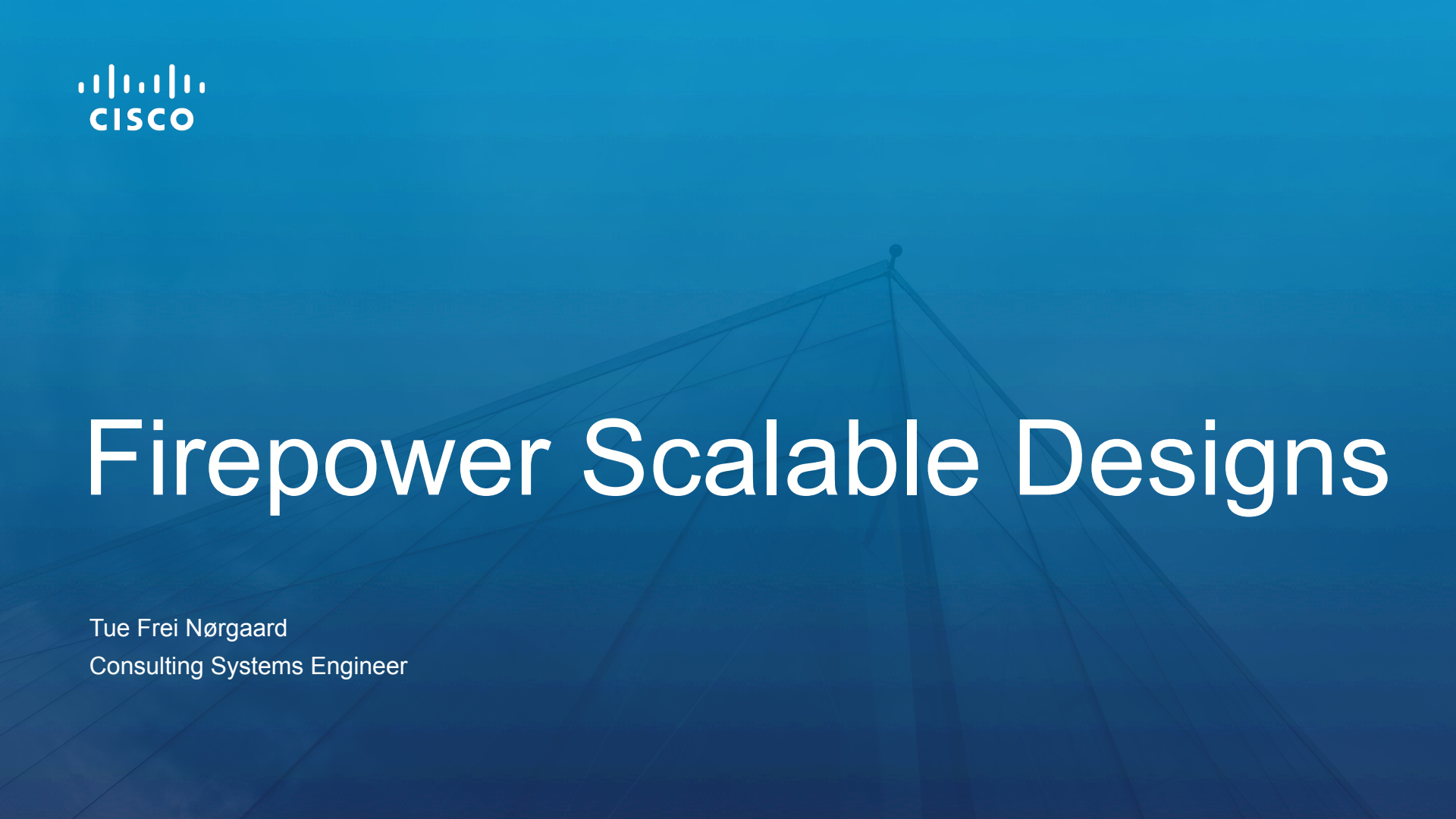


Firepower Scalable Designs

Tue Frei Nørgaard
Consulting Systems Engineer

Agenda

- Velkommen - introduktion
- Unified image – Firepower Threat Defense
- Hardware – 4100, 9300 and ASA 5500-X
- Firepower Management Center
- High Availability and Scalability
- Performance
- Use cases
- Q & A

