Обеспечение информационной безопасности на базе Cisco Next-Generation Firewall

Максим Порицкий

инженер по направлению Cisco, CCIE R&S

m.poritsky@elcoregroup.com

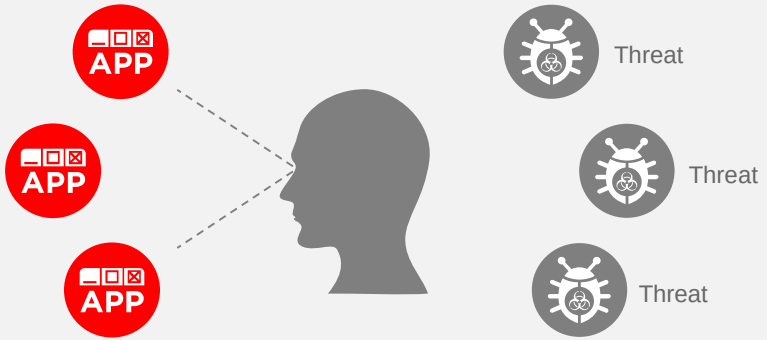
14.04.2018

What is a NGFW?

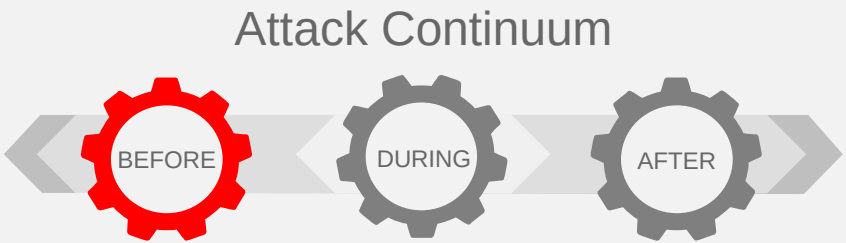
- Typical Firewall Features
- Application Visibility & Control
- Integrated Network IPS
- Extra Firewall Intelligence

Other “next-generation” firewalls fix some problems but create new ones

They’re only app-focused…



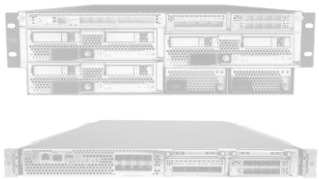
They can’t help you once you’ve been breached…



They’re another silo to manage…

cisco Elcore | elko.by

Cisco Firepower NGFW is a complete solution



Cisco Firepower™ NGFW

Stop more threats	Gain more insight	Detect earlier, act faster	Reduce complexity	Интеграция

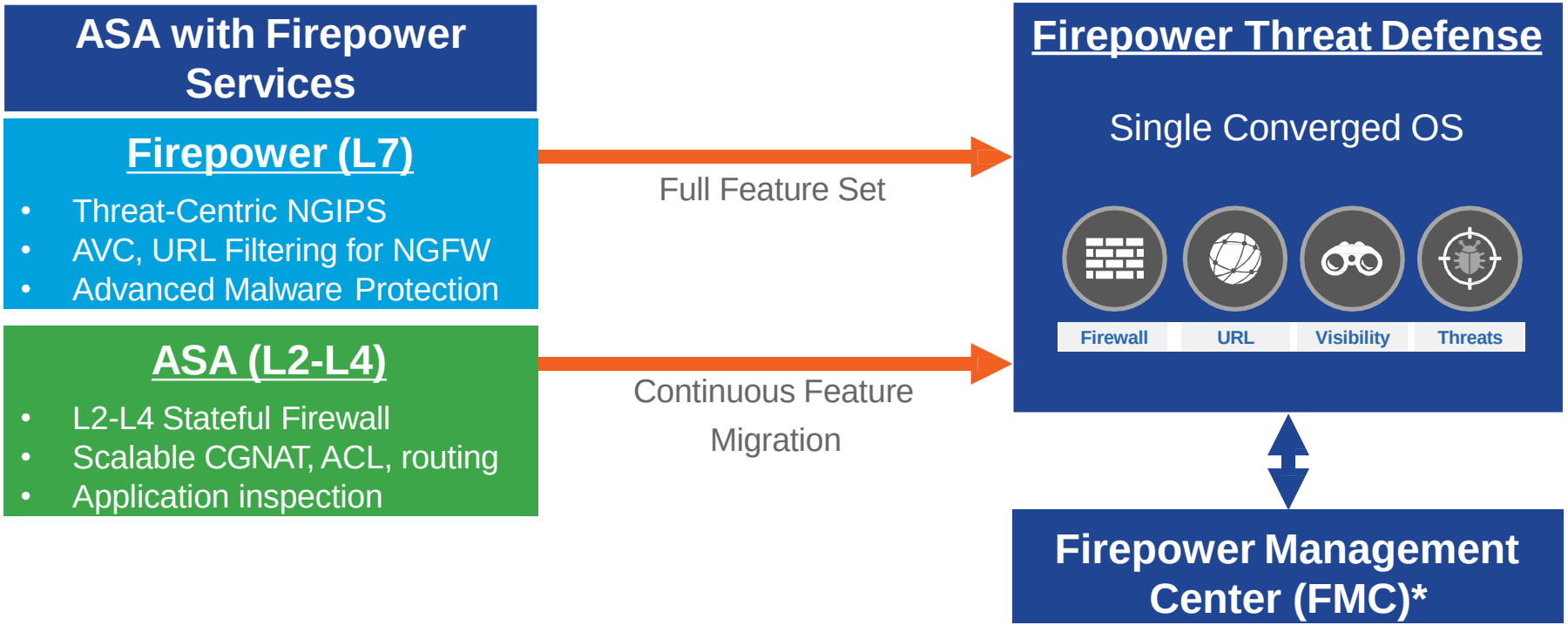
Threat Focused | Fully Integrated

NGFW = Cisco + Sourcefire

ASA and FirePOWER – Better Together

- Cisco ASA
  - Best-of-breed stateful inspection firewall
  - Applies NAT to embedded application protocol data
  - Integrates with many other solutions, including: Unified Communications technologies, Active Directory, etc.
  - Acts as a VPN termination: Site-to-site, remote access, and clientless VPN
- FirePOWER
  - URL filtering
  - Application visibility and control (AVC)
  - Threat protection (NGIPS) and Advanced Malware Protection (AMP)

Firepower Threat Defense (FTD) Software



cisco elcore | elko.by

* Also manages Firepower Appliances and FirePOWER Services (not ASA Software)

Feature Comparison: ASA with Firepower Services and Firepower Threat Defense

	Features	Firepower Threat Defense	Firepower Services for ASA
SIMILARITIES	Routing +NAT	✓ (OSPF, BGP, Static, RIP, Multicast, EIGRP/PBR via FlexConfig)	✓ (OSPF, BGP, EIGRP, static, RIP, Multicast)
	OnBox Management	✓	✓
	HA (Active/Passive)	✓	✓
	Clustering (Active/Active)	✓	✓
	Site to Site VPN	✓	✓
	Policy based on SGT tags	✓	✓
DIFFERENCES	Unified ASA and Firepower rules and objects	✓	✗
	Hypervisor Support	✓ (AWS, VMware, KVM, Azure 6.2)	✗
	Smart Licensing Support	✓	✗
	Multi-Context Support	✗ (Coming Soon!)	✓
	Remote Access VPN	✓ (6.2.1)	✓

NGFW Portfolio

Cisco NGFW Product Portfolio

ASA 5506-X

SMB/SOHO

ASA 5508-X
ASA 5516-X

Branch

FPR2110
FPR2120
FPR2130
FPR2140

ASA 5555-X
ASA 5545-X
ASA 5525-X

HQ/Internet Edge

FPR4110
FPR4120
FPR4140
FPR4150

Data Center

FPR9K-SM-24
FPR9K-SM-36
FPR9K-SM-44

Service Provider

Cisco NGFW Product Portfolio

ASA 5500-X with FirePOWER Services

- Small businesses, branch offices, distributed enterprises
- Firewall throughput and threat inspection from 256 to 1750 megabytes
- Stateful firewall, AVC, NGIPS, AMP, URL filtering

Cisco Firepower 2100 Series

- Internet edge to small data center environments. Better security, more visibility
- Firewall throughput and sustained performance with threat inspection from 2.0 to 8.5 gigabytes
- Stateful firewall, AVC, NGIPS, AMP, URL filtering

Cisco Firepower 4100 Series

- Internet edge, high-performance enterprise environments
- Firewall throughput and threat inspection from 20 to 60 gigabytes
- Stateful firewall, AVC, NGIPS, AMP, URL filtering, DDoS (Radware vDP)

Cisco Firepower 9300 Security Appliance

- Service provider, data center
- Firewall throughput up to 225 gigabytes and threat inspection up to 90 gigabytes
- Firewall, AVC, NGIPS, AMP, URL filtering, DDoS (Radware vDP)

NGFW – некоторые функции

Важность контекста
Понимание своей инфраструктуры


Vulnerabilities


Services


Applications


Users


Hosts


Communications

Сенсоры - **ASA**
Пассивное обнаружение

FireSIGHT -
система осведомления,
в режиме реального времени,
информации об инфраструктуре

- The FireSIGHT использует функционал **network discovery** для мониторинга сетевого трафика и построения карты сети
- Управляемые устройства пассивно собирают информацию, распознавая типы узлов, ОС, ПО, открытые порты и т.д. и информируют об этом **Firepower Management Center**
- **User Agents** на Microsoft Active Directory пересылают информацию об LDAP аутентификации пользователей
- Информация по сбору может быть расширена за счет NetFlow, сканирования и др. методов

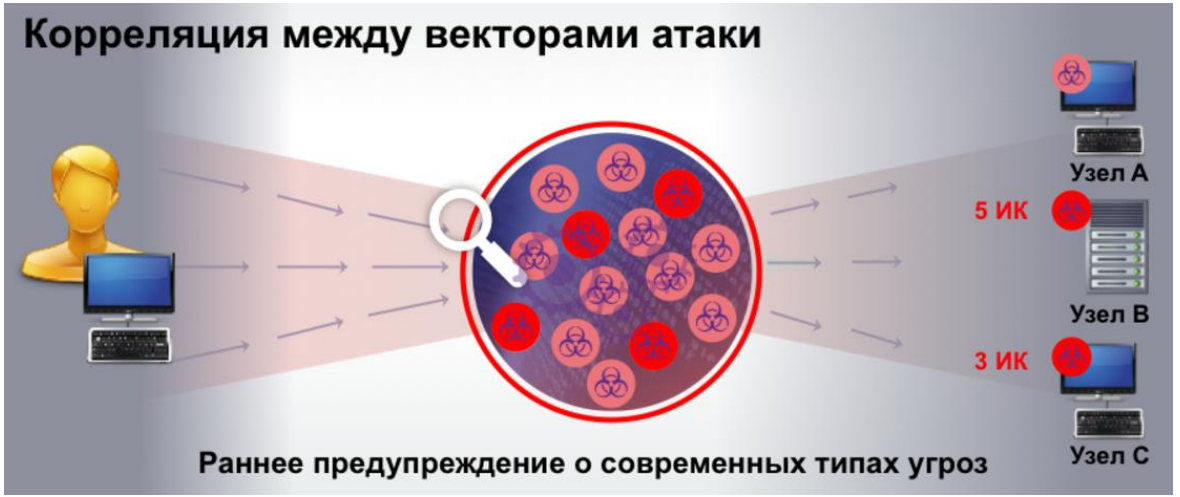
Отличительные особенности – приоритезация угроз

- Приоритезация угроз, опираясь на контекстную информацию об атакуемых узлах
- Использовать контекст совершения атаки для отделения важных событий от неважных, для приоритезации усилий специалистов по безопасности по отражению угроз

Отличительные особенности - корреляция событий
защита от мультивекторных атак

- Мультивекторные угрозы - используют для вторжения сразу несколько способов проникновения

- Каждый такой способ может характеризоваться событиями, которые по отдельности не представляют интереса и имеют низший приоритет. Однако в совокупности эти события могут означать серьезную целенаправленную угрозу



Отличительные особенности – адаптируемость динамические механизмы безопасности

- Автоматизации настроек сигнатур и правил в политике безопасности (это делается на базе анализа сетевого и прикладного трафика и распознавания используемых в сети узлов, устройств, протоколов, приложений, операционных систем и др.)

