 23

[redacted]

Van: [redacted]
Verzonden: maandag 30 juni 2008 13:07
Aan: [redacted]
Onderwerp: Nadere documenten RIES

[redacted]

In navolging van de brief aan de Staatssecretaris, hebben wij bijgevoegde documenten en broncode aan Fox-it nagezonden, voor de audit van RIES internetstemmen.

Met vriendelijke groet,

[redacted]

Programmamanager

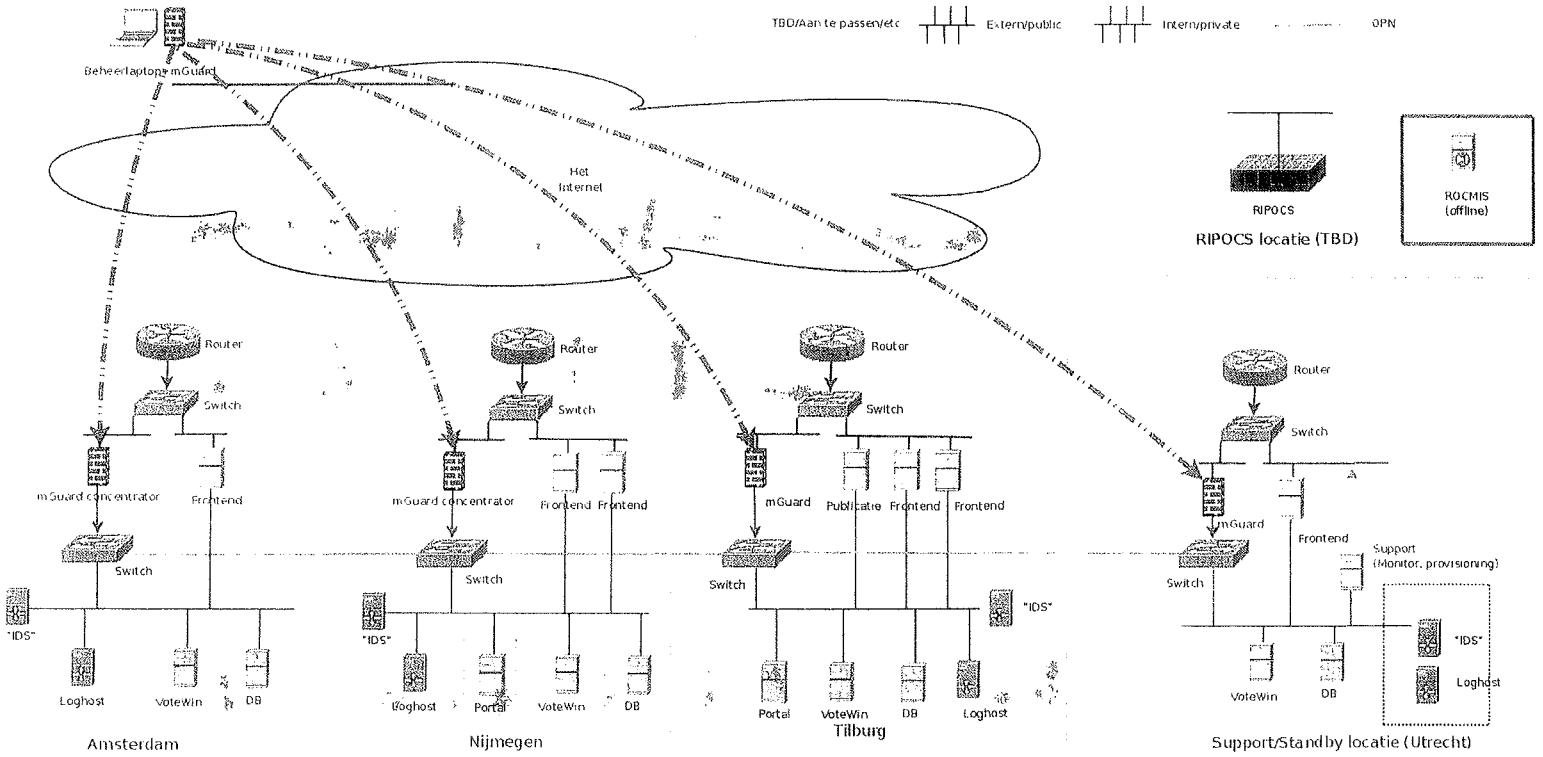
Het Waterschapshuis
p/a Breestraat 59, Leiden
Postbus 130
1135 ZK Edam
[redacted]