Next Generation Firewall (NGFW) Essentials

Cisco Collective Security Intelligence Enabled

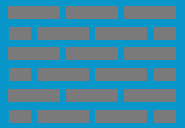
High Availability

NGIPS

Analytics & Automation

Advanced Malware Protection

URL Filtering



Network Firewall
Routing | Switching

Application
Visibility & Control

Built-in Network Profiling

Identity-Policy Control & VPN

One Operating System + One Management

Cisco NGFW Platforms

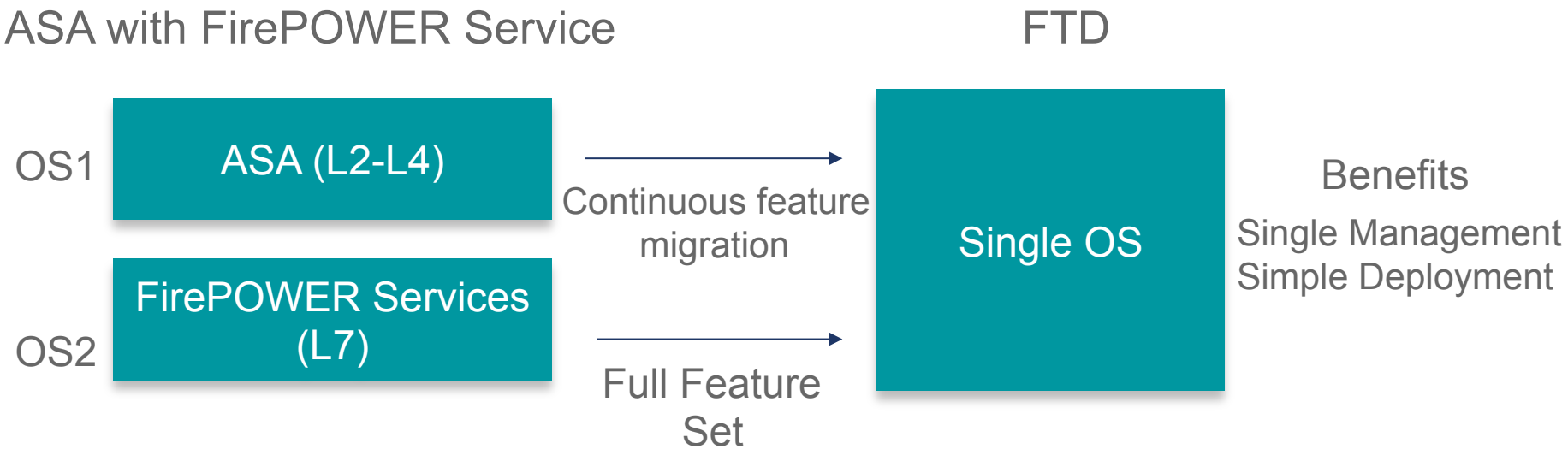
New Appliances

Firepower 4100 Series and Firepower 9300	Firepower Threat Defense for ASA 5500-X*	Firepower Services on ASA 5500-X and 5585-X

All Managed by Firepower Management Center - FMC

* Not ASA5585

Firepower Threat Defense (FTD) is a NGFW SW Platform that Delivers Unified Code (Single OS) and Single Management



Firepower Threat Defense (FTD)

New Converged ASA+FirePOWER Image

- All FirePOWER capabilities plus select ASA features
- Single Manager: Firepower Management Center 6.0*

Same subscriptions as FirePOWER Services

- Delivered via Smart Licensing only
  - Threat (IPS + SI)
  - Malware (AMP + ThreatGrid)
  - URL Filtering

Firepower Threat Defense 6.0.1 ASA features

Unified ASA and Firepower Rules and Objects

ASA Dynamic and Static NAT

ASA Routing Support: OSPFv2, BGP4, RIP, Static, no PIM

Syn Cookies, Anti-Spoofing

ASA ALGs (fixed configuration)

VMware and AWS Support

Smart Licensing Support

* Also manages Firepower Appliances and Firepower Services, but not ASA Software

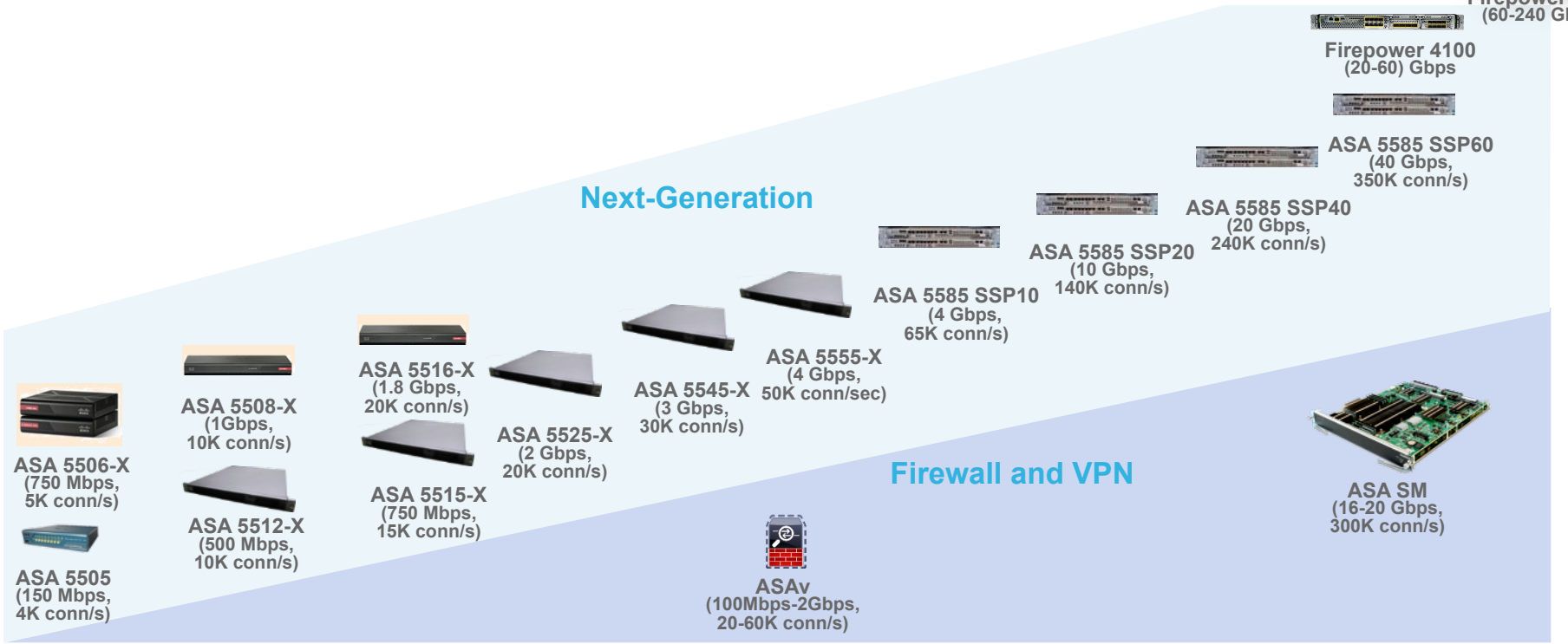
Firepower Threat Defense 6.1 – release July 2016

