Best practice e considerazioni sull'implementazione ISE Posture

Sommario

Introduzione

Questo documento descrive alcune configurazioni di base che risolvono diversi casi di utilizzo con la postura basata sul reindirizzamento. In queste configurazioni il client rimane conforme, ma il dispositivo di accesso alla rete (NAD) limita l'accesso in quanto si trova nello stato di reindirizzamento.

Restrizioni

Le configurazioni riportate in questo documento funzionano per i Cisco NAD, ma non necessariamente per i NAD di terze parti.

Comportamento client postura

Il client di postura attiverà le sonde in questi momenti:

- Accesso iniziale
- Modifica layer 3 (L3)/Modifica NIC (Network Interface Card) (nuovo indirizzo IP, modifica stato NIC)

Scenari d'uso

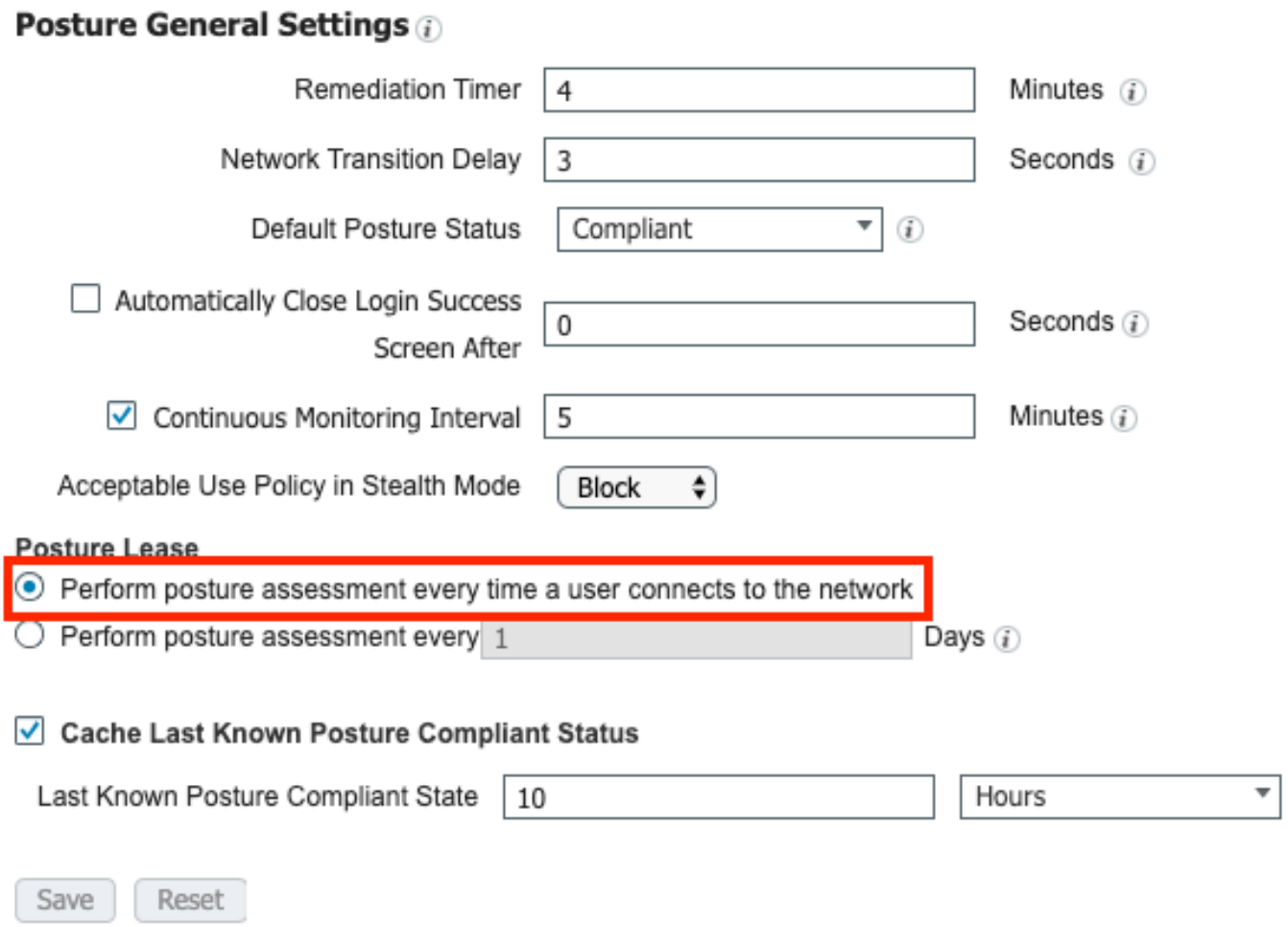
Caso di utilizzo 1 - La riautenticazione del client forza NAD a generare un nuovo ID

