Network Admission Control: introduzione

Cosa dovresti sapere...

- L'articolo presuppone una conoscenza sommaria di networking e di sicurezza. È avvantaggiato nel comprendere le sfumature tecniche chi ha già esperienza nella Sicurezza degli Accessi e nei protocolli di protezione delle reti locali.

Sull'autore

Ethical Hacker e Ricercatore, nonché progettista di soluzioni per la Sicurezza infrastrutturale, Stefano lavora nell'IT da più di dieci anni. Le sue competenze spaziano tra lo Storage Networking, il Wireless, il Networking e la Sicurezza, ambienti per i quali ha collaborato sia su progetti nazionali che internazionali. È attualmente impegnato allo sviluppo di un framework e alcune soluzioni di Sicurezza per l'analisi dei Sistemi soprattutto in riferimento alle tematiche dell'Admission Control e della Posture Validation sia in ambito wired che wireless.

Introduzione

La Sicurezza ha visto, negli ultimi cinque anni, il crescere dell'iinteresse verso l'ambito infrastrutturale, l'ambito degli accessi. Sia che si parli di accesso dal perimetro (VPN, Remote Access, Virtualizzazioni), sia che si parli di Accesso alla rete LAN attraverso il comune terminale di rete o l'ormai frequente presenza di connessione Wi-Fi, ognuno di questi settori è stato via via sempre più integrato all'interno degli elementi critici da „normalizzare" in una struttura aziendale.

Il crescere della mobilità fuori e dentro il perimetro dell'azienda è stato sicuramante un ottimo sprone alla ricerca di soluzioni per quest'area. D'altra parte controllare gli accessi dei dispositivi alle reti aziendali è sempre più difficile con il muoversi di questi dispositivi dentro e fuori delle stesse reti.

Al giorno d'oggi le minacce: dal virus al trojan al DdoS, vedono sempre di più l'ambito locale come il vero tallone d'achille delle reti domestiche e aziendali. Molti di questi preferiscono puntare all'esploitazione dei sistemi attraverso gli end-point (postazioni, client, host) aggirando la sicurezza del perimetro. Un esempio di questo è il Zotob Worm dell'Agosto 2005.

Questo virus colpisce grazie ad una vulnerabilità del sistema Plug and Play delle piattaforme Microsoft[1] e si propaga attraverso i network in maniera casuale inviando pacchetti TCP/Syn alla porta 445 di sistemi verso i quali dirige randomicamente le connessioni. Individuata una macchina il worm si copia sulla nuova vittima grazie alla vulnerabilità già indicata e prosegue poi nella sua opera di diffusione.

Come molti sistemisti sanno, la porta che questo worm utilizza è la stessa di numerosi altri worm, tra i quali i famosi Sasser e SpyBot, worm contro i quali le infrastrutture di rete perimetrale già da molto tempo vengono predisposte, bloccando il traffico diretto alla porta 445.

E allora come è stato possibile che Zotob si è diffuso largamente nonostante le condizioni a corredo sembrava non ci fossero? La risposta è nella "mobilità". Il worm è riuscito a colpire facilmente in ambienti esterni all'azienda, laddove le difese sono al massimo legate ad un sistema antivirus installato sulla macchina. Quando poi gli utenti, tornando in azienda, si connettevano alla rete essi erano gli ignari vettori del virus, che a quel punto non doveva più scontrarsi con i sistemi perimetrali, la mobilità degli utenti aveva svolto il lavoro di "aggiramento" delle difese e ora l'intera rete era aperta al contagio.

1 Vulnerability in Plug and Play Could Allow Remote Code Execution and Elevation of Privilege (899588) http://www.microsoft.com/technet/security/Bulletin/MS05-039.mspx

Il Network Admission Control

Per rispondere e risolvere le problematiche aperte da elementi quali il proliferare di Zotob la ricerca nell'ambito della Sicurezza ha puntato a presentare una nuova prospettiva di lavoro introducendo la standardizzazione per il protocollo 802.1x (anche noto come *dot1x*, protocollo standardizzato nel 2001), un protocollo basato su EAP che fortifica la protezione degli accessi alla rete fisica impedendo l'accesso a chi non abbia preventivamente fornito delle credenziali valide. Questo sistema però non ha risolto i problemi di chi nella rete è entrato perché titolare di un accesso valido, ma che nel contempo ha raccolto, fuori dell'azienda, un virus come Zotob e che quindi all'accesso potrà distribuirlo a tutti gli altri client.

Per risolvere questo aspetto è stato introdotto ed è in via di standardizzazione un ulteriore protocollo che, al pari del dot1x è in realtà un insieme di protocolli e best practices volte a fornire una serie di possibili scenari applicativi nei quali introdurre controlli e verifiche: il Network Admission Control, anche noto come Network Access Protection.

Questo approccio tende a:

- Imporre delle politiche di sicurezza impedendo contemporaneamente il traffico proibito;
- Identificare e contenere gli utenti che violano le regole o non siano conformi alle policy;
- Mitigare l'impatto delle minacce portate dai sistemi mobili e garantire la difesa degli utenti interconnessi.

L'obiettivo dichiarato del NAC/NAP è quello di controllare, valutare e stabilire se un client che avviasse una connessione all'interno del network aziendale sia o meno conforme alle politiche aziendali. In questo ambito è essenziale che le politiche stesse vengano tradotte in profili di conformità, in altre parole è necessario che, prima di integrare una qualunque soluzione di Admission Control si proceda ad individuare quali programmi, quali Sistemi, quali attività in avvio sono considerate „valide" dalla Sicurezza aziendale in modo da poter verificare lo stato della macchina all'accesso rispetto a questi profili.

Il processo di validazione delle posture (Posture Validation Process) si basa su una architettura suddivisa nelle seguenti aree:

1. Dispositivi oggetto della verifica (***Subject***);
2. Attuazione delle policy (***Enforcement***);
3. Decisione (***Decision***);
4. Correzione (***Remediation***)

Una domanda che potrebbe sorgere a questo punto è: ma cosa ha ispirato il NAC, da cosa nasce questo approccio?

La risposta è l'RFC 2753 del Gennaio 2000.

