Configurazione dell'integrazione di Active Directory con ASDM per l'autenticazione Single Sign-On e Captive Portal (gestione integrata)

Sommario

Introduzione

Questo documento descrive la configurazione dell'autenticazione Captive Portal (Active Authentication) e Single Sign-On (Passive Authentication) sul modulo Firepower con ASDM (Adaptive Security Device Manager).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza del firewall ASA (Adaptive Security Appliance) e di ASDM
- Knowledge Base del modulo FirePOWER
- LDAP (Light Weight Directory Service)
- Firepower UserAgent

Componenti usati

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

- Moduli ASA FirePOWER (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) con software versione 5.4.1 e successive.
- Modulo ASA FirePOWER (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X) con software 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 immettere più volte le credenziali utente. L'autenticazione Single Sign-On può essere eseguita tramite l'agente utente Firepower o l'autenticazione del browser NTLM.

> **Nota**:autenticazione Captive Portal, l'appliance ASA deve essere in modalità di routing.

> **Nota:** Il comando Captive Portal è disponibile in ASA versione 9.5(2) e successive.

Configurazione

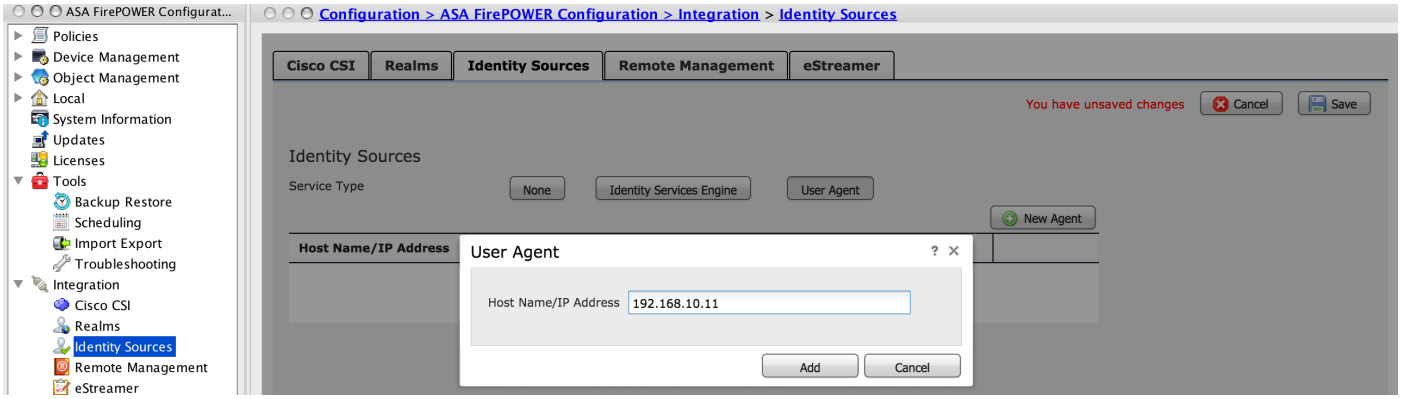
Passaggio 1. Configurare l'agente utente Firepower per Single Sign-On.

Questo articolo spiega come configurare Firepower User Agent nel computer Windows:

Installazione e disinstallazione di Sourcefire User Agent

Passaggio 2. Integrare Firepower Module (ASDM) con User Agent.

Accedere ad ASDM, selezionare **Configuration > ASA FirePOWER Configuration > Integration > Identity Sources** (Configurazione ASA FirePOWER > Integrazione > Origini identità), quindi fare clic sull'opzione **User Agent**. Dopo aver fatto clic sull'opzione **Agente utente** e aver configurato l'indirizzo IP del sistema Agente utente. fare clic su **Add** (Aggiungi), come mostrato nell'immagine:



Fare clic sul pulsante **Salva** per salvare le modifiche.

Passaggio 3. Integrare Firepower con Active Directory.

Passaggio 3.1 Creazione del realm.

Accedere ad ASDM, selezionare **Configuration > ASA FirePOWER Configuration > Integration > Realms** (Configurazione ASA FirePOWER > Integrazione > Realm). Fare clic su **Aggiungi nuovo 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 NETBIOS).