Naam	Locatie	Type	Aanschafdatum	Onderhoud tot	Rooth/ebbend/v	Status	Functie	Factuur?	IP extern	Subnet	IP intern	Subnet	Dis
Lokatie Utrecht													
nes-uti-portal-1	Utrecht	Dell 1850			SURFnet	Spare	Portal	nvt			10.4.1.40/29	30G	
nes-uti-stemsserver-1	Utrecht	Dell 1650			SURFnet	Spare	VoteWin	nvt			10.4.1.24/29	72G	
nes-uti-fe-1	Utrecht	Dell 650			SURFnet	Spare	SSL/Apache frontend	nvt			10.4.1.16/29	72G	
nes-uti-rkpocs-1	Utrecht	Dell 1950			SURFnet	Spare	RIPOCS-1	nvt			10.4.1.120/29		
nes-uti-rkpocs-2	Utrecht	Dell 1950	30-05-2006	29-5-2011 (4 hour)	HWH	Productie	RIPOCS-2						146GB (2x)
nes-mon-mguard	Utrecht	Mguard			HWH	Productie	VPN beheer-LAN						
nes-rkcmis-1	Utrecht	Dell T7400	13-3-2006	12-3-201 (NBD)	HWH	Productie	Crypto-cloning	TBD					
nes-uti-support-1	Utrecht	Dell 1950	14-05-2007	13-5-2010 (gold)	HWH	Productie	Supporting Services	SN270690			10.4.1.128/27	72G	
nes-uti-db-1	Utrecht	Virtueel				Spare	stembuis				10.4.1.32/29		
nes-uti-mon-1	Utrecht	Virtueel				Productie	Monitoring intern						
nes-uti-dist-1	Utrecht	Virtueel				Productie	distributie - NTP						
nes-uti-cm-1	Utrecht	Virtueel				Spare	configuratie management						
nes-mon-2004	Utrecht	Dell 1850			SURFnet		Monitoring 2004	nvt					
nes-dist-2004	Utrecht	Dell 1750			SURFnet		SW-distributie +NTP 2004	nvt					
nestab1(virtueel a tm d en g1 t/m g5)	Utrecht	Dell 2650	3-7-2006	2-7-2009 (4 hour)	HWH	Ontwikkel	Frontend/Votewin/PortalCM	pre 2008		192.87.110.0/25			
nestab2 (virtueel a t/m d)	Utrecht	Dell 2650	3-7-2006	2-7-2009 (4 hour)	HWH	Ontwikkel	stembussen (a t/m c)	pre 2008		192.87.110.0/24			
nestab3	Utrecht	Dell 1750			SURFnet	Ontwikkel	RIPOCS	nvt		192.87.110.0/24			
nestab3a	Utrecht	Dell 1750			SURFnet	Ontwikkel	RIPOCS	nvt		192.87.110.0/24			
nes-dist (oud)	Utrecht	Dell	2007		HWH	Ontwikkel	SW-distributie 2004	pre 2008					
nes-mon (oud)	Utrecht	Dell	2007		HWH	Ontwikkel	SW-distributie 2004	pre 2008					
Nieuwe RIES servers													
nes-uti-rkpocs-1	Utrecht (tijd. opslag)	Dell 1950	30-05-2006	29-5-2011 (4 hour)	HWH	bestemd	Productie	RIPOCS-2					146GB (2x)
server 2	Utrecht (tijd. opslag)	Dell 1950	30-05-2006	29-5-2011 (4 hour)	HWH	bestemd	Productie	SSL/Apache front-end					146GB (2x)
