BEYAZ KAĞIT

OT Ağı Çevre Bütünlüğünü Koruyun

Ağınızın Güvenliğini Tek Yönlü Donanım Tabanlı Data Diyot TAP'ler ile Nasıl Sağlayabilirsiniz

GARLAND TECHNOLOGY

Value-Added Distributor
OTD BİLİŞİM
www.onlineteknikdestek.com

ICT OTD PREFER EXPERIENCE ONLINE Since 2011

İÇİNDEKİLER TABLOSU

OT AĞI ÇEVRE BÜTÜNLÜĞÜNÜ KORUYUN

Ağınızın Güvenliğini Tek Yönlü Donanım Tabanlı Data Diyot TAP'ler ile Nasıl Sağlayabilirsiniz

3 | Giriş

4 | OT Ortamlarındaki Görünürlük Problemleri

5 | Kritik Sistemlerinize Erişimi Nasıl Engelleyebilirsiniz

6 | Kritik Sistemlerinize Erişimi Nasıl Engelleyebilirsiniz

7 | Data Diyot TAP'ler nasıl çalışır?

10 | Ortamınıza Data Diyot TAP'leri nasıl ekleyebilirsiniz

14 | Tek Yönlü Diyot TAP'leri Test Etme

Kendinizi Tek Yönlü Görünürlük Başarısına Hazırlayın

GİRİŞ

Günümüzün kritik altyapı düzenlemesi WiFi, internet ve telefonlarla ile kurduğumuz en basit bağlantıdan enerji, su, imalat ve ulaşım sistemleri gibi kıymetini bilemediğimiz kaynaklara kadar yaşadığımız bağlı dünyanın temel yapı taşlarını oluşturur. Savunma Bakanlığı ve birçok Federal kuruluş gibi ulusal güvenliğimiz dahi benzer operasyonel teknoloji (OT) ortamlarına bağlıdır. Bu kritik altyapı toplumumuza devamlı ve güvenilir kaynaklar sağlar ve ne pahasına olursa olsun korunması gerekir.

Siber Güvenlik Tehditlerine karşı OT Yeni Sınır

Gartner'ın En İyi OT Güvenlik Uygulamalarına göre, "2021 yılına kadar varlık merkezli kuruluşların %25'i uzman OT güvenlik teknolojisinin yanı sıra kullanılan geleneksel güvenlik ile operasyonel teknoloji (OT) ortamlarının güvenliğini sağlamak için hibrit bir model kullanacaktır, ki bu oran 2018'de %10 olarak belirlenmiştir.

Diğer bir deyişle, modern OT ve BT ortamlarının yakınsamasından ve operasyonların verimliliğini, performansını ve hizmetlerin kalitesini geliştirme amacından kaynaklanan güvenlik sorunları giderek büyüyen bir tehdittir. Endüstriyel spektrum genelinde kuruluşları bu zorlukları gidermek üzere ağ görünürlüklerini yeniden değerlendirmeye zorlamak önemli bir ilk adımdır.

Bu zayıflık, hackerın tesis kontrol sistemine eriştiği ve sudaki sudkostik miktarını tehlikeli seviyelere çıkardığı son Oldsmar, Florida su sistemleri saldırısı sırasında görülmüştür. Geleneksel güvenlik duvarları ve sanal özel ağ (VPN) erişimi bazen sistemleri dış saldırılara maruz bıraktığı gerçeğini vurgulamak gerekir.

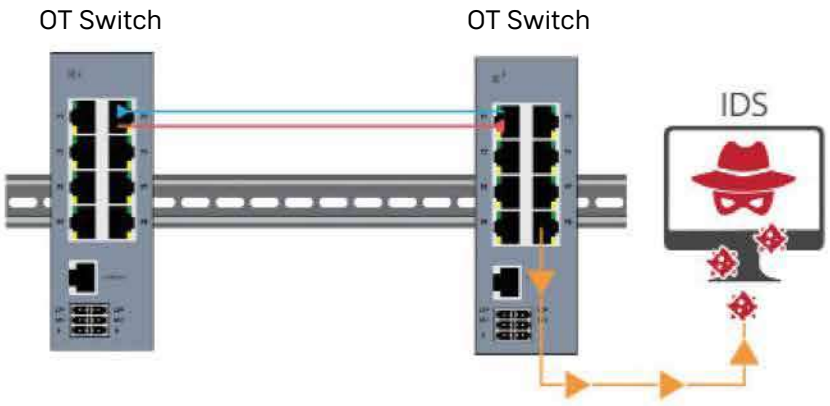
OT ORTAMLARINDAKİ GÖRÜNÜRLÜK PROBLEMLERİ

Bazı OT ortamları, koruma sağlamak üzere tasarlanmış ağ altyapısı ile ağ segmentlerini gelen tehditlere karşı korumada problemler yaşamaktadır. Bu durumlar segmentler veya tesisler arasında tek yönlü bir veri transferi gerektirmektedir. Tek yönlü veri akışı OT ağlarını dış tehditlere karşı koruyacak ve güç iletim ve dağıtıma ilişkin AB siber güvenlik yönetmeliklerine uygunluğu sağlayacak şekilde tasarlanmıştır:

· NERC CIP v5 düzenlemeleri3
· NRC kılavuzları

Ortak görünürlük kullanım gereklilikleri Switch üzerindeki SPAN portundan bir güvenlik veya izleme aracına yansımalı trafik yönlendirmektir. SPAN (Switch Port Analizörü) olarak da bilinen port yansıtması bir ağ Switch'i üzerinde paketlerin analiz edilebileceği belli bir port üzerinde görülen ağ paketlerinin yansıtmaya veya kopya göndermeye programlanmış bir portudur.

· İzleme için paketlere erişim sağlar.
· SPAN oturumları Switch'in normal çalışmasına müdahale etmez.
· Switch'e bağlı olan herhangi bir sistem üzerinden konfigüre edilebilir.



