Configurazione dell'integrazione di Active Directory con Firepower Appliance per l'autenticazione del portale captive & Single-Sign-On

Sommario

Introduzione

In questo documento viene descritta la configurazione dell'autenticazione Captive Portal (autenticazione attiva) e Single Sign-On (autenticazione passiva).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Dispositivi Sourcefire Firepower
- Modelli di dispositivi virtuali
- LDAP (Light Weight Directory Service)
- Firepower UserAgent

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Firepower Management Center (FMC) versione 6.0.0 e successive
- Sensore Firepower versione 6.0.0 e successive

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.

Premesse

L'autenticazione Captive Portal o l'autenticazione attiva richiede una pagina di accesso e le credenziali utente sono necessarie affinché un host possa accedere a Internet.

L'autenticazione Single Sign-On o passiva fornisce all'utente l'autenticazione senza interruzioni per le risorse di rete e l'accesso a Internet senza più occorrenze delle credenziali utente. L'autenticazione Single Sign-On può essere eseguita tramite l'agente utente Firepower o l'autenticazione del browser NTLM.

Nota: per l'autenticazione Captive Portal, l'accessorio deve essere in modalità di routing.

Configurazione

Passaggio 1. Configurare l'agente utente Firepower per Single Sign-On

Questo articolo spiega come configurare l'agente utente Firepower in un computer Windows:

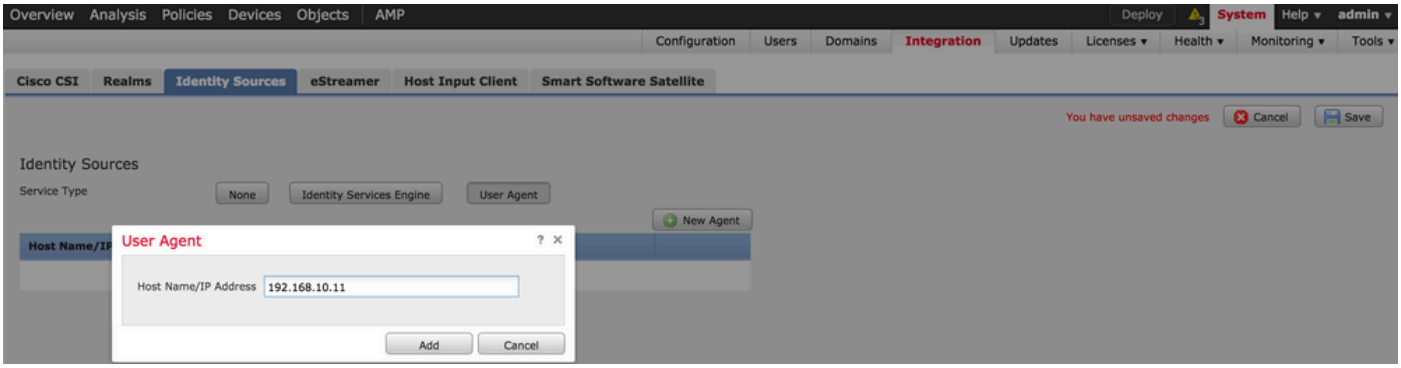
Installazione e disinstallazione di Sourcefire User Agent

Passaggio 2. Integrazione di Firepower Management Center (FMC) con User Agent

Accedere a Firepower Management Center, selezionare Sistema > Integrazione > Origini identità. Fare clic sull'opzione Nuovo agente. Configurare l'indirizzo IP del sistema User Agent e

fare clic sul pulsante Add.

Fare clic sul pulsante Salva per salvare le modifiche.



Passaggio 3. Integrare Firepower con Active Directory

Passaggio 3.1 Creazione del realm

Accedere al CCP, selezionare Sistema > Integrazione > Realm. Fate clic sull'opzione Aggiungi nuovo realm (Add New Realm).

Nome e descrizione: fornire un nome o una descrizione per identificare in modo univoco il realm.

Tipo: AD

Dominio primario AD: nome di dominio di Active Directory

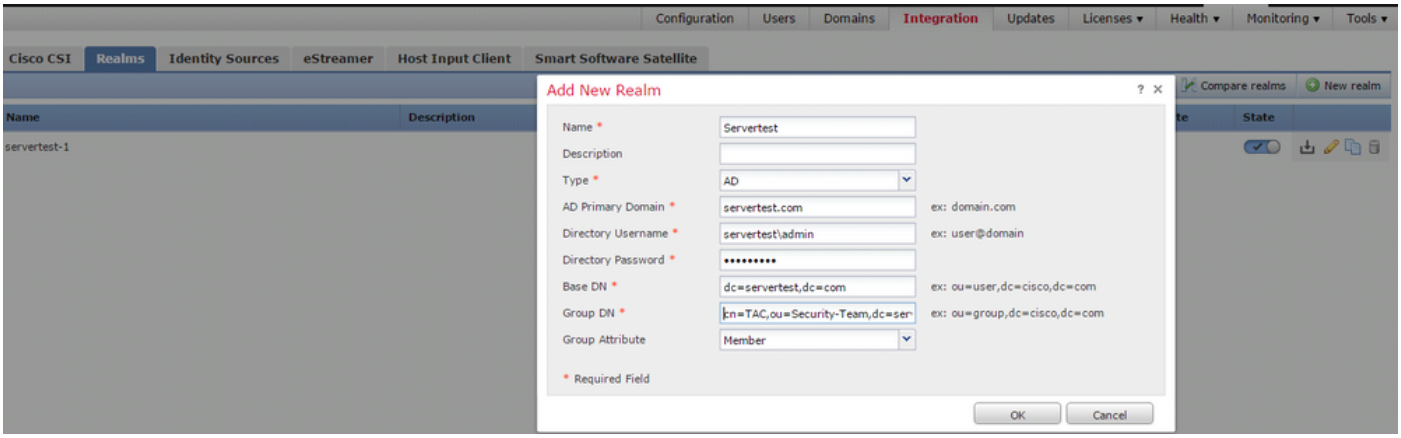
Nome utente directory: <nomeutente>

Password directory: <password>

Nome distinto di base: nome distinto dell'unità organizzativa di dominio o specifica da cui il sistema avvia una ricerca nel database LDAP.

