

**BoNet™**

RETI & SICUREZZA

ANALISI DI RETE — RELAZIONE

Relazione di analisi di rete su sette livelli

Dalla mappa della rete al piano di intervento: rilevamento, topologia, prestazioni, sicurezza, configurazioni e continuità di un'azienda su due sedi collegate in VPN attraverso Internet.

Meccanotecnica Alfa S.r.l. — sede di Padova (direzione e produzione) e sede di Bologna (commerciale e magazzino), unite da un tunnel IPsec site-to-site.

CLIENTE

Meccanotecnica Alfa S.r.l. (esempio)

PERIODO DI RILEVAMENTO

1-10 settembre 2026

VERSIONE

1.0

RIFERIMENTO MANDATO

MA-2026-014

DATA RELAZIONE

15 settembre 2026

REDATTO DA

BoNet™ — un progetto di Euro Buchberger

Documento dimostrativo. Ragione sociale, sedi, persone, indirizzi IP e criticità descritte in questa relazione sono inventati a scopo illustrativo e non si riferiscono ad alcun cliente reale. BoNet la pubblica come esempio del formato e del livello di dettaglio di una relazione di analisi di rete — non contiene le soluzioni tecniche di dettaglio, che sono oggetto di un preventivo separato.

Indice

– Sintesi per la direzione

1 Introduzione e metodologia

1.1 Obiettivo dell'analisi · 1.2 Perimetro ed esclusioni · 1.3 Mandato, autorizzazione e NDA ·
1.4 Raccolta dati e strumenti · 1.5 Come leggere questa relazione

2 Il contesto: Meccanotecnica Alfa

2.1 Profilo dell'azienda · 2.2 Le due sedi · 2.3 Dalle interviste

3 Livello 1 — Rilevamento e inventario

4 Livello 2 — Topologia e instradamento

5 Livello 3 — Prestazioni e capacità

6 Livello 4 — Sicurezza e segmentazione

7 Livello 5 — Configurazioni e aggiornamenti

8 Livello 6 — Affidabilità e continuità

9 Registro consolidato delle criticità

10 Livello 7 — Piano di intervento

A Legenda e criteri di gravità

B Strumenti utilizzati

C Riservatezza e validità della relazione

SINTESI

Sintesi per la direzione

Tra il 1° e il 10 settembre 2026 BoNet ha condotto un'analisi di rete su sette livelli per Meccanotecnica Alfa S.r.l., azienda manifatturiera con sede direzionale e produttiva a Padova e sede commerciale e di magazzino a Bologna, collegate da un tunnel IPsec site-to-site attraverso Internet.

L'analisi ha coperto in sequenza il rilevamento degli apparati, la topologia e l'instradamento, le prestazioni, la sicurezza e la segmentazione, le configurazioni, l'affidabilità e la continuità operativa, fino a un piano di intervento prioritizzato. Il metodo e il livello di dettaglio sono descritti nel capitolo 1.



Il quadro complessivo mostra una rete funzionale ma cresciuta per aggiunte successive più che per progetto. Tre osservazioni riassumono il resto della relazione:

- **Il collegamento tra le due sedi non ha controlli sufficienti su cosa vi transita.** Il tunnel instrada l'intera rete di una sede verso l'altra senza selezione né priorità: un trasferimento pesante può saturare la linea di Bologna e degradare la voce, come già segnalato dagli utenti.
- **I servizi centrali esistono in un'unica copia, a Padova.** Directory, DNS interno e file server non hanno una copia funzionante a Bologna: un'interruzione del tunnel lascia la sede commerciale senza login né documenti, non solo senza posta.
- **La sicurezza perimetrale della sede secondaria presenta lacune che vanno oltre la normale amministrazione** — in particolare un apparato ancora con le credenziali di fabbrica e un'interfaccia di gestione raggiungibile da Internet senza restrizione.

Nessuna delle criticità rilevate richiede un fermo immediato dell'attività. Le quattro criticità classificate come alte o critiche (capitolo 9, righe 1, 3, 7 e 8) meritano un intervento entro poche settimane; le restanti si prestano a una pianificazione ordinaria nei mesi successivi.

Il capitolo 10 propone un piano diviso tra interventi rapidi e interventi strutturali, ordinato per impatto e sforzo. **Questa relazione descrive cosa è stato rilevato e cosa andrebbe fatto, non come realizzarlo né a quale costo:** la progettazione di dettaglio e il preventivo sono oggetto di un documento separato, senza impegno.

CAPITOLO 1

Introduzione e metodologia

1.1 Obiettivo dell'analisi

Fotografare lo stato della rete informatica di Meccanotecnica Alfa nelle sue due sedi, individuare le criticità secondo un criterio uniforme e fornire una base oggettiva su cui decidere dove intervenire prima. L'analisi non entra nel merito degli applicativi gestionali (ERP, sistema di gestione del magazzino) se non per la parte che riguarda la rete che li trasporta.