In questo documento non si parla di standard o di sicurezza in particolare, ma di un sistema che, partendo dalla QoS[1] e dalla sua architettura, possa in base a criteri quali l'autenticazione, l'orario o la criticità di un'applicazione, fornire ad un utente dell'infrastruttura accesso preferenziale o esclusivo a determinate porzioni della rete o delle risorse in essa contenute.

In sintesi l'RFC parla di criteri di controllo dell'identità in base ai quali organizzare i flussi comunicativi.

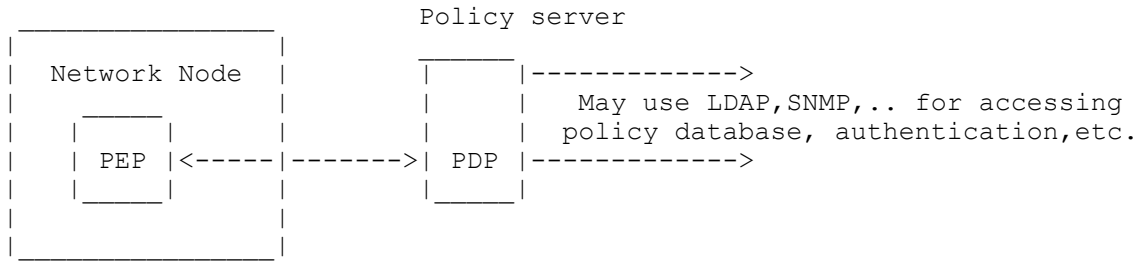
L'architettura con la quale svolgere i controlli si basa su due elementi imprescindibili: il Policy Enforcement Point (PEP) e il Policy Decision Point (PDP).
Il PEP è un componente che opera allo stesso livello dei nodi di rete, mentre il PDP è un'entità remota che svolge le funzioni di policy server. In sostanza il PEP opera in base ai criteri configurati e attuati nel PDP. In questo senso è il PDP che discrimina e determina l'uso di un tipo di protocollo di autenticazione piuttosto che un altro.

Il flusso interattivo che porta al controllo e alla successiva applicazione di una politica per il singolo accesso

1 QoS = Quality of Service è un framework che nasce dall'idea che la velocità di trasmissione e il tasso di errori possono essere misurati, migliorati ed in alcuni casi bisogna garantirne una percentuale minima. QoS è particolarmente importante quando si trattano comunicazioni che includono video e voce o comunque informazioni di tipo multimediali, poiché questi tipi di dati devono essere gestiti in modo differenziato rispetto ai dati puri.

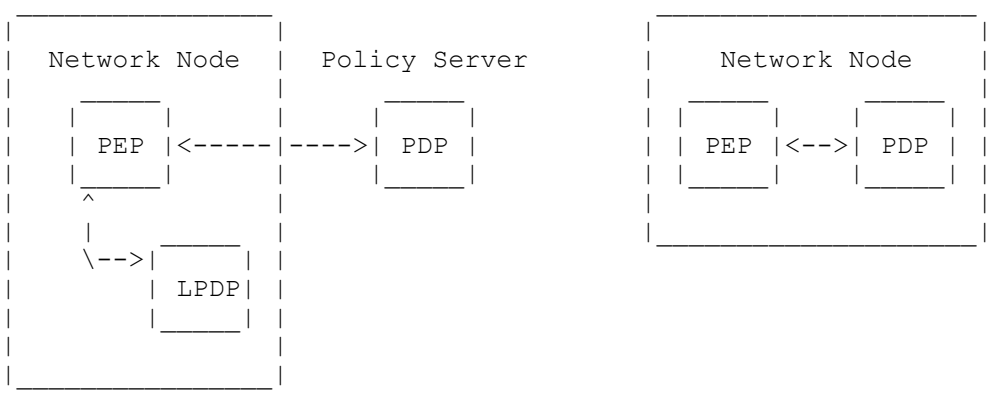
parte dal PEP che per primo interagisce con l'host e che richiede al PDP decisioni in merito alle singole entità di rete (ammissione al network, allocazione di banda, indicazione sulla criticità del servizio richiesto, ecc...). Una richiesta del PEP può contenere una o più richieste di policy incapsulate in uno o più policy object, in aggiunta alle informazioni di admission control. L'attivazione della richiesta parte sempre da un evento che avvia il processo di identificazione a livello del PEP. Il PDP risponde con una “decisione” che viene poi attuata dal PEP. Il PDP potrebbe anche includere informazioni aggiuntive nella sua risposta (per esempio messaggi di errore).

Lo schema sotto indicato meglio definisce il tutto:



Il PDP può, in maniera opzionale, contattare server esterni per i servizi di autenticazione, accounting e billing.

Dal punto di vista strettamente operativo il funzionamento del sistema è legato in maniera indissolubile alla capacità di rendere coerenti e consistenti le politiche di sicurezza della rete in modo da avere mappature chiare e non ambigue tra le procedure di autenticazione, l'allocazione dei servizi e dei segmenti di rete e le azioni da intraprendere in assenza o in carenza dei requisiti stabiliti per policy. Questo comporta la possibilità, offerta dal framework, di co-locare parte delle funzionalità del PDP localmente sul nodo PEP, come da schema:



Il modello in questione illustra la flessibile divisione dei compiti. Da una parte un policy server centralizzato, responsabile delle politiche dell'intera infrastruttura e capace di implementare le politiche in un ampio spettro su tutto il dominio di rete. Dall'altra parte le politiche che dipendono da informazioni e condizioni locali di un particolare componente di rete (router, switch, firewall, ecc...), più dinamiche e relative, possono essere implementate localmente sul PEP attraverso il componente LPDP (local PDP). Ovviamente in questo caso deve esistere un modello di comunicazione tra PDP e LDPD che permetta l'aggiornamento e il consolidamento delle policy applicate localmente rispetto a quelle generali.

Altra possibile configurazione di un'architettura di controllo è quella che ipotizza PEP e PDP operanti direttamente a livello di nodo. Questa, come vedremo, è la soluzione più utilizzata in contesti VPN e remoti, laddove anche il NAC trova difficoltà a svolgere controlli direttamente a livello di accesso locale.