DN gruppo: DN gruppo

Attributo gruppo: Membro



In questo articolo vengono illustrati i valori del DN di base e del DN gruppo.

[Identifica attributi oggetto LDAP di Active Directory]

Passaggio 3.2 Aggiungere il server delle directory

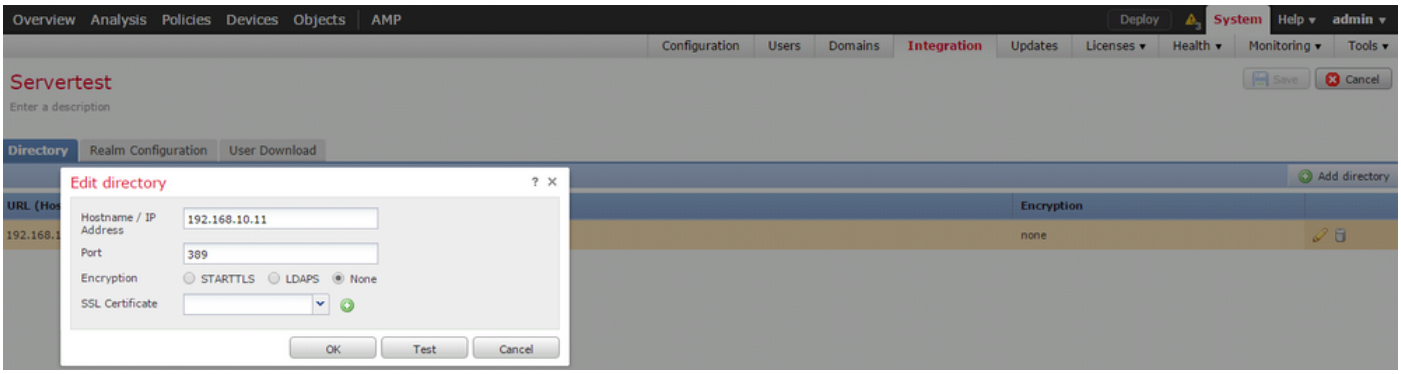
Fare clic sul pulsante Add per passare al passaggio successivo e quindi fare clic sull'opzione Add directory.

Nome host/Indirizzo IP: configurare l'indirizzo IP o il nome host del server AD.

Porta: 389 (numero di porta LDAP di Active Directory)

Crittografia/certificato SSL: (facoltativo) Per crittografare la connessione tra FMC e il server AD, fare riferimento alla

articolo: [Verifica dell'oggetto di autenticazione sul sistema FireSIGHT per l'autenticazione AD Microsoft tramite SSL/TLS]



Fare clic sul pulsante Test per verificare se FMC è in grado di connettersi al server AD.

Passo 3.3 Modifica della configurazione del realm

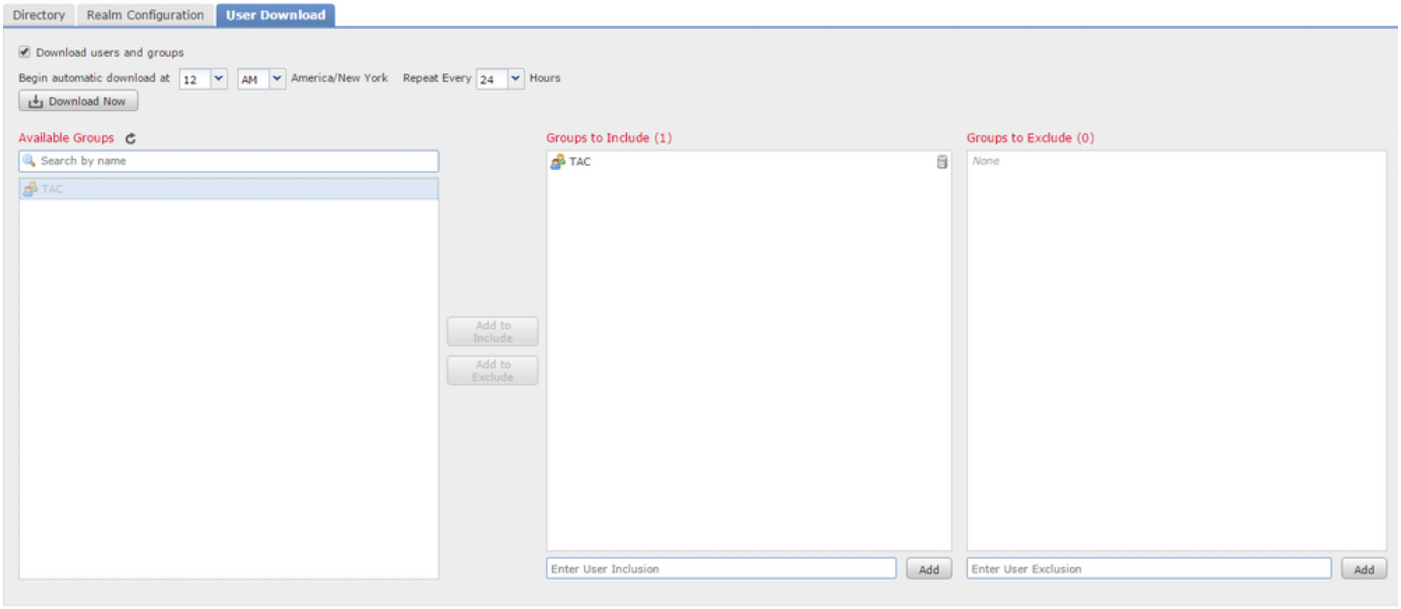
Passare a Configurazione realm per verificare la configurazione di integrazione del server AD ed è possibile modificare la configurazione di AD.

