NAeS Consulting SRL

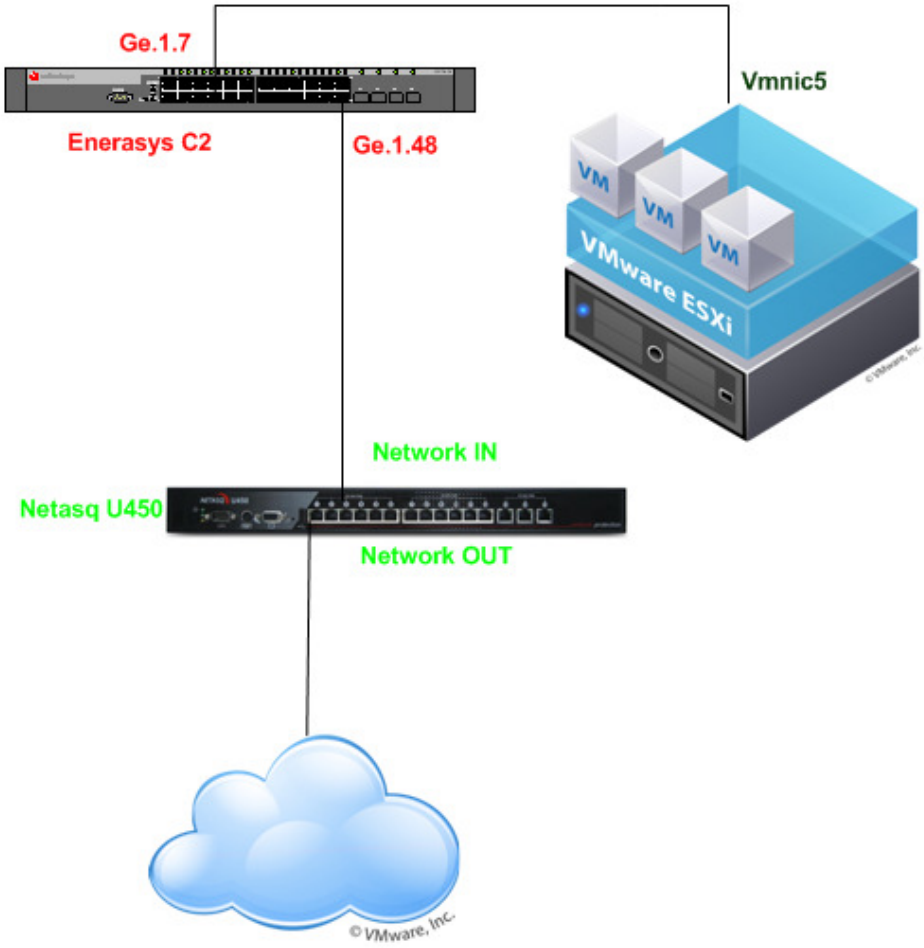
Costruire una sonda a basso costo

Versione V1

Ing . Jacopo Saladini
18/05/2012

Introducendo la virtualizzazione molte aziende hanno dismesso dei server, questi possono essere recuperati e trasformati in sonde a basso costo . L'idea è quella di installare su questi server ESXi e Cascade Virtual Shark e collegare le porte fisiche del server virtuale a porte in mirroring dello switch. In questo esempio l'obbiettivo è analizzare il traffico della porta collegata all'interfaccia in del firewall con Cascade Virtual Shark.

