Esempio di configurazione di TrustSec Cloud con 802.1x MACsec sugli switch Catalyst serie 3750X

Sommario

Introduzione

In questo documento viene descritto come configurare un cloud Cisco TrustSec (CTS) con crittografia dei collegamenti tra due switch Catalyst serie 3750X (3750X).

In questo articolo viene illustrato il processo di crittografia MACsec (Media Access Control Security) da switch a switch che utilizza il protocollo SAP (Security Association Protocol). Questo processo utilizza la modalità IEEE 802.1x invece della modalità manuale.

Di seguito è riportato un elenco delle operazioni da effettuare:

- Provisioning delle credenziali di accesso protetto (PAC) per dispositivi di origine e non di origine
- Autenticazione NDAC (Network Device Admission Control) e negoziazione MACsec con SAP per la gestione delle chiavi
- Aggiornamento dell'ambiente e delle regole

- Autenticazione porta per client
- Tagging del traffico con il tag del gruppo di sicurezza (SGT)
- Applicazione dei criteri con l'ACL del gruppo di sicurezza (SGACL)

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base dei componenti CTS
- Conoscenze base della configurazione CLI degli switch Catalyst
- Esperienza nella configurazione di Identity Services Engine (ISE)

Componenti usati

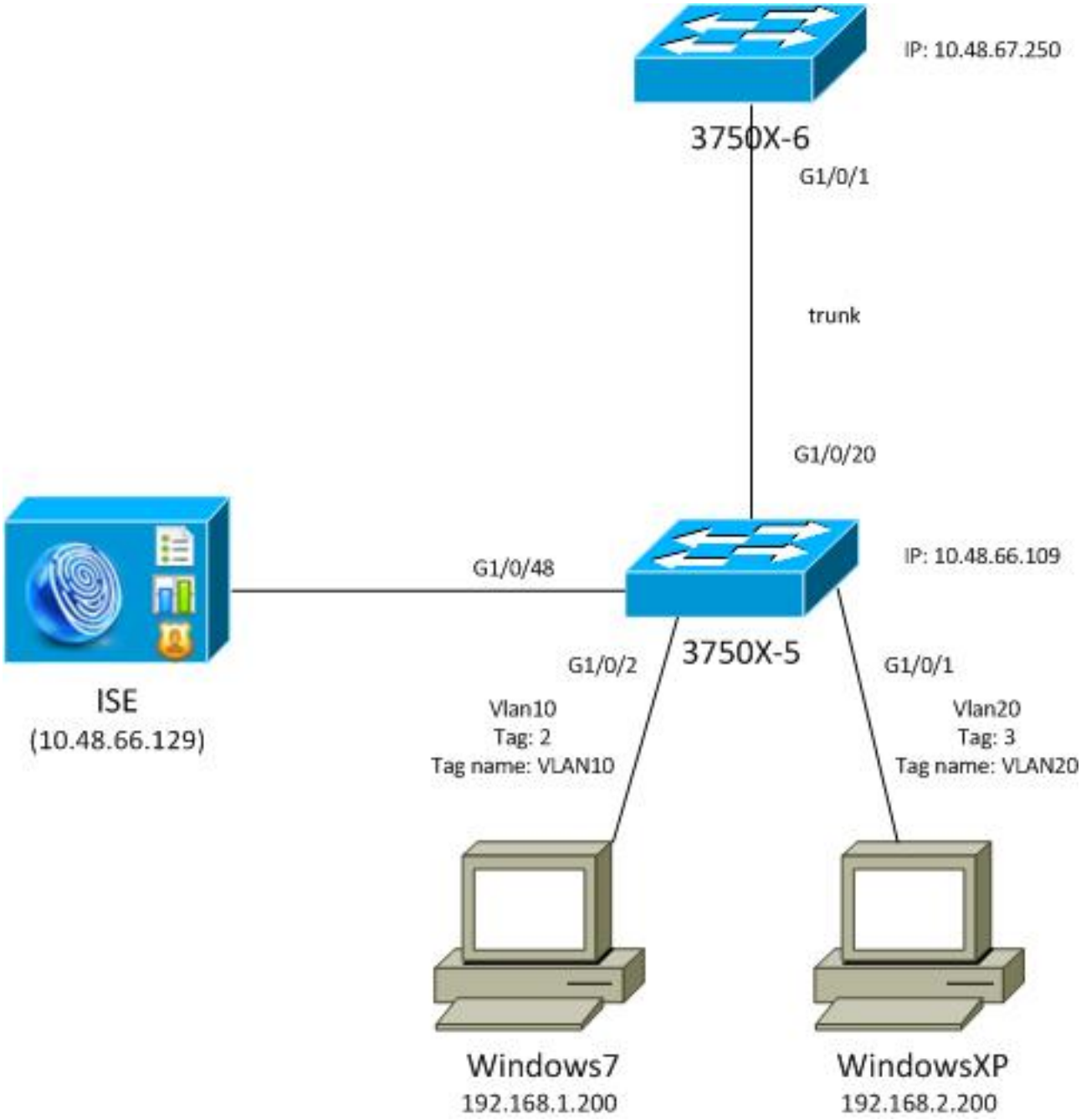
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Microsoft (MS) Windows 7 e MS Windows XP
- Software 3750X, versioni 15.0 e successive
- Software ISE, versioni 1.1.4 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.

Configurazione

Esempio di rete



In questo diagramma della topologia di rete, lo switch 3750X-5 è il dispositivo di inizializzazione che conosce l'indirizzo IP dell'ISE e scarica automaticamente la PAC utilizzata per la successiva autenticazione nel cloud CTS. Il dispositivo di inizializzazione funge da autenticatore 802.1x per i dispositivi non di inizializzazione. Cisco Catalyst serie 3750X-6 Switch (3750X-6) è il dispositivo non-seed. Agisce come supplicant 802.1x al dispositivo di inizializzazione. Dopo l'autenticazione del dispositivo senza seeding all'ISE tramite il dispositivo di seeding, viene autorizzato l'accesso al cloud CTS. Dopo un'autenticazione riuscita, lo stato della porta 802.1x sullo switch 3750X-5 viene modificato in **autenticato** e la crittografia MACsec viene negoziata. Il traffico tra gli switch viene quindi contrassegnato con SGT e criptato.

L'elenco seguente riepiloga il flusso del traffico previsto:

- Il seed 3750X-5 si connette all'ISE e scarica la PAC, che viene successivamente utilizzata per un aggiornamento dell'ambiente e delle policy.
- Lo switch 3750X-6 non-seed esegue l'autenticazione 802.1x con il ruolo supplicant per autenticare/autorizzare e scaricare la PAC dall'ISE.
- Lo switch 3750X-6 esegue una seconda sessione di autenticazione flessibile e protocollo

802.1x Extensible Authentication Protocol tramite Secure Protocol (EAP-FAST) per autenticarsi con il tunnel protetto basato sulla PAC.
- Lo switch 3750X-5 scarica le policy SGA per se stesso e per conto di 3750X-6.
- Si verifica una sessione SAP tra lo switch 3750X-5 e lo switch 3750X-6, vengono negoziate le cifrature MACsec e viene scambiata la policy.
- Il traffico tra gli switch è contrassegnato e crittografato.

Configurazione di switch seed e non Seed

Il dispositivo di inizializzazione (3750X-5) è configurato per utilizzare ISE come server RADIUS per CTS:

```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa authorization network ise group radius
aaa accounting dot1x default start-stop group radius

cts authorization list ise

radius-server host 10.48.66.129 pac key cisco
radius-server host 10.48.66.129 auth-port 1812
radius-server vsa send accounting
radius-server vsa send authentication
```

L'imposizione RBACL (Role-Based Access Control List) e SGACL (Security Group Based Access Control List) sono abilitate (vengono utilizzate in seguito):

```
cts role-based enforcement
cts role-based enforcement vlan-list 1-1005,1007-4094
```

Il dispositivo non-seed (3750X-6) è configurato solo per l'autenticazione, l'autorizzazione e l'accounting (AAA) senza la necessità di un'autorizzazione RADIUS o CTS:

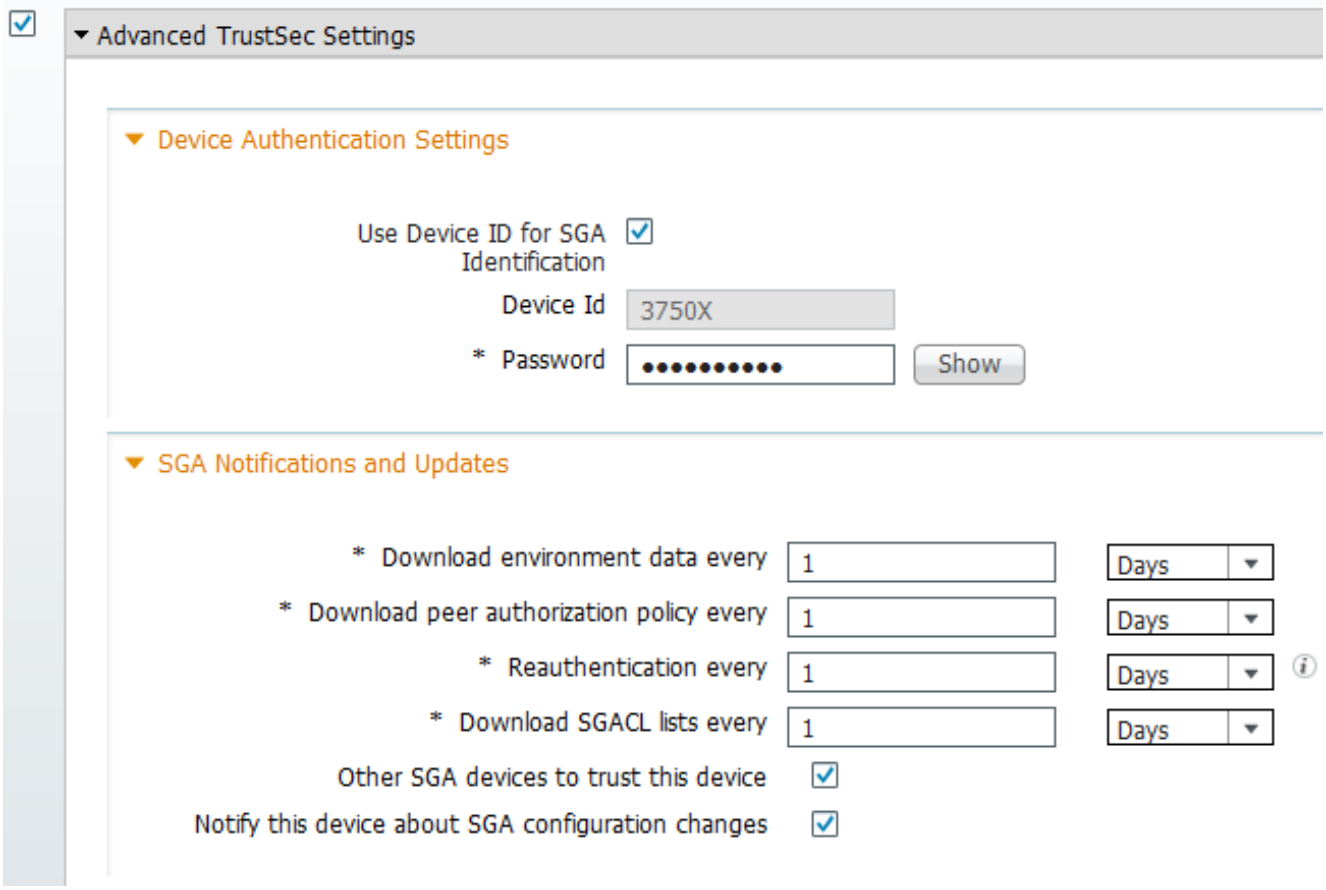
```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
```

Prima di abilitare 802.1x sull'interfaccia, è necessario configurare l'ISE.

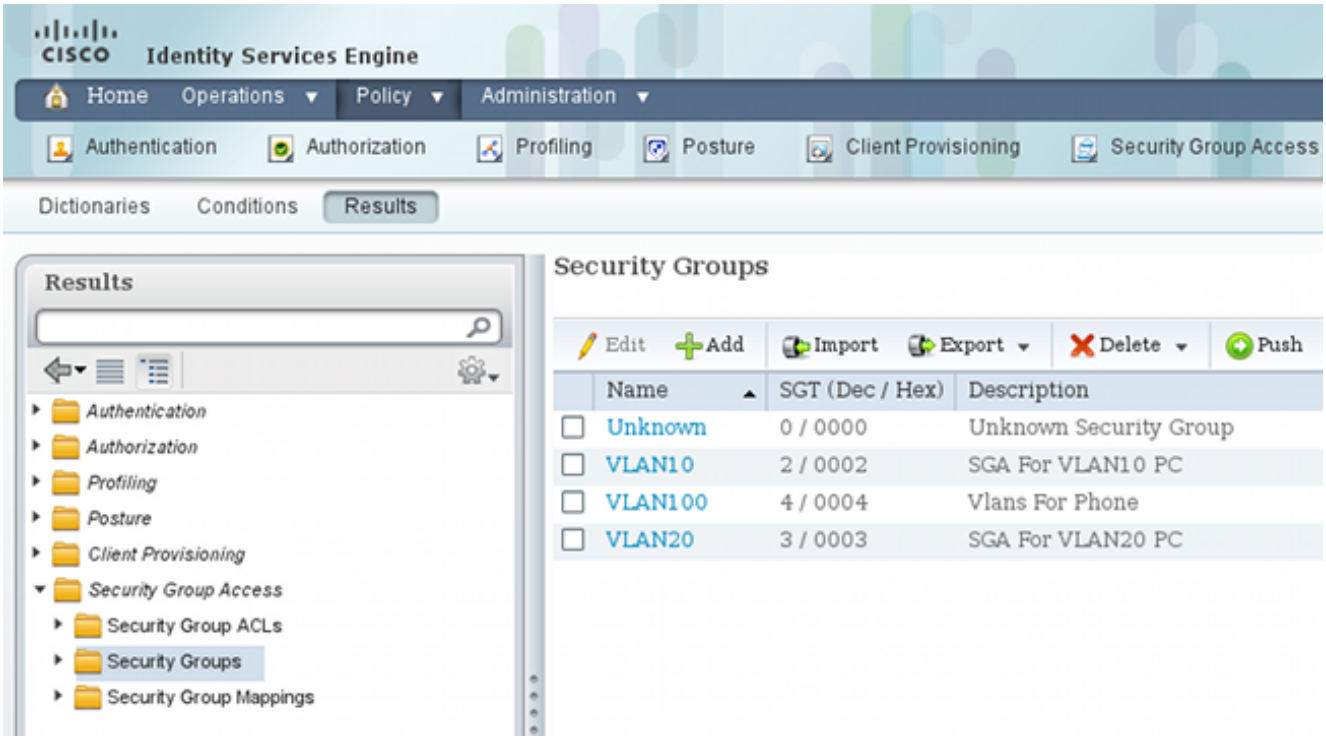
Configurazione dell'ISE

Per configurare l'ISE, completare la procedura seguente:

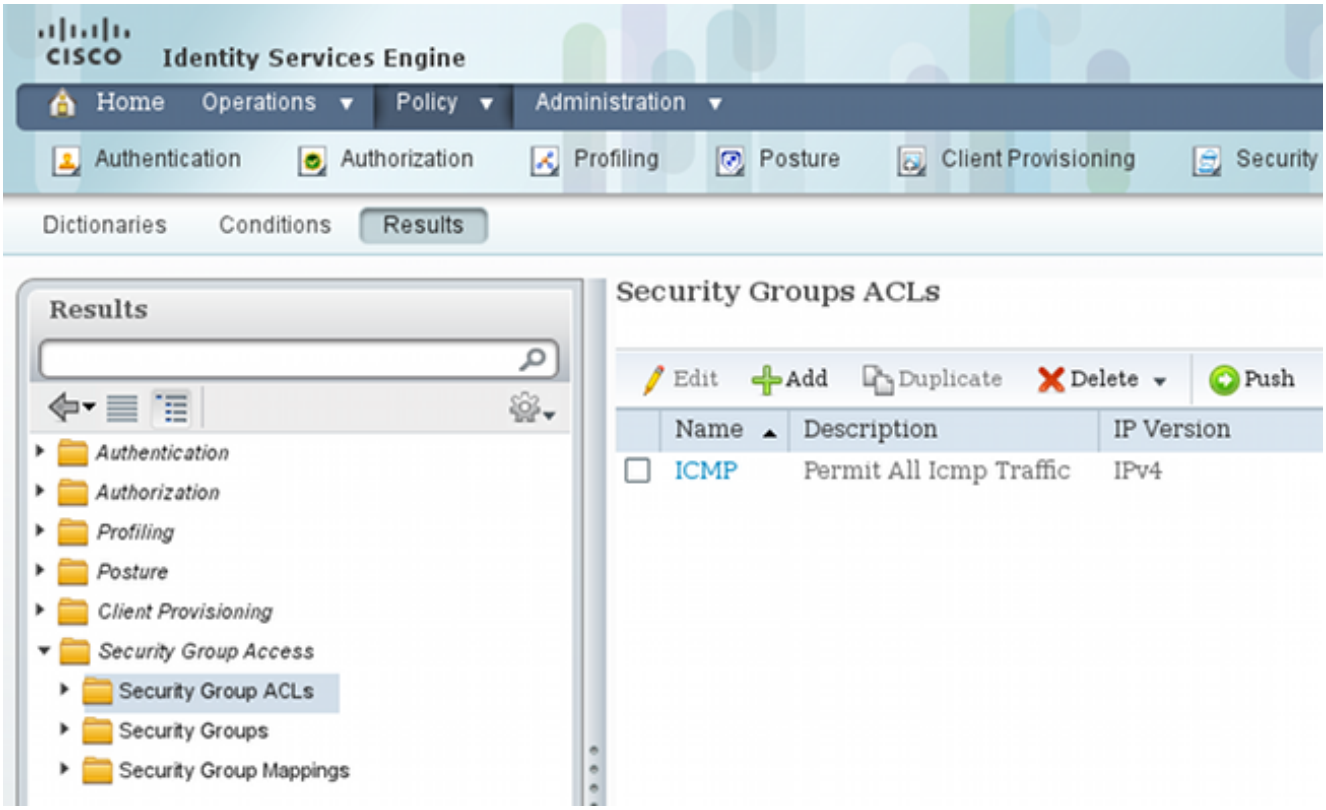
1. Selezionare **Amministrazione > Risorse di rete > Dispositivi di rete**, quindi aggiungere entrambi gli switch come dispositivi di accesso alla rete (NAD). In **Advanced TrustSec Settings**, configurare una password CTS per un utilizzo successivo nella CLI dello switch.