Konsept yeterince basit — Switch zaten ortama yönelik tasarlanmıştır. Sadece güvenlik çözümünüze bağlamanız yeterli. Tamamdır. Ancak pek çok zaman en basit yol en iyi yol değildir.

SPAN görünürlüğünün en çok zorlandığı konular şunlardır:

· SPAN'ın Switch üzerinden yüksek değere sahip portlar alması
· Bazı eski Switch'lerin mevcut SPAN portları olmaması
· SPAN portlarının güvenlik ve düzenleme çözümleri için ekstra bir risk olan paketler bırakabilmesi

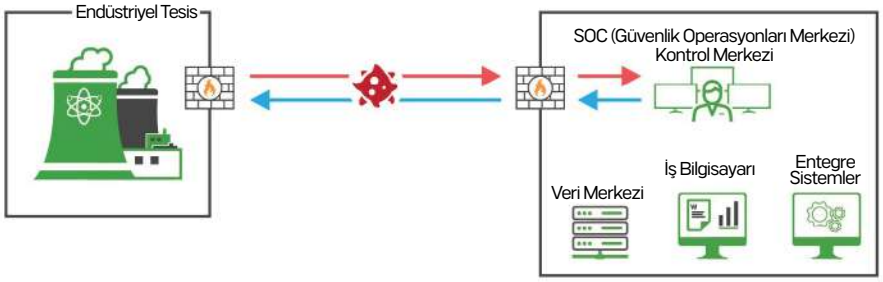
SPAN kavramı mevcut olduğu için kulağa kolay gelebilir, ancak paket kaybın ve değiştirilmiş çerçeveleri tarttıktan sonra ek SPAN güvenliği hususları şunları içermektedir:

· İki yönlü trafik trafiğin ağa doğru arka akışını sağlar, bu da Switch'i ele geçirilmeye yatkın hale getirir.
· SPAN için idare/programlama maliyetleri devamlı olarak daha zaman yoğun ve maliyetli olur.

OT ortamları gibi kritik ağ kullanımlarında sadece SPAN kullanımı kabul edilmez.

KRİTİK SİSTEMLERİNİZE UZAKTAN ULAŞMAK İSTEYEN TEHDİTLER NASIL ENGELLENİR

Bazı ICS ortamları, koruma sağlamak üzere tasarlanmış ağ altyapısı ile kritik ağ segmentlerini gelen tehditlere karşı korumada problemler yaşamaktadır. OT ve BT ağ ortamlarının birçoğu tehditleri analiz etmek ve tehditlere yanıt vermek üzere güvenlik ve izleme araçlarına bant dışı Ethernet paket kopyaları gönderir. Birçok görünürlük mimarisi veya yapısı söz konusu analiz için bu bant dışı trafiği ayrı tesislerden merkezi veya kurumsal bir ağa iletir. Bu BT çözümleri ve entegre sistemler, bu etkileşimsiz altyapıyı dış saldırı ve tehditlere dolaylı olarak maruz bırakarak ağı İnternete bağlar.

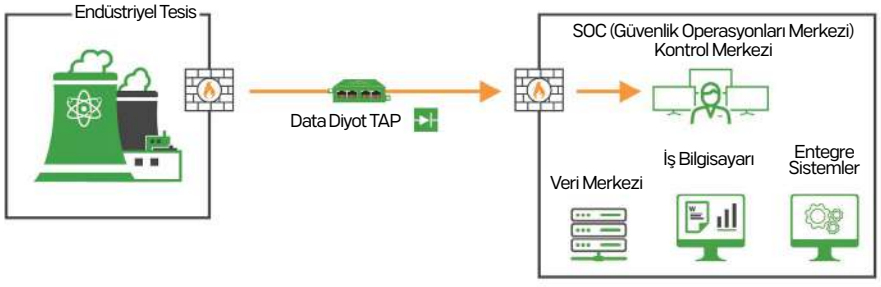


Şema 1, kötü amaçlı aktivitenin iki yönlü trafik ile farklı tesis segmentleri arasında nasıl iletildiğini ve ağı etkisi altına alabildiğini göstermektedir.

Bu sorunları gidermek için segmentler veya tesisler arasında tek yönlü bir veri transferi gerekli olabilir. Güvenlik duvarları, saldırı tespit sistemleri (IDS) ve güvenlik bilgileri ve olay yönetimi (SIEM) gibi modern OT/BT güvenlik araçlarına ek olarak, hızlı bir şekilde kritik ICS altyapısının kilit unsuru haline gelen bir donanım parçası vardır — data diyotları.

Data diyotlarında tek yönlü veri akışı, izlemek için gerekli olan bant dışı veri akışını sağlarken OT ağ segmentlerine gelen veri akışını ve nihayetinde dış tehditleri de ortadan kaldırarak OT ağlarını dış tehditlere karşı güvenlik altına alacak şekilde tasarlanmıştır.

Data Diyot TAP teknolojisi, mühendislerin sıklıkla doğrudan saldırı tespit sistemlerine (IDS) veya segment tesisleri arasında izleme araçlarına bağlandıkları bir ağ Switch'inden gelen SPAN portlarına kıyasla daha güvenli bir seçenektir. SPAN portları güvenlik zayıflıklarını gizleyerek yalnızca paket bırakmazlar, SPAN aynı zamanda Switch'i ele geçirilmeye yatkın hale getirerek trafiğin ağ doğru arka akışını açan iki yönlü trafiğe sahiptir.

