

Progettazione e sviluppo di una rete sicura:

La tua sicurezza, la nostra priorità.



Programma della presentazione

Argomenti principali di discussione

01	02	03	04	05	06
Presentazione del progetto di rete e componenti.	Analisi dei sistemi di sicurezza.	Rappresentazione del progetto.	Difesa dei sistemi critici.	Criticità e limiti della rete.	Honeypot. 02

Come si sviluppa la rete:

1 - Sistemi di rete e switch

Il progetto di rete si sviluppa su 6 piani di un edificio, ognuno dei quali presenta una ventina di sistemi per l'utilizzo da parte dei dipendenti collegati ad uno switch presente in ogni piano del suddetto, a loro volta, questi ultimi, sono connessi ad un router centrale.

2 - Router-Firewall IDS/IPS

Il router selezionato implementa al suo interno una tecnologia Firewall, ed è collegato ad una DMZ di cui sono facenti parte un WEB server ed un NAS per lo storage dei dati da parte dei dipendenti.

3 - Web server e Firewall hardware

Il server WEB è situato all'interno della rete, ed è responsabile di garantire l'accesso ai clienti a tutte le funzioni di e-commerce dell'azienda ed è all'interno di una DMZ delimitata da un unico Firewall diretto.

Sistemi Firewall implementati:



Difesa WEB - NAS

A difesa del Web server e del NAS, parti essenziali per lo svolgimento delle attività lavorative dell'azienda, abbiamo pensato di installare un Firewall IDS/IPS con funzione di Reverse-Proxy, per la protezione specifica del Web server, si utilizzerà una WAF, che offre un'elevata protezione a livello http/https, mentre per il NAS, si utilizzerà un sistema HIDS, ottimale per il monitoraggio e il controllo dell'integrità di file critici all'interno dello storage.



Sistema Software Snort

Per la gestione della sicurezza della rete interna, si è optato per un sistema di sicurezza Firewall open-source, il quale implementa tecnologia IDS e IPS per un miglior controllo e tempo di reazione in caso venga rivelato un potenziale rischio.



