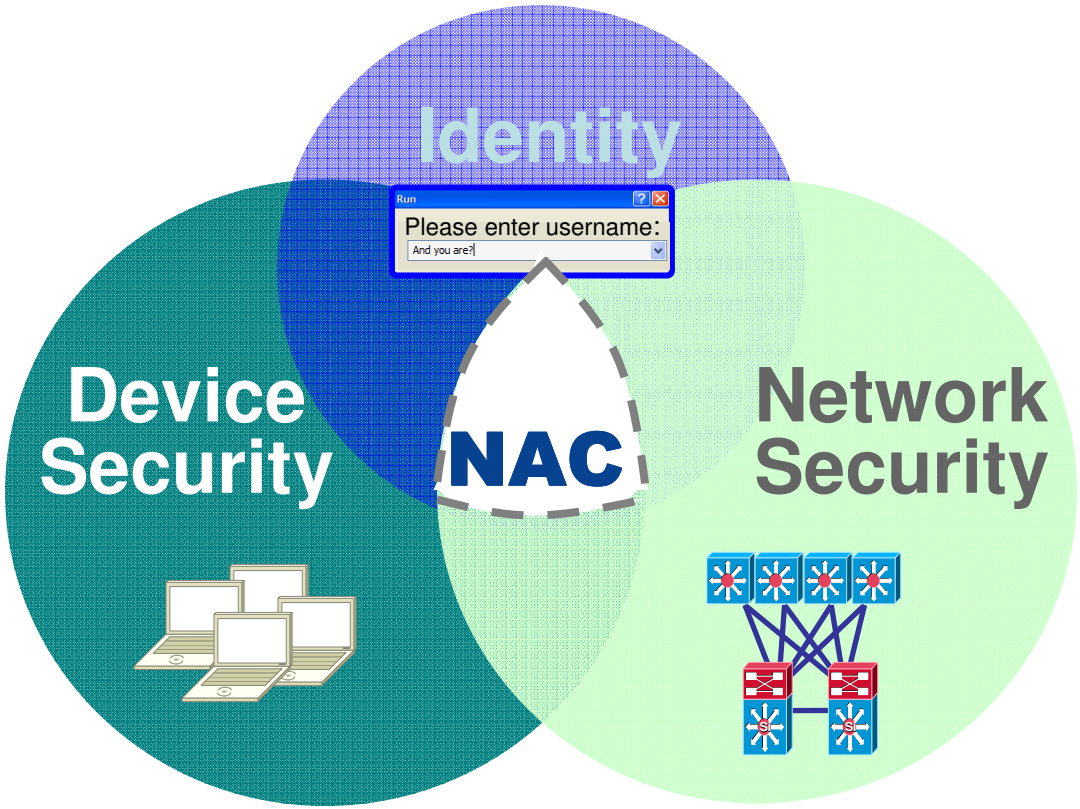
Gli attacchi si propagano nel giro di pochi secondi.

E' ora di implementare una Sicurezza Proattiva

Il Framework



Cos'è il Network Admission Control?



- **Attraverso la rete è possibile far rispettare le policy aziendali, in tal modo si accerta che i dispositivi connessi siano conformi.**

Network Admission Control (NAC)

- *Il Network Admission Control (NAC),* è una Soluzione tesa a limitare i danni provocati dalle emergenti minacce di sicurezza quali virus e worms
- In NAC, si può limitare l'accesso all'infrastruttura solo a dispositivi identificati con certezza e conformi (quali PC, Server, PDA) e si può vietare o limitare l'accesso a tutti i dispositivi non conformi ai requisiti di Sicurezza
- Questa Soluzione si sta imponendo come standard *de facto* nella Sicurezza delle Infrastrutture

- **Grazie al NAC si può garantire un deciso potenziamento della sicurezza all'Accesso**

Quattro ambiti del NAC

	Identificazione certa di utenti e dispositivi	Enforce consistent Policy	Quarantine and Remediation	Setup and Control
Che cosa significa…	Utenti univocamente associati ai vari dispositivi di rete.	Valutare e applicare le policy di sicurezza costantemente su tutta l'intera rete.	Isolare e sanare I Dispositivi non conformi.	Creare e controllare con facilità le policy.
Senza cosa accade?…	Senza associazioni univoche tra utente e macchina è difficile garantire una adeguata applicazione delle policy	Un sistema di policy decentralizzato può rappresentare un punto debole per la sicurezza.	Non basta identificare un dispositivo non conforme se non si ha la possibilità di normalizzarlo.	Le politiche troppo complesse o difficili da gestire verranno ben presto abbandonate o non applicate.

Un' efficace soluzione NAC richiede un'azione in tutti e quattro gli ambiti.

I Benefici del NAC

- Potenziamento della Sicurezza contro gli Accessi di dispositivi non conformi
- Aumento della resistenza e della produttività della Rete
- Gestione automatizzata o semi-automatizzata dell'infrastruttura di Rete
- Garanzia dell'investimento nei Sistemi Antivirus

