Lavori di realizzazione di un sistema integrato di videocontrollo territoriale costituito da un sottosistema di videosorveglianza delle zone interessate e uno di riconoscimento automatico delle targhe dei veicoli in transito.

Progetto Vi.So.Re. Trevigiano

Security Target

Sottosistema Network Visore (SNV)

Versione 1.0

N.	Versione	Stato	Data	Autore	Approvato	Tipo di modifica
1	1.0	Rilasciato	09/12/2013	A.Mennini	A. Hummer	Prima Versione
2	1.1	Rilasciato	17/08/2015	A.Mennini	A. Hummer	Modifiche a seguito variazioni rispetto al progetto originale
3	1.2	Rilasciato	13/11/2015	A.Mennini	A. Hummer	Modifiche a seguito ROA n. 1
4	1.3	Rilasciato	15/12/2015	A.Mennini	A. Hummer	Modifiche a seguito ROA n. 2

Tabella 1 - Riepilogo delle modifiche

Riferimento per l'amministrazione di stato e versione:
Stato:
Elaborato ("Processed") il documento è in corso di elaborazione
Rilasciato ("Released") il documento è stato verificato e rilasciato dal controllo qualità; può essere modificato solo se viene aggiornato il numero di versione.
Versioni:
Presentano due fasi. I documenti accettati ricevono il successivo numero intero di versione.
00-01, 00-02 ecc. versioni non rilasciate, con stato **"Elaborato"**
01 prima versione rilasciata con stato **"Rilasciato"**
01-01, 01-02 ecc. versioni che integrano la versione 01-00 e hanno stato **"Elaborato"**
02 seconda versione rilasciata con stato **"Rilasciato"**

Copyright

Sommario

Indice delle tabelle

Indice delle figure

1. PREMESSA

Questo Security Target (ST) descrive gli obiettivi di sicurezza, i requisiti e le motivazioni del Sottosistema Network Vi.So.Re (SNV) del progetto Vi.So.Re. Trevigiano, di seguito chiamato ODV, progettato e realizzato dal RTI Kapsch TrafficCom s.r.l. con Infracom Italia S.p.A. (nel seguito anche semplicemente RTI).

1.1 OBIETTIVI DEL DOCUMENTO

Questo Security Target (ST) esprime i requisiti di sicurezza oggetto di valutazione del Sottosistema Network Vi.So.Re (SNV) nel seguito descritto.

Il sottosistema SNV è stato progettato e realizzato dal RTI Kapsch TrafficCom s.r.l. con Infracom Italia S.p.A.

Il committente della valutazione è Kapsch TrafficCom s.r.l..

L'ambito del ST, nel contesto del processo di valutazione è coerente con quanto previsto nei Common Criteria for Information Technology Security Evaluation [CC]. In particolare, un Security Target definisce i requisiti di sicurezza del sottosistema oggetto di valutazione e specifica le misure di sicurezza funzionali e di garanzia previste dall'ODV nel contesto dei requisiti definiti nei Common Criteria.

1.2 STRUTTURA DEL DOCUMENTO

Il Security Target contiene le seguenti sezioni:

- **Descrizione dell'ODV [Rif. § 2]:** questa sezione fornisce una descrizione dell'ODV, ne fornisce le caratteristiche e ne definisce l'ambito.
- **Dichiarazione di Conformità [Rif. § 3]:** questa sezione presenta le conformità con i Common Criteria.
- **Obiettivi di sicurezza [Rif. § 4]:** questa sezione descrive in maniera dettagliata gli obiettivi di sicurezza dell'ambiente operativo dell'ODV.
- **Definizione di Componenti Estese [Rif. § 5]: q**uesta sezione definisce e giustifica l'utilizzo di componenti estese.
- **Requisiti di sicurezza [Rif. § 6]:** questa sezione definisce i Security Functional Requirements (SFR) ed i Security Assurance Requirements (SAR) per l'ODV.
- **Specifiche sommarie [Rif. § 7]:** questa sezione descrive le funzioni di sicurezza dell'ODV che soddisfano i requisiti di sicurezza.