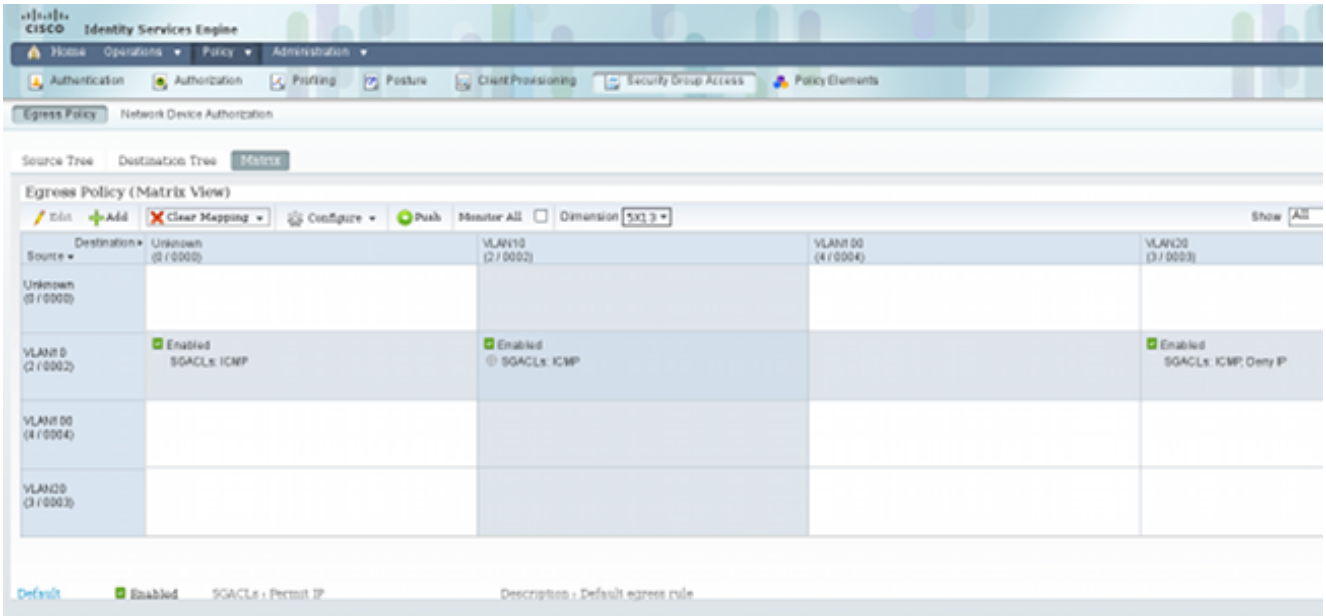
2. Passare a **Criterio > Elementi criteri > Risultati > Accesso al gruppo di sicurezza > Gruppi di sicurezza**, quindi aggiungere le SGT appropriate. Questi tag vengono scaricati quando gli switch richiedono un aggiornamento dell'ambiente.



3. Selezionare **Criteri > Elementi criterio > Risultati > Accesso al gruppo di sicurezza > ACL del gruppo di sicurezza** e configurare un SGACL.



4. Passare a **Criteri > Accesso al gruppo di sicurezza** e definire un criterio con la matrice.



Nota: è necessario configurare i criteri di autorizzazione per il supplicant di MS Windows in modo che riceva il tag corretto. Per una configurazione dettagliata, consultare l'esempio di configurazione e la guida alla risoluzione dei problemi dello switch ASA e Catalyst serie 3750X TrustSec.

Provisioning PAC per 3750X-5

La PAC è necessaria per l'autenticazione nel dominio CTS (come fase 1 per EAP-FAST) ed è utilizzata anche per ottenere i dati sull'ambiente e sulle policy dall'ISE. Senza la PAC corretta, non

è possibile ottenere tali dati dall'ISE.

Dopo aver fornito le credenziali corrette sullo switch 3750X-5, viene scaricata la PAC:

```
bsns-3750-5#cts credentials id 3750X password ciscocisco
bsns-3750-5#show cts pacs
 AID: C40A15A339286CEAC28A50DBBAC59784
 PAC-Info:
   PAC-type = Cisco Trustsec
   AID: C40A15A339286CEAC28A50DBBAC59784
   I-ID: 3750X
   A-ID-Info: Identity Services Engine
   Credential Lifetime: 08:31:32 UTC Oct 5 2013
 PAC-Opaque: 000200B000030001000400010C40A15A339286CEAC28A50DBBAC5978400060094
0003010076B969769CB5D45453FDCDEB92271C500000001351D15DD900093A8044DF74B2B71F
E667D7B908DB7AEEA32208B4E069FDB0A31161CE98ABD714C55CA0C4A83E4E16A6E8ACAC1D081
F235123600B91B09C9A909516D0A2B347E46D15178028ABFFD61244B3CD6F332435C867A968CE
A6B09BFA8C181E4399CE498A676543714A74B0C048A97C18684FF49BF0BB872405
 Refresh timer is set for 2y25w
```

La PAC viene scaricata tramite EAP-FAST con il protocollo MSCHAPv2 (Microsoft Challenge Handshake Authentication Protocol), con le credenziali fornite nella CLI e le stesse credenziali configurate sull'ISE.

La PAC viene utilizzata per l'aggiornamento dell'ambiente e dei criteri. Per questi switch, usare le richieste RADIUS con **cisco av-pair cts-pac-opaque**, che è derivato dalla chiave PAC e può essere decriptato sull'ISE.

Provisioning PAC per l'autenticazione 3750X-6 e NDAC

Affinché un nuovo dispositivo possa connettersi al dominio CTS, è necessario abilitare 802.1x sulle porte corrispondenti.

Il protocollo SAP viene utilizzato per la gestione delle chiavi e la negoziazione delle suite di cifratura. GMAC (Galois Message Authentication Code) viene utilizzato per l'autenticazione e GCM (Galois/Counter Mode) per la crittografia.

Sul commutatore di velocità:

```
interface GigabitEthernet1/0/20
 switchport trunk encapsulation dot1q
 switchport mode trunk
 cts dot1x
sap mode-list gcm-encrypt
```

Sul commutatore non-seed:

```
interface GigabitEthernet1/0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 cts dot1x
 sap mode-list gcm-encrypt
```

Questa funzionalità è supportata solo sulle porte trunk (switch-switch MACsec). Per MACsec

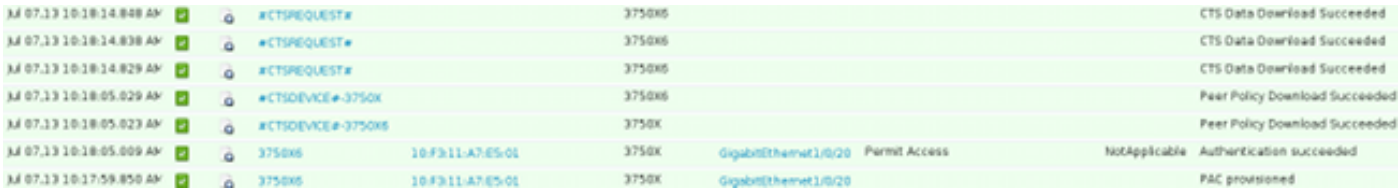
switch-host, che utilizza il protocollo MACsec Key Agreement (MKA) anziché SAP, fare riferimento alla configurazione della crittografia MACsec.

Subito dopo l'abilitazione di 802.1x sulle porte, lo switch non seed agisce come supplicant per lo switch seed, che è l'autenticatore.

Questo processo è denominato NDAC e ha lo scopo di connettere un nuovo dispositivo al dominio CTS. L'autenticazione è bidirezionale: il nuovo dispositivo dispone di credenziali che vengono verificate sul server di autenticazione ISE. Dopo la preparazione della PAC, il dispositivo è anche sicuro di connettersi al dominio CTS.

> **Nota**: il PAC viene usato per costruire un tunnel Transport Layer Security (TLS) per EAP-FAST. Lo switch 3750X-6 considera attendibili le credenziali PAC fornite dal server in modo simile al modo in cui un client considera attendibile il certificato fornito dal server per il tunnel TLS per il metodo EAP-TLS.