1.2 Perimetro ed esclusioni

Rientrano nel perimetro: la rete cablata e Wi-Fi di entrambe le sedi, gli apparati di instradamento e sicurezza, il collegamento site-to-site, la sala server di Padova, la fonia IP e la videosorveglianza limitatamente alla loro presenza in rete. Sono esclusi: la sicurezza fisica degli edifici (salvo il controllo accessi alla sala quadri, richiamato al capitolo 8), il contenuto e la logica degli applicativi gestionali, le postazioni di lavoro dal punto di vista applicativo.

1.3 Mandato, autorizzazione e NDA

L'analisi è stata svolta sulla base di un mandato scritto (rif. MA-2026-014) firmato dal referente aziendale, con perimetro e finestra temporale concordati, autorizzazione esplicita alla scansione attiva delle reti indicate e NDA reciproco. I dati raccolti nel corso dell'analisi — configurazioni, catture di traffico, credenziali di sola lettura fornite per l'occasione — sono stati cancellati alla consegna di questa relazione, come da accordo.

1.4 Raccolta dati e strumenti

La raccolta dati si è svolta in quattro fasi: interviste con il referente IT e con un responsabile per ciascuna area operativa (produzione, magazzino, commerciale); rilevamento automatico degli apparati da un nodo interno per ciascuna sede; accesso in sola lettura alle configurazioni degli apparati di rete; sopralluogo fisico degli armadi e delle sale quadri, con misura della copertura Wi-Fi sul posto. Le categorie di strumenti utilizzati sono elencate in appendice B.

1.5 Come leggere questa relazione

La relazione segue i sette livelli con cui BoNet organizza ogni analisi (L1 rilevamento, L2 topologia, L3 prestazioni, L4 sicurezza, L5 configurazioni, L6 continuità, L7 piano di intervento). Ogni criticità rilevata è numerata, classificata per gravità — **CRITICO** **ALTO** **MEDIO** **BASSO** — e riportata nel registro consolidato del capitolo 9, con i criteri di attribuzione descritti in appendice A.

CAPITOLO 2

Il contesto: Meccanotecnica Alfa

2.1 Profilo dell'azienda

Meccanotecnica Alfa S.r.l. progetta e produce componenti meccanici di precisione per il settore industriale. La sede storica di Padova ospita la direzione, gli uffici tecnici e lo stabilimento produttivo. La sede di Bologna, aperta alcuni anni dopo per seguire da vicino un'area di mercato in crescita, ospita l'area commerciale e un magazzino di distribuzione. Le due sedi condividono il gestionale ERP, ospitato a Padova, e la telefonia interna.

2.2 Le due sedi

DATI DI SINTESI

	SEDE DI PADOVA	SEDE DI BOLOGNA
Funzione	Direzione, uffici tecnici, produzione	Commerciale, magazzino di distribuzione
Postazioni	~60	~25
Rete locale	4 VLAN, core L3 ridondante lato switch, non lato firewall	3 VLAN, core L3 singolo
Servizi ospitati	Active Directory, ERP, file server, centralino VoIP, NVR	Controller di dominio secondario (RODC) con cache locale
Collegamento Internet	Fibra, un solo operatore	Fibra, un solo operatore
Interconnessione	Tunnel IPsec site-to-site attraverso Internet, sempre attivo	

2.3 Dalle interviste

Alcuni estratti, riportati in forma anonima, danno il tono di come la rete viene vissuta da chi la usa ogni giorno:

«Il tunnel lo abbiamo configurato anni fa e da allora non l'abbiamo più toccato, finché ha funzionato.»

REFERENTE IT

«Ogni tanto i lettori del magazzino perdono la connessione, soprattutto in fondo al capannone.»

RESPONSABILE PRODUZIONE

«Se salta la linea qui a Bologna non riusciamo nemmeno ad accedere ai PC, non solo alla posta.»

RESPONSABILE COMMERCIALE, BOLOGNA

CAPITOLO 3 · LIVELLO 1

Rilevamento e inventario

Chi c'è in rete: dispositivi, sistemi operativi, ruoli e indirizzi, in entrambe le sedi.

3.1 Metodo di rilevamento

Il rilevamento è stato condotto con scansione attiva da un nodo interno per ciascuna sede, incrociata con l'inventario fornito dal cliente e con un sopralluogo fisico degli armadi di rete. Dove possibile, gli apparati sono stati identificati per modello e versione firmware direttamente dall'interfaccia di gestione.

