



La soluzione Cisco Network Admission Control (NAC)

Oggi non è più sufficiente affrontare le problematiche relative alla sicurezza con i tradizionali prodotti per la sola difesa perimetrale. È necessario adottare soluzioni più complete, integrate e in grado di operare in modo esteso e pervasivo all'interno della Rete.

Per questo motivo Cisco ha progettato il Cisco® Network Admission Control (NAC), una soluzione innovativa che consente di applicare le policy di sicurezza su tutti i dispositivi finali collegati (sia gestiti, sia non gestiti dal dipartimento IT di un'organizzazione), indipendentemente dalla loro modalità di accesso, appartenenza, tipologia del dispositivo, configurazione applicativa, modelli di remediation. Cisco NAC assicura una protezione proattiva per la propria infrastruttura, migliora la resilienza della Rete e permette inoltre di proteggere l'infrastruttura di rete dell'azienda in maniera profonda ed estesa.

I. IL PANORAMA ATTUALE

Sono molteplici e di diversi tipi le sfide e le minacce alla sicurezza delle informazioni che le aziende oggi devono affrontare:

Attacchi criminali a scopo di lucro. Negli ultimi attacchi e tentativi di violazione della sicurezza aziendale si nota come l'obiettivo sia sempre più spesso economico e sempre meno legato alla ricerca di notorietà o alla curiosità del singolo pirata informatico. Il worm 'Zotob', ad esempio, è apparso per la prima volta nel 2005 e ha attaccato grandi gruppi come la CNN. L'FBI ha dichiarato di avere prove concrete per collegare questo attacco ad un gruppo di persone coinvolte in frodi nel settore delle carte di credito¹. Lo spyware e la più recente e pervicace ondata di phishing - soprattutto ai danni dei Clienti di istituti finanziari - sono altri eclatanti esempi delle finalità sulle quali oggi si concentrano gli attacchi informatici più diffusi.

Rapida diffusione delle minacce. Le minacce alla sicurezza dei sistemi informativi aumentano con rapidità esponenziale. Il tempo tra la scoperta di una vulnerabilità e la disponibilità di codice maligno per sfruttarla è passato dall'ordine di grandezza dei mesi, a quello delle settimane, poi dei giorni e successivamente delle ore. Le difficoltà dovute a indisponibilità dei sistemi IT, al recupero dei dati e al ripristino dei sistemi compromessi a seguito di queste minacce sono aspetti costosi e assai difficili da prevenire. Alle aziende resta davvero troppo poco tempo per correre ai ripari se si affidano solamente a misure di sicurezza reattive.



Nuovi ambienti di business con ridotta sicurezza perimetrale. Numerosi fattori tendono a cambiare gli ambienti di business e a trasformarli da entità chiuse ad aperte e distribuite. In molte aziende vi sono ormai parecchi utenti mobili che portano i loro laptop e i dispositivi portatili dentro e fuori dagli uffici, dentro e fuori dalla rete aziendale; utenti connessi da accessi remoti in luoghi pubblici; partner con importanti contratti di outsourcing che hanno bisogno di accedere al network interno. Inoltre crescono le esigenze di connessione di ospiti e personale temporaneo presenti nelle sedi aziendali. In questo nuovo tipo di ambiente lavorativo la sicurezza tradizionale, basata su prodotti studiati per proteggere ambienti chiusi con perimetri ben definiti, non è più efficace, oltre che sostanzialmente anacronistica rispetto ai livelli di agilità e flessibilità imposti dai nuovi modelli organizzativi e di business tipici delle aziende estese. E gli stessi utenti tradizionali che operano da postazioni fisse in ufficio sono soggetti a minacce che arrivano da Internet, dalle e-mail e attraverso l'Instant messaging (IM) o applicazioni peer-to-peer (P2P).

Gestione aziendale, conformità e audit. La sicurezza informatica non è solo una sfida tecnologica ma anche un problema di corporate governance. Le aziende devono definire e adottare le proprie policy di sicurezza e di business, e impegnarsi seriamente nell'adozione di controlli efficaci basati su queste policy. La sicurezza informatica deve essere concordata dal management - come ogni altra decisione critica - e deve essere integrata con i criteri operativi dell'impresa, con adeguamenti e miglioramenti costanti nel tempo. Le aziende che adottano questo tipo di strategia ne godranno certamente i benefici nel tempo, sia in termini di sicurezza dei propri processi interni, sia a livello di affidabilità ed efficacia dei livelli di controllo.