Il Programma NAC

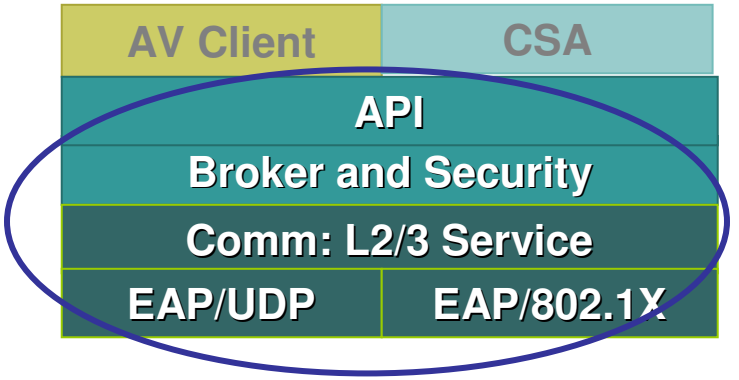
- Gli Sponsor del NAC sono, tra gli altri, i maggiori vendors di soluzioni antivirus, come: Network Associates, Symantec, and Trend Micro
- Tutte queste firme hanno prodotto una serie di client conformi alla gestione automatizzata del Sistema NAC, e anche degli agenti di sessione (non residenti)
- Futura espansione del NAC verso:
  - Tutti i dispositivi di rete
  - Tutti i Sistemi Operativi e le piattaforme applicative (OSs)
  - Standardizzazione

Network ASSOCIATES

symantec.

YOUR NETWORK. OUR

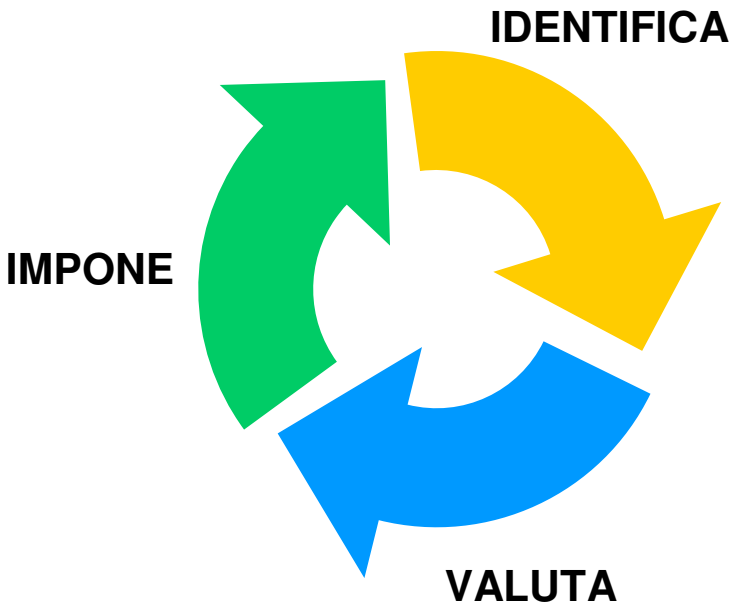
TREND MICRO



Trust Agent

Un sistema di Clean Access (CA) offre:

Prima di permettere agli utenti di accedere alla rete, sia in caso di connessione wireless che wired il sistema NAC:



Identifica:
Utenti, Dispositivi, e Ruoli (Ospite, Impiegato, Consulente)

Valuta:
Identifica le vulnerabilità

Impone:
Elimina le vulnerabilità prima dell'Accesso alla rete

NAC Features

Soluzione All-in-One di Policy Compliance e Remediation

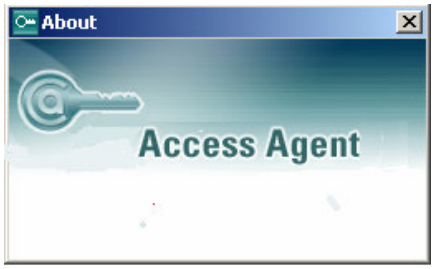
- **Role-based access control**
  - I server NAC implementano autorizzazioni e permessi
  - Supportano ruoli multipli per utente (e.g. guests, impiegato, e consulente)
- **Analisi via confronto**
  - Scansione per patch, AV, e software installato
  - Network scan per virus e worm
  - Network scan per vulnerabilità
- **Network quarantine**
  - Isola le macchine non conformi dal resto del network
  - MAC and IP-based quarantine efficace su base per-user
- **Normalizzazione**
  - Tools Rete per vulnerabilità e remediation
  - Help-desk integration

