## **Opdracht heeft deeltaken**

Context van de op dracht

Opsplitsen in deeltaken

Elke deeltaak

##### Beschrijving

##### Aanpak

##### Mogelijke of gewenste resultaat

##### Vaststellingen

##### Advies

## **Opdracht 0: Analyse netwerkwerkverkeer**

### Plan van aanpak – Tijdsduur

#### Taak 1: netwerk scannen (10 dagen)

##### Beschrijving

Netwerkverkeer scannen om zo een overzicht te hebben van het inkomende en uitgaande verkeer.

##### Aanpak

Er wordt gebruik gemaakt van Netflow voor de verkeer monitoring. Daarnaast moet Nbar de verschillende protocollen herkennen en classificeren, om een duidelijk overzicht te krijgen van de verkeerstroom binnen het netwerk. We laten dit 10dagen monitoren.

##### Mogelijke of gewenste resultaat

De bedoeling is om te zien of er een bepaalde soort verkeer is die hier niet moet zijn. #Dit zorgt voor extra verkeer op het netwerk die niet nodig is.

##### Vaststellingen

Na de analyse blijkt dat er veel skype verkeer aanwezig was, en er was ook bittorent in het netwerkverkeer.

##### Advies

Via QOS kunnen wij bepaalde protocolen tegenhouden. Ten tweede kunnen we er ook voor zorgen dat dat er een bepaalde aantal bandbreedte gereserveerd is voor specifiek protocolen.

#### Taak 2: resultaten analyseren (3 dagen)

##### Beschrijving

De resultaten van de vorige taak bekijken en ontleden om het probleem te vinden. Naar de oorsprong van de probleem gaan.

##### Aanpak

Zowel de Nbar uitslagen als de netflow resultaten bekijken omdat men daar meer gedetailleerde resultaten kan zien.

##### Mogelijke of gewenste resultaat

De bedoeling is om een meer gedetailleerd log te hebben van de gevonden problemen. Er moet duidelijk informatie zijn over wat en hoeveel ven de bandbreedte het inneemt etc.

##### Vaststellingen

Er zijn heel veel kleine verkeer die niet nodig of belangrijke zijn, alle verschillende soorten verkeren samen zorgen voor het innemen van een deel ven het verkeer. Dit is geen groot deel, maar wel groot genoeg om opgemerkt te worden.

##### Advies

Veel van dit verkeerstroom zijn protocollen die gebruikt worden bij andere taken die toch wel gebruikt worden in de dagdagelijkse handelingen. Er zal daarom geen toegang geweigerd worden aan die soorten protocollen maar de prioriteiten moeten laag staan zodat de belangrijkere protocollen prioriteit krijgen.

#### Taak 3 : voorstellen formuleren (3 dagen)

##### Beschrijving

Design en implementatie van de verschilde voorstellen voor de diverse problemen uitschrijven voor de opdrachtgever.

##### Aanpak

Er wordt twee documenten gemaakt, design en implementatie. In design wordt uitleg gegeven hoe dit precies zal gebeuren. Dus welke soorten oplossing zal er gebruikt worden. Welke interfaces kabels etc. bij implementatie gaan we nog dieper in detail en schrijven we de code op die gebruikt moeten worden en op welke manier.

##### Mogelijke of gewenste resultaat

Goedkeuring van het voorstel.

##### Vaststellingen

Voorstel werd goed gekeurd dus nu zal. Er wordt groen licht gegeven om de oplossing toe te passen.

##### Advies

Laat de monitoring software Netflow en Nbar in de achtergrond nog een paar weken draaien. Zo is er een up-to-date informatie over het netwerkverkeer, en kan tijdens het implementeren opgevraagd worden en de criteria van de implementatie veranderen ten opzichte van de weergegeven resultaten.

## **Opdracht 1 : Illegale download**

### Plan van aanpak – Tijdsduur

#### Taak 1: Monitoring (10 dagen)

##### Beschrijving

Net als bij opdracht 0 wordt er aan monitoring gedaan op het netwerk. De bedoeling is om dit keer specifiek naar verkeerstroming te kijken die met Bitttorent te maken hebben

##### Aanpak

Dit wordt natuurlijk ook weer 10 dagen uitgevoerd. Er moet dan gefilterd worden op Bitttorent en op de specifieke poorten die Bittorent gebruikt. Hierdoor kunne we exacte impact van Bittorent op het netwerkverkeer bestuderen.