sessione.

In questo caso di utilizzo, il client è ancora conforme, ma a causa della riautenticazione, NAD si trova nello stato di reindirizzamento (URL di reindirizzamento e elenco degli accessi).

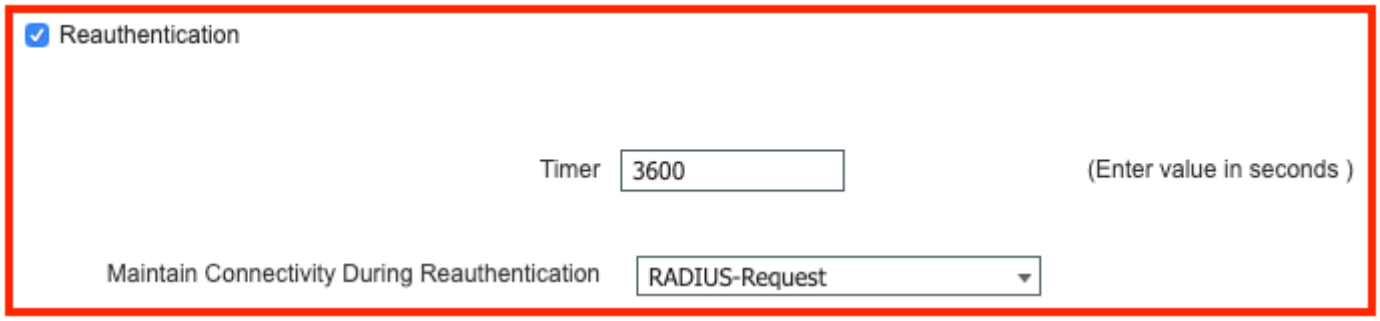
Per impostazione predefinita, Identity Services Engine (ISE) è configurato in modo da eseguire una valutazione della postura ogni volta che si connette alla rete, in particolare per ogni nuova sessione.

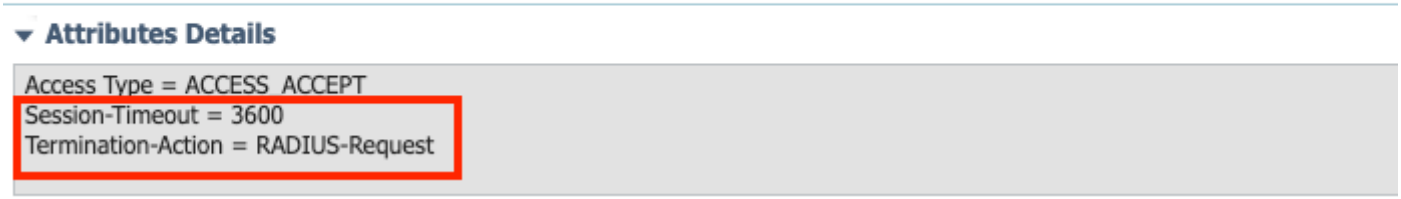
Questa impostazione è configurata in Centri di lavoro > Postura > Impostazioni > Impostazioni generali postura.