Software Support by Platform

	Firepower Threat Defense	Firepower NGIPS	ASA Firewall	Firepower Services on ASA
Old (Series 2) FirePOWER Appliances	✗	✗	✗	✗
FirePOWER 7000 Series	✗	✓	✗	✗
FirePOWER 8000 Series	✗	✓	✗	✗
ASA Low-end (5506/08/16)	✓ (reimage)	✗	✓	✓
ASA Mid-Range (5512/15/25/45/55)	✓ (reimage)	✗	✓	✓
ASA High-end (5585 SSP-10/20/40/60)	✗	✗	✓	✓
Firepower 4100, 9300 (SSP 3RU - SM-24/36)	✓	✗	✓	✗
VMware	✓	✓	✓	✗
AWS	✓	✗	✓	✗

Hardware overview

Cisco ASA Firewalls



Platforms and Places in the Network

IPS Performance and Scalability

FirePOWER 8300 Series
15 Gbps – 60 Gbps

FirePOWER 8100/8200
2 Gbps - 10 Gbps

FirePOWER
7120/7125/8120
1 Gbps - 2 Gbps

FirePOWER 7100 Series
500 Mbps – 1 Gbps

FirePOWER 7000 Series
50 Mbps – 250 Mbps

ROBO | Branch | Internet | Campus | Data

Firepower 4100 Overview

Built-in Supervisor and Security Module
- Same hardware and software architecture as 9300
- Fixed configurations (4110, 4120, 4140, 4150)
- **FXOS 1.1.4** for 4110-4140, **2.0.1** for 4150

Solid State Drives
- Independent operation (no RAID)
- Slot 1 today provides limited AMP storage
- Slot 2 will add 400GB of AMP storage in **FXOS 2.0.1**

1RU

Network Modules
- 10GE/40GE interchangeable with 9300
- Partially overlapping fail-to-wire controller options

Firepower 4100 Series Hardware Specification

Future

Description	FP 4110	FP 4120	FP 4140	FP 4150
Chassis & I/O	**1RU, 2xNetwork Module slots, 8 Fixed SFP+ ports, 2 SSD slots, Dual PSU Slots**			
PSU – Default CFG	Single AC	Single AC	Redundant AC	Redundant AC
Processor - Xeon	Single 12 Core	Dual 12 Core	Dual 18 Core	Dual 22 Core
DDR4 RAM	64GB	128GB	256GB	256GB
SSD – Default CFG.	**1 x 200GB**		**1 x 400GB**	
Security Acceleration Module	**Single Accelerator Card**	**Dual Accelerator Card**		

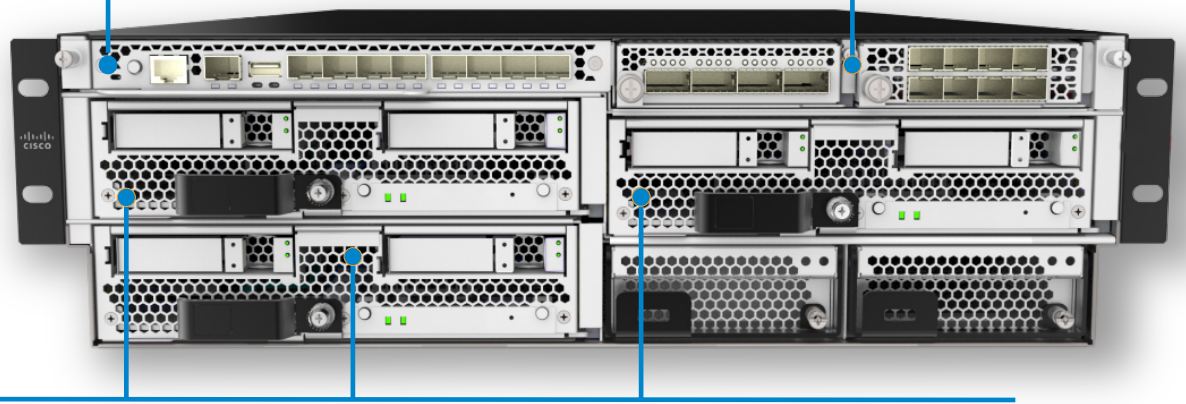
- 10 and 40G Port Modules are same for both FP 9300 and FP 4100 Series
- DC Power Supply for FP 4110/FP 4120 only. Estimated at FCS + 3 months.
- NEBS Certification completion for FP 4120 and FP 4140, 3 to 6 months after FCS

Firepower 9300 Overview

Supervisor
- Application deployment and orchestration
- Network attachment and traffic distribution
- Clustering base layer for ASA/FTD

Network Modules
- 10GE, 40GE, and 100GE
- Hardware bypass for inline NGIPS

3RU



Security Modules
- Embedded Smart NIC and crypto hardware
- Cisco (ASA, FTD) and third-party (Radware DDoS) applications
- Standalone or clustered within and across chassis

Firepower 9300 Security Modules

Future

Description	SM-24	SM-36	SM-44
Chassis & I/O	**3RU, 2xNetwork Module slots, 8 Fixed SFP+ ports, Dual PSU Slots**		
PSU – Default CFG	Redundant AC	Redundant AC	Redundant AC
Processor - Xeon	Dual 12 CPU	Dual 18 CPU	Dual 22 CPU
DDR4 RAM	128GB	256GB	256GB
SSD – Default CFG.	2*800GB SSD in RAID 1		
Security Acceleration Module	Dual Built-in hardware Smart NIC and Crypto Accelerator		