1.3 ACRONIMI

ACL	Access Control List
CC	Common Criteria
EAL	Evaluation Assurance Level
HA	High Availability
HIPERLAN	HIgh PErformance Radio LAN
IT	Information Technology
MPLS	Multi Protocol Label Switching
ODV	Oggetto Della Valutazione

PC	Personal Computer
PP	Protection Profile
RTI	RTI Kapsch TrafficCom s.r.l. con Infracom Italia S.p.A.
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SLT	Sottosistema di Lettura Targhe
SNV	Sottosistema Network Vi.So.Re.
ST	Security Target
ST	Security Target
SVC	Sottosistema Videosorveglianza Comunale
TOE	Target Of Evaluation
TSF	TOE Security Function
TSFI	TSF Interface
VPN	Virtual Private Network

Tabella 1 - Acronimi

2. INTRODUZIONE AL SECURITY TARGET (ASE_INT)

2.1 IDENTIFICAZIONE DEL SECURITY TARGET

Titolo: Security Target Sottosistema Network Vi.So.Re (SNV) v. 1.0

Versione del ST: 1.3

Data : 15/12/2015

2.2 IDENTIFICAZIONE DELL'ODV

Nome del prodotto: Sottosistema Network Vi.So.Re v. 1.0

2.3 PANORAMICA DELL'ODV

Il SNV è il sottosistema del progetto Vi.So.Re. che fornisce ai sottosistemi SVC e SLT il transito protetto dei dati. SNV è costituito per quasi tutto il suo sviluppo, da rete con tecnologia wireless ed IP.
La rete dati Vi.So.Re. si compone di tre parti fondamentali:

- rete di backbone o dorsale
  La rete di backbone è composta da una magliatura di ponti radio, su frequenza licenziata, il cui "centro stella" è il datacenter di Oderzo, certificato ISO/IEC:27001. Per garantire i vincoli di disponibilità del servizio, si è realizzata una architettura costituita da anelli logici che sono funzionali ad una ridondanza del collegamento in modo tale che i servizi sottesi non subiscano interruzioni nell'eventualità che un percorso di collegamento sia non disponibile. La rete è basata su logiche derivanti dal protocollo MPLS, che, rispetto ad una implementazione classica, permette di passare ad uno schema di erogazione dei servizi che in letteratura viene definito di tipo N:N.

- rete di raccolta locale geograficamente localizzata in ogni comune
  E' la rete di distribuzione che a partire dal backbone si ramifica nelle varie sedi comunali servite da SLT e SVC; è realizzata tramite tecnologia wireless Hiperlan. Anche in questo caso l'architettura prevede la realizzazione di anelli logici, ove possibile.
  Per ogni sito in cui sono presenti delle telecamere, è realizzata una sottorete dedicata a SLT e incapsulata in una specifica VPN SLT ed una sottorete dedicata a SVC e incapsulata nella specifica VPN SVC; inoltre le reti SLT e SVC sono fisicamente separate in quando sono dedicati apparati distinti per la terminazione delle VPN SLT e VPN SVC. In particolare presso il data center di Oderzo è installata una coppia di firewall in HA (High Availability) che termina le VPN SVC, mentre le VPN SLT sono terminate presso le forze della Polizia (Questura), come di seguito descritto. Le VPN SVC/SLT sono VPN IP Sec AES-128.

- rete di collegamento verso le Forze di Polizia

  La rete di collegamento alle Forze di Polizia è realizzata da tratte su portante fisica in fibra ottica. Presso le forze di Polizia (Questura) è installata una coppia di firewall in HA (High Availability) che termina le VPN SLT. Le VPN SLT sono VPN IP Sec AES-128.

  Inoltre, presso le altre sedi delle Forze di Polizia è installato un firewall che comunica con i server contenenti i dati del sistema di lettura targhe attraverso una VPN IP Sec AES-128.

2.3.1 DESCRIZIONE FLUSSI SVC E SLT

SOTTOSISTEMA SVC

Il Sottosistema di Videosorveglianza Comunale (SVC) è una componente del più ampio progetto Vi.So.Re, ed opera nell'ambito di iniziali 27 comuni della provincia di Treviso ed ha la finalità di prevenire attività di microcriminalità, atti vandalici, incendi dolosi, rilevare e ricostruire eventi criminosi. Il sottosistema SVC prevede un certo numero di telecamere installate in siti critici di diversi comuni, collegate con posti di visualizzazione/controllo mediante il sottosistema di comunicazione SNV. Ogni telecamera SVC accede alla rete SNV tramite un collegamento ethernet fino al relativo firewall. Il traffico viene successivamente incapsulato su una VPN IPSEC, VPN SVC, e, tramite un collegamento wireless hiperlan, trasportato fino al punto di raccolta comunale, e, successivamente, tipicamente con uno o più collegamenti in ponte radio, fino ai firewall dedicati in Data Center di Oderzo. Segue lo schema di dettaglio logico (VPN SVC) e il dettaglio del trasporto.