- Политики могут динамически адаптироваться в зависимости от изменения ситуации в сети — появления новых сервисов, узлов, пользователей и, конечно, же угроз

NGFW Capabilities

Get real-time protection against global threats

Talos

TALOS

Threat Intelligence

1.5 million daily malware samples

600 billion daily email messages

16 billion daily web requests

Security Coverage

Endpoints

WWW Web

Networks

NGIPS

Devices

Research Response

250+
Researchers

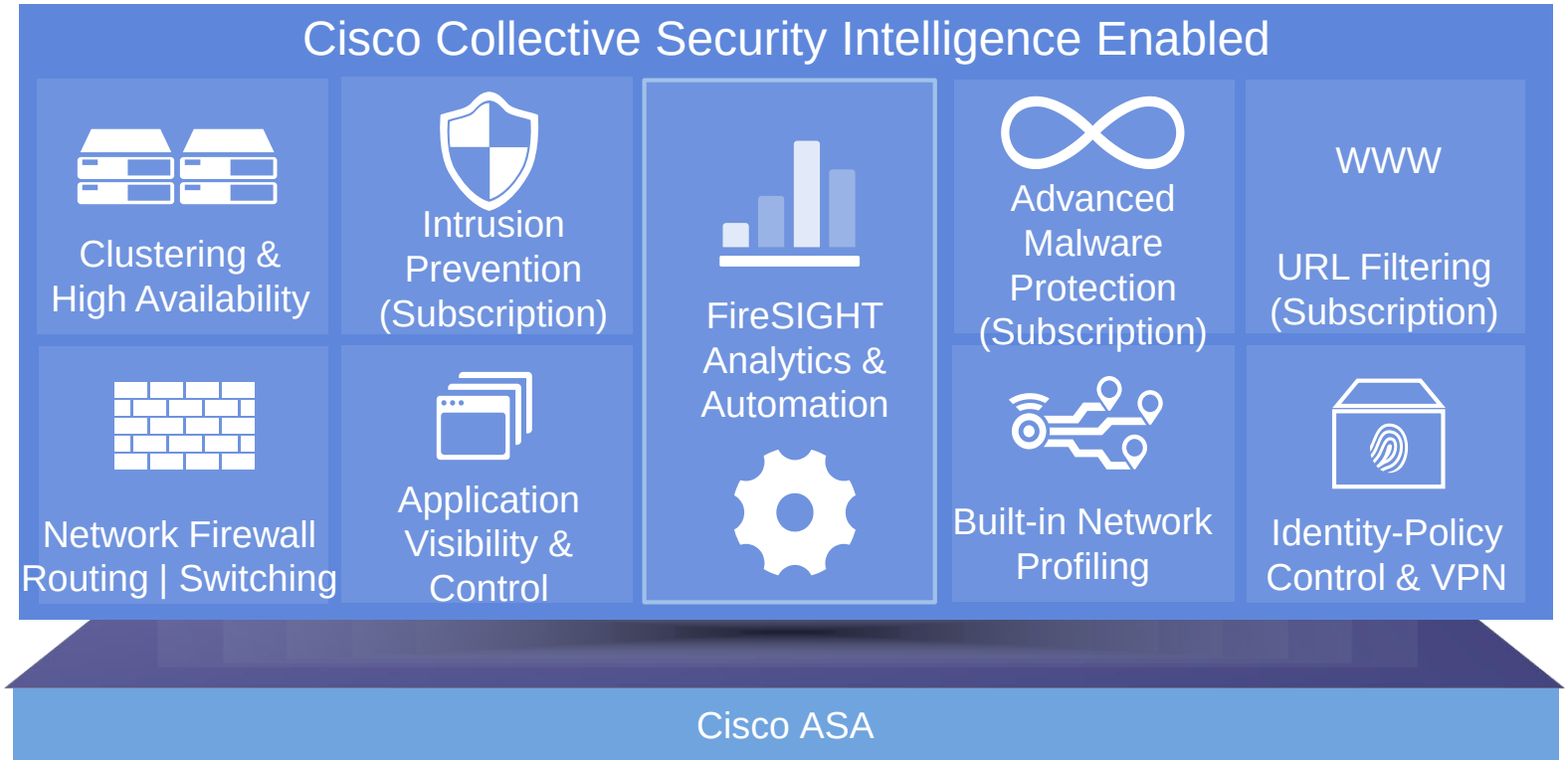
Jan

24 x 7 x 365
Operations

Identify advanced threats	Get specific intelligence	Catch stealthy threats	Stay protected with updates

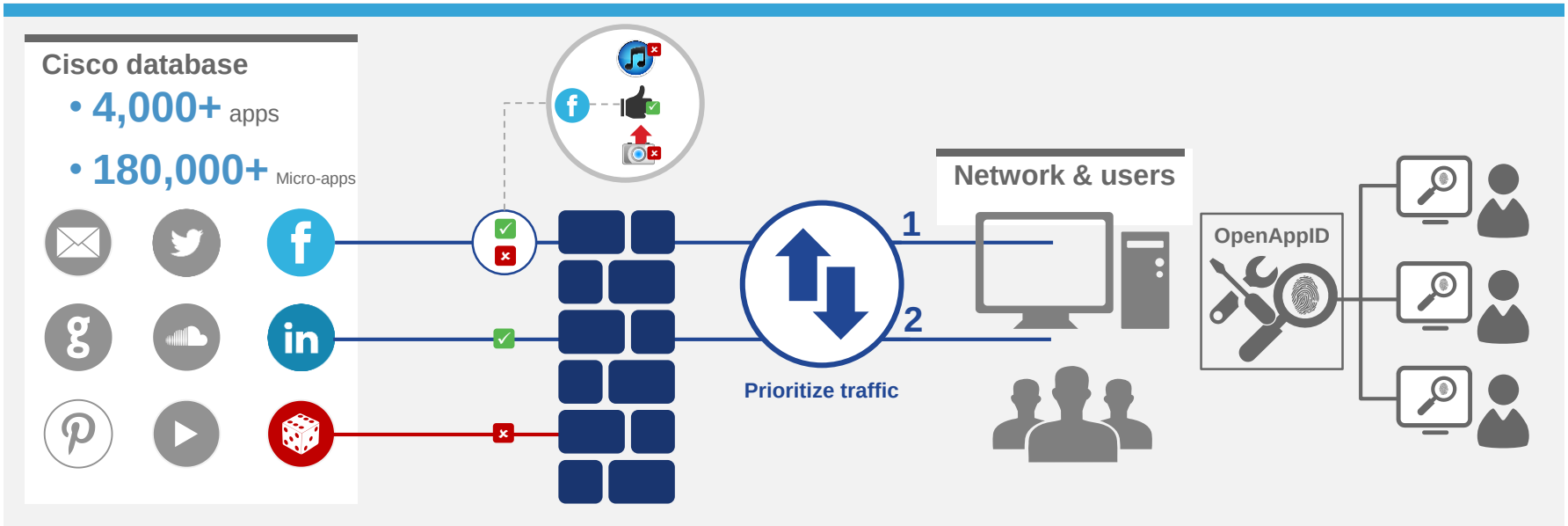
cisco elcore | elko.by

Features


Cisco Collective Security Intelligence Enabled
Clustering & High Availability
Intrusion Prevention (Subscription)
FireSIGHT Analytics & Automation
Advanced Malware Protection (Subscription)
WWW
URL Filtering (Subscription)
Network Firewall Routing | Switching
Application Visibility & Control
Built-in Network Profiling
Identity-Policy Control & VPN
Cisco ASA

Provide next-generation visibility into app usage

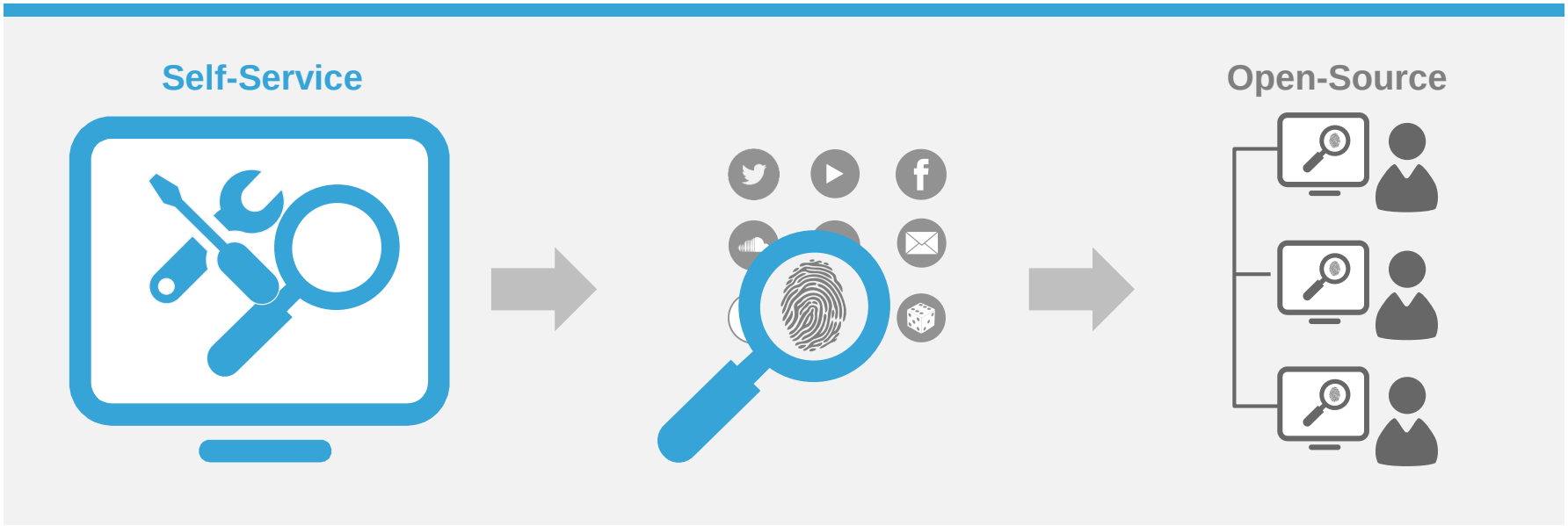
Application Visibility & Control



See and understand risks	Enforce granular access control	Prioritize traffic and limit rates	Create detectors for custom apps