Vengono scambiati più messaggi RADIUS:



La prima sessione dello switch 3750X (seed switch) viene utilizzata per la preparazione della PAC. EAP-FAST viene utilizzato senza PAC (viene creato un tunnel anonimo per l'autenticazione MSCHAPv2).

```
12131  EAP-FAST built anonymous tunnel for purpose of PAC provisioning
22037  Authentication Passed
11814  Inner EAP-MSCHAP authentication succeeded
12173  Successfully finished EAP-FAST CTS PAC provisioning/update
11003  Returned RADIUS Access-Reject
```

Vengono utilizzati il nome utente e la password MSCHAPv2 configurati tramite il comando **cts credentials**. Inoltre, alla fine viene restituito un messaggio di rifiuto dell'accesso RADIUS, in quanto, dopo il provisioning della PAC, non è necessaria un'ulteriore autenticazione.

La seconda voce nel registro fa riferimento all'autenticazione 802.1x. EAP-FAST viene utilizzato con la PAC di cui è stato eseguito il provisioning in precedenza.

```
12168  Received CTS PAC
12132  EAP-FAST built PAC-based tunnel for purpose of authentication
11814  Inner EAP-MSCHAP authentication succeeded
15016  Selected Authorization Profile - Permit Access
11002  Returned RADIUS Access-Accept
```

Questa volta, il tunnel non è anonimo, ma protetto da PAC. Anche in questo caso vengono utilizzate le stesse credenziali per la sessione MSCHAPv2. Quindi, viene verificato rispetto alle regole di autenticazione e autorizzazione sull'ISE e viene restituito un messaggio RADIUS Access-Accept. Quindi, lo switch di autenticazione applica gli attributi restituiti e la sessione 802.1x per quella porta passa a uno stato autorizzato.

Come appare il processo per le prime due sessioni 802.1x dallo switch seed?

Ecco i debug più importanti del seme. Il valore di inizializzazione rileva che la porta è attiva e tenta di determinare quale ruolo utilizzare per 802.1x - il richiedente o l'autenticatore:

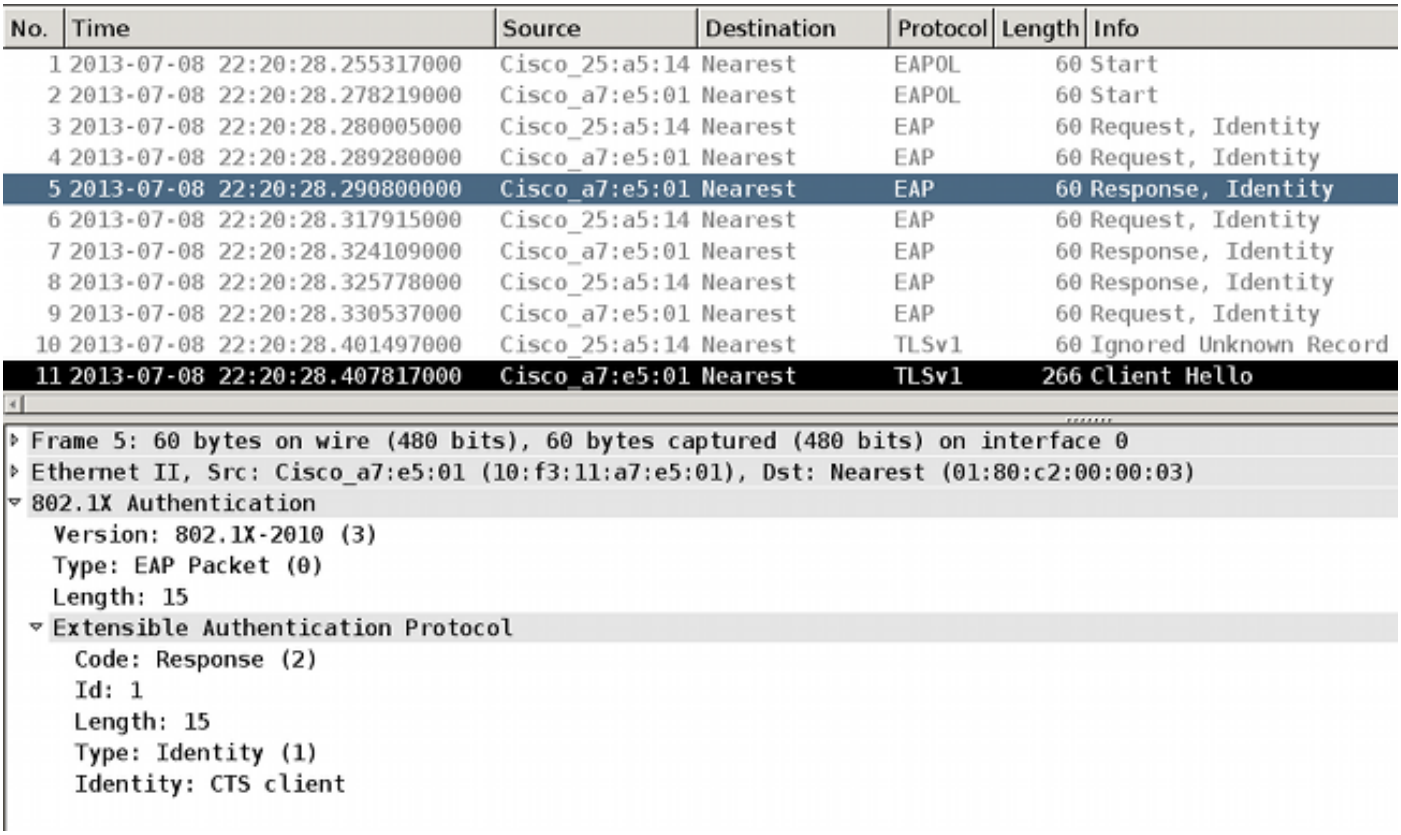
```
debug cts all
debug dot1x all
debug radius verbose
debug radius authentication

Apr 9 11:28:35.347: CTS-ifc-ev: CTS process: received msg_id CTS_IFC_MSG_LINK_UP
Apr 9 11:28:35.347: @@@ cts_ifc GigabitEthernet1/0/20, INIT: ifc_init ->
ifc_authenticating
Apr 9 11:28:35.356: CTS-ifc-ev: Request to start dot1x Both PAE(s) for
GigabitEthernet1/0/20
Apr 9 11:28:35.356: dot1x-ev(Gi1/0/20): Created authenticator subblock
Apr 9 11:28:35.356: dot1x-ev(Gi1/0/20): Created supplicant subblock

Apr 9 11:28:35.364: dot1x-ev:dot1x_supp_start: Not starting default supplicant
on GigabitEthernet1/0/20
Apr 9 11:28:35.381: dot1x-sm:Posting SUPP_ABORT on Client=7C24F2C

Apr 9 11:28:35.397: %AUTHMGR-5-START: Starting 'dot1x' for client (10f3.11a7.e501) on
Interface Gi1/0/20 AuditSessionID C0A800010000054135A5E32
```

Viene infine utilizzato il ruolo di autenticatore, in quanto lo switch ha accesso all'ISE. Nello switch 3750X-6 viene scelto il ruolo supplicant.

Dettagli sulla selezione dei ruoli 802.1x

> **Nota**: dopo aver ottenuto la PAC e ottenuto l'autenticazione 802.1x, lo switch supplicant scarica i dati di ambiente (descritti più avanti) e viene a conoscenza dell'indirizzo IP del server AAA. In questo esempio, entrambi gli switch hanno una connessione dedicata (backbone) per ISE. In seguito, i ruoli possono essere diversi: il primo switch che riceve una risposta dal server AAA diventa l'autenticatore, il secondo diventa il supplicant.

Ciò è possibile perché entrambi gli switch con il server AAA contrassegnato come ALIVE inviano un'identità di richiesta EAP (Extensible Authentication Protocol). L'utente che riceve per primo la risposta di identità EAP diventa l'autenticatore ed elimina le successive richieste di identità.



