

Progettazione e Sicurezza dell'Infrastruttura di Rete per Theta

Una presentazione sulle strategie avanzate per la sicurezza e la progettazione delle infrastrutture di rete aziendali

CERBERUS

CRIPTAZIONE DAW



CRIPTAZIONE DAW



Introduzione al Progetto di Rete per Theta

Introduzione al Progetto di Rete per Theta

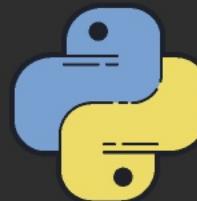
Questa presentazione illustra il progetto di rete eseguito da CERBERUS S.P.A. per il cliente Theta, coprendo gli aspetti fondamentali della progettazione, le misure di sicurezza implementate e le raccomandazioni finali per un miglioramento continuo.





CERBERUS

Chi Siamo



**CERTIFICATI
DA**



Partner Strategico per le Infrastrutture di Rete

CERBERUS S.P.A. è specializzata nella progettazione, implementazione e gestione di infrastrutture di rete sicure e scalabili, offrendo soluzioni integrate per aziende e enti pubblici.

Un Team di Esperti Coordinatori

Il nostro team è composto da professionisti esperti, guidati dal CEO Samuele Barba e comprendente figure chiave come Tegege Fael (CISO), Lorenzo Mantoni (CTO), Cosimo Chincoli (COO), Antonio Gangale (CFO) e Emanuele Di Leva (Responsabile Vendite e Marketing).

Partner Strategico per le Infrastrutture di Rete

CERBERUS S.P.A. è specializzata nella progettazione, implementazione e gestione di infrastrutture di rete sicure e scalabili, offrendo soluzioni integrate per aziende e enti pubblici.

Un Team di Esperti Coordinatori

Il nostro team è composto da professionisti esperti, guidati dal CEO Samuele Barba e comprendente figure chiave come Tegege Fael (CISO), Lorenzo Mantoni (CTO), Cosimo Chincoli (COO), Antonio Gangale (CFO) e Emanuele Di Leva (Responsabile Vendite e Marketing).

La Nostra Missione: I Tre Pilastri di CERBERUS

La missione di CERBERUS S.P.A. è fondamentale per la creazione di un'infrastruttura di rete sicura e performante. I nostri sforzi si concentrano su: 1. Proteggere le reti e i dati attraverso avanzate tecnologie di cybersecurity per difenderci da minacce interne ed esterne. 2. Connettere sedi e personale, garantendo una rete resiliente e una comunicazione fluida. 3. Controllare le prestazioni per assicurare efficienza operativa e conformità agli standard di settore.





Progettazione Logica della Rete

La progettazione della rete aziendale per Theta da parte di CERBERUS S.P.A. integra una logica di rete ben definita, comprendente sei piani e 120 host. Ogni piano è dotato di switch di layer 2 e un router centrale per garantire una connettività fluida e continua, riducendo i punti di guasto e migliorando l'affidabilità complessiva.



Sicurezza e Componenti Critici

Il progetto enfatizza la sicurezza attraverso componenti critici come un firewall perimetrale, un sistema di monitoraggio IDS/IPS e una zona demilitarizzata (DMZ) per isolare il web server. Questa architettura protegge i dati e le informazioni sensibili da attacchi esterni, garantendo al contempo prestazioni elevate e accesso centralizzato ai dati.



Architettura a Sei Piani

La progettazione logica della rete è articolata su sei piani, ognuno dei quali supporta fino a 20 host, per un totale di 120 dispositivi.

Ciascuna delle sei piani include una gestione efficace del traffico dati all'interno di ciascun piano, mentre un router centrale assicura la connettività tra le diverse aree della rete, evitando interruzioni in caso di guasti.



Performance e Scalabilità

Ogni piano è progettato per garantire performance elevate e ridondanza, permettendo il collegamento di 20 computer a uno switch dedicato.

Questa architettura facilita l'espansione futura della rete, mantenendo un equilibrio tra sicurezza e performance.



Accesso Centralizzato ai Dati

Il design logico della rete include anche un NAS collegato allo switch centrale, garantendo un accesso centralizzato ai dati per tutte le VLAN. Questo approccio centralizzato migliora l'affidabilità e la gestione del traffico di rete, ottimizzando le prestazioni complessive.



Dettagli della Progettazione Logica della Rete

Architettura a Sei Piani

La progettazione logica della rete è articolata su sei piani, ognuno dei quali supporta fino a 20 host, per un totale di 120 dispositivi connessi. Gli switch di layer 2 permettono una gestione efficace del traffico dati all'interno di ciascun piano, mentre un router centrale assicura la connettività tra le diverse aree della rete, evitando interruzioni in caso di guasti.



Performance e Scalabilità

Ogni piano è progettato per garantire performance elevate e ridondanza, permettendo il collegamento di 20 computer a uno switch dedicato. Questa architettura facilita l'espansione futura della rete, mantenendo un equilibrio tra sicurezza e performance.



