Configurazione della distribuzione ZTD (Zero Touch Deployment) di uffici/spoke VPN remoti

Sommario

Introduzione

In questo documento viene descritto come l'opzione ZTD (Zero Touch Deployment) rappresenti una soluzione conveniente e scalabile per le installazioni.

L'installazione sicura ed efficiente e la fornitura di router di uffici remoti (talvolta denominati spoke) possono essere attività difficili. Gli uffici remoti possono trovarsi in luoghi in cui è difficile che un tecnico sul campo configuri il router in loco e la maggior parte dei tecnici sceglie di non inviare router Spoke preconfigurati a causa dei costi e dei potenziali rischi per la sicurezza.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Qualsiasi router Cisco IOS® dotato di una porta USB che supporta le unità flash USB. Per maggiori informazioni, vedere Supporto per USB eToken e funzionalità flash USB.
- Èstato confermato che questa funzione funziona su quasi tutte le piattaforme Cisco 8xx. Per i

dettagli, vedere il white paper sui file di configurazione predefiniti (caratteristiche supportate su Cisco serie 800 ISR).
- Altre piattaforme dotate di porte USB, come le serie G2 e 43xx/44xx ISR (Integrated Service Router).

Componenti usati

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

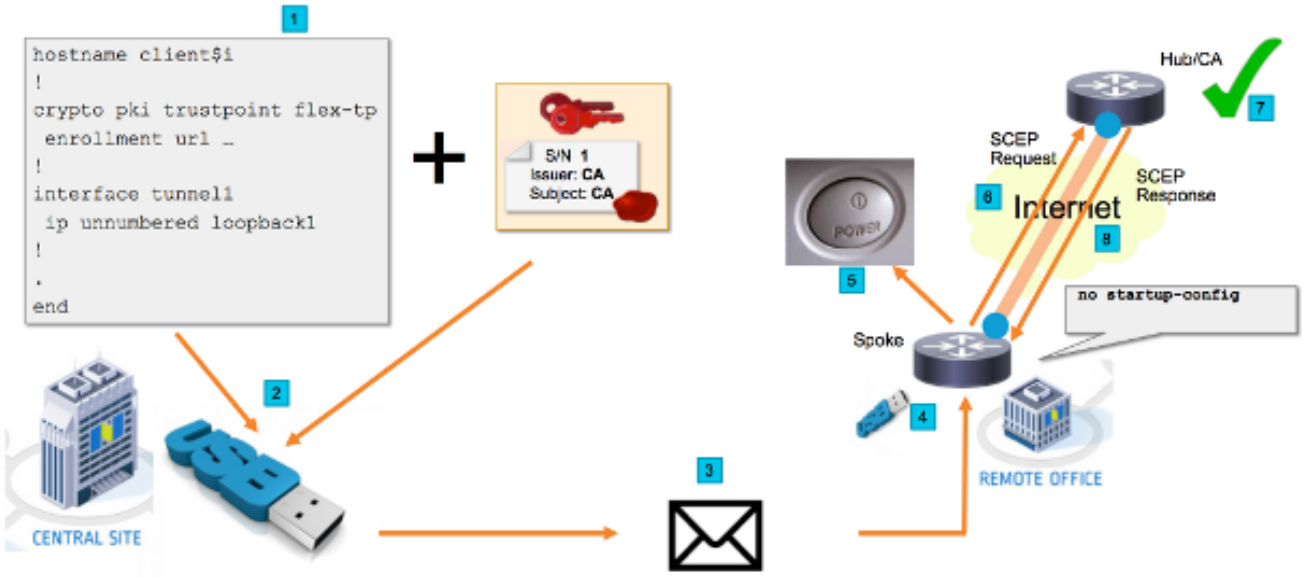
- Protocollo SCEP (Simple Certificate Enrollment Protocol)
- Installazione zero-touch tramite USB
- DMVPN/FlexVPN/VPN da sito a sito