I Componenti del NAC

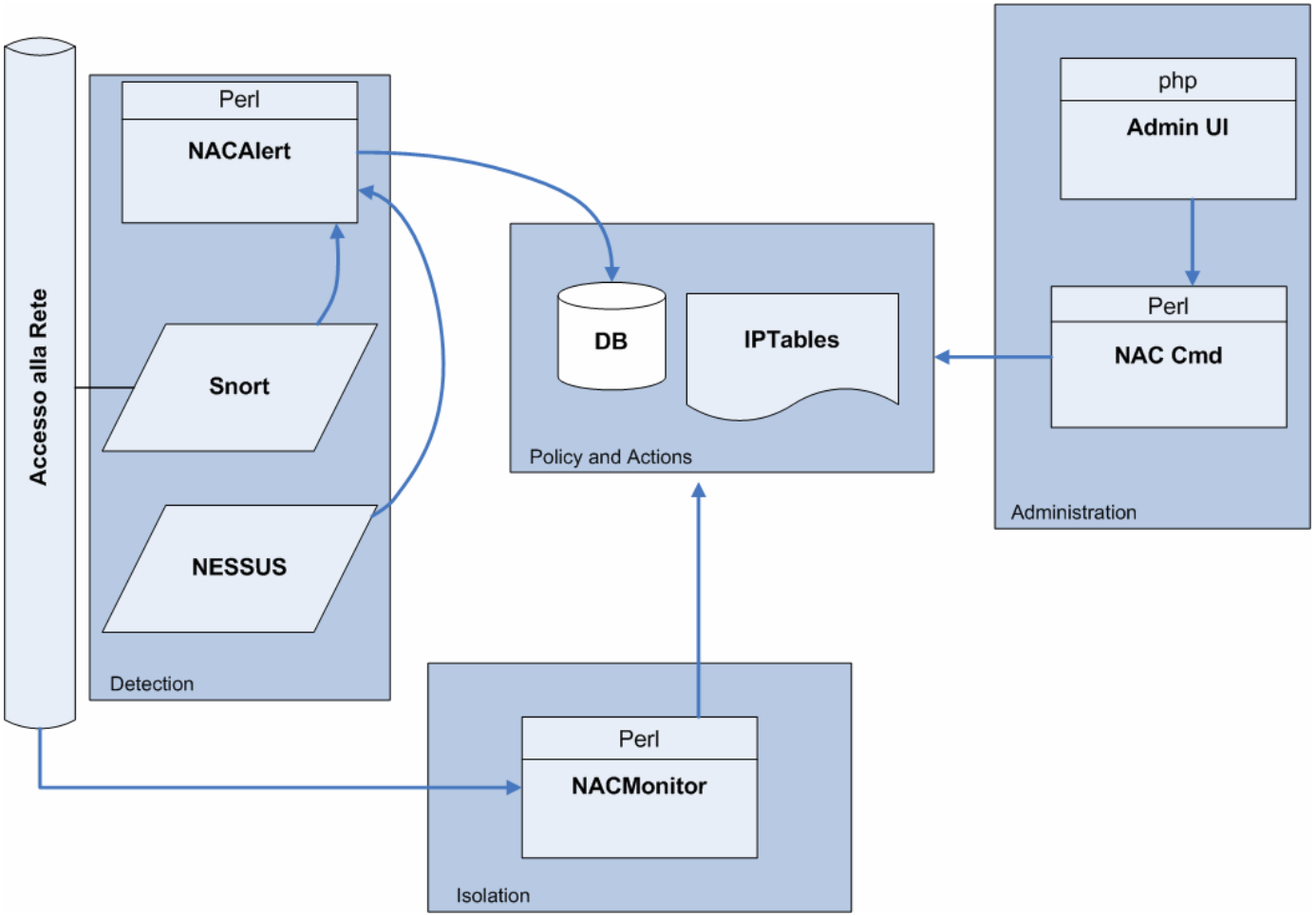
- Audit Server
  - E' il dispositivo che si occupa della scansione inline o out-of-band per la soluzione NAC

- Policy Manager
  - Dialoga via Snmp con gli apparati di rete
  - Centralizza la gestione degli Audit Server, delle policy e dei controlli per il NAC

- Agent
  - *Client Opzionale* per il controllo diacronico dei registri e delle posture degli host



Uno sguardo in-depth



Clean Access System Operation

THE GOAL

1. L'Utente prova ad accedere al Web o ad altra applicazione di rete

L'accesso alla Rete è bloccato fino a quando l'utente non fornisce credenziali valide

2. l'Utente è reindirizzato via Browser all'indirizzo dell'Audit Server per le credenziali

- Il server di Audit convalida le credenziali e può svolgere una scansione sulla macchina client. La scansione è variabile in base alle policy di conformità.

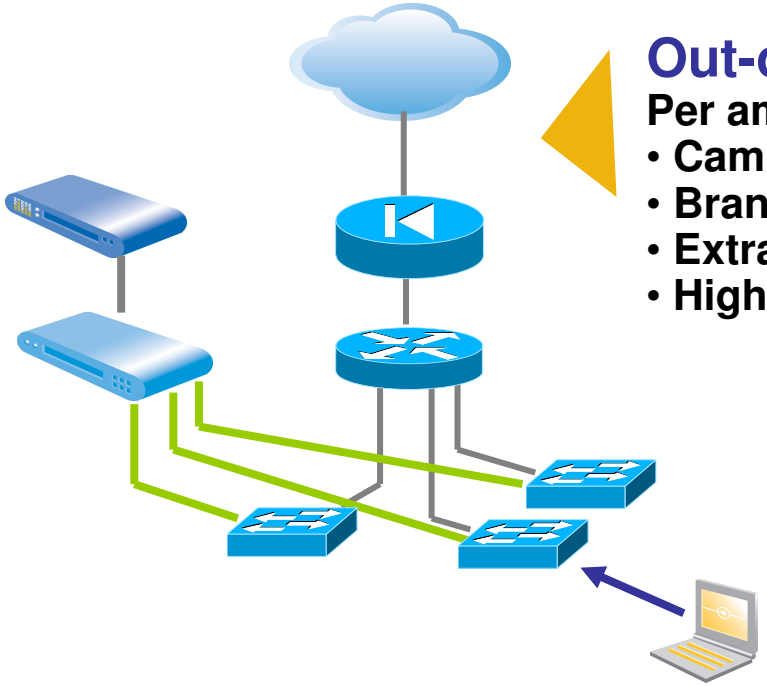
3a. Se il Device è Non-Conforme o il Login non è corretto

- All'utente è vietato l'accesso ed è assegnato dinamicamente alla Quarantena per garantirgli la possibilità di normalizzazione.

3b. Se il Device è "Conforme"

- Alla macchina è assegnata la "clean list" e le è permesso l'accesso.