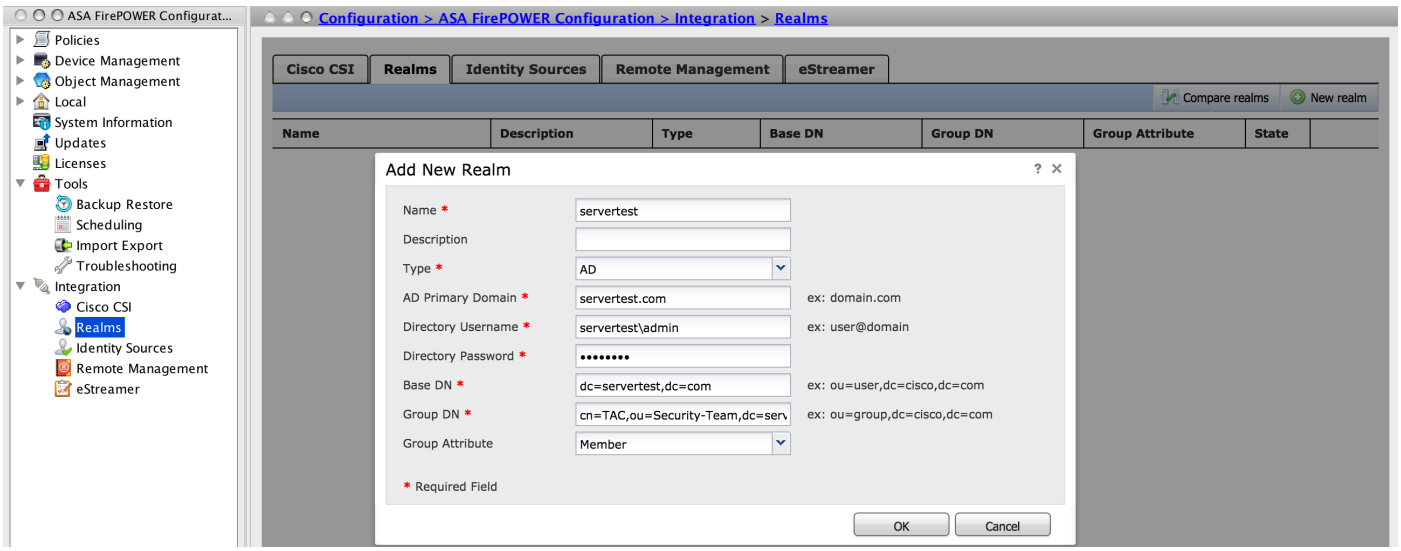
Nome utente directory: specificare <*nomeutente*>.

Password directory: Specificare la <*password*>.

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

DN gruppo: Specificare il DN del gruppo.

Attributo gruppo: Specificare l'opzione Member dall'elenco a discesa.



Fare clic su **OK** per salvare la configurazione.

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 l'indirizzo IP/il nome host del server delle directory.

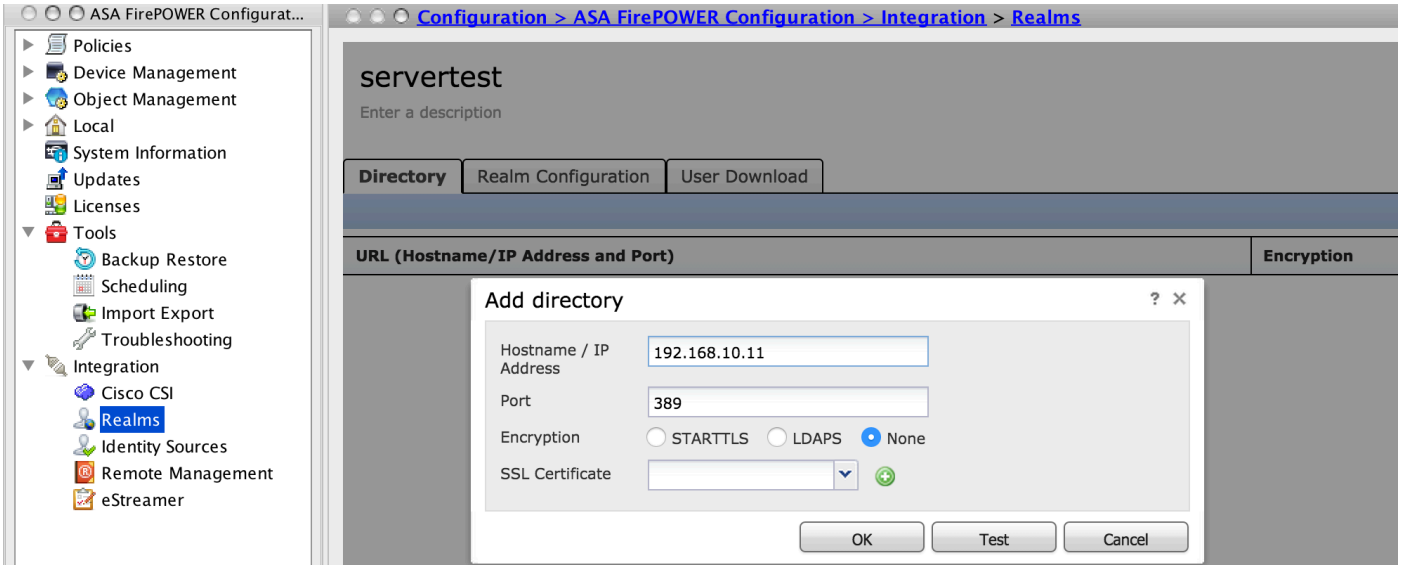
Per specificare l'indirizzo IP/nome host del server AD, fare clic su **Aggiungi directory**.