Accesso Centralizzato ai Dati

Il design logico della rete include anche un NAS collegato allo switch centrale, garantendo un accesso centralizzato ai dati per tutte le VLAN. Questo approccio centralizzato migliora l'affidabilità e la gestione del traffico di rete, ottimizzando le prestazioni complessive.



Schema Logico di Rete

Un'analisi dettagliata della struttura della rete interna e dei suoi componenti chiave.

Rete Interna

La rete interna è suddivisa in sei piani, ciascuno dotato di uno switch di layer 2 per connettere 20 postazioni.

Switch Centrale

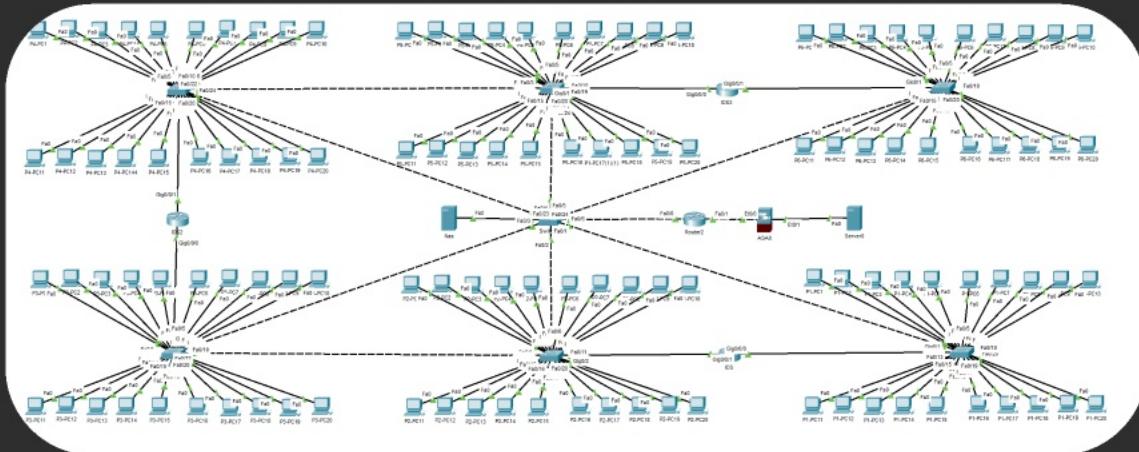
Un switch centrale collega tutti gli switch di piano e il router, garantendo la continuità della connettività in caso di guasto.

NAS

Il NAS è connesso allo switch centrale per un accesso centralizzato ai dati, migliorando l'efficienza e la velocità di comunicazione.

Schema Logico di Rete

Un'analisi dettagliata della struttura della rete interna e dei suoi componenti chiave.



Rete Interna

La rete interna è suddivisa in sei piani, ciascuno dotato di uno switch di layer 2 per connettere 20 postazioni.

Switch Centrale

Un switch centrale collega tutti gli switch di piano e il router, garantendo la continuità della connettività in caso di guasto.

NAS

Il NAS è connesso allo switch centrale per un accesso centralizzato ai dati, migliorando l'efficienza e la velocità di comunicazione.

Schema Logico di Rete

Un'analisi dettagliata della struttura della rete interna e dei suoi componenti chiave.

Rete Interna

La rete interna è suddivisa in sei piani, ciascuno dotato di uno switch di layer 2 per connettere 20 postazioni.

Switch Centrale

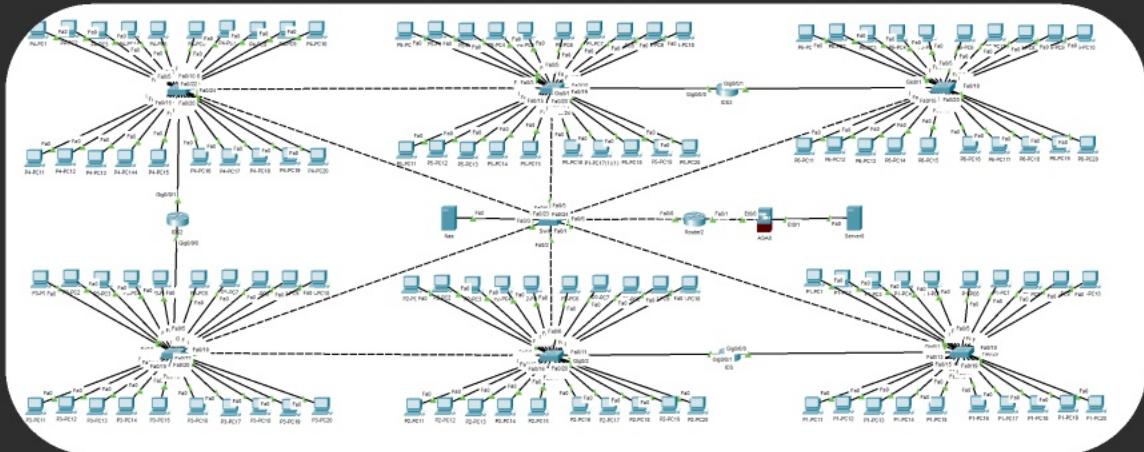
Un switch centrale collega tutti gli switch di piano e il router, garantendo la continuità della connettività in caso di guasto.