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

> **Nota:** per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete



Flusso di rete

1. Nel sito centrale (sede centrale della società) viene creato un modello della configurazione Spoke. Il modello contiene il certificato dell'Autorità di certificazione (CA) che ha firmato il certificato del router dell'hub VPN.
2. Viene creata un'istanza del modello di configurazione su una chiave USB in un file

denominato **ciscortr.cfg**. Questo file di configurazione contiene la configurazione specifica Spoke per il router da distribuire. **Nota:** La configurazione sull'USB non contiene informazioni riservate se non gli indirizzi IP e il certificato CA. Nessuna chiave privata del server Spoke o CA.

3. L'unità flash USB viene inviata all'ufficio remoto tramite la posta o una società di consegna pacchetti.
4. Il router Spoke viene inviato anche all'ufficio remoto direttamente da Cisco Manufacturing.
5. Nell'ufficio remoto, il router è collegato all'alimentazione e alla rete come spiegato nelle istruzioni incluse con l'unità flash USB. Successivamente, l'unità flash USB viene inserita nel router. **Nota:** Questa fase richiede competenze tecniche minime o nulle, pertanto può essere facilmente eseguita da qualsiasi membro del personale dell'ufficio.
6. Una volta avviato, il router legge la configurazione da **usbflash0:/ciscortr.cfg**. Non appena il router si accende, al server CA viene inviata una richiesta SCEP (Simple Certificate Enrollment Protocol).
7. Sul server CA è possibile configurare la concessione manuale o automatica in base ai criteri di sicurezza aziendali. Quando è configurata per la concessione manuale dei certificati, è necessario eseguire la verifica fuori banda della richiesta SCEP (controllo della convalida dell'indirizzo IP, convalida delle credenziali per il personale che esegue la distribuzione, ecc.). Questo passaggio può variare in base al server CA utilizzato.
8. Dopo che la risposta SCEP è stata ricevuta dal router Spoke, che ora dispone di un certificato valido, la sessione IKE (Internet Key Exchange) viene autenticata con l'hub VPN e il tunnel viene stabilito correttamente.

Autorizzazione basata su SUDI

La fase 7 prevede la verifica manuale della richiesta di firma del certificato inviata tramite il protocollo SCEP, che potrebbe essere complessa e difficile da eseguire per il personale non tecnico. Per aumentare la sicurezza e automatizzare il processo, è possibile utilizzare i certificati dei dispositivi SUDI (Secure Unique Device Identification). I certificati SUDI sono certificati incorporati nei dispositivi ISR 4K. Questi certificati sono firmati da Cisco CA. A ciascun dispositivo prodotto è stato rilasciato un certificato diverso e il numero di serie del dispositivo è indicato nel nome comune del certificato. Il certificato SUDI, la coppia di chiavi associata e l'intera catena di certificati sono memorizzati nel chip Trust Anchor antimanomissione. Inoltre, la coppia di chiavi è associata crittograficamente a un chip Trust Anchor specifico e la chiave privata non viene mai esportata. Questa funzione rende praticamente impossibile la duplicazione o lo spoofing delle informazioni di identità.

La chiave privata SUDI può essere utilizzata per firmare la richiesta SCEP generata dal router. Il server CA è in grado di verificare la firma e leggere il contenuto del certificato SUDI del dispositivo. Il server CA può estrarre le informazioni dal certificato SUDI (come un numero di serie) ed eseguire l'autorizzazione in base a tali informazioni. Il server RADIUS può essere utilizzato per rispondere a tale richiesta di autorizzazione.

L'amministratore crea un elenco dei router spoke e dei numeri di serie associati. I numeri di serie possono essere letti dal case del router da personale non tecnico. Questi numeri di serie vengono memorizzati nel database del server RADIUS e il server autorizza le richieste SCEP in base a tali informazioni, consentendo la concessione automatica del certificato. Notare che il numero di serie è associato crittograficamente a un dispositivo specifico tramite il certificato SUDI firmato da Cisco, quindi è impossibile falsificarlo.