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

Port: Specificare il numero di porta LDAP di Active Directory (Predefinito 389).

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

[Verifica dell'oggetto di autenticazione sul sistema FireSIGHT per l'autenticazione di Microsoft AD su SSL/T...]



Clic **Test** per verificare la connessione del CCP al server AD. Fare clic su **OK** per salvare la configurazione.

Passo 3.3 Modifica della configurazione del realm.

Per modificare e verificare la configurazione dell'integrazione del server AD, passare a **Configurazione realm**.

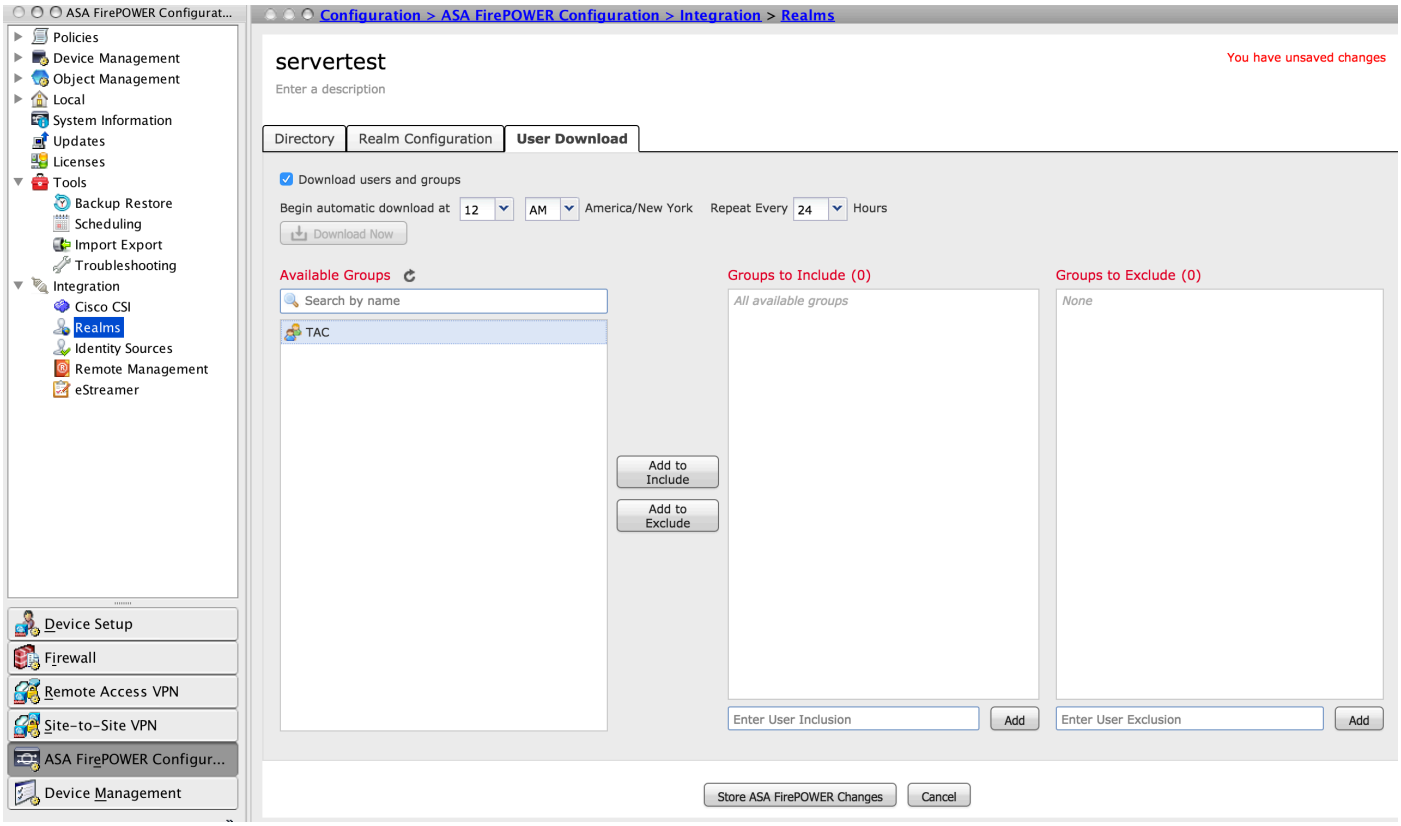
Passaggio 3.4 Scaricare il database degli utenti.

Passare a **Download utente** per recuperare il database utenti dal server AD.

Selezionare la casella di controllo per scaricare **utenti e gruppi** e definire l'intervallo di tempo con cui il modulo Firepower contatta il server AD per scaricare il database utenti.