3.2 Inventario apparati — Sede di Padova

APPARATO	RUOLO	INDIRIZZO	VLAN
Router WAN PD	Terminazione linea Internet	203.0.113.10	—
Firewall PD	Perimetro, NAT, VPN site-to-site	10.1.99.1	PD99
Core switch L3 PD	Instradamento inter-VLAN	10.1.99.2	PD99
Switch accesso Uffici (×2)	Accesso postazioni uffici e direzione	10.1.10.2 – .3	PD10
Switch accesso Produzione (×3)	Accesso linee e postazioni reparto	10.1.20.2 – .4	PD20
Access point Wi-Fi (×6)	Copertura uffici e capannone	10.1.10.50 – .55	PD10
Server room — Hypervisor	Host di virtualizzazione	10.1.40.5	PD40
Server room — Domain Controller	Active Directory, DNS interno	10.1.40.10	PD40
Server room — ERP	Gestionale aziendale	10.1.40.11	PD40
Server room — File server	Condivisioni documentali	10.1.40.12	PD40
Server room — Backup NAS	Backup locale	10.1.40.13	PD40
Centralino VoIP	Fonia interna, ~40 interni	10.1.40.15	PD40
NVR videosorveglianza	Registrazione 12 telecamere	10.1.40.20	PD40

3.3 Inventario apparati — Sede di Bologna

APPARATO	RUOLO	INDIRIZZO	VLAN
Router WAN BO	Terminazione linea Internet	198.51.100.20	—
Firewall BO	Perimetro, NAT, VPN site-to-site	10.2.99.1	BO99
Core switch L3 BO	Instradamento inter-VLAN	10.2.99.2	BO99

APPARATO	RUOLO	INDIRIZZO	VLAN
Switch accesso Uffici	Accesso postazioni commerciale	10.2.10.2	BO10
Switch accesso Magazzino	Accesso terminali e postazioni magazzino	10.2.20.2	BO20
Access point Wi-Fi (×4)	Copertura uffici e magazzino	10.2.10.40 – .43	BO10
RODC + cache DNS locale	Login e risoluzione nomi in assenza di tunnel	10.2.20.5	BO20
NAS locale	Backup dati magazzino	10.2.20.6	BO20
Gateway VoIP locale	Trunk SIP verso il centralino di Padova	10.2.10.15	BO10

3.4 Osservazioni

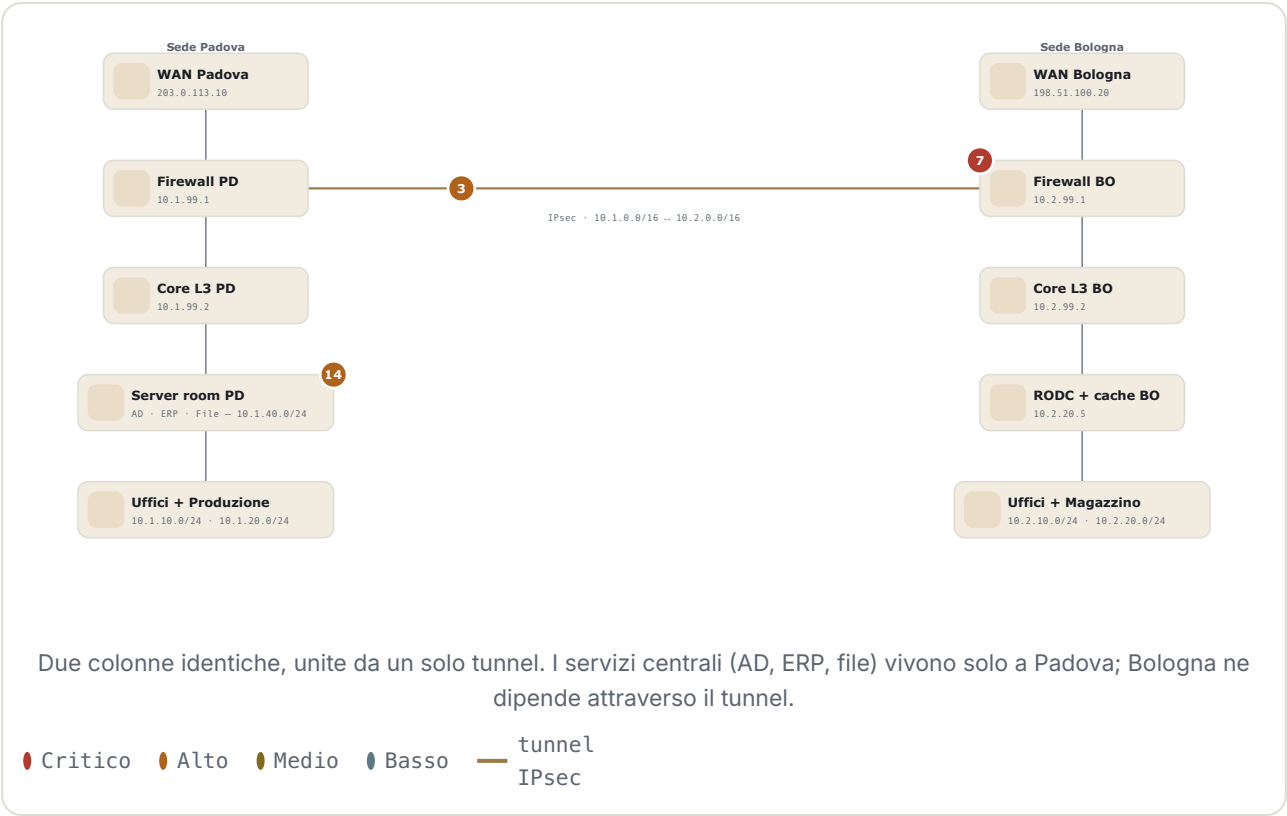
L'inventario ha fatto emergere due scostamenti rispetto a quanto dichiarato dal cliente: tre switch di reparto a Padova non risultavano nell'elenco fornito, installati nel tempo per estendere le porte disponibili senza aggiornare la documentazione (**Criticità 1**); un sottoinsieme di postazioni del reparto produzione condivide la stessa password amministrativa locale, impostata all'origine e mai differenziata (**Criticità 2**). Per il resto, l'inventario rilevato corrisponde a quanto dichiarato.