Il NAC, sostanzialmente, è partito da questo approccio per sviluppare poi delle caratteristiche proprie. Anzitutto il concetto di valutazione dello stato del dispositivo (***Posture***) in riferimento a dei profili stabiliti per policy dall'Azienda. La valutazione delle posture presuppone l'esistenza di una serie di politiche di Sicurezza che possano identificare in maniera inequivocabile tutte le configurazioni e le attività degli host possibili o permesse all'accesso. In effetti il NAC punta ad evidenziare quali dispositivi siano conformi e quali non lo siano rispetto ad un preciso elenco di caratteristiche e credenziali fornite o detenute dalla macchina e dal suo proprietario.

Gli elementi strutturali del NAC

Rispetto all'RFC 2753 gli elementi che compongono la piattaforma NAC sono un numero notevolmente maggiore, ma in sintesi buona parte delle funzionalità già individuate nell'RFC sono state poi riprese e potenziate e da qui è nata anche la ulteriore specializzazione delle funzioni inizialmente raccolte all'interno del PEP e del PDP.

Nel NAC abbiamo un soggetto, uno o più Policy Enforcement Point, una serie di Policy Server che segmentano le funzionalità del PDP del vecchio approccio e, novità, uno o più sistemi di Quarantena e Remediation che garantiscono in maniera automatizzata o semiautomatizzata di correggere o normalizzare l'host non conforme, o altresì di renderlo inoffensivo alla rete.

Dettagliando meglio le funzioni e gli attori del NAC possiamo enumerarli e catalogarli così:

Dispositivi oggetto della verifica (Subject).

Sono i soggetti sottoposti al controllo di accesso o gli elementi che coadiuvano il controllo dello stato della macchina che richiede di accedere. Quindi:

(a) ***Host*** - è la macchina o il dispositivo che tenta di accedere alla rete.

(b) ***Posture Agent (PA)*** - è un agente software che risiede sull'host, raccoglie le informazioni relative al dispositivo, come ad esempio lo stato di aggiornamento dell'antivirus e del sistema operativo installati, e comunica con la rete.

(c) ***Remediation Client*** - è una componente aggiuntiva, non necessaria al controllo, ma utile ad aggiornare alcuni specifici software installati sull'host (patch del sistema operativo, aggiornamenti antivirus) sulla base di policy aziendali predefinite.

Attuazione delle policy (Enforcement).

È solitamente l'apparato che svolge la funzione di attuatore delle policy di accesso sulla base di template di stato delle macchine forniti dai sistemi di Decisione. In sintesi:

(a) ***Network Access Device*** **(NAD)** è il dispositivo di rete che svolge la funzione di *enforcement point*, cioè è la parte di infrastruttura di accesso su cui vengono messe in atto le politiche di accesso. Può essere ad esempio un router, un VPN Gateway, uno switch Layer 2 e Layer 3 o un Access Point wireless.

(a) ***Audit Server*** è il server che esegue un Vulnerability Assessment (VA) su un host per stabilirne il livello di compatibilità alle policy prima di garantirgli accesso alla rete.

Questo apparato raccoglie i dati direttamente dall'host (attraverso il Client NAC o la scansione agentless) comparandoli con i profili presenti sul Posture Validation Server e, dialogando poi con il RADIUS, sposta l'utente in base al profilo di rischio all'interno della Vlan ad esso spettante o alla Vlan di quarantena o di isolamento.

Decisione (Decision)

Questa funzione viene svolta dagli apparati di rete più importanti nel processo di autenticazione, controllo e gestione dei dispositivi. In effetti in quest'ambito troviamo i seguenti componenti:

(a) ***Authentication Server*** (Server di Autenticazione) è il server RADIUS che gestisce le policy di accesso per utente o per macchina.

(b) ***Directory Server*** è il directory server centralizzato per l'autenticazione delle macchine e/o degli utenti. Possono essere usati server LDAP, Microsoft Active Directory (AD), Novell Directory Services (NDS), e token one-time password (OTP).

(c) ***Posture Validation Server*** **(PVS)** è il server che convalida le *posture* degli host sulla base di policy specifiche per ciascun tipo di applicazione, ad esempio antivirus o altre applicazioni di sicurezza. È questo il vero cuore del sistema NAC essendo questo l'apparato in cui le policy ad alto livello diventano delle politiche di permesso o blocco delle macchine e degli utenti che tentano l'accesso.

Correzione (Remediation)

(a) ***Remediation Server*** è il server che si occupa di condurre alla compatibilità gli host non compatibili con le policy aziendali. Può essere ad esempio una applicazione di patch management o un sito di distribuzione software.

Si deve considerare che la parte riguardante la Correzione non è sempre presente in ambienti NAC in quanto essa presuppone un'automazione non sempre libera da complicazioni. In questo senso lo sforzo attuale, al di là della standardizzazione, è quello di realizzare delle piattaforme di Correzione capaci di offrire in maniera semplice e puntuale i rimedi necessari alla normalizzazione degli host. Nel presente documento non tratteremo di metodi di correzione, ci limiteremo alle aree di Attuazione delle policy (Enforcement) e Decisione (Decision) che sono il cuore del sistema NAC.

Come già si può capire, i controlli svolti durante la fase di primo accesso degli host sono fondamentali per garantire l'esclusione o la quarantena a quei sistemi che presentino più o meno palesi, ma individuabili anomalie o carenze di protezione che potrebbero mettere a repentaglio la loro sicurezza e più in generale la sicurezza dell'intera infrastruttura.

Questo approccio però può risultare miope in quanto non si considerano, in questo modo, tutti i rischi connessi alle attività svolte dagli utenti una volta entrati nella rete.

In realtà l'approccio che ho sviluppato congiuntamente con il mio gruppo intende offrire una soluzione completa nella quale il controllo di accesso, d'ora in poi detto Pre-Admission NAC, è solo una parte, sebbene significativa, dell'intero ambito.

In questo documento, per brevità, ci dedicheremo ad illustrare dettagliatamente i sistemi di Pre-Admission NAC, lasciando solo una sommaria definizione delle modalità di controllo Post-Admission. Sarà mia premura, qualora i lettori lo ritengano interessante, illustrare in futuro in maniera più dettagliata i sistemi di controllo post-admission.

Tornando alle soluzioni NAC di primo accesso, esse devono comprendere due fondamentali funzionalità: identificare nuovi dispositivi che si connettano alla rete e analizzare gli endpoint per valutarne l'aderenza alle policy con l'obiettivo di limitarne o vietarne l'accesso in caso di mancato rispetto dei criteri di accesso.

Come si può integrare il NAC in una rete?