No.	Time	Source	Destination	Protocol	Length	Info
1	2013-07-08 22:20:28.255317000	Cisco_25:a5:14	Nearest	EAPOL	60	Start
2	2013-07-08 22:20:28.278219000	Cisco_a7:e5:01	Nearest	EAPOL	60	Start
3	2013-07-08 22:20:28.280005000	Cisco_25:a5:14	Nearest	EAP	60	Request, Identity
4	2013-07-08 22:20:28.289280000	Cisco_a7:e5:01	Nearest	EAP	60	Request, Identity
5	2013-07-08 22:20:28.290800000	Cisco_a7:e5:01	Nearest	EAP	60	Response, Identity
6	2013-07-08 22:20:28.317915000	Cisco_25:a5:14	Nearest	EAP	60	Request, Identity
7	2013-07-08 22:20:28.324109000	Cisco_a7:e5:01	Nearest	EAP	60	Response, Identity
8	2013-07-08 22:20:28.325778000	Cisco_25:a5:14	Nearest	EAP	60	Response, Identity
9	2013-07-08 22:20:28.330537000	Cisco_a7:e5:01	Nearest	EAP	60	Request, Identity
10	2013-07-08 22:20:28.401497000	Cisco_25:a5:14	Nearest	TLSv1	60	Ignored Unknown Record
11	2013-07-08 22:20:28.407817000	Cisco_a7:e5:01	Nearest	TLSv1	266	Client Hello

Dopo aver selezionato il ruolo 802.1x (in questo scenario, lo switch 3750X-6 è il supplicant, in quanto non ha ancora accesso al server AAA), i pacchetti successivi coinvolgono lo scambio EAP-FAST per la preparazione della PAC. Il nome utente **client CTS** viene utilizzato per il nome utente della richiesta RADIUS e come identità EAP:

```
Apr  9 11:28:36.647: RADIUS:  User-Name           [1]   12  "CTS client"
Apr  9 11:28:35.481: RADIUS:  EAP-Message         [79]  17
Apr  9 11:28:35.481: RADIUS:   02 01 00 0F 01 43 54 53 20 63 6C 69 65 6E 74        [ CTS client]
```

Dopo la creazione del tunnel EAP-FAST anonimo, viene eseguita una sessione MSCHAPv2 per il nome utente **3750X6** (**credenziali CTS**). Non è possibile vederlo sullo switch, perché è un tunnel TLS (criptato), ma è provato dai log dettagliati sull'ISE per la preparazione della PAC. È possibile visualizzare **CTS Client** per il nome utente RADIUS e come risposta di identità EAP. Tuttavia, per il metodo interno (MSCHAP), viene utilizzato il nome utente **3750X6**:

EAP Authentication Method :	EAP-MSCHAPv2
EAP Tunnel Method :	EAP-FAST
Username:	3750X6
RADIUS Username :	CTS client
Calling Station ID:	10:F3:11:A7:E5:01

Viene eseguita la seconda autenticazione EAP-FAST. Questa volta viene utilizzato il PAC fornito in precedenza. Anche in questo caso, il **client CTS** viene utilizzato come nome utente e identità esterna RADIUS, mentre il valore **3750X6** viene utilizzato per l'identità interna (MSCHAP). Autenticazione riuscita:

RADIUS Status:	Authentication succeeded
NAS Failure:	
Username:	3750X6
MAC/IP Address:	10:F3:11:A7:E5:01
Network Device:	3750X : 10.48.66.109 : GigabitEthernet1/0/20
Allowed Protocol:	NDAC_SGT_Service
Identity Store:	Internal CTS Devices
Authorization Profiles:	Permit Access
SGA Security Group:	Unknown
Authentication Protocol :	EAP-FAST(EAP-MSCHAPv2)

Tuttavia, questa volta, l'ISE restituisce diversi attributi nel pacchetto RADIUS Accept:

Authentication Result

```
User-Name=3750X6
 State=ReauthSession:C0A800010000053A33FD79AF
 Class=CACS:C0A800010000053A33FD79AF:ise/162314118/3616
 Session-Timeout=86400
 Termination-Action=RADIUS-Request
 EAP-Key-Name=2b:54:e8:37:14:10:f0:3c:1b:90:f1:d7:ad:1c:0b:cc:62:e5:03:4c:6b
 cisco-av-pair=cts:security-group-tag=0000-01
 cisco-av-pair=cts:supplicant-cts-capabilities=sap
 MS-MPPE-Send-Key=ce:d6:28:6f:b4:c0:2a:96:69:93:fe:41:0d:1e:80:9d:31:e2:b8:c
 MS-MPPE-Recv-Key=d4:8c:13:cd:d7:18:c7:1f:57:21:0d:de:39:fa:cd:68:aa:ca:1b:4f
```

In questo caso, lo switch autenticatore cambia la porta in stato autorizzato:

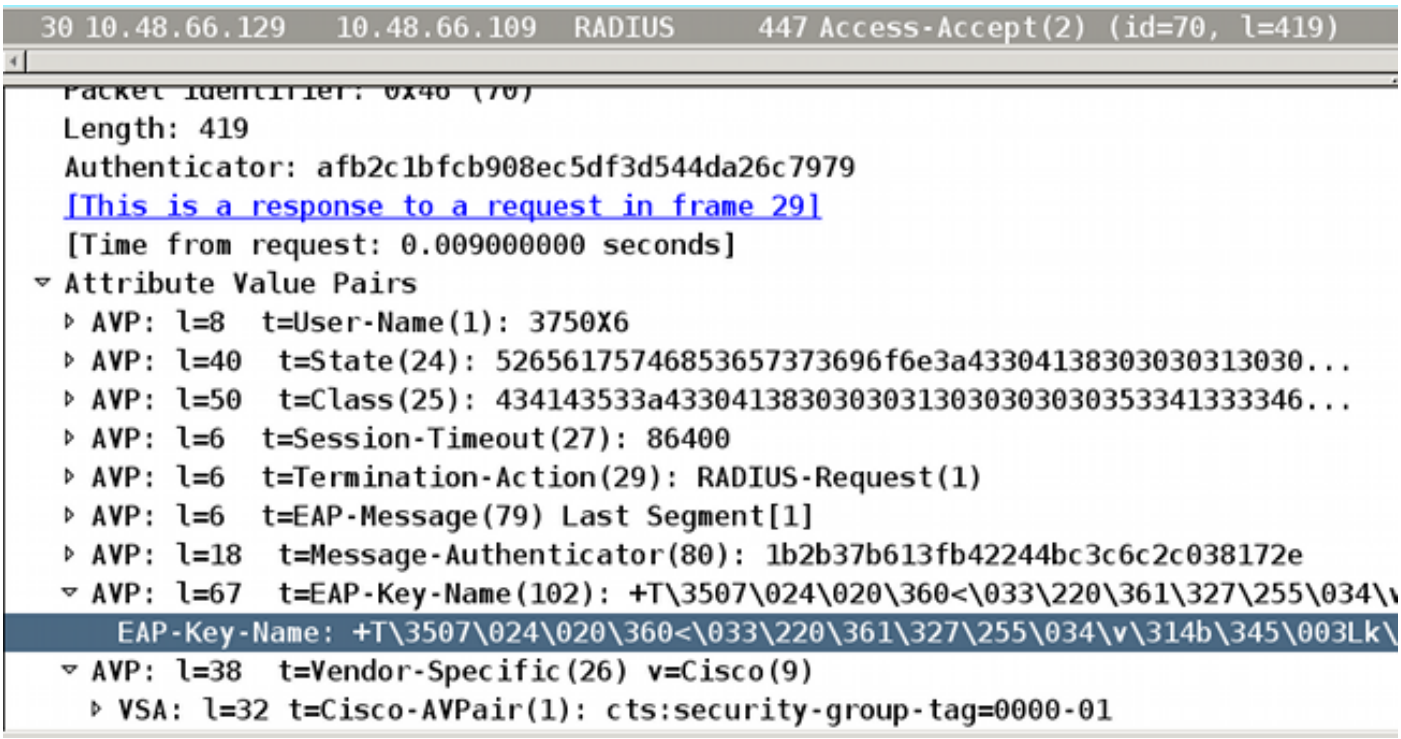
```
bsns-3750-5#show authentication sessions int g1/0/20
            Interface:  GigabitEthernet1/0/20
          MAC Address:  10f3.11a7.e501
           IP Address:  Unknown
             User-Name:  3750X6
                Status:  Authz Success
               Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  multi-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
     Session timeout:  86400s (local), Remaining: 81311s
      Timeout action:  Reauthenticate
        Idle timeout:  N/A
   Common Session ID:  C0A800010000054135A5E321
     Acct Session ID:  0x0000068E
              Handle:  0x09000542

Runnable methods list:
      Method   State
      dot1x    Authc Success
```

In che modo lo switch di autenticazione rileva che il nome utente è **3750X6**? Per il nome utente RADIUS e l'identità EAP esterna, viene utilizzato il **client CTS** e l'identità interna è crittografata e

non visibile per l'autenticatore. Il nome utente viene acquisito dall'ISE. L'ultimo pacchetto RADIUS (Access-Accept) contiene **username=3750X6**, mentre tutti gli altri contengono **username = Cts client**. Ecco perché lo switch supplicant riconosce il nome utente reale. Questo comportamento è conforme alla RFC. Dalla sezione 3.0 della RFC3579:

```
The User-Name attribute within the Access- Accept packet need not be the same
as the User-Name attribute in the Access-Request.
```

Nell'ultimo pacchetto della sessione di autenticazione 802.1x, ISE restituisce un messaggio RADIUS Accept **cisco-av-pair** con il **nome-chiave EAP**:

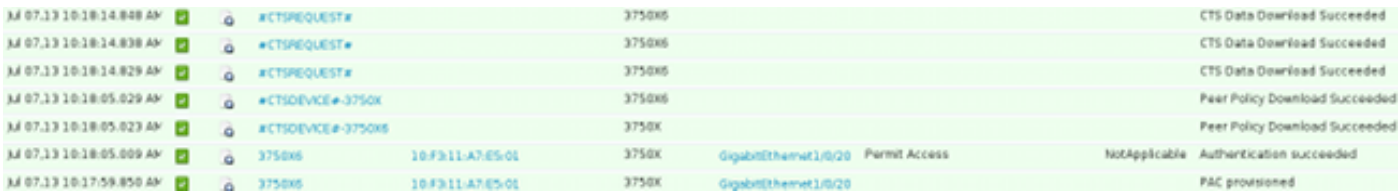


Viene utilizzato come materiale per le chiavi per la negoziazione SAP.