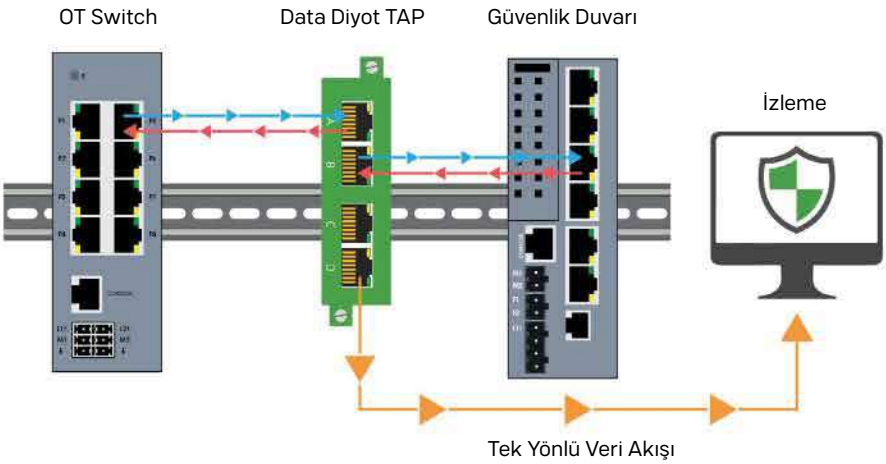


Diyagram 2, tek yönlü trafiğin farklı tesis bölümlerinden iletilen trafiğin emniyetli kalmasını sağlamaya nasıl yardım ettiğini göstermektedir.

Data diyotları en yaygın olarak federal savunma ve Endüstriyel IoT gibi farklı güvenlik sınıflarının iki veya daha fazla ağı arasındaki bağlantı görevini gördüğü yüksek güvenlik ortamlarında bulunabilir. Bu teknoloji şu anda nükleer güç tesisleri, elektrik üretim ve demiryolu ağları gibi güvenlik kritik sistemler gibi tesisler için endüstriyel kontrol düzeyinde bulunabilir.

DATA DİYOT TAP'LER NASIL ÇALIŞIR?

Data Diyot TAP'ler ham verilerin yalnızca tek yönlü çalışmasına izin veren özel amaçlı ağ donanım cihazlarıdır. Data Diyot TAP'ler endüstriyel kontrol sistemleri gibi bilgi güvenliğini veya kritik dijital sistemlerin örneğin gelen siber saldırılardan korunmasını sağlayan bir trafik uygulayıcısı olarak kullanılabilir.

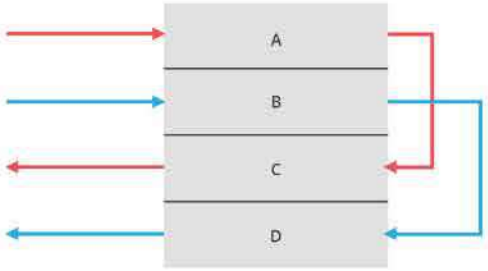


Şema 3, trafiğin varış yerinden güvenlik altına alınmasını sağlayarak bir data diyot TAP'in bir ağ segmentine nasıl yerleştirileceğini göstermektedir.

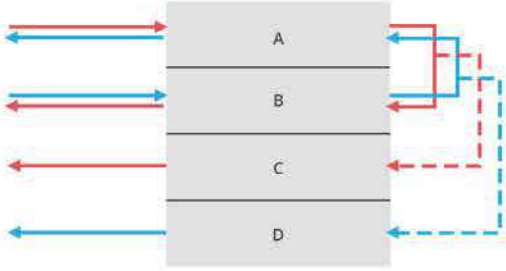
Bir network TAP devamlı olarak 365 gün 7/24 iki taraflı trafik akışının tam kopyasını oluşturur ve paket bırakmaz, gecikme yaratmaz veya verileri değiştirmez. Pasif veya "arıza emniyetli"dir, yani elektrik kesintisi olduğunda veya izleme aracı çıkarıldığında tek hata noktasının olmaması sağlanarak trafiğin ağ cihazları arasında akmaya devam etmesi anlamına gelir. Data Diyot TAPler de bant dışı trafiğin ağa geri dönüş yolu bulamamasını sağlayacak ekstra güvenlik ile Network TAP'ler ile aynı yüksek kalitede görünürlük sağlar.

Endüstride yaygın olarak kullanılan yazılım tabanlı Data Diyot ağ geçitlerinden farklı olarak bunlar donanım tabanlıdır. Donanım tabanlı olması konfigüre edilmesi gereken karmaşık yazılım veya ekstra bir yazılım hatası olmaması anlamına gelir. Data Diyot TAP'ler tak çalıştır özelliktedir ve nezaret gerektirmez.

Bu cihazlar A ve B arayüz portları aracılığıyla trafiği içeri alır. Veriler A Portundan C Portuna doğru akar, ancak C Portundan A Portuna herhangi bir bağlantı yoktur. Bu B Portu ve D Portu için de geçerlidir. Bu, C Portundan A/B Portuna veya D Portundan A/B Portuna herhangi bir veri akışı olamayacağı anlamına gelir.



Bu şema 4 portu göstermektedir (A, B, C, D). Data Diyot SPAN TAP, C Portundan A Portu akış trafiğini ve D Portundan B Portu akış trafiğini göstermektedir.



Bu şema 4 portu göstermektedir (A, B, C, D). Data Diyot Network TAP, B Portundan A Portunu akışını gösterir ve C Portundan bir kopya gönderir ve A Portundan B Portu akışını gösterir ve D Portundan bir kopya gönderir.

ORTAMINIZA DATA DİYOT TAP'LERİ NASIL EKLEYEBİLİRSİNİZ

Kullanım sırasında, bağlantı stratejiniz ve tasarımınıza uygun farklı faktörler vardır. Tek yönlü güvenliği sağlarken, 3 ana donanım tabanlı data diyot TAP'e dikkat edilmesi gerekir: Network TAP'ler, SPAN TAP'ler ve Aggregator TAP'ler.

Bunların her biri ağınızın performansı ve güvenliği için görünürlüğü optimize etmeye yönelik özel görünürlük ihtiyacını karşılar, ancak hepsinde ağ trafiğinizin güvenliğini korumak için Data Diyot işlevine dayanan Garland Technology donanımı bulunur.