CAPITOLO 4 · LIVELLO 2

Topologia e instradamento

Come è divisa la rete: VLAN e subnet, percorsi di routing, gateway, DNS e DHCP, punti singoli di guasto.

4.1 Schema generale



4.2 Piano di indirizzamento e VLAN

VLAN	SOTTORETE	RUOLO	SEDE
PD10	10.1.10.0/24	Uffici	Padova
PD20	10.1.20.0/24	Produzione / reparto	Padova
PD40	10.1.40.0/24	Server room (AD, ERP, file)	Padova
PD99	10.1.99.0/24	Gestione apparati	Padova
B010	10.2.10.0/24	Uffici	Bologna
B020	10.2.20.0/24	Magazzino + RODC	Bologna
B099	10.2.99.0/24	Gestione apparati	Bologna

4.3 Instradamento e tunnel IPsec

Il collegamento tra le due sedi è un tunnel IPsec site-to-site in IKEv2, terminato sui due firewall perimetrali (203.0.113.10 ↔ 198.51.100.20), sempre attivo. I selettori di traffico configurati coprono l'intera rete di una sede verso l'intera rete dell'altra (10.1.0.0/16 ↔ 10.2.0.0/16): qualunque host di una sede può raggiungere qualunque host dell'altra, senza distinzione tra ciò che deve effettivamente attraversare il tunnel e ciò che potrebbe restare locale.

4.4 DNS e DHCP

Il DNS interno è integrato con Active Directory ed è autoritativo a Padova; il DHCP è gestito localmente dal core switch di ciascuna sede, con ambiti coerenti con il piano di indirizzamento. A Bologna un controller di dominio in sola lettura (RODC) mantiene una cache locale di autenticazione e risoluzione nomi, pensata per garantire continuità in caso di interruzione del tunnel.

4.5 Punti singoli di guasto

Ogni sede dispone di un solo collegamento Internet, un solo operatore e un solo firewall, senza apparati di riserva né failover automatico. Il core switch di ciascuna sede è singolo. Nessuna delle due sedi ha un secondo percorso — via un operatore diverso o una connessione mobile — in caso di guasto della linea principale.

4.6 Criticità rilevate a questo livello

Il collegamento instradato senza selezione (**Criticità 3**) e l'assenza di ridondanza sul collegamento Internet di entrambe le sedi (**Criticità 4**) sono descritte in dettaglio nel registro del capitolo 9.

CAPITOLO 5 · LIVELLO 3

Prestazioni e capacità

Quanto regge la rete: latenza, jitter, perdita di pacchetti, banda reale contro nominale, copertura Wi-Fi, qualità della fonia.

5.1 Metodologia di misura

Le misure sono state condotte nell'arco di cinque giorni lavorativi, campionando tre fasce orarie (mattina, primo pomeriggio, notte durante la finestra di backup) per cogliere le condizioni di carico più diverse. La copertura Wi-Fi è stata rilevata con un sopralluogo e un analizzatore portatile in entrambe le sedi.