In sintesi, il server CA è configurato per concedere automaticamente le richieste che soddisfano entrambi i criteri seguenti:

- Sono firmate con una chiave privata associata a un certificato firmato da una CA SUDI Cisco
- Sono autorizzati dal server Radius in base alle informazioni sul numero di serie ricavate dal certificato SUDI

Scenari di distribuzione

Il server CA potrebbe essere esposto direttamente a Internet, consentendo così ai client di eseguire la registrazione prima che sia possibile creare il tunnel. Il server CA può anche essere configurato sullo stesso router dell'hub VPN. Il vantaggio di questa topologia è la semplicità. Lo svantaggio è una minore sicurezza, in quanto il server CA è direttamente esposto a varie forme di attacco via Internet.

In alternativa, è possibile espandere la topologia configurando il server Autorità di registrazione. Il ruolo del server Autorità registrazione è quello di valutare e inoltrare le richieste di firma del certificato valide al server CA. Il server Autorità registrazione integrità non contiene la chiave privata della CA e non può generare certificati da solo. In tale distribuzione, il server CA non deve essere esposto a Internet, il che aumenta la sicurezza complessiva.'

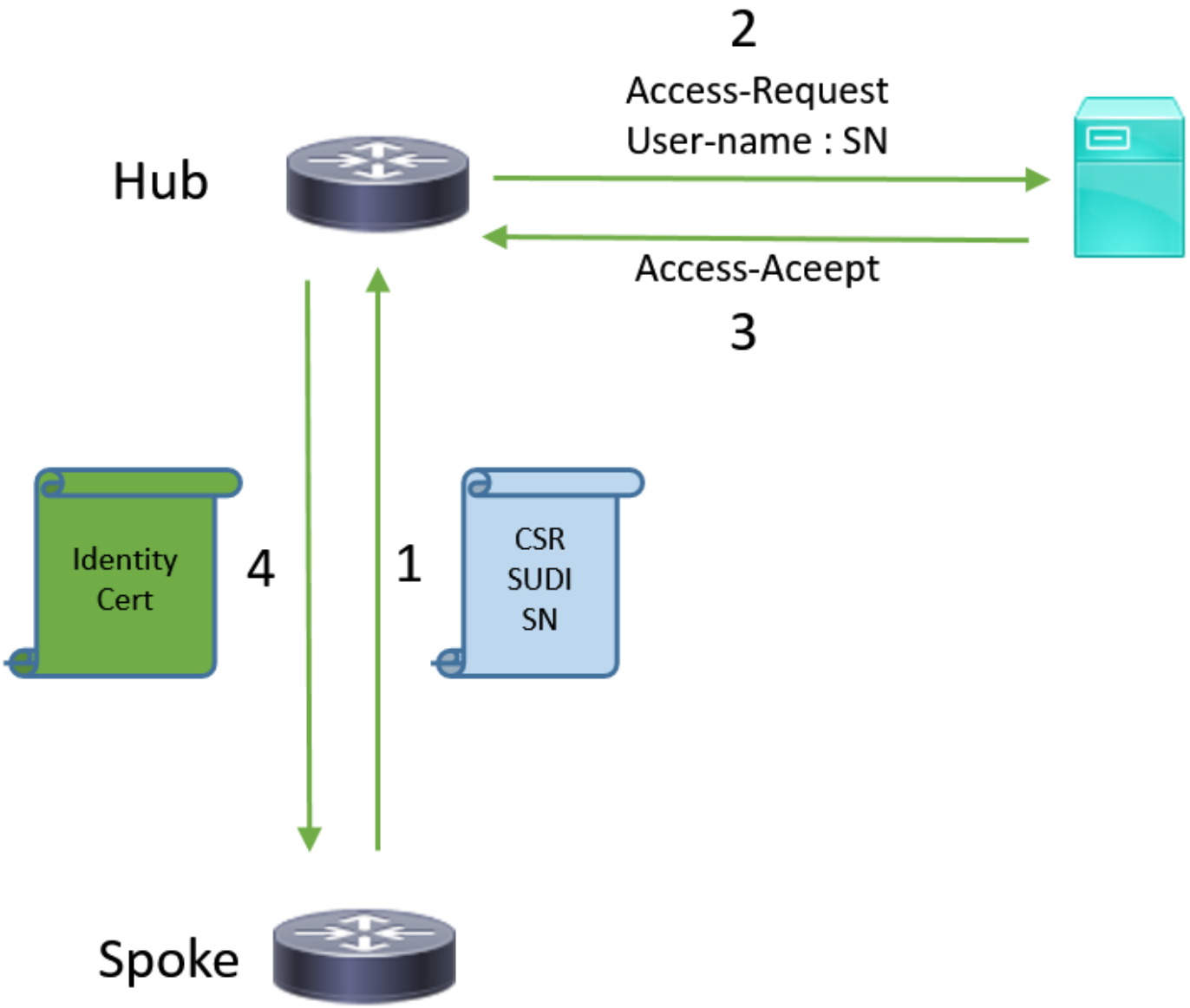
Flusso di rete

1. Il router Spoke crea la richiesta SCEP, la firma con la chiave privata del proprio certificato SUDI e la invia al server CA.

2. Se la richiesta è firmata correttamente, viene generata una richiesta RADIUS. Il numero di serie viene utilizzato come parametro del nome utente.

3. Il server RADIUS accetta o rifiuta la richiesta.

4. Se la richiesta viene accettata, il server CA la concede. Se viene rifiutato, il server CA risponde con lo stato "In sospeso" e il client ritenta la richiesta dopo la scadenza di un timer di fallback.



Configurazione solo con CA

```
!CA server

radius server RADSRV