server 3	Utrecht (tijd. opslag)	Dell 1950	30-05-2006	29-5-2011 (4 hour)	HWH	bestemd	Productie	VoteWin					146GB (2x)
server 4	Utrecht (tijd. opslag)	Dell 1950	30-05-2006	29-5-2011 (4 hour)	HWH	bestemd	Productie	stembint					146GB (2x)
server 5	Utrecht (tijd. opslag)	Dell 1950	30-05-2006	29-5-2011 (4 hour)	HWH	bestemd	Spare	SSL/Apache front-end					146GB (2x)
server 6	Utrecht (tijd. opslag)	Dell 1950	30-05-2006	29-5-2011 (4 hour)	HWH	bestemd	Spare	VoteWin					146GB (2x)
server 7	Utrecht (tijd. opslag)	Dell 1950	30-05-2006	29-5-2011 (4 hour)	HWH	bestemd	Spare	stembus					146GB (2x)
server 8 (defect DRAC kaart)	Utrecht (tijd. opslag)	Dell 1950	30-05-2006	29-5-2011 (4 hour)	HWH	bestemd	Productie	Portal-2?					146GB (2x)
Lokatie Amsterdam													
nes-switch-3													
nes-mguard-gw-1	Amsterdam	Mguard Pro			HWH	Productie	VPN beheer-LAN						
nes-stemsserver-1	Amsterdam	Dell 2650	1-4-2004	31-3-2007 (4 hour)	HWH	Demo	2004/KOA	pre 2008					
nes-vds-1	Amsterdam	Dell 650	1-4-2004	31-3-2007 (NBD)	HWH	Demo	2004/KOA	pre 2008					
nes-loghost-1	Amsterdam	Dell 650	1-4-2004	31-3-2007 (NBD)	HWH	Demo	2004/KOA	pre 2008					
nes-ams-stemsserver-1	Amsterdam	Dell 1950	15-10-2007	14-10-2010 (gold)	HWH	Productie	VoteWin	SN270690					146GB (2x)
nes-ams-db-1	Amsterdam	Dell 1950	15-10-2007	14-10-2010 (gold)	HWH	Productie	stembus	SN270690					146GB (2x)
nes-ams-fe-1	Amsterdam	Dell 1950	15-10-2007	14-10-2010 (gold)	HWH	Productie	SSL/Apache frontend	SN270690					146GB (2x)
Lokatie Nijmegen													
nes-switch-2	Nijmegen												
nes-mguard-gw-2	Nijmegen	Mguard Pro			HWH	Productie	VPN beheer-LAN						
nes-stemsserver-2	Nijmegen	Dell 2650	17-6-2004	16-6-2007 (4 hour)	HWH	Demo	2004/KOA	pre 2008					
nes-vds-2	Nijmegen	Dell 750	17-6-2004	16-6-2007 (NBD)	HWH	Demo	2004/KOA	pre 2008					
nes-loghost-2	Nijmegen	Dell 750	17-6-2004	16-6-2007 (NBD)	HWH	Demo	2004/KOA	pre 2008					
nes-nijm-stemsserver-1	Nijmegen	Dell 1950	15-10-2007	14-10-2010 (gold)	HWH	Productie	VoteWin	SN270690					146GB (2x)
nes-nijm-db-1	Nijmegen	Dell 1950	15-10-2007	14-10-2010 (gold)	HWH	Productie	stembus	SN270690					146GB (2x)