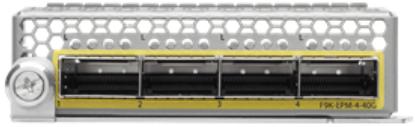
Standard Network Modules

- All external network modules require fiber or copper transceivers
- Support online insertion and removal

8x10GE

- Firepower 4100 and 9300
- Single width
- 1GE/10GE SFP

4x40GE



- Firepower 4100 and 9300
- Single width
- 4x10GE breakouts for each 40GE port

2x100GE

FXOS 1.1.4

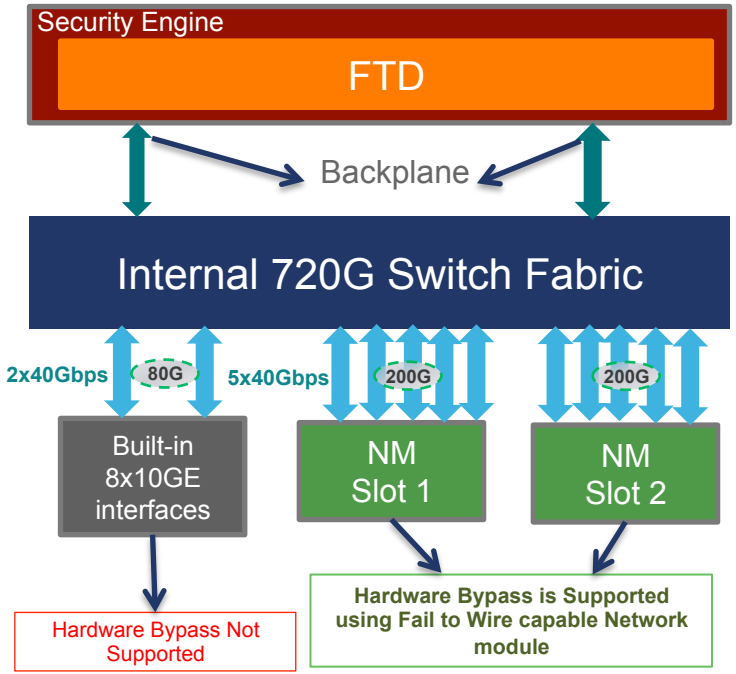
- Firepower 9300 only
- Double width
- QSFP28 connector
- No breakout support
- Single-width module requires Supervisor hardware change

Future

Future

Fail-To-Wire (Hardware Bypass)

- Support from FXOS 2.0.1 in both FP9300 and FP4100 Series
- Network Module should have the FTW capability
- Provides Hardware Bypass for network connectivity during software or certain hardware failure
- Used in the case where the network connectivity is important than the security during failure
- Only allowed on inline interface and inline interface tab mode in FTD App from version 6.1; not in ASA App



Future

Hardware-Bypass Capable Network Modules

Port Specification	1Gbps Fiber SX	10Gbps Fiber SR	10Gbps Fiber LR	40Gbps Fiber SR
Type	1000BASE-SX	10GBASE-MMSR	10GBASE-SMLR	40GBASE-SR4
PID	FPR9K-NM-6X1SX-F	FPR9K-NM-6X10SR-F	FPR9K-NM-6X10LR-F	FPR9K-NM-4X40G-F
Mode	Multi-mode	Multi-mode (SR)	Single-mode (LR)	Multi-mode
Interfaces	6	6	6	2
Interface Speed	1Gbps	10Gbps	10Gbps	40Gbps
Integrated /Programmable FTW	Yes	Yes	Yes	Yes
Breakout cable supported in FTW Ports	N	N	N	N
Transceivers SFP	Inbuilt	Inbuilt	Inbuilt	Inbuilt

Note: No SFP OIR and No Port-Channel Support

Flow Offload

- Trusted flow processing with limited security visibility in Smart NIC
  - Up to 39Gbps of single-flow UDP throughput with 1500-byte packets
  - 2.9us latency with 64-byte UDP packets
- Supports up to 128K offloaded stateful connections
  - Untagged IPv4 TCP/UDP (32K) and GRE (32K), 32K each with VLAN tags
- Static offload on ASA with IP/SGACL in MPF
  - Offload multicast in transparent mode with 2 bridge group ports in 9.6(2)
- Pre-filter offload policy for IP/TCP/UDP Trust rules in FTD 6.1
  - Dynamic offload for fast-forwarded connections in the future

Miscellaneous New Features

FXOS 2.0.1

- Lina (“ASA”) Dataplane bypass for FTD NGIPS interfaces
- Interface link state propagation for inline FTD NGIPS interfaces
- Support for 2048 VLAN subinterfaces
- Graceful chassis shutdown
- Scheduled Supervisor configuration export
- Miscellaneous changes for FIPS, CC, and USGv6 compliance
- Customizable chassis manager login banner

Firepower Management Center - FMC

Firepower Management Center - FMC

Models

FS750

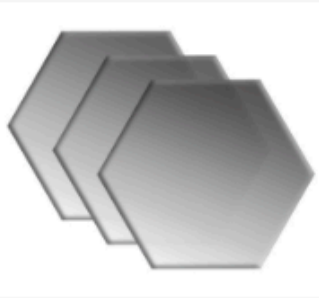
Up to 10 sensors managed
20 million maximum events
100 GB event storage
Network map up to 2K hosts, 2K users

FS2000

Up to 70 sensors managed
60 million maximum events
1.8 TB event storage
Network map up to 150K hosts, 150K users

FS4000

Up to 300 sensors managed
300 million maximum events
3.2 TB event storage
Network map up to 600K hosts, 600K users