Passaggio 3.4 Download del database degli utenti

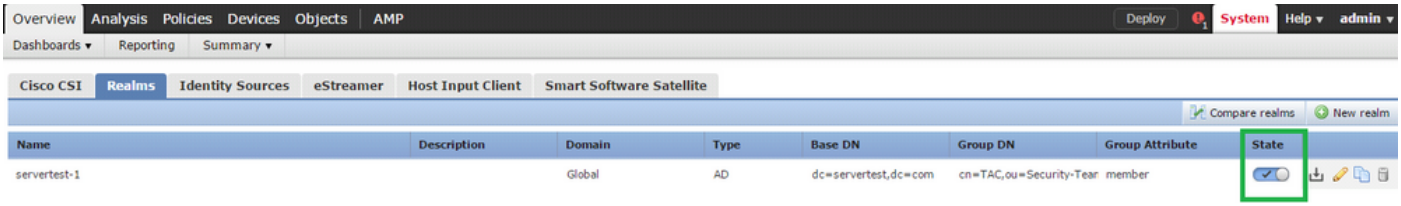
Passare all'opzione Download utente per recuperare il database utenti dal server AD.

Selezionare la casella di controllo per scaricare gli utenti e i gruppi Download e definire l'intervallo di tempo con cui la console Gestione risorse Desktop remoto contatta AD per il download del database utenti.

Selezionare il gruppo e inserirlo nell'opzione Includi per la quale si desidera configurare l'autenticazione.



Come mostrato nell'immagine, abilitare lo stato AD:



Passaggio 4. Configurare il criterio di identità

I criteri di identità eseguono l'autenticazione utente. Se l'utente non esegue l'autenticazione, l'accesso alle risorse di rete viene rifiutato. In questo modo viene applicato il controllo degli accessi basato sui ruoli (RBAC, Role-Based Access Control) alla rete e alle risorse dell'organizzazione.

Passaggio 4.1 Portale vincolato (autenticazione attiva)

Active Authentication richiede nome utente/password nel browser per identificare un'identità utente per consentire qualsiasi connessione. Il browser autentica l'utente con una pagina di autenticazione o esegue l'autenticazione in modo invisibile all'utente con autenticazione NTLM. NTLM utilizza il browser Web per inviare e ricevere informazioni di autenticazione. L'autenticazione attiva utilizza vari tipi per verificare l'identità dell'utente. I diversi tipi di autenticazione sono:

1. HTTP Basic: in questo metodo, il browser richiede le credenziali utente.
2. NTLM: NTLM utilizza le credenziali della workstation di Windows e le negozia con Active Directory tramite un browser Web. È necessario abilitare l'autenticazione NTLM nel browser. L'autenticazione dell'utente avviene in modo trasparente senza la richiesta di credenziali. Offre agli utenti un'esperienza di accesso singolo.
3. Negoziazione HTTP: in questo tipo, il sistema tenta di eseguire l'autenticazione con NTLM. In caso di errore, il sensore utilizza il tipo di autenticazione di base HTTP come metodo di

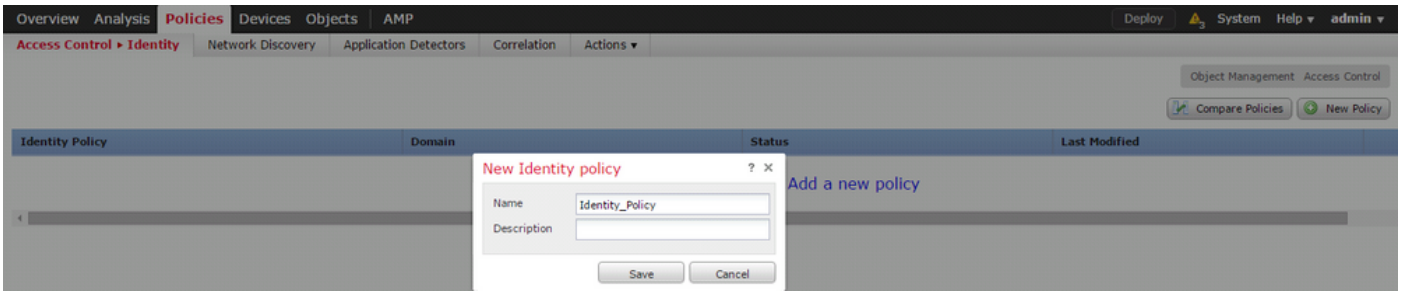
fallback e richiede le credenziali dell'utente in una finestra di dialogo.
4. Pagina Risposta HTTP: simile al tipo di base HTTP, tuttavia, in questa pagina viene richiesto all'utente di compilare l'autenticazione in un modulo HTML personalizzabile.

Ogni browser dispone di un modo specifico per abilitare l'autenticazione NTLM e pertanto rispetta le linee guida del browser per abilitare l'autenticazione NTLM.

