Vantaggi e svantaggi delle restrizioni di accesso al computer

Sommario

Introduzione

Questo documento descrive un problema incontrato con Machine Access Restriction (MAR) e fornisce una soluzione al problema.

Con la crescita dei dispositivi personali, è più importante che mai per gli amministratori di sistema fornire un modo per limitare l'accesso a determinate parti della rete solo alle risorse aziendali. Il problema descritto in questo documento riguarda la modalità di identificazione sicura di queste aree problematiche e la relativa autenticazione senza interruzioni della connettività degli utenti.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di 802.1x per una comprensione completa del presente documento. Questo documento presuppone una certa familiarità con l'autenticazione 802.1x dell'utente ed evidenzia i problemi e i vantaggi legati all'uso di MAR e, più in generale, all'autenticazione della macchina.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Problema

In sostanza, MAR tenta di risolvere un problema comune inerente alla maggior parte dei metodi EAP (Extensible Authentication Protocol) attuali e diffusi, ovvero che l'autenticazione del computer e l'autenticazione dell'utente sono processi separati e non correlati.

L'autenticazione utente è un metodo di autenticazione 802.1x familiare alla maggior parte degli amministratori di sistema. L'idea è che le credenziali (nome utente/password) vengano fornite a ogni utente e che l'insieme di credenziali rappresenti una persona fisica (può essere condiviso anche tra più persone). Pertanto, un utente può accedere da qualsiasi punto della rete con queste credenziali.

L'autenticazione di un computer è tecnicamente la stessa, ma in genere all'utente non viene richiesto di immettere le credenziali (o il certificato); il computer o la macchina lo fa da solo. È necessario che il computer disponga già di credenziali archiviate. Il nome utente inviato è **host/<MyPCHostname>**, a condizione che nel computer in uso **<MyPCHostname>** sia impostato come nome host. In altre parole, invia l'**host/** seguito dal nome host.

Sebbene non sia direttamente correlato a Microsoft Windows e Cisco Active Directory, il rendering di questo processo risulta più semplice se il computer viene aggiunto ad Active Directory perché il nome host del computer viene aggiunto al database del dominio e le credenziali vengono negoziate (e rinnovate ogni 30 giorni per impostazione predefinita) e archiviate nel computer. Ciò significa che l'autenticazione del computer è possibile da qualsiasi tipo di dispositivo, ma il rendering è molto più semplice e trasparente se il computer viene aggiunto ad Active Directory e le credenziali rimangono nascoste all'utente.

MAR come soluzione

Èfacile dire che la soluzione è destinata a Cisco Access Control System (ACS) o Cisco Identity Services Engine (ISE) per completare il processo di implementazione del protocollo MAR, ma prima di procedere è necessario valutare alcuni vantaggi e svantaggi. Come implementarlo è meglio descritto nelle guide per l'utente ACS o ISE, quindi questo documento descrive semplicemente se prenderlo in considerazione o meno, e alcuni possibili ostacoli.

I pro

La tecnologia MAR è stata inventata perché le autenticazioni utente e macchina sono totalmente separate. Pertanto, il server RADIUS non può imporre una verifica in base alla quale gli utenti devono eseguire l'accesso da dispositivi di proprietà della società. Con MAR, il server RADIUS (ACS o ISE, sul lato Cisco) impone, per una determinata autenticazione utente, che deve esistere un'autenticazione valida del computer nelle X ore (generalmente 8 ore, ma configurabile) che precedono l'autenticazione utente per lo stesso endpoint.

Pertanto, l'autenticazione di un computer ha esito positivo se le credenziali del computer sono note al server RADIUS, in genere se il computer fa parte del dominio, e il server RADIUS verifica questa condizione con una connessione al dominio. Spetta interamente all'amministratore di rete determinare se l'autenticazione di un computer ha esito positivo e consente l'accesso completo alla rete o se l'accesso è limitato; in genere, viene almeno aperta la connessione tra il client e Active Directory in modo che il client possa eseguire azioni quali il rinnovo della password utente o il download di oggetti Criteri di gruppo.

Se l'autenticazione dell'utente proviene da un dispositivo in cui non è stata effettuata l'autenticazione del computer nelle ultime due ore, l'utente viene rifiutato, anche se l'utente è normalmente valido.

L'accesso completo viene concesso a un utente solo se l'autenticazione è valida e completata da un endpoint in cui si è verificata l'autenticazione del computer nelle ultime due ore.

Svantaggi

In questa sezione vengono descritti gli svantaggi dell'utilizzo di MAR.

Supplicant MAR e Microsoft Windows

L'idea alla base di MAR è che per il successo di un'autenticazione utente, non solo l'utente deve avere credenziali valide, ma anche un'autenticazione computer riuscita deve essere registrato da quel client. In caso di problemi, l'utente non può eseguire l'autenticazione. Il problema che si verifica è che questa funzione a volte può bloccare inavvertitamente un client legittimo, il che costringe il client a riavviare per riottenere l'accesso alla rete.

