WDM Encrypted

Versleutelde data, de ultieme bescherming tegen cybercriminaliteit

- Encryptie op de optische laag
- Tot zeer hoge bandbreedtes tot en met 100 Gb/s
- Lage latency: < 1 msec. per 100 km
- Beveiliging is protocol-onafhankelijk
- Gecertificeerd FIPS 197 voor AES-256 encryptie
- Gecertificeerd FIPS 140-2 Level 2 voor hardware encryptie
- Gescheiden versleuteling voor authenticatie en encryptie o.b.v. X.509

Meer dan de helft van alle organisaties heeft jaarlijks te maken met een security-incident en cybercriminaliteit groeit met de dag. Het beschermen van data is voor de meeste organisaties dan ook een toenemende zorg. De overheid haakt hierop in met strengere wetgeving die er op toeziet dat organisaties hun data zorgvuldig verwerken én beveiligen. De security risico's minimaliseert u met WDM Encrypted van Eurofiber, waarmee uw datatransport intrinsiek wordt beveiligd.

Versleutelen van data is noodzakelijk

Voor het uitwisselen van data tussen verschillende locaties, wordt meestal een glasvezelverbinding gebruikt. Het glasvezelnetwerk van Eurofiber bevindt zich volledig onder de grond, in een stevige mantelbuis en robuuste hand-hole. Uiteindelijk komt een glasvezelverbinding ergens boven de grond uit. Bijvoorbeeld wanneer de glasvezel het pand binnengaat door een parkeergarage of een algemene MER- of SER-ruimte. Dat deze glasvezel afgetapt wordt is onwaarschijnlijk, maar niet uit te sluiten. Encryptie biedt aantoonbare zekerheid dat afgetapte data onderweg niet bruikbaar is voor de dader. WDM Encrypted van Eurofiber maakt het mogelijk om data die over een netwerk wordt verstuurd veilig te versleutelen.

Hoe werkt encryptie?

Coderingstechnieken zijn een belangrijk onderdeel van gegevensbeveiliging. Hiermee wordt vertrouwelijke informatie beveiligd tegen bedreigingen zoals misbruik via malware en ongeoorloofde toegang door derden. Encryptie is de procedure waarbij gegevens gecodeerd en gedecodeerd worden. Dit gebeurt door toepassing van een algoritme, waardoor deze gegevens niet meer hun oorspronkelijke vorm hebben en niet kunnen worden gelezen zonder een specifieke encryptiesleutel.

eurofiber

Drie soorten encryptie

Encryptie op het netwerk kan op verschillende manieren:

1. **Encryptie via hardware**
   Deelt u veel privacygevoelige en geheime informatie, dan is dit een goede methode. Er wordt namelijk specifieke hardware gebruikt die de encryptiesleutel verzorgd. Als een hacker in deze hardware probeert te komen en hij opent het, dan wordt de sleutel automatisch gewist.
2. **Encryptie via software**
   Bij deze oplossing is het mogelijk om een selectie te maken tussen data die wél of niet versleuteld moeten worden. Een nadeel is dat er meer vertraging wordt gegenereerd, wat de snelheid van de verbinding negatief beïnvloedt.
3. **Encryptie via het fysieke netwerk**
   Deze encryptie oplossing op de optische laag gaat niet ten koste van snelheid of prestaties. Daarbij is de data ook beschermd tegen aftappen tijdens het transport.

De voordelen van optische encryptie

Veel encryptie-oplossingen werken op de IP-laag (OSI-laag 3). Met WDM Encrypted wordt middels hardware en software encryptie op de optische laag toegepast (OSI-laag 1). Het voordeel hiervan is dat de latency tot duizend keer lager is. Bovendien is de beveiligingsslaag transparant en protocol onafhankelijk.

Onderliggende connectiviteitsdienst

Om een glasvezelverbinding efficiënt in te zetten, bijvoorbeeld tussen datacenter locaties, wordt de connectiviteitsdienst WDM (Wavelength Division Multiplexing) gebruikt waarop de encryptie wordt toegepast. Over dezelfde glasvezel, door het gebruik van verschillende frequenties, kunnen meerdere beveiligde verbindingen worden opgezet, zoals Fiber Channel voor storage en Ethernet voor servers.

FIPS 140-2 Level 2 en X.509 standaard

WDM Encryped van Eurofiber is FIPS 197 gecertificeerd voor AES-256 encryptie en FIPS 140-2 Level 2 voor encryptie hardware. Dit is een door de US federale overheid gehanteerde encryptienorm, die steeds meer navolging krijgt door centrale overheden, de financiële sector en de zorgsector. Het is de hoogste standaard (hoger dan de Duitse BSI) die meetbaar en te valideren is. Daarnaast maakt WDM Encrypted gebruik van de wereldwijde X.509 certificaten voor versleuteling van data en authenticatie. Het certificaat wordt geauthentiseerd en geverifieerd door de internationaal geaccepteerde digitale Public Key Infrastructuur (PKI).

Sleutelbeheer in eigen hand

Om de veiligheid verder te vergroten, faciliteren we uw organisatie om het sleutelbeheer zelf uit te voeren. Zo houdt u de regie over het uitgeven en controleren van de encryptiesleutels waarbij uw eigen PKI als basis dient. Er is geen derde partij nodig voor het sleutelbeheer. Hiermee wordt het risico dat data in handen van derden komt, verder verkleind. Eurofiber helpt u op weg met de configuratie van de software voor sleutelbeheer en traint de security officer.