Per evitare che NAD generi un nuovo ID sessione alla riautenticazione, configurare i valori di riautenticazione nel profilo di autorizzazione. Il timer di riautenticazione visualizzato non è un suggerimento standard. I timer di riautenticazione devono essere considerati per ogni distribuzione in base al tipo di connessione (wireless/cablata), alla progettazione (quali sono le regole di persistenza nel bilanciamento del carico) e così via.

Criterio > Elementi criterio > Risultati > Autorizzazione > Profili autorizzazione





Sugli switch, è necessario configurare ciascuna interfaccia, o modello, per ottenere il timer di riautenticazione da ISE.

```
authentication timer reauthenticate server
```

> **Nota:** Se è disponibile un servizio di bilanciamento del carico, è necessario verificare che la persistenza sia configurata in modo che le riautenticazioni vengano restituite al servizio criteri originale (PSN).

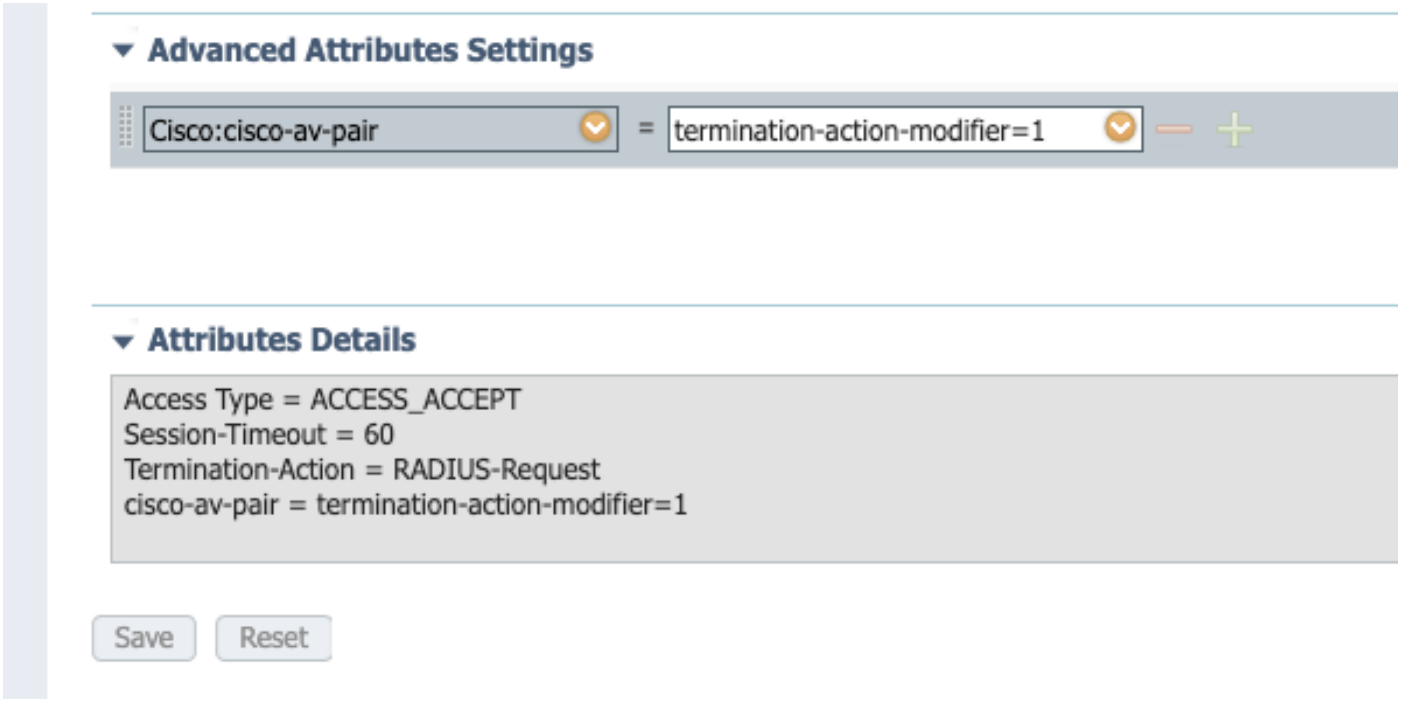
Caso di utilizzo 2 - Lo switch è configurato con ordine MAB DOT1X e priorità DOT1X MAB (cablato).