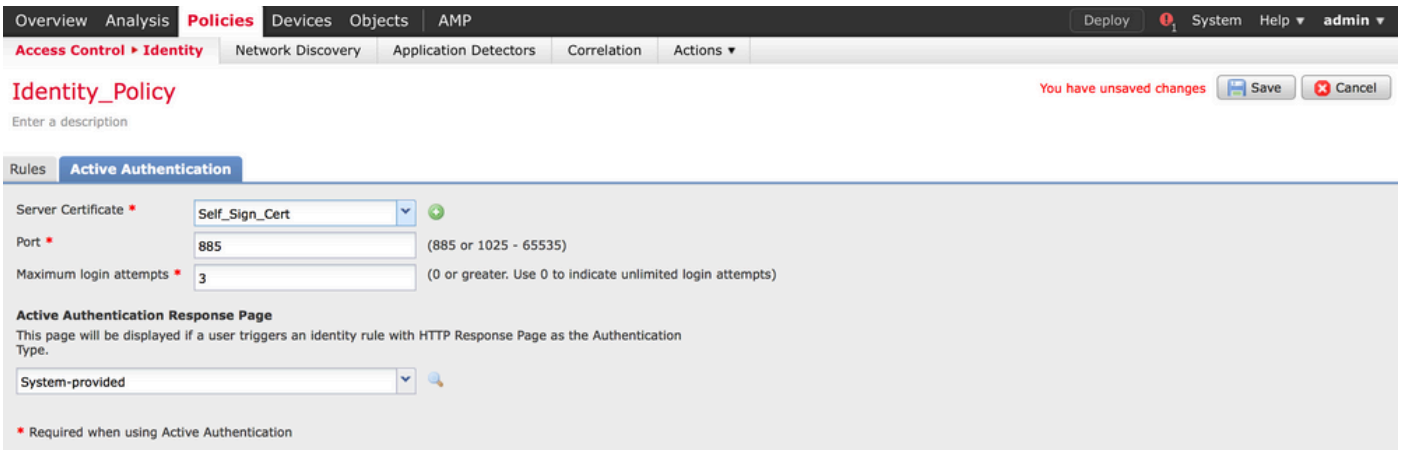
Per condividere in modo sicuro le credenziali con il sensore instradato, è necessario installare un certificato server autofirmato o un certificato server firmato pubblicamente nei criteri di identità.

```
Generate a simple self-signed certificate using openSSL -

Step 1.   Generate the Private key
          openssl genrsa -des3 -out server.key 2048

Step 2.   Generate Certificate Signing Request (CSR)
          openssl req -new -key server.key -out server.csr

Step 3.   Generate the self-signed Certificate.
          openssl x509 -req -days 3650 -sha256 -in server.csr -signkey server.key -out server.crt
```

Passare a Criteri > Controllo d'accesso > Identità. Fare clic su Aggiungi criterio & assegnare un nome al criterio e salvarlo.

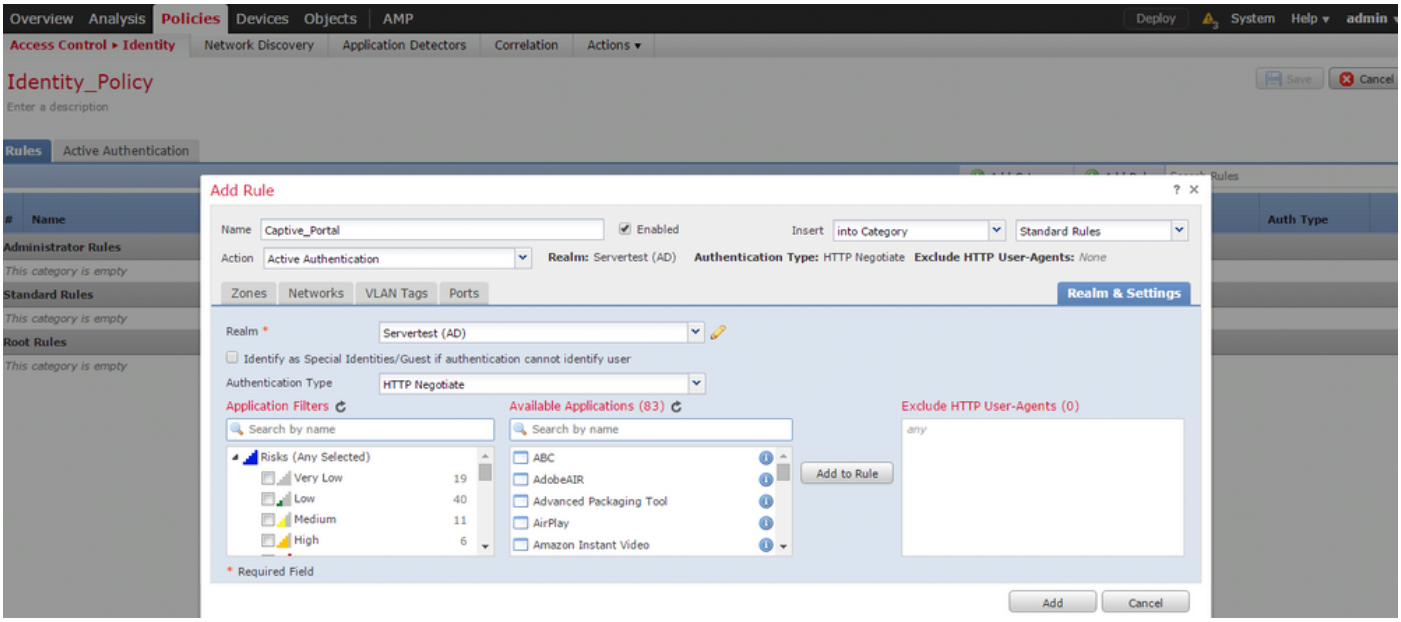


Passare alla scheda Active Authentication e nell'opzione Server Certificate fare clic sull'icona (+) e caricare il certificato e la chiave privata generati nel passaggio precedente con openSSL.



Fare clic sul pulsante Add rule e assegnare un nome alla regola e scegliere l'azione come Active Authentication. Definire la zona di origine/destinazione, la rete di origine/destinazione per la quale si desidera abilitare l'autenticazione utente.

Selezionare il realm configurato nel passaggio precedente e il tipo di autenticazione più adatto al proprio ambiente.



Configurazione ASA per Captive Portal

Per il modulo ASA Firepower, configurare questi comandi sull'appliance ASA per configurare il portale captive.

```
ASA(config)# captive-portal global port 1055
```

Verificare che la porta del server TCP 1055 sia configurata nell'opzione porta della scheda Autenticazione attiva criteri di identità.

Per verificare le regole attive e il relativo numero di passaggi, eseguire il comando:

```
ASA# show asp table classify domain captive-portal
```

Nota: il comando Captive Portal è disponibile a partire da ASA versione 9.5(2).