Risorse limitate. Per molte aziende l'elenco dei potenziali obiettivi e delle relative misure di sicurezza è lungo e ciò si scontra direttamente con i limiti nella disponibilità di budget e personale IT qualificato. A ciò si aggiungono le difficoltà create da minacce sempre più complesse e sofisticate, gruppi di utenti diversificati, infrastrutture miste, e - spesso - attività male organizzate. Con budget e personale limitato le aziende devono puntare ad ottimizzare i processi, diminuire i costi e ridurre gli incidenti per affrontare efficacemente i problemi di sicurezza.

II. UNA STRATEGIA VINCENTE

Una strategia di sicurezza esauriente e di provata efficacia utilizza una corretta e oculata combinazione di **persone**, **processi** e **tecnologie** per risolvere al meglio tutte le problematiche di sicurezza.

Il primo elemento è il fattore umano: il top management dell'azienda deve supportare le iniziative e le policy di sicurezza (il cosiddetto 'approccio top-down'). Inoltre vi deve essere la consapevolezza che la sicurezza è anche responsabilità di ognuno, e può rendersi necessaria una massiccia campagna di informazione rivolta all'utente finale (in questo caso, con approccio 'bottom-up').

Ovviamente è poi anche necessario che un'azienda sia preparata a gestire la sicurezza sia nelle normali attività giornaliere, sia all'insorgere di un incidente, con controlli efficienti, policy di sicurezza aggiornate e processi ben definiti e organizzati.

Le aziende possono in effetti raggiungere elevati livelli di sicurezza: per ottenere ciò devono adottare le migliori tecnologie e i migliori prodotti disponibili, realizzare un'architettura e un'infrastruttura ben progettata, e creare una difesa multilivello, con policy di sicurezza applicate attraverso tutti i dispositivi del network. Il migliore software di protezione degli host, ad esempio, potrebbe risultare del tutto inefficace se non installato e attivato su tutti i dispositivi finali. Invece, un sistema di applicazione delle policy di sicurezza che operi non solo sui dispositivi propri dell'azienda, ma anche su tutti i sistemi che a qualunque titolo tentano l'accesso al network, potrebbe effettivamente assicurare che ogni richiesta di accesso sia conforme ai requisiti previsti dalle policy in vigore. Cisco è la prima a fornire tutto questo con NAC.

III. LA SOLUZIONE NAC DI CISCO

La soluzione NAC di Cisco permette di delegare al network la verifica e il controllo della conformità alle policy di sicurezza per tutte le periferiche che cercano di accedere alla rete. L'accesso è permesso solamente a dispositivi conformi e affidabili (inclusi PC, server, telefoni IP e stampanti), mentre può essere negato a periferiche non conformi che in tal caso vengono reindirizzate ad un'area di quarantena ed eventuale remediation.

Cisco NAC cambia radicalmente l'approccio alla sicurezza perché permette di definire e di adottare policy di sicurezza complete e granulari, che possono essere trasformate in regole processabili e applicabili in modo affidabile, sistematico, automatico e pervasivo dalla Rete, garantendo una sicurezza proattiva ed estesa a tutta l'azienda. Cisco NAC realizza tutto ciò attraverso un'architettura scalabile, con una componente centralizzata per la definizione delle policy, una componente di verifica e controllo distribuita a livello di rete e con la possibilità di avere un'integrazione allargata con altri prodotti e tecnologie per la sicurezza.