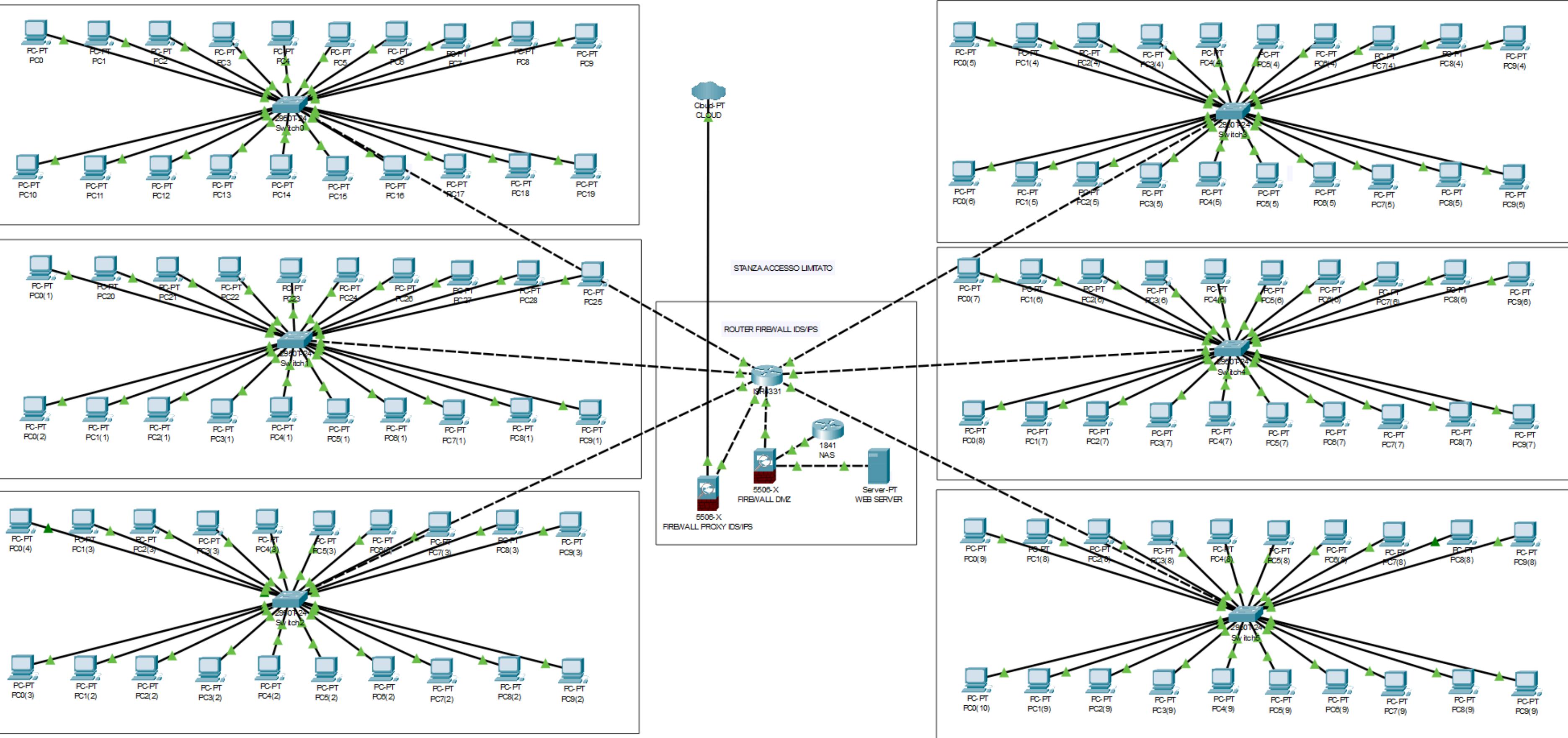
Router con Firewall incorporato

Per una migliore gestione di tutto il traffico al interno dell'azienda, si è pensato di implementare un router che abbia installato un sistema Firewall per la scansione e gestione, tramite tabelle di memoria, dei vari collegamenti.



Firewall perimetrale con funzione proxy

Per una maggiore protezione di tutta la rete interna, si è proceduto nel inserire un Firewall esterno alla rete con funzione di protezione perimetrale che implementi un sistema di proxy verso l'esterno, proteggendo i vari componenti interni da potenziali minacce.



