Elementi essenziali e gestione della sicurezza informatica per il settore energetico

CSP001_C_E

PRESENTAZIONE DI:
DAVIDE FERRARIS
UNIVERSITÀ DI MALAGA, SPAGNA

Ringraziamenti

- *Cofinanziato dall'Unione Europea. Le opinioni e i pareri espressi sono tuttavia esclusivamente quelli dell'autore/degli autori e non riflettono necessariamente quelli dell'Unione Europea o dell'HADEA. Né l'Unione Europea né l'autorità che ha concesso il finanziamento possono essere ritenute responsabili per essi.*
- *Accordo di progetto n. 101083594*

Argomento 5: Progettazione e implementazione di architetture sicure per i sistemi energetici

Panoramica

- Progettazione e implementazione di architetture di rete sicure per sistemi energetici sistemi
- Architettura di rete sicura nel settore energetico, compresi i sistemi SCADA, le reti intelligenti e altre risorse energetiche critiche
- Utilizzare la segmentazione della rete per isolare i sistemi critici e ridurre l'impatto degli attacchi informatici
- Configurazione di firewall e sistemi di controllo degli accessi per proteggere le reti energetiche e limitare gli accessi non autorizzati
- Implementare sistemi di rilevamento e prevenzione delle intrusioni (IDS/IPS) per monitorare e proteggere le reti
- Utilizza le VPN per un accesso remoto sicuro ai sistemi energetici e ai dati sensibili

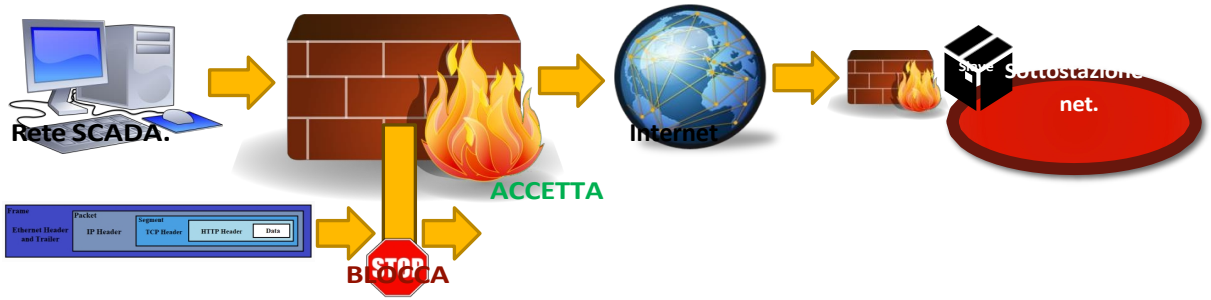
Argomento 5: Progettazione e implementazione di architetture sicure per i sistemi energetici

Panoramica

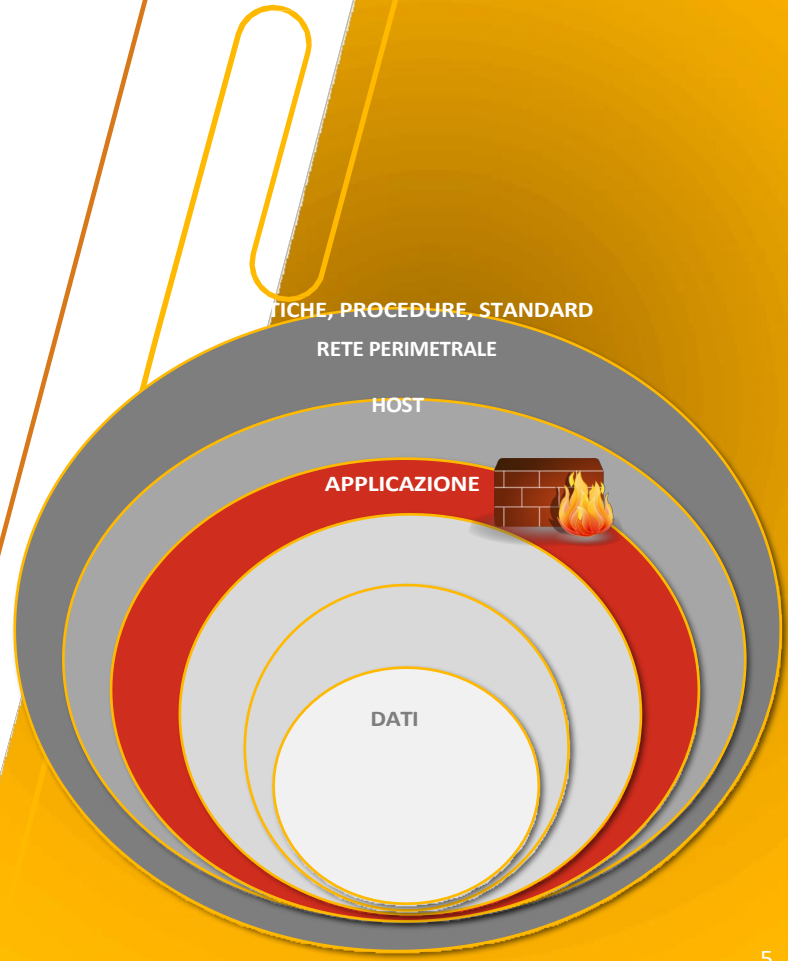
- Progettazione e implementazione di architetture di rete sicure per sistemi energetici sistemi
- Architettura di rete sicura nel settore energetico, compresi i sistemi SCADA, le reti intelligenti e altre risorse energetiche critiche
- Utilizzo della segmentazione di rete per isolare i sistemi critici e ridurre l'impatto degli attacchi informatici
- **Configurazione di firewall e sistemi di controllo degli accessi per proteggere le reti energetiche e limitare gli accessi non autorizzati**
- Implementare sistemi di rilevamento e prevenzione delle intrusioni (IDS/IPS) per monitorare e proteggere le reti
- Utilizzare VPN per garantire un accesso remoto sicuro ai sistemi energetici e ai dati sensibili

Firewall nei sistemi di controllo energetico

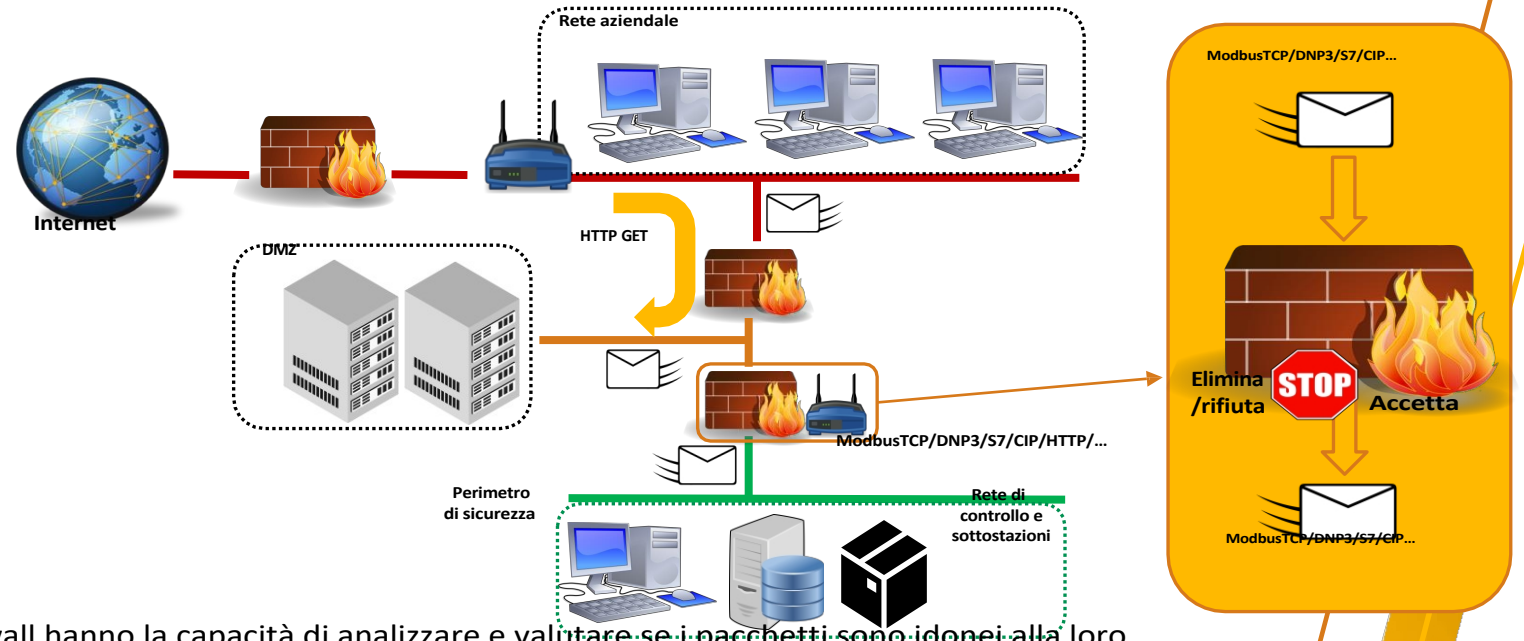
- Un firewall è un **componente HW/SW** del sistema o della rete, il cui scopo è quello di bloccare gli accessi non autorizzati, consentendo al contempo la comunicazione tra entità autorizzate
  - Ad esempio, bloccare le connessioni non autorizzate alle sottostazioni



