

Sicurezza per il Data Center basato sul Software Define Networking (SDN)

Alessandro Mauceri

Borsista GARR Bando 01/15 presso l'INFN di Catania

Tutor Dr. Giuseppe Andronico



7° Borsisti Day

20/01/2016

Roma – Consortium GARR



Indice

- Obiettivi della ricerca
- Organizzazione del lavoro da svolgere
- Programma temporale dell'attività

Obiettivi della ricerca

- Utilizzare SDN per affrontare problemi di sicurezza all'interno di un infrastruttura come quella della Sezione INFN di Catania
- Garantire la continuità di servizio e prevenire la perdita e modifica dei dati
- Definire e prototipare funzioni virtuali di sicurezza, quali firewall, DPI, IDS/IPS ecc..
- Studiare architetture gerarchiche e distribuite al fine di applicare le soluzioni in modo scalabile a reti di dimensioni più grandi

Organizzazione del lavoro (1)

- Studio e approfondimento del tema proposto
 - Sicurezza nei Data Center
 - Approfondimento Software Defined Networking (SDN)
 - Approfondimento Network Function Virtualization (NFV)



Organizzazione del lavoro (1)

- Studio e approfondimento del tema proposto
 - **Sicurezza nei Data Center**
 - attacchi DoS, DDoS
 - tentativi di accesso non autorizzati
 - applicazioni dannose
 - port scanning
 - Approfondimento Software Defined Networking (SDN)
 - Approfondimento Network Function Virtualization (NFV)



Organizzazione del lavoro (1)

- Studio e approfondimento del tema proposto

- Sicurezza nei Data Center

- **Approfondimento Software Defined Networking (SDN)**

- Comprensione di come SDN potrebbe migliorare le condizioni di sicurezza nella rete

- Approfondimento Frameworks di Sviluppo (i.e. OpenDayLight)

- Approfondimento Network Function Virtualization (NFV)



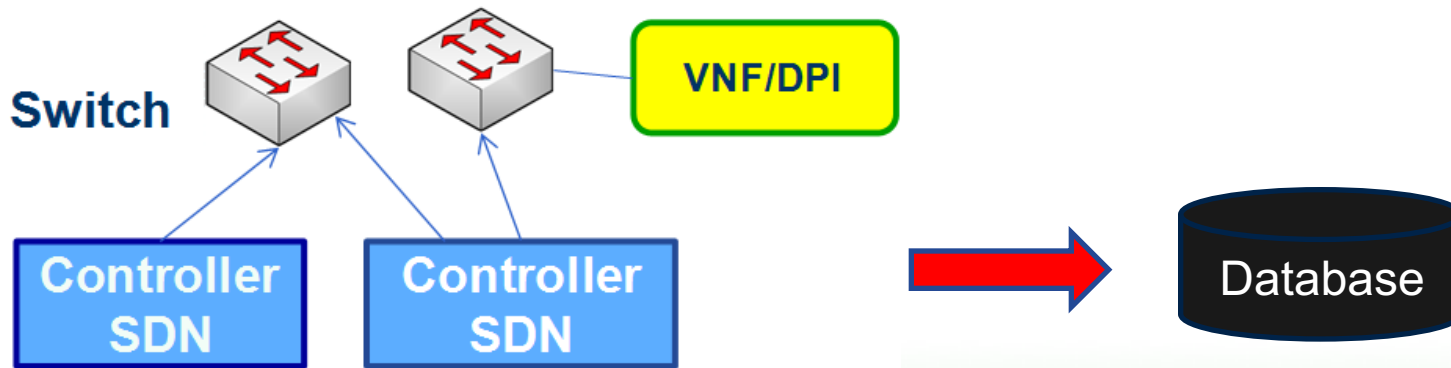
Organizzazione del lavoro (1)

- Studio e approfondimento del tema proposto
 - Sicurezza nei Data Center
 - Approfondimento Software Defined Networking (SDN)
 - **Approfondimento Network Function Virtualization (NFV)**
 - Comprensione di come definire e prototipare funzioni virtuali di sicurezza, quali firewall, DPI, IDS/IPS ecc..



Organizzazione del lavoro (2)

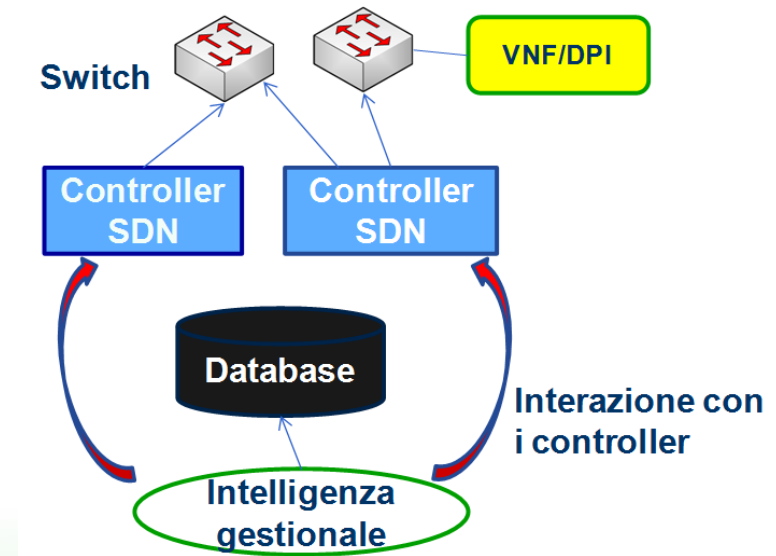
- Complementare i sistemi di sicurezza usando SDN
 - Correlare le informazioni rese accessibili da SDN con dati che provengono da altri sistemi di monitoraggio della rete
 - Comprendere quali politiche implementare per contenere le azioni che creano maggior disturbo



Organizzazione del lavoro (3)

- Reazioni proattive basate su SDN

- Comprensione di come utilizzare un controller SDN per reagire all'insorgere di problemi noti sulla rete
- Implementazione controller SDN



Organizzazione del lavoro (4)

- Partizionamento firewall
 - Studio di soluzioni basate su SDN e NFV che permettono dinamicamente di virtualizzare e allocare i firewall in modo opportuno
 - Implementazione di firewall virtuali ad hoc da fornire a tenant OpenStack o VLAN dipartimentali
- Studio della latenza, eventualmente, introdotta da SDN e NFV

Programma temporale dell'attività

ID	ATTIVITA'	1° ANNO & MESI											
		1	2	3	4	5	6	7	8	9	10	11	12
1	Studio e approfondimento del tema proposto												
1.1	Approfondimento sicurezza Data Center												
1.2	Approfondimento SDN												
1.3	Approfondimento NFV												
2	Complementare i sistemi di sicurezza utilizzando SDN												
2.1	Correlare le informazioni rese accessibili da SDN con dati provenienti da altri sistemi di monitoraggio della rete												
2.2	Comprendere quali politiche implementare per contenere le azioni che creano maggior disturbo												
3	Reazioni proattive												
3.1	Comprensione di cosa può offrire un controller SDN, in termine di reazioni automatiche												
3.2	Implementazione controller SDN												
4	Partizionamento firewall												
4.1	Studio di soluzioni basate su SDN e NFV												
4.2	Sviluppare dei firewall virtuali ad hoc da fornire a tenant OpenStack o VLAN dipartimentali												
5	Latenza introdotta da SDN e NFV												

Grazie per l'attenzione!

Domande