Cisco NAC è già disponibile, e viene rilasciato attraverso Cisco NAC Appliance (anche noto come Cisco Clean Access). Cisco NAC Appliance può essere rapidamente implementato in ogni rete aziendale, in aree circoscritte (come reti di accesso remoto o accessi wireless) per risolvere problematiche critiche in fatto di sicurezza. Cisco NAC Appliance fornisce valutazioni della conformità, autenticazioni dell'identità dell'utente, gestione ed attuazione delle policy, servizi di remediation in tutti i tipi di ambienti di rete. La soluzione si compone dei seguenti elementi:

Clean Access Manager. Clean Access Manager fornisce un'interfaccia Web per creare policy di sicurezza e gestire utenti online. Può funzionare anche come proxy di autenticazione per i server. Gli amministratori possono usare Clean Access Manager per stabilire ruoli-utenti, controlli della conformità e richieste di remediation. Clean Access Manager comunica e gestisce con Clean Access Server, che è il componente di attuazione della soluzione NAC.

Clean Access Server. Questo dispositivo di applicazione delle policy di sicurezza fornisce un'interfaccia Web per creare policy di sicurezza e gestire gli utenti online. Può essere implementato in-band o out-of-band, in Layer 2 o Layer 3, come gateway virtuale o come gateway IP reale, e può essere implementato centralmente o distribuito attraverso il network, perciò consente la massima flessibilità di implementazione per pressoché ogni possibile ambiente di rete e scelta di impiego.

Clean Access Agent (opzionale). Questo agente di sola lettura e minimo peso gira sui sistemi finali, quelli che richiedono l'accesso alla Rete. Clean Access Agent effettua una profonda ispezione preliminare del profilo di sicurezza di una macchina locale, analizzando il registro delle impostazioni, i servizi attivi e i file di sistema. Attraverso questa analisi si può determinare se una periferica ha installato e autorizzato un hotfix richiesto, la versione corretta del software antivirus, Cisco Security Agent (personal firewall, host intrusion detection/prevention system) e altri software per la sicurezza a livello client o host. Clean Access Agent è scaricabile anche in tempo reale all'atto della richiesta di connessione da parte di sistemi non gestiti (es. ospiti, consulenti, fornitori).

Cisco offre anche NAC Framework, che integra una infrastruttura di rete intelligente con soluzioni per oltre 90 tra i principali produttori di software antivirus, per la sicurezza e per la gestione della Sicurezza, delle Reti e dei Sistemi. Cisco NAC Framework fornisce lo stesso controllo delle policy di sicurezza di Cisco NAC Appliance e rappresenta un approccio 'embedded': integra infatti il controllo e l'applicazione delle policy di sicurezza all'interno degli stessi elementi di infrastruttura di una rete intelligente.

Cisco NAC Framework può essere ad ancora più alte prestazioni per alcuni clienti se sussiste una delle seguenti condizioni:

- Una profonda integrazione con un partner NAC
- L'implementazione di una soluzione 802.1x compatibile con NAC
- Cisco Secure Access Control Server (ACS) come server centrale di policy nell'implementazione di NAC.

Peraltro in futuro i componenti di Cisco NAC Appliance illustrati precedentemente saranno completamente interoperabili all'interno e con l'architettura NAC Framework qui descritta, fornendo la protezione degli investimenti dei clienti e un percorso di integrazione.