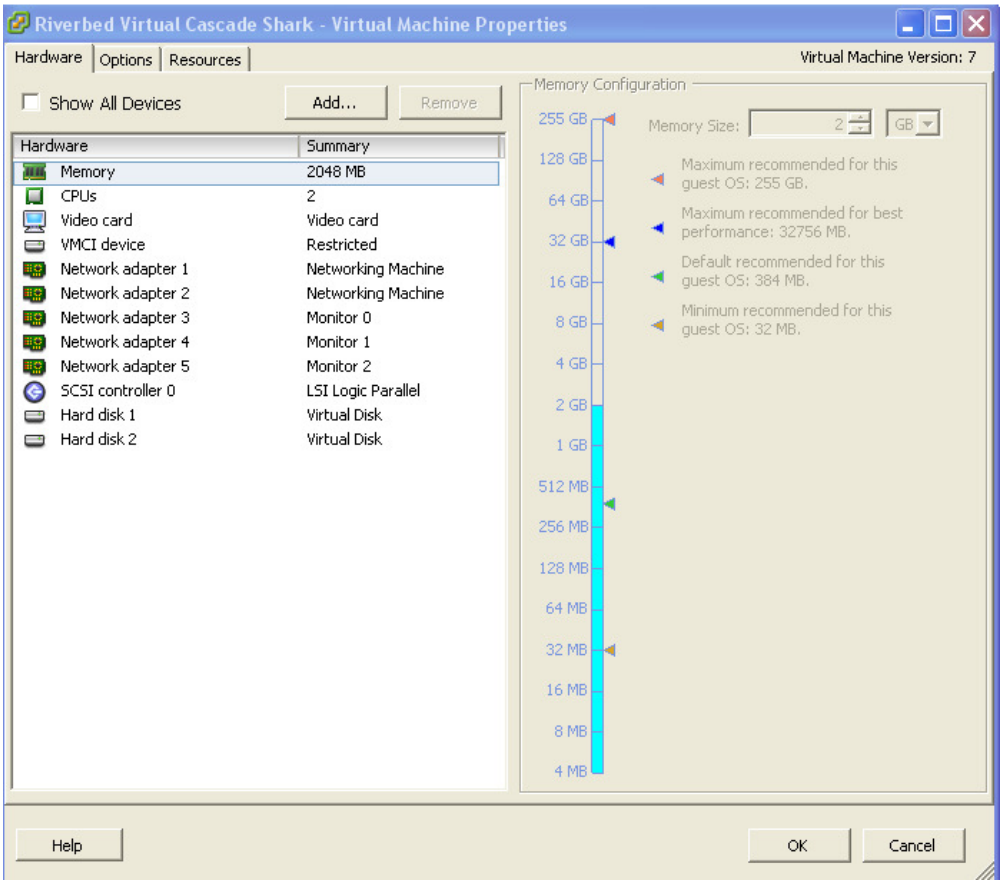
SCHEMA DI RETE



NAeS Consulting srl
WWW.NAES.IT
Via S. Senatore, 10 - 20122 Milano
Tel. +39 02 45487263 Fax. +39 02 70046685

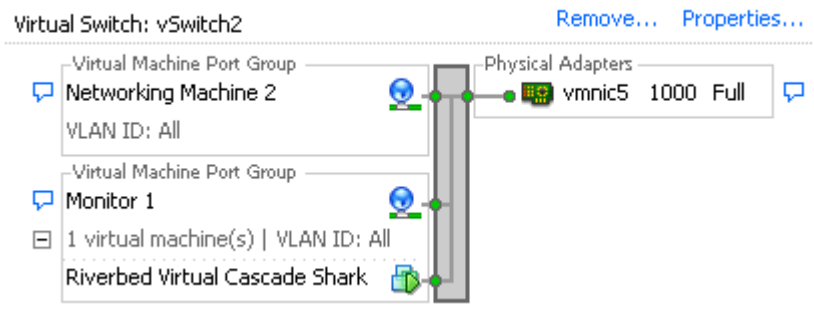
CONFIGURAZIONE ESXi

Per l'installazione di Cascade Virtual Shark in ESXi consultare questo articolo (http://www.naes.it/naesweb/naesweb.nsf/0/54B426D9E8E0BAD7C1257A0D00364975/%24File/CASCADE%20VIRTUAL%20SHARK.pdf?OpenElement). Installato il file ova nell'infrastruttura virtuale e aggiunti un hard disk per salvare i file di capture e due ulteriori porte di mirroring il risultato sarà il seguente:

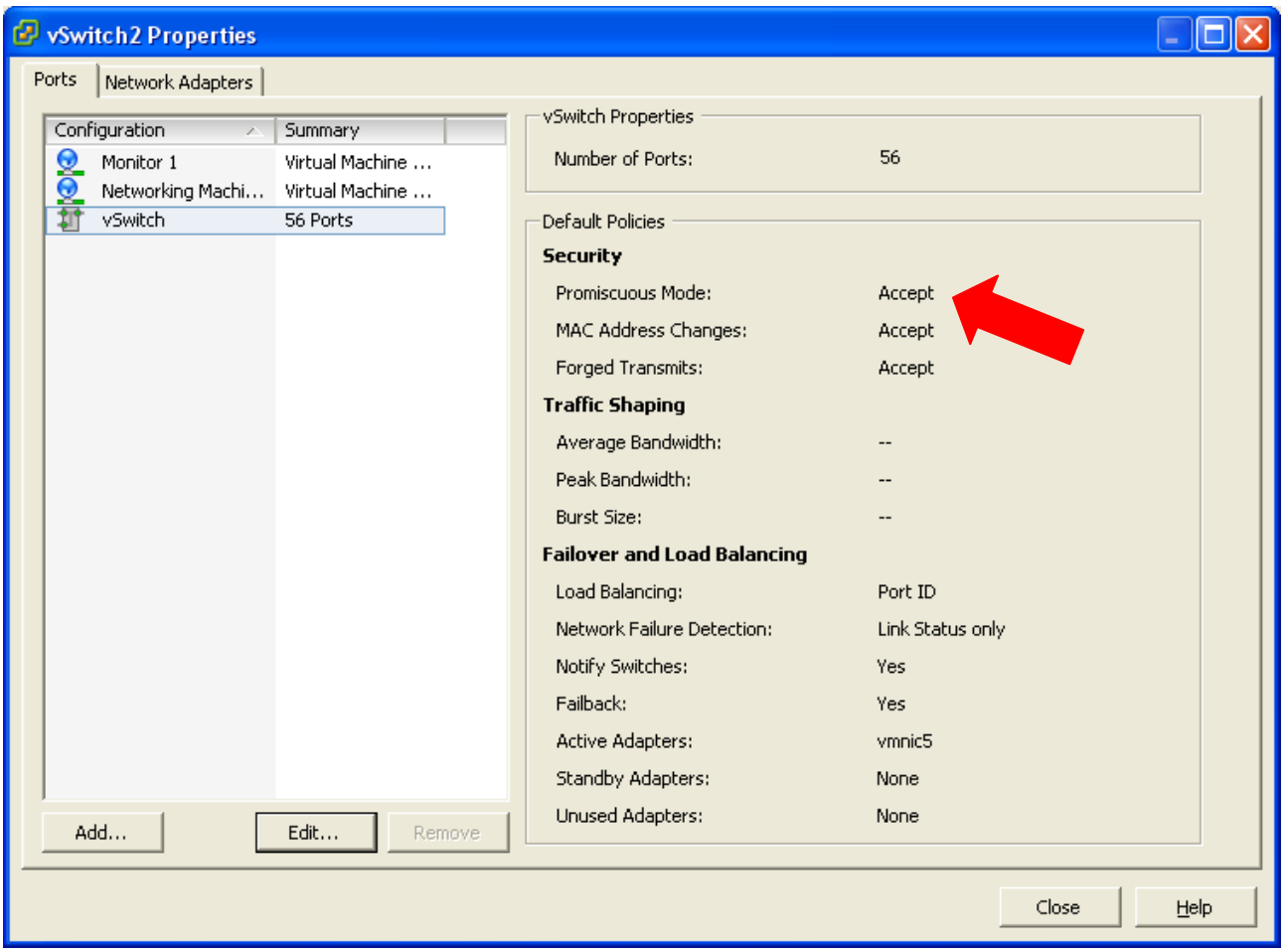


NAeS Consulting srl
WWW.NAES.IT
Via S. Senatore, 10 - 20122 Milano
Tel. +39 02 45487263 Fax. +39 02 70046685

Consideriamo per esempio la Monitor 1. La configurazione di networking ESXi dell'esempio è :



In cui il vswitch è stato configurato in promiscuous mode:



NAeS Consulting srl
WWW.NAES.IT
Via S. Senatore, 10 - 20122 Milano
Tel. +39 02 45487263 Fax. +39 02 70046685

Con questa configurazione il Virtual shark è pronto ad analizzare il traffico della porta vmnic5.

CONFIGURAZIONE SWITCH ENTERASYS

Come si vede nella figura di pagina 2 la porta vmnic5 è collegata alla ge.1.7 . Quindi per analizzare il traffico che va verso internet con la sonda virtuale bisogna mirrorare il traffico della porta ge.1.48 e mandarlo sulla porta ge.1.7 . Per gli switch enterasys la configurazione è :

set port mirroring create ge.1.48 ge.1.7

set port mirroring enable ge.1.48 ge.1.7

Se si hanno più porte fisiche sul server si possono replicare le operazioni precedenti fino ad un massimo di 4 porte per ogni Virtual Shark . Costruita la sonda a basso costo, per analizzare il traffico utilizziamo Cascade Pilot , per una introduzione alle potenzialità di analisi del software Cascade Pilot rimandiamo a questo articolo.
(http://www.naes.it/naesweb/naesweb.nsf/news.xsp?id=08876EEB1D90093CC1257A09004C24FB)

NAeS Consulting srl
WWW.NAES.IT
Via S. Senatore, 10 - 20122 Milano
Tel. +39 02 45487263 Fax. +39 02 70046685