- Nelle reti elettriche, i firewall sono uno dei principali sistemi di sicurezza elementi di sicurezza, inclusi come parte della prima "**linea di** difesa" e del perimetro di protezione della rete
  - Possono essere implementati su HMI, server SCADA, controller (se applicabile), gateway, router o switch e si basano principalmente su regole e azioni per il filtraggio dei pacchetti



Firewall nei sistemi di controllo dell'energia



- I firewall hanno la capacità di analizzare e valutare se i pacchetti sono idonei alla loro consegna finale
  - Ad esempio, se l'indirizzo IP e/o MAC è corretto, la porta è corretta, il protocollo TCP/UPD/ICMP è corretto, ecc.
- Dopo questa elaborazione, il firewall (i) decide se accettare o rifiutare il trasferimento finale del pacchetto alla destinazione e (ii) deve proteggere il perimetro di sicurezza

Quattro generazioni ed evoluzione

- Dalle loro origini negli anni '80 ad oggi, i firewall si sono evoluti fino alla quarta generazione

1ª generazione: filtraggio dei pacchetti (filtro dei pacchetti)

stateful)

(filtraggio delle applicazioni)

(NGFW)

Quattro generazioni ed evoluzione

- Dalle loro origini negli anni '80 ad oggi, i firewall si sono evoluti fino alla quarta generazione

1a generazione: Filtraggio dei pacchetti (filtro dei pacchetti)

2a generazione: firewall stateful (ispezione stateful)

3a generazione: firewall applicativi (filtraggio delle applicazioni)

Quarta generazione: firewall di nuova generazione (NGFW)

1a generazione: Filtraggio dei pacchetti

- Nel 1988 compaiono i primi sistemi di filtraggio dei pacchetti, noti come firewall "packet filtering".
- Questi sistemi si concentrano sulla fornitura di un'ispezione intensiva dei pacchetti in termini di:
  - IP, MAC, protocolli, porte
- Se c'è una corrispondenza con una delle regole, il pacchetto viene:
  - Accettato
  - Bloccato
- Le regole del firewall possono essere applicate a:
  - Traffico in entrata verso il firewall
  - Traffico in uscita dal firewall verso un'altra rete
  - Inoltro del traffico verso un altro firewall

Quattro generazioni ed evoluzione

- Dalle loro origini negli anni '80 ad oggi, i firewall si sono evoluti fino alla quarta generazione

1a generazione: Filtraggio dei pacchetti (filtro dei pacchetti)

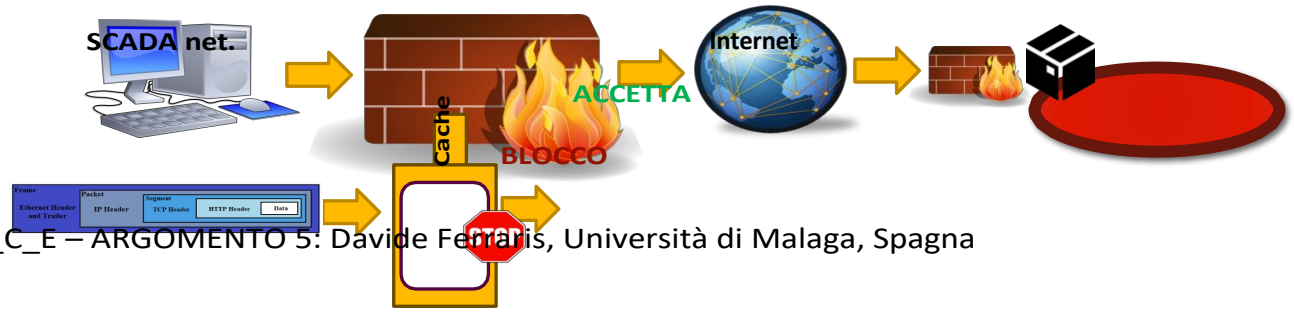
stateful)

3a generazione: firewall applicativi (filtraggio delle applicazioni)

Quarta generazione: firewall di nuova generazione (NGFW)

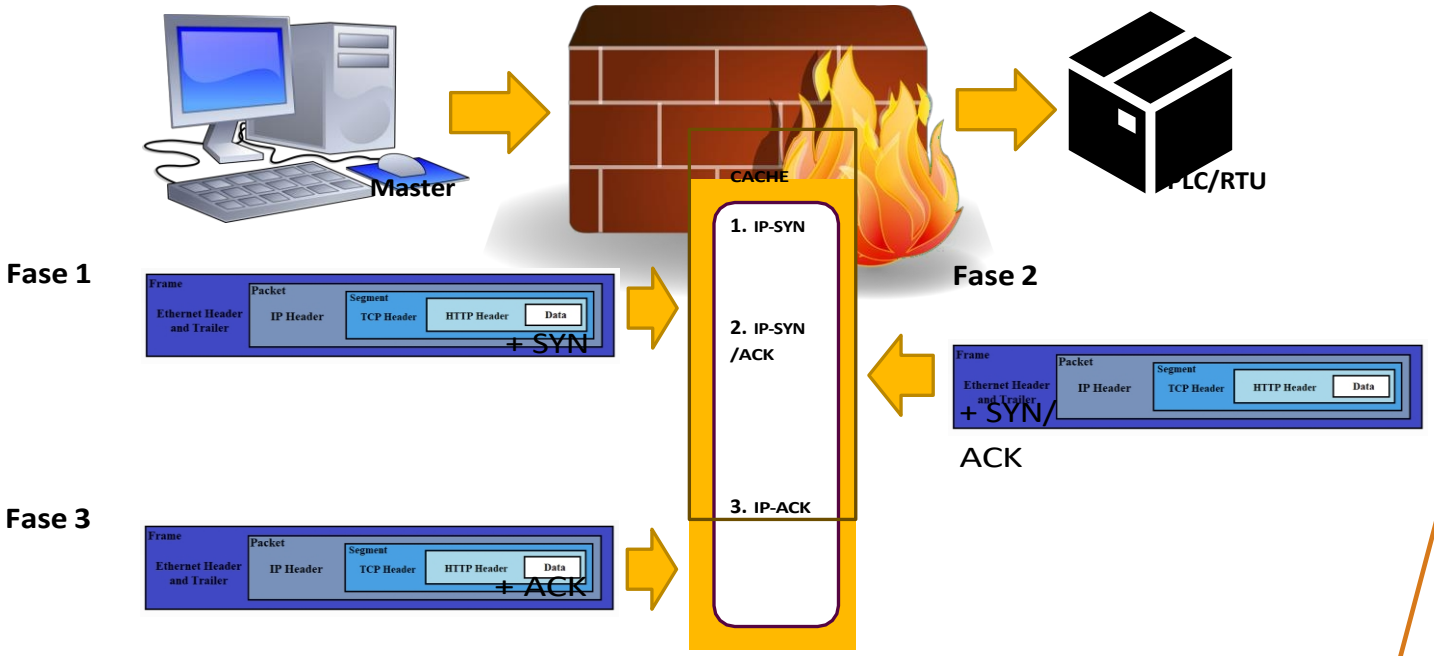
2a generazione: firewall stateful

- Questo tipo di firewall eredita le caratteristiche del sistema di filtraggio dei pacchetti, ma in aggiunta è in grado di registrare o "memorizzare" (tramite una cache interna) gli stati precedenti relativi alle connessioni ricevute (ad esempio SYN, SYN/ACK, ACK).
- Questo registro temporale consente di:
  - Accettare/rifiutare l'esistenza di nuove connessioni con stati specifici
  - Rilevare possibili abusi di una connessione esistente
  - Rilevare irregolarità nelle connessioni



Esempio della sua utilità

- Un esempio è rappresentato dalle connessioni TCP a 3 handshake, dove è necessario controllare gli stati SYN, ACK e SYN/ACK.



Quattro generazioni ed evoluzione

- Dalle loro origini negli anni '80 ad oggi, i firewall si sono evoluti fino alla quarta generazione

1ª generazione: filtraggio dei pacchetti (filtro dei pacchetti)

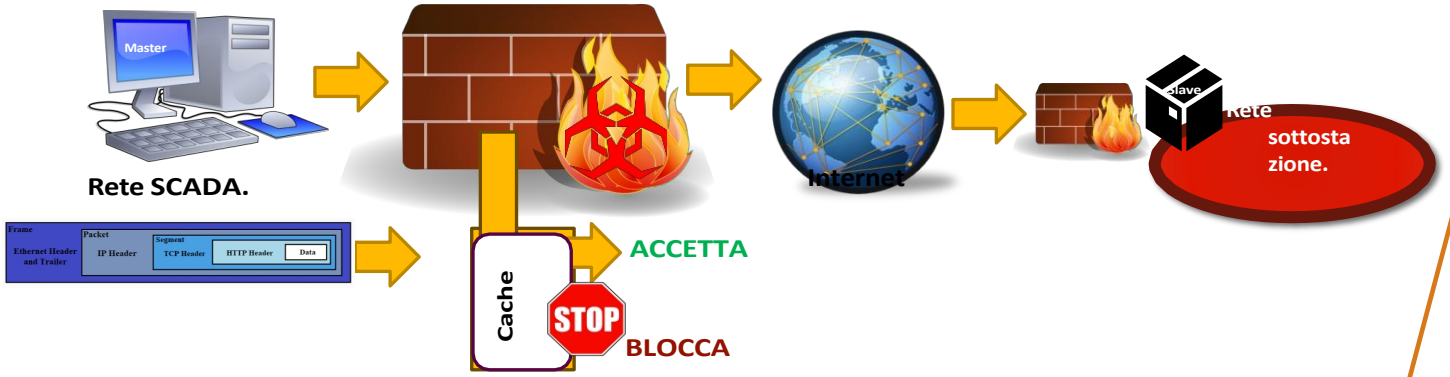
2a generazione: firewall stateful (ispezione stateful)