##### Mogelijke of gewenste resultaat

Door deze specifieke test te doen kunnen we filteren op alleen Bittorent, en een duidelijk beeld krijgen over de impact van dit verkeer op het netwerk.

##### Vaststellingen

Bittorent is een protocol die herkend wordt door Nbar, en we zien deze protocol elke keer in de top 10. Dit betekent dat het toch wel wat bandbreedte van het netwerkverkeer in beslag neemt.

##### Advies

Dit verkeer volledige stoppen omdat het niet noodzakelijk is voor in de dagelijkse werking van het bedrijf.

#### Taak 2: Mogelijke oplossingen onderzoeken (3 dagen)

##### Beschrijving

Nu er een duidelijk beeld is over het verkeer, en kunnen confirmeren dat Bittorent aanwezig is moet dit geblokkeerd worden

##### Aanpak

Onderzoeken op Cisco site specifiek voor QoS.

##### Mogelijke of gewenste resultaat

Mogelijkheid om Bittorent tegen te houden via poorten te blokkeren of het tegenhouden van het protocol zelf.

##### Vaststellingen

Via Qos Kan Specifiek protocollen tegengehouden worden maar ook ervoor zorgen dat specifieke verkeer een heel laag prioriteit hebben.

##### Advies

Bittorent tegen door met QoS . Voor de zekerheid gaan we alle verkeer van bittorent vertragen, mocht er door een error toch BitTorent verkeer binnen kommen.

#### Taak 3: Design en implementatie voorstellen (3 dagen)

##### Beschrijving

Nu het duidelijk is hoe deze probleem opgelost zal worden moet de oplossingen uitgeschreven en een voorstel opgesteld worden voor de opdrachtgever.

##### Aanpak

Er worden twee documenten opgemaakt. De design en de implementatie. In het design van de oplossing wordt uitleg gegeven over de oplossing en hoe en waar het toegepast zal worden. De implementatie document is meer in detail, hier wordt uitleg gegeven over hoe het precies gedaan moet worden. In deze document vinden we ook configuraties codes, interface connecties

##### Mogelijke of gewenste resultaat

Door deze documenten openstellen, wordt de oplossingen al een keer toegepast op een virtuele toestel. Hierdoor wordt het duidelijker hoe dit toegepast moet worden en zal de werkelijke implementatie duidelijker en eenvoudiger.

##### Vaststellingen

Het toepassen van de Qos maatregels zijn een eenvoudige en werken goed op de toestellen.

##### Advies

Er zijn drie verschillende oplossingen voor de Bittorent probleem. Gebruik alle drie voor de zekerheid. Het is geen slecht idee om de andere oplossingen ook toe te passen, mocht de hoofdoplossing niet meer werken door een defect dan is er nog een extra maatregel voor de Qos.

#### Taak 4: Implementeren en testen (3 dagen)

##### Beschrijving

Na de goedkeuring van de opdrachtgever kan de oplossingen geïmplanteerd worden en getest worden

##### Aanpak

Met Nbar Qos kunnen we dan de BitTorent blokkeren via die class-policy.

Er wordt een ACL-list gemaakt, die gelinkt word met de class policy. In die map moet er een policy-map worden aangemaakt die de prioriteit van BitTorent zal verminderen door MQC Low Latency.

Hierna moet en test gedaan worden door Bittorent proberen te downloaden tec.

##### Mogelijke of gewenste resultaat

##### Vaststellingen

##### Advies

Laat Nbar en Netflow nog scannen om elke keer een up-to-date resultaat van het netwerkverkeer te kunnen opvragen.