Extend AVC to proprietary and custom apps

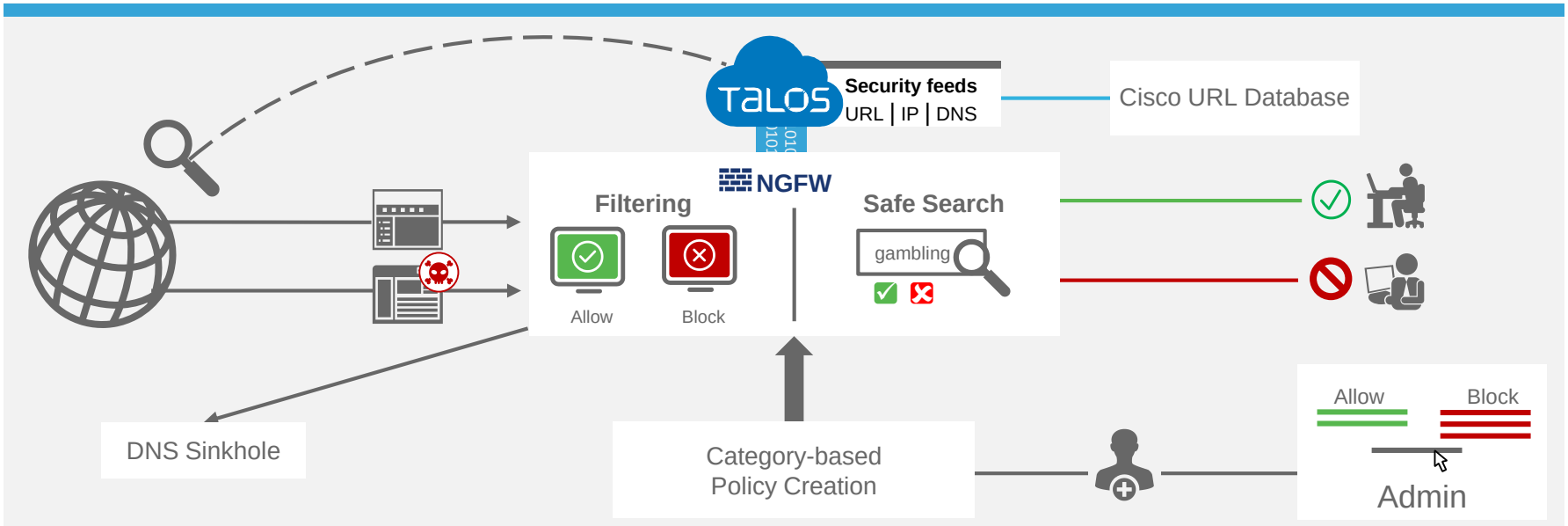
OpenAppID



Easily customize application detectors	Detect custom and proprietary apps	Share detectors with other users

Block or allow access to URLs and domains

Web controls



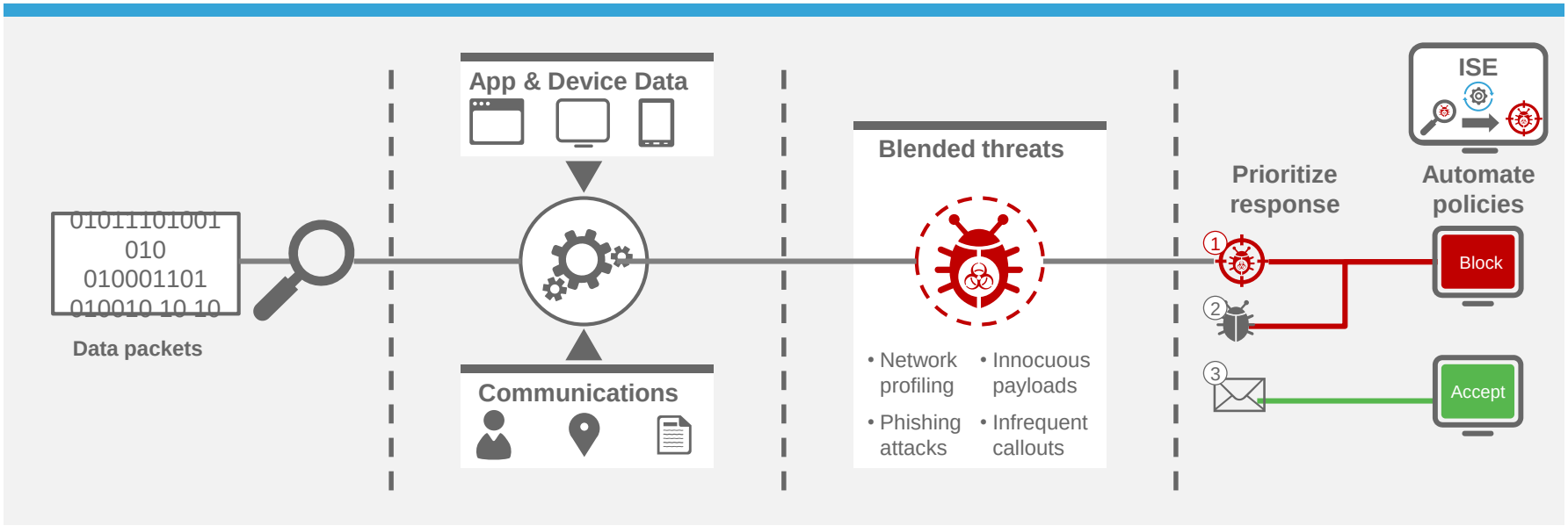
Classify 280M+ URLs

Filter sites using 80+ categories

Manage “allow/block” lists easily

Block latest malicious URLs

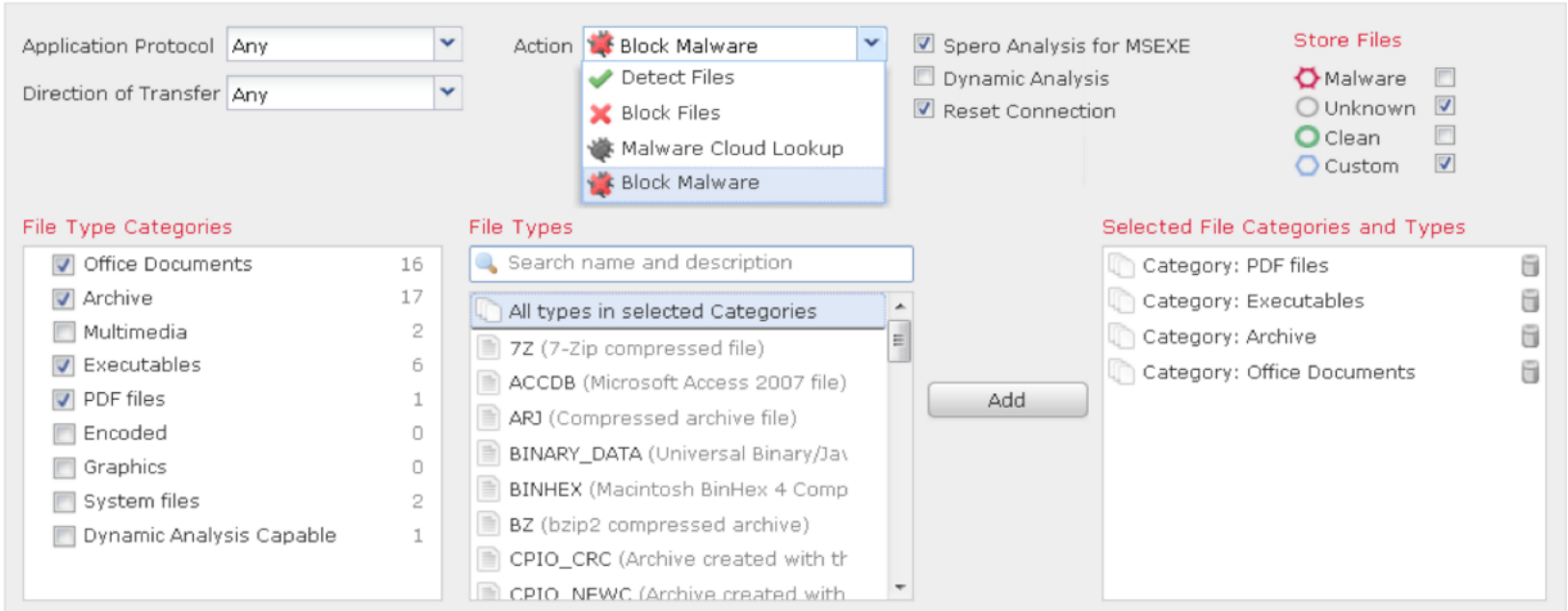
Understand threat details and quickly respond
Next-Generation Intrusion Prevention System (NGIPS)



Scan network traffic	Correlate data	Detect stealthy threats	Respond based on priority

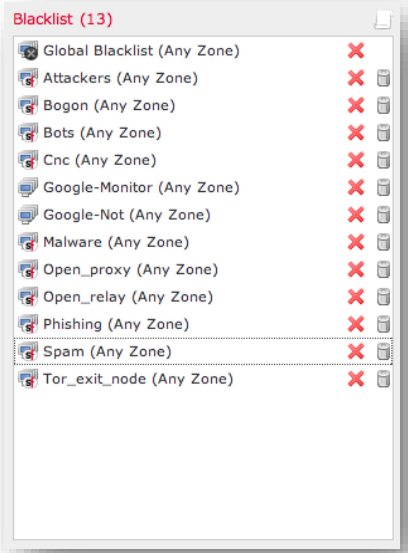
File Control (контроль по типам файлов)

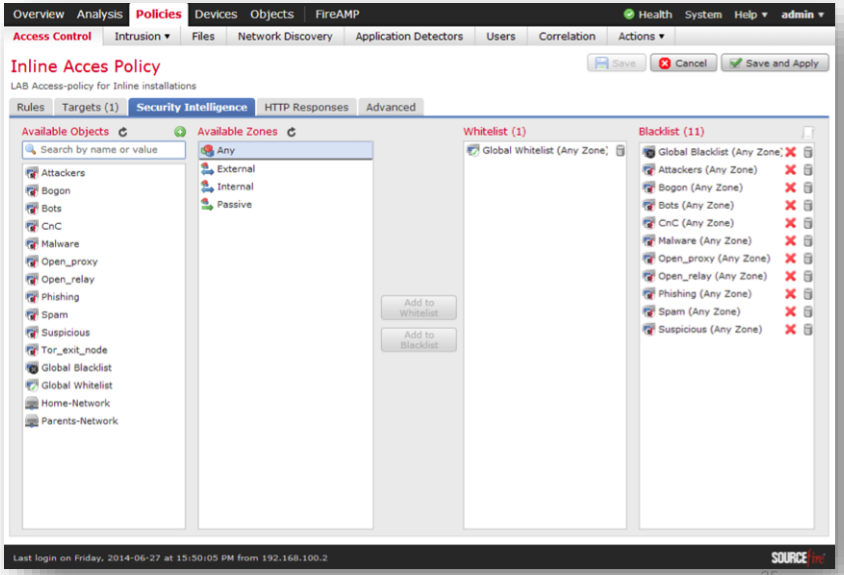
идентификация и блокирование файлов по их типам



Security Intelligence динамические “черные списки”

- можно назначить политику фильтрации Security Intelligence - постоянно обновляемые списки IP адресов спаммеров, центров ботнетов, открытых proxy и т.д.
- выбирать из имеющихся списков, либо загрузить свои собственные списки фильтрации из файла, либо указать системе URL, откуда эти списки забирать
- позволяет не обрабатывать доверенный трафик и блокировать изначально вредоносный