address ipv4 10.10.20.30 auth-port 1812 acct-port 1813
key cisco123

aaa group server radius RADSRV
server name RADSRV

aaa authorization network SUDI group RADSRV

crypto pki server CA
! will grant certificate for requests signed by SUDI certificate automatically
grant auto trustpoint SUDI
issuer-name CN=ca.example.com
hash sha256
lifetime ca-certificate 7200
lifetime certificate 3600

crypto pki trustpoint CA
rsakeypair CA 2048
```

```
crypto pki trustpoint SUDI
! Need to import the SUDI CA certificate manually, for example with "crypto pki import" command
enrollment terminal
revocation-check none
! Authorize with Radius server
authorization list SUDI
! SN extracted from cert will be used as username in access-request
authorization username subjectname serialnumber
```

!CLIENT

```
crypto pki trustpoint FLEX
enrollment profile PROF
! Serial-number, fqdn and ip-address fields need to be defined, otherwise the interactive prompt
will prevent the process from starting automatically
serial-number none
fqdn none
ip-address none
! Password needs to be specified to automate the process. However, it will not be used by CA
server
password 7 110A1016141D5A5E57
subject-name CN=spoke.example.com
revocation-check none
rsakeypair FLEX 2048
auto-enroll 85 crypto pki profile enrollment PROF ! CA server address enrollment url
http://192.0.2.1 enrollment credential CISCO_IDEVID_SUDI ! By pre-importing CA cert you will
avoid “crypto pki authenticate” step. If auto-enroll is configured, enrollment will also start
automatically crypto pki certificate chain FLEX certificate ca 01 30820354 3082023C A0030201
02020101 300D0609 2A864886 F70D0101 04050030 3B310E30 0C060355 040A1305 43697363 6F310C30
0A060355 040B1303 54414331 ----- output truncated ---- quit
```

RADIUS server:

The Radius needs to return Access-Accept with the following Cisco AV Pair to enable certificate enrollment:

```
pki:cert-application=all
```