NAS

Il NAS è connesso allo switch centrale per un accesso centralizzato ai dati, migliorando l'efficienza e la velocità di comunicazione.

Schema Logico di Rete

Un'analisi dettagliata della struttura della rete interna e dei suoi componenti chiave.



Rete Interna

La rete interna è suddivisa in sei piani, ciascuno dotato di uno switch di layer 2 per connettere 20 postazioni.

Switch Centrale

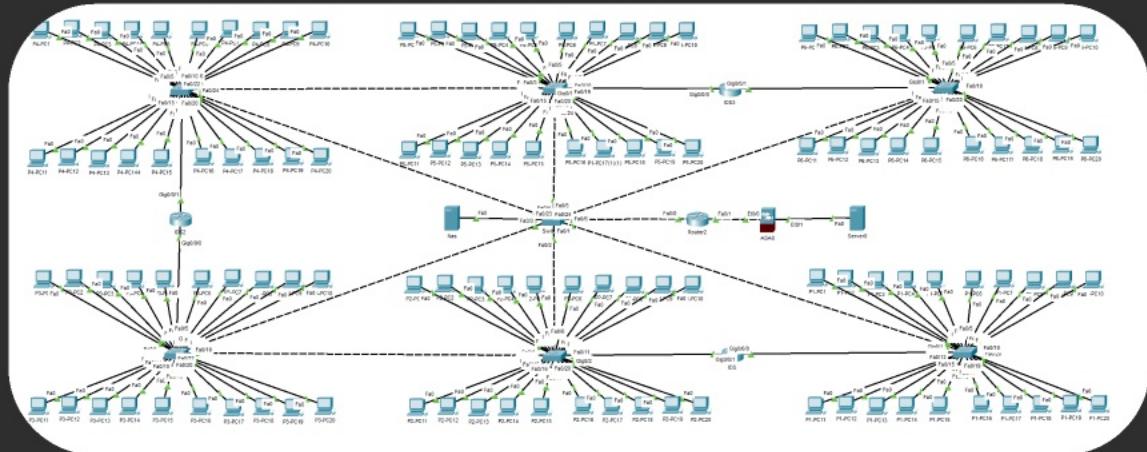
Un switch centrale collega tutti gli switch di piano e il router, garantendo la continuità della connettività in caso di guasto.

NAS

Il NAS è connesso allo switch centrale per un accesso centralizzato ai dati, migliorando l'efficienza e la velocità di comunicazione.

Schema Logico di Rete

Un'analisi dettagliata della struttura della rete interna e dei suoi componenti chiave.



Rete Interna

La rete interna è suddivisa in sei piani, ciascuno dotato di uno switch di layer 2 per connettere 20 postazioni.

Switch Centrale

Un switch centrale collega tutti gli switch di piano e il router, garantendo la continuità della connettività in caso di guasto.

NAS

Il NAS è connesso allo switch centrale per un accesso centralizzato ai dati, migliorando l'efficienza e la velocità di comunicazione.

Rete Interna

La rete interna è suddivisa in sei piani, ciascuno dotato di uno switch di layer 2 per connettere 20 postazioni.

Switch Centrale

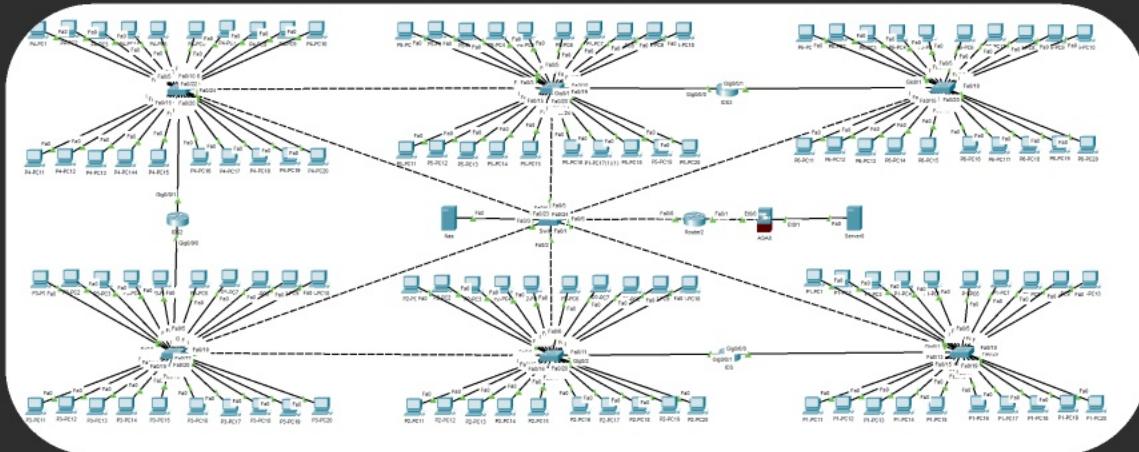
Un switch centrale collega tutti gli switch di piano e il router, garantendo la continuità della connettività in caso di guasto.