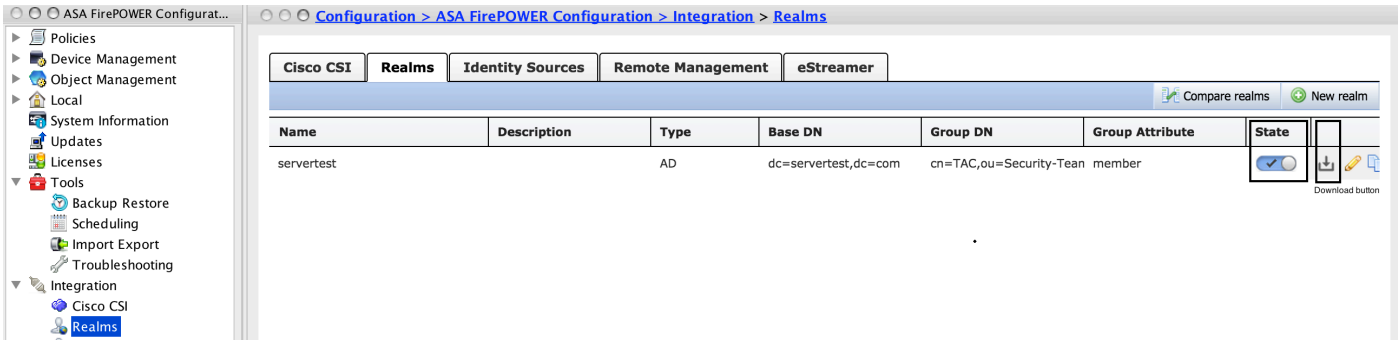
Selezionare il gruppo e aggiungerlo all'opzione **Includi** per cui si desidera configurare

l'autenticazione. Se non si sceglie di includere i gruppi, per impostazione predefinita vengono selezionati tutti i gruppi.



Fare clic su **Store ASA Firepower Changes** per salvare la configurazione dell'area di autenticazione.

Abilitare lo stato del realm e fare clic sul pulsante di download per scaricare gli utenti e i gruppi, come mostrato nell'immagine.



Passaggio 4. Configurare il criterio di identità.

I criteri di identità eseguono l'autenticazione dell'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) alla rete e alle risorse dell'organizzazione.

Passaggio 4.1 Portale vincolato (autenticazione attiva).

Active Authentication richiede nome utente e password nel browser per identificare un'identità utente per consentire qualsiasi connessione. Il browser autentica l'utente presentando la pagina di autenticazione o esegue l'autenticazione in modo invisibile all'utente con l'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:

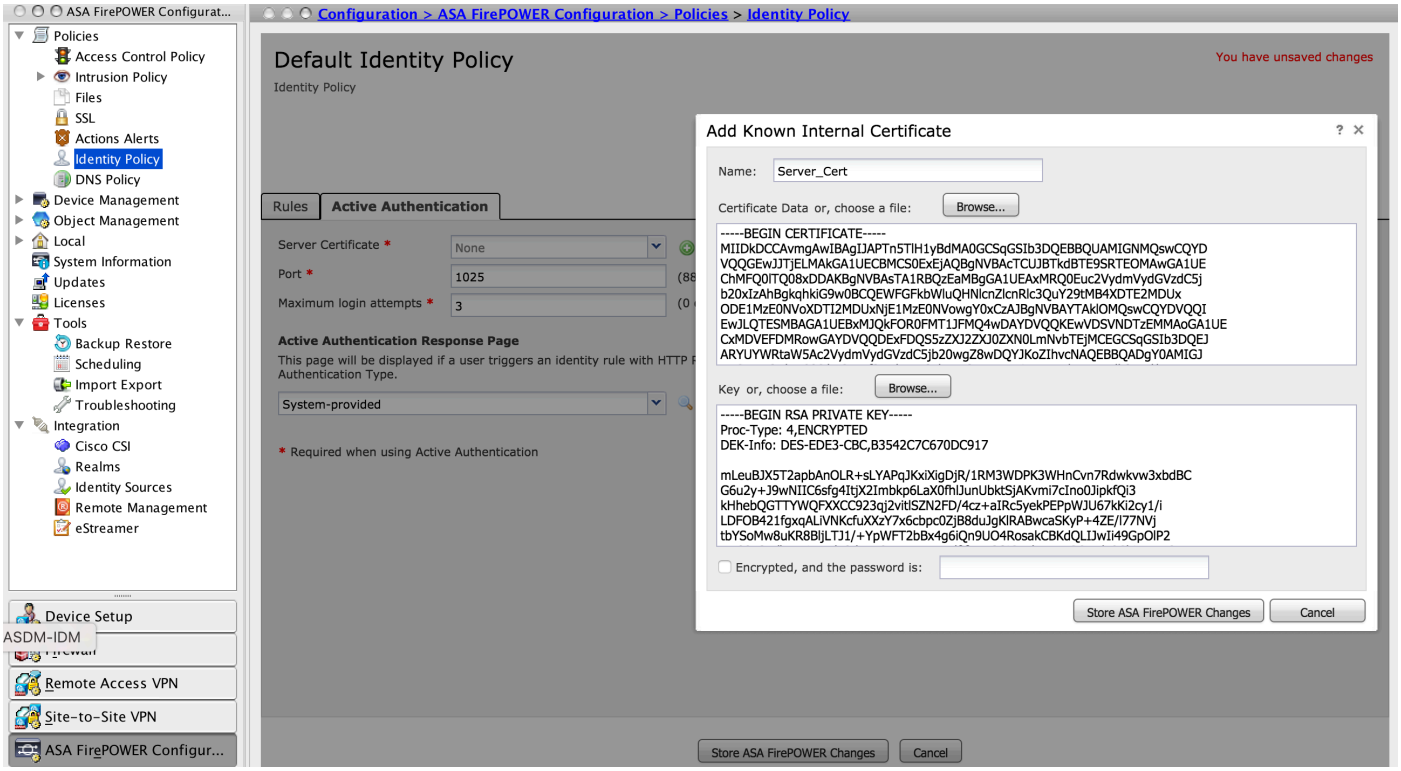
1. **HTTP Basic: in questo metodo, il browser richiede le credenziali dell'utente.**
2. **NTLM: NTLM utilizza le credenziali della workstation Windows e le negozia con Active Directory utilizzando un browser Web. È necessario abilitare l'autenticazione NTLM nel browser. L'autenticazione dell'utente avviene in modo trasparente senza richiedere credenziali. Offre agli utenti un'esperienza di accesso singolo.**
3. **Negoziazione HTTP:** in questo tipo, il sistema tenta di eseguire l'autenticazione utilizzando NTLM. Se l'operazione non riesce, 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 di compilare l'autenticazione in un modulo HTML personalizzabile.**