nes-nijm-fe-1	Nijmegen	Dell 1950	15-10-2007	14-10-2010 (gold)	HWH	Productie	SSL/Apache frontend	SN270690					146GB (2x)
Lokatie Saasveld													
nes saasstemsserver 1	Saasveld	Dell 1950	15-10-2007	14-10-2010 (gold)	HWH	Ontwikkel	Ontwikkel	SN270690					146GB (2x)
nes-rkcmis-2	Saasveld	Dell T7400	27-3-2008	26-3-2011 (NBD)	HWH	Ontwikkel	Crypto-cloning	TBD					
nes-rkcmis-printer	Saasveld	Samsung ML-2010R	nvt	16-4-2008	16-4-2009 (on-site)	HWH	Ontw/Productie	Crypto-cloning	TBD				
nes-saasveld-fe-1	Saasveld	Dell SC 1425			MC	Ontwikkel	Ontwikkel	nvt					
nes-saasveld-db-1	Saasveld	Dell SC 1425			MC	Ontwikkel	Ontwikkel	nvt					
Overig													
nes-beheer-1	Tilburg	Inspiron 1150	4-4-2004	S+K 2007(Complete Care /NBD)	HWH	Productie	Beheerlaptop	pre 2008					
nes-beheer-2	Utrecht	Inspiron 1150	4-4-2004	S+K 2007(Complete Care /NBD)	HWH	Productie	Beheerlaptop	pre 2008					
nes-beheer-3	Tilburg	Inspiron 1150	4-4-2004	S+K 2007(Complete Care /NBD)	HWH	Stuk	disk zit in 1	Beheerlaptop	pre 2008				
nes-beheer-4	Utrecht	Inspiron 1150	4-4-2004	S+K 2007(Complete Care /NBD)	HWH	Productie	Beheerlaptop	pre 2008					
nes-beheer-5	Saasveld	Inspiron 1150	18-8-2004	17-8-2005	HWH	Spare	Beheerlaptop	pre 2008					
nes-beheer-6	Utrecht	D600			SURFnet	Uitleen	Beheerlaptop	pre 2008					
nes-beheer-D610	Utrecht	D610			SURFnet	Uitleen/stuk	Beheerlaptop	pre 2008					
Crypto-kaarten	11x	IBM 4764	6-2-2007 2x 2-3-2007 1x 3-5-2007 3x 8-2-2008 2x 27-2-2008 2x 11-3-2008 1x 30-5-2008 1x gemuld		HWH	Productie	HW Crypto	HWH/TTP					
Battery replacement-kits	5x				HWH	Productie	HW Crypto	HWH					
Mguards	6x + spares		2004/2006		HWH	Productie	VPN beheer-LAN	pre 2008					
Mguards Pro	3x + spares		2004/2006		HWH	Productie	VPN beheer-LAN	pre 2008					
Broadcom Crypto-accelerator	*2x*		*2004*		HWH	*Demo*	SSL accelerator	pre 2008					
Broadcom Crypto-accelerator	1x		2004		HWH	Spare	SSL accelerator	pre 2008					
Dell Cliëntpc	4x		2007		HWH	Ontwikkel	SSL-accelerator	pre 2008					
Cisco Catalyst 2950 Switch	2x		2004		HWH	Productie	beheer-LAN	pre 2008					
Remote Power Switch	2x (@SARA)				SURFnet	Productie	beheer-LAN RPS	nvt					
3com gig-switch	Utrecht				SURFnet	Productie	beheer LAN	nvt					