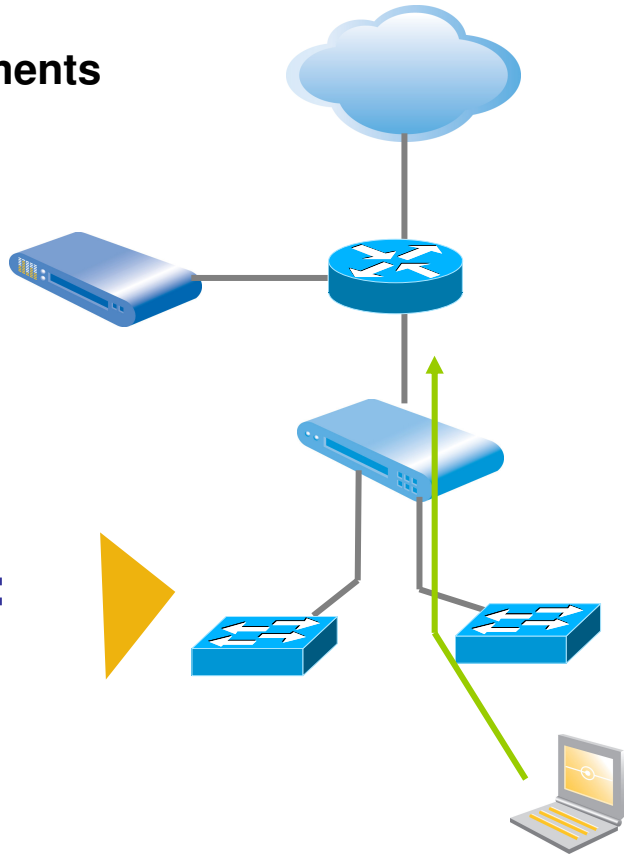
Architetture di NAC



Out-of-band:

Per ambienti di:

- **Campus**
- **Branch Offices**
- **Extranet**
- **Highly routed Environments**

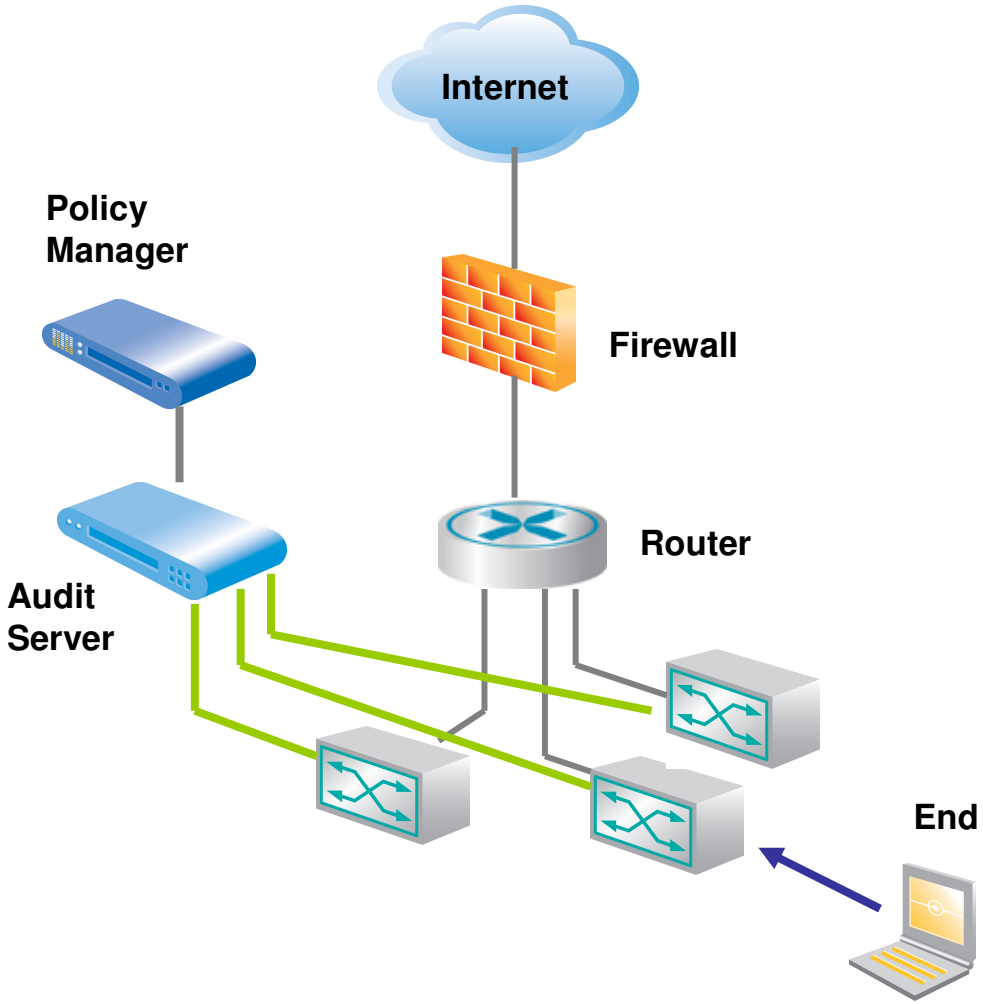


Inline (in band):

Supporta ambienti come:

- **Wireless**
- **Hubs**
- **Shared Media**

Clean Access Architettura Out Of Band



Integrabile solo con infrastrutture layer 2/3 compliant, fornisce una soluzione out of band a basso impatto.