(filtraggio delle applicazioni)

Quarta generazione: firewall di nuova generazione (NGFW)

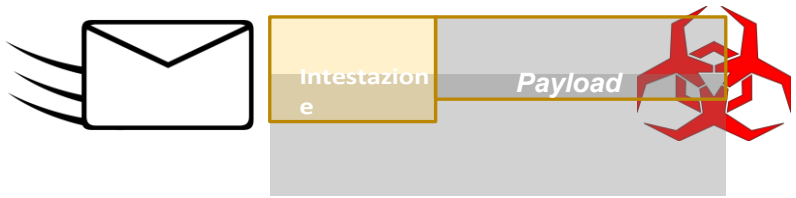
Terza generazione: firewall applicativi

- Questo tipo di firewall aggiunge nuove applicazioni a livello applicativo dello stack TCP/IP, quali:
  - "**Deep Packet Inspection**" (DPI) per rilevare irregolarità o infezioni da malware nei contenuti dei pacchetti
  - Sistemi di rilevamento e prevenzione delle intrusioni
  - anti-malware
  - VPN
  - TLS
  - ...



Deep Packet Inspection - DPI

- La DPI è una tecnica avanzata che consiste semplicemente nell'ispezionare il "contenuto" dei pacchetti di rete per rilevare modelli di attacco o condizioni irregolari nei pacchetti
  - Questa caratteristica deriva dal fatto che i firewall analizzano SOLO l'intestazione del pacchetto (IP e TCP/UDP) SENZA esaminare il payload (contenuto del messaggio o payload).
- Pertanto, la DPI mira a rilevare:
  - Formati di pacchetti irregolari
  - Pacchetti grandi/piccoli
  - Infezioni nel payload
  - ….
- Tuttavia, l'utilità del DPI è limitata
  - Analizza solo determinate condizioni del pacchetto senza esplorare in dettaglio l'esistenza di vettori o modelli di attacco



Quattro generazioni ed evoluzione

- Dalle loro origini negli anni '80 ad oggi, i firewall si sono evoluti fino alla quarta generazione

1a generazione: Filtraggio dei pacchetti (filtro dei pacchetti)

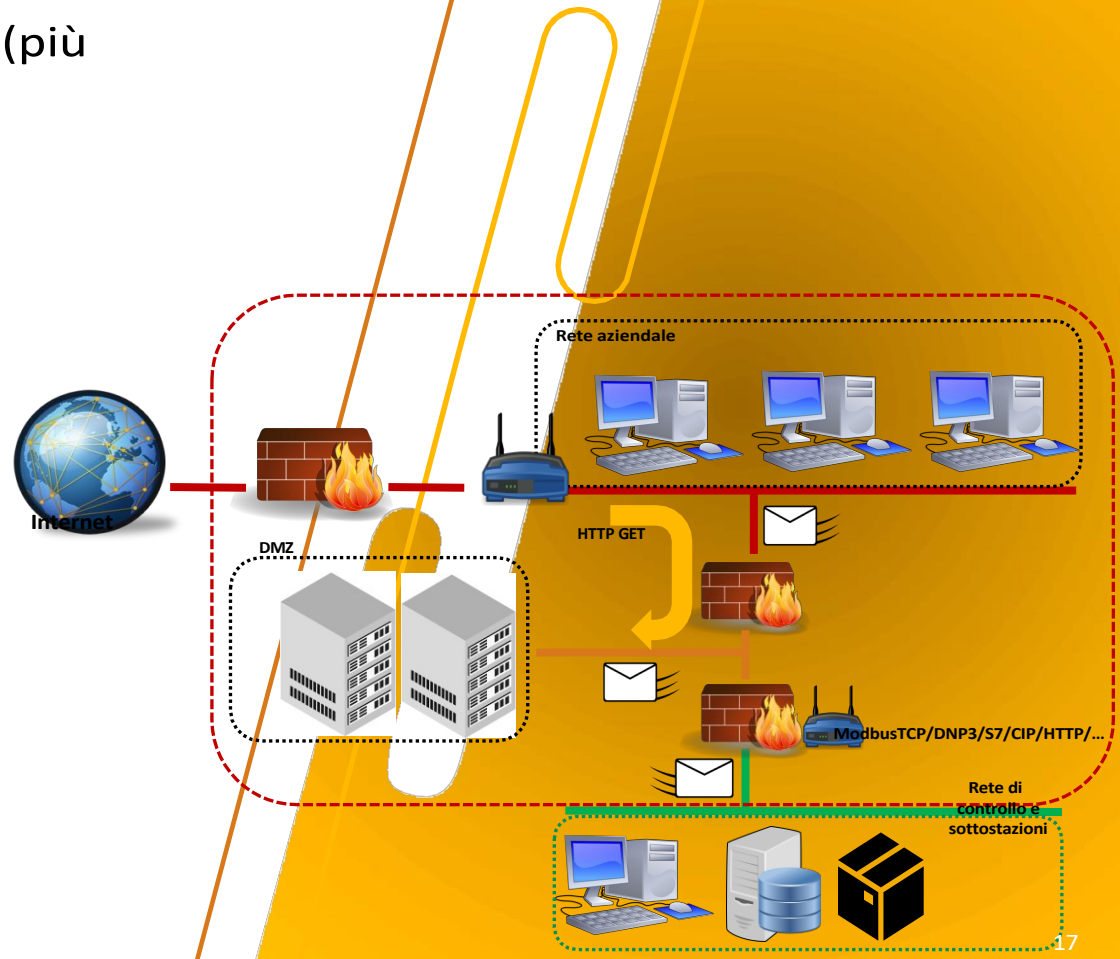
2a generazione: firewall stateful (ispezione stateful)

3a generazione: firewall applicativi (filtraggio delle applicazioni)

(NGFW)

Quarta generazione: firewall di nuova generazione

- I sistemi basati su NGFW incorporano applicazioni (più avanzate) a livello di rete aziendale, quali:
  - DPI
  - Gestione e monitoraggio di utenti e applicazioni
  - Controllo degli attacchi APT (Advanced Persistent Threat)
  - Convalida delle applicazioni
  - Isolamento dei dati
  - Protezione dei sistemi di rete nel cloud
  - Controllo e gestione da piattaforme mobili
  - ecc.

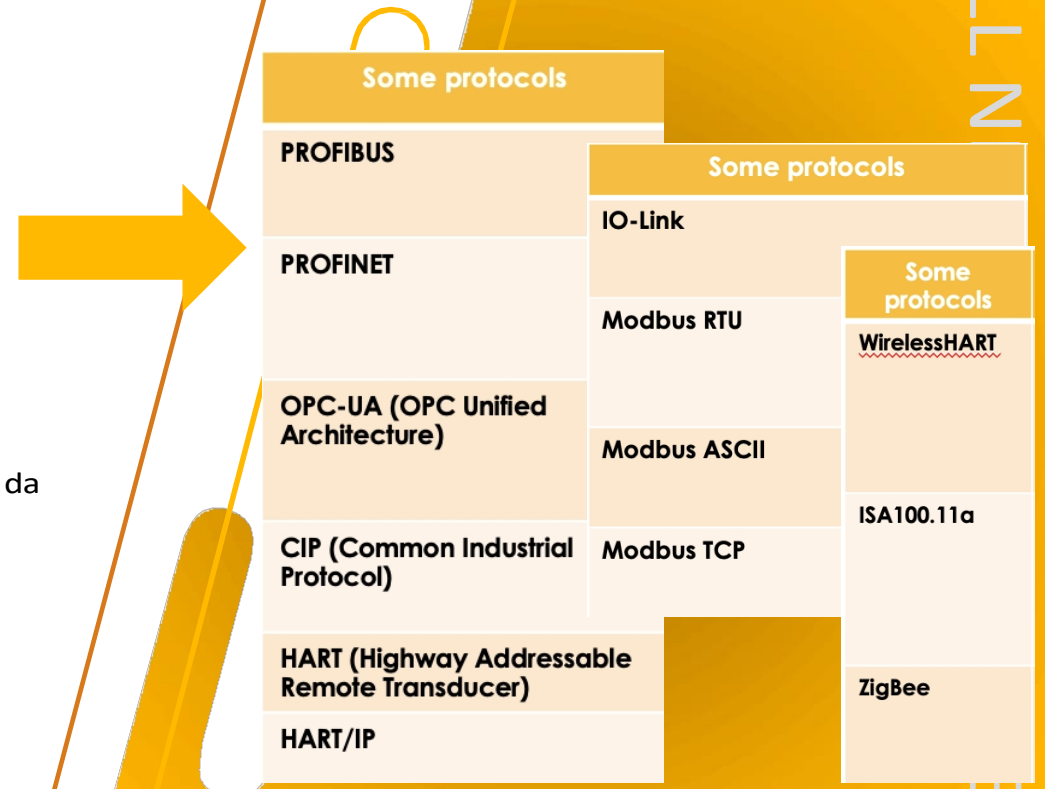


Vantaggi del suo utilizzo

- **Proteggono le reti più critiche** (ad esempio le sottostazioni) dagli attacchi provenienti da Internet, riducendo l'esposizione delle apparecchiature alle reti esterne attraverso regole di azione
- Promuovere **la segmentazione e l'isolamento** della rete
- Controllano **lo stato del traffico di rete**, generando avvisi in caso di attacchi o anomalie
- **Monitorare le attività sospette** sulla rete di destinazione analizzando i parametri di rete e le sue risorse, come processi e connessioni
  - Ad esempio, abusi di un IP specifico di una rete, abusi di determinate porte, ecc.