5.2 Latenza e perdita di pacchetti tra le sedi

FASCIA ORARIA	LATENZA MEDIA	JITTER	PERDITA DI PACCHETTI
Mattina (09–11)	19 ms	3 ms	0,1%
Pomeriggio (14–16)	22 ms	4 ms	0,2%
Notte, durante il backup (01–03)	84 ms	31 ms	2,4%

Il degrado notturno coincide con la finestra del backup incrementale tra le sedi (**Criticità 3**): non essendoci priorità di traffico sul tunnel, un trasferimento pesante occupa la banda disponibile indistintamente.

5.3 Banda reale contro nominale

	BANDA CONTRATTUALE	BANDA MISURATA (ORA DI PUNTA)
Padova	1 Gbps simmetrica	~890 Mbps
Bologna	200 Mbps simmetrica	~178 Mbps in condizioni normali, satura durante il backup notturno

5.4 Copertura Wi-Fi

ZONA	SEGNALE MEDIO	ESITO
Uffici Padova	-52 dBm	Buono
Capannone Padova, lato ingresso	-58 dBm	Buono
Capannone Padova, fondo	-79 dBm	Insufficiente — disconnessioni
Uffici Bologna	-49 dBm	Buono
Magazzino Bologna	-71 dBm	Al limite, disconnessioni occasionali

Nella zona in fondo al capannone di Padova e nel magazzino di Bologna la copertura è insufficiente per un uso continuativo dei terminali radio (**Criticità 5**), coerentemente con quanto segnalato in intervista.

5.5 Fonia IP e qualità delle chiamate

In condizioni normali la qualità delle chiamate tra le sedi è buona (punteggio MOS stimato 4.1 su 5). Durante i trasferimenti pesanti sul tunnel — non solo il backup notturno, anche invii occasionali di file di grandi dimensioni in orario di lavoro — il punteggio scende a 2.6 su 5, con effetti percepibili dagli utenti (**Criticità 6**): la causa è l'assenza di priorità di traffico (QoS) sul tunnel, non la banda disponibile in sé.

5.6 Criticità rilevate a questo livello

Copertura Wi-Fi insufficiente in due aree (**Criticità 5**) e assenza di priorità per la voce sul tunnel (**Criticità 6**), entrambe riportate nel registro del capitolo 9.

CAPITOLO 6 · LIVELLO 4

Sicurezza e segmentazione

Cosa è esposto: porte e servizi raggiungibili, isolamento tra reti, regole di firewall e NAT, VPN, credenziali.

6.1 Superficie esposta verso Internet

INDIRIZZO PUBBLICO	SERVIZI RAGGIUNGIBILI	OSSERVAZIONE
203.0.113.10 (Padova)	IPsec (tunnel), portale VPN utenti mobili	Coerente con l'uso previsto
198.51.100.20 (Bologna)	IPsec (tunnel), interfaccia di gestione del firewall	L'interfaccia di gestione non dovrebbe essere raggiungibile da Internet

L'interfaccia di amministrazione del firewall di Bologna risulta raggiungibile da qualunque indirizzo Internet, senza una lista di IP sorgenti autorizzati (**Criticità 8**).

6.2 Segmentazione interna

La matrice seguente riassume, per le coppie di VLAN rilevanti, se il traffico è bloccato, permesso senza restrizioni o permesso solo verso servizi specifici.

	PD10 Uffici	PD20 Produzione	PD40 Server	BO10 Uffici	BO20 Magazzino
PD10 Uffici	—	No	Solo servizi	Sì (tunnel)	Solo servizi
PD20 Produzione	No	—	Sì, non filtrato	No	No
PD40 Server	Solo servizi	Sì, non filtrato	—	Sì (tunnel)	Sì (tunnel)
BO10 Uffici	Sì (tunnel)	No	Sì (tunnel)	—	Solo servizi
BO20 Magazzino	Solo servizi	No	Sì (tunnel)	Solo servizi	—

L'unica cella non filtrata è quella tra **Produzione** e **Server room**: qualunque postazione del reparto raggiunge direttamente ERP e file server, senza passare da una regola dedicata (**Criticità 9**). Le altre coppie sono ragionevolmente controllate o limitate ai soli servizi necessari.

6.3 Regole firewall e NAT

Il ruleset di Padova è organizzato per oggetti nominati e commentati; quello di Bologna presenta diverse regole ereditate dalla configurazione iniziale del fornitore, non più documentate, insieme a alcune regole ampie (sorgente e destinazione "qualsiasi") il cui uso reale non è stato possibile confermare in sede di analisi.

6.4 VPN e accessi remoti

Oltre al tunnel site-to-site, quattro utenti commerciali dispongono di accesso VPN remoto per consultare l'ERP fuori sede. L'accesso è protetto da una chiave precondivisa (PSK) condivisa tra tutti gli utenti, senza certificati individuali né autenticazione a più fattori (**Criticità 10**).