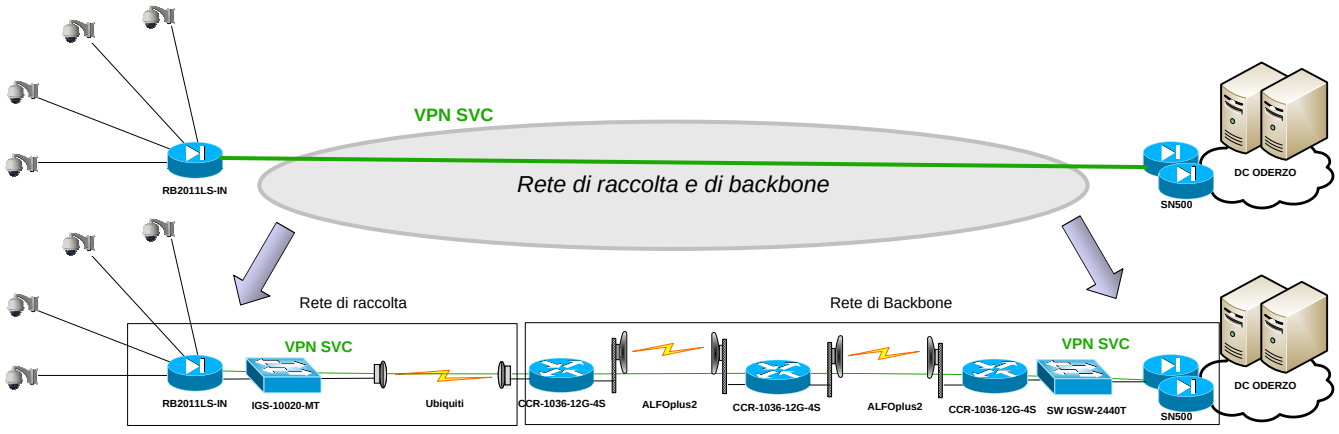


Figura 1 - Schema di dettaglio logico VPN SVC

SOTTOSISTEMA SLT

Il Sottosistema di Lettura Targhe (SLT) è una componente del più ampio progetto Vi.So.Re, ed opera opera lungo i principali nodi stradali nell'ambito di 12 comuni iniziali della provincia di Treviso ed ha la finalità di effettuare la lettura delle targhe e rilevare l'immagine di contesto dei veicoli in transito così da consentire la segnalazione del transito alle forze di Polizia dello Stato territoriali e al SCNTT. Il sottosistema SLT prevede un certo numero di telecamere installate presso i principali nodi stradali dei comuni interessati, collegate con posti di visualizzazione/controllo e il sistema centrale di elaborazione (SCE) mediante il sottosistema di comunicazione SNV. Ogni telecamera SLT accede alla rete SNV tramite un collegamento ethernet fino al firewall di appartenenza. Il traffico viene successivamente incapsulato su una VPN IPSEC, VPN SLT, e, tramite un collegamento wireless hiperlan, trasportato fino al punto di raccolta comunale, e, successivamente, tipicamente con uno o più collegamenti in ponte radio e su portante in fibra ottica fino ai firewall dedicati in Data Center Questura.

Segue lo schema di dettaglio logico (VPN SLT) e il dettaglio del trasporto.