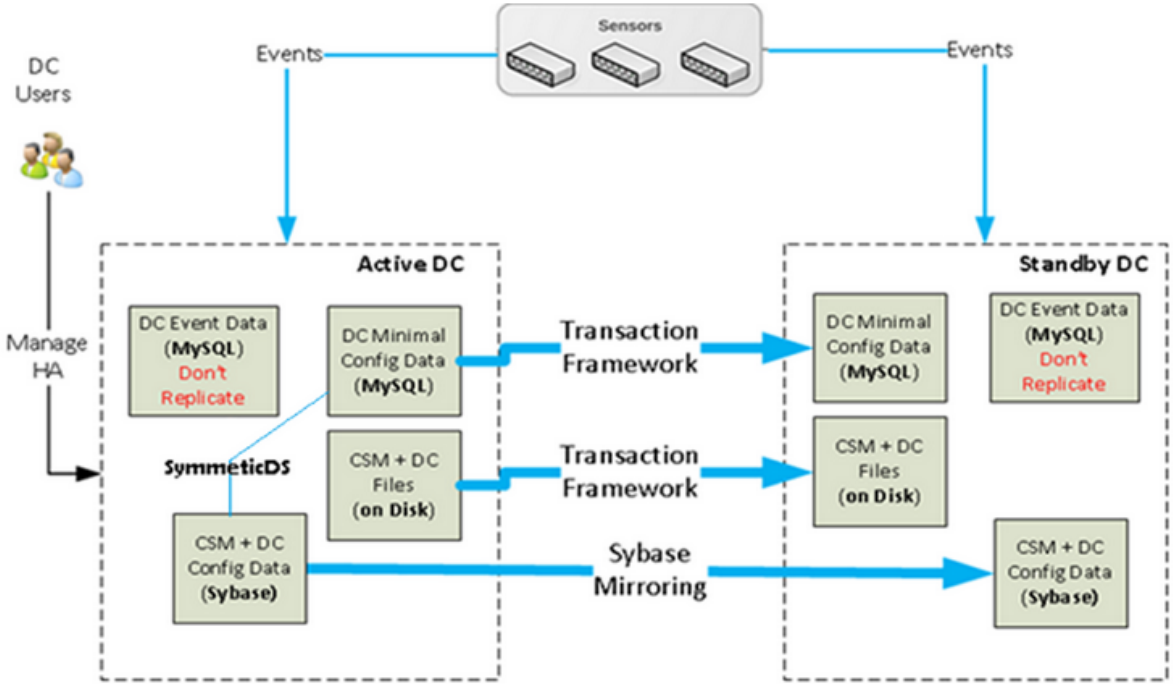


Virtual

Up to 25 sensors managed
10 million maximum events
250 GB event storage
Network map up to 50K hosts, 50K users

FMC HA

- Very different from 5.4 FMC HA
- Active/Standby Deployment
- Failover manual
- Sybase database duplicated
  - Both FMC nodes receive events from each sensor
  - Policy changes made on primary are copied over to the secondary



FMC HA 5.4 vs 6.1.0

- FMC HA is Active/Standby. In 5.4.x, it was Active/Active
- Active FMC: fully functional. As good as standalone
- Standby FMC: read-only. Most of the tabs/sub-tabs on UI are hidden.
- Standby FMC: No CSM processes. Except VmsDbEngine.
- Standby FMC: Configuration database (Sybase) is read-only.
- No sync for events. Events are pushed to both the FMCs (no change from 5.4.x)
- FMC HA is supported on 4K, 2K, 3500 and 1500. Not supported on Virtual
- All configuration related tables of MySQL are moved to Sybase
- FMC HA 5.4 FMC HA managed FP only; FMC HA 6.1 managed HA for both FP and FTD

FMC – logging

- You can’t log all connections in a large - or even medium - environment and expect to get weeks of history on the FMC.
- Tune your AC policy to log the connections you really need and reduce the “noisy” connection events (DNS, Dropbox, etc.)
- You will always get connection events for any IPS alerts regardless of your connection event logging settings in the AC policy. However if you try and log too many these valuable events will be purged along with the noise.
- The “important” events are typically much less noisy and we can keep months or years of history (IPS, Malware, IOCs, etc.)
- If you have to keep these connection events longer, then send them off to a SIEM. Syslog seems to be more efficient at this than eStreamer.
- Be careful increasing the log storage too high. Even though the FS4000 supports 1 billion connection events that will impact your query performance (analysis).