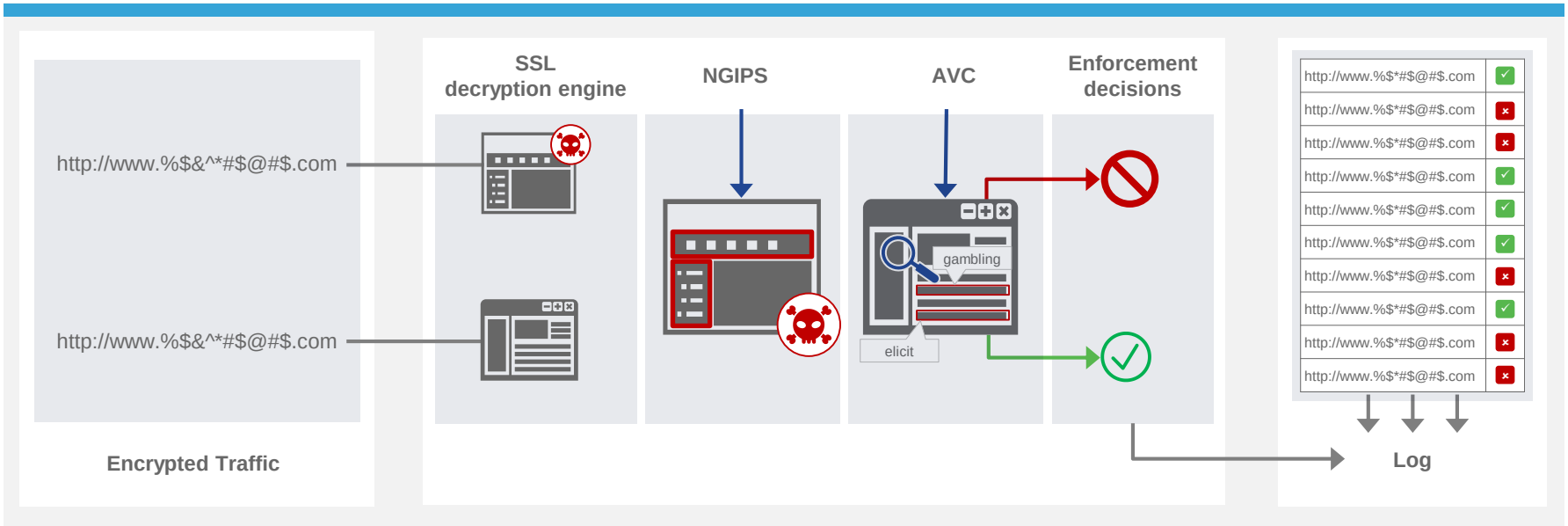




cisco elcore | elko.by

Uncover hidden threats at the edge

SSL decryption engine



Decrypt **3.5 Gbps** traffic over **five million** simultaneous flows

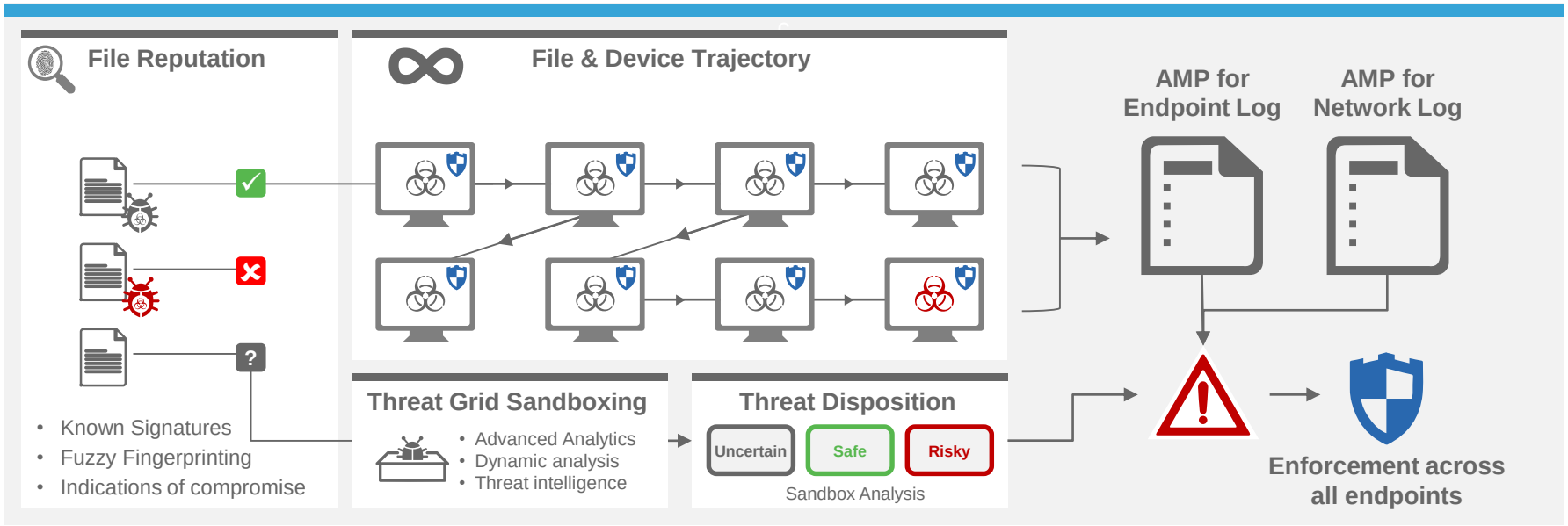
Inspect deciphered packets

Track and log all SSL sessions

cisco elcore | elko.by

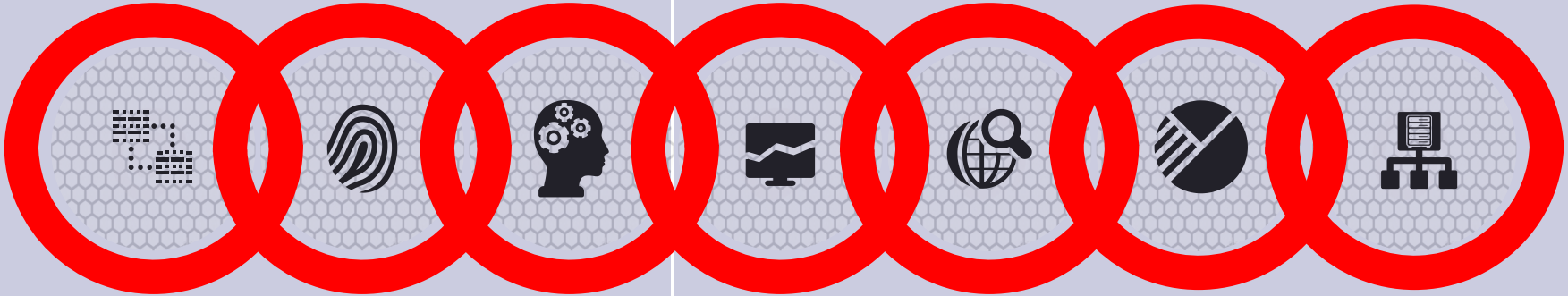
Uncover hidden threats in the environment

Advanced Malware Protection (AMP)



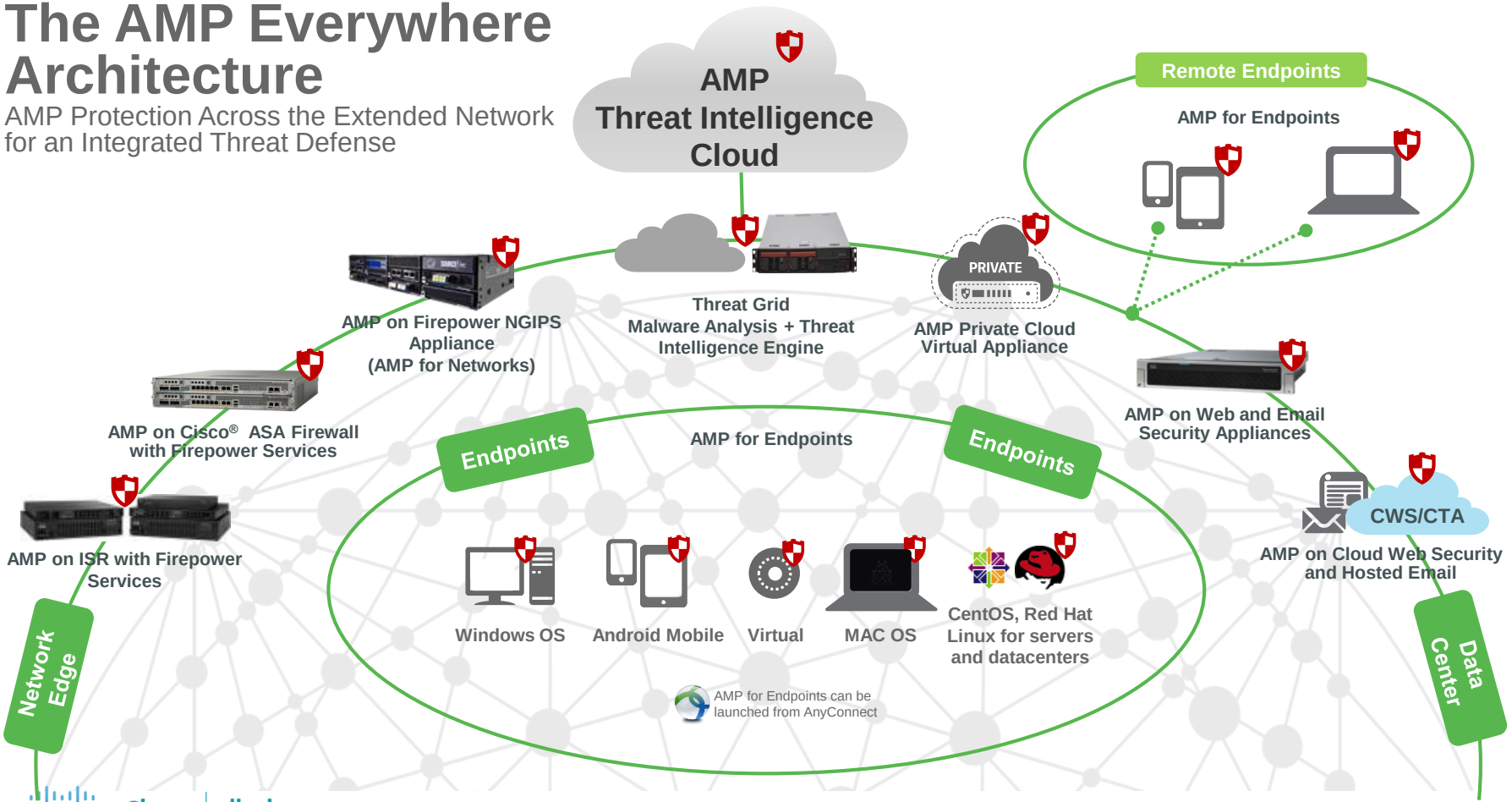
Block known malware | Investigate files safely | Detect new threats | Respond to alerts

Обнаружение вредоносного кода с помощью AMP

Фильтрация по репутации			Поведенческое обнаружение			
						
Точная сигнатура	Нечеткие отпечатки (похожие элементы файла)	Машинное обучение (атрибуты файла – 400 шт)	Признаки вторжения (поведение в сети)	Динамический анализ (песочница)	Расширенная аналитика (от разных устройств безопасности)	Корреляция потоков

The AMP Everywhere Architecture

AMP Protection Across the Extended Network for an Integrated Threat Defense



Network File Trajectory for 0517f034...588e1374

File SHA-256	0517f034...588e1374
File Name	WindowsMediaInstaller.exe
File Type	MSEXE
File Category	Executables
Current Disposition	Malware
Threat Score	High

First Seen	2013-12-06 10:57:13 on 10.4.10.183
Last Seen	2013-12-06 18:17:27 on 10.4.10.183
Event Count	7
Seen On	4 hosts
Seen On Breakdown	2 senders → 3 receivers

Trajectory

Events Transfer | Block | Create | Move | Execute | Scan | Retrospective | Quarantine

Dispositions Unknown | Malware | Clean | Custom | Unavailable

Events

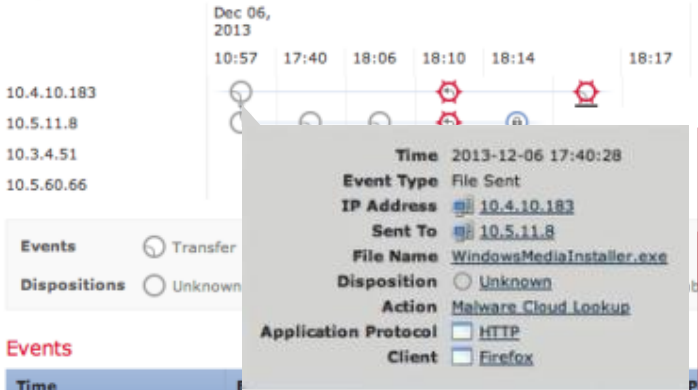
Time	Event Type	Sending IP	Receiving IP	File Name	Disp...	Action	Protocol	Client	Web Ap...	Description
2013-12-06 10:57:13	Retrospectiv...				Malwa...					
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...					
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...					
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox		