In questo caso, le riautenticazioni verranno terminate, perché verrà inviato un arresto di accounting per la sessione 802.1x quando si tenta di ignorare l'autenticazione MAC (MAB) durante la riautenticazione.

- L'arresto dell'accounting inviato per il processo MAB quando l'autenticazione non riesce è corretto, in quanto il nome utente del client passa dal nome utente 802.1X al nome utente MAB.
- Anche il dot1x come ID metodo nell'interruzione della contabilità è corretto, in quanto il metodo di autorizzazione era dot1x.
- Quando il metodo Dot1x ha esito positivo, invia un inizio di accounting con ID metodo come dot1x. Anche qui, questo comportamento è come previsto.

Per risolvere il problema, configurare cisco-av-pair:terminal-action-modifier = 1 sul profilo authZ utilizzato quando un endpoint è conforme. Questa coppia attributo-valore (AV) specifica che NAD deve riutilizzare il metodo scelto nell'autenticazione originale indipendentemente dall'ordine

configurato.



Caso di utilizzo 3 - I client wireless eseguono il roaming e le autenticazioni per i diversi access point vengono inviate a controller diversi.

In questo caso, la rete wireless dovrà essere progettata in modo che i punti di accesso (AP) a portata di altri AP per il roaming utilizzino lo stesso controller attivo. Un esempio è rappresentato dal failover di switching stateful (SSO) del controller WLC (Wireless LAN Controller). Per ulteriori informazioni su High Availability (HA) SSO per WLC, vedere High Availability (SSO) Deployment Guide.

Caso di utilizzo 4 - Installazioni con load balancer (Patch 6 precedente alla 2.6, Patch P2 2.7 e Patch 3.0).