Configurazione con CA e RA

!CA server

```
crypto pki server CATEST
   issuer-name CN=CATEST.example.com,OU=TAC,O=Cisco
   ! will grant the requests coming from RA automatically
   grant ra-auto
crypto pki trustpoint CATEST
   revocation-check crl
   rsakeypair CATEST 2048
```

!RA server

```
radius server RADSRV
   address ipv4 10.10.20.30 auth-port 1812 acct-port 1813
   key cisco123

aaa group server radius RADSRV
   server name RADSRV
```

```
aaa authorization network SUDI group RADSRV

crypto pki server RA
   no database archive
   ! will forward certificate requests signed by SUDI certificate automatically
   grant auto trustpoint SUDI
   mode ra

crypto pki trustpoint RA
   ! CA server address
   enrollment url http://10.10.10.10
   serial-number none
   ip-address none
   subject-name CN=ra1.example.com, OU=ioscs RA, OU=TAC, O=Cisco
   revocation-check crl
   rsakeypair RA 2048

crypto pki trustpoint SUDI
   ! Need to import the SUDI CA certificate manually, for example with "crypto pki import"
command
   enrollment terminal
   revocation-check none
   ! Authorize with Radius server
   authorization list SUDI
   ! SN extracted from cert will be used as username in access-request
   authorization username subjectname serialnumber
```

!CLIENT

```
crypto pki trustpoint FLEX
   enrollment profile PROF
   ! Serial-number, fqdn and ip-address fields need to be defined, otherwise the interactive
prompt will prevent the process from starting automatically
   serial-number none
   fqdn none
   ip-address none
   ! Password needs to be specified to automate the process. However, it will not be used by CA
server
   password 7 110A1016141D5A5E57
   subject-name CN=spoke.example.com
   revocation-check none
   rsakeypair FLEX 2048
   auto-enroll 85

crypto pki profile enrollment PROF
   ! RA server address
   enrollment url  http://192.0.2.1
   enrollment credential CISCO_IDEVID_SUDI


! By pre-importing CA cert you will avoid “crypto pki authenticate” step. If auto-enroll is
configured, enrollment will also start automatically
crypto pki certificate chain FLEX
   certificate ca 01
  30820354 3082023C A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  3B310E30 0C060355 040A1305 43697363 6F310C30 0A060355 040B1303 54414331
 ----- output truncated ----
  quit
```

RADIUS server:

The Radius needs to return Access-Accept with the following Cisco AV Pair to enable certificate enrollment:

pki:cert-application=all

Configurazioni/modello

Questo output di esempio mostra una configurazione di ufficio remoto FlexVPN esemplare inserita nell'unità flash nel file usbflash0:/ciscortr.cfg.

```
hostname client1
!
interface GigabitEthernet0
 ip address dhcp
!
crypto pki trustpoint client1
! CA Server's URL
 enrollment url http://10.122.162.242:80
! These fields needs to be filled, to avoid prompt while doing enroll
! This will differ if you use SUDI, please see above
serial-number none
 ip-address none
 password
 subject-name cn=client1.cisco.com ou=cisco ou
!
crypto pki certificate chain client1
 certificate ca 01
 ! CA Certificate here
       quit
!
crypto ikev2 profile default
 match identity remote any
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint client1
 aaa authorization group cert list default default
!
interface Tunnel1
 ip unnumbered GigabitEthernet0
 tunnel source GigabitEthernet0
 tunnel mode ipsec ipv4
! Destination is Internet IP Address of VPN Hub
 tunnel destination 172.16.0.2
 tunnel protection ipsec profile default
!
event manager applet import-cert
! Start importing certificates only after 60s after bootup
! Just to give DHCP time to boot up
 event timer watchdog time 60
 action 1.0 cli command "enable"
 action 2.0 cli command "config terminal"
! Enroll spoke's certificate
 action 3.0 cli command "crypto pki enroll client1"
! After enrollement request is sent, remove that EEM script
 action 4.0 cli command "no event manager applet import-cert"
 action 5.0 cli command "exit"
```

```
event manager applet write-mem
 event syslog pattern "PKI-6-CERTRET"
 action 1.0 cli command "enable"
 action 2.0 cli command "write memory"
 action 3.0 syslog msg "Automatically saved configuration"
```

