



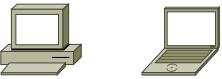
Bijlage 3

Sjabloon Testrapport – Variant 1

Inleiding

De beheeractiviteiten zijn in drie delen gecategoriseerd.

Om de beheeractiviteiten uit te voeren zijn de volgende tools ter beschikking gesteld.

Tool- ID	Tool	Symbol
Ti-1	Testhost (pc of laptop)	
Ti-2	Testserver	
Ti-3	Testrouter	
Ti-4	Testswitch	
Ti-5	Test-MLS	
Ti-6	Device CLI	Device> _
Ti-7	Device GUI	
Ti-8	Sniffer	

1a Inventarisatie (LLDP)

Log via SSH in op de *devices* zoals in de tabel is weergegeven. Vraag via LLDP de neighbour-gegevens op en noteer die in de tabel.

Device	IP-adres	Interface	Verbonden met		
			Device	Interface	Trunk/ Access
Core	172.30.0.1	G3/1	MLS	G1/0/2	Trunk
		G0/0/0	EDGE	G1/0/1	
		G3/1	CORE	G1/0/2	
DMZ	10.20.02	G0/0/1	SW-Backbone	Fa0/1	
Edge	10.0.0.2	G0/0/1	SW-backbone	FA0/2	
		G0/0/0	MLS	G1/0/1	

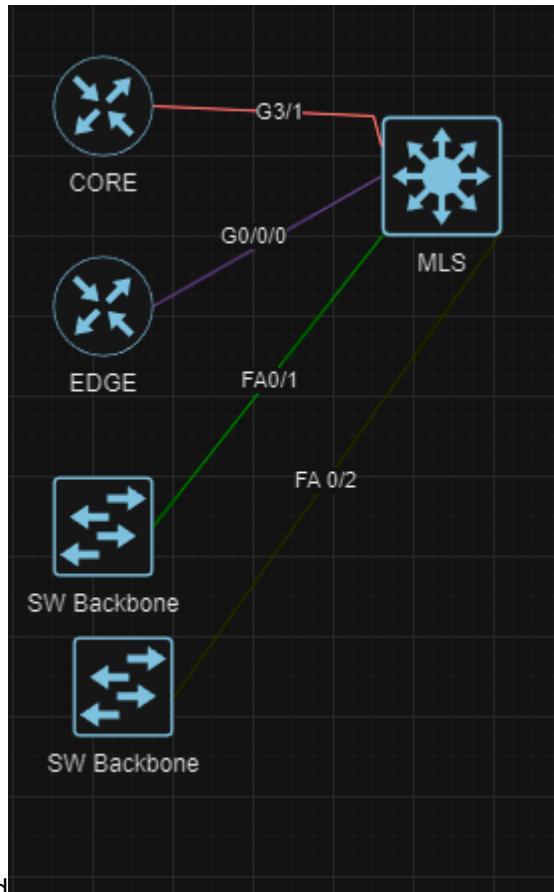
1b Inventarisatie (Netwerktekening)

Maak een netwerktekening van de backbone-infrastructuur aan de hand van de tabel en plaats die op de volgende bladzijde. Benoem in de tekening:

- De servers in het serverdomein (*Intranet, FTP, NTP/Syslog, DHCP, DNS*)
- De routers en switches in de infrastructuur-backbone (*Core, MLS, DMZ, SW-Backbone, Edge*)
- Noteer bij alle verbindingen de transmissiesnelheid.

Voorbeeld:





Plaats hier de afbeelding van het netwerkschema.

2 Controleactiviteiten

Beheeractiviteit C2.08	
Controle	Er is een wachtwoord geconfigureerd voor console-toegang.
Devices	Voer de controles uit op de volgende devices: <i>Core, DMZ, Edge, MLS, AS1</i>

Gekozen tool(s)	Zie blz 2. 
Uitvoering	<p>MLS Enable Show running-config</p> <pre>version 16.3.2 service timestamps log datetime msec no service timestamps debug datetime msec service password-encryption ! hostname MLS ! logging userinfo ! enable secret 5 \$1\$mERr\$ic6JmWpCmRUkn63ir3URr0 ! ! ! ! ! ! no ip cef ip routing ! no ipv6 cef ! ! ! username admin password 7 0832584F1B0D username c password 7 0822 ! ! lldp run ! ! !</pre>
Verwacht resultaat	MLS:Ik verwacht een voltooide resultaat

Afwijkingen	Ik heb geen afwijking geconcludeerd.
Impact/risico	Hoog: Omdat het risico hoog is zou ik de volgende commando invoeren om alles dicht te maken.
Advies	

Beheeractiviteit		C2.06
Controle	De wachtwoorden zijn versleuteld opgeslagen.	
Devices	Voer de controles uit op de volgende devices: <i>Core, DMZ, Edge, MLS, AS1</i>	

Gekozen tool(s)	 Zie blz 2.
Uitvoering	Enable Show running-config
Verwacht resultaat	Ik verwacht dat ik in de config een wachtwoord encryption zie. <pre>logging userinfo ! enable secret 5 \$1\$mERr\$ic6JmWpCmRUkn63ir3URr0 ! !</pre>

Afwijkingen	Nee
Impact/risico	Hoog
Advies	

3 Testactiviteiten

Beheeractiviteit	T4.01
Toelichting	Dataverkeer tussen de VLAN's is niet mogelijk door geconfigureerde ACL's in de MLS.

Gekozen tool(s)	 Zie blz 2.
Uitvoering	Enable Show acces-lists
Verwacht resultaat	Ik verwacht dat ik zie welke vlans geen traffic mogen ontvangen en welke subnetten het zijn van de vlans. <pre>MLS#show access-lists Extended IP access list 120 10 deny ip 172.20.0.0 0.0.255.255 172.21.0.0 0.0.255.255 20 deny ip 172.20.0.0 0.0.255.255 172.22.0.0 0.0.255.255 30 deny ip 172.20.0.0 0.0.255.255 172.23.0.0 0.0.255.255 40 permit ip any any (3649 match(es)) Extended IP access list 121 10 deny ip 172.21.0.0 0.0.255.255 172.20.0.0 0.0.255.255 20 deny ip 172.21.0.0 0.0.255.255 172.22.0.0 0.0.255.255 30 deny ip 172.21.0.0 0.0.255.255 172.23.0.0 0.0.255.255 40 permit ip any any (2409 match(es)) Extended IP access list 122 10 deny ip 172.22.0.0 0.0.255.255 172.20.0.0 0.0.255.255 20 deny ip 172.22.0.0 0.0.255.255 172.21.0.0 0.0.255.255 30 deny ip 172.22.0.0 0.0.255.255 172.23.0.0 0.0.255.255 40 permit ip any any (2003 match(es)) Extended IP access list 123 10 deny ip 172.23.0.0 0.0.255.255 172.20.0.0 0.0.255.255 20 deny ip 172.23.0.0 0.0.255.255 172.21.0.0 0.0.255.255 30 deny ip 172.23.0.0 0.0.255.255 172.22.0.0 0.0.255.255 40 permit ip any any (2094 match(es))</pre>

Afwijkingen	Nee
--------------------	-----

Impact/risico	Hoog
Advies	