Data Diyot Network TAP'ler

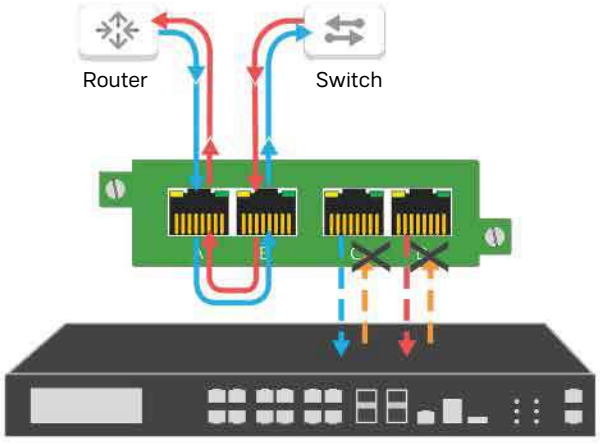
Data Diyot Network TAP'ler kritik bağlantıyı destekleyen ağ Switch'i ve güvenlik duvarı gibi iki aracı bağlayan bir ağ segmentinde yer alır. Data Diyot TAP'ler bu trafiğin tek yönlü bir kopyasını iki araç arasındaki bağlantı etkilenmeden bant dışı izleme araçlarına gönderir. Data Diyot izleme portları ile ağ arasında fiziksel bir bağlantı yoktur, varış yerinden herhangi bir saldırı riski ortadan kaldırılmıştır.

· Farklı güvenlik gereksinimlerine sahip ağ segmentleri arasındaki veri akışlarının kaynağını korur.
· Fiziksel donanım separasyonu ağ segmentleri arasındaki tek yönlü trafiği garanti altına alır.
· Tap 'kesintisi', yığınını, rejenerasyonunu / SPAN modu destekler.

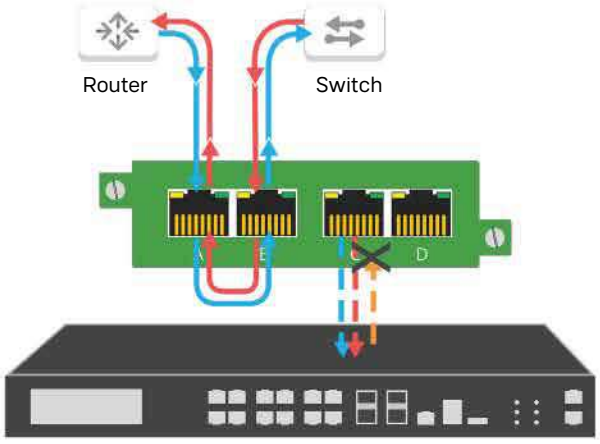
Bu senaryoda bir bağlantıya DOKUNABİLİR ve paket ağa geri gönderilmeden trafiğin tek yönlü 'Kesinti' kopyalarını sağlayabilirsiniz.

Ürün Detayları

Data Diyot SPAN TAP
10M/100M/1000M (1G) Tek yönlü data diyodu devre tasarımı
Model # PT100
Model # P1GCCB
Model # P1GCCAS
Model # P1GMCA
Model # P1GMSA
Model # P1GSCA
Model # P1GSSA
Model # P100FXCA



Bu senaryoda 2 SPAN portunun her birinin ağa geri paket gönderimi yapmadan 1 tek yönlü trafik kopyası oluşturmasını sağlayabilirsiniz.



Bu senaryoda 1 SPAN portunun ağa geri paket gönderimi yapmadan 1-3 tek yönlü trafik kopyası oluşturmasını sağlayabilirsiniz.

Data Diyot SPAN TAP

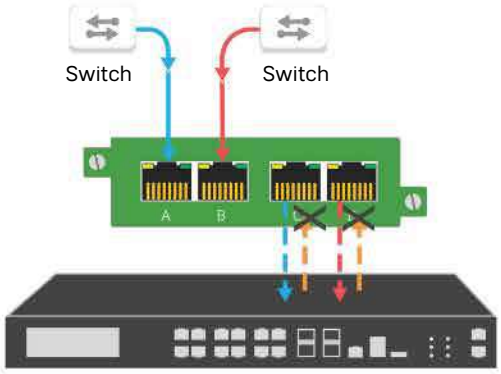
Data Diyot SPAN TAP'ler bant dışı izleme için ağ trafiği sağlar, özellikle trafiği ağa geri gönder-meyecek şekilde tasarlanmıştır. Bu özel amaçlı ağ donanım cihazları, endüstriyel kontrol sistemleri (ICS) gibi kritik dijital sistemlerin gelen siber tehditlerden korunmasını sağlaya-rak fiziksel donanım separasyonu ile Switch SPAN bağlantıları için tek yönlü bir veri akışı gerçekleştirir.

· Farklı güvenlik gereksinimlerine sahip ağ segmentleri arasındaki SPAN portları gibi veri akışlarının kaynağını korur.
· Fiziksel donanım separasyonu ağ segmentleri arasındaki tek yönlü trafiği garanti altına alır.
· Rejenerasyonu / SPAN modu destekler.

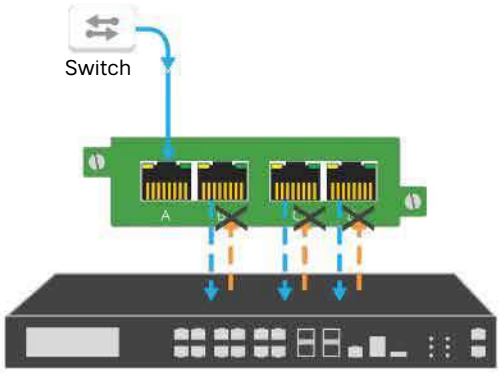
Ürün Detayları

Data Diyot SPAN TAP
10M/100M/1000M (1G) Tek yönlü data diyodu devre tasarımı

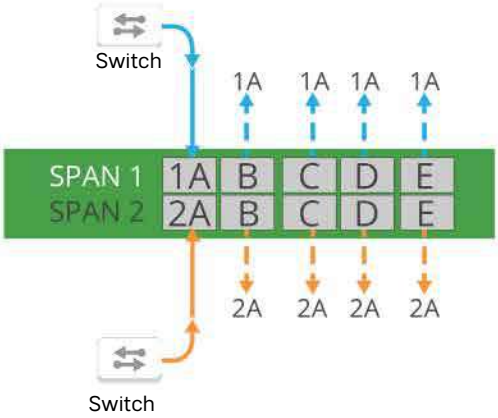
Model # P1GCCAS-Custom
Model # CTAP-P1GCCREG
Model # INT10G10SP1



Bu senaryoda 2 SPAN portunun her birinin ağa geri paket gönderimi yapmadan 1 tek yönlü trafik kopyası oluşturmasını sağlayabilirsiniz.