Ogni browser dispone di un modo specifico per abilitare l'autenticazione NTLM e pertanto è possibile seguire 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.

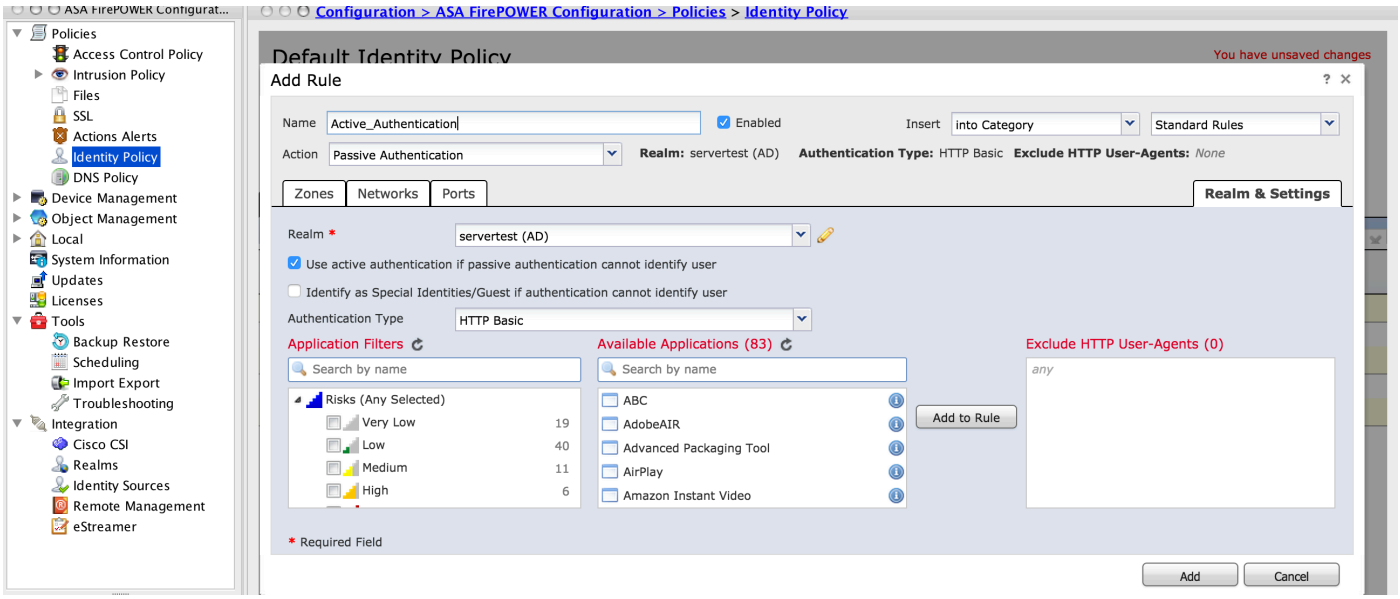
```
Generate a simple self-signed certificate using openSSL -

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
```

Selezionare **Configurazione > Configurazione ASA FirePOWER > Criteri > Criteri di identità**. Passare alla scheda **Autenticazione attiva** e nell'opzione **Certificato server** fare clic sull'**icona (+)** e caricare il certificato e la chiave privata generati nel passaggio precedente utilizzando openSSL, come mostrato nell'immagine:



Fare clic su **Add rule** (Aggiungi regola) per assegnare un nome alla regola e scegliere l'azione come **Active Authentication** (Autenticazione attiva). Definire la zona di origine/destinazione, la rete di origine/destinazione per la quale si desidera abilitare l'autenticazione utente.