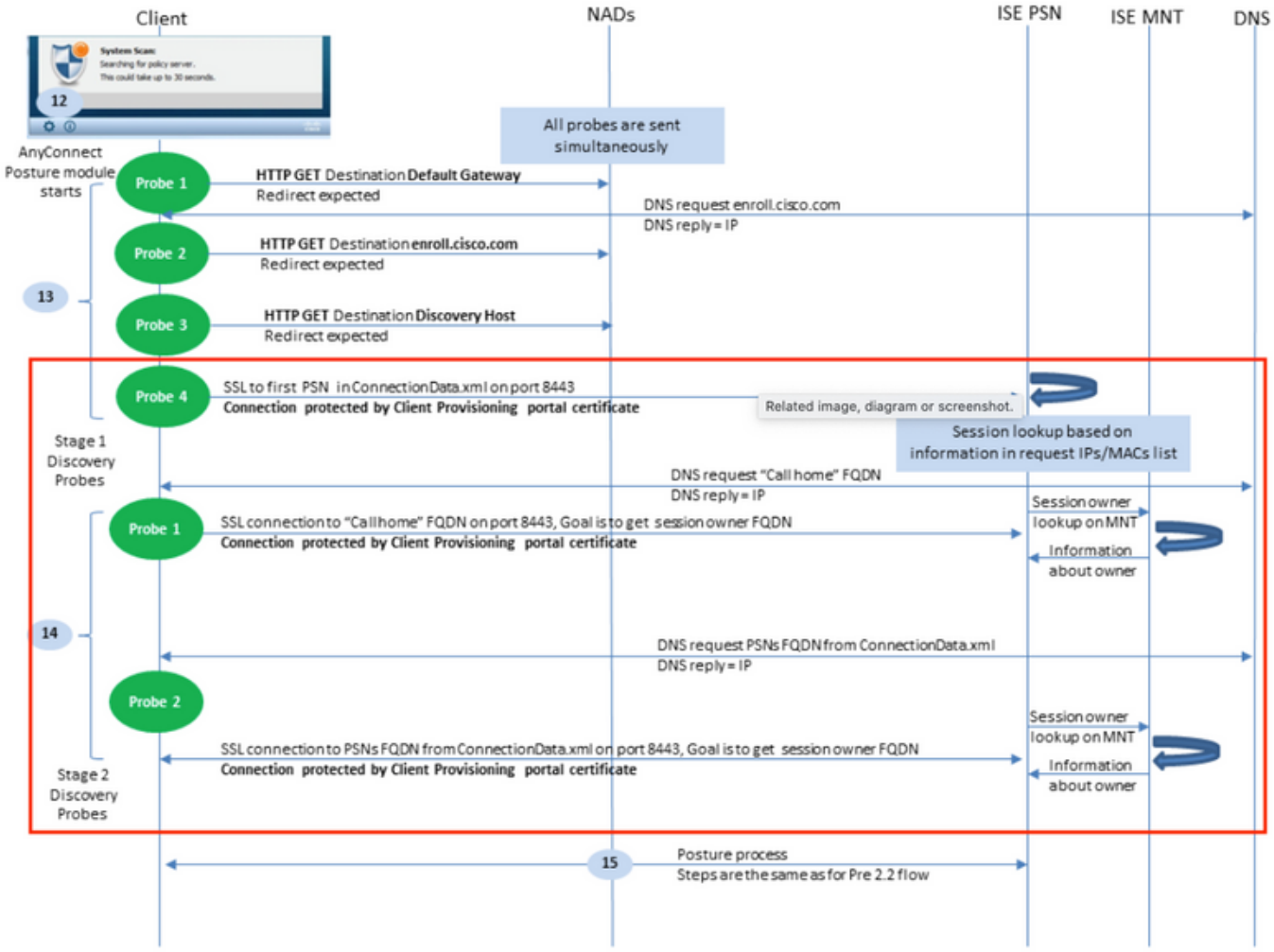
Nelle distribuzioni con bilanciamenti del carico coinvolti, è importante assicurarsi che, dopo aver apportato le modifiche nei casi di utilizzo precedenti, le sessioni continuino a passare allo stesso PSN. Prima delle versioni/patch elencate per questo passo, lo stato della postura non viene replicato tra i nodi tramite Light Data Distribution (in precedenza Light Session Directory). Per questo motivo, è possibile che diversi PSN restituiscano risultati di stato di postura diversi.

Se la persistenza non è configurata correttamente, le sessioni che eseguono la riautenticazione potrebbero passare a un PSN diverso da quello utilizzato in origine. In questo caso, il nuovo PSN potrebbe contrassegnare lo stato di conformità delle sessioni come sconosciuto e passare il risultato authZ con l'elenco di controllo di accesso (ACL)/URL di reindirizzamento e limitare l'accesso agli endpoint. Anche in questo caso, questo cambiamento sul NAD non sarebbe riconosciuto dal modulo di postura e le sonde non saranno attivate.

Per ulteriori informazioni su come configurare i load balancer, vedere la Guida all'implementazione di Cisco e F5: ISE Load Balancing con BIG-IP. Offre una panoramica di alto livello e la configurazione specifica F5 di un progetto di best practice per le implementazioni ISE in un ambiente con carico bilanciato.

Caso di utilizzo 5 - Le richieste di rilevamento della fase 2 vengono risposte da un server diverso da quello con cui il client viene autenticato (Patch 6 precedente alla 2.6, Patch 2 2.7 e 3.0).

Date un'occhiata alle sonde all'interno del riquadro rosso in questo diagramma.