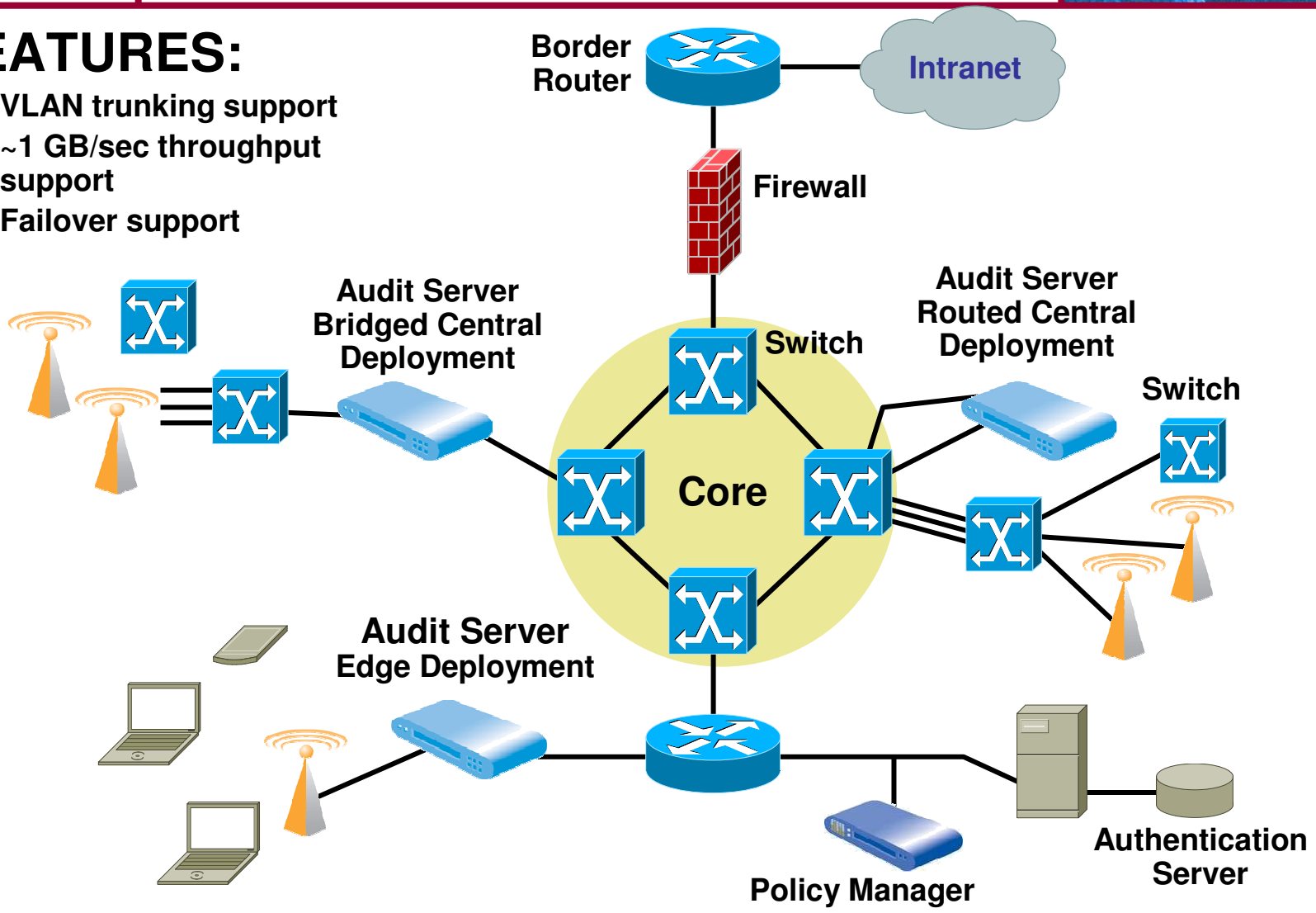
Offre Network Access Control agli utenti LAN.

E' raccomandabile in ambieti Layer 3 con numerosi segmenti di rete e dove le appliance in-line non siano appropriate.
Ha lo svantaggio di non essere applicabile a Layer 2 ancora (in evoluzione).

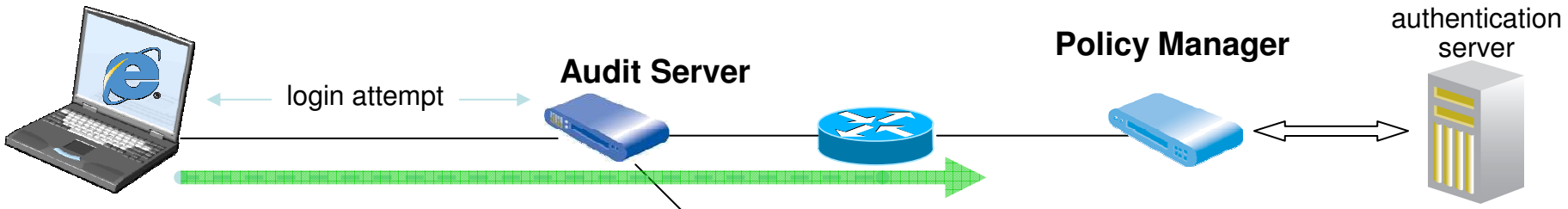
Clean Access Inline Deployment

FEATURES:

- VLAN trunking support
- ~1 GB/sec throughput support
- Failover support



Login Validation In-band



Utente del Laptop apre il browser ed è reindirizzato ad una weblogin SSL

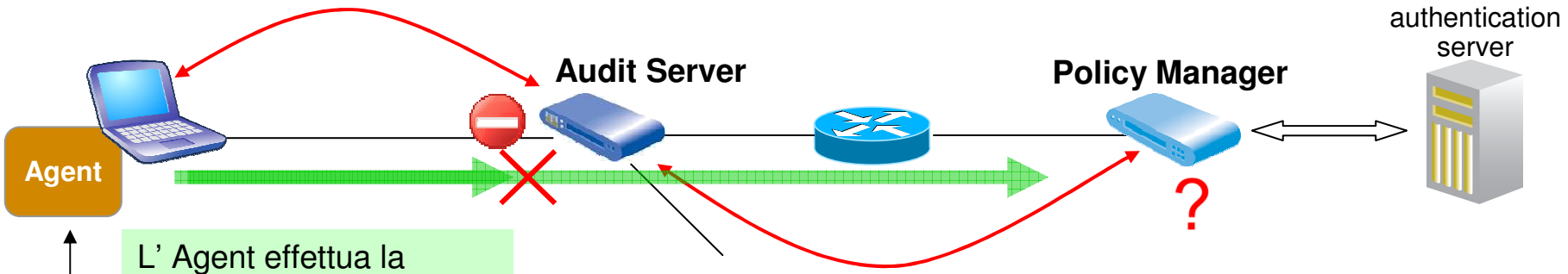
Access Enabled

Credenziali di log dell'utente

L'utente è autenticato " ruolo impiegati"

Allow Access

Clean Access Posture Validation In-band



L' Agent effettua la valutazione di integrità del client e invia al Policy Manager Server i dati tramite l'Audit Server.