### Plan van aanpak – Evaluatie

De enige manier dat werk kunne evalueren of de oplossing gelukt is door de testing. We zullen op verschillende locaties en scenario’s proberen te downloaden via Bittorent, als dit lukt dan moeten we onze oplossing veranderen. We moeten dan nog Nbar her verkeer laten scannen en de verslag bekijk of we nog sporen van Bittorent zien. Als we na twee weken geen verkeer van Bittorent terugvinden kunnen we concluderen dat deze probleem opgelost is.

## **Probleem 2 : Telefonie en Communicatie**

### 2.1 Plan van aanpak – Tijdsduur

#### Taak 1: Monitoring (10 dagen)

##### Beschrijving

Net als bij opdracht 1 wordt er aan monitoring gedaan op het netwerk. De bedoeling is om dit keer specifiek naar verkeerstroming te kijken die met VoIP te maken hebben

##### Aanpak

Dit wordt natuurlijk ook weer 10 dagen uitgevoerd. Dit keer filteren we op RTP-verkeerstroom, en SIP-verkeerstroom

##### Mogelijke of gewenste resultaat

Er wordt dagelijks veel met telefonie gedaan, dus RTP moet zeker in de top 10 van het netwerkverkeer zitten.

##### Vaststellingen

De rtp verkeersstroom komt niet zo vaak voor als de SIP-verkeerstroom. De SIP is het protocol die gebruikt wordt voor de initiatie van het verkeer. De RTP os het protocol die gebruikt wordt voor de werkelijke gesprekken. Ziet eruit dat er veel meer geïnitieerd. Het kan zijn dat er na de initiatie pakketjes gedropt worden omdat er te veel verkeer is in het netwerk.

##### Advies

We moeten ervoor zorgen dat VOIP altijd prioriteit heeft op alle andere verkeer. En er moet een bepaalde aantal bandbreedte gereserveerd worden voor VOIP. Hierdoor zullen er geen storing of pakketverlies meer plaatsvinden bij de VOIP.

##### Beschrijving

##### Aanpak

##### Mogelijke of gewenste resultaat

##### Vaststellingen

##### Advies

#### Taak 2: VOIP en Communicatie optimalisatie onderzoeken (3 Dagen)

##### Beschrijving

Er zijn momenteel 10 telefoons in het bedrijf. Het scenario die geschetst wordt is dat er op alle lijnen tegelijkertijd een gesprek gevoerd wordt. Tijdens de normaal werkuren moet het mogelijke zijn om gesprekken op alle lijnen te voeren zonder dat er een VOIP-pakket wegvalt.

##### Aanpak

Hier is de bedoeling om ten eerste een manier te vinden om ervoor te zorgen dat bandbreedte gereserveerd is voor de tien telefoonlijnen. De volledige uitleg en berekening is te vinden in *ResearchMogelijkeOplossingen.docx* Ten tweede moeten we ervoor zorgen dat de VOIP-pakketjes voorrang krijgen op alle verkeer.

##### Mogelijke of gewenste resultaat

De totaalaantal nodige bandbreedte voor de telefonie kunnen berekenen en voorrang geven aan de VOIP.

##### Vaststellingen

Het is mogelijk voor ons om via Auto-QoS die automatische voor ons te berekenen en de juiste meest optimale configuratie voor ons netwerk te toepassen. Dit gaan we misschien niet kunne toepassen op onze toestellen omdat de toestellen oude toestellen zijn en waarschijnlijk de auto-QoS niet ondersteunen. Alles zal Manuel moeten geconfigureerd worden.

##### Advies

De toestellen moeten in de nabije toekomst vervangen worden voor nieuw toestellen of zulle problemen in de toekomt te voorkomen. De oplossing handmatige toepassen, Er zullen wat workaround moeten gebeuren om sommige taken toch te kunne voltooien.

#### Taak 3:Design en Implementatie voorstellen (3 dagen)

##### Beschrijving

Nu het duidelijk is hoe deze probleem opgelost zal worden moet de oplossingen uitgeschreven en een voorstel opgesteld worden voor de opdrachtgever.