NAS

Il NAS è connesso allo switch centrale per un accesso centralizzato ai dati, migliorando l'efficienza e la velocità di comunicazione.

Schema Logico di Rete

Un'analisi dettagliata della struttura della rete interna e dei suoi componenti chiave.



Rete Interna

La rete interna è suddivisa in sei piani, ciascuno dotato di uno switch di layer 2 per connettere 20 postazioni.

Switch Centrale

Un switch centrale collega tutti gli switch di piano e il router, garantendo la continuità della connettività in caso di guasto.

NAS

Il NAS è connesso allo switch centrale per un accesso centralizzato ai dati, migliorando l'efficienza e la velocità di comunicazione.

```
(kali㉿kali)-[~/Documents]
(kali㉿kali)-[~/Documents]
$ sudo python Sniffer_v2.py
Avvio sniffer per traffico HTTP (porta 80) ... Premi CTRL+C per fermare.
Cercando dati di login ...
— [ Pacchetto HTTP con possibili credenziali trovato! ] —
POST /dvwa/login.php HTTP/1.1
Host: 192.168.20.10
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 44
Origin: http://192.168.20.10
Connection: keep-alive
Referer: http://192.168.20.10/dvwa/login.php
Cookie: security=high; PHPSESSID=0b6c8cce668a738335e5db4274c99160
Upgrade-Insecure-Requests: 1
Priority: u=0, i

username=admin&password=password&Login=Login
— [ Pacchetto HTTP con possibili credenziali trovato! ] —
GET /dvwa/index.php HTTP/1.1
Host: 192.168.20.10
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.20.10/dvwa/login.php
Connection: keep-alive
Cookie: security=high; PHPSESSID=0b6c8cce668a738335e5db4274c99160
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

VERBS / SNIFFER

La sua funzione informatica è catturare, registrare e analizzare il traffico dati che viaggia attraverso una rete.

In pratica, funziona come un microfono ambientale sulla rete:

Intercetta tutte le "conversazioni" (pacchetti di dati) tra i dispositivi.

Registra il contenuto di queste conversazioni (anche password e informazioni sensibili, se non cifrate).

Mostra all'analista (amministratore di rete o hacker) cosa sta succedendo sulla rete.



Username

admin

Password

Login

```
(kali㉿kali)-[~/Documents]
$ sudo python HttpRequest_v3.py
Digita l'indirizzo IP del target (es. 192.168.20.10): 192.168.20.10
Digita il percorso della risorsa (es. /index.php o /mutillidae/): /dvwa/login.php
```

Inizio la scansione dei verbi su: http://192.168.20.10/dvwa/login.php

— Test con verbo: GET —
Risposta: 200 OK

— Test con verbo: POST —
Risposta: 200 OK

— Test con verbo: PUT —
Risposta: 200 OK
⇒ ATTENZIONE! Il server ha risposto 200 OK a una richiesta potenzialmente pericolosa.

— Test con verbo: DELETE —
Risposta: 200 OK
⇒ ATTENZIONE! Il server ha risposto 200 OK a una richiesta potenzialmente pericolosa.

Scansione completata.

```
└─(kali㉿kali)-[~/Documents]
└─(kali㉿kali)-[~/Documents]
└─$ sudo python Sniffer_v2.py
Avvio sniffer per traffico HTTP (porta 80) ... Premi CTRL+C per fermare.
Cercando dati di login ...
—[ Pacchetto HTTP con possibili credenziali trovato! ]—
POST /dvwa/login.php HTTP/1.1
Host: 192.168.20.10
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 44
Origin: http://192.168.20.10
Connection: keep-alive
Referer: http://192.168.20.10/dvwa/login.php
Cookie: security=high; PHPSESSID=0b6c8cce668a738335e5db4274c99160
Upgrade-Insecure-Requests: 1
Priority: u=0, i

username=admin&password=password&Login=Login
_____
—[ Pacchetto HTTP con possibili credenziali trovato! ]—
GET /dvwa/index.php HTTP/1.1
Host: 192.168.20.10
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.20.10/dvwa/login.php
Connection: keep-alive
Cookie: security=high; PHPSESSID=0b6c8cce668a738335e5db4274c99160
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