High availability and scalability for 4100 and 9300

High Availability and Scalability Options

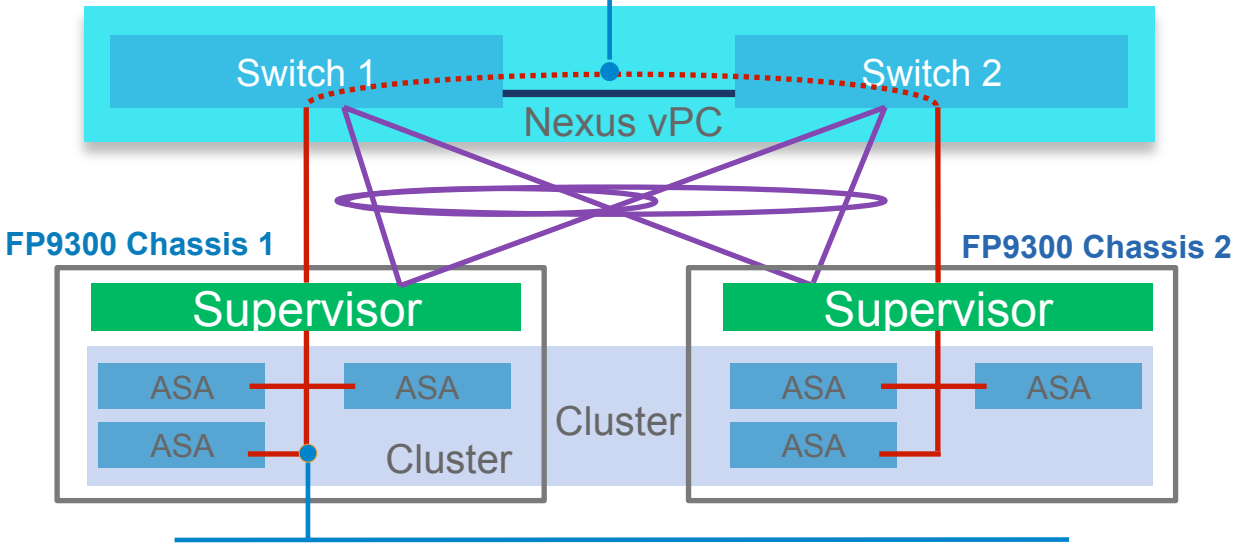
	High Availability	High Scalability	High Availability and Scalability
ASA	Active/Standby Failover (2 modules) Active/Active Failover (2 modules)	Intra-Chassis Clustering* (≤3 modules) Inter-Chassis Clustering ((≤16 modules)	Inter-chassis clustering (≤16 modules, 1.2Tbps)
FTD	Active/Standby Failover (2 modules)	Intra-chassis Clustering* (≤3 modules)	-
Radware vDP	-	Intra-chassis Clustering (≤3 modules)	-

* Not applicable for FP4100 platforms.

Application Clustering with FP9300

Inter-Chassis Cluster Control Link

- Cluster of up to 16 modules across 5+ chassis
- Off-chassis flow backup for complete redundancy



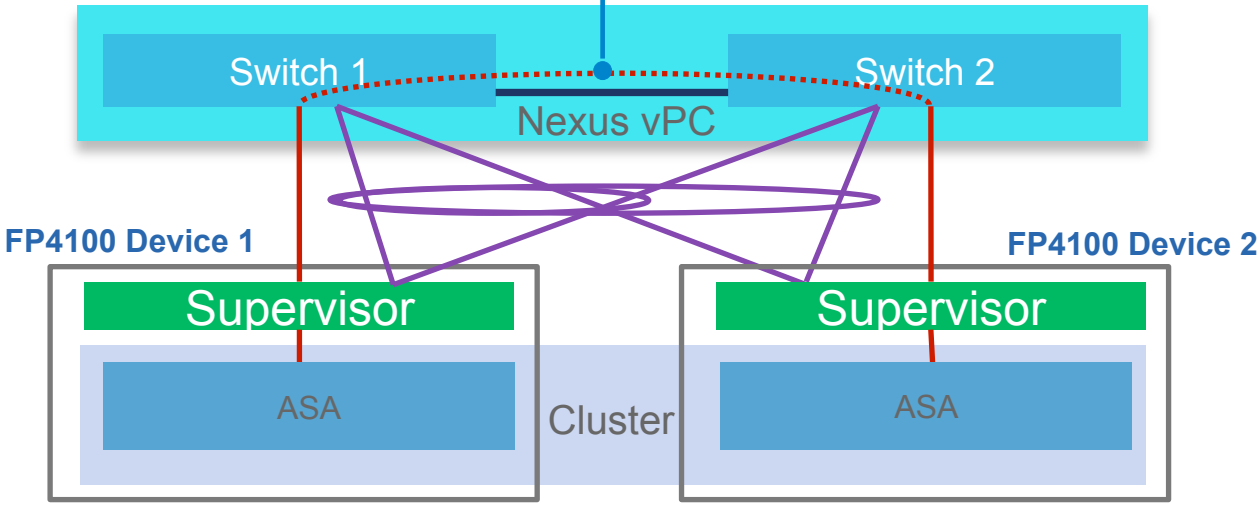
Intra-Chassis Cluster Control Link

- Same-application modules can be clustered within chassis
- Bootstrap configuration is applied by Supervisor

Application Clustering with FP4100

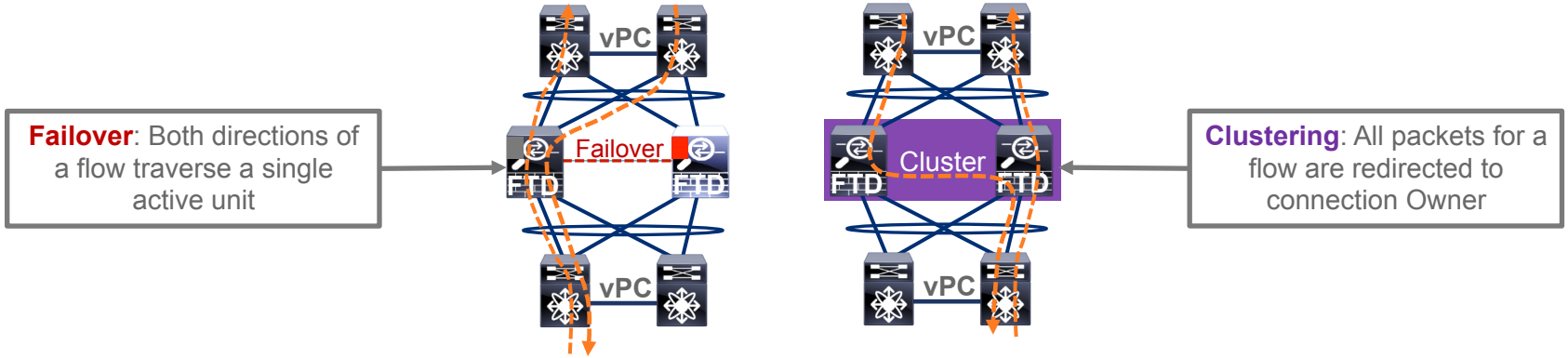
Inter-Chassis Cluster Control Link

- Cluster of up to 16 Device
- Off-chassis flow backup for complete redundancy



FTD Failover and Clustering

- FTD uses ASA data plane and similar failover/clustering infrastructure
  - Enhanced to replicate full NGFW/NGIPS configuration and opaque flow state
  - Current intra-chassis clustering support on Firepower 9300 platform **only**
  - Module-level Active/Standby failover for inter-chassis high availability
- Ensures full stateful flow symmetry in both NGIPS and NGFW modes