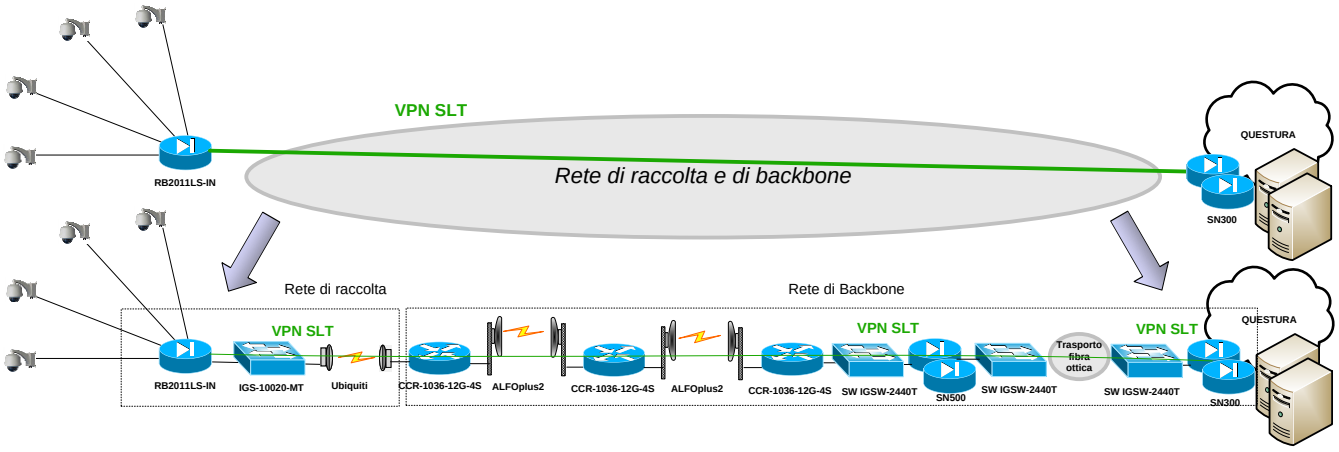


Figura 2 - Schema di dettaglio logico VPN SLT

Inoltre presso le altre sedi delle Forze di Polizia è installato un firewall modello Mikrotik RB2011LS-IN che comunica con i server contenenti i dati del sistema di lettura targhe presenti in Questura attraverso una VPN IP.

2.4 DESCRIZIONE DELL'ODV

L'ODV è costituito dalle VPN configurate sui firewall dei due sottosistemi SLT e SVC.

2.4.1 AMBITO FISICO

Si precisa che il servizio erogato dalla rete del sottosistema SNV nelle sue componenti (backbone, raccolta locale e collegamento alle forze di polizia) sono le VPN SVC/SLT; tali VPN sono instaurate/terminate fra i firewall locali

direttamente collegati alle telecamere e i firewall presso il data center di Oderzo e le forze di Polizia (Questura). Gli altri apparati del sistema SNV, ovvero ponti radio, link wireless Hiperlan, router, switch, collegamenti in fibra ottica, eseguono solo funzionalità di trasporto dei dati delle VPN SVC/SLT. Pertanto l'ambito fisico dell'ODV è costituito dalle configurazioni stabilite all'installazione del sistema fra le seguenti apparecchiature (firewall):

- 2 Stormshield SN500 in HA per le terminazione su Oderzo (sottosistema SVC)
- 2 Stormshield SN300 in HA per la terminazione sulla Questura di Treviso (sottosistema SLT)
- 1 Microtik RB2011LS-IN per ogni sito di raccolta delle immagini dalle telecamere (sottosistema SVC)
- 1 Microtik RB2011LS-IN per ogni sito di raccolta delle sistema SLT (sottosistema SLT).

2.4.2 AMBITO LOGICO

Come già indicato in premessa, il servizio erogato dalla rete del sottosistema SNV nelle sue componenti (backbone, raccolta locale e collegamento alle forze di polizia) sono le VPN SVC/SLT; tali VPN sono terminate/instaurate fra i firewall locali direttamente collegati alle telecamere e i firewall presso il data center di Oderzo e le forze di Polizia (Questura). Gli altri apparati del sottosistema SNV, ovvero ponti radio, link wireless Hiperlan, router, switch, collegamenti in fibra ottica, eseguono solo funzionalità di trasporto dei dati delle VPN SVC/SLT. **L'ambito logico dell'ODV è rappresentato dalle funzioni di separazione e di indipendenza delle VPN dedicate ai sottosistemi SVC e SLT.**

2.5 AMBIENTE OPERATIVO

COMPONENTI DEL BACKBONE

La rete di backbone utilizza:

- ponti radio PDH su frequenza licenziata, produttore SIAE MICROELETTRONICA, modello ALfoPlus2
- router Mikrotik Routerboard CCR1036-12G-4S
- switch Planet SW IGSW-2440T

completano la rete di backbone i firewall di terminazione delle VPN SVC e SLT:

- n° 2 Firewall Stormshield SN500 in HA
- n° 2 Firewall Stormshield SN300 in HA

COMPONENTI RETE RACCOLTA COMUNI

La rete di raccolta che collega i nodi di backbone ai siti comunali utilizza apparati wireless Ubiquiti:

- NanoBridge M5
- Rocket M5
- Nanostation LOCO

Su ognuno dei siti a supporto dei sottosistemi SVC/SLT sono presenti:

- uno switch industriale Planet IGS-10020-MT
- due router/firewall, Mikrotik RB2011LS-IN: uno per garantire la privacy-by-design della parte SVC ed uno per garantire la privacy-by-design della parte SLT. Su tali apparati, come precedentemente descritto, sono terminate le VPN SVC e SLT

COMPONENTI COLLEGAMENTO FORZE DI POLIZIA

Presso le altre sedi delle Forze di Polizia è installato un firewall modello Mikrotik RB2011LS-IN che comunica con i server contenenti i dati del sistema di lettura targhe attraverso una VPN IP.