Passaggio 4.2 Single Sign-On (Autenticazione passiva)

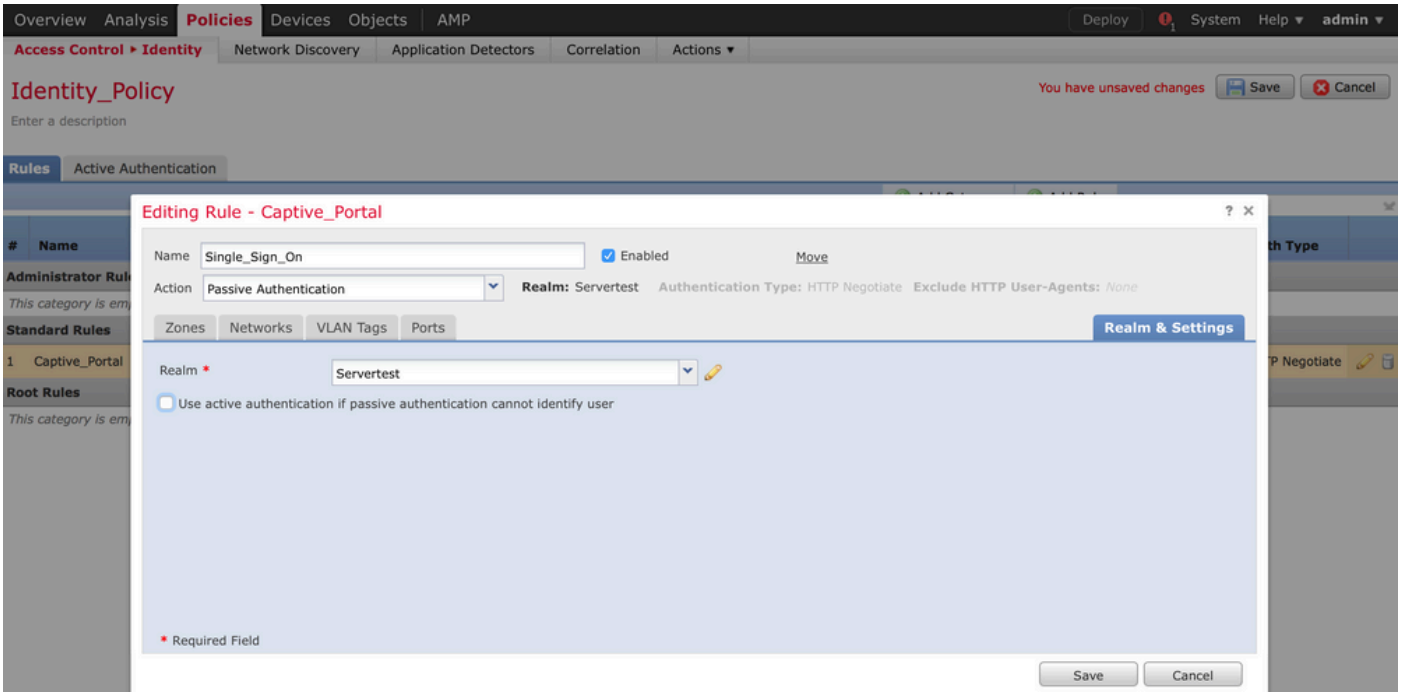
Nell'autenticazione passiva, quando un utente di dominio accede ad Active Directory e può autenticarlo, l'agente utente Firepower esegue il polling dei dettagli di mapping User-IP dai log di

sicurezza di Active Directory e condivide queste informazioni con Firepower Management Center (FMC). FMC invia questi dettagli al sensore per applicare il controllo degli accessi.

Fare clic sul pulsante Aggiungi regola e assegnare un nome alla regola e scegliere Azione come Autenticazione passiva. Definire la zona di origine/destinazione, la rete di origine/destinazione per la quale si desidera abilitare l'autenticazione utente.

Selezionare il realm configurato nel passaggio precedente e il tipo di autenticazione più adatto all'ambiente, come illustrato in questa immagine.

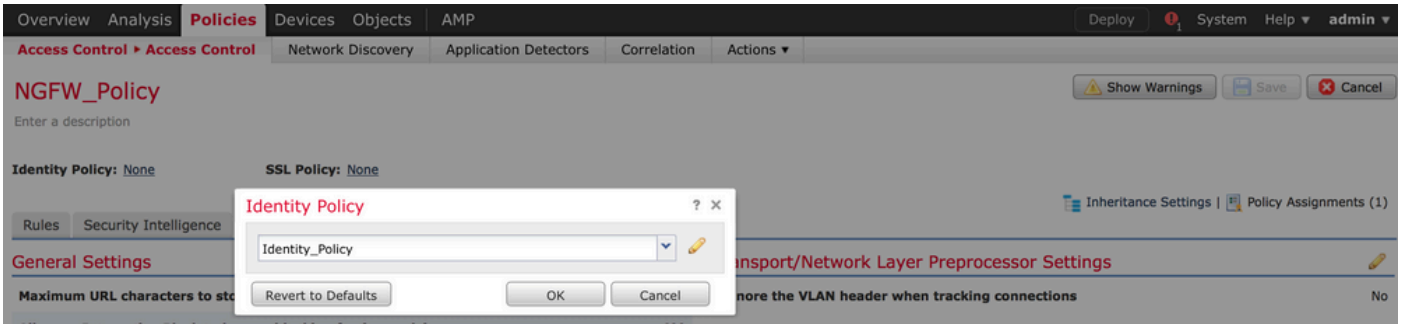
È possibile scegliere il metodo di fallback come autenticazione attiva se l'autenticazione passiva non è in grado di identificare l'identità dell'utente.