##### Aanpak

Er worden twee documenten opgemaakt. De design en de implementatie. In het design van de oplossing wordt uitleg gegeven over de oplossing en hoe en waar het toegepast zal worden. De implementatie document is meer in detail, hier wordt uitleg gegeven over hoe het precies gedaan moet worden. In deze document vinden we ook configuraties codes, interface connecties

##### Mogelijke of gewenste resultaat

Door deze documenten openstellen, wordt de oplossingen al een keer toegepast op een virtuele toestel. Hierdoor wordt het duidelijker hoe dit toegepast moet worden en zal de werkelijke implementatie duidelijker en eenvoudiger.

##### Vaststellingen

Na de eerste poging bij het toepassen van de Auto-QoS, kan er nu geconfirmeerd worden dat auto-QoS niet toegepast kan worden op deze toestellen.

##### Advies

#### Taak 4:

Na de goedkeuring van de opdrachtgever kan de oplossingen geïmplanteerd worden. Na de implementatie moet dit gecontroleerd worden. We kunne zien in de configuratie of er wel de juist hoeveelheid bandbreedte toegekend is, en de regels van de prioriteiten bekijken. *(3 dagen)*

### 2.2 Plan van aanpak – Evaluatie

Testen met ***Agilent N2X???***

## **Probleem 3 : Wachtwoorden**

### Plan van aanpak – Tijdsduur

#### Taak 1:Privicy Policy Onderzoeken (3 Dagen)

##### Beschrijving

Momenteel is eer geen wachtwoord policy die ervoor zorgt dat de werknemers hun wachtwoorden periodiek veranderen. Hierdoor zijn de achtwoorden nooit veranderd geweest, dit kan heel gevaarlijk zijn.

##### Aanpak

Onderzoek over de officiële best practices van de BBB(Better Business Bereau). Met deze regels kan er een wachtwoord policy en een checklist voor de nieuwe wachtwoorden aangemaakt worden.

##### Mogelijke of gewenste resultaat

De antwoord krijgen voord bepaalde vragen over *Best practises*  voor pasword policy, zoals min- en max password age etc. Checklist voor een het aanmaken van een goed wachtwoord.

##### Vaststellingen

Er moet minstens een min wachtwoord age zijn wat momenteel niet van toepassing is. Eén checklist voor de wachtwoorden om ervoor te zorgen dat de gekozen wachtwoorden sterk genoeg zijn.

##### Advies

En min password age van 90 dagen en max password age van 120 dagen. Dit bedenkt dat de gebruikers hun wachtenwoorden na 3 maanden kunnen veranderen, maar moeten hun wachtwoorden na 4 maanden zeker veranderen.

Ook moeten er bepaalde vereisten zijn die de gekozen wachtwoorden aan moeten voldoen, en een bepaalde securitymaatregel die ervoor zorgt dat er een shutdown is bij het ingeven van het verkeerde wachtwoord.

#### Taak 2: Primaire test ( 6 Dagen)

##### Beschrijving

De nieuwe maatregelen moeten getest. Door dit op een aparte toestel voor een kleine loop tijd te testen, kan er een beeld geschetst worden over de werking van de nieuwe policy.

##### Aanpak

De test zal 6 dagen duren. De boelding is om deze nieuwe policy in te stellen voor 6 dagen in plaats van de 4 maanden. Zo kan er een observatie gemaakt worden en vergeleken naar wat er verwacht kan worden bij de implementatie.

##### Mogelijke of gewenste resultaat

Een paar dagen voor de deadline een notificatie ontvangen met een herinnering dat het wachtwoord veranderd moet worden. De nieuwe ingegeven wacht zal allen geaccepteerd worden wanner ze voldoen aan de checklist.

##### Vaststellingen

Het hele proces is heel eenvoudige en snel.

##### Advies

Om de security te verbeteren moet dit ook gedaan worden. Na de goed keuring motetten de nieuwe policy direct toegepast worden.

#### Taak 3: Design en Implementatie voorstellen (3 dagen)

##### Beschrijving

Nu het duidelijk is hoe deze probleem opgelost zal worden moet de oplossingen uitgeschreven en een voorstel opgesteld worden voor de opdrachtgever.