2.6 RUOLI UTENTE

Non sono previsti ruoli utente per l'ODV, in quanto la gestione e l'amministrazione dell'ODV è di esclusiva pertinenza dell'ambiente IT, che controlla il sottosistema SNV attraverso le figure di Amministratore e di Gestore:

- Amministratore - Gli utenti con ruolo "Amministratore" possono accedere alle funzioni di configurazione degli apparati di rete del sottosistema SNV.
- Gestore - Gli utenti con il ruolo "Gestore" sono gli operatori addetti alla gestione del sottosistema SNV e hanno le credenziali in sola lettura per accedere agli apparati di rete.

Anche l'identificazione e la autenticazione degli utenti Amministratore e Gestore è a carico dell'ambiente operativo.

2.7 FUNZIONI DI SICUREZZA

La tabella seguente mostra le funzioni di sicurezza dell'ODV.

Codice	Funzione di sicurezza	Descrizione
ODV_COM	**Secure Communication**	L'ODV garantisce la protezione del traffico dati, attraverso l'implementazione di VPN dedicate che realizzano l'indipendenza e la separazione dei flussi dei sottosistemi SVC e SLT.

Tabella 2 - Funzioni di sicurezza dell'ODV

3. DICHIARAZIONE DI CONFORMITA' (ASE_CCL)

Il ST e l'ODV sono conformi alla versione 3.1 (Revision 4) of the Common Criteria for Information Technology Security Evaluation.

La dichiarazione di conformità si riferisce a:

- Common Criteria for Information Technology Security Evaluation. Version 3.1 Rev.4 Part 1 september 2012
- Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, Version 3.1 Rev. 4 september 2012
- Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, Version 3.1 Rev. 4 september 2012

Il pacchetto di garanzia dichiarato è EAL1.

Questo ST non dichiara la conformità ad alcun Protection Profile.

Questo ST non prevede l'utilizzo di componenti estese.

4. OBIETTIVI DI SICUREZZA (ASE_OBJ)

In linea con quanto previsto dal livello di garanzia EAL1, il paragrafo contiene definizioni concise degli obiettivi che devono essere soddisfatti dall'ambiente a supporto dell'ODV.

4.1 OBIETTIVI DI SICUREZZA PER L'AMBIENTE OPERATIVO

Obiettivo	Descrizione
OE.Admin	L'amministrazione dell'ODV rientra nelle attività previste per la gestione del sottosistema SNV, rispettando le regole di distribuzione delle responsabilità stabilite. Tutto il personale indirettamente coinvolto nella gestione dell'ODV deve essere scelto tra personale fidato e addestrato alla corretta gestione dell'ODV.
OE.Physical	I responsabili dell'ODV devono assicurare che l'infrastruttura tecnologica dell'ODV sia custodita in locali nei quali l'accesso è consentito solamente al personale autorizzato.
OE.Identif	L'ambiente dell'ODV deve provvedere alla identificazione e autenticazione degli utenti Amministratore, in modo da disciplinare l'accesso alle apparecchiature del sottosistema SNV, limitandolo a utenti validi ed in base alle funzioni operative stabilite, oltre che di tenere traccia degli accessi degli utenti stessi. Devono essere implementate politiche di gestione della password (scadenza, complessità, non ripetibilità).

Tabella 3 - Obiettivi di sicurezza per l'ambiente

5. DEFINIZIONE DI COMPONENTI ESTESE (ASE_ECD)

Questo ST non definisce alcuna componente estesa.

6. REQUISITI DI SICUREZZA (ASE_REQ)

6.1 GENERALITA'

Questa sezione definisce i requisiti di sicurezza e di garanzia soddisfatti dall'ODV.

Ogni requisito è stato estratto dai Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, Version 3.1 Rev. 4 september 2012 e dai Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, Version 3.1 Rev. 4 september 2012.

6.2 CONVENZIONI

Il presente documento utilizza le seguenti convenzioni:

Assegnazione L'operazione di assegnazione consente di specificare un parametro all'interno di un requisito. Le assegnazioni sono indicate usando un testo in grassetto all'interno di parentesi quadre **[assegnazione]**.

Iterazione L'operazione di iterazione permette di utilizzare più di una volta un componente per effettuare operazioni diverse. Una iterazione si effettua ponendo uno slash "/" alla fine del componente seguito da un unico nome che identifica l'iterazione.