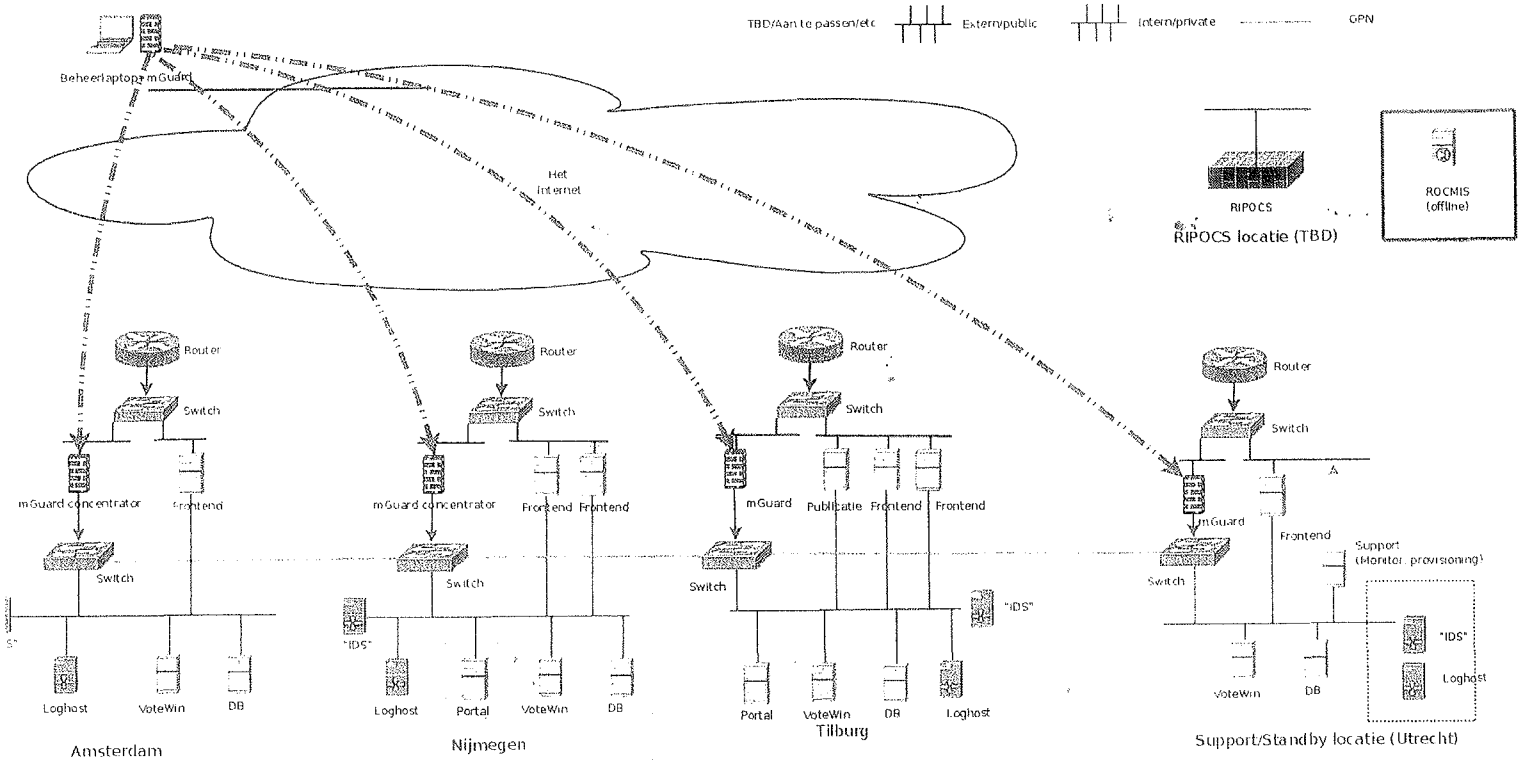
Legenda Cursief — Afgeschreven maar nog in gebruik
Nog uit te zoeken
Eigendom Magic Choice (niet op project)
Eigendom SURFnet (niet op project)
Te verplaatsen/aan te passen
Ontmenteld