Passare alla scheda **Realm & Settings**. Selezionare il **Realm** dall'elenco a discesa configurato nel passaggio precedente e selezionare il **Tipo di autenticazione** dall'elenco a discesa che meglio si adatta al proprio ambiente di rete.



Passaggio 4.2 Configurazione ASA per Captive Portal.

Passaggio 1. Definire il traffico interessante che verrà reindirizzato a Sourcefire per l'ispezione.

```
ASA(config)# access-list SFR_ACL extended permit ip 192.168.10.0 255.255.255.0 any
ASA(config)#
ASA(config)# class-map SFR_CMAP
```

```
ASA(config-cmap)# match access-list SFR_ACL


ASA(config)# policy-map global_policy
ASA(config-pmap)# class SFR_CMAP
ASA(config-pmap-c)# sfr fail-open
ASA(config)#service-policy global_policy global
```

Passaggio 2. Configurare questo comando sull'appliance ASA per abilitare il portale captive.

```
ASA(config)# captive-portal interface inside port 1025
```

> **Suggerimento**: captive-portal può essere abilitato a livello globale o per singola interfaccia.

> **Suggerimento**: Verificare che la porta del server TCP 1025 sia configurata nell'opzione relativa alla porta della scheda Autenticazione attiva dei criteri di identità.

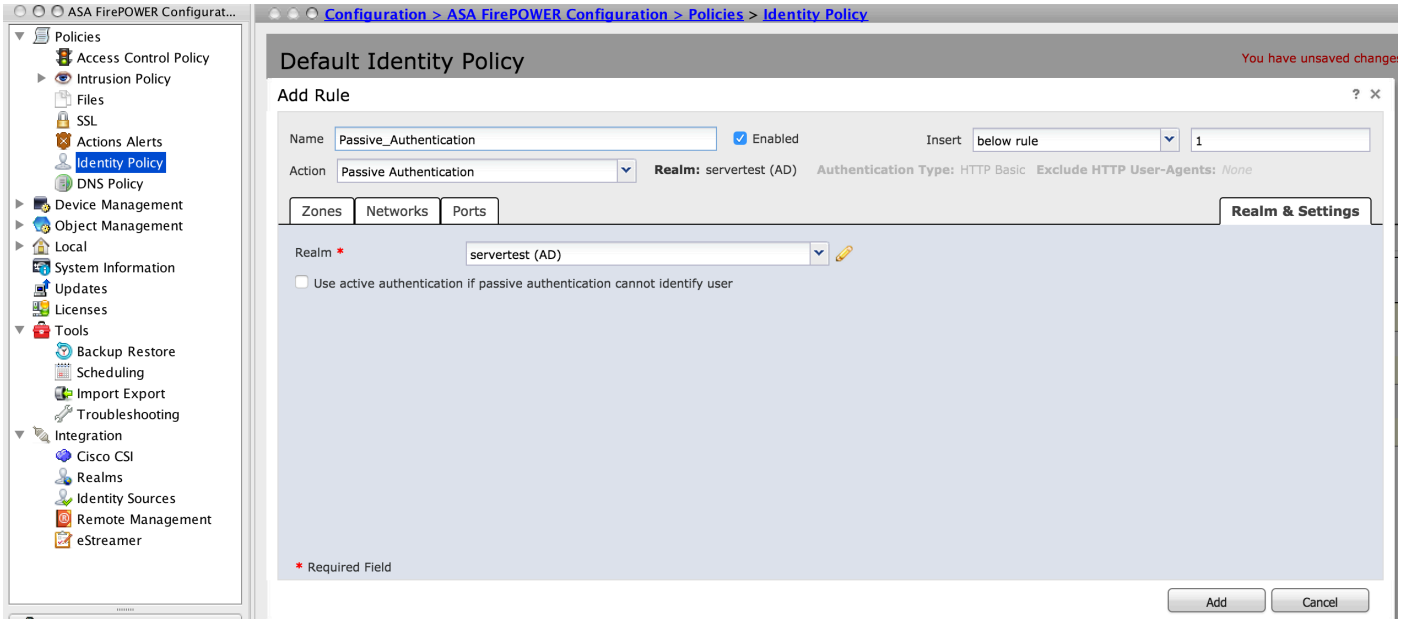
Passaggio 4.3 Single Sign-On (Autenticazione Passiva).

Nell'autenticazione passiva, quando un utente di dominio accede ad Active Directory e può autenticarlo, l'agente utente Firepower esegue il polling dei dettagli del mapping User-IP dai log di sicurezza di Active Directory e condivide queste informazioni con Firepower Module. Il modulo Firepower utilizza questi dettagli per applicare il controllo degli accessi.