Performance

Performance (Same for ASA w/Firepower Services and FTD)

Model	5506-X	5508-X	5512-X	5515-X	5516-X	5525-X	5545-X	5555-X
Max AVC Throughput	250 Mbps	450 Mbps	300 Mbps	500 Mbps	850 Mbps	1100 Mbps	1500 Mbps	1750 Mbps
Max AVC and IPS Throughput	125 Mbps	250 Mbps	150 Mbps	250 Mbps	450 Mbps	650 Mbps	1000 Mbps	1250 Mbps
AVC or IPS Sizing Throughput	**90 Mbps**	**180 Mbps**	**100 Mbps**	**150 Mbps**	**300 Mbps**	**375 Mbps**	**575 Mbps**	**725 Mbps**
Max Connections	50,000	100,000	100,000	250,000	250,000	500,000	750,000	1,000,000
Max CPS	5,000	10,000	10,000	15,000	20,000	20,000	30,000	50,000

Firepower Appliances – 7100/8100/8300

FP Appliance	TAM/TAMC Performance	AMP Appliance	TAM/TAMC Performance
FP7120	400 Mb/s	AMP7150	500 Mb/s
FP7125	500 Mb/s	AMP7150	500 Mb/s
FP8120	700 Mb/s	AMP8050	1 Gb/s
FP8130	1 Gb/s	AMP8150	2 Gb/s
FP8140	2 Gb/s	AMP8150	2 Gb/s
FP8350	5 Gb/s	AMP8350	5 Gb/s
FP8360	10 Gb/s	AMP8360	10 Gb/s
FP8370	15 Gb/s	AMP8370	15 Gb/s
FP8390	20 Gb/s	AMP8390	20 Gb/s

AMP7150/8150 include additional CPU, RAM, and Storage

AMP8050 leverages 8130 platform AND includes additional 400Gb Malware Storage SSD

AMP83xx leverages 83xx platform AND includes additional 400Gb Malware Storage SSD in each 8350 chassis

FTD Performance

	4110	4120	4140	SM-24	SM-36	SM-36x3
Max Throughput: Application Control (AVC)	12G	20G	25G	25G	35G	100G
Max Throughput: Application Control (AVC) and IPS	10G	15G	20G	20G	30G	90G
Sizing Throughput: AVC (450B)	4G	8G	10G	9G	12.5G	30G
Sizing Throughput: AVC+IPS (450B)	3G	5G	6G	6G	8G	20G
Maximum concurrent sessions w/AVC	4.5M	11M	14M	28M	29M	57M

ASA Performance

	4110	4120	4140	SM-24	SM-36	SM-36x3
Stateful inspection firewall throughput (maximum)	20G	40G	60G	75G	80G	225G
Stateful inspection firewall throughput (multiprotocol)	10G	20G	30G	50G	60G	100G
Concurrent firewall connections	10M	15M	25M	55M	60M	70M
New connections per second	150K	250K	350K	0.6M	0.9M	2M
Security contexts	250	250	250	250	250	250
Virtual Interfaces	1024	1024	1024	1024	1024	1024
IPSec 3DES/AES VPN Throughput	8G	10G	14G	15G	18G	18G

Use cases

Use cases – what to use where ?

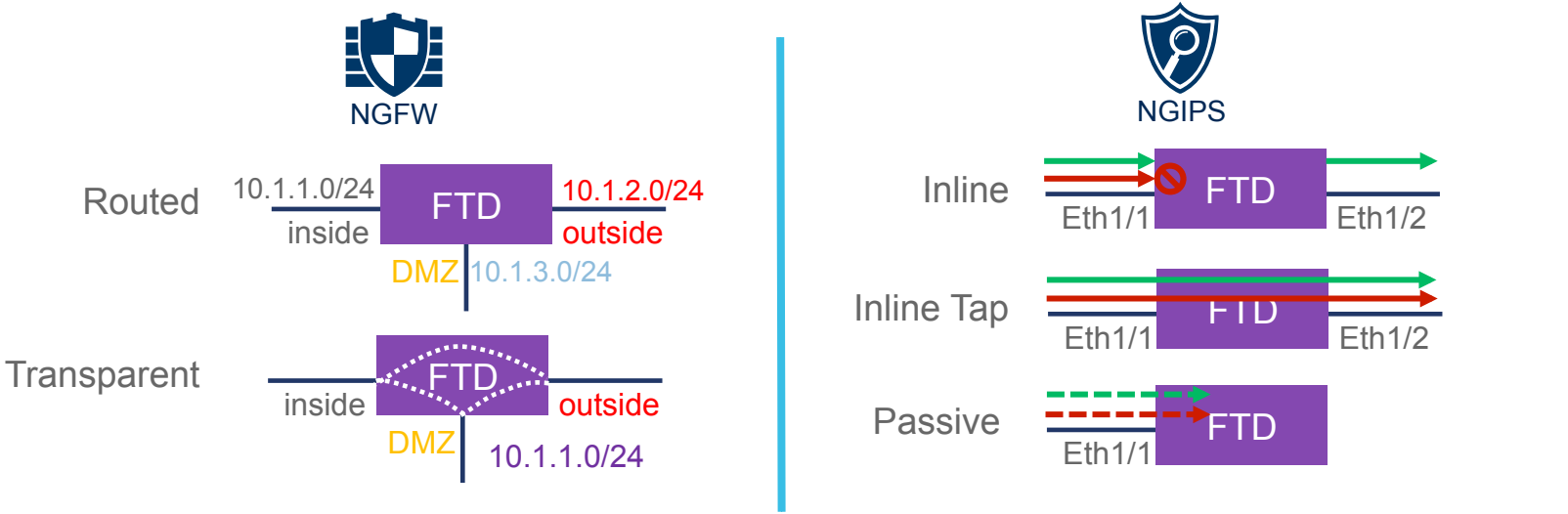
- **ASA** is a powerful and scalable solution for basic stateful segmentation
  - Ease of integration and scaling in large and distributed data centers
  - Real-time trading and high performance application protection with Flow Offload
  - Infrastructure and Internet edge protection for service providers