Passaggio 5. Configurare i criteri di controllo di accesso

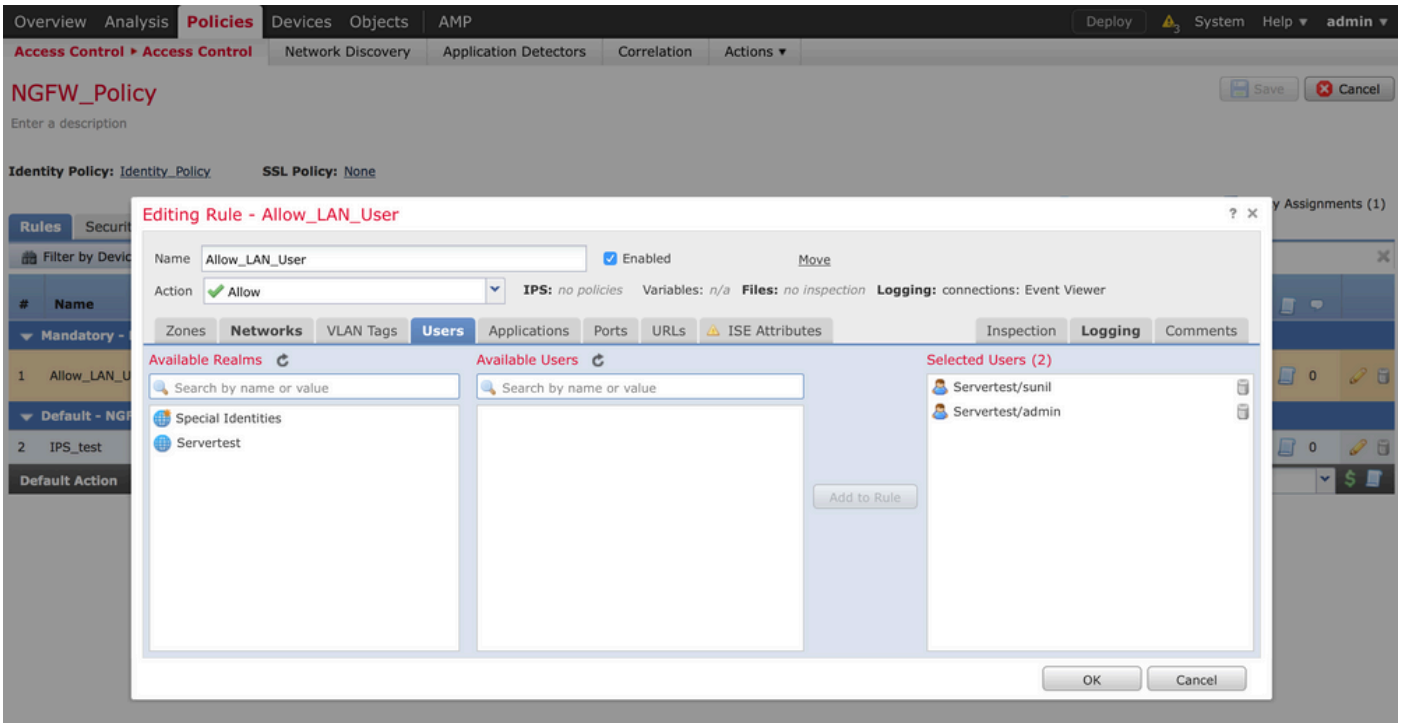
Passare a Criteri > Controllo d'accesso > Crea/Modifica un criterio.

Fare clic sul criterio di identità (parte superiore sinistra), scegliere il criterio di identità configurato nel passaggio precedente e fare clic sul pulsante OK, come mostrato nell'immagine.



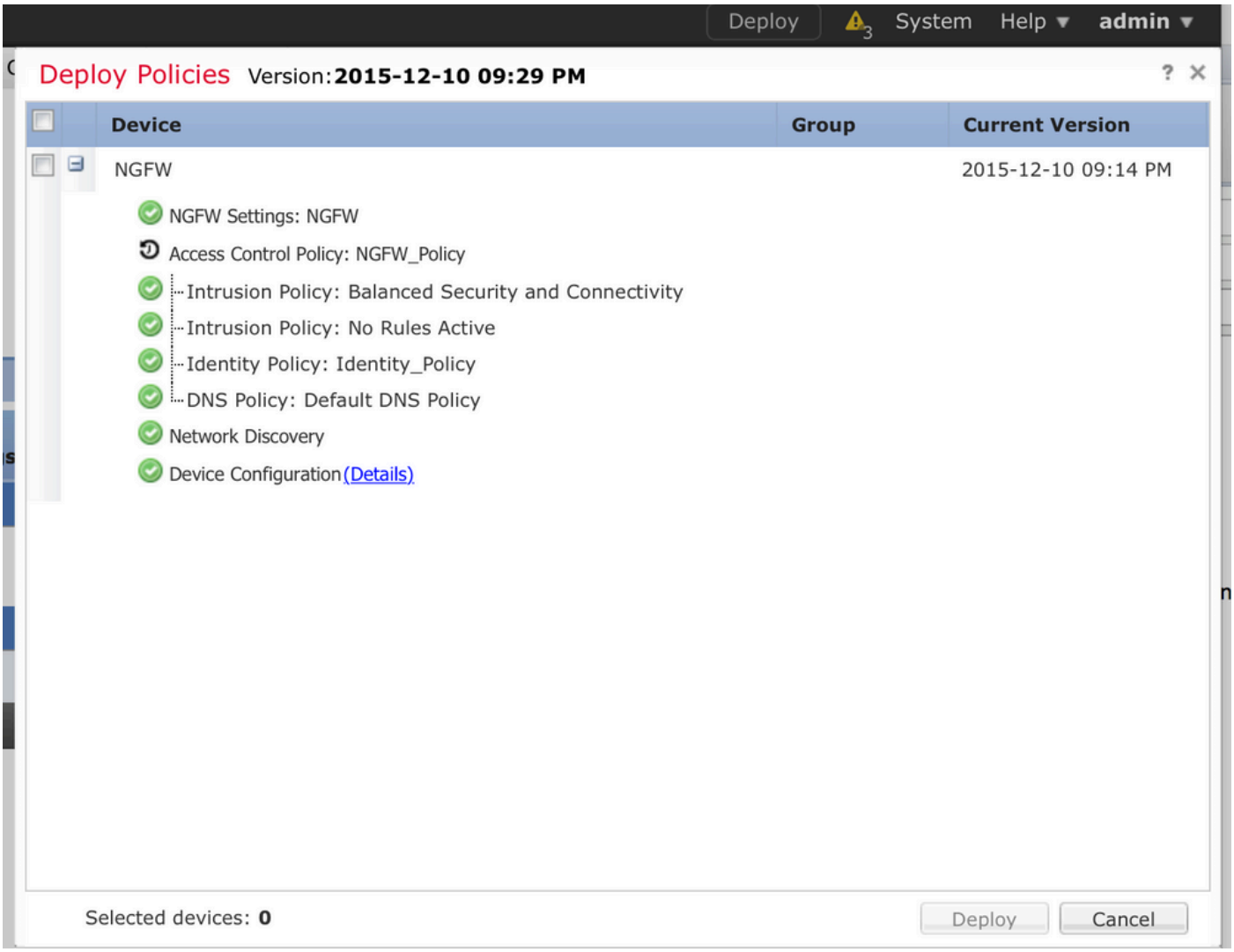
Fare clic sul pulsante Aggiungi regola per aggiungere una nuova regola. Passare a Utenti e selezionare gli utenti per i quali viene applicata la regola di controllo di accesso, come mostrato