Svantaggi del loro utilizzo

- Le funzionalità dei firewall sono soggette a **regole predefinite** e a determinati parametri quali IP, porte o "caratteristiche del protocollo".
- Esistono **troppi protocolli di comunicazione industriale** che rendono difficile trovare un firewall unificato in grado di interpretare tutti i protocolli, come già illustrato nella sezione precedente.
- **Qualsiasi condizione non definita dalle regole può essere accettata**
  - Se una porta è aperta e non coperta da regole di filtraggio, ciò può portare ad attacchi
- Lo svantaggio precedente comporta **aggiornamenti costanti**
  - E a seconda delle dimensioni della rete, le regole del firewall possono essere noiose da mantenere
- La definizione delle **regole del firewall è fondamentale** per la sua corretta utilità
  - Le regole più restrittive dovrebbero essere definite più in basso nell'elenco
  - Le regole del firewall vengono lette come "IF-THEN" (SE-ALLORA): se la regola non viene soddisfatta, si passa alla regola successiva, mentre se viene soddisfatta, viene eseguita l'azione e il firewall viene chiuso.
- Non garantiscono protezione contro **attacchi di social engineering o infezioni**, nelle applicazioni o nei processi del sistema operativo



Firewall nelle interfacce uomo-macchina (HMI) e nei server

- Le interfacce uomo-macchina (HMI) e i server nelle sottostazioni, nelle reti di controllo e nelle reti aziendali si basano principalmente sui sistemi operativi tradizionali **Windows o Linux.**
- Inoltre, molti dei componenti industriali dipendono fortemente dipendenti dai "*sistemi operativi legacy*"
  - Secondo Trend Micro nel suo rapporto "*Securing Smart Factories: Threats to Manufacturing Environments in the Era of Industry 4.*0" (Proteggere le fabbriche intelligenti: minacce agli ambienti di produzione *nell'era dell'Industria 4.0*), si osserva la prevalenza di Windows XP (inclusa la versione a 64 bit) il cui supporto è terminato nel 2014!
    - Questa situazione è dovuta alla mentalità del "*non toccare un sistema che funziona*" e al lungo ciclo di sostituzione delle apparecchiature hardware e software nei sistemi di controllo industriale
- È essenziale seguire la visione "proibitiva" quando definire le regole del firewall
  - Soprattutto per limitare le porte HTTP, FTP o Telnet non protette

Fonte: Trend Micro, Securing Smart Factories: Threats to Manufacturing Environments in the Era of Industry 4.0, https://documents.trendmicro.com/assets/white_papers/wp-threats-to-manufacturing-environments-in-the-era-of-industry-4.pdf

Firewall in Windows 10/11

- Vai al firewall di Windows 10/11:
  - 🔎 : *Pannello di controllo Sistema e sicurezza > Windows Firewall*
    - Verrà indicato lo stato attuale del firewall Normalmente è in modalità "*Abilitato*"
    - In "Applicazioni e funzionalità consentite" è possibile aggiungere nuove applicazioni o servizi all'elenco del firewall
  - 🔎 : *Console di Windows Firewall con sicurezza avanzata*, è anche possibile definire regole o criteri di sicurezza
    - Seleziona *Regole in entrata*, quindi *Azione* e *Nuova regola*
    - Stabilire la *nuova regola in entrata* selezionare *Personalizzata,* quindi selezionare *Avanti*
    - Selezionare il *percorso del software*

Fonte: Configurare le regole con i criteri di gruppo, 2024.
https://learn.microsoft.com/en-us/windows/security/operating-system-security/network-security/windows-firewall/configure

Firewall in Linux

- Linux incorpora nella console il firewall **ufw** (uncomplicated firewall) come impostazione predefinita, eseguibile dalla riga di comando

Comandi ufw

Installare e abilitare i pacchetti ufw:
$ sudo apt install -y ufw
$ sudo systemctl enable ufw
$ sudo systemctl restart ufw
$ yes | sudo ufw enable

Imposta la localizzazione delle regole di configurazione:
$ ls /etc/ufw/applications.d/
$ sudo ufw app list

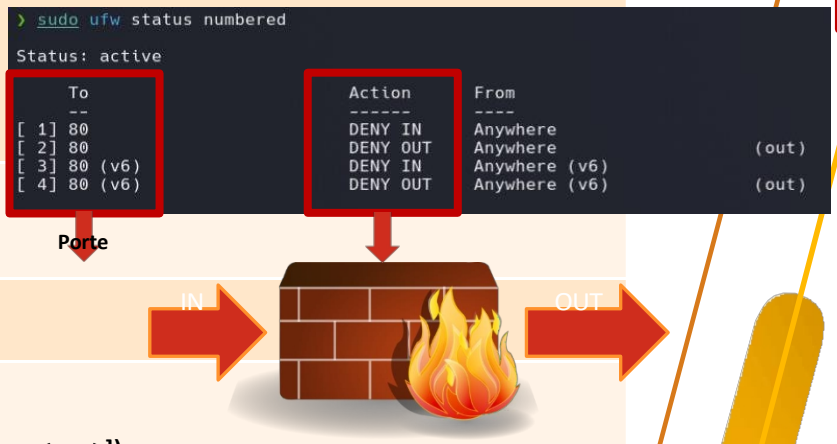
Visualizza l'elenco delle regole:
$ sudo ufw status

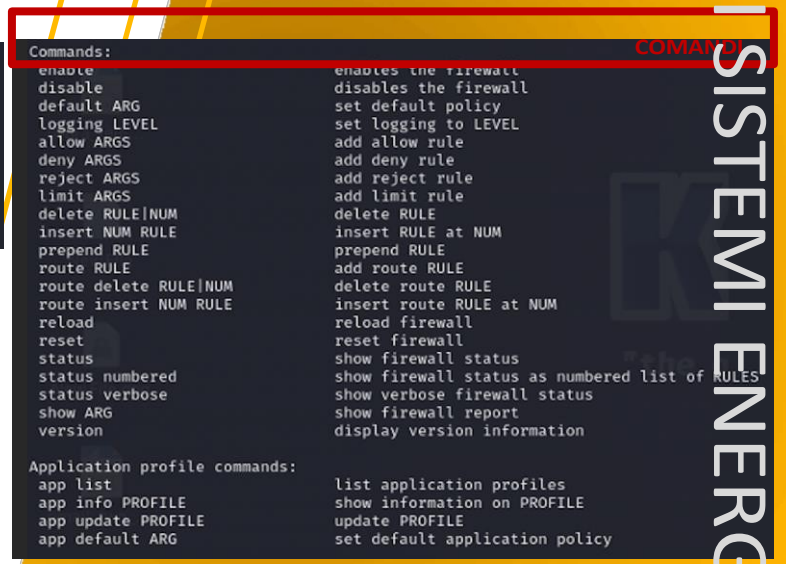
Aggiungere o eliminare regole
$ sudo ufw allow/deny ([<porta>/<protocollo>][<servizi>] [app <apps>])
$ sudo ufw delete allow/deny ([<porta>/<protocollo>][<servizi>] [app <app>])

Ricaricare le regole del firewall:
$ sudo ufw reload

Abilita o disabilita la registrazione (il log viene generato in */var/log/ufw.log*):
$ sudo ufw logging on
$ sudo ufw logging off