È importante comprendere che, se si vuole attuare una soluzione NAC, occorre avere o predisporre una serie importante e imprescindibile di condizioni operative, prima fra tutte un sistema di identificazione dei dispositivi che tentano l'accesso, siano essi conosciuti, o nuovi. In questo settore operano ormai da tempo tecnologie quali il già citato 802.1x, ma anche sistemi DHCP, sistemi di Autenticazione Single Sign-on, Sistemi RADIUS o altri sistemi di controllo „in-band".

Lasciamo ad altri ambiti l'onere di approfondire queste soluzioni tecnologiche, ma chiariamo già in questa fase che l'assenza di un pre-esistente sistema di identificazione e controllo che funga da "repository" per i profili degli utenti "conosciuti" da quelli "non conosciuti" comporta un'onere aggiuntivo non trascurabile nella realizzazione di un sistema NAC che non si limita alla creazione degli stessi profili, ma che impatta pesantemente anche il "sizing" (la scelta e le dimensioni del sistema NAC).

Mancando un "deposito logico" di utenze "conosciute" si dovrà procedere ad implementare una soluzione necessariamente "in-band" che dovrà non solo controllare la postura degli utenti che tentano l'accesso, ma anche l'autenticazione degli stessi. In altre condizioni, con la presenza del già citato "meccanismo di autenticazione terzo", possiamo lasciare al NAC il solo onere, non certo leggero, di verificare lo stato della macchina che tenta la connessione, cosa che di per sé può essere fatta in maniera "discreta" attraverso un'architattura "out-of-band". Imporre via NAC anche l'autenticazione comporta appunto l'obbligo di puntare su una soluzione in-band per garantire il blocco del traffico del client in assenza di credenziali.

Vediamo più da vicino le alternative già citate.

Il protocollo 802.1x

Una soluzione di sicuro interesse è quella che poggia l'identificazione dei sistemi all'accesso attraverso lo standard 802.1x.

Questo standard definisce un protocollo di comunicazione sicuro tra i tre elementi logici che lo costituiscono:

Supplicant, Authenticator e Server di Autenticazione (RADIUS).

Il *Supplicant* è il client software (ormai embedded nei moderni sistemi operativi) operante a livello utente (nella sua workstation), l'*Authenticator* è l'apparato di rete (solitamente lo switch o l'Access Point) che garantisce l'accesso all'infrastruttura e le richieste di credenziali svolte al momento stesso della connessione dall'Authenticator e fornite dal client sono passate poi al *Server di Autenticazione* (AAA Server).

802.1x usa l'EAP (Extensible Authentication Protocol) per comunicare le credenziali tra il supplicant e il Server di Autenticazione attraverso l'Authenticator. Tipicamente il protocollo EAP può permettere l'invio anche di informazioni aggiuntive sull'integrità dell'host al Server, elemento questo che ci garantisce un opportuno supporto per il NAC.

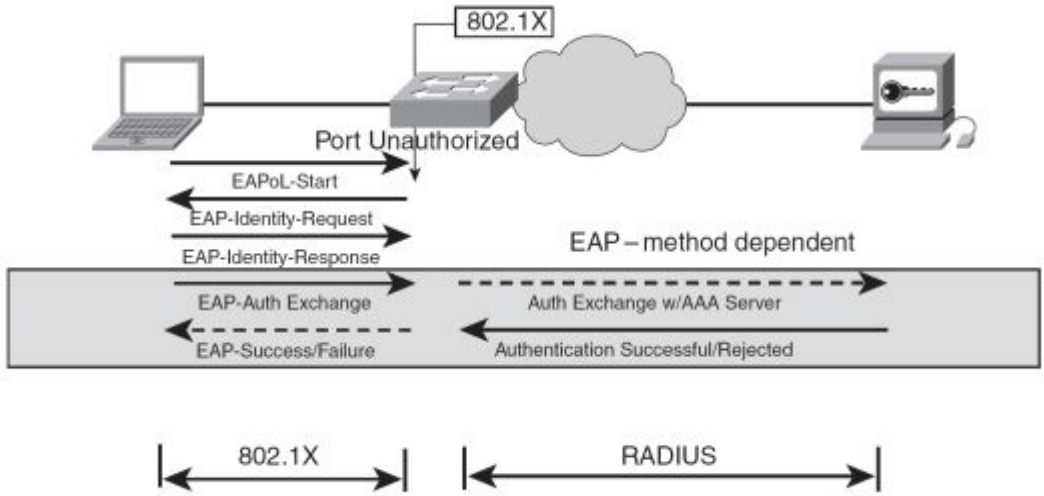


Illustrazione 1: Schema di autenticazione 802.1x

Tra gli aspetti positivi dell'802.1x c'è il fatto che esso individua l'host che tenta la connessione prima che abbia un indirizzo IP e che possa provocare disordini nel network, inoltre l'host non ha nessuna possibilità di interagire con la rete fino a quando non termina la procedura di autenticazione.

L'aspetto negativo è la necessità di implementare una architettura diffusa ed efficiente che sia completamente organizzata intorno al protocollo 802.1x e che forzi l'autenticazione per tutte le stazioni della rete imponendo di fatto la necessità di migrare gli endpoint a sistemi operativi e client software conformi al protocollo, così come sostituire gli apparati di rete non conformi.

Il DHCP e il DHCP Proxy

Un altro approccio teso a identificare gli endpoint e impedire l'accesso di questi a porzioni di rete protette è offerto dall'uso di un DHCP server e DHCP proxy.

In questa architettura un dispositivo che intendesse utilizzare i servizi di una rete dovrebbe necessariamente abilitare l'utilizzo di un IP address dinamico, pena la mancanza di accesso alla rete.