Overzicht bijgewerkt op 12-6-2008

DRAFT 25-6-2008



DRAFT 25-6-2008



Implementatie RIES 2008 server- en netwerkinfrastructuur

In dit document worden kort de onderdelen van de RIES 2008 infrastructuur beschreven waar eind juni 2008 nog aan gewerkt wordt. Het betreft hier aanvullingen en vernieuwingen van de bestaande infrastructuur (zoals gebruikt bij verkiezingen in 2004 en 2006). Nadruk in dit document is dat betrokken partijen zich tot het uiterste inspannen teneinde een veilige en betrouwbare stemvoorziening te leveren tijdens de stemperiode en de voorbereidings periode voorafgaand aan de stemperiode.

1. Provisioning (installatie, softwaredistributie en configuratiemanagement)

Alle RIES-servers en beheer-laptops zullen vanuit een centraal provisoning-systeem geinstalleerd en geconfigureerd worden. Elk type server zal vanuit de provisoning server een minimale installatie krijgen met alleen die onderdelen van het OS die strict noodzakelijk zijn en alleen de voor de beoogde functie noodzakelijke software-pakketten. Ook de specifieke configuratie per type machine zal vanuit die provisioning server plaatsvinden (naar aanleiding van de resultaten van de zo genaamde system hardening. Daarbij wordt gebruik gemaakt van functie- en locatie-specifieke profielen. Ook security fixes kunnen via het provisioning systeem op een uniforme en gecontroleerde wijze verspreid worden. Provisioning vindt plaats op/via het interne afgeschermde RIES-beheernetwerk. Ingebruikname van dit systeem wordt eind juni 2008 verwacht.

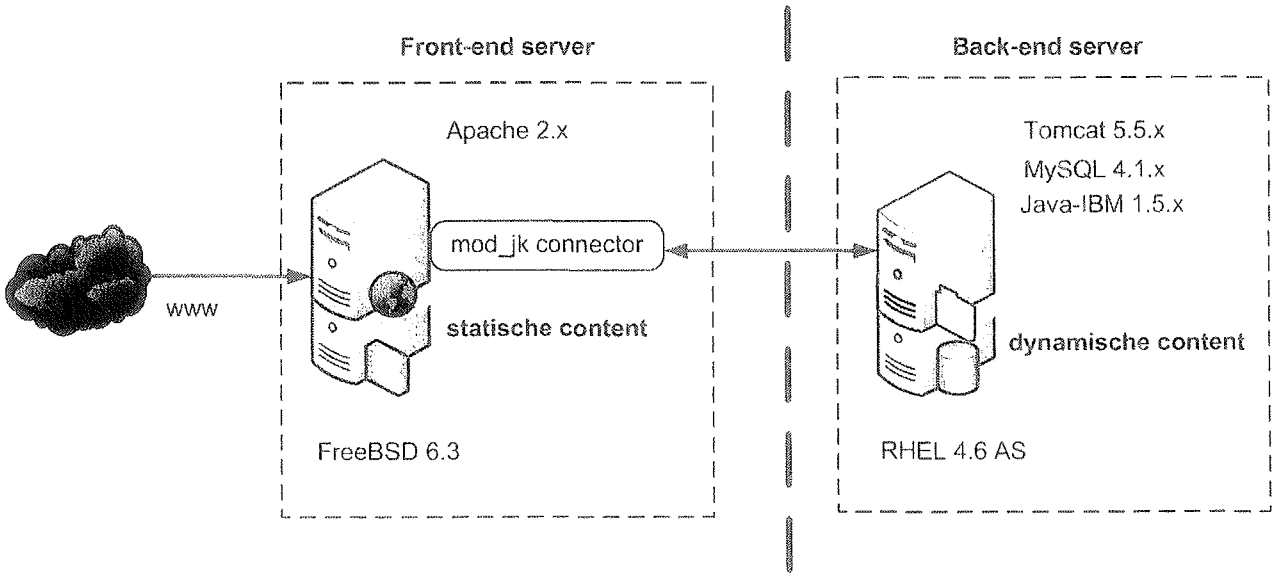
De baseline die voor de inrichting van servers en andere systemen ten behoeve van het RIES system geldt is dat alleen onderdelen, autorisaties enz die nodig zijn, zowel qua OS als firewall-rules als applicaties, worden toegestaan/geïnstalleerd. Verder gelden de in bestaande documentatie genoemde ontwerp-principes.

De RIES serversystemen kunnen onderverdeeld worden in drie categorieen. Voor elke categorie gelden de volgende versies voor OS (Operating System):

- Frontends: FreeBSD 6.3 (laatste versie inclusief laatste vendor-updates tot aan freeze)
- Backends: Red Hat RHEL4.6 (laatste versie inclusief laatste vendor-updates tot aan freeze)
- Ondersteunende servers: Red Hat RHEL4.6 (laatste versie inclusief laatste vendor-updates tot aan freeze)

Voor applicatiesoftware boven het OS (uitgezonderd de RIES applicaties zelf) geldt dat daar de door de vendor geleverde en gesupporte versies gebruikt

worden. In figuur 1 staan de cruciale componenten voor een typische set van frontend/backend-server.