Reimposta le politiche del firewall:
$ sudo ufw reset



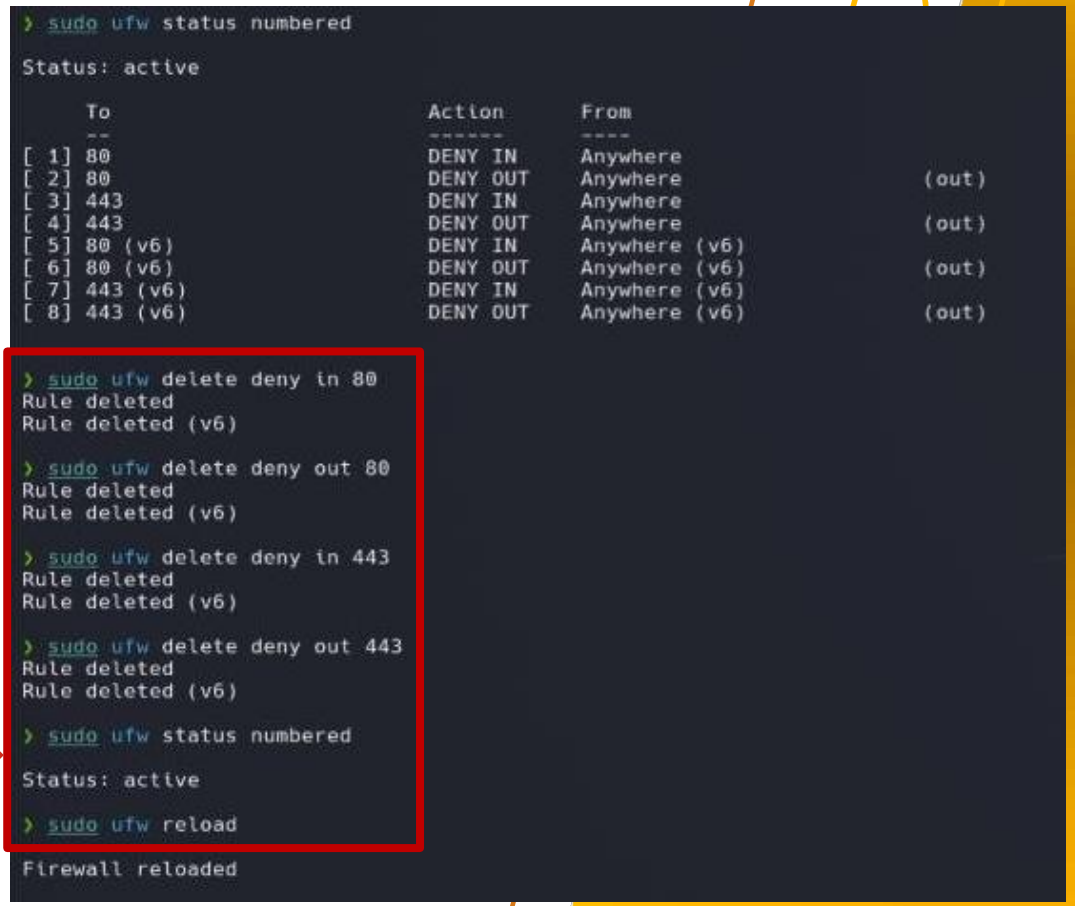


Firewall in Linux - Esempi

- Bloccare un indirizzo specifico
  - **$ sudo ufw deny from 1.1.1.1**
  - Bloccare le connessioni a un'interfaccia di rete
    - **$ sudo ufw deny in on eth0 from 15.15.15.51**
- Consentire un tipo di connessione e un servizio
  - **$ sudo ufw allow ssh**
  - **$ sudo ufw allow 22**
    - Consenti connessioni in entrata da IP/sottorete
      - **$ sudo ufw allow from 1.1.1.0/24 to any port 22**
- Consenti traffico HTTP e HTTPS in entrata
  - **$ sudo ufw allow http // sudo ufw allow 80**
  - **$ sudo ufw allow https // sudo ufw allow 443**
  - **$ sudo ufw allow proto tcp da qualsiasi indirizzo a qualsiasi indirizzo porta 80,443**
- Consenti il traffico da un IP/sottorete a una porta specifica
  - **$ sudo ufw allow da 1.1.1.0/24 a qualsiasi porta 3306**

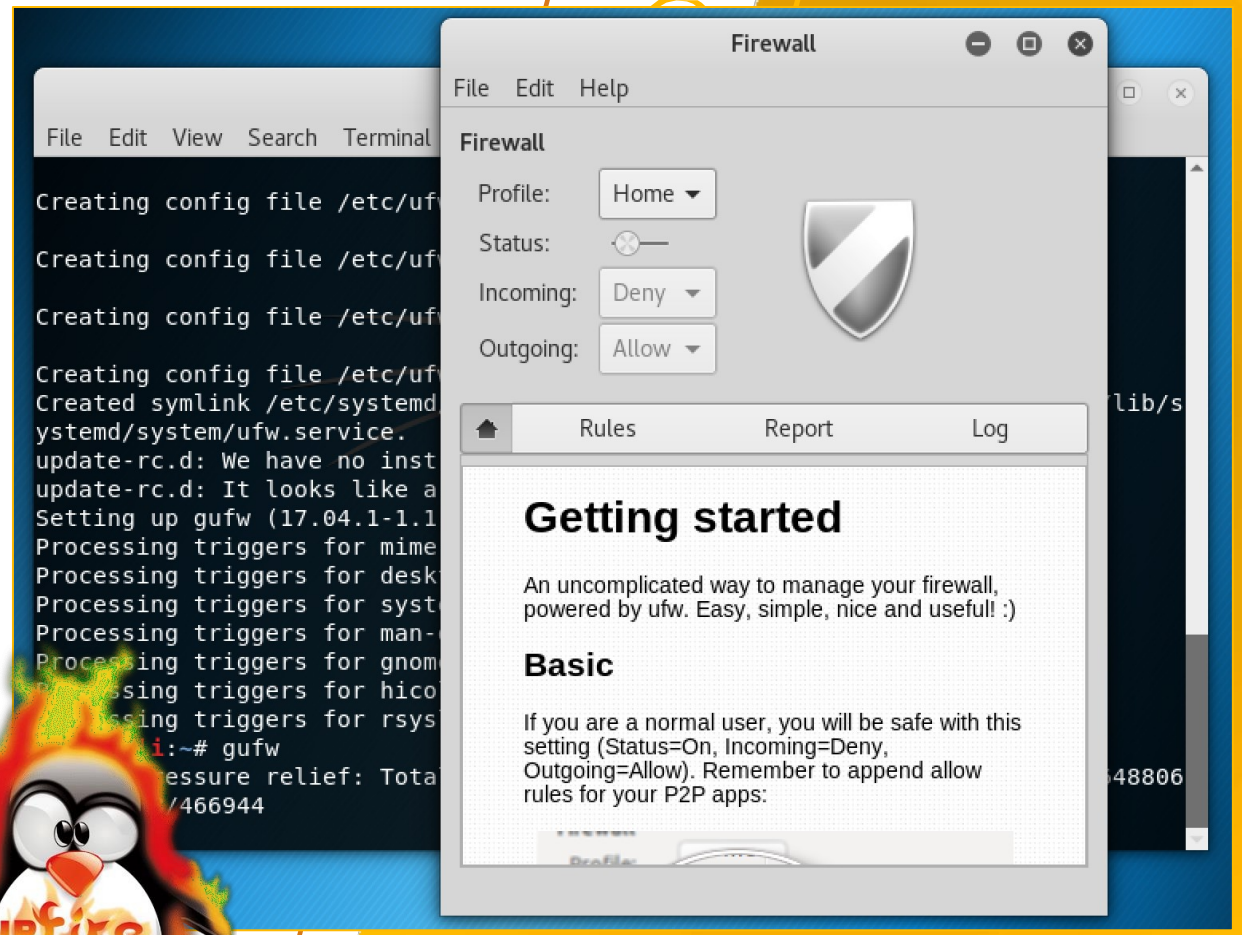
Firewall in Linux - Esempi

- Negare una porta o un servizio in entrata
  - **$ sudo ufw deny 25/tcp**
  - **$ sudo ufw deny 143/tcp**
  - **$ sudo ufw deny 993/tcp**
  - **$ sudo ufw deny 110/tcp**
  - **$ sudo ufw deny 995/tcp**
- Negare una porta o un servizio in uscita
  - **$ sudo ufw deny out 25/tcp**
  - **$ sudo ufw deny out 143/tcp**
- Negare una porta o un servizio in uscita
  - **$ sudo ufw deny out 25/tcp**
  - **$ sudo ufw deny out 143/tcp**
- Rimuovere una politica specifica
  - **$ sudo ufw delete deny in 443**
  - **$ sudo ufw status numbered**
  - **$ sudo ufw reload**



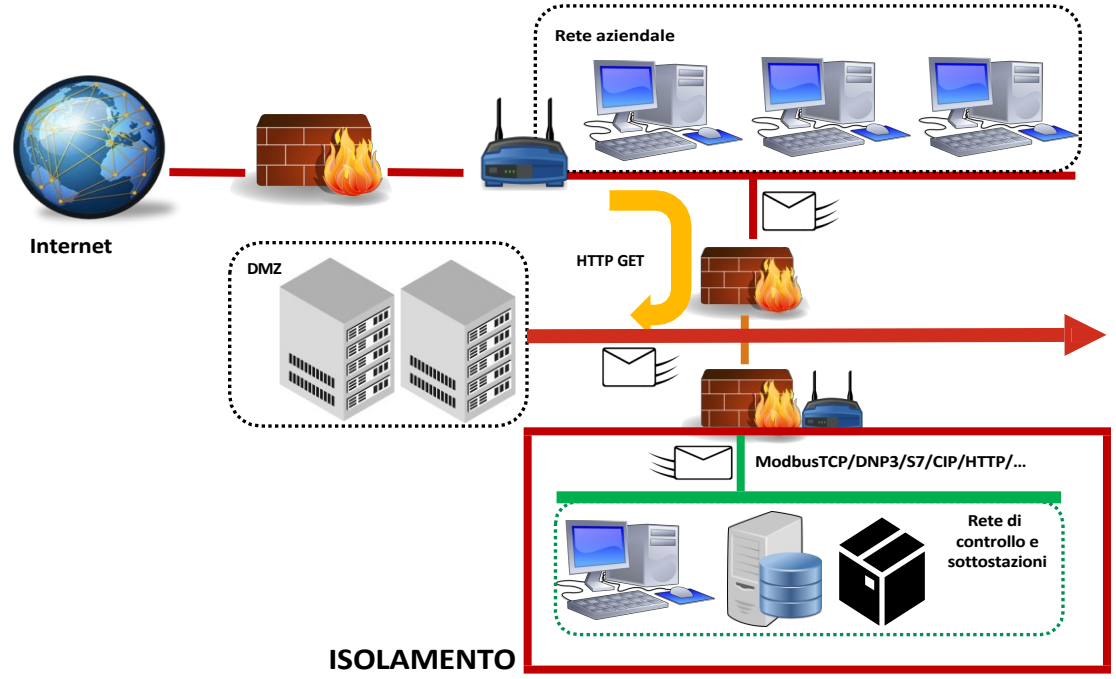
Firewall in Linux

- In Linux è anche possibile utilizzare l'interfaccia grafica ufw, nota come **gufw**
  - Installare l'interfaccia grafica ufw:
    - **$ sudo apt install –y gufw**
  - Esegui la GUI dall'interfaccia a riga di comando (CLI):
    - **$ sudo gufw**
- Tuttavia, esistono molti altri firewall per Linux, come ad esempio:
  - IPfire
  - Smoothwall
  - IPCop
  - CSF,
  - …