nell'immagine. Per salvare le modifiche, fare clic su OK e su Salva.



Passaggio 6. Distribuire i criteri di controllo di accesso

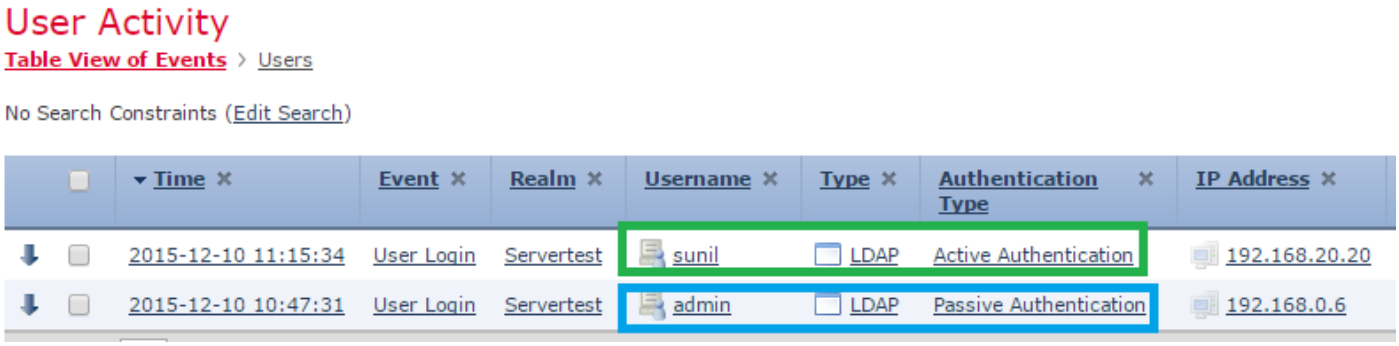
Passare all'opzione Deploy, scegliere il dispositivo e fare clic sull'opzione Deploy per inviare la modifica della configurazione al sensore. Monitorare la distribuzione dei criteri dall'opzione Icona centro messaggi (icona tra l'opzione Distribuisci e l'opzione Sistema) e verificare che i criteri vengano applicati correttamente, come mostrato nell'immagine.



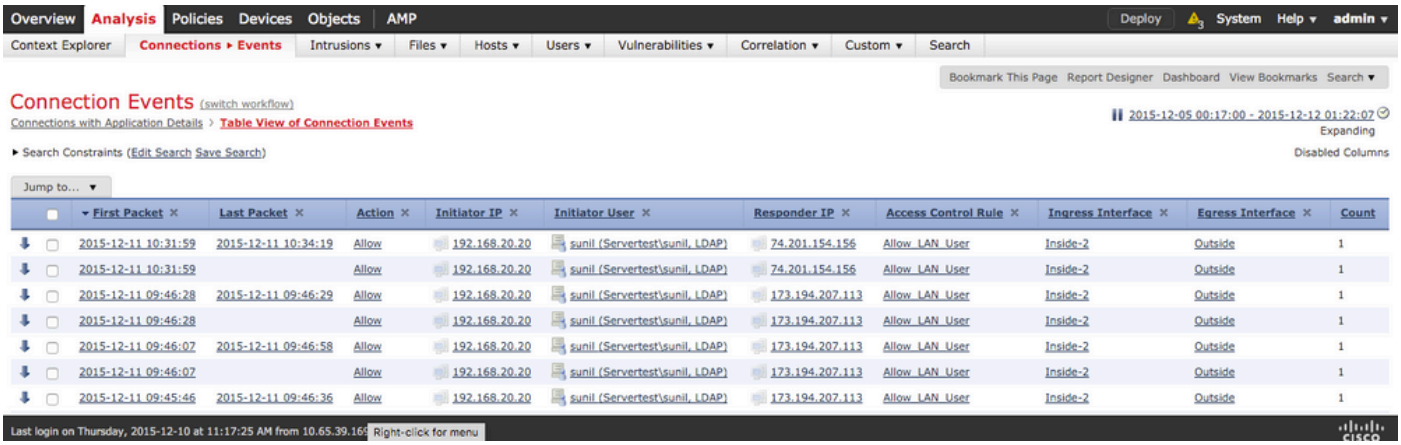
Passaggio 7. Monitorare gli eventi utente e gli eventi di connessione

Le sessioni utente attualmente attive sono disponibili nella sezione Analisi > Utenti > Utenti.