Inoltre, il SGT è passato. Ciò significa che il commutatore di autenticazione contrassegna il traffico proveniente dal supplicant con un **valore predefinito = 0**. È possibile configurare un valore specifico sull'ISE in modo che restituisca qualsiasi altro valore. Questo vale solo per il traffico senza tag; il traffico con tag non viene riscritto perché, per impostazione predefinita, lo switch di autenticazione considera attendibile il traffico proveniente dal supplicant autenticato (ma questa impostazione può essere modificata anche sull'ISE).

Download criteri SGA

Sono disponibili altri scambi RADIUS (senza EAP) oltre alle prime due sessioni 802.1x EAP-FAST (la prima per la preparazione della PAC e la seconda per l'autenticazione). Di seguito vengono riportati i log di ISE:



Il terzo log (**Peer Policy Download**) indica un semplice scambio RADIUS: richiesta RADIUS e accettazione RADIUS per l'utente **3760X6**. Questa operazione è necessaria per scaricare i criteri per il traffico proveniente dal supplicant. I due attributi più importanti sono:

```
▽ AVP: l=31  t=Vendor-Specific(26) v=Cisco(9)
  ▷ VSA: l=25 t=Cisco-AVPair(1): cts:trusted-device=true
▽ AVP: l=38  t=Vendor-Specific(26) v=Cisco(9)
  ▷ VSA: l=32 t=Cisco-AVPair(1): cts:security-group-tag=0000-01
▽ AVP: l=38  t=Vendor-Specific(26) v=Cisco(9)
  ▷ VSA: l=32 t=Cisco-AVPair(1): cts:authorization-expiry=86400
```

Per questo motivo, il commutatore di autenticazione considera attendibile il traffico con tag SGT del supplicant (**cts:trusted-device=true**) e contrassegna il traffico senza tag con **tag=0**.

Il quarto log indica lo stesso scambio RADIUS. Tuttavia, questa volta è per l'utente **3750X5** (autenticatore). Ciò è dovuto al fatto che entrambi i peer devono disporre di criteri reciproci. È interessante notare che il richiedente non conosce ancora l'indirizzo IP del server AAA. Per questo motivo lo switch di autenticazione scarica il criterio per conto del supplicant. Queste informazioni vengono successivamente passate al richiedente (insieme all'indirizzo IP ISE) nella negoziazione SAP.

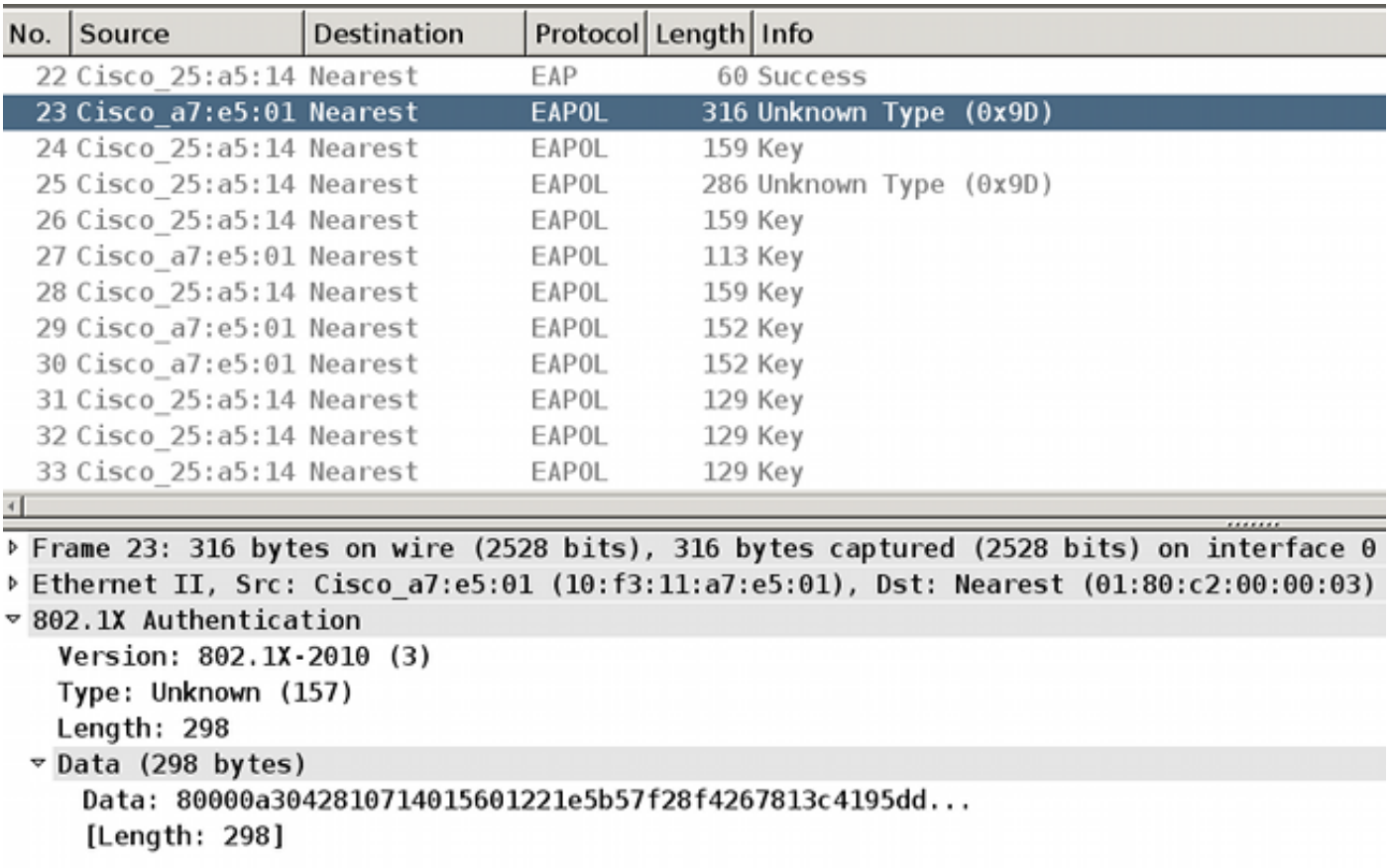
Negoziazione SAP

Subito dopo il completamento della sessione di autenticazione 802.1x, viene eseguita la negoziazione SAP. Questa negoziazione è necessaria per:

- Negoziare i livelli di crittografia (con il comando **sap mode-list gcm-encrypt**) e le suite di crittografia
- Deriva chiavi di sessione per traffico dati
- Sottoporsi al processo di rigenerazione delle chiavi
- Eseguire controlli di sicurezza aggiuntivi e assicurarsi che i passaggi precedenti siano protetti

SAP è un protocollo progettato da Cisco Systems sulla base di una versione bozza di 802.11i/D6.0. Per i dettagli, richiedere l'accesso alla pagina [Cisco TrustSec Security Association Protocol - protocol support Cisco Trusted Security per Cisco Nexus 7000](#).

SAP Exchange è compatibile con 802.1AE. Tra il richiedente e l'autenticatore viene eseguito uno scambio di chiavi EAPOL (Extensible Authentication Protocol over LAN) per negoziare una suite di cifratura, scambiare i parametri di sicurezza e gestire le chiavi. Sfortunatamente, Wireshark non ha un decodificatore per tutti i tipi EAP richiesti:



No.	Source	Destination	Protocol	Length	Info
22	Cisco_25:a5:14	Nearest	EAP	60	Success
23	Cisco_a7:e5:01	Nearest	EAPOL	316	Unknown Type (0x9D)
24	Cisco_25:a5:14	Nearest	EAPOL	159	Key
25	Cisco_25:a5:14	Nearest	EAPOL	286	Unknown Type (0x9D)
26	Cisco_25:a5:14	Nearest	EAPOL	159	Key
27	Cisco_a7:e5:01	Nearest	EAPOL	113	Key
28	Cisco_25:a5:14	Nearest	EAPOL	159	Key
29	Cisco_a7:e5:01	Nearest	EAPOL	152	Key
30	Cisco_a7:e5:01	Nearest	EAPOL	152	Key
31	Cisco_25:a5:14	Nearest	EAPOL	129	Key
32	Cisco_25:a5:14	Nearest	EAPOL	129	Key
33	Cisco_25:a5:14	Nearest	EAPOL	129	Key

Il completamento di queste attività determina la creazione di un'associazione di protezione (SA, Security Association).