6.5 Credenziali e accessi amministrativi

Oltre alla password locale condivisa già rilevata al capitolo 3 (**Criticità 2**), uno degli access point Wi-Fi di Bologna — installato più recentemente, in un ampliamento della copertura del magazzino — mantiene ancora le credenziali amministrative di fabbrica. L'apparato è raggiungibile anche dalla rete ospiti, rendendo la credenziale di fatto esposta a chiunque si connetta a quella rete (**Criticità 7**).

6.6 Criticità rilevate a questo livello

Questo livello concentra la criticità più grave della relazione (**Criticità 7**, credenziali di fabbrica esposte) insieme a tre criticità alte o medie (**Criticità 8, 9, 10**), tutte riportate nel registro del capitolo 9.

CAPITOLO 7 · LIVELLO 5

Configurazioni e aggiornamenti

Com'è tenuta la rete: versioni di firmware, configurazioni incoerenti, backup, accessi amministrativi, log e ora sincronizzata.

7.1 Versioni firmware e sistema

APPARATO	VERSIONE RILEVATA	STATO
Firewall PD	10.4.2	Aggiornato
Firewall BO	8.1.0	Due versioni maggiori indietro, aggiornamenti di sicurezza non applicati da oltre un anno
Core switch PD	17.6.3	Aggiornato
Core switch BO	17.3.1	Una versione indietro, nessun problema noto
Access point (entrambe le sedi)	varie	Non gestiti centralmente, versioni disallineate

Il ritardo sul firewall di Bologna è la criticità più rilevante di questo capitolo (**Criticità 11**).

7.2 Coerenza delle configurazioni

Le configurazioni dei due firewall sono divergenti oltre quanto giustificato dalle differenze tra le sedi: oggetti e regole sono stati rinominati manualmente nel tempo, senza una convenzione comune né un controllo di versione che permetta di confrontare le due configurazioni o tornare a uno stato precedente in caso di errore (**Criticità 12**).

7.3 Backup delle configurazioni

Padova dispone di un backup automatico giornaliero delle configurazioni degli apparati principali. A Bologna il backup è manuale e non regolare: l'ultima copia disponibile al momento del rilevamento risaliva a quattro mesi prima.

7.4 Log e sincronizzazione oraria

Gli apparati di Padova sincronizzano l'ora tramite un server NTP interno; a Bologna diversi switch e access point mantengono l'ora locale non sincronizzata. In caso di incidente che coinvolga entrambe le sedi, i log non sono correlabili con precisione temporale (**Criticità 13**).

7.5 Criticità rilevate a questo livello

Firmware disallineato (**Criticità 11**), configurazioni divergenti senza controllo di versione (**Criticità 12**) e assenza di sincronizzazione oraria (**Criticità 13**): dettagli nel registro del capitolo 9.

CAPITOLO 8 · LIVELLO 6

Affidabilità e continuità

Cosa succede quando qualcosa si rompe: comportamento sotto guasto, alimentazione, monitoraggio, tempi di ripristino.

8.1 Comportamento sotto guasto

SCENARIO	EFFETTO OSSERVATO O STIMATO
Interruzione della linea Internet di Bologna	Perdita del tunnel: nessun accesso a login, ERP, file, fonia con Padova. Operatività locale sospesa.
Interruzione della linea Internet di Padova	Padova isolata da Internet (nessun impatto sulla rete locale); Bologna perde il tunnel e quindi i servizi centrali.
Guasto del core switch di Padova	Fermo dell'intera sede: nessuna comunicazione inter-VLAN, inclusi i servizi della server room.
Guasto del firewall di una sede	Perdita di Internet e del tunnel per quella sede, senza apparato di riserva.

Lo scenario più critico è la dipendenza di Bologna dal tunnel per servizi essenziali come il login (**Criticità 14**), già evidenziata nelle interviste.

8.2 Alimentazione e continuità elettrica

La sala server di Padova dispone di un gruppo di continuità dimensionato per l'intera server room, con test semestrale documentato. A Bologna un gruppo di continuità più piccolo protegge solo il firewall e il core switch nella sala quadri; non risulta un test periodico né una verifica recente della sua autonomia reale (**Criticità 15**). L'accesso alla sala quadri di Bologna non è controllato: la porta resta abitualmente aperta durante l'orario di lavoro.

8.3 Monitoraggio e allarmi

Padova dispone di un sistema di monitoraggio attivo sui principali apparati, con notifica via email in caso di anomalia. Bologna non ha alcun monitoraggio: un guasto viene rilevato solo quando qualcuno se ne accorge sul posto.

