

COME CONFIGURARE I PROTOCOLLI DI RETE SUI DISPOSITIVI

Descrizione:

Questo documento intende guidarvi nella configurazione di un apparato Hikvision, mostrando le funzioni che usano servizi internet per eventualmente disabilitarle qualora non siano necessarie.

La configurazione dei parametri di Gateway e Server DNS possono dare la possibilità, a livello fisico, di utilizzare il router per uscire dalla rete locale e accedere a servizi esterni.

La sicurezza del dispositivo è progettata per garantire che tutti i componenti principali abbiano un alto profilo di sicurezza, di base ci sono dei servizi interni programmabili (SSH, SNMP, UPnP) e altri invece volutamente non presenti (Telnet).

Altri servizi esterni come **NTP** (Network Time Protocol) e **Hik-connect** (cloud Hikvision), sono servizi che comunicheranno con l'esterno. Tramite degli applicativi sniffer connessi alla rete è possibile analizzare tutto il traffico di rete.

Attenzione: gli sniffer intercettano tutto il traffico sia remoto che locale, come broadcast, e le normali e numerosissime comunicazioni che sono alla base del protocollo TCP/IP.

Test sui Dispositivi

Nei dispositivi (Telecamere, DVR, NVR) sono stati configurati soltanto i parametri di rete come Indirizzo IP, Gateway, Server DNS e in tutte le prove effettuate **NON** si riscontrano richieste verso indirizzi IP pubblici esterni con i servizi disabilitati.

E' stata collegata la telecamera ad uno switch di rete (configurato con una porta in *mirroring*) e ad un NVR. Analizzando il traffico di rete tramite sniffer si riscontrano attività generate esclusivamente da comunicazioni interne tra i due dispositivi.

Di seguito vengono descritti i significati dei servizi esterni sopra citati e il tipo di comunicazione inviata:

1. NTP (Regolazione Data/Ora)

Qualora venga impostata nella modalità "**NTP**" (Network Time Protocol), l'apparato cerca l'omonimo servizio NTP all'indirizzo IP o FQDN indicato nel campo "**Indirizzo Server**".

NOTA: nel campo "**Indirizzo Server**", può essere impostato un indirizzo di rete LAN interna, ad esempio l'IP di un server locale, oppure un indirizzo IP pubblico su internet come riportato nella tabella seguente:

NTP SERVER	INDIRIZZO IP PUBBLICO
ntp1.inrim.it	193.204.114.232
ntp2.inrim.it	193.204.114.233
time.inrim.it	193.204.114.105

Di seguito è riportato l'esempio di configurazione di un NTP esterno, con la porta di default 123 (liberamente configurabile) utilizzata dal servizio e l'intervallo di aggiornamento dell'ora:

The screenshot shows the Hikvision configuration web interface. The 'Configurazione' (Configuration) tab is selected. Under 'Impostazioni sistema' (System Settings), the 'Impostazioni ora' (Time Settings) section is active. The 'Fuso orario' (Time Zone) is set to '(GMT+01:00) Amsterdam, Berlin, Rome, Paris'. The 'NTP' section is expanded, showing the following settings: 'Indirizzo Server' (Server Address) is 193.204.114.232, 'Porta NTP' (NTP Port) is 123, and 'Intervallo' (Interval) is 1 minute. A 'Sincr.ora manuale' (Manual Sync Time) button is visible at the bottom of the NTP settings box.

Di seguito è indicata la stringa visualizzabile da uno sniffer che mostra il traffico verso l'esterno.

Ricordiamo che la scelta del server NTP, che sia in rete locale, o in Italia, o in Europa è a discrezione di chi si occupa della configurazione del sistema di videosorveglianza. Di conseguenza il traffico generato sarà verso il server NTP scelto in fase di configurazione.

3996	31.170694	192.168.10.26	193.204.114.232	NTP	90 NTP Version 4, client
4001	31.186705	193.204.114.232	192.168.10.26	NTP	90 NTP Version 4, server

Attraverso un sito web di geo localizzazione, è possibile risalire alla posizione del server che gestisce il servizio. (<https://www.iplocation.com>).

2. CLOUD

La funzionalità Cloud è necessaria per poter utilizzare il dispositivo da remoto attraverso l'app Hik-Connect (per utilizzatori finali), e della piattaforma di manutenzione Hik-ProConnect (dedicata agli installatori).

Attivando la funzione "Accesso piattaforma" e impostando la voce "Hik-connect", i dispositivi eseguono dei tentativi di chiamata verso il server "*litedev.eu.hik-connect.com*":

System (Sistema)
Rete
Impost. di base
Imp. Avanzate
Video e audio
Immagine
Evento
Memorizzazione
Rilevazione veicolo
VCA

Vista live Playback Immagine Applicazione **Configurazione**

SNMP Email **Accesso piattaforma** Servizio di rete 802.1x Altro Protocollo di integrazione Scorrevolezza flusso Log Server Configuration

Modalità accesso piattaforma... **Hik-Connect**

☒ Abilita

Indirizzo Server ☐ Personalizza

Registra stato **Online**

Codifica flusso/Chiave di ...