Bu senaryoda 1 SPAN portunun ağa geri paket gönderimi yapmadan 1-3 tek yönlü trafik kopyası oluşturmasını sağlayabilirsiniz.



Bu senaryoda 2 SPAN portunun her birinin ağa geri paket gönderimi yapmadan 1-4 tek yönlü trafik kopyası oluşturmasını sağlayabilirsiniz.

AggregatorTAP: Data Diyotları

AggregatorTAP: Data Diyotları bant dışı izleme için ağ trafiği sağlar, özellikle trafiği ağa geri göndermeyecek şekilde tasarlanmıştır. Bu özel amaçlı ağ donanım cihazları, endüstriyel kontrol sistemleri (ICS) gibi kritik dijital sistemlerin gelen siber tehditlerden korunmasını sağlayarak fiziksel donanım separasyonu ile Switch SPAN bağlantıları için çoklu ağ segmentlerinden bir izleme varış noktasına doğru tek yönlü bir veri akışı gerçekleştirir.

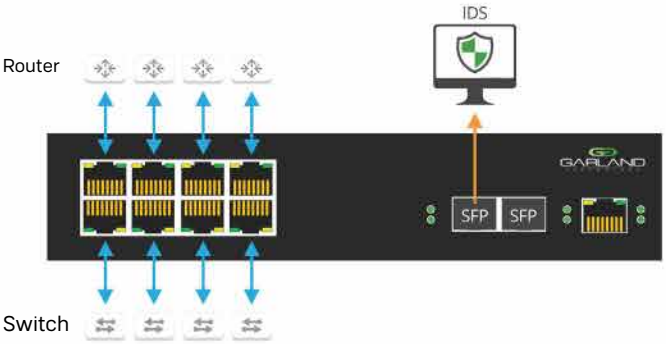
· Farklı güvenlik gereksinimlerine sahip ağ segmentleri arasındaki veri akışlarının kaynağını korur.
· 1 veya 2 izleme portuna doğru 4'e kadar TAP bağlantısı toplar.
· 1 veya 2 izleme portuna doğru 8'e kadar SPAN bağlantısı toplar.

Ürün Detayları

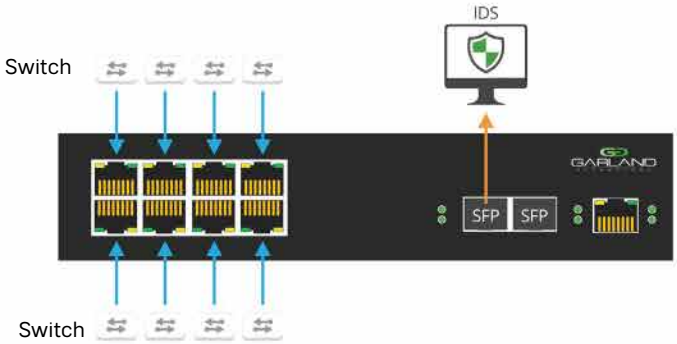
AggregatorTAP: Data Diyodu
10M/100M/1000M (1G) T1U ½ raf | Yığın Rejenerasyon | Tek yönlü data diyot devre tasarımı

Model # INT1G10CSA
Model # INT1G10CSA-DC
Model # INT1G10CSASP
Model # INT1G10CSASPDC

SPAN'ı koruyarak izleme portlarına giden tek yönlü bir iletişim yolunun fiziksel olarak korunmasını sağlar.

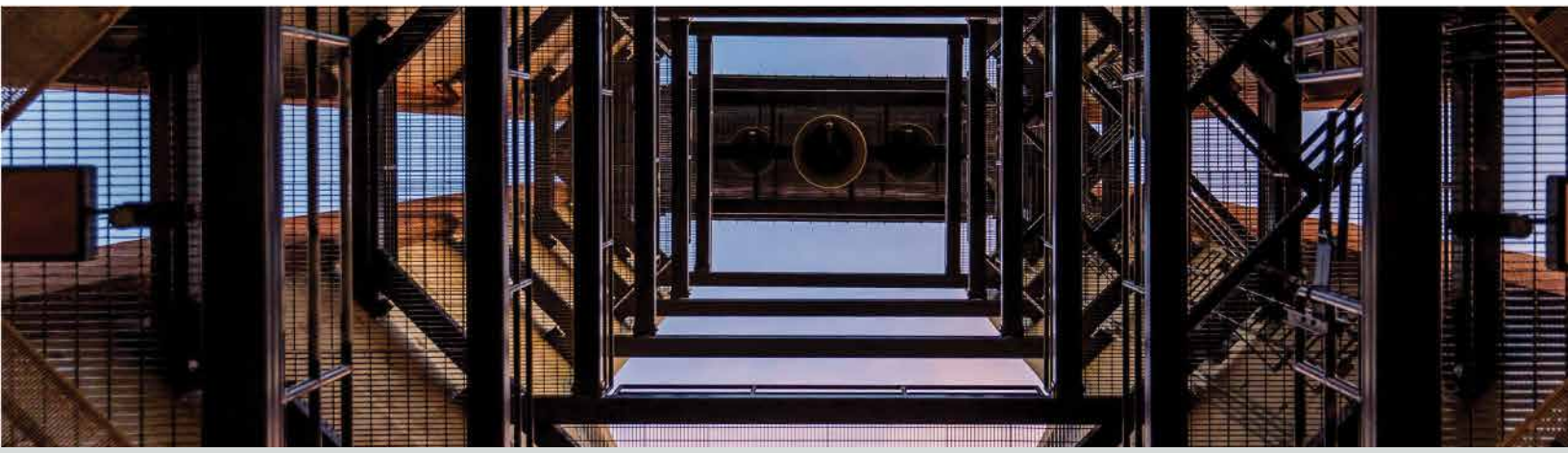


Bu senaryoda 4 bağlantıya DOKUNABİLİR ve ağa geri paket gönderimi yapmadan bir veya iki porta toplanan trafiğin tek yönlü TAP kopyaları sağlayabilirsiniz.