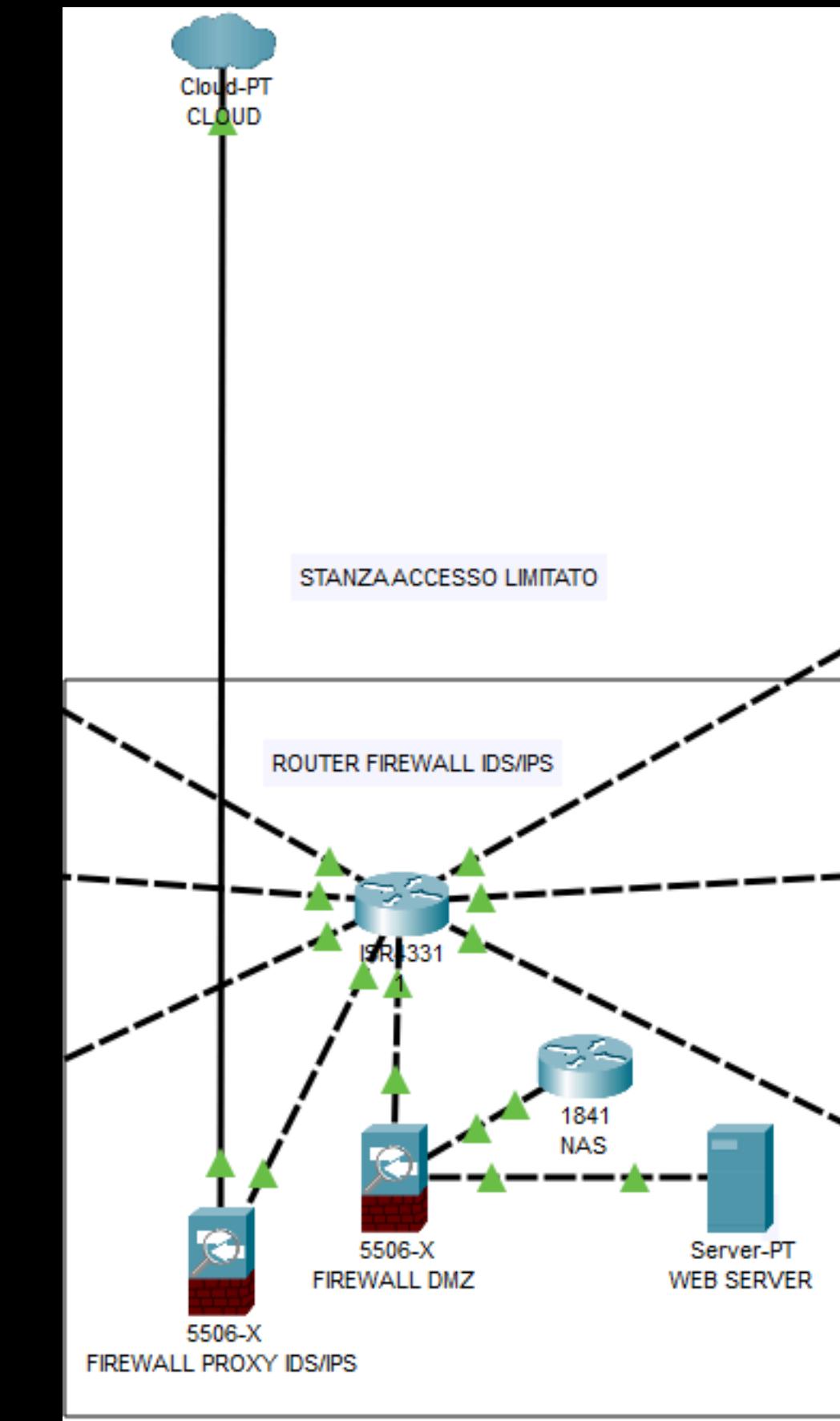
Specifiche progettuali sul posizionamento dei sistemi critici:

Stanza ad accesso limitato

Per un'ulteriore protezione da agenti interni, fisici, si è suggerito di realizzare una stanza sigillata con un accesso limitato all'ultimo piano dell'edificio, allo scopo di impedire la manomissione e/o qualsiasi intaccamento ai componenti essenziali per lo svolgimento delle attività lavorative.

Componenti presenti

- Router centrale
- NAS
- WEB server e relativo Firewall
- Firewall perimetrale



Criticità e limiti della rete:

Il progetto è stato sviluppato seguendo le istruzioni e le richieste dell'azienda cliente, ci sono però dei punti che vorremmo sottolineare riguardanti una migliore organizzazione di quest'ultima.

Sistemi di ridondanza

Sarebbe opportuno utilizzare eventuali sistemi di ridondanza, la ridondanza consiste nell'implementare duplicati di componenti critici, come server o dischi rigidi, per assicurare che un guasto hardware non comprometta la continuità operativa.

Stanza ad accesso limitato

- Videocamera di sorveglianza
- Controllo degli accessi
- Sistemi di allarme
- Sistemi di Backup dei dati

VLAN

E' inoltre consigliabile, per una maggiore sicurezza d'accesso ai dati, di realizzare delle sottoreti VLAN ad alto livello di amministrazione, allo scopo di limitare l'accesso a dati sensibili a dipendenti non autorizzati o che potrebbero facilmente compromettere l'integrità dei dati.