I PSN memorizzano i dati della sessione per cinque giorni, quindi a volte i dati della sessione per una sessione "conforme" continuano a esistere sul PSN originale anche se il client non esegue più l'autenticazione con quel nodo. Se alle richieste incluse nella casella rossa viene risposto da un PSN diverso da quello che attualmente autentica la sessione E che il PSN ha precedentemente posseduto e contrassegnato come conforme a questo endpoint, è possibile che vi sia una mancata corrispondenza tra lo stato di postura del modulo di postura sull'endpoint e il PSN di autenticazione corrente.

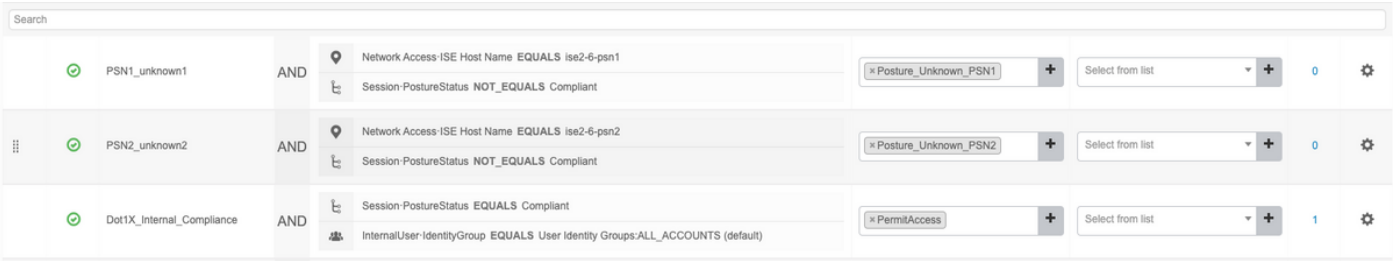
Di seguito sono riportati alcuni scenari comuni in cui può verificarsi questa mancata corrispondenza:

- Quando un endpoint si disconnette dalla rete, non viene ricevuta alcuna interruzione di accounting.
- Failover di NAD da un PSN a un altro.
- Un load balancer inoltra le autenticazioni a diversi PSN per lo stesso endpoint.

Per proteggersi da questo comportamento, ISE può essere configurato in modo da consentire solo alle sonde di rilevamento di un particolare endpoint di raggiungere il numero PSN su cui è attualmente autenticato. A tale scopo, configurare un criterio di autorizzazione diverso per ogni