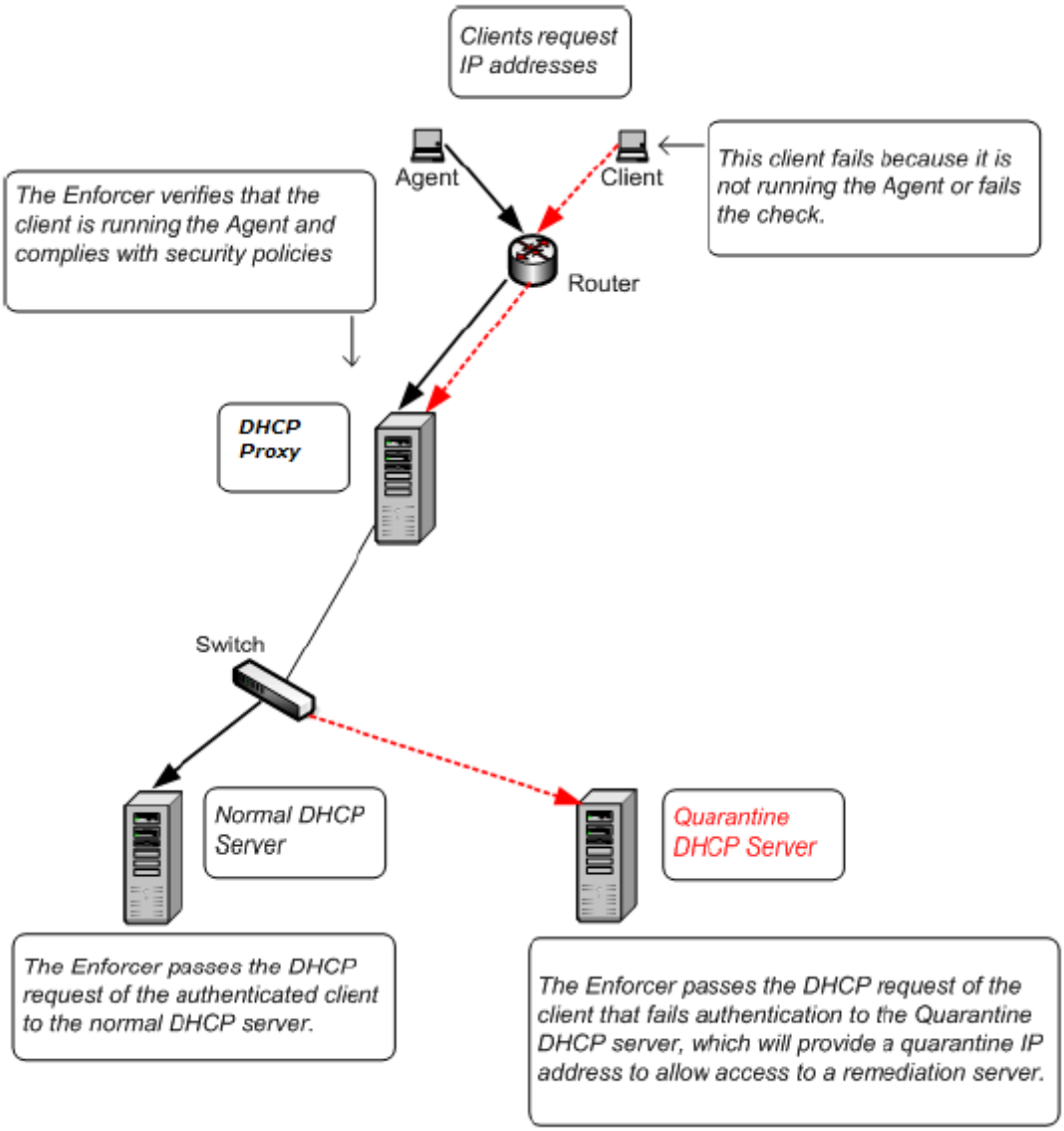


Illustrazione 2: Schema di Autenticazione via DHCP

Tipicamente questo approccio non è molto sicuro se non è corredato da un preciso sistema di monitoraggio e verifica delle risorse di rete e degli accessi, ma è spesso una buon punto di partenza per il NAC, dal momento che la maggior parte delle aziende usa i Server DHCP per allocare indirizzi ai loro host e quindi è un buon modo per individuare i nuovi host che si presentano nella rete. Un altro vantaggio è dato dal fatto che questo sistema funziona anche per apparati non conformi con 802.1x ed è in generale più semplice da installare.

Ci sono comunque vari aspetti negativi per questo approccio. In primis anche in questo caso occorrono dispositivi che siano equipaggiati con agenti software che devono essere gestiti e mantenuti aggiornati. In assenza di questi agenti non si può avere una discriminazione all'accesso tra chi richiede e deve ottenere un IP address e chi, pur non avendone diritto, richiede e ottiene un IP e quindi l'accesso alla rete.

Oltre a ciò, la maggior parte dei client sono ristretti ai sistemi Microsoft.

Ma nell'ombra rimangono due pericoli ancor più grandi. Il primo è il fatto che con un IP statico, della stessa subnet di quelli assegnati dinamicamente, sia facile aggirare la sicurezza offerta dal DHCP. Questo può indurre un utente informato o un cybercriminale ad implementare un indirizzo IP statico e penetrare tranquillamente nella rete.

Un secondo importante pericolo è dato dal fatto che, in un ambiente enterprise, la creazione di una LAN di Quarantena pone seri pericoli per l'incolumità di quei malcapitati host che sono costretti a condividerla con macchine già infette e sono quindi esposti al contagio, con il risultato di trasformare la LAN di Quarantena in

una Colonia Virale.

Il Sistema di Autenticazione

Un terzo approccio volto ad identificare e controllare l'accesso alla rete è possibile attraverso l'integrazione con il processo di autenticazione, questo è l'approccio che Microsoft sta perseguendo con la sua "NAP Initiative". In merito a questa soluzione chi scrive non ha ancora avuto modo di sperimentare soluzioni o architetture che ne facciano uso, ma stante ai dati che vengono forniti ci sono due soluzioni basate su questo modello. Nella prima, un proxy per l'autenticazione è implementato in-line[1] con il Server di autenticazione (AAA) esistente; nel secondo al posto dell'Authentication server tradizionale viene impiegato un server aggiornato con del software che possa riconoscere sia la validità delle credenziali di autenticazione che la loro integrità. In entrambe le situazioni l'integrità degli endpoint determina a quali segmenti di rete e a quali risorse gli host possano accedere.

In conclusione possiamo affermare che questi sistemi si affidano più all'infrastruttura server che all'infrastruttura di rete per avviare i controlli di integrità sugli host e che questo è utile maggiormente per restringere l'accesso agli applicativi di rete e ai servizi che non ad impedire un accesso alla rete in generale.