Network File Trajectory for 0517f034...588e1374

File SHA-256	0517f034...588e1374
File Name	WindowsMediaInstaller.exe
File Type	MSEXE
File Category	Executables
Current Disposition	Malware
Threat Score	High

First Seen	2013-12-06 10:57:13 on 10.4.10.183
Last Seen	2013-12-06 18:17:27 on 10.4.10.183
Event Count	7
Seen On	4 hosts
Seen On Breakdown	2 senders → 3 receivers

Trajectory



An unknown file is present on IP: 10.4.10.183, having been downloaded from Firefox

Events

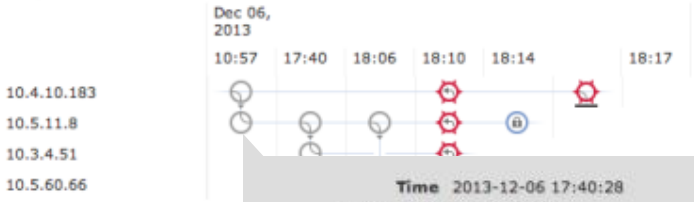
Time	Event Type	Sending IP	Receiving IP	File Name	Disp...	Action	Protocol	Client	Web Ap...	Description
2013-12-06 10:57:13	Retrospectiv...				Malwa...					
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...					
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...					
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox		

Network File Trajectory for 0517f034...588e1374

File SHA-256	0517f034...588e1374
File Name	WindowsMediaInstaller.exe
File Type	MSEXE
File Category	Executables
Current Disposition	Malware
Threat Score	High

First Seen	2013-12-06 10:57:13 on 10.4.10.183
Last Seen	2013-12-06 18:17:27 on 10.4.10.183
Event Count	7
Seen On	4 hosts
Seen On Breakdown	2 senders → 3 receivers

Trajectory



Events Transfer

Dispositions Unknown

Time	2013-12-06 17:40:28
Event Type	File Received
IP Address	10.5.11.8
Received From	10.4.10.183
File Name	WindowsMediaInstaller.exe
Disposition	Unknown
Action	Malware Cloud Lookup
Application Protocol	HTTP
Client	Firefox

At 10:57, the unknown file is from IP 10.4.10.183 to IP: 10.5.11.8

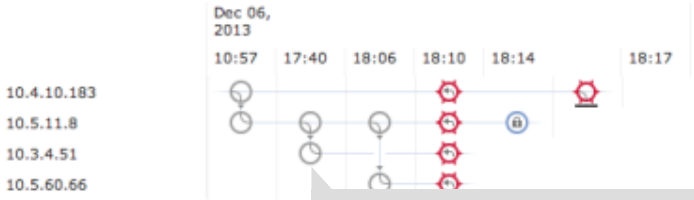
Events

Time	E			File Name	Disp...	Action	Protocol	Client	Web Ap...	Description
2013-12-06 10:57:13	Retrospectiv...				Malwa...					
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...					
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...					
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox		

Network File Trajectory for 0517f034...588e1374

File SHA-256	0517f034...588e1374
File Name	WindowsMediaInstaller.exe
File Type	MSEXE
File Category	Executables
Current Disposition	Malware
Threat Score	High
First Seen	2013-12-06 10:57:13 on 10.4.10.183
Last Seen	2013-12-06 18:17:27 on 10.4.10.183
Event Count	7
Seen On	4 hosts
Seen On Breakdown	2 senders → 3 receivers

Trajectory



Events Transfer
Dispositions Unknown

Time 2013-12-06 18:06:03
Event Type File Received
IP Address 10.3.4.51
Received From 10.5.11.8
File Name WindowsMediaInstaller.exe
Disposition Unknown
Action
Application Protocol NetBIOS-ssn (SMB)

Seven hours later the file is then transferred to a third device (10.3.4.51) using an SMB application

Events

Time	Event Ty			File Na				Client	Web Ap...	Description
2013-12-06 10:57:13	Retrospec				Malwa...					
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...					
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...					
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox		

Network File Trajectory for 0517f034...588e1374

File SHA-256	0517f034...588e1374
File Name	WindowsMediaInstaller.exe
File Type	MSEXE
File Category	Executables
Current Disposition	Malware
Threat Score	High

First Seen	2013-12-06 10:57:13 on 10.4.10.183
Last Seen	2013-12-06 18:17:27 on 10.4.10.183
Event Count	7
Seen On	4 hosts
Seen On Breakdown	2 senders → 3 receivers

Trajectory

Events Transfer Block
Dispositions Unknown Malware

Time	2013-12-06 18:10:03
Event Type	File Received
IP Address	10.5.60.66
Received From	10.5.11.8
File Name	WindowsMediaInstaller.exe
Disposition	Unknown
Action	
Application Protocol	NetBIOS-ssn (SMB)

The file is copied yet again onto a fourth device (10.5.60.66) through the same SMB application a half hour later

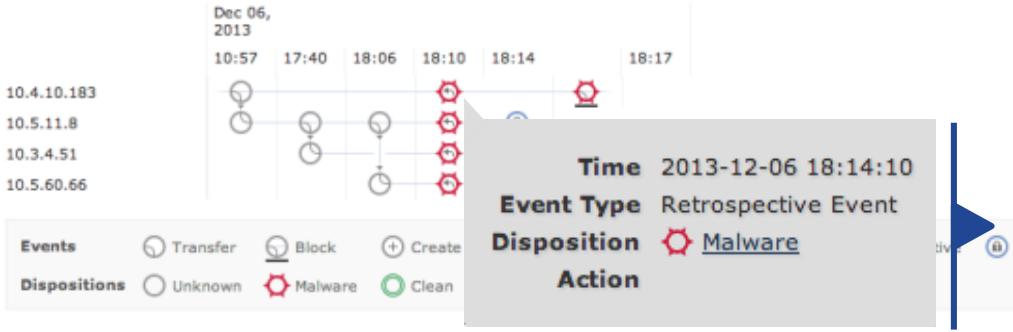
Events

Time	Event Type	Se							Web Ap...	Description
2013-12-06 10:57:13	Retrospectiv...									
2013-12-06 17:40:28	Transfer	10								Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...					
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...					
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox		

Network File Trajectory for 0517f034...588e1374

File SHA-256	0517f034...588e1374	**First Seen**	2013-12-06 10:57:13 on 10.4.10.183
File Name	WindowsMediaInstaller.exe	**Last Seen**	2013-12-06 18:17:27 on 10.4.10.183
File Type	MSEXE	**Event Count**	7
File Category	Executables	**Seen On**	4 hosts
Current Disposition	Malware	**Seen On Breakdown**	2 senders → 3 receivers
Threat Score	High		

Trajectory



The Cisco Collective Security Intelligence Cloud has learned this file is malicious and a retrospective event is raised for all four devices immediately.

Events

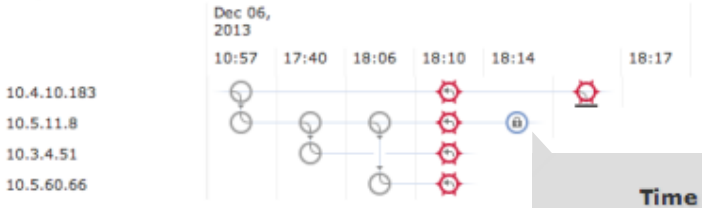
Time	Event Type	Sending IP	Receiving IP	File Name	Disp...	Action	Protocol	Client	Web Ap...	Description
2013-12-06 10:57:13	Retrospectiv...				Malwa...					
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...					
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...					
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox		

Network File Trajectory for 0517f034...588e1374

File SHA-256	0517f034...588e1374
File Name	WindowsMediaInstaller.exe
File Type	MSEXE
File Category	Executables
Current Disposition	Malware
Threat Score	High

First Seen	2013-12-06 10:57:13 on 10.4.10.183
Last Seen	2013-12-06 18:17:27 on 10.4.10.183
Event Count	7
Seen On	4 hosts
Seen On Breakdown	2 senders → 3 receivers

Trajectory



Events: Transfer | Block | Create | Mo...
Dispositions: Unknown | Malware | Clean | Cu...

Time	2013-12-06 18:14:23
Event Type	File Quarantined
IP Address	10.5.11.8
File Name	WindowsMediaInstaller.exe
Disposition	Malware
Action	

At the same time, a device with the FireAMP endpoint connector reacts to the retrospective event and immediately stops and quarantines the newly detected malware

Events

Time	Event Type	Sending IP			Disp...	A...			...ption
2013-12-06 10:57:13	Retrospectiv...				Malwa...				
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox	Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...				
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...				
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox	

Network File Trajectory for 0517f034...588e1374

File SHA-256	0517f034...588e1374
File Name	WindowsMediaInstaller.exe
File Type	MSEXE
File Category	Executables
Current Disposition	Malware
Threat Score	High

First Seen	2013-12-06 10:57:13 on 10.4.10.183
Last Seen	2013-12-06 18:17:27 on 10.4.10.183
Event Count	7
Seen On	4 hosts
Seen On Breakdown	2 senders → 3 receivers

Trajectory

Events: Transfer | Block | Create | Move
Dispositions: Unknown | Malware | Clean | Custom

Time	2013-12-06 18:17:27
Event Type	File Sent
IP Address	10.4.10.183
Blocked Recipient	10.5.11.8
File Name	WindowsMediaInstaller.exe
Disposition	Malware
Action	Malware Block
Application Protocol	HTTP
Client	Firefox

8 hours after the first attack, the Malware tries to re-enter the system through the original point of entry but is recognized and blocked.

Events

Time	Event Type	Sending IP	Receiving IP	File Name	Disp...	Action	Protocol	Client	Web Ap...	Description
2013-12-06 10:57:13	Retrospectiv...				Malwa...					
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...					
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...					
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox		

DDOS protection

Firepower DDoS Mitigation is provided by Radware Virtual DefensePro (vDP) Maximum Performance

Parameter	Value for 41xx
Maximum mitigation capacity/throughput	10 Gbps
Maximum legitimate concurrent sessions	209,000 Connections Per Second (CPS)
Maximum DDoS flood attack prevention rate	1,800,000 Packets Per Second (PPS)

Parameter	Firepower 9300 with 1 Security Module	Firepower 9300 with 2 Security Modules	Firepower 9300 with 3 Security Modules
Maximum mitigation capacity/throughput	10 Gbps	20 Gbps	30 Gbps
Maximum legitimate concurrent sessions	209,000 Connections Per Second (CPS)	418,000 Connections Per Second (CPS)	627,000 Connections Per Second (CPS)
Maximum DDoS flood attack prevention rate	1,800,000 Packets Per Second (PPS)	3,600,000 Packets Per Second (PPS)	5,400,000 Packets Per Second (PPS)

Radware vDP Availability on Cisco Firepower Running Either ASA or FTD Software Image

Firepower	ASA	FTD
9300 – SM 44	✓	✓
9300 – SM 36	✓	✓
9300 – SM 24	✓	✓
4150	✓	✓
4140	✓	✓
4120	✓	✓
4110	✗	✓

vDP License Support:
FPR-RVDP-**10**G
FPR-RVDP-**5**G
FPR-RVDP-**2**G
FPR-RVDP-**1**G
FPR-RVDP-**500**M
FPR-RVDP-**200**M

Purchase vDP licenses based on the amount of the client's peak legitimate traffic flow

Expected ASA or FTD Image Performance with 6 of the Available Cores Assigned to vDP

Firepower	Expected Performance FTD + vDP	Pass Fail
9300 – SM 44	93.2%	✓
9300 – SM 36	91.7%	✓
9300 – SM 24	87.5%	✓
4150	93.2%	✓
4140	91.7%	✓
4120	87.5%	✓
4110	75.0%	✓

Performance Criteria

- vDP fixed at 6 cores
- Subtract vDP cores from total cores
- vDP may affect performance
- Percentage of remaining cores = Expected Performance
- Pass = Tested performance was equal or better than Expected Performance (within error)