Bu senaryoda 8 SPAN portunun her birinin ağa geri paket gönderimi yapmadan bir veya iki tek yönlü trafik kopyası oluşturmasını sağlayabilirsiniz.

Bu özel tasarlanan TAP'ler 10/100/1000M ağları için "enjeksiyonsuz" TAP görünürlüğü sağlar. Bu donanım tabanlı tek yönlü veri transferi hiçbir Ethernet paketinin fiziksel olarak canlı Ağ TAP portlarına veya SPAN portlarına gönderilmemesini sağlar.· 1 veya 2 izleme portuna doğru 4'e kadar TAP bağlantısı toplar.
· 1 veya 2 izleme portuna doğru 8'e kadar SPAN bağlantısı toplar.



ÜRÜN TESTİ

TEK YÖNLÜ DİYOT TAP'LERİ TEST ETME

Toplam Kalite Taahhüdü: Garland Technology özel test ve kabul sürecinin tüm kalite kontrollerden geçmesini sağlar. Örnek testinin yeterli düzeyde kanı sağlamadığına inanmadığımız için, müşteriye göndermeden önce canlı ağa sahip her cihazı test ediyoruz. Toplam geri dönüş oranı %0.5'ten azdır ve ilk geçiş oranı (FTPR) %0'dır.

Tek yönlü veri transferini doğrulamak için yapılan güvenlik testlerinde, Garland Technology'nin Data Diyot TAP'lerinin beklenen şekilde performans gösterip göstermediğini ve paketleri ağ portlarına geri göndermediğini görmeyi amaçlıyoruz.

DATA DİYOT TAP TESTİ 1

Test Tarihi: 07/09/20
Testi Gerçekleştiren: Mike Heiberger, Donanım Mühendisi, Garland Technology
Test 1 Ekipmanı: Xena Ethernet Tester
Test edilen ürün Modeli #: CTAP-P1GCCREG

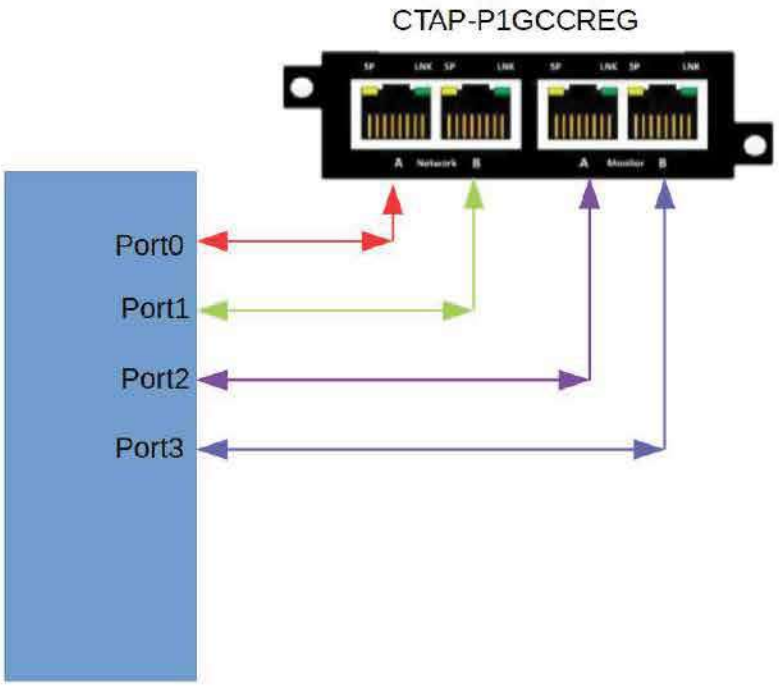
Tüm portları test ekipmanına bağlayın.

1. A Portuna 1000 paket gönderin ve 1000 paketin YALNIZCA C Portundan çıktığını gösterin.
2. B Portuna 1000 paket gönderin ve 1000 paketin YALNIZCA D Portundan çıktığını gösterin.

3. C Portuna 1000 paket gönderin ve bu paketlerin kutumuza doğru akma izinlerinin olmadığını gösterin.

4. D Portuna 1000 paket gönderin ve bu paketlerin kutumuza doğru akma izinlerinin olmadığını gösterin.

TEST KURULUMU



Xena Ethernet Tester

Test #1 – Xena port0'dan 1000 paket iletilir.

Beklenen sonuçlar = 1000 paket yalnızca Xena port2'e alınır.

Ana Port Trafik İstatistikleri

İsim	TX (%	TX L1 (bit/s	TX L2 (bit/	TX (pps)	TX (bayt)	TX (paket)	RX (%)	RX L1 (bit/s)	RX L2 (bit/	RX (pps)	RX (bayt)	RX (paket)
P-3-0-0	0.000	0	0	0	4,447,393	1,000	0.000	0	0	0	0	0
P-3-0-1	0.000	0	0	0	0	0	0.000	0	0	0	0	0
P-3-0-2	0.000	0	0	0	0	0	0.000	0	0	0	4,447,393	1,000
P-3-0-3	0.000	0	0	0	0	0	0.000	0	0	0	0	0

Test #2 – Xena port1'den 1000 paket iletilir.

Beklenen sonuçlar = 1000 paket yalnızca Xena port3'e alınır.