Sullo switch supplicant:

```
bsns-3750-6#show cts interface g1/0/1
Global Dot1x feature is Enabled
Interface GigabitEthernet1/0/1:
    CTS is enabled, mode:    DOT1X
   IFC state:               OPEN
    Authentication Status:   SUCCEEDED
       Peer identity:       "3750X"
       Peer's advertised capabilities: "sap"
       802.1X role:         Supplicant
       Reauth period applied to link:  Not applicable to Supplicant role
   Authorization Status:    SUCCEEDED
       Peer SGT:            0:Unknown
       Peer SGT assignment: Trusted
   SAP Status:              SUCCEEDED
       Version:             2
        Configured pairwise ciphers:
            gcm-encrypt

       Replay protection:      enabled
       Replay protection mode: STRICT

        Selected cipher:        gcm-encrypt

   Propagate SGT:           Enabled
   Cache Info:
       Cache applied to link : NONE

   Statistics:
```

```
        authc success:              12
        authc reject:               1556
        authc failure:              0
        authc no response:          0
        authc logoff:               0
        sap success:                12
        sap fail:                   0
        authz success:              12
        authz fail:                 0
        port auth fail:             0

   L3 IPM:   disabled.

Dot1x Info for GigabitEthernet1/0/1
-----------------------------------
PAE                       = SUPPLICANT
StartPeriod               = 30
AuthPeriod                = 30
HeldPeriod                = 60
MaxStart                  = 3
Credentials profile       = CTS-ID-profile
EAP profile               = CTS-EAP-profile
```

Nell'autenticatore:

```
bsns-3750-5#show cts interface g1/0/20
Global Dot1x feature is Enabled
Interface GigabitEthernet1/0/20:
    CTS is enabled, mode:    DOT1X
   IFC state:               OPEN
   Interface Active for 00:29:22.069
   Authentication Status:   SUCCEEDED
        Peer identity:       "3750X6"
       Peer's advertised capabilities: "sap"
        802.1X role:         Authenticator
       Reauth period configured:       86400 (default)
       Reauth period per policy:       86400 (server configured)
       Reauth period applied to link:  86400 (server configured)
       Reauth starts in approx. 0:23:30:37 (dd:hr:mm:sec)
       Peer MAC address is 10f3.11a7.e501
       Dot1X is initialized
   Authorization Status:    ALL-POLICY SUCCEEDED
        Peer SGT:            0:Unknown
       Peer SGT assignment: Trusted
    SAP Status:              SUCCEEDED
       Version:             2
       Configured pairwise ciphers:
            gcm-encrypt
           {3, 0, 0, 0} checksum 2

       Replay protection:      enabled
       Replay protection mode: STRICT

        Selected cipher:        gcm-encrypt

   Propagate SGT:           Enabled
   Cache Info:
       Cache applied to link : NONE
       Data loaded from NVRAM: F
       NV restoration pending: F
       Cache file name       : GigabitEthernet1_0_20_d
       Cache valid           : F
       Cache is dirty        : T
```

```
        Peer ID               : unknown
        Peer mac              : 0000.0000.0000
        Dot1X role            : unknown
        PMK                   :
             00000000 00000000 00000000 00000000
             00000000 00000000 00000000 00000000

    Statistics:
        authc success:              12
        authc reject:               1542
        authc failure:              0
        authc no response:          0
        authc logoff:               2
        sap success:                12
        sap fail:                   0
        authz success:              13
        authz fail:                 0
        port auth fail:             0

    L3 IPM:   disabled.

Dot1x Info for GigabitEthernet1/0/20
-----------------------------------
PAE                       = AUTHENTICATOR
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
```

In questa modalità, le porte utilizzano la modalità **gcm-encrypt**, ossia il traffico viene autenticato e crittografato, oltre a essere contrassegnato correttamente dal tag SGT. Nell'ISE, nessuna delle due periferiche utilizza criteri di autorizzazione delle periferiche di rete specifici; ciò significa che tutto il traffico proveniente dalla periferica utilizza il tag predefinito **0**. Inoltre, entrambi gli switch considerano attendibili i SGT ricevuti dal peer (a causa degli attributi RADIUS della fase di download dei criteri peer).

Aggiornamento ambiente e criteri

Dopo la connessione di entrambi i dispositivi al cloud CTS, viene avviato un aggiornamento dell'ambiente e dei criteri. L'aggiornamento dell'ambiente è necessario per ottenere le schede SGT e i nomi ed è necessario un aggiornamento delle policy per scaricare il SGACL definito sull'ISE.

In questa fase, il richiedente conosce già l'indirizzo IP del server AAA, quindi può farlo da solo.

Per i dettagli sull'ambiente e sull'aggiornamento delle policy, consultare l'esempio di configurazione e la guida alla risoluzione dei problemi dello switch ASA e Catalyst serie 3750X TrustSec.

Lo switch supplicant ricorda l'indirizzo IP del server RADIUS, anche quando non è configurato alcun server RADIUS e quando il collegamento CTS non è attivo (verso lo switch di autenticazione). Tuttavia, è possibile forzare lo switch a dimenticarlo:

```
bsns-3750-6#show run | i radius
aaa authentication dot1x default group radius
```

```
aaa authorization network default group radius
aaa authorization network ise group radius
aaa accounting dot1x default start-stop group radius
radius-server vsa send authentication

bsns-3750-6#show cts server-list
CTS Server Radius Load Balance = DISABLED
Server Group Deadtime = 20 secs (default)
Global Server Liveness Automated Test Deadtime = 20 secs
Global Server Liveness Automated Test Idle Time = 60 mins
Global Server Liveness Automated Test = ENABLED (default)

Preferred list, 1 server(s):
 *Server: 10.48.66.129, port 1812, A-ID C40A15A339286CEAC28A50DBBAC59784
         Status = ALIVE
         auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins,
deadtime = 20 secs
Installed list: CTSServerList1-0001, 1 server(s):
 *Server: 10.48.66.129, port 1812, A-ID C40A15A339286CEAC28A50DBBAC59784
         Status = ALIVE
         auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins,
deadtime = 20 secs

bsns-3750-6#show radius server-group all
Server group radius
   Sharecount = 1  sg_unconfigured = FALSE
   Type = standard  Memlocks = 1
Server group  private_sg-0
    Server(10.48.66.129:1812,1646) Successful Transactions:
   Authen: 8   Author: 16      Acct: 0
   Server_auto_test_enabled: TRUE
   Keywrap enabled: FALSE

bsns-3750-6#clear cts server 10.48.66.129

bsns-3750-6#show radius server-group all
Server group radius
   Sharecount = 1  sg_unconfigured = FALSE
   Type = standard  Memlocks = 1
Server group  private_sg-0
```

Per verificare l'ambiente e la policy sullo switch supplicant, immettere questi comandi:

```
bsns-3750-6#show cts environment-data
CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
 SGT tag = 0-01:Unknown
Server List Info:
Security Group Name Table:
    0-00:Unknown
    2-00:VLAN10
    3-00:VLAN20
    4-00:VLAN100
Environment Data Lifetime = 86400 secs
Last update time = 03:23:51 UTC Thu Mar 31 2011
Env-data expires in   0:13:09:52 (dd:hr:mm:sec)
Env-data refreshes in 0:13:09:52 (dd:hr:mm:sec)
Cache data applied           = NONE
State Machine is running
```

```
bsns-3750-6#show cts role-based permissions
```

Perché non vengono visualizzati i criteri? Non viene visualizzato alcun criterio, in quanto è necessario abilitare l'**applicazione** dei **criteri** per poterli applicare:

```
bsns-3750-6(config)#cts role-based enforcement
bsns-3750-6(config)#cts role-based enforcement vlan-list all
bsns-3750-6#show cts role-based permissions
IPv4 Role-based permissions default:
       Permit IP-00
IPv4 Role-based permissions from group 2:VLAN10 to group Unknown:
        ICMP-20
```

Perché il richiedente dispone di un solo criterio per **raggruppare Sconosciuto** mentre l'autenticatore ne dispone di più?

```
bsns-3750-5#show cts role-based permissions
IPv4 Role-based permissions default:
       Permit IP-00
IPv4 Role-based permissions from group 2:VLAN10 to group Unknown:
       ICMP-20
IPv4 Role-based permissions from group 2:VLAN10 to group 3:VLAN20:
        ICMP-20
        Deny IP-00
```

Autenticazione porta per client

Il client MS Windows è connesso e autenticato alla porta **g1/0/1** dello switch 3750-5:

```
bsns-3750-5#show authentication sessions int g1/0/1
       Interface:  GigabitEthernet1/0/1
         MAC Address:  0050.5699.4ea1
           IP Address:  192.168.2.200
            User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  multi-auth
    Oper control dir:  both
       Authorized By:  Authentication Server
          Vlan Policy:  20
             ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2
                  SGT:  0003-0
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A80001000001BD336EC4D6
     Acct Session ID:  0x000002F9
              Handle:  0xF80001BE


Runnable methods list:
      Method   State
      dot1x    Authc Success
      mab      Not run
```

In questo caso, lo switch 3750-5 sa che il traffico proveniente dall'host deve essere contrassegnato con **SGT=3** quando viene inviato al cloud CTS.

Traffic Tagging con SGT

Come è possibile sniffare e verificare il traffico?

Questa operazione è difficile perché:

- Embedded Packet Capture è supportato solo per il traffico IP (si tratta di un frame Ethernet modificato con payload SGT e MACsec).
- Porta SPAN (Switched Port Analyzer) con la parola chiave **replication** - questa operazione potrebbe funzionare, ma il problema è che tutti i PC con Wireshark connesso alla porta di destinazione di una sessione di monitoraggio perdono i frame a causa della mancanza di supporto di 802.1ae, che può verificarsi a livello hardware.
- La porta SPAN senza la parola chiave **replication** rimuove l'intestazione **ct** prima che venga inserita su una porta di destinazione.