Username

admin

Password

```
└─(kali㉿kali)-[~/Documents]
└─(kali㉿kali)-[~/Documents]
└─$ sudo python Sniffer_v2.py
Avvio sniffer per traffico HTTP (porta 80) ... Premi CTRL+C per fermare.
Cercando dati di login ...
—[ Pacchetto HTTP con possibili credenziali trovato! ]—
POST /dvwa/login.php HTTP/1.1
Host: 192.168.20.10
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 44
Origin: http://192.168.20.10
Connection: keep-alive
Referer: http://192.168.20.10/dvwa/login.php
Cookie: security=high; PHPSESSID=0b6c8cce668a738335e5db4274c99160
Upgrade-Insecure-Requests: 1
Priority: u=0, i

username=admin&password=password&Login=Login
_____
—[ Pacchetto HTTP con possibili credenziali trovato! ]—
GET /dvwa/index.php HTTP/1.1
Host: 192.168.20.10
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.20.10/dvwa/login.php
Connection: keep-alive
Cookie: security=high; PHPSESSID=0b6c8cce668a738335e5db4274c99160
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

Username

admin

Password

Perimetro di Sicurezza (DMZ)

Il perimetro di sicurezza della rete è strutturato con un firewall perimetrale posizionato tra il router interno e Internet, insieme a una zona demilitarizzata (DMZ) che ospita il web server. Questa configurazione è progettata per isolare il web server dalla rete interna, garantendo un filtraggio efficace del traffico e proteggendo le risorse aziendali da accessi non autorizzati e attacchi esterni.



Sistemi di Monitoraggio Avanzati

Intrusion Detection System (IDS)

Il sistema IDS (Intrusion Detection System) rileva attività dannose e comportamenti anomali nella rete, avvisando gli amministratori di rete. È fondamentale per la difesa contro attacchi esterni e minacce interne.

Intrusion Prevention System (IPS)

Il sistema IPS (Intrusion Prevention System) non solo rileva le intrusioni ma interviene attivamente per bloccare attacchi in tempo reale, rendendo le reti più sicure e resilienti contro minacce immediate.

Alert Log View Settings

Instance to View: (WAN) WAN
Choose which instance alerts you want to inspect.

Save or Remove Logs: Download, Clear
All alert log files for selected interface will be downloaded

Save Settings: Save, Refresh (checked)
Save auto-refresh and view settings, Default is ON

Number of alerts to display: 250 (Default is 250)

Alert Log View Filter

Last 250 Alert Entries. (Most recent entries are listed first)

Note: Alerts triggered by DROP rules that resulted in dropped (blocked) packets are shown with highlighted rows below.

Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
10/17/2025 10:44:46	⚠️	2	TCP	Misc Attack	151.242.132.119	9001	10.0.2.15	38361	1:2522197	ET TOR Known Tor Relay/Router (Not Exit) Node
					🔍	🌐	➕		➕	Traffic group 198
10/17/2025 10:44:45	⚠️	2	TCP	Misc Attack	202.71.14.100	9000	10.0.2.15	7531	1:2522331	ET TOR Known Tor Relay/Router (Not Exit) Node
					🔍	🌐	➕		➕	Traffic group 332
10/17/2025 10:44:44	⚠️	2	TCP	Misc Attack	45.132.126.29	9100	10.0.2.15	28800	1:2522399	ET TOR Known Tor Relay/Router (Not Exit) Node
					🔍	🌐	➕		➕	Traffic group 400
10/17/2025 10:44:44	⚠️	2	TCP	Misc Attack	37.120.171.188	443	10.0.2.15	16904	1:2522384	ET TOR Known Tor Relay/Router (Not Exit) Node
					🔍	🌐	➕		➕	Traffic group 385
10/17/2025 10:44:44	⚠️	2	TCP	Misc Attack	37.143.117.173	9050	10.0.2.15	8238	1:2522386	ET TOR Known Tor Relay/Router (Not Exit) Node
					🔍	🌐	➕		➕	

Interfaces Global Settings Updates Alerts Blocks Files Pass Lists Suppress Logs View Logs Mgmt SID Mgmt

Sync IP Lists

Interface Settings Overview

Interface	Suricata Status	Pattern Match	Blocking Mode	Description	Actions
WAN (vtnet0)	🟢 C ⓘ	AUTO	INLINE IPS	WAN	📝 🗑️

+ Add, Delete

Intrusion Detection System (IDS)

Il sistema IDS (Intrusion Detection System) rileva attività dannose e comportamenti anomali nella rete, avvisando gli amministratori di rete. È fondamentale per la difesa contro attacchi esterni e minacce interne.

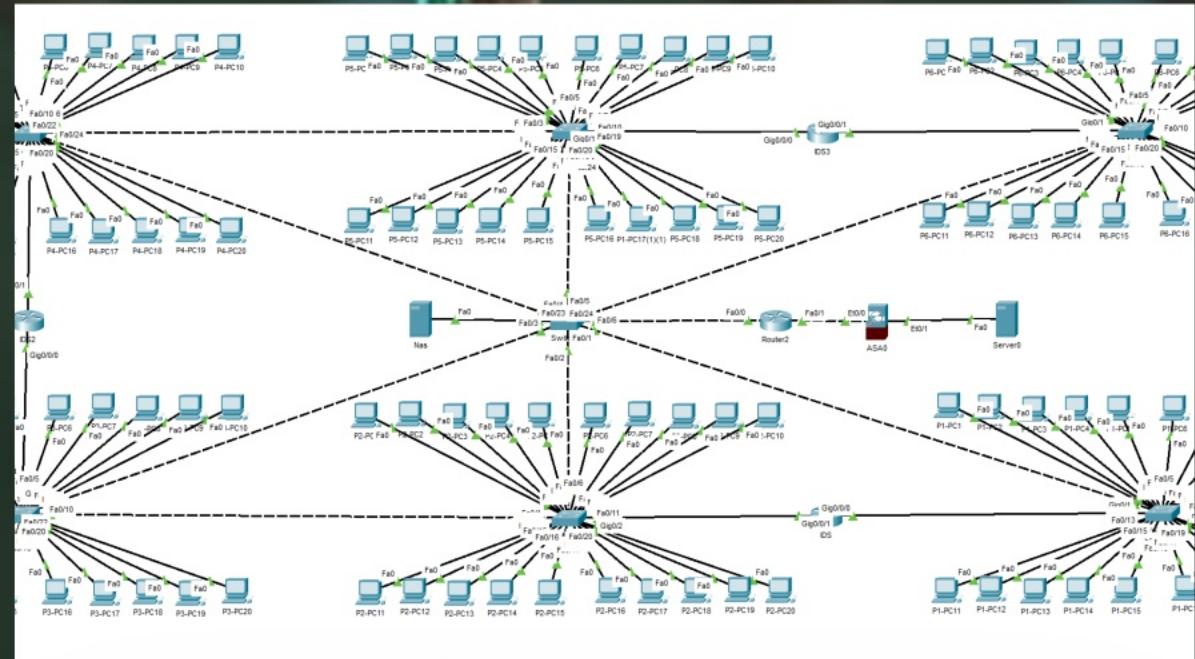
Intrusion Prevention System (IPS)

Il sistema IPS (Intrusion Prevention System) non solo rileva le intrusioni ma interviene attivamente per bloccare attacchi in tempo reale, rendendo le reti più sicure e resistenti contro minacce immediate.