DMZ nei sistemi di controllo energetico

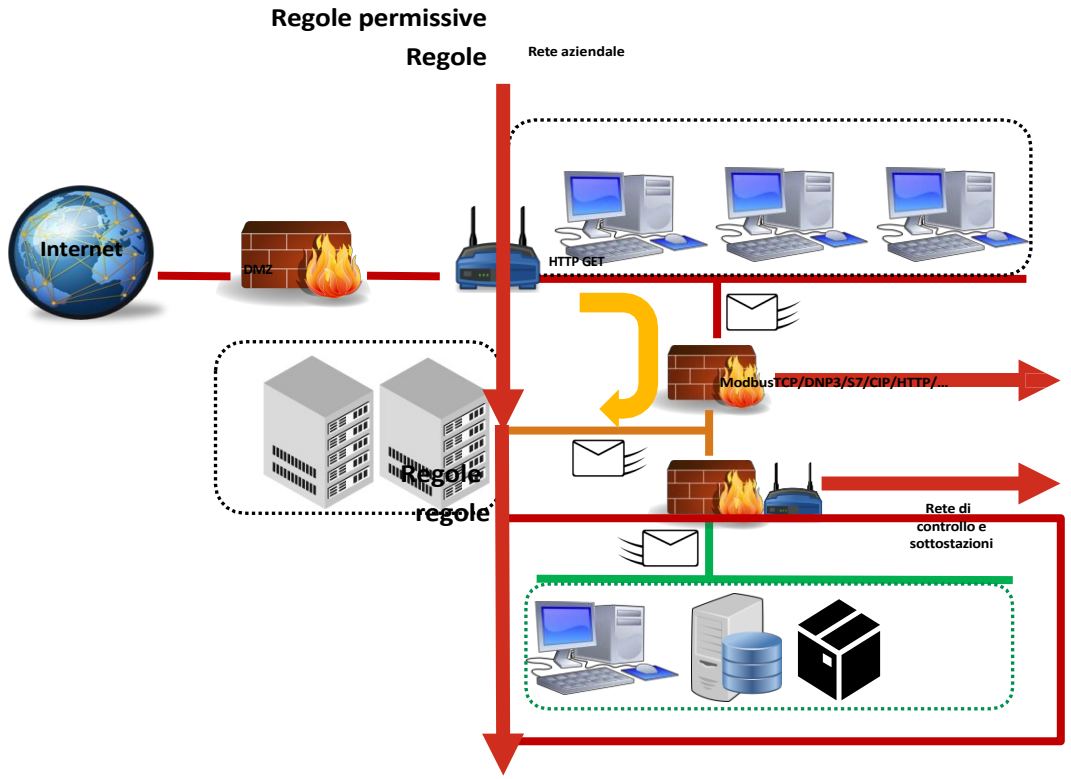
- Attraverso le regole del firewall è possibile isolare le reti di controllo dalle query ai server di database e dalle reti esterne
  - Questa prevenzione avviene attraverso zone demilitarizzate (DMZ)



Poiché queste zone fanno parte della rete aziendale, è necessario "isolare" la rete di controllo da (i) Internet e da (ii) la DMZ per evitare possibili penetrazioni esterne dalla DMZ

DMZ nei sistemi di controllo energetico

- Attraverso le regole del firewall è possibile isolare le reti di controllo dalle query ai server di database e dalle reti esterne
  - Questa prevenzione avviene attraverso zone demilitarizzate (DMZ)



Pertanto, le regole specifiche della DMZ dovrebbero essere:

- **Permissive**: se le connessioni provengono da Internet alla rete DMZ o dalla DMZ a Internet
- **Proibitive**: se le connessioni provengono dalla DMZ alla rete intranet dell'organizzazione

Controllo degli accessi nelle reti energetiche

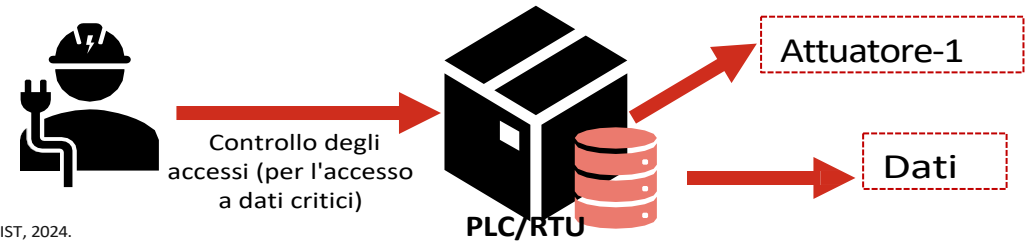
- L'Agenzia dell'Unione europea per la sicurezza informatica (ENISA) nel documento "***Misure di sicurezza adeguate per le reti intelligenti***" sottolinea l'importanza del controllo degli accessi come misura prioritaria per la sicurezza dei sistemi informativi e delle loro risorse, quali:
  - HMI (compresi i dispositivi mobili), sistemi operativi e applicazioni
  - Workstation e server, come i server SCADA
  - Controller, sensori, attuatori
  - Database e file
  - Infrastrutture o sistemi di rete (ad esempio, cloud-edge, IIoT, gemelli digitali, blockchain, ...)
  - Modelli di intelligenza artificiale, modelli digitali, gemelli digitali
  - Ecc.
- Le misure identificate dall'ENISA si basano sulle norme ISO/IEC-27002 – ISO/IEC TR 27019 e NISTIR-7628 per le reti intelligenti.
  - Risultato della misura: "**Controllo logico degli accessi**" (SM 9.3)
  - Questo è definito come "*Il fornitore dovrebbe applicare l'accesso logico alle entità autorizzate sui sistemi informativi delle reti intelligenti e sui* perimetri *di sicurezza*".

ID	SM 9.3
Measure	Logical access control.
Definition	The provider should enforce logical access to authorized entities on smart grid information systems and security perimeters.
Example	[From NERC CIP-003-4 - Requirement 5. Access Control] The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information. [From IEC 62443 - 4.3.3.7.2 Establish appropriate logical and physical permission methods to access IACS devices] The permission to access industrial automation and control system devices shall be logical (rules that grant or deny access to known users based on their roles).

Fonte: ENISA, "Misure di sicurezza adeguate per le reti intelligenti. Linee guida per valutare la sofisticatezza dell'attuazione delle misure di sicurezza", 2012.
URL: https://www.enisa.europa.eu/publications/appropriate-security-measures-for-smart-grids

Controllo degli accessi nelle reti energetiche

- Per comprendere il concetto **di "controllo degli accessi"**, il National Istituto Nazionale di Standard e Tecnologia (NIST) lo definisce come segue:
  - "*Il processo di* ***autorizzazione o limitazione dell'accesso*** *alle applicazioni* ***a livello granulare****, ad esempio per utente, per gruppo e per risorsa*".
- Il processo prevede due ulteriori azioni:
  - **Autenticazione**: "*Verifica dell'identità di un utente, processo o dispositivo, spesso come prerequisito per consentire l'accesso alle risorse in un* sistema".
  - **Autorizzazione**: "*Privilegi di accesso concessi a un utente, un programma o un processo o l'atto di concedere tali* privilegi".
- Ciò significa anche che gli operatori/utenti umani devono prima dimostrare la propria identità e poi verificare i propri permessi per ottenere l'accesso alle risorse richieste



Fonte: CSRC, "Glossario", NIST, 2024.
URL: https://csrc.nist.gov/glossary

Ad esempio, utilizzando credenziali di sicurezza quali nome utente/password, PIN, smart card, certificati digitali, ecc.

Si noti che l'autenticazione sarà descritta in dettaglio nel prossimo argomento, mentre qui ci occuperemo solo della parte relativa all'autorizzazione.