##### Aanpak

Er worden twee documenten opgemaakt. De design en de implementatie. In het design van de oplossing wordt uitleg gegeven over de oplossing en hoe en waar het toegepast zal worden. De implementatie document is meer in detail, hier wordt uitleg gegeven over hoe het precies gedaan moet worden. In deze document vinden we ook configuraties codes, interface connecties

##### Mogelijke of gewenste resultaat

Door deze documenten openstellen, wordt de oplossingen al een keer toegepast op een virtuele toestel. Hierdoor wordt het duidelijker hoe dit toegepast moet worden en zal de werkelijke implementatie duidelijker en eenvoudiger.

##### Vaststellingen

Dit keer werd eerst de test op het aparte systeem voor deze documentaties gedaan. Hierdoor ging het proces voor het opstellen van deze twee documenten veel vlotter.

##### Advies

Bij de test was er een kleiner reminder van Windows zelf als herinnering. Het is mogelijk om zelfs een mail notificatie in te schakelen, dit moet gedaan worden bij de echte implementatie.

#### Taak 4: Implantatie (3 Dagen)

##### Beschrijving

Op deze moment moet de policy geïmplementeerd worden voor alles gebruikers.

##### Aanpak

Via Ad kan de Admin de nieuwe polices implementeren voor alle grebruikers.

##### Mogelijke of gewenste resultaat

Net als bij de test zal er geen error te voorschijnkomen. Alles zal vlot moeten werken zoals ondervonden tijdens de test.

##### Vaststellingen

##### Advies

Na de goedkeuring van de opdrachtgever kan de oplossingen geïmplanteerd worden. Het eerste effect van de oplossing zullen we pas in drie maanden zien. Met deze oplossing moet er niets meer extra gedaan worden alles wordt automatisch gedaan. *(3 dagen)*

### 3.2 Plan van aanpak – Evaluatie

Bij implementatie een test periode van 30 dagen om te zien of alles goed werk, na de 30 dagen is de eerste mogelijkheid om wachtwoorden te wisselen, dat zal de eerste test zijn. Wanneer de gebruikers de wisseling doen kan er dan gecontroleerd worden of alles werkt zoals het hoort.

## **Probleem 4: Redudantie**

### Plan van aanpak – Tijdsduur

#### Taak 1:

Er gaat veel verkeer door de Core switch en er zijn geen redundante wegen naar de verschillende connectie. Dit wordt opgelost met STP. In deze fase gaan we onderzoeken hoe dit toegepast kan worden in het netwerk, hoe de extra bekabelingen gedaan kan worden. *(3 dagen)*

#### Taak 2:

Nu moet de design en de implementatie van de oplossing in elkaar gezet worden. Met pakket tracer kan de topologie getekend worden, om zo een duidelijk beeld te kunnen schetsen van wat er precies moet gebeuren. Deze documenten worden aan de werkgever gegeven voor goedkeuring. *(3 dagen)*

#### Taak 3:

Na de goedkeuring, moet er eerst extra bekabeling gelegd worden daar kunnen we natuurlijk met de configuraties beginnen. *(3 dagen)*

#### Taak 4:

Nadat deze taak afgerond is moet dit getest worden. Om dit te testen moet er een connectie verbroken worden tijdens het versturen van een test pakket, als het pakket toch verstuurd wordt door de andere weg dan is de test geslaagd. *(3 dagen)*

### Plan van aanpak – Evaluatie

Om dit te testen zullen we zoals in taak 4 besproken is test pakketjes versturen over een onderbroken connectie. Door de SPT moet er automatische een nieuwe weg gevonden worden. Dit kan getest worden bij de verschillende connectie om zeker te zijn dat er op de verschillende connectie redundantie is.

## **Probleem 5: Backup**

### Plan van aanpak – Tijdsduur

Taak 1 : onderzoek tftp metode…..*(3 dagen*

Taak2: designe en implementatie …….*(3 dagen*

Taak 3 : testen op mijn pc. En desgine en implementatie van voorstelen*(3 dagen*

Taak 4 : Na de goedkeuring van de opdrachtgever kan de oplossingen geïmplanteerd worden. *(3 dagen*

### Plan van aanpak – Evaluatie

Sammenstellen informatie pakket (20 dagen)