Verifica

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

Lo strumento Output Interpreter (solo utenti registrati) supporta alcuni comandi **show.** Usare lo strumento Output Interpreter per visualizzare un'analisi dell'output del comando **show.**

Èpossibile verificare sul spoke se i tunnel sono saliti:

```
client1#show crypto session
Crypto session current status

Interface: Tunnel1
Profile: default
Session status: UP-ACTIVE
Peer: 172.16.0.2 port 500
 Session ID: 1
 IKEv2 SA: local 172.16.0.1/500 remote 172.16.0.2/500 Active
 IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
       Active SAs: 2, origin: crypto map
```

Èinoltre possibile verificare sul spoke se il certificato è stato registrato correttamente:

```
client1#show crypto pki certificates
Certificate
  Status: Available
  Certificate Serial Number (hex): 06
  Certificate Usage: General Purpose
  Issuer:
    cn=CA
  Subject:
    Name: client1
    hostname=client1
    cn=client1.cisco.com ou=cisco ou
  Validity Date:
    start date: 01:34:34 PST Apr 26 2015
    end   date: 01:34:34 PST Apr 25 2016
  Associated Trustpoints: client1
  Storage: nvram:CA#6.cer

CA Certificate
 Status: Available
 Certificate Serial Number (hex): 01
 Certificate Usage: Signature
 Issuer:
   cn=CA
 Subject:
   cn=CA
 Validity Date:
   start date: 01:04:46 PST Apr 26 2015
   end   date: 01:04:46 PST Apr 25 2018
 Associated Trustpoints: client1
 Storage: nvram:CA#1CA.cer
```

Risoluzione dei problemi

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

Avvertenze e problemi noti

Cisco ID bug CSCuu93989 - La Configurazione guidata arresta il flusso PnP sulle piattaforme G2 e potrebbe impedire al sistema di caricare la configurazione da usbflash:/ciscortr.cfg. È possibile che il sistema si arresti alla funzionalità della Configurazione guidata:

```
         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:
```

Nota: Assicurarsi di utilizzare una versione che contenga una correzione per il difetto.

ZTD tramite USB e file di configurazione predefiniti

La funzione **Default Configuration Files** utilizzata in questo documento è diversa da **Zero Touch Deployment via USB** descritta in Panoramica sull'implementazione di Cisco serie 800 ISR.

-	**Installazione zero-touch tramite USB**	**File di configurazione predefiniti**
Piattaforme supportate	Limitato a pochi router 8xx. Per i dettagli, vedere Panoramica dell'implementazione di Cisco serie 800 ISR	Tutti gli ISR G2, 43xx e 4
Nome file	cfg	ciscorr.cfg
Salva la configurazione sulla memoria flash locale	Sì, automaticamente	No, è necessario Embedd Event Manager (EEM)

Poiché la funzionalità **File di configurazione predefiniti** supporta più piattaforme, questa tecnologia è stata scelta per la soluzione illustrata in questo articolo.

Riepilogo

La configurazione predefinita USB (con nome file **ciscortr.cfg** da un'unità flash USB) consente agli amministratori di rete di distribuire VPN per router Spoke di uffici remoti (ma non solo VPN) senza la necessità di accedere al dispositivo dalla postazione remota.

Informazioni correlate

- Protocollo SCEP (Simple Certificate Enrollment Protocol)
- Installazione zero-touch tramite USB
- DMVPN/FlexVPN/VPN da sito a sito
- Documentazione e supporto tecnico – Cisco Systems
- Tecnologia di ancoraggio Cisco