Access Enabled

Compliant host

SI

Role: Trusted Employee

Allow Access

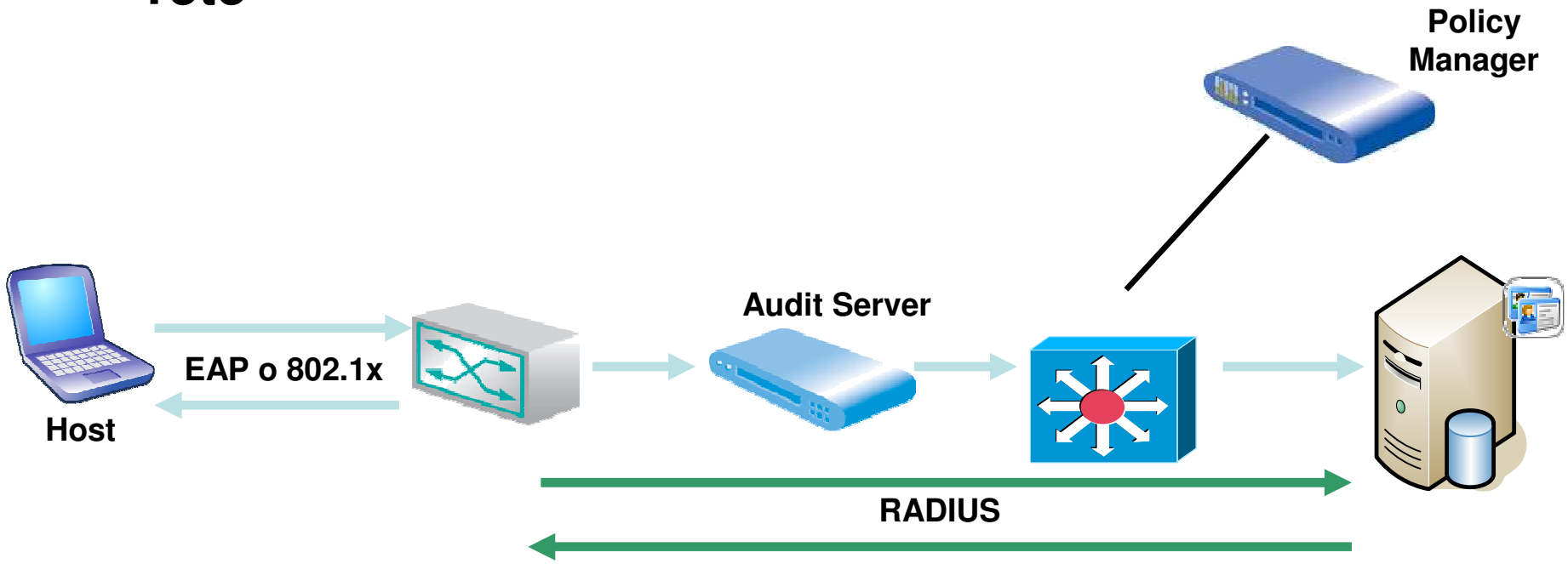
NO

Utente inserito in quarantena

Rimedio

NAC L2 802.1x

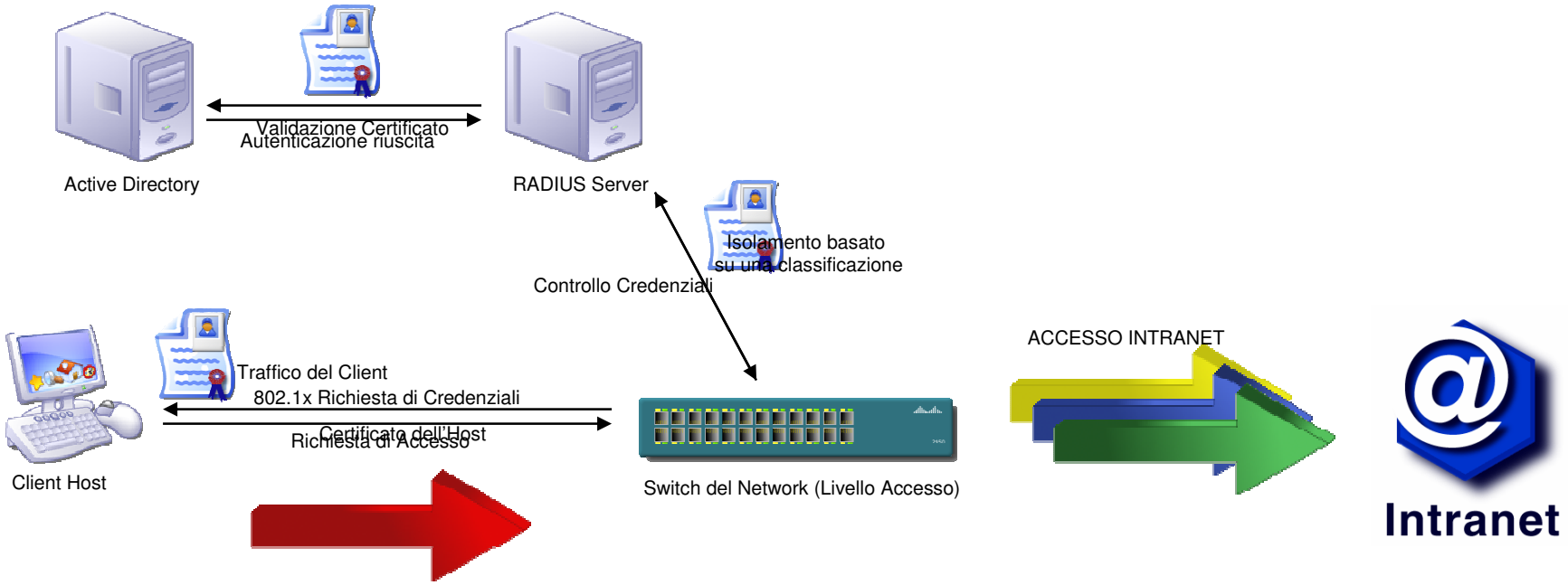
- **Attualmente il modo più rigido e completo di controllare gli accessi alla propria infrastruttura di rete**



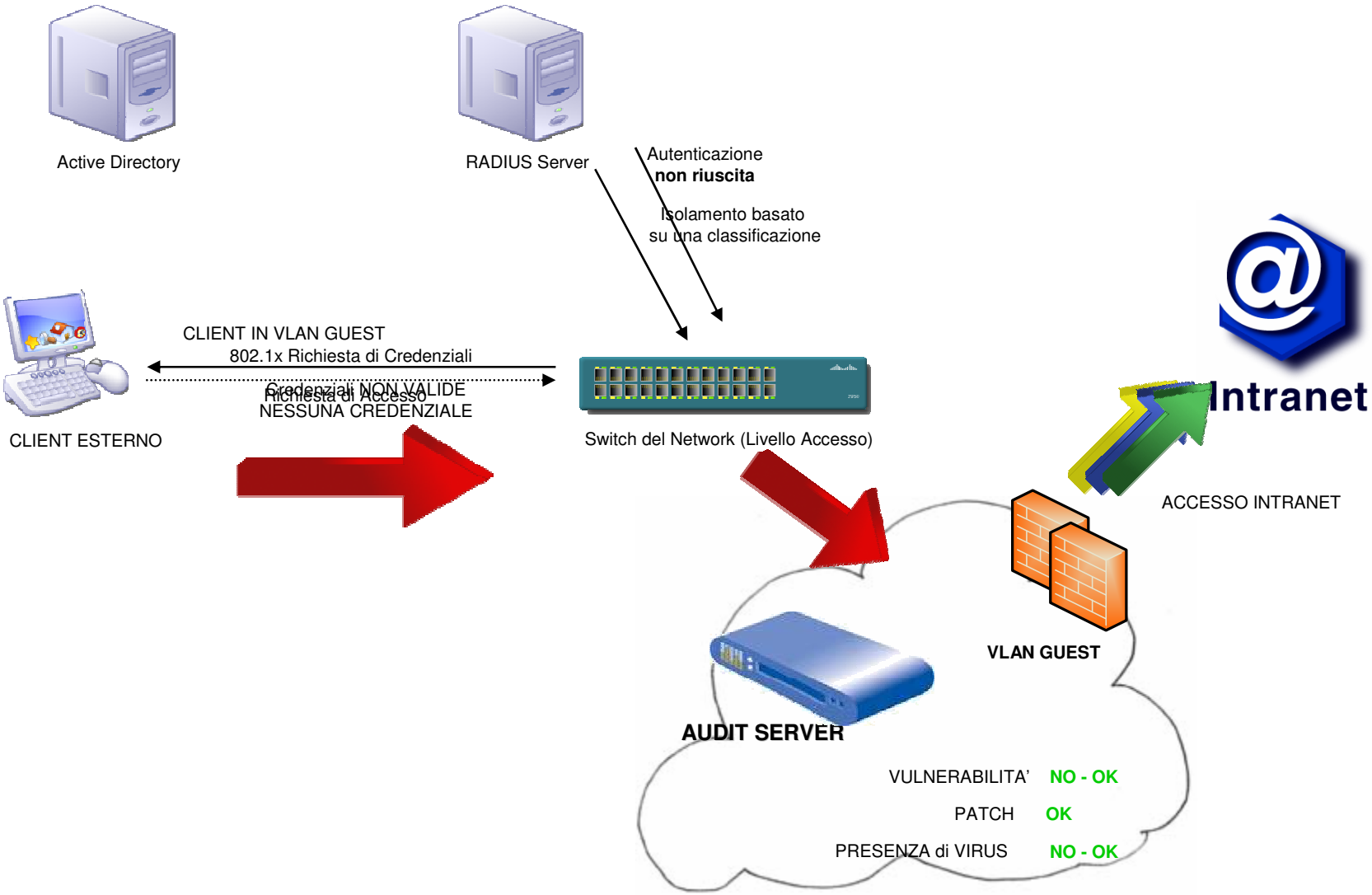
Un esempio di integrazione

- **Vediamo ora un esempio di integrazione tra 802.1x e sistemi NAC.**
- **Il caso: Consulenti…**