Ana Port Trafik İstatistikleri

İsim	TX (%	TX L1 (bit/s	TX L2 (bit/	TX (pps)	TX (bayt)	TX (paket)	RX (%)	RX L1 (bit/s)	RX L2 (bit/	RX (pps)	RX (bayt)	RX (paket)
P-3-0-0	0.000	0	0	0	0	0	0.000	0	0	0	0	0
P-3-0-1	0.000	0	0	0	4,447,393	1,000	0.000	0	0	0	0	0
P-3-0-2	0.000	0	0	0	0	0	0.000	0	0	0	0	0
P-3-0-3	0.000	0	0	0	0	0	0.000	0	0	0	4,447,393	1,000

Test #3 – Xena port2'den 1000 paket iletilir.

Beklenen sonuçlar = 1000 paket yalnızca Xena port3'e alınır.

Ana Port Trafik İstatistikleri

İsim	TX (%	TX L1 (bit/s	TX L2 (bit/	TX (pps)	TX (bayt)	TX (paket)	RX (%)	RX L1 (bit/s)	RX L2 (bit/	RX (pps)	RX (bayt)	RX (paket)
P-3-0-0	0.000	0	0	0	0	0	0.000	0	0	0	0	0
P-3-0-1	0.000	0	0	0	0	0	0.000	0	0	0	0	0
P-3-0-2	0.000	0	0	0	4,447,393	1,000	0.000	0	0	0	0	0
P-3-0-3	0.000	0	0	0	0	0	0.000	0	0	0	0	0

Test #4 – Xena port3'den 1000 paket iletilir.

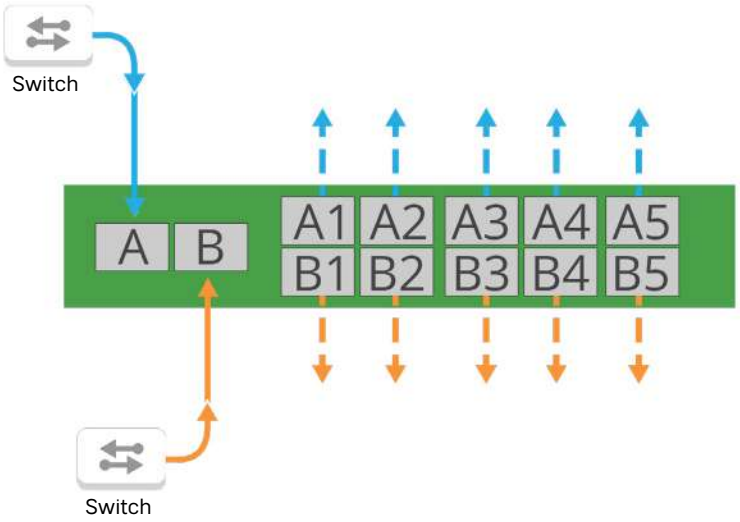
Beklenen sonuçlar = Herhangi bir Xena portuna 0 paket alınır.

Ana Port Trafik İstatistikleri

İsim	TX (%	TX L1 (bit/s	TX L2 (bit/	TX (pps)	TX (bayt)	TX (paket)	RX (%)	RX L1 (bit/s)	RX L2 (bit/	RX (pps)	RX (bayt)	
P-3-0-0	0.000	0	0	0	0	0	0.000	0	0	0	0	0
P-3-0-1	0.000	0	0	0	0	0	0.000	0	0	0	0	0
P-3-0-2	0.000	0	0	0	0	0	0.000	0	0	0	0	0
P-3-0-3	0.000	0	0	0	4,447,393	1,000	0.000	0	0	0	0	0

DATA DİYOT TAP TESTİ 2

Test Tarihi: 07/13/20
Tüm SFP+ portları test ekipmanına bağlanır.-
Test 1 Ekipmanı: Xena Ethernet Tester
Test edilen ürün Modeli #: INT10G10SP1



Tüm SFP+ portları test ekipmanına bağlanır.

1. Giriş portu olan sol üstteki porta 1000 paket gönderin.

· 1000 paketin tamamının yalnızca o portun sağında yer alan 4 porttan çıktığını gösterin.

2. Giriş portu olan sol alttaki porta 1000 paket gönderin.

· 1000 paketin tamamının yalnızca o portun sağında yer alan 4 porttan çıktığını gösterin.

3. 8 izleme portuna 1000 paket gönderin ve bu paketlerin kutumuza doğru akma izinlerinin olmadığını ve net bir şekilde bırakıldığını gösterin.

On (10) portun tamamı 10G SFP+ kafesidir.

INT10G10SP1'deki tüm portlar aşağıdaki tabloda gösterildiği üzere Xena 10G Test Setine bağlıdır:

Xena10G Test Seti Port Numarası	INT10G10SP1 Port Numarası
P-0-4-0	1A
P-0-4-1	1B
P-0-4-2	1C
P-0-4-3	1D
P-0-4-4	1E
P-0-5-0	2A
P-0-5-1	2B
P-0-5-2	2C
P-0-5-3	2D
P-0-5-4	2E

1. 1A Portuna 1000 paket gönderir. 1000 paketin tamamı yalnızca 1B, 1C, 1D ve 1E portlarından çıkar.

Ana Port Trafik İstatistikleri

İsim	TX (%)	TX L1 (bit/s)	TX L2 (bit/s)	TX (pps)	TX (bayt)	TX (paket)	RX (%)	RX L1 (bit/s)	RX L2 (bit/s)	RX (pps)	RX (bayt)	RX (palet)
P-0-4-0	0.000	0	0	0	100,000	1,000	0.000	0	0	0	0	0
P-0-4-1	0.000	0	0	0	0	0	0.000	0	0	0	100,000	1,000
P-0-4-2	0.000	0	0	0	0	0	0.000	0	0	0	100,000	1,000
P-0-4-3	0.000	0	0	0	0	0	0.000	0	0	0	100,000	1,000
P-0-4-4	0.000	0	0	0	0	0	0.000	0	0	0	100,000	1,000
P-0-5-0	0.000	0	0	0	0	0	0.000	0	0	0	0	0
P-0-5-1	0.000	0	0	0	0	0	0.000	0	0	0	0	0
P-0-5-2	0.000	0	0	0	0	0	0.000	0	0	0	0	0
P-0-5-3	0.000	0	0	0	0	0	0.000	0	0	0	0	0
P-0-5-4	0.000	0	0	0	0	0	0.000	0	0	0	0	0

2. 2A Portuna 1000 paket gönderir. 1000 paketin tamamı yalnızca 2B, 2C, 2D ve 2E portlarından çıkar.