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	192.168.50.10	*	OPT1 address	22 (SSH)	*	none	SSH solo da amministratore interno	
<input type="checkbox"/>	✓	0/0 B	IPv4 UDP	*	*	OPT1 subnets	53 (DNS)	*	none	Permetti risoluzione DNS	
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	*	*	OPT1 address	80 (HTTP)	*	none	Redirect HTTP to HTTPS	
<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP	*	*	OPT1 address	443 (HTTPS)	*	none	permitti accesso HTTPS da indirizzi ip pubblici		
<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP	*	*	OPT1 subnets	22 - 23	*	none	Blocca porta 22 per bruteforce e 23 (telnet)		
<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP	*	*	OPT1 subnets	135	*	none	Blocca porta 135 (rischio bruteforce)		
<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP	*	*	OPT1 address	445 (MS DS)	*	none	porta 445 (brute)		
<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP	*	*	OPT1 subnets	3389 (MS RDP)	*	none	porta 3389 (brute)		
<input checked="" type="checkbox"/>	0/0 B	IPv4 ICMP	echoreq	*	*	OPT1 subnets	*	*	none	Limita ping	
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	192.168.50.10	*	OPT1	*	*	none	Permetti l'accesso a indirizzi ip privati	

Virtualizzazione con pfSense

La virtualizzazione consente di testare e configurare in modo sicuro ambienti di rete, isolando le risorse e garantendo una gestione efficiente dei servizi. Utilizzando pfSense come firewall virtuale, è stato possibile simulare la protezione della rete aziendale contro minacce esterne, mantenendo al contempo la funzionalità dei servizi interni.



Simulazione di Rete con Packet Tracer

La simulazione Packet Tracer ha permesso di visualizzare e analizzare il traffico di rete in tempo reale. Grazie a questa tecnologia, sono stati implementati scenari di test per il firewall, verificando l'efficacia delle regole di sicurezza e l'integrità della rete. Questo approccio ha consentito di ottimizzare la configurazione prima della reale implementazione.

Obiettivi della Configurazione Firewall

Obiettivi della Configurazione Firewall

La configurazione del firewall è essenziale per salvaguardare l'integrità della rete aziendale. Gli obiettivi principali comprendono la protezione da attacchi esterni, limitando l'accesso non autorizzato e garantendo comunicazioni sicure tra le diverse reti. Inoltre, si mira a proteggere i servizi critici e a gestire in modo efficace gli accessi interni, assicurando un monitoraggio continuo e un'adeguata risposta agli incidenti.



Analisi delle Regole Implementate

Blocco di Servizi ad Alto Rischio

Sono state implementate regole di sicurezza rigorose per bloccare servizi ad alto rischio come SSH, Telnet e RDP, noti per essere vulnerabili ad attacchi brute-force e exploit. Queste misure riducono significativamente il rischio di accessi non autorizzati e potenziali violazioni della rete.



Limitazione del Protocollo ICMP

La limitazione del protocollo ICMP è stata attuata per ridurre la visibilità della rete, prevenendo la mappatura della rete tramite scanner automatici e attacchi DDoS. Questa configurazione migliora la privacy e protegge le risorse interne da potenziali minacce.



Blocco di Servizi ad Alto Rischio

Sono state implementate regole di sicurezza rigorose per bloccare servizi ad alto rischio come SSH, Telnet e RDP, noti per essere vulnerabili ad attacchi brute-force e exploit. Queste misure riducono significativamente il rischio di accessi non autorizzati e potenziali violazioni della rete.

The screenshot shows a network configuration interface for creating a new security rule. The rule is set to 'Block' and applies to 'OPT1' interface, IPv4, and TCP protocol. The source is set to 'Any' and the destination is 'OPT1 subnets' with ports SSH (22) and Telnet (23). The 'Extra Options' section is visible at the bottom.

Action: Block
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled: Disable this rule
Set this option to disable this rule without removing it from the list.

Interface: OPT1