1Figu

ur 1: Software-levels voor VotingWindow en Portal servers.

2. Change management procedure

Na freeze van de situatie in augustus: vendor security updates op gecontroleerde wijze aanbrengen conform een change management procedure waarbij elke update beoordeeld wordt op impact/risico alvorens de update aangebracht wordt.

3. Monitoring, logging, anomalie-detectie

De in 2004 en 2006 gebruikte systeem- en netwerkmonitoring wordt opnieuw geïmplementeerd waarbij alle systeem lokaal gemonitord worden en via een centraal systeem worden verzameld en weergegeven. Dit centrale systeem monitort ook de beschikbaarheid van machines en services op het interne beheernetwerk. De beschikbaarheidsmonitoring vanuit het Internet blijft (uitgezonderd toevoegen van nieuwe te monitoren systemen) ongewijzigd.

Naast systeem en netwerkmonitoring zal systeemlogging van alle servers zowel per lokatie op een lokale logserver als op 1 centrale (lokatieonafhankelijke) logserver verzameld worden. Logging van gebruikersactiviteit is expliciet zonder potentieel identificerende informatie (IP-adres, browser etc). Logging van beheerdersactiviteiten is expliciet inclusief identificerende informatie (IP-adres, beheerlaptop etc). Voor de (de-)centrale logservers geldt een receive-only policy. Oplevering staat voor augustus 2008 gepland.

Aan de servers wordt "tripwire" functionaliteit toegevoegd, volgens planning begin September. Dit is een vorm van checksumming op de geïnstalleerde applicatiesoftware op de verschillende servers waarmee afwijkingen/aanpassingen

aan de systemen gedetecteerd kunnen worden.

Het eind augustus op te leveren IDS-system detecteert anomalieen in het verkeer, voornamelijk afwijkend verkeer op ongebruikte poorten of via ongeplande routes.

4. Vernieuwing beheerlaptops

Vervanging van de huidige beheerlaptops, inclusief opnieuw inrichten (zie ook 1.) is eind juli 2008 gepland.
Beheerlaptops zijn allen bruikbaar met hardware matige VPN verbinding (verbonden met M-Guard – zie afbeelding met netwerk topologie). De beheerlaptops zijn persoonsgebonden en verstrekking van reserve beheerlaptops (uit beveiligde opslag) gaat na registratie.

5. Inrichten lokatie Tilburg

Als derde hoofdlokatie naast Amsterdam en Nijmegen zal in augustus 2008 Tilburg in gebruik genomen worden.

6. Uitbreiding en vernieuwing beheernetwerk

Mede gekoppeld aan de ingebruikname van een dedicated OPN (Optical Private Network, zie bijlage) en oplevering van lokatie Tilburg zal het afgeschermde beheernetwerk aangepast worden. Dit behelst uitbreiding/herinrichting van het mGuard-gebaseerde VPN voor toegang met de dedicated beheerlaptops. Koppelingen tussen lokaties die nu via het mGuard-VPN lopen worden overgezet naar het begin augustus op te leveren OPN. Dit OPN bestaat uit een ring van protected lichtpaden tussen de vier lokaties aangevuld met twee unprotected gekruiste lichtpaden om bij uitval maximaal twee lokaties altijd altijd de overige lokaties onderling bereikbaar te laten zijn. Oplevering staat 16 augustus 2008 gepland.

7. RIPOCS servers en housing

RIPOCS wordt onder specifieke randvoorwaarden en beveiligingseisen geïnstalleerd . Specifiek zal RIPOCS in een speciale braakbestendige kluiskast worden geïnstalleerd.
Definitieve inrichting van de RIPOCS-servers zal eind augustus plaats vinden (dit hangt mede af van uitgewerkte beheer en toegangsprocedure) .