Microsoft Windows esegue l'autenticazione del computer solo all'avvio (quando viene visualizzata la schermata di accesso); non appena l'utente immette le credenziali utente, viene eseguita l'autenticazione dell'utente. Inoltre, se l'utente si disconnette (torna alla schermata di accesso), viene eseguita una nuova autenticazione del computer.

Di seguito è riportato uno scenario di esempio che illustra il motivo per cui a volte MAR causa problemi:

L'utente X ha lavorato tutto il giorno sul suo laptop, che era collegato tramite una connessione wireless. Alla fine della giornata, chiude semplicemente il notebook e lascia il lavoro. In questo modo il notebook entra in modalità di sospensione. Il giorno successivo, torna in ufficio e apre il suo portatile. Ora non riesce a stabilire una connessione wireless.

Quando viene sospeso, Microsoft Windows acquisisce un'istantanea del sistema nello stato corrente, che include il contesto dell'utente connesso. Durante la notte, la voce della cache MAR per il notebook utente scade e viene eliminata. Tuttavia, quando il laptop è acceso, non esegue l'autenticazione del computer. Al contrario, entra direttamente in un processo di autenticazione dell'utente, dal momento che questo è ciò che ha registrato l'ibernazione. L'unico modo per risolvere il problema è disconnettere l'utente o riavviare il computer.

Anche se MAR è una buona funzionalità, può causare interruzioni alla rete. Queste interruzioni sono difficili da risolvere finché non si comprende il funzionamento di MAR; quando si implementa il sistema MAR, è importante informare gli utenti finali su come spegnere correttamente i computer e disconnettersi da ogni computer alla fine di ogni giornata.

Server MAR e RADIUS

Ècomune disporre di più server RADIUS nella rete a scopo di bilanciamento del carico e ridondanza. Non tutti i server RADIUS supportano tuttavia una cache di sessione MAR condivisa. Solo ACS versione 5.4 e successive e ISE versione 2.3 e successive supportano la sincronizzazione della cache MAR tra i nodi. Prima di queste versioni, non è possibile eseguire l'autenticazione di un computer su un server ACS/ISE e l'autenticazione di un utente su un altro, in

quanto non corrispondono.

MAR e switching wireless cablato

La cache MAR di molti server RADIUS si basa sull'indirizzo MAC. Si tratta semplicemente di una tabella con l'indirizzo MAC dei notebook e la data e l'ora dell'ultima autenticazione di sistema riuscita. In questo modo, il server può sapere se il client è stato autenticato dal computer nelle ultime X ore.

Tuttavia, cosa succede se si avvia il notebook con una connessione cablata (e quindi si esegue l'autenticazione di un computer dal MAC cablato) e poi si passa al wireless durante il giorno? Il server RADIUS non è in grado di correlare l'indirizzo MAC wireless all'indirizzo MAC cablato e di verificare di essere stati autenticati dal computer nelle ultime X ore. L'unico modo è disconnettersi e richiedere a Microsoft Windows di eseguire l'autenticazione di un altro computer tramite la modalità wireless.

Soluzione

Tra le molte altre funzionalità, Cisco AnyConnect ha il vantaggio di profili preconfigurati che attivano l'autenticazione del computer e dell'utente. Tuttavia, si verificano le stesse limitazioni di Microsoft Windows supplicant, per quanto riguarda l'autenticazione del computer che si verifica solo alla disconnessione o al riavvio.

Inoltre, con AnyConnect versione 3.1 e successive, è possibile eseguire EAP-FAST con il concatenamento EAP. Si tratta fondamentalmente di una singola autenticazione, in cui vengono inviate due coppie di credenziali, il nome utente/password del computer e il nome utente/password dell'utente, contemporaneamente. In questo modo, ISE può verificare con maggiore facilità il successo di entrambe le soluzioni. Senza l'utilizzo della cache e senza la necessità di recuperare una sessione precedente, si ottiene una maggiore affidabilità.

All'avvio del PC, AnyConnect invia solo l'autenticazione del computer, in quanto non sono disponibili informazioni sull'utente. Tuttavia, dopo l'accesso dell'utente, AnyConnect invia contemporaneamente le credenziali del computer e dell'utente. Inoltre, se il cavo viene scollegato o scollegato/ricollegato, sia la macchina che le credenziali dell'utente vengono nuovamente inviate con un'unica autenticazione EAP-FAST, che è diversa dalle versioni precedenti di AnyConnect senza concatenamento EAP.

EAP-TEAP è la soluzione migliore a lungo termine, in quanto è fatta soprattutto per supportare questo tipo di autenticazione, ma EAP-TEAP non è ancora supportato nel supplicant nativo di molti sistemi operativi a partire da oggi