Per configurare la regola di autenticazione passiva, fare clic su **Aggiungi regola** per assegnare un nome alla regola, quindi 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.

Passare alla **Realm e impostazioni** . Selezionare il **Area autenticazione** dall'elenco a discesa configurato nel passaggio precedente.

Qui è possibile scegliere il metodo di fallback come **autenticazione attiva se l'autenticazione passiva non riesce a identificare l'identità dell'utente**, come mostrato nell'immagine:

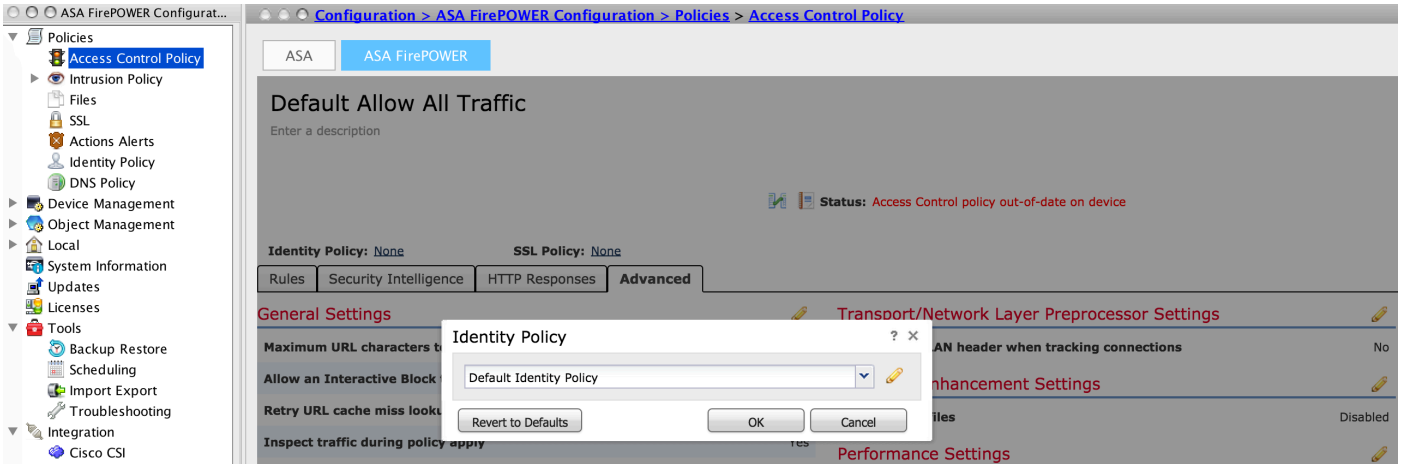


Fare clic su **Store ASA Firepower Changes** per salvare la configurazione del criterio di identità.

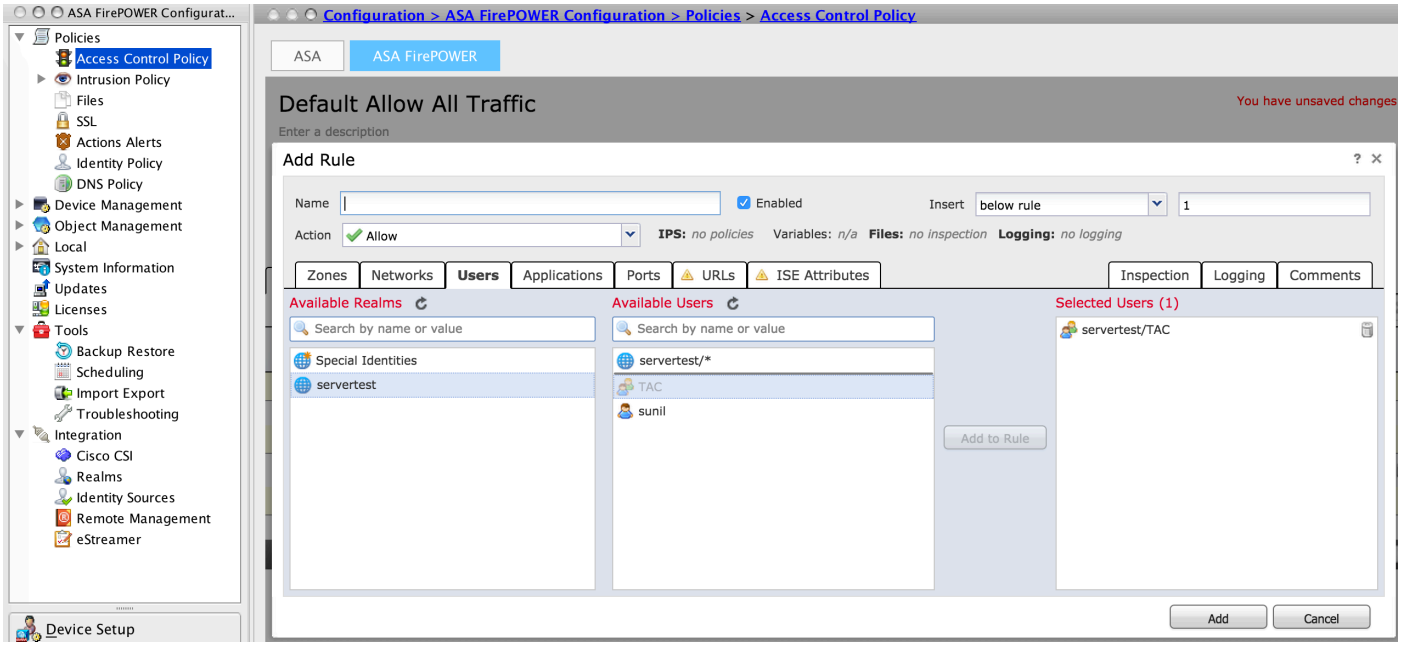
Passaggio 5. Configurare i criteri di controllo di accesso.