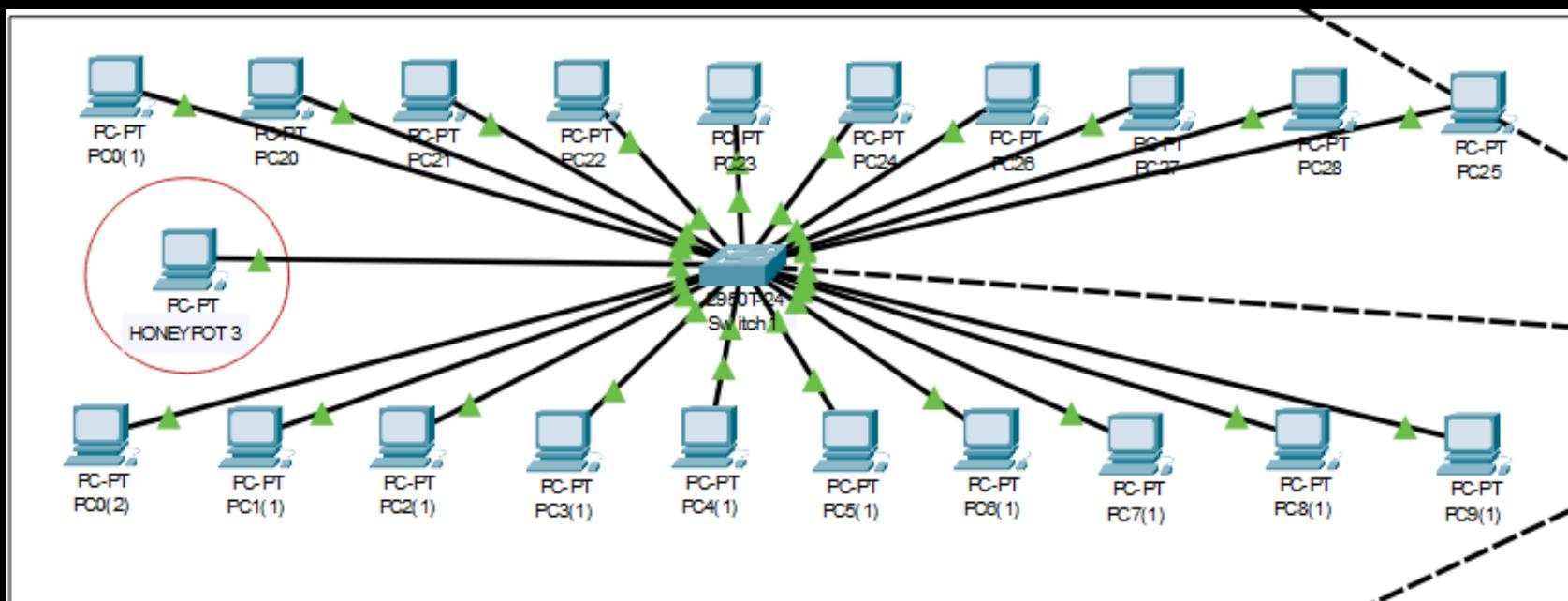


Installazione di sistema Honeypot:

A seguito della richiesta di implementazione di Honeypot, si è pensato alle seguenti soluzioni:

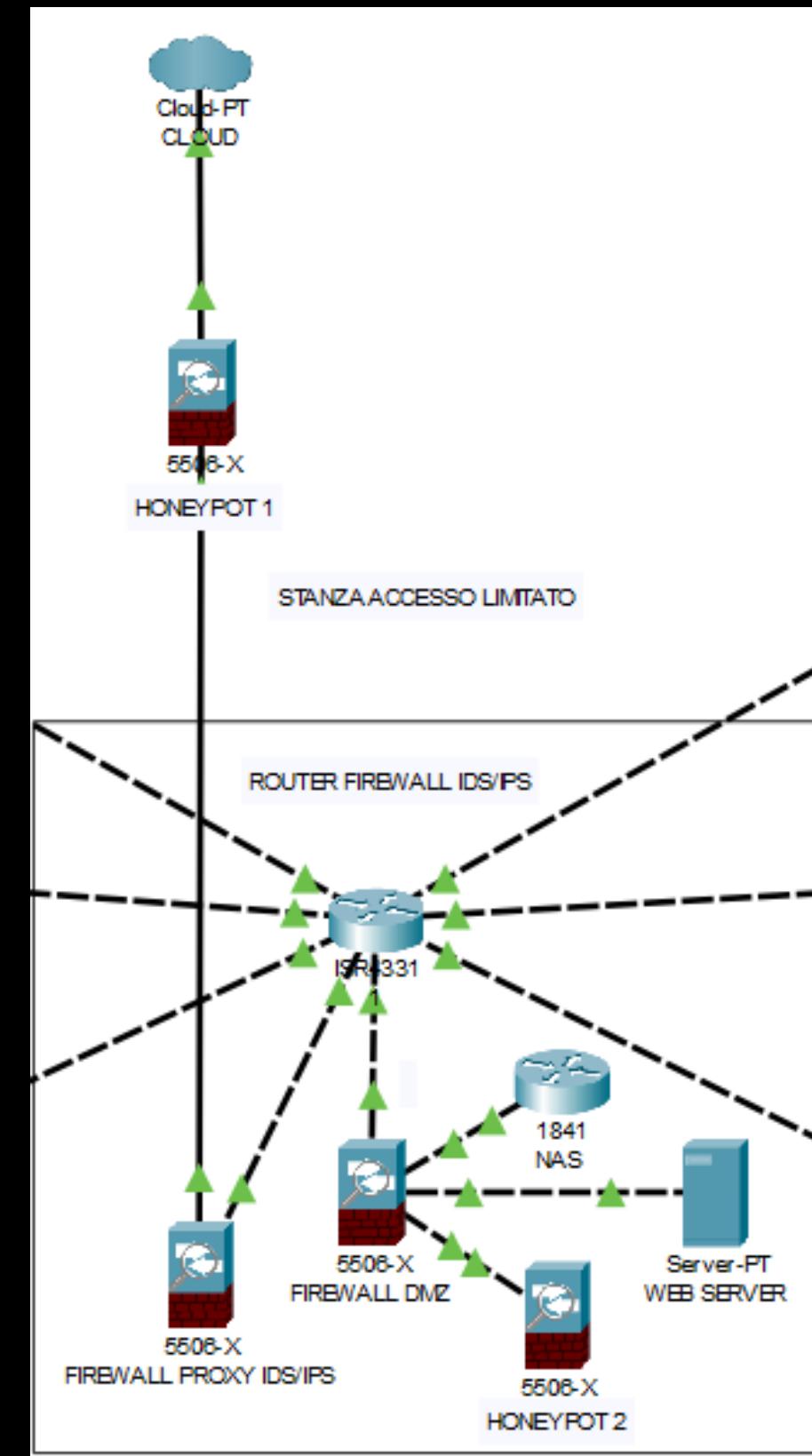
Honeypot pc

In caso di attacco alla rete di pc aziendali, si è pensato di inserire degli Honeypot collegato ad ogni switch, così da poter simulare al meglio una finta criticità interna ad una rete ben protetta.



Honeypot perimetrale - server

Installare un Honeypot perimetrale che finga di essere un Firewall vulnerabile e facilmente penetrabile all'interno della nostra rete, quest'ultimo avrà lo scopo di riconoscere il file malevolo e, in caso di attacco al Web server, indirizzarlo verso un Honeypot che lo simuli, che in realtà archivierà i dati dell'attacco.





Grazie per aver scelto PanterPwners!

Per qualsiasi domanda
non esitare a contattarci.