In ogni caso il sistema può offrire il fianco ad una falla critica che porta ad una pericolosa e ironica possibilità: i dispositivi non gestiti non iniziano l'autenticazione al Server, il che significa che nessun controllo verrebbe svolto su questi sistemi. Per definizione, i sistemi non gestiti o non individuati sono i più pericolosi, e quindi si potrebbe concludere che i dispositivi che più dovrebbero essere controllati sono poi quelli che non vengono neppure analizzati.

Una volta individuato il tentativo di accesso dell'host, entra in gioco il NAC, o almeno questo dovrebbe essere lo schema di integrazione del NAP. Prima individuo un tentativo di accesso, poi lo controllo, poi verifico lo stato della macchina che accede ed infine, se è conforme, la destino logicamente alla sua porzione di network. Ma è così facile raggiungere questo risultato? La risposta è no, in molti casi l'uso delle soluzioni sopra elencate non è in grado di risolvere il problema dell'individuazione di un tentativo di accesso.

I Sistemi di Scansione in-band

Risulta allora essenziale, nei casi più complessi, rivolgersi ad Appliance di network specifiche, una soluzione percorribile quando si ha l'obiettivo di individuare l'accesso di un host alla rete e controllarne l'integrità. Il modo di implementare questo approccio si distingue poi in base alle tipologie di appliance, ne esistono alcune che lavorano in-line, altre out-of-band[2].

La soluzione in-line permette di "vedere" il traffico, di individuare gli host e di iniziare controlli di integrità e conformità post-accesso. Alternativamente le appliance in-line possono essere impiegate in concatenazione con i server DHCP o di Autenticazione e quindi poste in esercizio in maniera simile a quella discussa precedentemente. Per questi stessi motivi il loro utilizzo è meno desiderabile vista la facilità con la quale gli host possono bypassare i controlli di sicurezza, in questo caso. I vantaggi dell'impiego in-line di questi dispositivi NAC è dato dal fatto che essi possono vedere gli host che tentano l'accesso al network e possono controllarne il traffico efficacemente in quanto tutte le comunicazioni fluiscono attraverso di loro. Questo approccio porta però a investimenti ingenti in tempo e denaro costringendo alla reingegnerizzare l'architettura di rete.

I Sistemi di Scansione out-of-band

Una soluzione infine è data dall'impiego di appliance dedicate in maniera modalità "out-of-band".

Questo permette di raggiungere risultati ottimali soprattutto se l'appliance può essere in grado di mantenere una mappatura degli IP in tempo-reale e può essere capace di individuare quando un dispositivo necessita di essere controllato e verificato. In questo senso ci sono vari approcci. Alcuni usano PEP quali il DHCP o l'Authentication Server, o piuttosto architetture 802.1x. Altri puntano a mantenere un controllo sul traffico

1 In-line: sullo stesso segmento di rete Layer 2 e/o Layer 3 in maniera da costringere il traffico di autenticazione a passare prima per il proxy e poi per il Server di Autenticazione.

2 Out-of-Band con connessione separata ed esclusiva per i flussi comunicativi da e verso le risorse poste sotto analisi.

IP a livello 2 e 3 via NIDS (Network Intrusion Detection System) e ad usare l'ARP per isolare gli endpoint da testare rispetto a quelli già acceduti al network.

Gli aspetti positivi di questo approccio sono dovuti al fatto che l'host può essere controllato anche dopo l'accesso, che non si ha la necessità di implementare costose e dolorose migrazioni e che l'appliance si può integrare perfettamente con soluzioni quali 802.1x o può anche vivere di vita propria poggiandosi su procedure di autenticazione e su sistemi più semplici.

Le soluzioni attualmente percorribili.

Quanto finora espresso raccoglie la gran parte delle "filosofie" NAC attualmente disponibili sul mercato.

Esistono altri approcci che sono un ibrido di queste soluzioni, ma che comportano il più delle volte un onere aggiuntivo e non certo leggero: cambiare i dispositivi di rete Layer 2. Chi scrive si è trovato a valutare molte di queste soluzioni commerciali e ritengo che le soluzioni più efficienti e percorribili, anche perché meno onerose sono quelle legate alla scansione in-band con o senza 802.1x e quelle out-of-band che però ancora non riescono ad integrare 802.1x, ma solo ambiti ristretti che contemplano un'autenticazione di tipo single Sign-on e DHCP, soluzione questa che non gradisco per gli evidenti rischi di esposizione che possono indurre e che bene hanno evidenziato i ricercatori del gruppo Blackhat in una recente demo pubblicamente accessibile.

Di certo uno dei maggiori vantaggi che può introdurre il NAC è la possibilità di gestire sistemi agentless, ovvero sistemi che non hanno software interni che "parlino" con la struttura aziendale e la informino sullo "stato" della macchina. Queste soluzioni sono molto utili nella gestione delle macchine di consulenti, terze parti e ospiti.

Il modello di scansione in questo caso è determinante per garantire l'accesso alla rete anche alle sole porzioni inerenti e pensate per gli "ospiti" e quindi separate in vario modo dalla rete interna. Rimane il fatto che i modelli di scansione possibili, essendo le macchine ignote alla struttura, almeno in avvio, sono vari.

Esistono modalità di scansione completamente esterne e basate sul "comportamento" dell'host all'accesso, nelle quali la prima analisi si basa sulla valutazione delle porte "aperte" dall'host. Si possono poi invece incontrare sistemi di scansione più ingegnosi che costringono, all'avvio della connessione, il client che cerca di entrare, a scaricarsi un plugin Java che funge da agente di "sessione" per la scansione "dall'interno" dell'host stesso, ed esistono altre forme di controllo che vertono invece sul "comportamento post-accesso" da parte dell'host (sul principio degli IPS).

Di questi approcci finora quello che più sembra convincere è quello legato all'agente di sessione ("On-demand agentless NAC), agente che alla disconnessione o allo spegnimento della macchina andrà cancellato e dovrà essere quindi di nuovo scaricato al successivo accesso.

In effetti gli altri approcci cadono vittima, fatalmente, delle restrizioni imposte dai vari personal firewall ai tentativi di scansione dall'esterno e quindi non sembrano particolarmente efficaci e affidabili nella valutazione di un host.

La componente più importante in queste soluzioni è sicuramente il cosidetto Audit Server, l'elemento che stabilisce, con un'analisi sull'host, se questi è conforme o meno ai requisiti minimi di protezione e sicurezza necessari ad entrare nel network Extranet del nostro cliente.