- **FTD** is a comprehensive threat-centric security solution
  - NGIPS for data center and service provider environments
  - NGFW for edge protection and smaller data centers

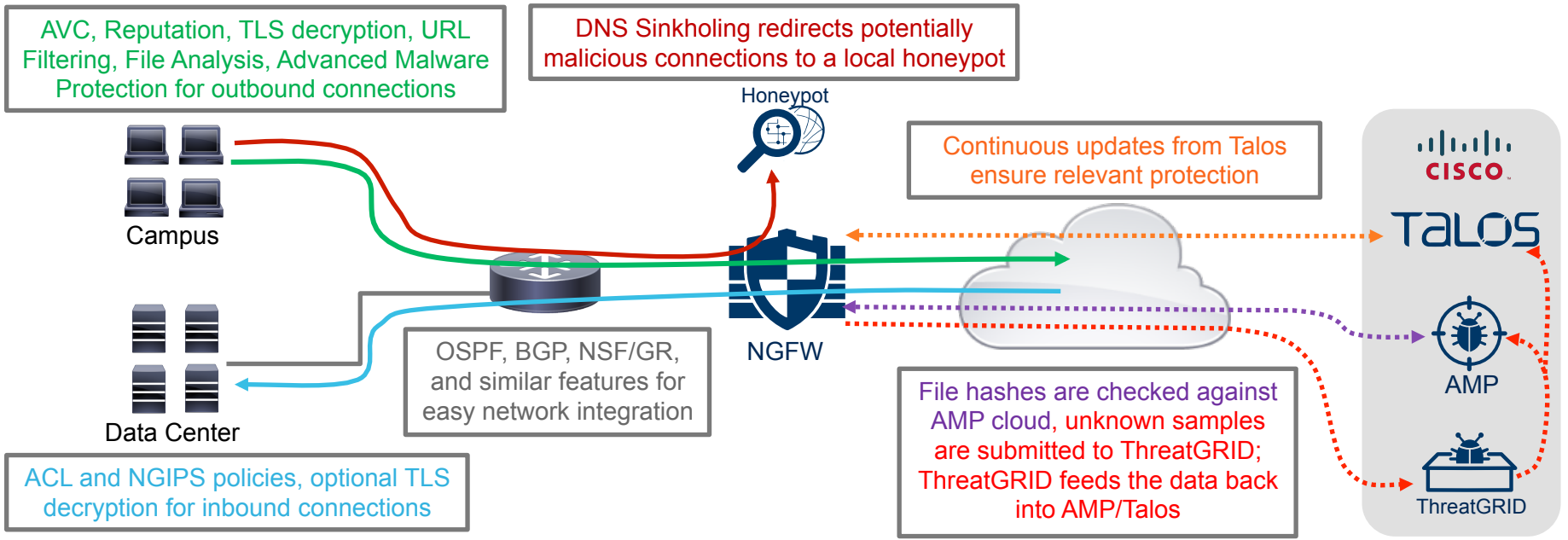
- **Radware vDP** is a behavioral DDoS mitigation solution
  - Internet edge protection for web commerce and service provider environments

FTD Deployment Modes

- FTD is both NGFW and NGIPS on different network interfaces
  - NGFW inherits operational modes from ASA and adds FirePOWER features
  - NGIPS operates as standalone FirePOWER with limited ASA data plane functionality



FTD as NGFW at the Edge



Key Takeaways

Key takeaways

- FTD is the new unified software – one management platform
- ASA 5500-x can be an NGIPS device with FTD
- Consider 41xx and 9300 for high performance environments
- Scale based on feature functionality needed.
- Reach out to Cisco DK or Partner Helpline (partners)

Q & A

Seminarkalender 2016

DANMARK
UDDANNELSE & SEMINARER
- **Packetville**
- **Uddannelse**
- **Seminarkalender 2016**

Juni | **Alle**

Juni

Dato	Seminar/event	Målgruppe	Sted
1.	Cisco Virtual Update – Firepower Scaleable Designs	Slutkunder/Partnere	Online
14.	Cisco Virtual Update – Cisco Spark	Slutkunder/Partnere	Online
15.	Cisco Virtual Update – Nexus Access Switching	Slutkunder/Partnere	Online
21. & 23.	Cisco Tech Update - ACI & Switching	Slutkunder/Partnere	Århus & København

Del

Genveje

RSS Feeds
Job hos Cisco
Seminarkalender
Nyhedsbreve
Pressemeddelelser og nyheder
Kundereferencer
Seminar materialer