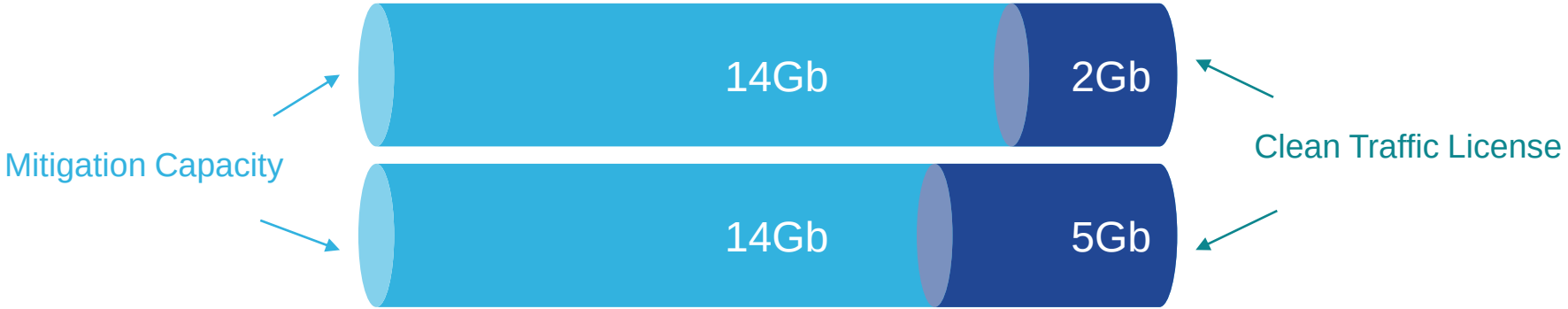
Capacity vs. Licensing

Inspection and mitigation capacity

- Capacity based on # cores assigned to the VM
- Fixed at 6 cores (1 management, 5 software)
- vDP @ 6 cores = 14Gb Inspection Capacity per Instance
  - vDP 8.10 is 40% more efficient than previous version @ 10Gb

Licensing is based on max peace time traffic

- Peace time traffic is a known value, attack size is unknown
- If peak traffic is 2Gb, purchase a 2Gb clean traffic license
- 14Gb – 2Gb = 12Gb of DDoS Scrubbing on Box



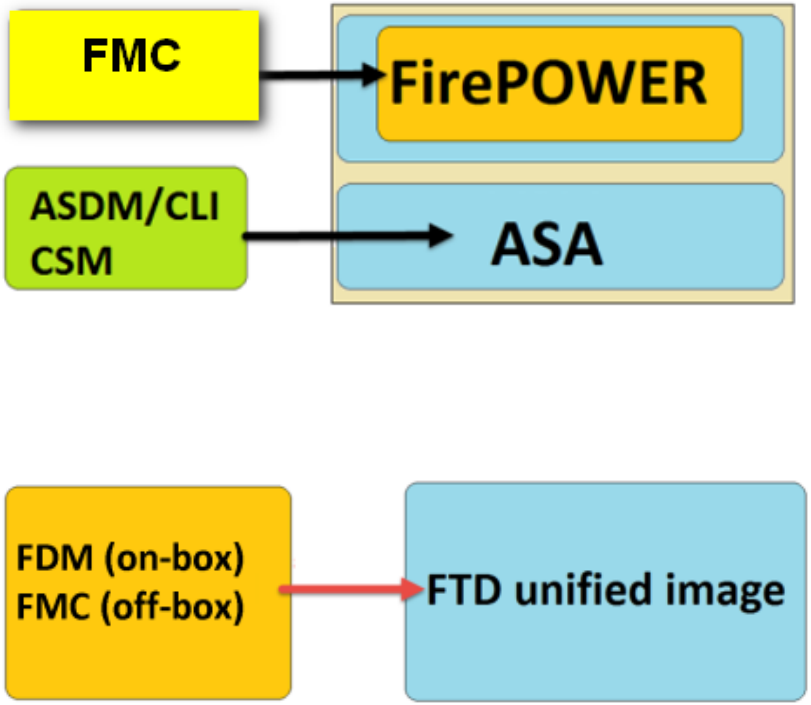
***Future**: Ability to change # of cores assigned to VM*

NGFW Management

FirePOWER on ASA vs FTD

FirePOWER on ASA
Requires 2 software images
2 Operating Systems on same HW
2 management applications

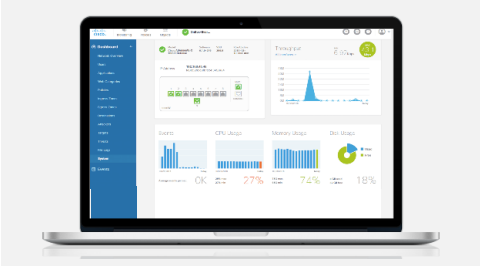
FTD
Requires 1 software images
1 Operating Systems on same HW
1 management applications



Cisco offers multiple management solutions

On-box, web-based management

Firepower Device Manager



- Consolidated management
- Enhanced control
- Easy set-up

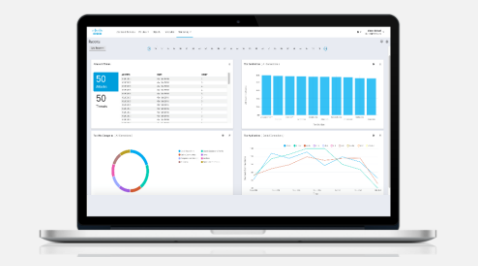
Centralized management for multiple devices

Firepower Management Center

- Unified insight
- Scalable management
- Intelligent automation

Cloud-based policy orchestration for multiple sites

Cisco Defense Orchestrator



- Simple interface
- Efficient management
- Streamlined user experience

FMC Platforms

Virtual (2-10-25)

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

FMC1000	FMC2500	FMC4500
• Up to 50 sensors managed • 60 million maximum events • 900 GB event storage • Network map up to 50K hosts, 50K users	• Up to 300 sensors managed • 60 million maximum events • 1.8 TB event storage • Network map up to 150K hosts, 150K users	• Up to 750 sensors managed • 300 million maximum events • 3.2 TB event storage • Network map up to 600K hosts, 600K users

https://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/datasheet-c78-736775.html

NGFW Performance

Performance Details

[1] HTTP sessions with an average packet size of 1024 bytes

[2] 1024 bytes TCP firewall performance

Features	Cisco Firepower Model			
	9300 with 1 SM-24 Module	9300 with 1 SM-36 Module	9300 with 1 SM-44 Module	9300 with 3 SM-44 Modules
Throughput FW + AVC (Cisco Firepower Threat Defense)[1]	30 Gbps	42 Gbps	54 Gbps	135 Gbps
Throughput: FW + AVC + NGIPS (Cisco Firepower Threat Defense)[1]	24 Gbps	34 Gbps	53 Gbps	133 Gbps

Performance Details

[1] HTTP sessions with an average packet size of 1024 bytes

[2] 1024 bytes TCP firewall performance

Features	Cisco Firepower Model							
	2110	2120	2130	2140	4110	4120	4140	4150
Throughput FW + AVC (Cisco Firepower Threat Defense)[1]	2.0 Gbps	3 Gbps	4.75 Gbps	8.5 Gbps	12 Gbps	20 Gbps	25 Gbps	30 Gbps
Throughput: FW + AVC + NGIPS (Cisco Firepower Threat Defense)[1]	2.0 Gbps	3 Gbps	4.75 Gbps	8.5 Gbps	10 Gbps	15 Gbps	20 Gbps	24 Gbps

Performance Details

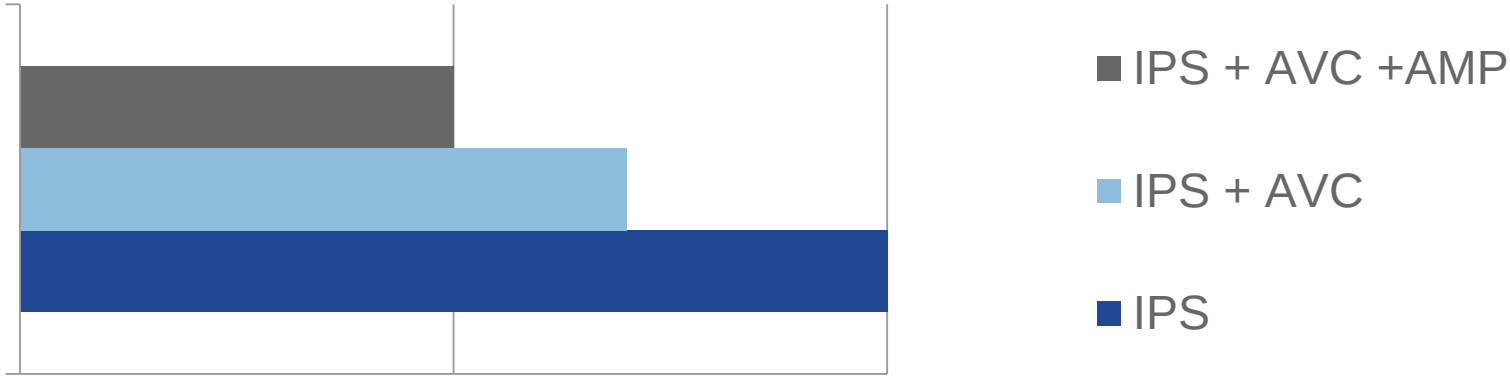
[1] HTTP sessions with an average packet size of 1024 bytes

[2] 1024 bytes TCP firewall performance

Features	Cisco ASA 5500-FTD-X Model							
	5506-FTD-X	5506W-FTD-X	5506H-FTD-X	5508-FTD-X	5516-FTD-X	5525-FTD-X	5545-FTD-X	5555-FTD-X
Throughput FW + AVC (Cisco Firepower Threat Defense)[1]	250 Mbps	250 Mbps	250 Mbps	450 Mbps	850 Mbps	1100 Mbps	1500 Mbps	1750 Mbps
Throughput: FW + AVC + NGIPS (Cisco Firepower Threat Defense)[1]	125 Mbps	125 Mbps	125 Mbps	250 Mbps	450 Mbps	650 Mbps	1000 Mbps	1250 Mbps

Performance Impact of Multiple Services

- Reduce the datasheet IPS throughput by:
  - 30-45% for IPS + AVC
  - 50-65% for IPS + AVC + AMP
  - URL filtering does not significantly affect performance.