Il monitoraggio dell'attività dell'utente consente di individuare l'utente associato all'indirizzo IP e il modo in cui l'utente viene rilevato dal sistema mediante l'autenticazione attiva o passiva. Analisi > Utenti > Attività utente



Selezionare Analisi > Connessioni > Eventi per controllare il tipo di traffico utilizzato dall'utente.



Verifica e risoluzione dei problemi

Passare a **Analisi > Utenti** per verificare l'autenticazione utente/il tipo di autenticazione/il mapping IP utente/la regola di accesso associata al flusso di traffico.

Verifica della connettività tra FMC e agente utente (autenticazione passiva)

Firepower Management Center (FMC) utilizza la porta TCP 3306 per ricevere i dati del registro attività utente dall'agente utente.

Per verificare lo stato del servizio del CCP, utilizzare questo comando nel CCP.

```
admin@firepower:~$ netstat -tan | grep 3306
```

Eseguire l'acquisizione dei pacchetti nel FMC per verificare la connettività con l'agente utente.

```
admin@firepower:~$ sudo tcpdump -i eth0 -n port 3306
```

Passare ad Analisi > Utenti > Attività utente per verificare se FMC riceve i dettagli di accesso dell'utente dall'agente utente.

Verifica della connettività tra FMC e Active Directory

Per recuperare il database utenti da Active Directory, FMC utilizza la porta TCP 389.

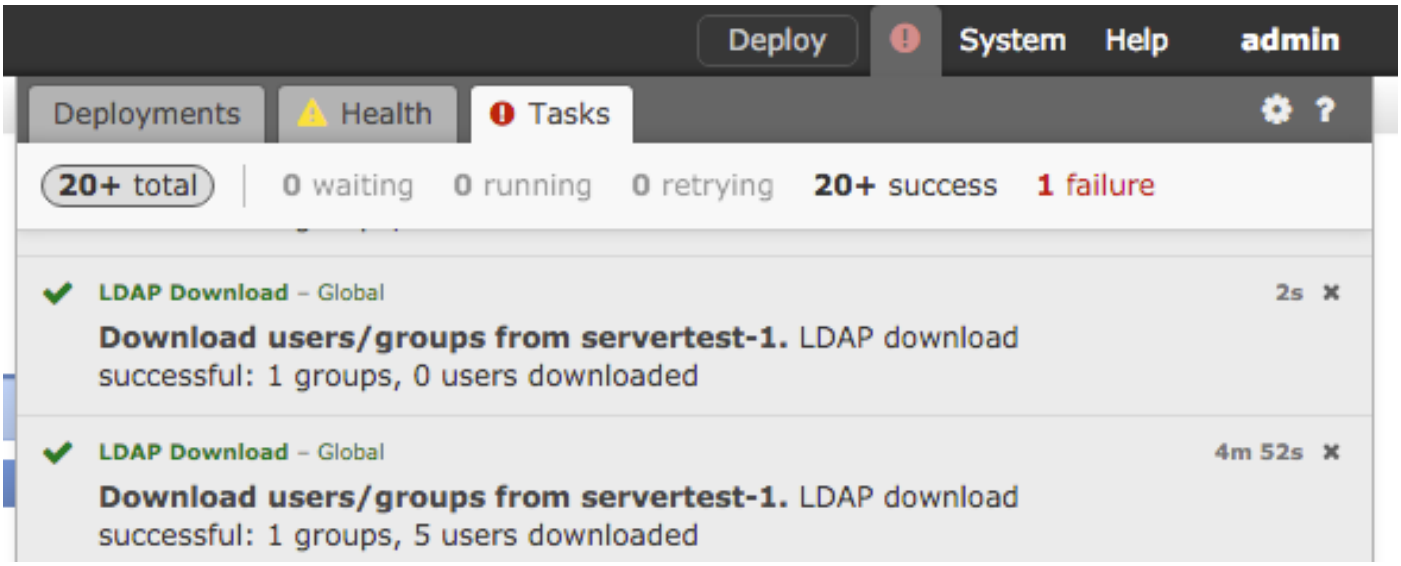
Eseguire l'acquisizione dei pacchetti nel FMC per verificare la connettività con Active Directory.

```
admin@firepower:~$ sudo tcpdump -i eth0 -n port 389
```

Verificare che le credenziali utente utilizzate nella configurazione del realm FMC dispongano di privilegi sufficienti per recuperare il database utenti di Active Directory.

Verificare la configurazione dell'area di autenticazione FMC e assicurarsi che gli utenti/gruppi vengano scaricati e che il timeout della sessione utente sia configurato correttamente.

Passare a Centro messaggi > Attività e verificare che il download dell'attività utenti/gruppi venga completato correttamente, come mostrato nell'immagine.



Verifica della connettività tra il sensore Firepower e il sistema terminale (autenticazione attiva)

Per l'autenticazione attiva, verificare che il certificato e la porta siano configurati correttamente nei criteri di identità FMC. Per impostazione predefinita, il sensore Firepower resta in ascolto sulla porta TCP 885 per l'autenticazione attiva.

Verifica della configurazione dei criteri e della distribuzione dei criteri

Verificare che i campi Realm, Tipo di autenticazione, Agente utente e Azione siano configurati correttamente in Criteri di identità.

Verificare che i criteri di identità siano associati correttamente ai criteri di controllo di accesso.

Passare a Centro messaggi > Attività e verificare che la distribuzione dei criteri sia stata completata correttamente.

Analizzare i registri eventi

È possibile utilizzare gli eventi Connection (Connessione) e User Activity (Attività utente) per diagnosticare se l'accesso dell'utente ha esito positivo o meno.Questi eventi

è inoltre in grado di verificare quale regola di controllo di accesso viene applicata al flusso.

Passare ad Analisi > Utente per controllare i registri degli eventi utente.

Passare ad Analisi > Eventi connessione per controllare gli eventi di connessione.

Informazioni correlate

- **Documentazione e supporto tecnico – Cisco Systems**

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).