Nel momento in cui i sistemi di primo controllo (quali ad esempio il RADIUS Server del protocollo 802.1x) smistano il compito di definire lo status dell'host al server di Audit, si attiva il processo di valutazione.

Il Sistema in questione può essere configurato con vari livelli di aderenza alle politiche aziendali, per semplicità si consideri il caso in cui esistano solo due profili: uno ***healthy*** (conforme) e uno ***unhealthy*** (non conforme). In realtà questi profili, come detto, potrebbero essere ulteriormente atomizzati in vari altri con vari livelli di conformità facendo si che al termine dell'Audit l'host possa ereditare un accesso più o meno ampio nella rete „ospiti".

I sistemi di Audit Pre-admission NAC possono arrivare ad analisi anche molto approfondite nei confronti degli host, individuando vulnerabilità più o meno note a diversi livelli di criticità.

È però da evidenziare che per avere un report completo dell'host occorrono vari minuti e questo complica notevolmente il lavoro dell'infrastruttura di analisi allorquando, come accade nelle grandi aziende, l'ingresso in rete delle risorse avviene in un intervallo temporale piuttosto ristretto.

La tendenza tecnologica, per risolvere questa problematica, volge a poter configurare il Server di Audit in modo da permettergli di svolgere analisi diverse attraverso l'identificazione e la differenziazione tra host completamente nuovi alla struttura e quelli che hanno già subito audit approfonditi nelle precedenti 24-72 ore. O ancora è possibile ridurre i tempi di analisi a circa 3 minuti sulla base di una selezione predeterminata di elementi da controllare o meno.

Dove può arrivare il NAC: I profili di Rischio

Nei sistemi On-Demand agentless NAC, una volta che un host sia individuato esso potrà essere testato. L'analisi può prendere varie forme, dal semplice controllo di autenticazione e dei servizi attivi fino a scansioni più approfondite del registro e delle applicazioni per determinare se il sistema operativo dell'host (OS) e le applicazioni di sicurezza rilevanti siano aggiornate o meno e aderiscano ai requisiti di sicurezza aziendali.

Deve essere evidenziato che le scansioni di Pre-Admission NAC sono generalmente rapide e verificano solo se un dispositivo sia conforme o meno alle policy di sicurezza o sia vulnerabile alle minacce, ma non produrrà molte informazioni su ipotetiche infezioni in corso. Questo rende chiaro come il tradizionale monitoraggio post-ammissione (Post-Admission) rimanga comunque un elemento critico e imprescindibile.

Aderenza alle Policy

La maggior parte delle soluzioni NAC presenta, almeno in minima parte, delle analisi sugli endpoint per il controllo della conformità dell'host alle policy come prerequisito per l'ammissione alla rete.

L'analisi degli endpoint identifica quelli non conformi ai criteri stabiliti dall'amministratore della Sicurezza. Questi test possono includere check per i servizi o le applicazioni, per esempio peer-to-peer (P2P) o FTP server, livelli di patch del Sistema Operativo, signature (aggiornamenti) dell'Antivirus e tutti i processi volti ad identificare dispositivi o utenti non gestiti o non autenticati.

Servizi Applicativi

Anche nel caso di sistemi On-Demand Il controllo ad un endpoint viene volto verso i processi in corso e i servizi vietati, come le applicazioni P2P, o richiesti, come il software Antivirus e altre applicazioni di sicurezza, ma il modo di condurre l'analisi è ovviamente facilitato con la distribuzione dell'agente in quanto il software impiegato sugli endpoint agisce come PEP, lasciando al Policy Server le funzioni di PDP per assicurare che i risultati definiti dagli agent sugli endpoint corrispondono alle policy di accesso configurate nel Server di Autenticazione.

Livello di aggiornamento del Sistema Operativo

È possibile spingere i controlli in questi sistemi di Audit NAC verso la valutazione delle patch del Sistema Operativo e conseguentemente al livello di esposizione alle vulnerabilità dell'endpoint. In questo senso le soluzioni commerciali variano equamente tra due approcci.

Nel primo approccio, un livello minimo di patch è testato sull'endpoint. L'host che non raggiunga il livello minimo di patch sarà inviato o all'area di quarantena o gli sarà impedito l'accesso. Il vantaggio di questo approccio è dato dalla chiara definizione dei requisiti di accesso e dalle conseguenze della mancata aderenza a questi requisiti: la quarantena o il blocco.

Ci sono anche dei contro, in ogni caso.

Per prima cosa nell'aggiornamento dei prerequisiti può essere problematico, al pari una stringente imposizione di costanti aggiornamenti può comportare complesse operazioni di *Software Distribution*. Inoltre, per controllare realmente il livello di patch senza aprire pericolose comunicazioni sugli endpoint, è necessario implementare agenti sulle macchine client.

Un secondo approccio è legato all'analisi delle vulnerabilità degli endpoint ad attacchi provenienti dall'infrastruttura. Questo approccio esamina cosa le patch del sistema operativo vogliono prevenire, per esempio vulnerabilità di servizi che possono essere utilizzati per exploit sui sistemi. Un vantaggio di questo approccio è che gli endpoint possono essere controllati dal network, senza agenti (*agentless*), per vulnerabilità definite dagli amministratori di rete e della sicurezza. Uno svantaggio è che questo approccio non identifica immediatamente i sistemi che necessitano di patch durante l'accesso alla rete. È possibile per un sistema proteggersi da una minaccia, ma contemporaneamente non avere un corretto livello di patch in quanto la minaccia era stata risolta attraverso work-around o metodi alternativi.

In generale è raccomandato l'uso di entrambi gli approcci *agentless*, sebbene questo vada ad impattare negativamente con l'ammontare di lavoro di gestione che gli amministratori di rete dovranno svolgere.

Livelli di Aggiornamento e Signature degli Antivirus

Un altro comune controllo svolto dai prodotti NAC è legato all'Antivirus (AV Signature level).

Il concetto dietro a questo metodo di controllo è che i dispositivi aggiornati sono meno esposti a contagi e minacce. Un agente all'interno dell'endpoint deve provvedere, interagendo con il Policy Server, a fornire indicazioni in merito al livello di aggiornamento delle Signature antivirali.