8.4 Tempi di ripristino stimati

In assenza di ridondanza, i tempi di ripristino dipendono dalla disponibilità di un apparato sostitutivo e dall'intervento di un tecnico. Sulla base della configurazione attuale, un guasto hardware al firewall o al core switch di una sede comporta un fermo stimabile in alcune ore fino a un giorno lavorativo, tempi non garantiti in assenza di un contratto di assistenza con SLA dedicato.

8.5 Criticità rilevate a questo livello

Dipendenza di Bologna dai servizi centrali di Padova (**Criticità 14**) e continuità elettrica non verificata a Bologna (**Criticità 15**), entrambe nel registro del capitolo 9.

CAPITOLO 9

Registro consolidato delle criticità

Le quindici criticità rilevate nei capitoli precedenti, in un unico registro ordinato per livello.

#	GRAVITÀ	LIV.	AREA	SEDE	EVIDENZA
1	ALTO	L1	Inventario	Padova	Tre switch di reparto non censiti, installati senza documentazione né aggiornamento firmware.
2	BASSO	L1	Credenziali	Padova	Password amministrativa locale condivisa su un sottoinsieme di postazioni di produzione.
3	ALTO	L2	Instradamento	Entrambe	Il tunnel instrada l'intero /16 verso /16: un job di backup notturno satura la banda di Bologna anche di giorno.
4	MEDIO	L2	Ridondanza	Entrambe	Nessuna ridondanza sul collegamento Internet: un solo operatore, nessun failover.
5	MEDIO	L3	Wi-Fi	Entrambe	Copertura insufficiente in fondo al capannone (PD) e in magazzino (BO): disconnessioni dei terminali.
6	MEDIO	L3	Fonia	Entrambe	Nessuna priorità (QoS) sul tunnel: la voce peggiora durante i trasferimenti pesanti.
7	CRITICO	L4	Sicurezza perimetrale	Bologna	Un access point espone ancora le credenziali amministrative di fabbrica, raggiungibile dalla rete ospiti.
8	ALTO	L4	Sicurezza perimetrale	Bologna	Interfaccia di gestione del firewall raggiungibile da Internet senza restrizione di IP sorgente.
9	MEDIO	L4	Segmentazione	Padova	Nessuna regola tra VLAN Produzione e VLAN Server: accesso diretto a ERP e file server.
10	MEDIO	L4	VPN	Entrambe	Accesso VPN remoto con chiave precondivisa di gruppo, nessun certificato individuale né MFA.
11	MEDIO	L5	Aggiornamenti	Bologna	Firmware del firewall due versioni indietro, senza aggiornamenti di sicurezza da oltre un anno.
12	BASSO	L5	Gestione	Entrambe	Configurazioni dei due firewall divergenti, nessun controllo di versione.
13	BASSO	L5	Log	Bologna	Orologi non sincronizzati via NTP: log non correlabili con precisione tra le sedi.
14	ALTO	L6	Continuità	Entrambe	AD, DNS e file esistono solo a Padova: senza tunnel, Bologna resta senza login né documenti.

#	GRAVITÀ	LIV.	AREA	SEDE	EVIDENZA
15	BASSO	L6	Alimentazione	Bologna	Gruppo di continuità non testato periodicamente, autonomia reale non nota.

Distribuzione per gravità: 1 critica, 4 alte, 6 medie, 4 basse — 15 criticità complessive.

CAPITOLO 10 · LIVELLO 7

Piano di intervento

Cosa fare, in che ordine: criticità pesate per impatto, urgenza e sforzo; interventi rapidi separati da quelli strutturali.

10.1 Criteri di prioritizzazione

Ogni criticità è stata valutata secondo tre dimensioni qualitative — **impatto** sull'operatività o sulla sicurezza, **urgenza** nel tempo, **sforzo** necessario per intervenire — e collocata in uno dei due gruppi seguenti. Questo capitolo indica **cosa** andrebbe fatto e in quale ordine, non **come** realizzarlo né a quale costo: la progettazione di dettaglio e il relativo preventivo sono oggetto di un documento separato, senza impegno (§10.4).

10.2 Interventi rapidi

Basso sforzo, realizzabili nel giro di giorni o poche settimane, senza modifiche strutturali alla rete.