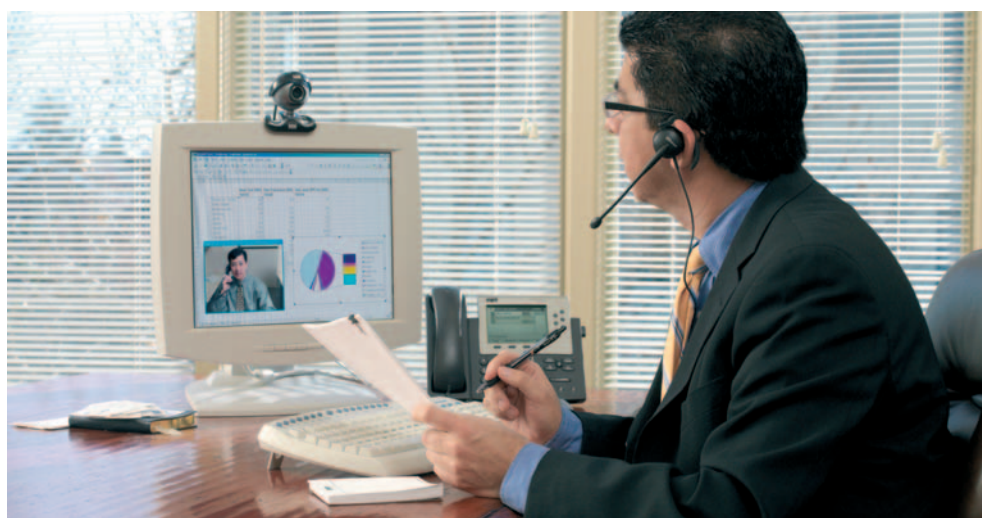
IV. I VANTAGGI DI CISCO NAC

Cisco NAC è una soluzione completa; può essere implementata con facilità, si integra pienamente con molte componenti di sicurezza pre esistenti e/o aggiuntive, e assicura una serie di vantaggi solitamente non disponibili attraverso prodotti che operano isolati a livello di singolo punto o di perimetro.

Proteggere le risorse (aziendali e non). Cisco NAC rappresenta una solida base per realizzare un'infrastruttura sicura, poiché garantisce che gli standard di configurazione richiesti dalle proprie policy di Sicurezza siano applicati a tutti gli asset, sia aziendali che esterni, prima ancora che ad essi sia assegnato un indirizzo IP all'atto della connessione alla Rete. Un asset management efficace ha poi come risultato la standardizzazione, la riduzione dei costi del ciclo di vita della soluzione e costi operativi inferiori.

Riduzione dei rischi legati alle vulnerabilità. Cisco NAC riduce e controlla su vasta scala usi impropri ed attacchi che sfruttano vulnerabilità, assicurando che tutte le periferiche in rete abbiano la protezione adatta installata e attivata (software antivirus, fix, patch e aggiornamenti di sicurezza, personal firewall). Questo è particolarmente utile per quelle aziende in cui gli asset aziendali sono controllati individualmente dagli utenti ai quali sono stati assegnati. Questi asset sono facili obiettivi per i virus, e un eventuale contagio ha ovviamente un immediato impatto negativo sulla produttività.

I software di sicurezza host-based da soli non risolvono il problema di un dispositivo non gestito, a causa della mancanza di meccanismi di rilascio. Cisco NAC fornisce una soluzione efficiente per imporre la conformità alle policy a tutti gli asset, indipendentemente dal fatto che siano gestiti direttamente dall'azienda oppure appartenenti ad un ospite, un consulente o un fornitore cui capita di connettersi alla Rete aziendale.





Prevenzione degli accessi non autorizzati. Cisco NAC può essere implementato anche in un ambiente aperto, permettendo agli ospiti di connettersi se rispettano determinati requisiti di sicurezza. Cisco NAC può assegnare diversi tipi di accesso al network in base alle credenziali e ai profili degli utenti; così, ad esempio, agli ospiti può essere fornito un accesso ad Internet senza per questo esporre il network interno a rischi. Cisco NAC può anche controllare le connessioni da una sede remota, e ciò è ovviamente molto utile quando si tratta di permettere la connessione ad un partner in applicazioni extranet. Si tratta di un caso delicato, nel quale è solitamente impossibile determinare esattamente chi si sta collegando alla rete dalla sede del partner. La possibilità di controllare l'accesso prima, durante e dopo che un utente è stato autenticato fornisce uno schema molto efficace per il mantenimento della sicurezza e la protezione delle informazioni riservate dell'azienda.

Conformità alle policy e riduzione delle minacce interne. Cisco NAC aumenta il livello di controllo perché offre un'applicazione delle policy di sicurezza in maniera capillare, granulare e diffusa sull'intera rete, permettendo alle aziende di ridurre le minacce alla sicurezza causate dalla vulnerabilità del perimetro, da accessi non autorizzati e dal rischio di attacchi interni. Applicando le policy di sicurezza, Cisco NAC supporta le aziende anche nel rispetto delle richieste di conformità alle normative, come quelle sulla Privacy, la Sarbanes-Oxley, l'HIPAA e GLBA e quelle orientate al controllo del rischio operativo, quali Basilea II e le direttive di Banca d'Italia per le Aziende che operano nel settore dei servizi finanziari.