Ana Port Trafik İstatistikleri

İsim	TX (%)	TX L1 (bit/s)	TX L2 (bit/s)	TX (pps)	TX (bayt)	TX (paket)	RX (%)	RX L1 (bit/s)	RX L2 (bit/s)	RX (pps)		RX (palet)
P-0-4-0	0.000	0	0	0	0	0	0.000	0	0	0	0	0
P-0-4-1	0.000	0	0	0	0	0	0.000	0	0	0	0	0
P-0-4-2	0.000	0	0	0	0	0	0.000	0	0	0	0	0
P-0-4-3	0.000	0	0	0	0	0	0.000	0	0	0	0	0
P-0-4-4	0.000	0	0	0	0	0	0.000	0	0	0	0	0
P-0-5-0	0.000	0	0	0	100,000	1,000	0.000	0	0	0	0	0
P-0-5-1	0.000	0	0	0	0	0	0.000	0	0	0	100,000	1,000
P-0-5-2	0.000	0	0	0	0	0	0.000	0	0	0	100,000	1,000
P-0-5-3	0.000	0	0	0	0	0	0.000	0	0	0	100,000	1,000
P-0-5-4	0.000	0	0	0	0	0	0.000	0	0	0	100,000	1,000

3. Sekiz (8) izleme portunun her birine 1000 paket gönderir (1B, 1C, 1D, 1E, 2B, 2C, 2D, ve 2E). Tüm paketler düşürülür, bu da INT10G10SP1'e doğru akma izinlerinin olmadığını gösterir.

Ana Port Trafik İstatistikleri

İsim	TX (%)	TX L1 (bit/s)	TX L2 (bit/s)	TX (pps)	TX (bayt)	TX (paket)	RX (%)	RX L1 (bit/s)	RX L2 (bit/s)	RX (pps)		RX (palet)
P-0-4-0	0.000	0	0	0	0	0	0.000	0	0	0	0	0
P-0-4-1	0.000	0	0	0	100,000	1,000	0.000	0	0	0	0	0
P-0-4-2	0.000	0	0	0	100,000	1,000	0.000	0	0	0	0	0
P-0-4-3	0.000	0	0	0	100,000	1,000	0.000	0	0	0	0	0
P-0-4-4	0.000	0	0	0	100,000	1,000	0.000	0	0	0	0	0
P-0-5-0	0.000	0	0	0	0	0	0.000	0	0	0	0	0
P-0-5-1	0.000	0	0	0	100,000	1,000	0.000	0	0	0	0	0
P-0-5-2	0.000	0	0	0	100,000	1,000	0.000	0	0	0	0	0
P-0-5-3	0.000	0	0	0	100,000	1,000	0.000	0	0	0	0	0
P-0-5-4	0.000	0	0	0	100,000	1,000	0.000	0	0	0	0	0

Test Sonucu

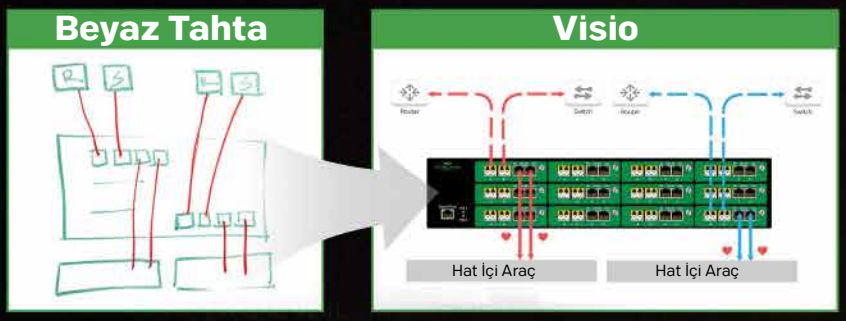
Test, Garland Technology'nin CTAP-P1GCCREG ve INT10G10SP1 Tek Yönlü diyotlarının tek yönlü trafik akışında başarılı olduğu sonucuna varılmıştır.

DATA DİYOT TAP'LERİN NİHAİ HEDEFİ

Ağın süreç içerisinde gelen trafikten kaynaklanan ek zayıflıklar yaratmaksızın uygun şekilde analiz edilmesi ve korunmasını sağlamak adına "Her bit, byte ve paket" sloganıyla OT/BT güvenlik izleme çözümleri sunmaktır. Bu nedenle, modern ICS güvenlik stratejileri bu çözümleri ağ TAP'leri ve paket aracısı görünürlük yapıları ile birlikte kullanmaktadır.

Kendinizi Görselleştirme Başarısına Hazırlayın

Yazılımlarınıza TAP görünürlüğü eklemek istiyor, ancak nereden başlayacağınızı bilmiyor musunuz? Kısa bir ağ Tasarımı - Tasarım-BT danışmanlığı veya deneme sürümü için bize katılın. Zorlama yok - Sevdiğimiz şeyi yapıyoruz.



Daha fazla bilgi almak için lütfen https://www.garlandtechnology.com/design-it adresini ziyaret edin

1- https://industrialcyber.co/article/florida-water-treatment-plant-attack-highlights-dangers-of-remote-access/

2- https://www.nerc.com/pa/CI/Pages/Transition-Program.aspx

Bizimle İletişime Geçin
otd.salesgrp@onlineteknikdestek.com

GARLAND TECHNOLOGY | Value-Added Distributor OTD BİLİŞİM www.onlineteknikdestek.com

ICT OTD PREFER EXPERIENCE ONLINE Since 2011