Un problema potrebbe sorgere allorquando ci si trovasse con una sola politica di controllo, quella antivirus appunto, come spesso accade.

Se il livello di aggiornamento dell'antivirus è l'elemento principale per determinare l'accesso o meno alla rete da parte dell'host, questo potrebbe portare a frequenti casi di utenti disconnessi, vista la frequenza con la quale gli aggiornamenti antivirali escono ogni settimana.

Il vero problema però è legato a tutti i possibili rischi che passano inosservati laddove sia solo l'antivirus Signature level il criterio di accesso NAC o laddove, per velocizzare l'accesso la scansione delle firme virali sia fatta in maniera approssimativa.

Vista la rapidità della diffusione di virus, questo approccio potrebbe non essere determinante nel bloccare infezioni virali non segnalate nei minuti appena successivi ad un'infestazione diffusa a livello globale (come nel caso di Nimda o di Code Red, per esempio).

Gestione dei dispositivi

Un controllo finale per gli endpoint che tentano accesso alla rete è determinato dal fatto che al loro presentarsi possano essere identificati come sistemi "conosciuti" o meno. Questo controllo è determinante nei confronti dell'infrastruttura e non degli host. O piuttosto solo di quegli host che non sono mai entrati nella rete e che dovranno per questo sottostare ad un livello di scansione molto più approfondito.

Quello che si deve verificare è che esistano metodi per "ricordare" l'host che già ha avuto accesso alla rete (credenziali erogate o registrazione di log) e che, una volta individuata una richiesta da parte di un host già conosciuto, si possa accettarlo senza doverlo sottoporre a pesanti e onerosi controlli che ha già subito, magari, pochi giorni prima. Ovviamente i test, approfonditi o meno, dovranno sempre essere svolti nell'area di stazionamento (Quarantena o Guest) prima di offrire accesso all'infrastruttura di rete.

Profilazione delle minacce

Un altro tipo di test che può essere condotto durante la fase di ammissione alla rete è quello sulle minacce. A differenza dei Policy check, che danno un'indicazione del profilo di rischio dell'endpoint, questi test sono effettuati con l'obiettivo di verificare il livello di minaccia che può presentare l'host al suo accesso alla rete.

Due sono gli approcci base per controllare le minacce di cui si possono far portatori gli endpoint:

- L'host può essere analizzato per minacce portate al momento del suo inserimento in rete,
- o può essere monitorato dal network per identificare le minacce che possono originarsi dall'endpoint stesso durante la normale attività quotidiana.

Test delle Infezioni

Controllare le minacce sugli endpoint può significare anche mantenere attiva una scansione antivirale ogni volta che si avvia una sessione web. Questi test sono piuttosto onerosi e votati ad intercettare sessioni minacciate o utilizzate dai più recenti virus. Ciò comporta che questo approccio possa essere usato raramente in quanto poco attendibile, poco efficace o piuttosto troppo oneroso da risultare ingestibile.

Questo tipo di scansione presenta inoltre lo svantaggio di non poter intercettare una minaccia "zero day", poiché in questo caso, per essere efficace, la signature Antivirus deve essere aggiornata e deve già contenere il virus dal quale ci si deve difendere. Manca quindi la possibilità di lavorare in maniera diversa da quella preordinata dal fornitore del software antivirus.ù

Individuazione delle minacce

Un secondo approccio alla profilazione delle minacce è dato dall'esame del traffico originato da un endpoint,

per identificare e fermare le minacce da esso stesso portate in seno alla rete.

Questo può condurre ad una *signature-based* o *behavioral-based* detection (individuazione basata su segnali o su comportamenti) attraverso l'analisi del traffico originato dall'endpoint.

Il vantaggio di questo approccio è che esso è trasparente all'utente finale e solitamente controlla il traffico dall'endpoint sia per l'accesso che durante le fasi successive dell'attività dell'host.

L'aspetto negativo è che, come le soluzioni antivirus, le soluzioni basate su ***signature*** devono essere aggiornate frequentemente e ci sono rischi di falsi positivi su molti dei sistemi che gestiscono le anomalie. È anche importante controllare la velocità di individuazione e la velocità di mitigazione, al momento dell'individuazione della minaccia, in quanto molte minacce si diffondono in pochi secondi.

Gli approcci al Pre-Admission NAC sono molto vari, al pari delle minacce che queste soluzioni sono destinate ad annullare. Ovviamente il Pre-Admission è solo una parte del puzzle. Per una soluzione NAC robusta, infatti, Post-Admission NAC, Quarantena e Remediation sono ambienti altrettanto necessari.

Terminologia

- EAP - Extensible Authentication Protocol
- EAPoL - Extensible Authentication Protocol over LAN
- EAPoW - Extensible Authentication Protocol over Wireless
- RADIUS - Remote Authentication Dial-In User Service. Un protocollo frequentemente utilizzato per l'autenticazione, l'autorizzazione e l'accounting di accesso alla rete centralizzato.
- X.509 - X.509 è uno standard ITU-T per infrastrutture a chiave pubblica (Public Key Infrastructure - PKI). X.509 definisce, tra le altre corse, i formati standard per certificati digitali ed un algoritmo per la validazione del percorso di certificazione.
- ACL - Access Control List
- LDAP - Lightweight Directory Access Protocol è un protocollo di rete utilizzato per interrogare e modificare servizi di directory su TCP/IP.
- VLAN - Il termine VLAN (Virtual LAN) indica un insieme di tecnologie che permettono di segmentare il dominio di broadcast, che si crea in una rete locale (tipicamente IEEE 802.3) basata su switch, in più reti non comunicanti tra loro.
- NAD – Network Access Device, indica il dispositivo di rete verso cui si dirige l'accesso da parte dell'host e congiuntamente il dispositivo che svolge la funzione di Policy Enforcement Point per le regole di accesso basate su controllo di conformità.
- PEP – Policy Enforcement Point, indica l'elemento di rete che, già secondo l'RFC 2753, dove si applicano i controlli e le policy in base alla conformità dell'host richiedente accesso.
- PDP – Policy Decision Point, è il Sistema server dove le politiche di Sicurezza vengono tradotte in controlli. Questo stesso Sistema Server è, secondo l'architettura definita nell'RFC 2753, il contenitore delle policy di controllo utilizzato per distribuire le stesse nella rete verso i vari PEP.