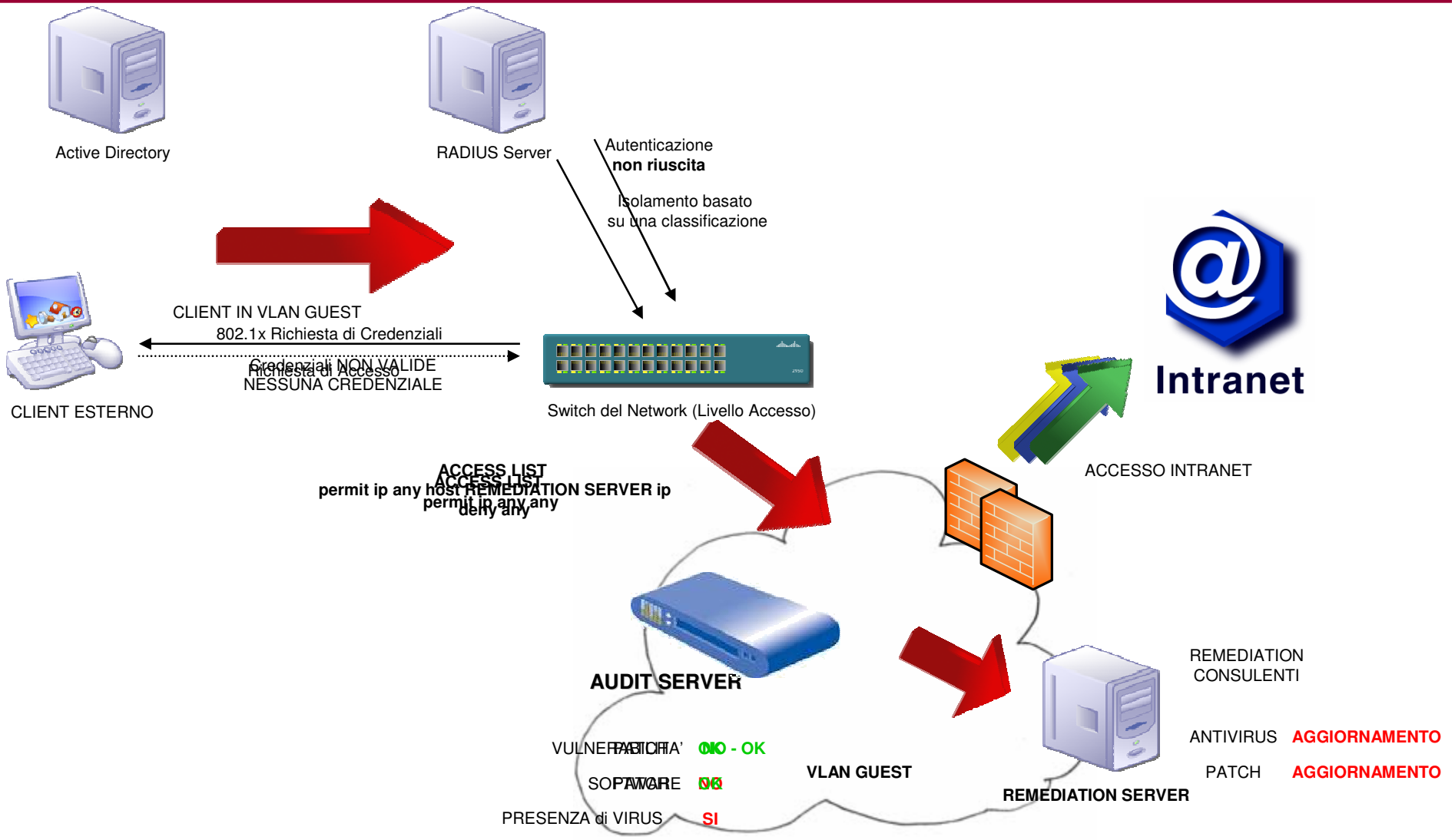
Client Interno



Client ESTERNO (Consulente)



Client ESTERNO (Consulente)



Bibliografia e sitografia :

Cisco Network Admission Control, Volume I: NAC Framework Architecture and Design.
Autori: D.Helfrich, L.Ronnau, J.Frazier, P.Forbes. Edito da Cisco Press, 2006

Cisco Network Admission Control, Volume II: NAC Network Deployment and Troubleshooting.
Autori: J.Frahim, O.Santos, D.White Jr.. Edito da Cisco Press, 2006

http://en.wikipedia.org/wiki/Network_Admission_Control

http://en.wikipedia.org/wiki/Network_Access_Control

http://www.cisco.com/en/US/netsol/ns466/networking_solutions_package.html

http://www.packetfence.org/

Altri Riferimenti :

- Network Admission Control

di Stefano Maccaglia
Articolo pubblicato dalla rivista Hakin9 nel numero 2/2007

- http://www.ietf.org/html.charters/nea-charter.html

Introduzione alla tematica NAC da parte dell'IETF

- http://www.ietf.org/internet-drafts/draft-ietf-nea-requirements-02.txt

Draft per la standardizzazione dei sistemi di Access Control.

GRAZIE PER L'ATTENZIONE

Stefano Maccaglia

Email: stefano.maccaglia@gmail.com
Mobile: 3401864035