Choose the interface from which packets must come to match this rule.

Address Family: IPv4
Select the Internet Protocol version this rule applies to.

Protocol: TCP
Choose which IP protocol this rule should match.

Source

Source: Invert match Any Source Address /

Display Advanced
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

Destination

Destination: Invert match OPT1 subnets Destination Address /

Destination Port Range: SSH (22) From Custom Telnet (23) To Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Limitazione del Protocollo ICMP

La limitazione del protocollo ICMP è stata attuata per ridurre la visibilità della rete, prevenendo la mappatura della rete tramite scanner automatici e attacchi DDoS. Questa configurazione migliora la privacy e protegge le risorse interne da potenziali minacce.

The screenshot shows a configuration window for a firewall rule. The rule is set to 'Block' and applies to 'OPT1' interface, 'IPv4' version, and 'ICMP' protocol. The ICMP subtype is set to 'Echo request'. There are options to invert the match and log packets handled by the rule. A note at the bottom suggests using the 'Status: System Logs: Settings page' for logging.

Block

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is rejected whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disable this rule
Set this option to disable this rule without removing it from the list.

OPT1

Choose the interface from which packets must come to match this rule.

IPv4

Select the Internet Protocol version this rule applies to.

ICMP

Choose which IP protocol this rule should match.

Alternate Host
Datagram conversion error
Echo reply
Echo request

For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.

Invert match Any Source Address

Invert match OPT1 subnets Destination Address

Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a Status: System Logs: Settings page).



Software e PC per la Segreteria e Assistenza Clienti

Ogni piano della rete aziendale è stato progettato per soddisfare specifiche esigenze operative, con la distribuzione di software e PC adattata ai requisiti di ciascun dipartimento. Il primo piano, ad esempio, è dedicato alla segreteria, equipaggiato con 20 PC e software per la gestione amministrativa. Altri piani comprendono soluzioni per produzione, sicurezza informatica, grafica e marketing, ciascuno con hardware e software mirati per massimizzare l'efficienza del lavoro.

Software e PC per Produzione e Logistica

L'approccio dettagliato alla pianificazione include non solo le specifiche tecniche, ma anche un budget chiaro per ogni dipartimento. Le stime di costo variano da un massimo di 30.000 euro per la dirigenza a 5.000 euro per la segreteria, evidenziando l'importanza di investire in tecnologia adeguata per garantire prestazioni ottimali. Questo modello di distribuzione è essenziale per supportare le diverse funzioni aziendali e promuovere un ambiente di lavoro produttivo e sicuro.

Costi Totali del Progetto: 209.277 Euro + IVA

Il budget complessivo per il progetto di rete realizzato per Theta è stimato in 230.000 euro, comprendente sia i costi dei materiali che della manodopera. Questa cifra rappresenta un investimento significativo per garantire una rete sicura e scalabile, integrando infrastrutture avanzate e misure di sicurezza adeguate.





Cronoprogramma del Progetto di Rete per Theta

Fasi di implementazione della rete da parte di CERBERUS S.P.A.

Sopralluogo

Esecuzione di un sopralluogo e preparazione del progetto esecutivo.

Posa Cavi

Posa dei cavi rame/fibra e installazione dei patch panel, pianificata in 5-6 giorni con 2 tecnici.

Montaggio Apparati

Montaggio degli apparati e cablaggio dei rack, previsto in 1 giorno.

Configurazione Rete

Configurazione della rete e delle misure di sicurezza, prevista in 2-3 giorni.

Collaudo e Formazione

Collaudo finale, documentazione e formazione del personale, programmati in 0.5-1 giorno.

Sopralluogo

Esecuzione di un
sopralluogo e
preparazione del
progetto esecutivo.

Posa Cavi

Posa dei cavi rame/
fibra e installazione dei