6.3 REQUISITI FUNZIONALI DI SICUREZZA

Functional Requirements		
Classes	**Families**	**Description**
FDP: User data protection	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
	FDP_ITC.1	Import of user data without security attributes
	FDP_ETC.1	Export of user data without security attributes

Tabella 4 - ODV Security Functional Requirements

6.4 DETTAGLIO DEI REQUISITI FUNZIONALI

FDP_IFC.1/SLT	
Hierarchical to:	No other components.
FDP_IFC.1.1	The TSF shall enforce [**regole di flusso**] on: [**Soggetti: componenti del sottosistema SLT che inviano dati attraverso l'ODV** **Informazioni: dati identificativi dei pacchetti in transito** **Operazioni: instradamento dei flussi SLT**].
Dependencies:	FDP_IFF.1 Simple security attributes
Notes:	

FDP_IFF.1/SLT	
Hierarchical to:	No other components.
FDP_IFF.1.1	The TSF shall enforce the [**regole di flusso**] based on the following types of subject and information security attributes: [**Attributi di sicurezza dei soggetti: indirizzo IP** **Attributi di sicurezza delle informazioni: indirizzo IP del destinatario e indirizzo IP del sorgente**].
FDP_IFF.1.2	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **[gli indirizzi IP del sorgente e del destinatario devono essere quelli appartenenti alla VPN SLT].**
FDP_IFF.1.3	The TSF shall enforce the [**none**].
FDP_IFF.1.4	The TSF shall explicitly authorise an information flow based on the following rules: [**none**].
FDP_IFF.1.5	The TSF shall explicitly deny an information flow based on the following rules: [**none**].
Dependencies:	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation
Notes:	

FDP_ITC.1/SLT	
Hierarchical to:	No other components.
FDP_ITC.1.1	The TSF shall enforce the [**regole di flusso**] when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.1.2	The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.
FDP_ITC.1.3	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [**none**]
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialisation
Notes:	

FDP_ETC.1/SLT	
Hierarchical to:	No other components.
FDP_ETC.1.1	The TSF shall enforce the [**regole di flusso**] when exporting user data, controlled under the SFP, from outside of the TOE.
FDP_ETC.1.2	The TSF shall export the user data without the user data's associated security attributes.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
Notes:	

FDP_IFC.1/SVC	
Hierarchical to:	No other components.
FDP_IFC.1.1	The TSF shall enforce [**regole di flusso**] on: [**Soggetti: componenti del sottosistema SVC che inviano dati attraverso l'ODV** **Informazioni: dati identificativi dei pacchetti in transito** **Operazioni: instradamento dei flussi SVC**

	].
Dependencies:	FDP_IFF.1 Simple security attributes
Notes:	

FDP_IFF.1/SVC	
Hierarchical to:	No other components.
FDP_IFF.1.1	The TSF shall enforce the [**regole di flusso**] based on the following types of subject and information security attributes: [**Attributi di sicurezza dei soggetti: indirizzo IP** **Attributi di sicurezza delle informazioni: indirizzo IP del destinatario e indirizzo IP del sorgente**].
FDP_IFF.1.2	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **[gli indirizzi IP del sorgente e del destinatario devono essere quelli appartenenti alla VPN SVC].**
FDP_IFF.1.3	The TSF shall enforce the [**none**].
FDP_IFF.1.4	The TSF shall explicitly authorise an information flow based on the following rules: [**none**].
FDP_IFF.1.5	The TSF shall explicitly deny an information flow based on the following rules: [**none**].
Dependencies:	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation
Notes:	

FDP_ITC.1/SVC	
Hierarchical to:	No other components.
FDP_ITC.1.1	The TSF shall enforce the [**regole di flusso**] when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.1.2	The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [**none**]
Dependencies:	[FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialisation
Notes:	

FDP_ETC.1/SVC	
Hierarchical to:	No other components.
FDP_ETC.1.1	The TSF shall enforce the [**regole di flusso**] when exporting user data, controlled under the SFP, from outside of the TOE.
FDP_ETC.1.2	The TSF shall export the user data without the user data's associated security attributes.
Dependencies:	[FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control]
Notes:	

6.5 REQUISITI DI GARANZIA

I requisiti di garanzia per l'ODV sono quelli previsti al livello EAL1, come specificato nella Parte 3 dei Common Criteria, senza potenziamenti.

EAL1 è stato scelto come livello di garanzia in quanto l'ODV opererà in un ambiente segregato e dedicato, con amministratori competenti e con utenti specializzati e fidati.

Assurance Class	Assurance components
ADV: Development	ADV_FSP.1 Basic functional specification
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE
	ALC_CMS.1 TOE CM coverage

Assurance Class	Assurance components
ATE: Tests	ATE_IND.1 Independent testing - conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey
ASE: Security Target Evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.1 Security objectives
	ASE_REQ.1 Stated security requirements
	ASE_TSS.1 TOE summary specification

Tabella 5 - Security Assurance Requirements

ADV_FSP.1 Basic functional specification

Dependencies:

None.