Applicazione delle policy con SGACL

L'applicazione dei criteri nel cloud CTS viene sempre eseguita alla porta di destinazione. Infatti solo l'ultimo dispositivo conosce il SGT di destinazione del dispositivo dell'endpoint collegato direttamente allo switch. Il pacchetto contiene solo il SGT di origine. Per prendere una decisione sono necessari sia l'SGT di origine che quello di destinazione.

Ecco perché i dispositivi non devono scaricare tutte le policy dall'ISE. ma solo la parte del criterio correlata all'SGT per cui il dispositivo dispone di dispositivi connessi direttamente.

Questo è lo switch 3750-6:

```
bsns-3750-6#show cts role-based permissions
IPv4 Role-based permissions default:
       Permit IP-00
IPv4 Role-based permissions from group 2:VLAN10 to group Unknown:
       ICMP-20
```

Ci sono due politiche qui. Il primo è l'impostazione predefinita per il traffico senza tag (da/a). Il secondo valore è compreso tra **SGT=2** e SGT senza tag, ovvero **0**. Questo criterio esiste perché il dispositivo stesso utilizza il criterio SGA dell'ISE e appartiene a **SGT=0**. Inoltre, **SGT=0** è un tag predefinito. È pertanto necessario scaricare tutti i criteri che dispongono delle regole per il traffico **da/verso SGT=0**. Se si esamina la matrice, verrà visualizzato un solo criterio di questo tipo: **da 2 a 0**.

Questo è lo switch 3750-5, ossia lo switch di autenticazione:

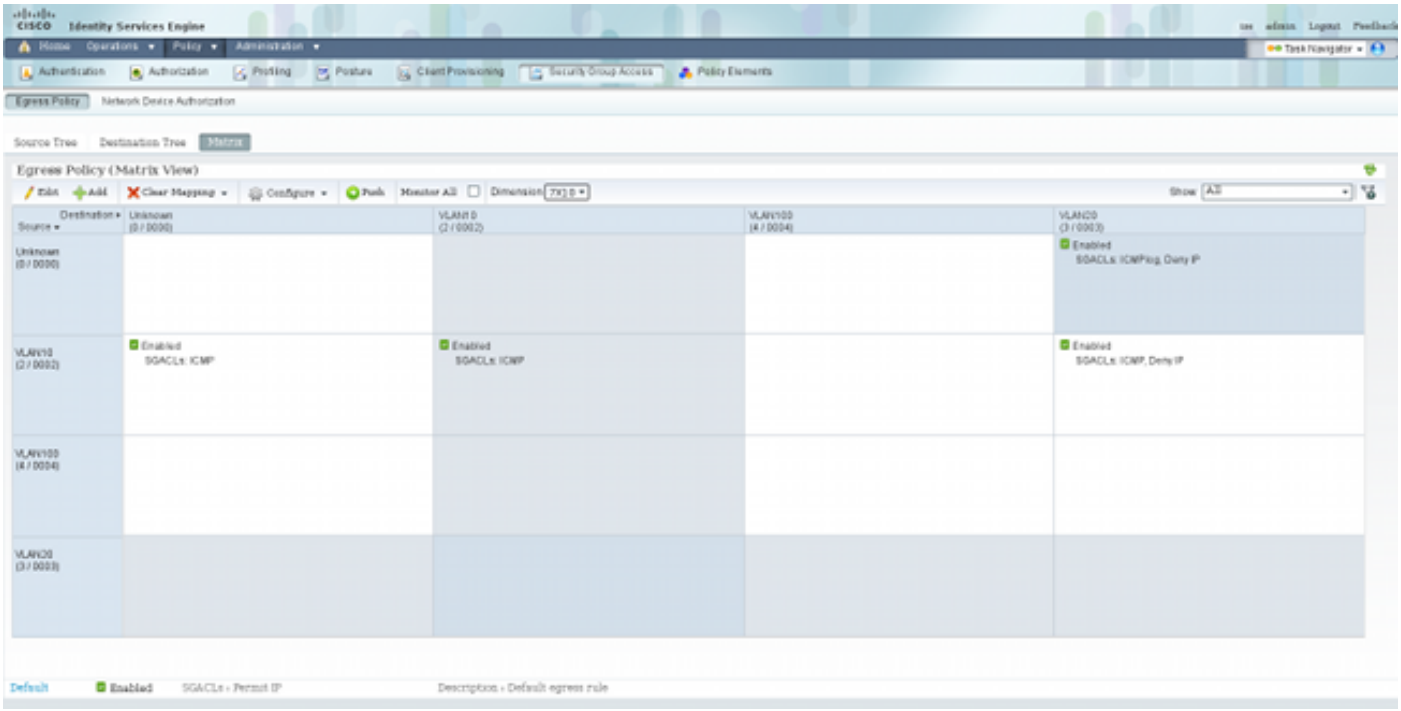
```
bsns-3750-5#show cts role-based permissions
IPv4 Role-based permissions default:
       Permit IP-00
IPv4 Role-based permissions from group 2:VLAN10 to group Unknown:
       ICMP-20
IPv4 Role-based permissions from group 2:VLAN10 to group 3:VLAN20:
       ICMP-20
       Deny IP-00
```

C'è un'altra politica qui: **dalle 2 alle 3**. Ciò è dovuto al fatto che il client 802.1x (MS Windows) è connesso a **g1/0/1** e contrassegnato con **SGT=3**. Per questo motivo è necessario scaricare tutti i

criteri **in SGT=3**.

Provare a eseguire il ping tra 3750X-6 (**SGT=0**) e MS Windows XP (**SGT=3**). Lo switch 3750X-5 è il dispositivo di imposizione.

In precedenza, è necessario configurare una policy sull'ISE per il traffico da **SGT=0 a SGT=3**. Nell'esempio seguente è stato creato un registro ICMP (Internet Control Message Protocol) SGACL contenente solo la riga **allow icmp log**, che viene quindi utilizzata nella matrice per il traffico da **SGT=0 a SGT=3**:



Di seguito viene riportato un aggiornamento della policy sullo switch di imposizione e una verifica della nuova policy:

```
bsns-3750-5#cts refresh policy
Policy refresh in progress

bsns-3750-5#show cts role-based permissions
IPv4 Role-based permissions default:
       Permit IP-00
IPv4 Role-based permissions from group 2:VLAN10 to group Unknown:
       ICMP-20
IPv4 Role-based permissions from group Unknown to group 3:VLAN20:
        ICMPlog-10
        Deny IP-00
IPv4 Role-based permissions from group 2:VLAN10 to group 3:VLAN20:
       ICMP-20
       Deny IP-00
```

Per verificare che l'Access Control List (ACL) sia stato scaricato dall'ISE, immettere questo comando:

```
bsns-3750-5#show ip access-lists ICMPlog-10
Role-based IP access list ICMPlog-10 (downloaded)
   10 permit icmp log
```

Per verificare che l'ACL sia applicato (supporto hardware), immettere questo comando:

```
bsns-3750-5#show cts rbacl | b ICMPlog-10
 name    = ICMPlog-10
 IP protocol version = IPV4
 refcnt = 2
 flag    = 0x41000000
   POLICY_PROGRAM_SUCCESS
   POLICY_RBACL_IPV4
 stale   = FALSE
 ref_q:
   acl_infop(74009FC), name(ICMPlog-10)
 sessions installed:
   session hld(460000F8)
 RBACL ACEs:
 Num ACEs: 1
    permit icmp log
```

Di seguito sono riportati i contatori prima di ICMP:

```
bsns-3750-5#show cts role-based counters
Role-based IPv4 counters
# '-' in hardware counters field indicates sharing among cells with identical
policies
From    To      SW-Denied       HW-Denied       SW-Permitted    HW-Permitted

2       0       0               0               4099            224

*       *       0               0               321810          340989

0       3       0               0               0               0

2       3       0               0               0               0
```

Di seguito viene riportato un ping tra **SGT=0** (switch 3750-6) e MS Windows XP (**SGT=3**) e i contatori:

```
bsns-3750-6#ping 192.168.2.200
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.200, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

bsns-3750-5#show cts role-based counters
Role-based IPv4 counters
# '-' in hardware counters field indicates sharing among cells with identical
policies
From    To      SW-Denied       HW-Denied       SW-Permitted    HW-Permitted

2       0       0               0               4099            224

*       *       0               0               322074          341126

0       3       0               0               0               5

2       3       0               0               0               0
```

Di seguito sono riportati i contatori ACL:

```
bsns-3750-5#show ip access-lists ICMPlog-10
```

```
Role-based IP access list ICMPlog-10 (downloaded)
    10 permit icmp log (5 matches)
```

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

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

Informazioni correlate

- Guida alla configurazione di Cisco TrustSec per 3750
- Guida alla configurazione di Cisco TrustSec per ASA 9.1
- Implementazione di Cisco TrustSec e roadmap
- 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).