CONTROLLO DEGLI ACCESSI NEI SISTEMI ENERGETICI

Autorizzazione nelle reti energetiche

- Per garantire il "controllo degli accessi", l'ENISA aggiunge anche nella SM 9.3 alcune raccomandazioni:

Alcune raccomandazioni relative all'autorizzazione (locale e remota)	A tal fine, è necessario:
• **I metodi consentiti di controllo degli accessi** sono identificati e documentati • Il sistema informativo della rete intelligente **applica le autorizzazioni assegnate per controllare l'accesso** al sistema informativo della rete intelligente **in conformità con la politica definita dall'organizzazione** • Agli account utente **vengono concessi i diritti e i privilegi più restrittivi o l'accesso** necessario per l'esecuzione di compiti specifici	• Identificare **il tipo di autenticazione e lo schema di autorizzazione** • Disporre dell'elenco degli **utenti e dei relativi diritti di accesso**
• **Le funzioni principali** del sistema **sono separate** tramite autorizzazioni di accesso assegnate • **Le funzioni di sicurezza sono limitate** al numero minimo di utenti necessario per garantire la sicurezza dell'ambiente	• Elenco degli **utenti autorizzati che possono accedere alle funzioni di sicurezza**

Fonte: ENISA, "Misure di sicurezza adeguate per le reti intelligenti. Linee guida per valutare la sofisticatezza dell'attuazione delle misure di sicurezza", 2012.
URL: https://www.enisa.europa.eu/publications/appropriate-security-measures-for-smart-grids

Autorizzazione nelle reti energetiche

- Per garantire il "controllo degli accessi", l'ENISA aggiunge anche nella SM 9.3 alcune raccomandazioni:

Alcune raccomandazioni relative all'autorizzazione (locale e remota)	Per farlo, è necessario:
• **I metodi consentiti di controllo degli accessi** siano identificati e documentati • Il sistema informativo della rete intelligente **applica le autorizzazioni assegnate per controllare l'accesso** al sistema informativo della rete intelligente **in conformità con la politica definita dall'organizzazione** • Agli account utente **vengono concessi i diritti e i privilegi più restrittivi o l'accesso** necessario per l'esecuzione di compiti specifici	• Identificare **il tipo di autenticazione e lo schema di autorizzazione** • Disporre dell'elenco degli **utenti e dei relativi diritti di accesso**
• **Le funzioni principali** del sistema **sono separate** tramite autorizzazioni di accesso assegnate • **Le funzioni di sicurezza sono limitate** al numero minimo di utenti necessario per garantire la sicurezza dell'ambiente	• Elenco degli **utenti autorizzati che possono accedere alle funzioni di sicurezza**

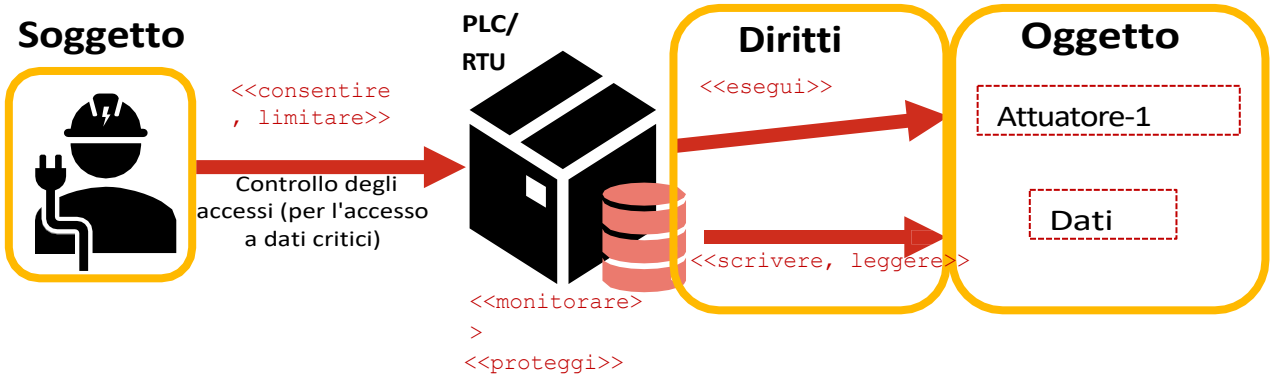
- Pertanto, è necessario identificare gli utenti, gli oggetti da proteggere, i metodi e i diritti di accesso all'oggetto

CHI – COSA – COME

Fonte: ENISA, "Misure di sicurezza adeguate per le reti intelligenti. Linee guida per valutare la sofisticatezza dell'attuazione delle misure di sicurezza", 2012.
URL: https://www.enisa.europa.eu/publications/appropriate-security-measures-for-smart-grids

Autorizzazione nelle reti energetiche

- Infatti, quando si definisce una politica di controllo degli accessi, sono necessari **metodi o meccanismi** per implementare la conformità a quei criteri di sicurezza che:
  - Consentono, limitano
  - Monitorano, proteggono
- Gli elementi fondamentali di un meccanismo di controllo degli accessi sono:
  - **Oggetto**: risorsa a cui è controllato l'accesso, ad esempio PLC/RTU
  - **Soggetto**: entità che potenzialmente accede agli oggetti - Operatore
  - **Diritto di accesso**: descrive il modo in cui il soggetto può accedere all'oggetto: lettura, scrittura, esecuzione, cancellazione, creazione, ...



Meccanismi di autorizzazione tipici

- I meccanismi di controllo degli accessi si dividono principalmente in diverse categorie:

DAC (Controllo discrezionale degli accessi)	MAC (Controllo obbligatorio degli accessi)	RBAC (Controllo degli accessi basato sui ruoli)	ABAC (Controllo degli accessi basato sugli attributi)
Basato **sull'identità del richiedente e sulle regole di accesso** (che indicano quali richiedenti sono autorizzati o meno a compiere determinate azioni)	Basato sul confronto tra **le etichette di sicurezza** (che indicano la criticità delle risorse) **e** le **autorizzazioni** di sicurezza (che indicano quali entità sono autorizzate ad accedere a determinate risorse)	Basato sul **ruolo che ciascun utente ha** all'interno del sistema **e sulle regole** che indicano quali accessi sono consentiti a coloro che hanno un determinato ruolo	Basato sugli **attributi associati all'utente** e, a seconda dell'attributo, l'accesso a un sistema è consentito o meno

Meccanismi di autorizzazione tipici

- I meccanismi di controllo degli accessi si dividono principalmente in diverse categorie:

DAC (Controllo discrezionale degli accessi)	MAC (Controllo obbligatorio degli accessi)	RBAC (Controllo degli accessi basato sui ruoli)	ABAC (Controllo degli accessi basato sugli attributi)
Basato **sull'identità del richiedente e sulle regole di accesso** (che indicano quali richiedenti sono autorizzati o meno a compiere determinate azioni)	Basato sul confronto tra **le etichette di sicurezza** (che indicano la criticità delle risorse) **e** le **autorizzazioni** di sicurezza (che indicano quali entità sono autorizzate ad accedere a determinate risorse)	In base al **ruolo che ciascun utente ha** all'interno del sistema **e alle regole** che stabiliscono quali accessi sono consentiti a coloro che hanno un determinato ruolo	in base **agli attributi associati all'utente** e, a seconda dell'attributo, l'accesso a un sistema è consentito o meno

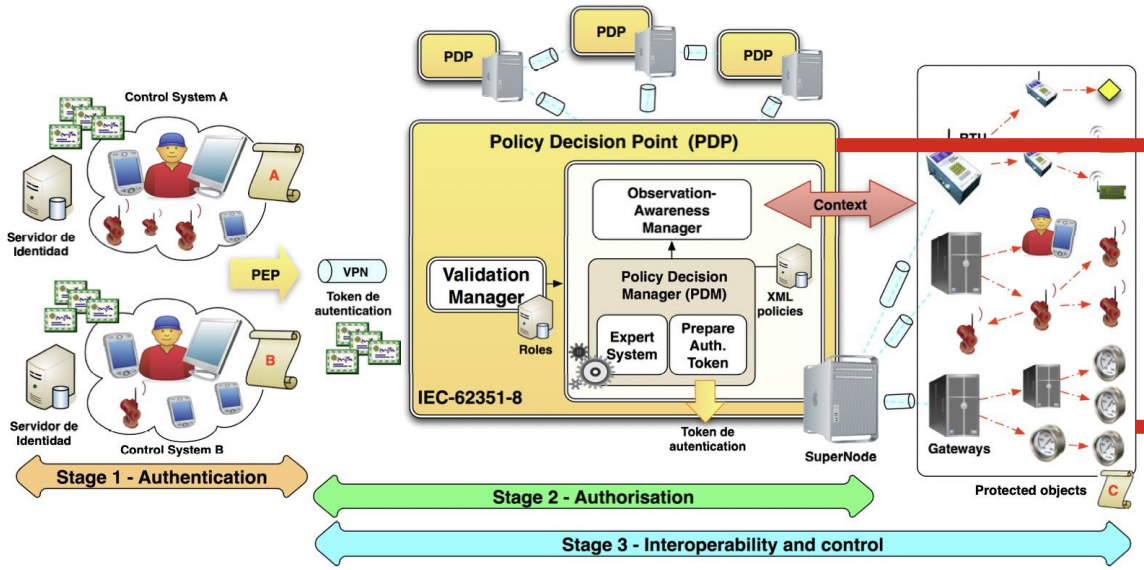
- Queste politiche non si escludono a vicenda
  - DAC + MAC; DAC + RBAC + ABAC; RBAC + ABAC; DAC + MAC + RBAC + ABAC ...
- Data la natura critica dei sistemi di controllo energetico, è importante anche conservare i registri degli accessi effettuati
  - Questo processo favorirà **la tracciabilità e la verifica** in caso di accesso indesiderato alle risorse

RESPONSABILITÀ

Tracciabilità dei dati➔ auditing

Esempio (I) di un'architettura di controllo degli accessi per ambienti Smart Grid