Selezionare **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy (Configurazione ASA FirePOWER > Criteri > Policy di controllo dell'accesso).**

Fare clic sul **criterio di identità** (angolo superiore sinistro), selezionare il criterio di identità configurato nel passaggio precedente dall'elenco a discesa e fare clic su **OK**, come mostrato nell'immagine.



Fare clic su **Aggiungi regola** per aggiungere una nuova regola, passare a **Utenti** e selezionare gli utenti per i quali verrà applicata la regola di controllo di accesso, come mostrato in questa immagine e fare clic su **Aggiungi**.



Fare clic su **Archivia modifiche ASA Firepower** per salvare la configurazione dei criteri di controllo di accesso.

Passaggio 6. Distribuire i criteri di controllo di accesso.

Ènecessario distribuire i criteri di controllo di accesso. Prima di applicare il criterio, nel modulo verrà visualizzata un'indicazione di criteri di controllo dell'accesso non aggiornata. Per distribuire

le modifiche al sensore, fare clic su **Distribuisci** e scegliere l'**opzione Distribuisci modifiche FirePOWER** quindi fare clic su **Distribuisci** nella finestra popup.

> **Nota:** Nella versione 5.4.x, per applicare la policy di accesso al sensore, è necessario fare clic su Apply ASA FirePOWER Changes (Applica modifiche FirePOWER ASA)

> **Nota:** Selezionare Monitoraggio > Monitoraggio di ASA Firepower > Stato task. Verificare che l'attività debba completare l'applicazione della modifica alla configurazione.

Passaggio 7. Monitorare gli eventi utente.

Selezionare **Monitoraggio > ASA FirePOWER Monitoring > Eventi in tempo reale** per monitorare il tipo di traffico utilizzato dall'utente.

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

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.

Connettività tra Firepower Module e User Agent (autenticazione passiva)

Firepower Module utilizza la porta TCP 3306 per ricevere i dati del log delle attività dell'utente dall'agente utente.

Per verificare lo stato del servizio del modulo Firepower, usare questo comando nel FMC.

```
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
```

Connettività tra FMC e Active Directory

Il modulo Firepower utilizza la porta TCP 389 per recuperare il database utente da Active Directory.

Eseguire l'acquisizione dei pacchetti sul modulo Firepower 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 dispongano di privilegi sufficienti per recuperare il database utenti di Active Directory.

Verificare la configurazione del realm e assicurarsi che gli utenti/gruppi vengano scaricati e che il timeout della sessione utente sia configurato correttamente.

Passare a Monitoraggio dello stato delle attività di monitoraggio di ASA Firepower e verificare che il download dell'attività da parte di utenti/gruppi venga completato correttamente, come mostrato nell'immagine.

Connettività tra l'appliance ASA e il sistema terminale (autenticazione attiva)

autenticazione attiva, verificare che il certificato e la porta siano configurati correttamente in Firepower module Identity policy e ASA (comando captive-portal). Per impostazione predefinita, ASA e il modulo Firepower sono in ascolto sulla porta TCP 885 per l'autenticazione attiva.

Per verificare le regole attive e il numero di accessi, eseguire questo comando sull'appliance ASA.

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

Input Table
in  id=0x2aaadf516030, priority=121, domain=captive-portal, deny=false
   hits=10, user_data=0x0, cs_id=0x0, flags=0x0, protocol=6
   src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
   dst ip/id=19.19.19.130, mask=255.255.255.255, port=1025, tag=any, dscp=0x0
   input_ifc=inside, output_ifc=identity

Output Table:

L2 - Output Table:

L2 - Input Table:

Last clearing of hits counters: Never
```

Configurazione delle policy e distribuzione delle policy

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 Monitoraggio > Monitoraggio di ASA Firepower > Stato attività e verificare che la distribuzione delle policy venga completata correttamente.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems
- Configurazione dell'integrazione di Active Directory con Firepower Appliance per l'autenticazione Single Sign-On e Captive Portal