patch panel, pianificata
in 5-6 giorni con 2
tecnicici.

Montaggio Apparati

Montaggio degli
apparati e
cablaggio dei rack,
previsto in 1 giorno.

Configurazione Rete

Configurazione della
rete e delle misure
di sicurezza, prevista
in 2-3 giorni.

Collaudo e Formazione

Collaudo finale,
documentazione e
formazione del
personale, programmati
in 0.5-1 giorno.



Cronoprogramma del Progetto di Rete per Theta

Fasi di implementazione della rete da parte di CERBERUS S.P.A.

Sopralluogo

Esecuzione di un sopralluogo e preparazione del progetto esecutivo.

Posa Cavi

Posa dei cavi rame/fibra e installazione dei patch panel, pianificata in 5-6 giorni con 2 tecnici.

Montaggio Apparati

Montaggio degli apparati e cablaggio dei rack, previsto in 1 giorno.

Configurazione Rete

Configurazione della rete e delle misure di sicurezza, prevista in 2-3 giorni.

Collaudo e Formazione

Collaudo finale, documentazione e formazione del personale, programmati in 0.5-1 giorno.

Controllo degli Accessi

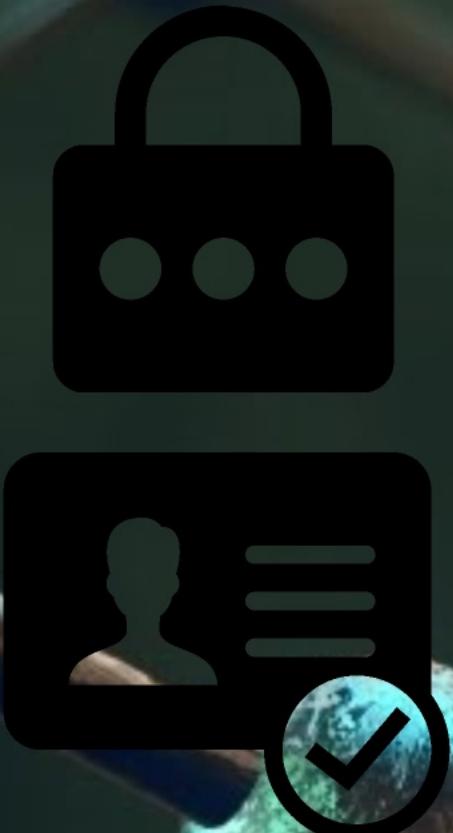
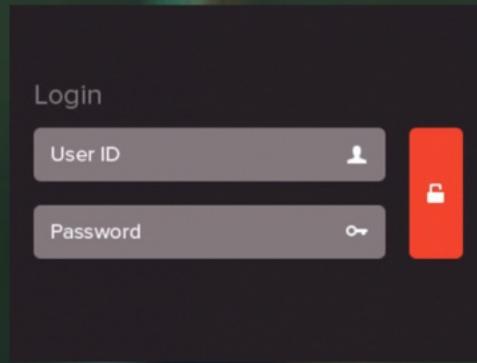
Il controllo degli accessi alla rete è realizzato tramite l'implementazione di politiche di NAC/802.1X, che garantiscono l'autenticazione port-based per gli utenti e i dispositivi autorizzati.

Gestione dei Log

La gestione dei log è fondamentale per monitorare e analizzare gli eventi di sicurezza. L'uso di sistemi Syslog/SIEM consente una gestione centralizzata e un'analisi approfondita delle informazioni e degli eventi di sicurezza.

Segmentazione Zero-Trust

La segmentazione della rete secondo la strategia Zero-Trust assicura che non ci sia fiducia implicita tra i vari segmenti, richiedendo l'autenticazione continua per ogni accesso.



Misure di Sicurezza e Conformità

Controllo degli Accessi

Il controllo degli accessi alla rete è realizzato tramite l'implementazione di politiche di NAC/802.1X, che garantiscono l'autenticazione port-based per gli utenti e i dispositivi autorizzati.

Gestione dei Log

La gestione dei log è fondamentale per monitorare e analizzare gli eventi di sicurezza. L'uso di sistemi Syslog/SIEM consente una gestione centralizzata e un'analisi approfondita delle informazioni e degli eventi di sicurezza.

Segmentazione Zero-Trust

La segmentazione della rete secondo la strategia Zero-Trust assicura che non ci sia fiducia implicita tra i vari segmenti, richiedendo l'autenticazione continua per ogni accesso.

Conclusioni e Raccomandazioni per Theta

Il progetto ha consegnato una rete aziendale robusta e scalabile, predisposta per affrontare le sfide future. Le seguenti raccomandazioni sono essenziali per garantire una sicurezza continua: implementazione di un hardening del server, aggiornamenti regolari dei software, regole firewall rigorose e monitoraggio costante della rete.



Progettazione e Sicurezza dell'Infrastruttura di Rete per Theta

Una presentazione sulle strategie avanzate per la sicurezza e la progettazione delle infrastrutture di rete aziendali



CERBERUS

The collage includes the following sections:

- CRIPTAZIONE DAW**: Shows three computer monitors displaying a blue dog logo and the word "CERBERUS".
- Progetto di Rete per Theta**: Includes a timeline from 2014 to 2016, a budget summary, and a slide titled "Costi Totali del Progetto: 200,277 Euro + IVA".
- Chi Siamo**: Features logos for Python, C, Java, Go, and Google.
- Progetto di Rete per Theta**: A large screenshot showing network monitoring and analysis tools.
- La nostra Mission**: Includes a video thumbnail of a person speaking.
- VERBS / SNIFTER**: A screenshot of a network traffic analysis tool.
- DVWA**: A screenshot of a web application security testing environment.
- Network Monitoring**: A screenshot of a network monitoring dashboard.
- Defensor IT per la Seguridad Informatica**: Includes a video thumbnail and a screenshot of a server room.
- Defensor IT per la Seguridad Informatica**: Includes a video thumbnail and a screenshot of a server room.
- Defensor IT per la Seguridad Informatica**: Includes a video thumbnail and a screenshot of a server room.