Cisco NAC permette agli utenti e ai loro sistemi di rispettare le policy ed essere protetti anche quando lavorano in ambienti differenti. Cisco NAC mette in quarantena le periferiche non conformi, in modo che non siano utilizzate per nascondere la provenienza di un attacco, e successivamente le può aggiornare per renderle conformi alle policy. Oltre alle funzionalità di autenticazione, Cisco NAC può registrare e analizzare le attività dell'utente. Le informazioni presenti nel registro di log possono essere usate per migliorare la reazione ad attacchi o per essere usate come prova o come strumento di analisi forensica e reportistica.

Il ritorno dell'investimento è calcolabile. Cisco NAC permette un ritorno dell'investimento (ROI) rapido e quantificabile. I clienti possono calcolare il risparmio basandosi sulle minacce e i rischi che un'azienda intende affrontare efficacemente usando NAC. I clienti enterprise che recentemente hanno adottato Cisco NAC, ad esempio, hanno calcolato che subiscono ogni anno tra i 3.000 e i 4.000 incidenti relativi a PC con accessi non controllati alla loro rete.

Usando un modello di questo tipo, basato sul costo degli incidenti, si stima che ogni incidente costi tra i 750 e i 1.000 dollari. Di conseguenza il costo della soluzione Cisco NAC verrebbe coperto in un lasso di tempo che va dai sei ai nove mesi, permettendo successivamente milioni di dollari di risparmio annuale³.

Integrazione e collaborazione con Cisco Self-Defending Network. Cisco NAC è un elemento strategico di Cisco Self-Defending Network. Operando insieme ad altri componenti Self-Defending Network come Cisco Security Agent e Cisco Security Monitoring, Analysis e Response System (Cisco Security MARS), Cisco NAC aiuta le aziende ad ottenere una più accurata identificazione e prevenzione delle minacce, e inoltre aumenta l'efficienza del patch management. In breve, Cisco NAC fornisce sicurezza proattiva per l'infrastruttura aziendale e migliora notevolmente la resilienza della rete. Questo permette una difesa estesa e profonda dell'infrastruttura di rete. Un ambiente stabile, efficiente e sicuro aiuta le aziende a migliorare la produttività dei dipendenti, a proteggere le informazioni confidenziali, a ridurre i costi totali del ciclo di vita della soluzione e, in ultima istanza, ad affrontare con successo le sfide dei mercati.

Per maggiori informazioni: <http://www.cisco.com/go/nac/>

Note

1. Lattacco Zotob è connesso ad un tentativo di frode con le carte di credito:

<http://www.securityfocus.com/news/11297>

2. Cisco NAC Partner Program:

<http://www.cisco.com/go/nac/program>

3. I risparmi ed il ROI ottenibili con Cisco NAC ROI in ambito enterprise:

http://searchnetworking.techtarget.com/originalContent/0,289142,sid7_gcit195099,00.html



Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706 USA
<http://www.cisco.com>
Tel.: 001 408 526-4000
Fax: 001 408 526-4100

Sede italiana
Cisco Systems Italy
Via Torri Bianche, 7
20059 Vimercate (MI)
<http://www.cisco.com/it>
Numero verde: 800 787854
Fax: 039 6295 299

Filiale di Roma
Cisco Systems Italy
Via del Serafico, 200
00142 Roma
Numero verde: 800 787854
Fax: 06 51645001

Le filiali Cisco nel mondo sono oltre 200. Gli indirizzi, i numeri di telefono e di fax sono disponibili sul sito Cisco all'indirizzo: www.cisco.com/go/offices.

©2007 Dicembre Cisco Systems, Inc. Tutti i diritti riservati. CCVP, il logo Cisco, and il logo Cisco Square Bridge sono marchi registrati di Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn è un service mark di Cisco Systems, Inc.; Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, il logo Cisco Certified Internetwork Expert, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, il logo Cisco Systems, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, il logo iQ, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, e TransPath sono marchi registrati di Cisco Systems, Inc. e/o di società partner negli Stati Uniti e in determinati altri paesi.

Tutti gli altri marchi o marchi registrati in questo documento o sul sito Web sono proprietà delle rispettive aziende. L'utilizzo della parola partner non implica una relazione di partnership tra Cisco e qualsiasi altra azienda.