NGFW Deployment use cases

Pick from many deployment modes

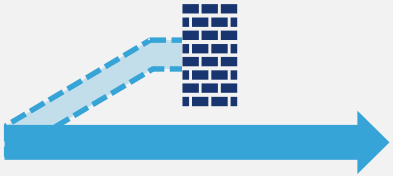
Firewall deployment modes

Inline or Passive

Inline

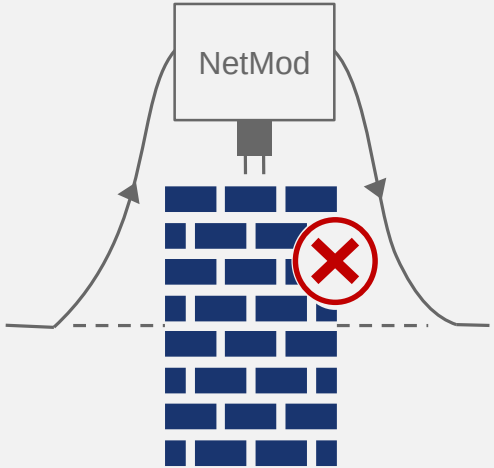
Inline Tap

Passive



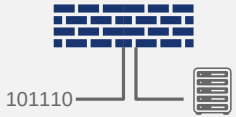
NGFW interfaces in three modes

Fail-to-wire NetMods

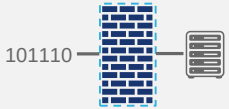


Additional options

Routed



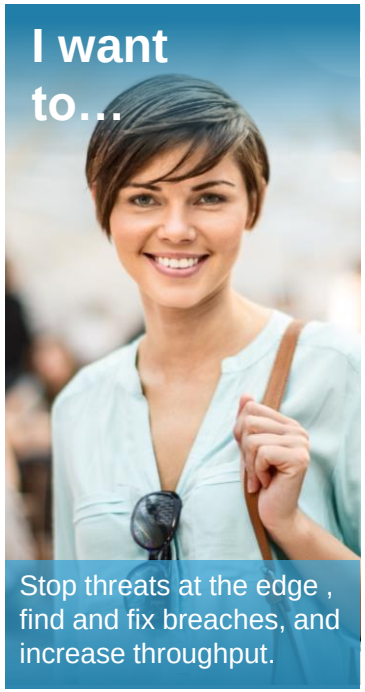
Transparent

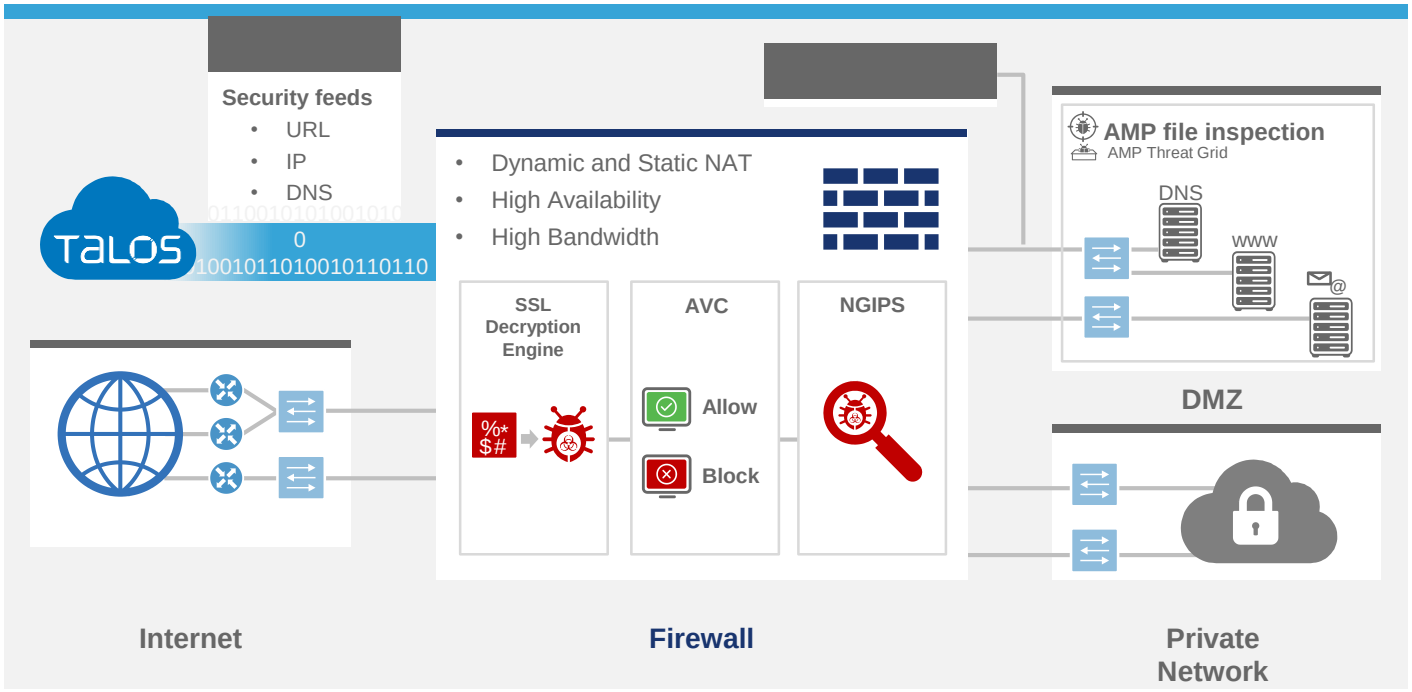


Virtual or Physical

firewall mode

Secure your company's internet edge





Protect your local data center at the edge

Prepare | Secure | Define policies | Uncover threats | Respond | Remediate

Security feeds
URL | IP | DNS

TALOS

HR
Finance
DevOps
TrustSec

- High Availability
- High Bandwidth

SSL Decryption Engine
AVC
Allow
Block
NGIPS

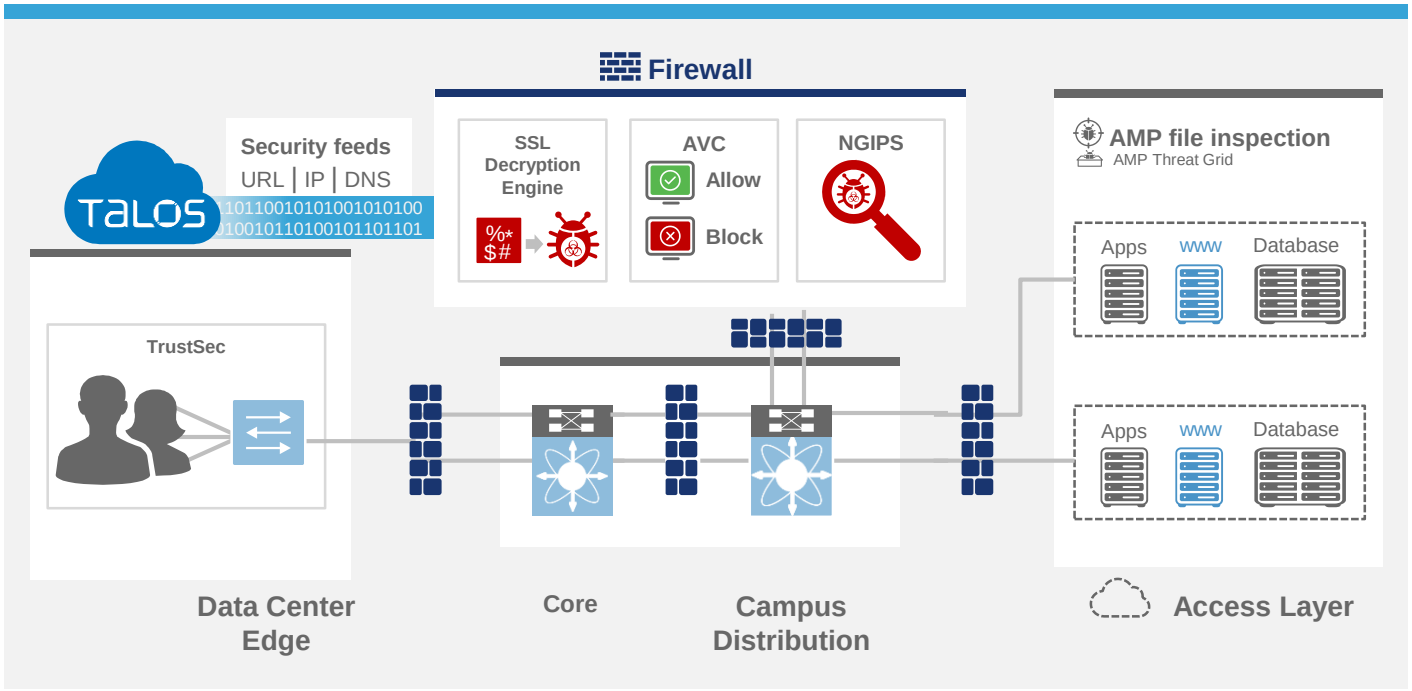
AMP file inspection
AMP Threat Grid

- Clustering
- Support for North-South and East-West traffic

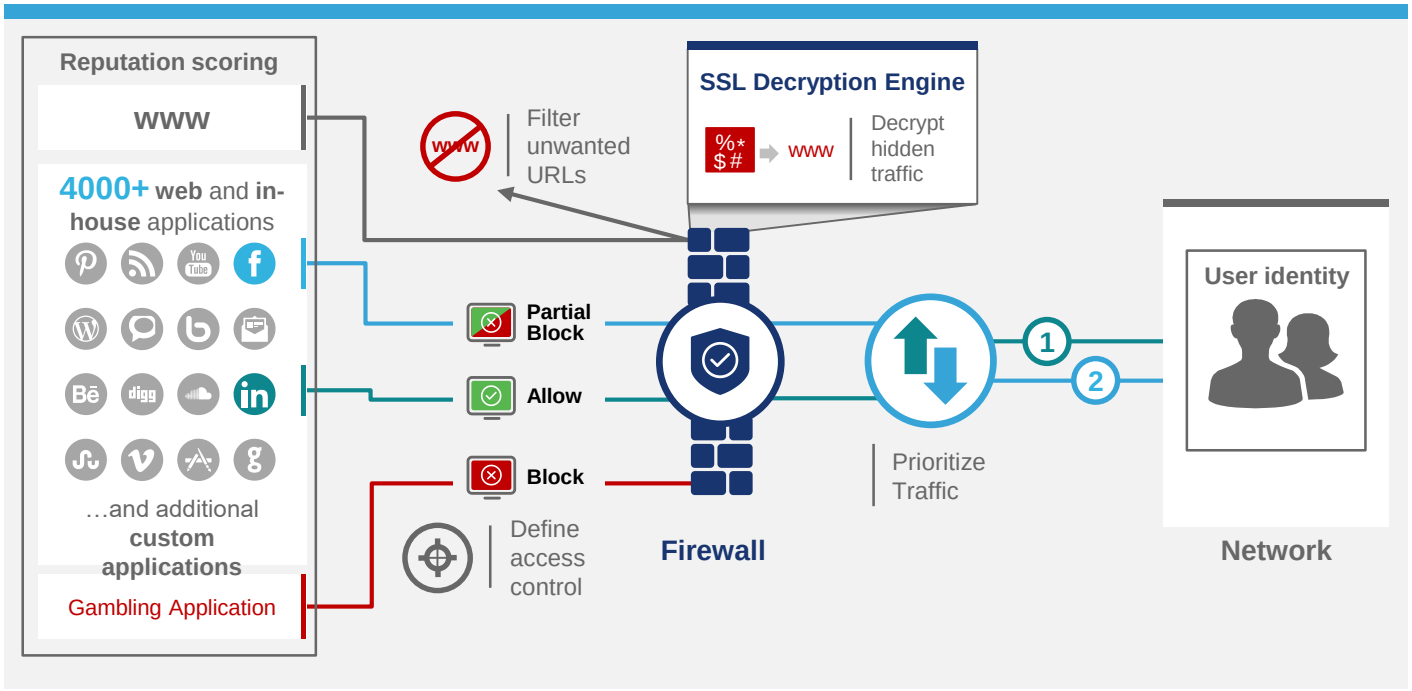
Financial data
HR data
In-house app

Data Center Edge | **Firewall** | **Data Center Network**

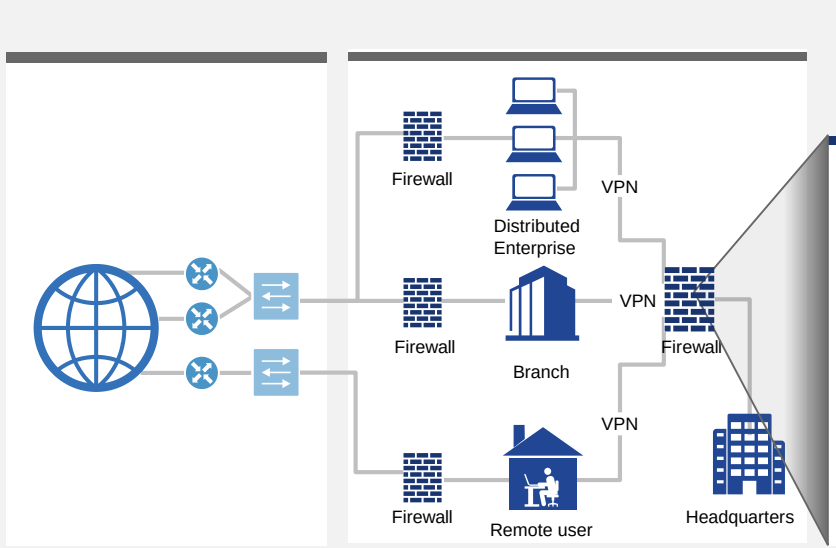
Keep threats out of campus security domains