- 1 **Sostituire le credenziali di fabbrica** sull'access point interessato e isolarne la gestione dalla rete ospiti. → Criticità 7

- 2 **Restringere l'interfaccia di gestione del firewall di Bologna** a un elenco di indirizzi autorizzati. → Criticità 8

- 3 **Introdurre una regola dedicata tra Produzione e Server room**, con permessi limitati ai soli servizi necessari. → Criticità 9

- 4 **Differenziare la password amministrativa locale** sulle postazioni di produzione interessate. → Criticità 2

- 5 **Aggiornare il firmware del firewall di Bologna** all'ultima versione stabile. → Criticità 11

- 6 **Attivare la sincronizzazione oraria (NTP)** su switch e access point di Bologna. → Criticità 13

- 7 **Programmare un test dell'autonomia del gruppo di continuità** di Bologna. → Criticità 15

- 8 **Censire e mettere in sicurezza gli switch non documentati** del reparto produzione. → Criticità 1

10.3 Interventi strutturali

Richiedono progettazione, una finestra di intervento concordata e, in alcuni casi, un investimento in apparati: da pianificare nei mesi successivi, in ordine di impatto.

- 1 **Restringere e prioritizzare il traffico sul tunnel**: selettori di traffico dedicati per flusso, finestra di replica definita per il backup, priorità (QoS) per la voce. → Criticità 3, 6

-
- 2 **Dare a Bologna una copia funzionante dei servizi centrali:** attivazione del controller di dominio secondario già presente, sincronizzazione dei file di uso comune. → Criticità 14

 - 3 **Introdurre un secondo percorso Internet** per entrambe le sedi, con failover automatico. → Criticità 4

 - 4 **Estendere la copertura Wi-Fi** nelle due aree segnalate, con una verifica sul campo dopo l'intervento. → Criticità 5

 - 5 **Passare a certificati individuali e autenticazione a più fattori** per l'accesso VPN remoto. → Criticità 10

 - 6 **Allineare e portare sotto controllo di versione le configurazioni** dei due firewall, con backup automatico anche a Bologna. → Criticità 12

 - 7 **Introdurre un monitoraggio attivo** anche per la sede di Bologna. → §8.3
-

10.4 Nota sul preventivo

Il piano qui descritto stabilisce le priorità, non i dettagli realizzativi: prodotti, configurazioni specifiche, tempi di fornitura e costi sono oggetto di un preventivo a parte, elaborato solo su richiesta e senza alcun impegno per il cliente. La relazione di analisi — questo documento — è offerta gratuitamente per reti di questa dimensione; per contesti enterprise la relazione stessa può prevedere un costo, comunicato prima dell'avvio.

APPENDICE A

Legenda e criteri di gravità

CRITICO

Facilmente sfruttabile e con impatto esteso su sicurezza o operatività. Richiede intervento immediato.

ALTO

Impatto rilevante su sicurezza o continuità operativa. Intervento consigliato entro poche settimane.

MEDIO

Impatto limitato o condizioni aggravanti necessarie perché si manifesti. Pianificabile nei mesi successivi.

BASSO

Miglioramento consigliato per buona pratica. Nessuna urgenza operativa.

La gravità tiene conto sia della probabilità che una criticità causi un problema concreto, sia dell'estensione del danno se questo si verifica; non è una misura automatica, ma il giudizio di chi ha condotto l'analisi, spiegato caso per caso nel testo dei capitoli 3–8.

APPENDICE B

Strumenti utilizzati

- **Discovery e inventario di rete** — rilevamento automatico di apparati, sistemi operativi e servizi attivi da un nodo interno per sede.
- **Analizzatore di pacchetti** — cattura su porte mirror per le misure di prestazione e per la verifica del traffico sul tunnel.
- **Misura punto-punto di banda, latenza e perdita di pacchetti** — campagne ripetute in più fasce orarie tra le due sedi.
- **Analizzatore Wi-Fi portatile** — sopralluogo e mappatura del segnale nelle aree indicate.
- **Scanner di porte e servizi** — eseguito da postazione autorizzata, sugli indirizzi pubblici e sulle reti interne indicate nel mandato.
- **Accesso di sola lettura alle configurazioni** — fornito dal cliente per la durata dell'analisi, revocato alla consegna della relazione.

APPENDICE C

Riservatezza e validità della relazione

Questa relazione fotografa lo stato della rete nel periodo di rilevamento indicato in copertina. Configurazioni, apparati o criticità successivi a quella data non sono riflessi nel documento. È redatta per l'uso esclusivo del destinatario del mandato e non costituisce parere legale né garanzia di sicurezza assoluta: descrive quanto osservato con gli strumenti e nei tempi concordati, non esclude la presenza di criticità non rilevabili con questo livello di analisi.

La versione integrale di una relazione reale, comprensiva di indirizzi, configurazioni di dettaglio e dei nominativi coinvolti, è riservata e consegnata esclusivamente al cliente. **Questa è la versione dimostrativa**, pubblicata da BoNet come esempio del formato e del livello di dettaglio con cui viene condotta e restituita un'analisi di rete su sette livelli.

© BoNet™ — un progetto di Euro Buchberger · Padova, Veneto · bonet.tech
Tutti i diritti riservati.