Service Level Agreement

WDM Encrypted heeft, afhankelijk van de configuratie, een beschikbaarheid van minimaal 99,9% per jaar. Als de dienst onverhoopt niet beschikbaar is, kunt u 24/7 contact opnemen met het Eurofiber Network Monitoring Centre om het probleem te melden. Bij een bedrijfskritische storing garanderen we dat deze binnen 4 uur* na melding is verholpen.

Gewapend tegen cybercriminaliteit

Hackers staan niet stil en ontwikkelen steeds nieuwe manieren om gevoelige gegevens van derden in handen te krijgen. Bescherm uw data met WDM Encrypted van Eurofiber. Zo bent u beter gewapend tegen de toenemende cybercriminaliteit en voldoet u aan de strenger privacywetgeving.

*In het geval van een glasvezelbreuk bedraagt de reparatietijd maximaal 8 uur.

Drie oplossingen op maat

WDM Encrypted wordt mede bepaald door de specifieke toepassing voor uw situatie, maar kent drie basis proposities:

1. Site-to-site verbinding

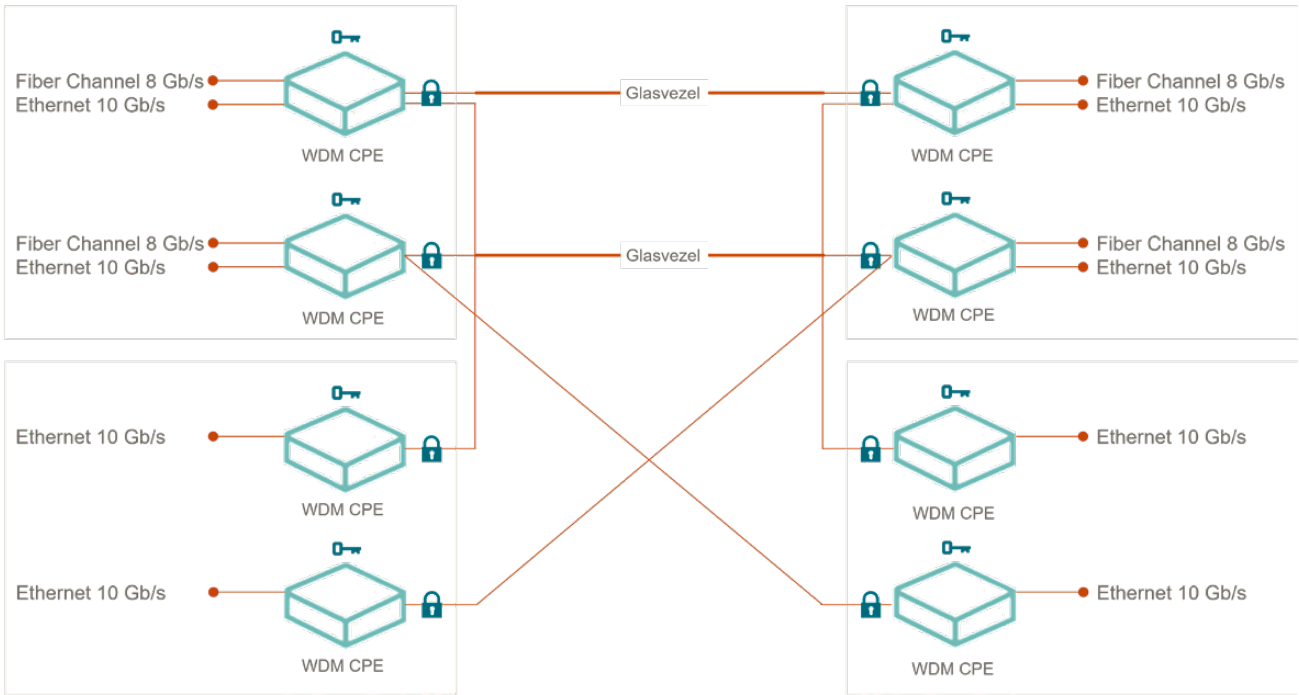
Deze oplossing voorziet in een enkelvoudige versleutelde LAN-koppeling tussen twee locaties waarbij een bepaald protocol en bandbreedte kan worden gekozen.

In dit voorbeeld is de verbinding geconfigureerd met tweemaal 10 Gb/s Ethernet. De beschikbaarheid van de verbinding bedraagt 99,9% per kalenderjaar.

2. Twin DCI verbinding

Deze oplossing voorziet in een volledig gescheiden redundante koppeling tussen twee datacenters ten behoeve van data replicatie. Er is een breed scala aan bandbreedtes beschikbaar voor Ethernet- en Fiber Channel protocollen. In dit voorbeeld is op iedere route 1x Fiber Channel met een bandbreedte van 8 Gb/s en 1x Ethernet met een bandbreedte van 10 Gb/s geconfigureerd. De gecombineerde beschikbaarheid van de oplossing bedraagt 99,98% per kalenderjaar.

3. Twin DCI + Sites



Deze oplossing is een combinatie van de bovengenoemde Twin DCI oplossing en een redundante verbinding vanaf twee locaties naar beide datacenters. Naast hetgeen is beschreven bij Twin DCI worden beide sites verbonden met een datacenter en Ethenet -verbinding van 10 Gb/s. Deze configuratie wordt vaak toegepast in een private cloud omgeving, waarin bedrijfs- kritische applicaties zijn gehost in de datacenters en vanuit de kantoorlocaties worden benaderd.

Contact

Neem voor meer informatie over WDM Encrypted
contact op met onze salesafdeling,
via +31 (0)30 242 87 00 of info@eurofiber.com.