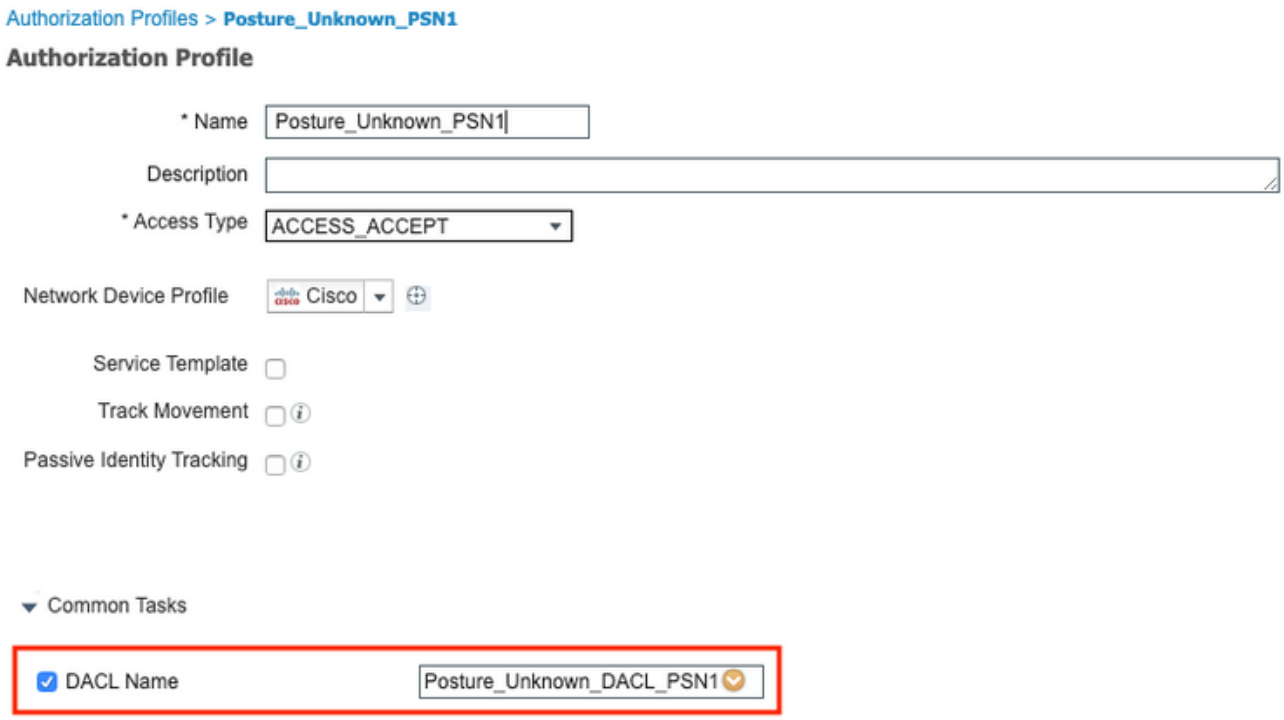
PSN nella distribuzione. In questi criteri, fare riferimento a un profilo authZ diverso contenente un elenco di controllo di accesso scaricabile (DACL, Downloadable Access Control List) che consente di eseguire le richieste SOLO al numero PSN specificato nella condizione authZ. Vedere questo esempio:

Ogni PSN avrà una regola per lo stato di postura sconosciuto:

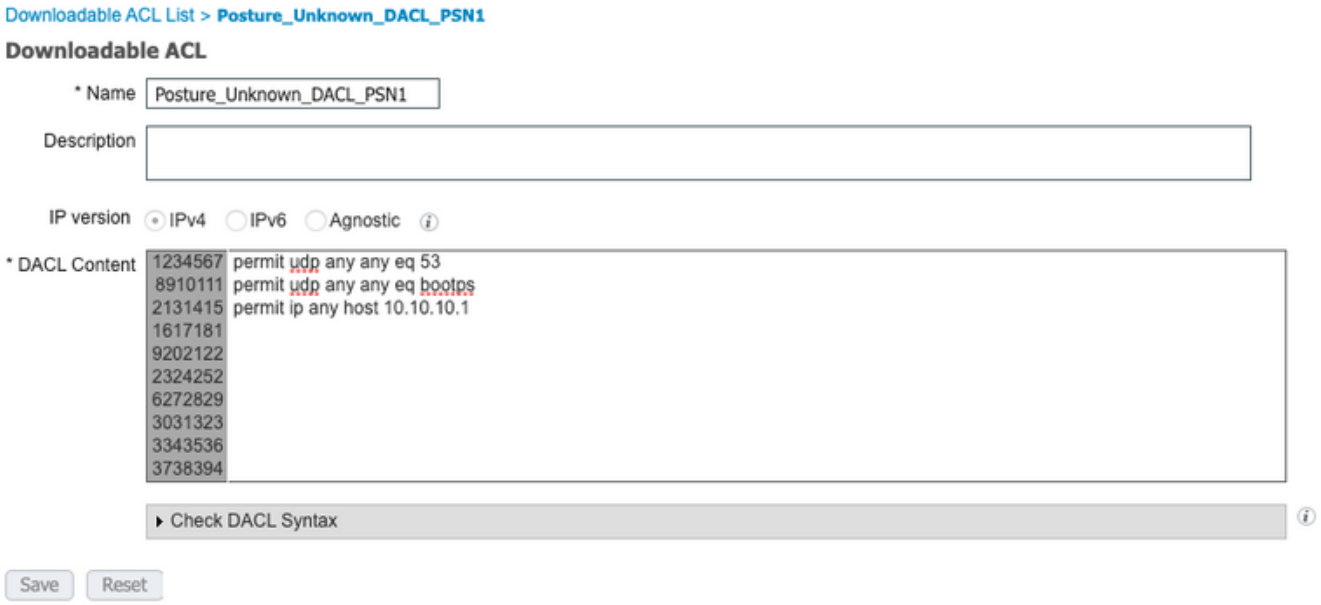


Ogni singolo profilo fa riferimento a un DACL diverso.

Nota: Per le configurazioni wireless, usare gli ACL Airespace.



Ogni DACL consente solo l'accesso probe al PSN che gestisce l'autenticazione.



Nell'esempio precedente, 10.10.10.1 è l'indirizzo IP del PSN 1. Il DACL a cui si fa riferimento può essere modificato per qualsiasi servizio/IP aggiuntivo in base alle esigenze, ma deve limitare l'accesso solo al PSN che gestisce l'autenticazione.

Patch 6, Patch 2 e Patch 3.0 per modifica comportamento post 2.6

Lo stato della postura è stato aggiunto nella directory di sessione RADIUS tramite il framework Distribuzione dati luce. Ogni volta che si riceve un aggiornamento dello stato di postura in un PSN, questo verrà replicato in TUTTI i PSN della distribuzione. Una volta applicata la modifica, le implicazioni delle autenticazioni e/o delle richieste che raggiungono diversi PSN su diverse autenticazioni vengono rimosse e qualsiasi PSN deve essere in grado di rispondere a tutti gli endpoint indipendentemente dal punto in cui sono attualmente autenticati.

Nei cinque casi di utilizzo descritti in questo documento, tenere in considerazione i seguenti comportamenti:

Caso di utilizzo 1 - La riautenticazione del client forza NAD a generare un nuovo ID sessione. Il client è ancora conforme, ma a causa della riautenticazione, NAD si trova nello stato di reindirizzamento (URL di reindirizzamento e elenco degli accessi).

- Il comportamento non cambia e la configurazione deve essere ancora implementata sull'ISE e sui NAD.

Caso di utilizzo 2 - Lo switch è configurato con ordine MAB DOT1X e priorità DOT1X MAB (cablato).

- Il comportamento non cambia e la configurazione deve essere ancora implementata sull'ISE e sui NAD.

Caso di utilizzo 3 - I client wireless eseguono il roaming e le autenticazioni per i diversi access point vengono inviate a controller diversi.

- Il comportamento non cambia e la configurazione deve essere ancora implementata sull'ISE e

sui NAD.

Caso di utilizzo 4 - Distribuzioni con load balancer.

- È comunque necessario seguire le best practice definite nella guida al bilanciamento del carico, ma nel caso in cui le autenticazioni vengano inoltrate a diversi PSN dal bilanciamento del carico, lo stato di postura corretto deve essere restituito al client.

Caso di utilizzo 5 - I probe di individuazione della fase 2 ricevono risposta da un server diverso da quello con cui il client viene autenticato

- Il nuovo comportamento non dovrebbe causare problemi e il profilo di autorizzazione per PSN non dovrebbe essere necessario.

Considerazioni sulla gestione dello stesso ID sessione

Quando si utilizzano i metodi elencati in questo documento, un utente che rimane connesso alla rete potrebbe rimanere conforme per lunghi periodi di tempo. Anche se vengono riautenticati, l'ID sessione non cambia e pertanto ISE continuerà a passare il risultato AuthZ per la regola corrispondente allo stato di conformità.

In questo caso, è necessario configurare la rivalutazione periodica in modo che la postura sia necessaria per garantire la conformità dell'endpoint alle policy aziendali a intervalli definiti.

Questa può essere configurata in Centri di lavoro > Postura > Impostazioni > Configurazioni di rimessa.