- Nel lavoro di C. Alcaraz *et al.*, un'architettura di controllo degli accessi che utilizza una serie di termini quali "punto di applicazione delle politiche di controllo degli accessi
  - **Punto di applicazione delle politiche (PEP)** in cui viene applicata la politica
  - **Punto di decisione della politica (PDP)** in cui vengono implementati i meccanismi di cui sopra come RBAC (ruoli estratti dalla norma IEC 62351-8)
    + ABAC (stati contestuali delle sottostazioni)



IEC 62351

	Rights associated with IEC-62351-8 roles										
Roles	View	Read	Dataset	Reporting	Fileread	Filewrite	Filemgnt	Control	Config	Settinggroup	Security
Viewer[a]	✓			✓							
Operator[b]	✓	✓		✓				✓			
Engineer[c]	✓	✓	✓	✓		✓	✓		✓		
Installer[d]	✓	✓		✓		✓			✓		
SECADM[e]	✓	✓	✓			✓	✓	✓	✓	✓	✓
SECAUD[f]	✓	✓		✓	✓						
RBACMNT[g]	✓	✓					✓		✓	✓	

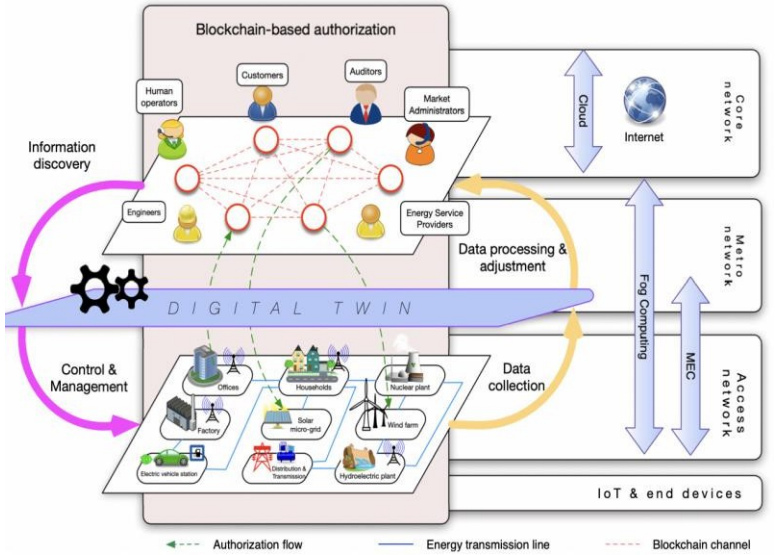
A seconda dello stato di ciascuna sottostazione, determinati utenti con determinati ruoli e autorizzazioni potranno accedere

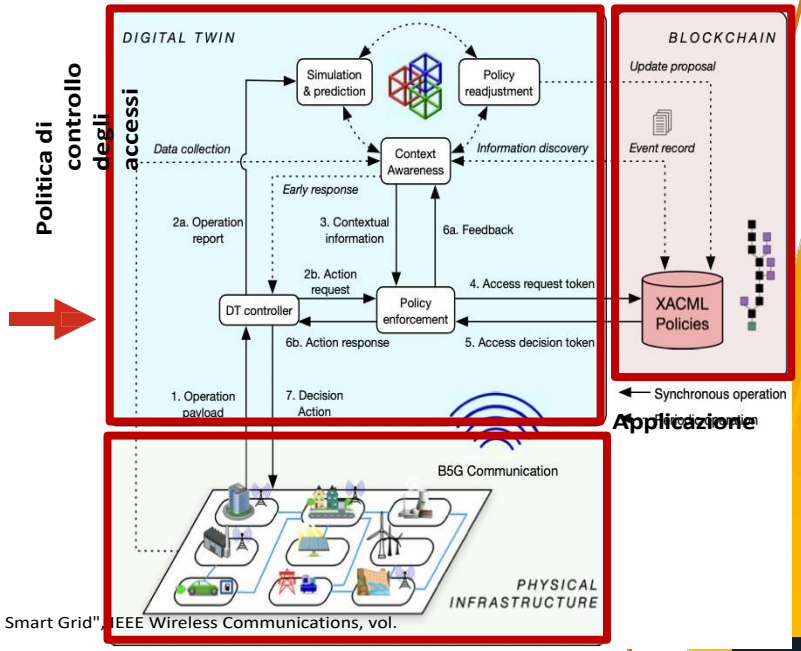
Ad esempio, nelle sottostazioni completamente colpite da un attacco, solo gli operatori o i tecnici potranno accedere, al fine di mitigare l'effetto e riportare il sistema a uno stato stabile

Fonte: C. Alcaraz, J. Lopez e S. Wolthusen, "Policy Enforcement System for Secure Interoperable Control in Distributed Smart Grid Systems", Journal of Network and Computer Applications, vol. 59, pp. 301314, 2016.

Esempio (II) di un'architettura di controllo degli accessi per ambienti Smart Grid

- Nel lavoro *di* J. Lopez *et al.*, un'altra architettura di controllo degli accessi, le cui politiche sono aggiornate dai gemelli digitali:
  - Simulazione: prevedere la migliore politica da applicare sulla base di RBAC+ABAC
  - Blockchain: conservare i registri relativi agli attributi dell'utente e al contesto
  - 5G/6G + Cloud-edge: facilitare l'applicazione delle politiche in tempo reale





Responsabilità

- Abusi da parte di utenti malintenzionati o negligenti
- Stati contestuali di sottostazioni, micro-reti e DER

Fonte: J. Lopez, J. E. Rubio e C. Alcaraz, "Digital Twins for Intelligent Authorization in the B5G-enabled Smart Grid", IEEE Wireless Communications, vol. 28, pagg. 48-55, 2021.

Considerazioni finali

- I sistemi energetici e le loro infrastrutture di controllo dovrebbero basarsi sui ben noti **firewall**
  - È stato quindi introdotto il concetto della tecnologia e la sua evoluzione attraverso le sue quattro generazioni
  - Inoltre, sono stati evidenziati sia i vantaggi che gli svantaggi per i sistemi di controllo, sottolineando la difficoltà di gestire più protocolli di comunicazione industriali
  - Infine, sono stati introdotti i firewall dei sistemi operativi, nonché il concetto di DMZ, molto utile per quegli ambienti aziendali che rendono pubblico l'accesso ai server locali, come server web, database, repository, ecc.
- Ma, oltre a ciò, è necessario considerare **i modelli di controllo degli accessi** esistenti:
  - Esistono molti meccanismi tradizionali che possono essere applicati (DAC, MAC, RBAC, ABAC), ma anche modi per combinarli con le nuove tecnologie
  - Attraverso le nuove tecnologie (digital twins, blockchain, 5G/6G e cloud-fog-edge), potremmo arricchire le potenziali caratteristiche delle politiche di controllo degli accessi e le loro funzioni principali
- Infine, ma non meno importante, è sempre consigliabile tenere conto delle raccomandazioni fornite dagli standard e dalle linee guida esistenti

Riferimenti e fonti

1. T. Piens, K. Wens, Mastering Palo Alto Networks, Creazione, configurazione e implementazione di soluzioni di rete per la vostra infrastruttura utilizzando le funzionalità di PAN-OS, 2022
2. Trend Micro, Protezione delle fabbriche intelligenti: minacce agli ambienti di produzione nell'era dell'Industria 4.0, URL: https://documents.trendmicro.com/assets/white_papers/wp-threats-to-manufacturing-environments-in-the-era-of-industry-4.pdf
3. Configurare le regole con i criteri di gruppo, 2024. URL: https://learn.microsoft.com/en-us/windows/security/operating-system-security/network-security/windows-firewall/configure
4. Archlinux, "Uncomplicated Firewall", 2024 URL: https://wiki.archlinux.org/title/Uncomplicated_Firewall
5. Microsoft, Attiva Windows Defender Firewall, URL: https://learn.microsoft.com/en-us/mem/intune/user-help/you-need-to-enable-defender-firewall-windows
6. ENISA, "Misure di sicurezza adeguate per le reti intelligenti. Linee guida per valutare la sofisticatezza dell'implementazione delle misure di sicurezza", 2012. URL:https://www.enisa.europa.eu/publications/appropriate-security-measures-for-smart-grids

Riferimenti e fonti

7. DeepL Translator per la revisione. URL: https://www.deepl.com/translator
8. CSRC, "Glossario", NIST, 2024. URL:https://csrc.nist.gov/glossary
9. Fonte: J. Lopez, J. E. Rubio e C. Alcaraz, "Digital Twins for Intelligent Authorization in the B5G-enabled Smart Grid", IEEE Wireless Communications, vol. 28, pagg. 48-55, 2021
10. C. Alcaraz, J. Lopez e S. Wolthusen, "Policy Enforcement System for Secure Interoperable Control in Distributed Smart Grid Systems", Journal of Network and Computer Applications, vol. 59, pagg. 301314, 2016

Connettiti con CyberSecPro: come registrarsi e altre informazioni pratiche

1. Sito web: www.cybersecpro-project.eu
2. X (Twitter): https://twitter.com/CyberSecPro_eu
3. LinkedIn: https://www.linkedin.com/company/cybersecpro-euproject/

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.

Project Agreement no. 101083594

Grazie

Per qualsiasi domanda, non esitate a esitare a contattare:

- Davide Ferraris
  Professore supplente
  Università di Malaga
  ferraris@uma.es