Developer action elements:

ADV_FSP.1.1D The developer shall provide a functional specification.

ADV_FSP.1.2D The developer shall provide a tracing from the functional specification to the SFRs.

AGD_OPE.1 Operational user guidance

Dependencies:

ADV_FSP.1 Basic functional specification

Developer action elements:

AGD_OPE.1.1D The developer shall provide operational user guidance.

AGD_PRE.1 Preparative procedures

Dependencies:

None.

Developer action elements:

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

ALC_CMC.1 Labeling of the TOE

Dependencies:

ALC_CMS.1 TOE CM coverage

Developer action elements:

ALC_CMC.1.1D The developer shall provide the TOE and a reference for the TOE.

ALC_CMS.1 TOE CM coverage

Dependencies:

None.

Developer action elements:

ALC_CMS.1.1D The developer shall provide a configuration list for the TOE.

ASE_INT.1 ST introduction

Dependencies:

None.

Developer action elements:

ASE_INT.1.1D The developer shall provide an ST introduction.

ASE_CCL.1 Conformance claims

Dependencies:

ASE_INT.1 ST introduction

ASE_ECD.1 Extended components definition

ASE_REQ.1 Stated security requirements

Developer action elements:

ASE_CCL.1.1D The developer shall provide a conformance claim.

ASE_CCL.1.2D The developer shall provide a conformance claim rationale.

ASE_OBJ.1 Security objectives for the operational environment

Dependencies:

None.

Developer action elements:

ASE_OBJ.1.1D The developer shall provide a statement of security objectives.

ASE_ECD.1 Extended components definition

Dependencies:

No dependencies.

Developer action elements:

ASE_ECD.1.1D The developer shall provide a statement of security requirements.

ASE_ECD.1.2D The developer shall provide an extended components definition.

ASE_REQ.1 Stated security requirements

Dependencies:

ASE_ECD.1 Extended components definition

Developer action elements:

ASE_REQ.1.1D The developer shall provide a statement of security requirements.

ASE_REQ.1.2D The developer shall provide a security requirements rationale.

ASE_TSS.1 TOE summary specification

Dependencies:

ASE_INT.1 ST introduction

ASE_REQ.1 Stated security requirements

ADV_FSP.1 Basic functional specification

Developer action elements:

ASE_TSS.1.1D The developer shall provide a TOE summary specification.

ATE_IND.1 Independent testing - conformance

Dependencies:

ADV_FSP.1 Basic functional specification

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

Developer action elements:

ATE_IND.1.1D The developer shall provide the TOE for testing.

AVA_VAN.1 Vulnerability survey

Dependencies:

ADV_FSP.1 Basic functional specification

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

Developer action elements:

AVA_VAN.1.1D The developer shall provide the TOE for testing.

6.6 ANALISI DELLE DIPENDENZE

La seguente tabella mostra le dipendenze richieste dai Common Criteria per ogni SFR e SAR a livello di garanzia EAL1.

Functional Requirements	Dipendenze richieste dai CC	Dipendenze soddisfatte
SFR		
FDP_IFC.1/SLT	FDP_IFF.1 Simple security attributes	FDP_IFF.1/SLT
FDP_IFF.1/SLT	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation	FDP_IFC.1/SLT **NOTA 1**
FDP_ITC.1/SLT	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialisation	FDP_IFC.1/SLT **NOTA 1**
FDP_ETC.1/SLT	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FDP_IFC.1/SLT
FDP_IFC.1/SVC	FDP_IFF.1 Simple security attributes	FDP_IFF.1/SVC
FDP_IFF.1/SVC	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation	FDP_IFC.1/SVC **NOTA 1**
FDP_ITC.1/SVC	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialisation	FDP_IFC.1/SVC **NOTA 1**
FDP_ETC.1/SVC	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FDP_IFC.1/SVC
SAR		
ADV_FSP.1	None	None

Functional Requirements	Dipendenze richieste dai CC	Dipendenze soddisfatte
AGD_OPE.1	ADV_FSP.1 Basic functional specification	ADV_FSP.1 Basic functional specification
AGD_PRE.1	None	None
ALC_CMC.1	ALC_CMS.1 TOE CM coverage	ALC_CMS.1 TOE CM coverage
ALC_CMS.1	None	None
ATE_IND.1	ADV_FSP.1 Basic functional specification AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures	ADV_FSP.1 Basic functional specification AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures
AVA_VAN.1	ADV_FSP.1 Basic functional specification AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures	ADV_FSP.1 Basic functional specification AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures

Tabella 6 - Analisi delle dipendenze

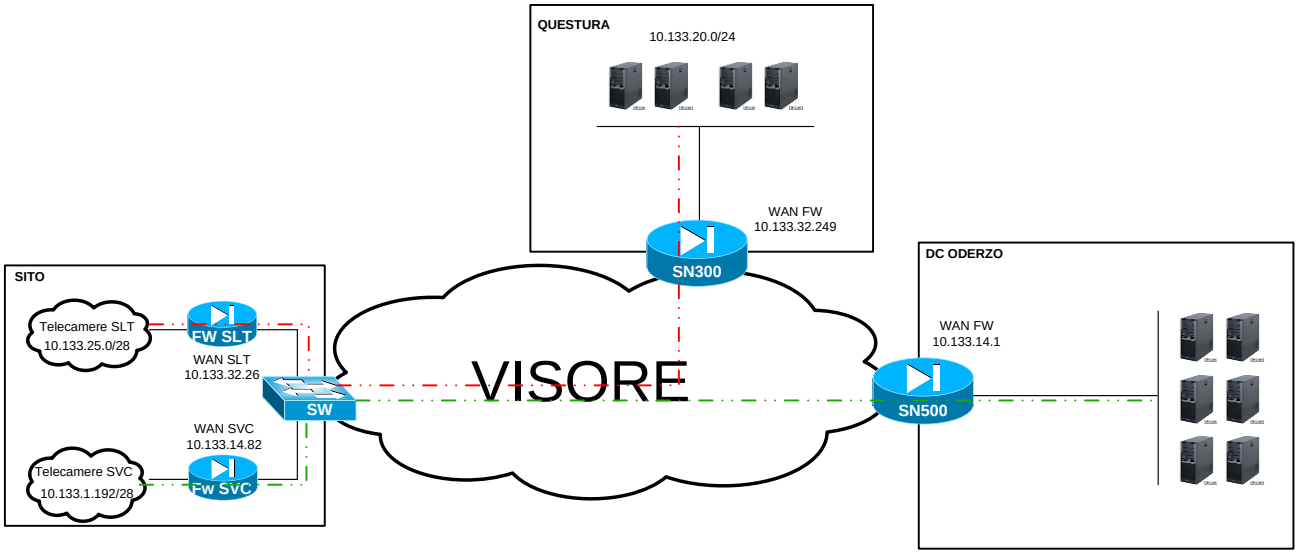
NOTA 1 – La dipendenza FMT_MSA.3, richiesta da FDP_IFF.1/SLT, da FDP_ITC.1/SLT, da FDP_IFF.1/SVC e da FDP_ITC.1/SVC, non è rispettata in quanto i valori degli attributi di sicurezza sono assegnati all'inizializzazione del sistema dall'ambiente operativo.

7. SPECIFICHE SOMMARIE (ASE_TSS)

Questa sezione fornisce le specifiche sommarie dell'ODV, una definizione ad alto livello delle funzioni di sicurezza che soddisfano i requisiti funzionali e di garanzia.

ODV_COM – SECURE COMMUNICATION

L'ODV implementa due VPN dedicate SLT e SVC che 'nascono' da apparati Mikrotik RB2011LS-IN distinti, da subnet distinte e sono terminate su apparati Stormshield SN300 e SN500 distinti. Nello scherma seguente si evidenzia la separazione delle VPN SLT e SVC, così come realizzata dall'ODV (tratteggio ROSSO e tratteggio VERDE).



L'ODV gestisce specifiche regole di flusso tramite le quali collega logicamente le componenti dei sistemi SVC e SLT. I collegamenti logici così realizzati dall'ODV garantiscono la separazione dei flussi tra le componenti dei due sottosistemi SVC e SLT mediante operazioni di instradamento tra l'IP del sorgente e quello del destinatario dei pacchetti in transito. L'ODV si occupa, secondo le regole di flusso definite, del trasporto (ricezione e consegna) delle informazioni delle componenti dei due sistemi SVC e SLT senza tener conto di attributi di sicurezza.

Queste operazioni realizzano le SFR **FDP_IFC.1/SLT, FDP_IFF.1/SLT, FDP_ITC.1/SLT, FDP_ETC.1/SLT, FDP_IFC.1/SVC, FDP_IFF.1/SVC, FDP_ITC.1/SVC, FDP_ETC.1/SVC**.