8. ROCMIS

Stand alonemachine, wordt opgeslagen in een fysieke kluis met vergelijkbare

veiligheidswaarborgen als RIPOCS.

9. Portal

Definitieve implementatie van de Portal-functionaliteit (dubbele uitvoering met hot-standby) staat voor eind augustus 2008 gepland. Toegang tot de Portal-server(s) zal dan alleen nog maar kunnen vanaf een beperkte set IP-adressen (op te leveren door de Waterschappen).

10. Failover/redundancy

Het huidige failover/reduncy mechanisme voor externe toegang tot de stemservers is gebaseerd op een eenvoudig maar robuust round-robin DNS-mechanisme. Een aanvullend mechanisme gebaseerd op flowbased anycast zal, bij goed resultaat van de tests, naar verwachting eind augustus geimplementeerd worden.

11. Performance, tuning en capaciteitsplanning

Tot uiterlijk eind oktober 2008 zullen doorlopend performance/quality-metingen gedaan worden op basis waarvan bepaald wordt of er mogelijk extra capaciteit (hardware) voor de stemserver-functionaliteit ingezet moet worden. Extra capaciteit zal geïmplementeerd worden onder dezelfde condities en met dezelfde instellingen als bij de reeds eerder opgeleverde systemen. Dit wordt geborgd door aanschaf van identieke hardware en het provisioning principe (zie ook 1.).

11. Ingebruikname stem.nl domein (inclusief bijbehorende certificaten)

Voor toegang voor de kiezers is het domein www.stem.nl aangeschaft door Het Waterschapshuis. Gepland is om dit medio augustus in gebruik te nemen, samen met de juiste SSL certificaten.

Bijlage: OPN

Vijf voordelen lichtpaden

Capaciteit
SURFnet6 biedt gebruikers lichtpaden van 150 Mbit/s, 600 Mbit/s, 1 Gbit/s. Hoewel het netwerk van SURFnet ook snelheden van 10 Gigabits per seconde kan realiseren, is de apparatuur in het netwerk van de aangesloten instellingen hier doorgaans nog niet op berekend.

Kwaliteit
De optische apparatuur die lichtpaden mogelijk maakt, is eenvoudiger en robuuster dan de gebruikelijke router en switches die voor IP-verkeer worden gebruikt. Ook worden de datastromen niet gehinderd door ander verkeer op het netwerk, maar gaan ze via gescheiden lichtpaden op hoge snelheid van verzender naar ontvanger. Daardoor is het verkeer op het netwerk ook stabieler. Gemeten over de maximale afstand binnen Nederland tussen twee poorten bedraagt de maximale round trip time (RTT) van een lichtpad minder dan 20 milliseconde.

Veiligheid
Daar waar internetverbindingen risico's van inbraak of afluisteren kennen, is dat bij lichtpaden nagenoeg onmogelijk. Het is namelijk een directe verbinding tussen twee punten op de optische laag van het netwerk.

Transparantie
Een lichtpad is onafhankelijk van de daarover te gebruiken protocollen. SURFnet biedt lichtpaden standaard aan met een Ethernet koppelvlak. Andere protocollen zoals Fiber Channel kunnen als maatwerk worden aangeboden.

Internationale uitbreidbaarheid
Hoewel SURFnet6 een Nederlands netwerk is, zijn lichtpaden niet beperkt tot onze grenzen. Dankzij de het optische knooppunt Netherlight in Amsterdam dat SURFnet heeft gerealiseerd, zijn koppelingen mogelijk met een groot aantal onderzoeksnetwerken in Europa, de VS, Azië en Australië.

De komende jaren zullen de mogelijkheden voor connectiviteit van internationale lichtpaden naar verwachting aanzienlijk groter worden doordat zowel via het Europese onderzoeksnetwerk GEANT2 als via de Global Lambda Integrated Facility (GLIF) steeds meer netwerken worden ontsloten.