Lunghezza consentita da 6 a 12 caratteri, comprendenti lettere maiuscole, minuscole e numeri. Per garantire la sicurezza del dispositivo, si consiglia una combinazione di 6 caratteri "ABCDEF" e altre simili combinazioni in ordine alfabetico di caratteri maiuscoli e minuscoli non sono ammesse.

Salva

La funzione, ad alta sicurezza, prevede di conoscere la password di accesso al dispositivo, obbligatoriamente impostata in fase di installazione, e un'ulteriore Chiave di cifratura, scelta anch'essa in fase di installazione, per garantire la comunicazione criptata e protetta. Solamente l'app utente, configurata opportunamente con quella stessa chiave di cifratura, avrà accesso ad immagini e dati cifrati verso la app Hik-connect.

Il SERVER nel quale risiede il servizio Cloud, non è identificato con un solo indirizzo IP bensì è gestito da diversi data center ridondati dislocati in Europa.

Negli esempi riportati, la connessione al server ***litedev.hik-connect.com*** avviene raggiungendo 2 indirizzi IP diversi: 52.49.136.209 e 99.80.155.28.

5723 67.373350	192.168.10.26	8.8.8.8	DNS	83 Standard query 0x66ea A litedev.hik-connect.com
5724 67.385315	192.168.10.26	99.80.155.28	TCP	66 46706 → 8666 [SYN] Seq=0 Win=14000 Len=0 MSS=1400 SACK_PERM=1 WS=128
5725 67.385316	8.8.8.8	192.168.10.26	DNS	215 Standard query response 0x66ea A litedev.hik-connect.com CNAME litedev.eu.hik-connect.com
5742 67.421160	99.80.155.28	192.168.10.26	TCP	66 8666 → 46706 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1460 SACK_PERM=1 WS=512
5743 67.421703	192.168.10.26	99.80.155.28	TCP	60 46706 → 8666 [ACK] Seq=1 Ack=1 Win=14080 Len=0

Attraverso un sito web di geo localizzazione, è possibile risalire alla posizione del server che gestisce il servizio. <https://www.iplocation.com>).

Entrambi sono localizzati in Irlanda.

3. UPnP Servizio Intero Plug&Play (alternativo al servizio Cloud)

È il protocollo di negoziazione dati per la pubblicazione e visualizzazione da remoto.
Se abilitato, necessita dell'utilizzo del router.

Il protocollo UPnP permette ai dispositivi di semplificare la connessione alla WAN attraverso il router, in ambienti domestici e aziendali.

Con la funzione abilitata come da immagine seguente, non è necessario configurare la mappatura delle porte nel router.

HIKVISION®

Vista live

Playback

Immagine

Configurazione

Locale

System (Sistema)

Rete

Impost. di base

Imp. Avanzate

Video e audio

Immagine

Evento

Memorizzazione

TCP/IP

DDNS

PPPoE

Porta

NAT

Multicast

☐ Abilita UPnP™

Nome

HIKVISION DS-2CD2023G0-I - 2

Tipo Mappatura Porta

Auto

Tipo Porta	Porta Esterna	Indirizzo IP esterno	Porta interna	Stato
HTTP	80	0.0.0.0	80	Non valido
HTTPS	443	0.0.0.0	443	Non valido
RTSP	554	0.0.0.0	554	Non valido
Porta Server	8000	0.0.0.0	8000	Non valido

NOTA: è opportuno che la funzionalità UPnP sia abilitata anche nel router.
L'effettivo funzionamento dipende anche dal grado di compatibilità tra i dispositivi e il router stesso.

Di seguito mostriamo alcuni esempi di quelle che sono normali comunicazioni locali che non devono essere confuse, con traffico generato all'esternato come precedentemente descritto. Ricordiamo, che gli sniffer intercettano tutto il traffico di rete sia remoto che locale, come broadcast, e le normali e numerosissime comunicazioni che sono alla base del protocollo TCP/IP.

4. BROADCAST (comunicazione interna di livello 2)

Una telecamera IP o registratore, appena collegato si identificherà sulla rete facendo una richiesta broadcast all'indirizzo 255.255.255.255 e che rimane confinata solo sulla rete locale LAN.

No.	Time	Source	Destination	Protocol	Length	Info
282	166.064745	192.168.10.26	255.255.255.255	ADwin ...	142	

Il Simple Service Discovery Protocol (SSDP) è un protocollo di rete per l'individuazione e l'annuncio della presenza di servizi di rete locale. Nell'immagine seguente è evidenziato con l'indirizzo di rete locale (livello 2) 239.255.255.250, viene utilizzato in rete LAN affinché il dispositivo possa essere riconosciuto e per poter essere attivato e configurato dal nostro software (SADP):

5382	65.410143	192.168.10.26	239.255.255.250	UDP	60	37020 → 37020 Len=1494
5554	66.749157	192.168.10.26	239.255.255.250	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=d960) [Reassembled in #5555]
5555	66.749158	192.168.10.26	239.255.255.250	UDP	409	37020 → 37020 Len=1847