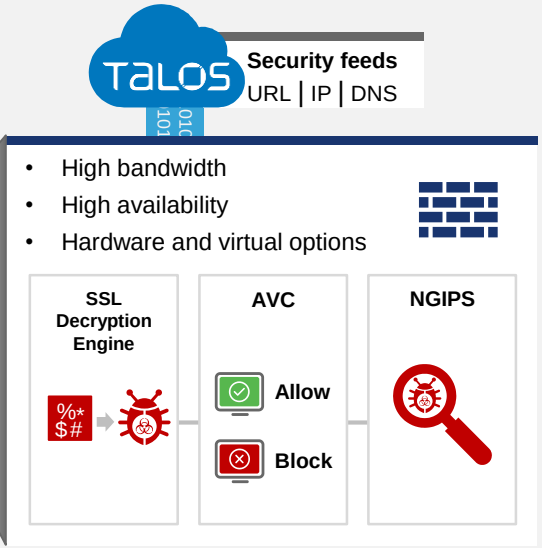


Enforce acceptable (App) use within the organization



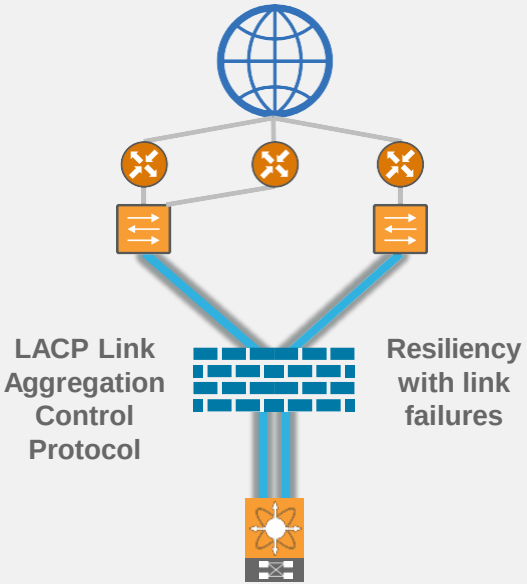
Extend secure access to other locations (WAN+RA)



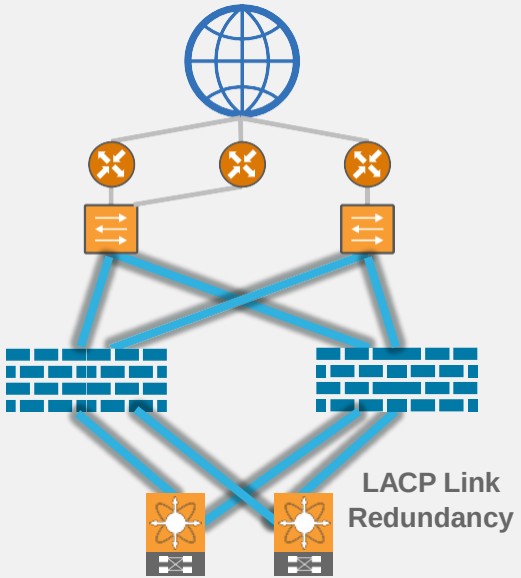


Firewall Link Aggregation – High Availability - Clustering

Link Redundancy



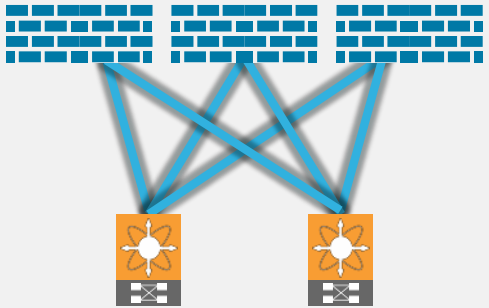
High Availability



A/S HA на ПО FTD

A/A и A/S HA на ПО ASA

Inter-chassis Clustering



6*41xx, 5*93xx (по 3) на ПО FTD

2*ASA55xx, 16*41xx, 5*93xx (по 3) на ПО ASA

cisco Elcore | elko.by

NEW NGFW Platforms

Firepower 9300 Overview

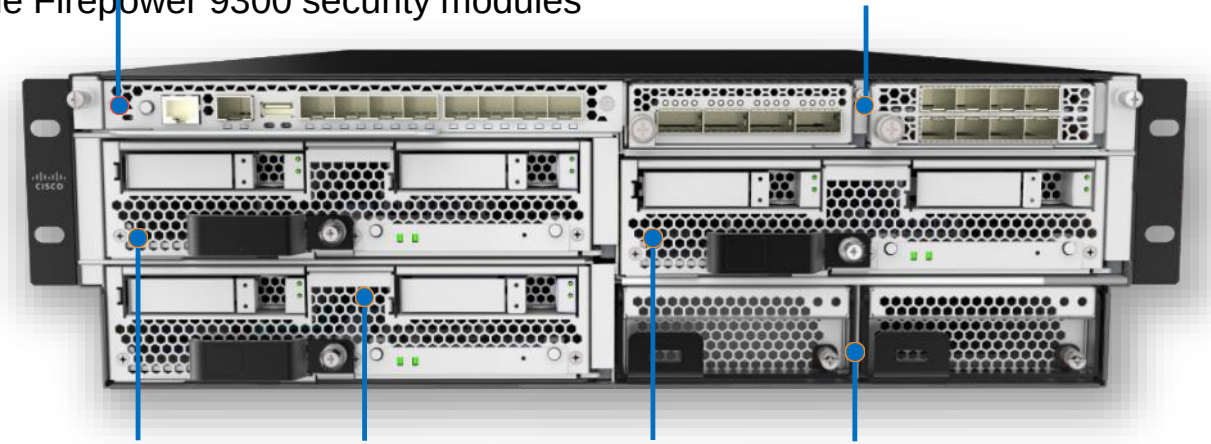
Supervisor

- provides chassis management
- Network connection 8*1/10G SFP+
- directs traffic to/from the Firepower 9300 security modules

Network Modules

- Дополнительные сетевые порты 10GE, 40GE, 100GE
- Отдельные модули с Hardware bypass Fail-to-Wire (FTW) 10GE, 40GE

3RU

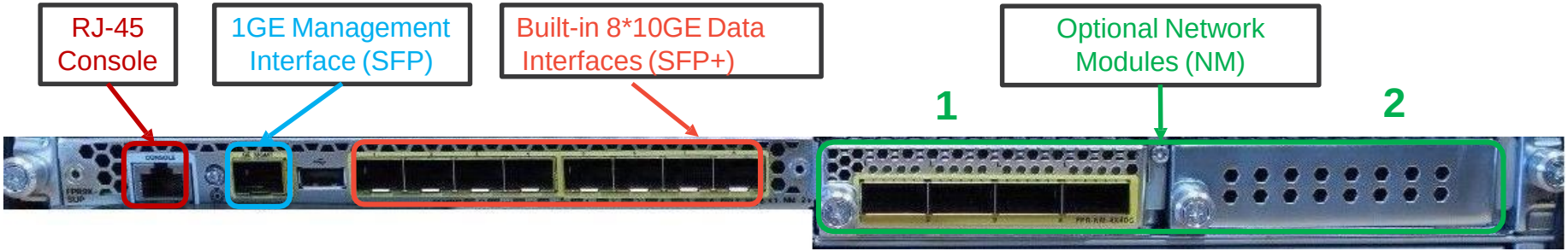


Security Modules

- Embedded packet/flow classifier (Smart NIC) and crypto hardware
- CPUs with a total of 24, 36 or 44 physical cores (48, 72 or 88 with hyperthreading) + 2*800-GB SSDs in a default RAID 1
- Standalone or clustered within (up to 240Gbps) and across (1Tbps+) chassis
- Cisco (**ASA**, **FTD**) and third-party (**Radware DDoS**) applications
- Standalone or clustered within and across chassis

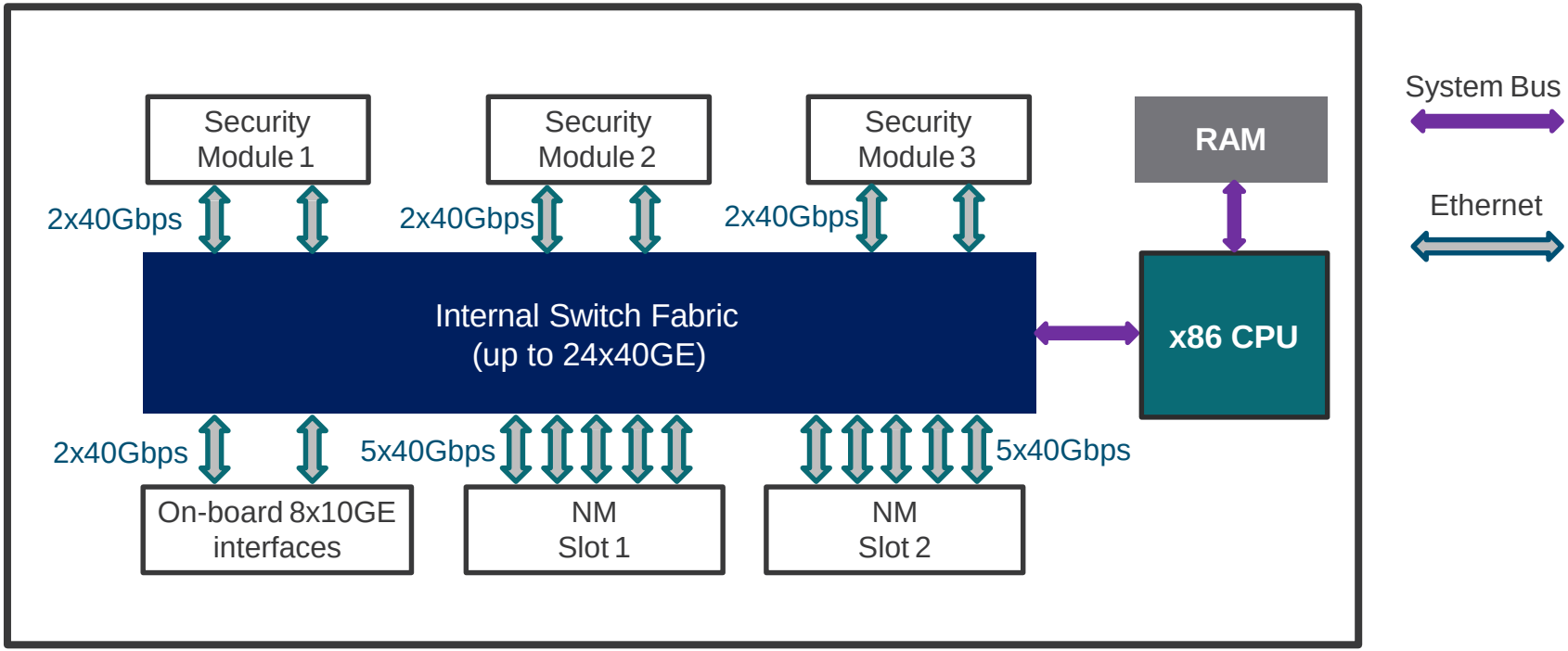
Redundant Power supplies and Fans

Supervisor Module



- Overall chassis management and network interaction
  - Network interface allocation and module connectivity (960Gbps internal fabric)
  - Application image storage, deployment, provisioning, and service chaining
  - Clustering infrastructure for supported applications
  - Smart Licensing and NTP for entire chassis

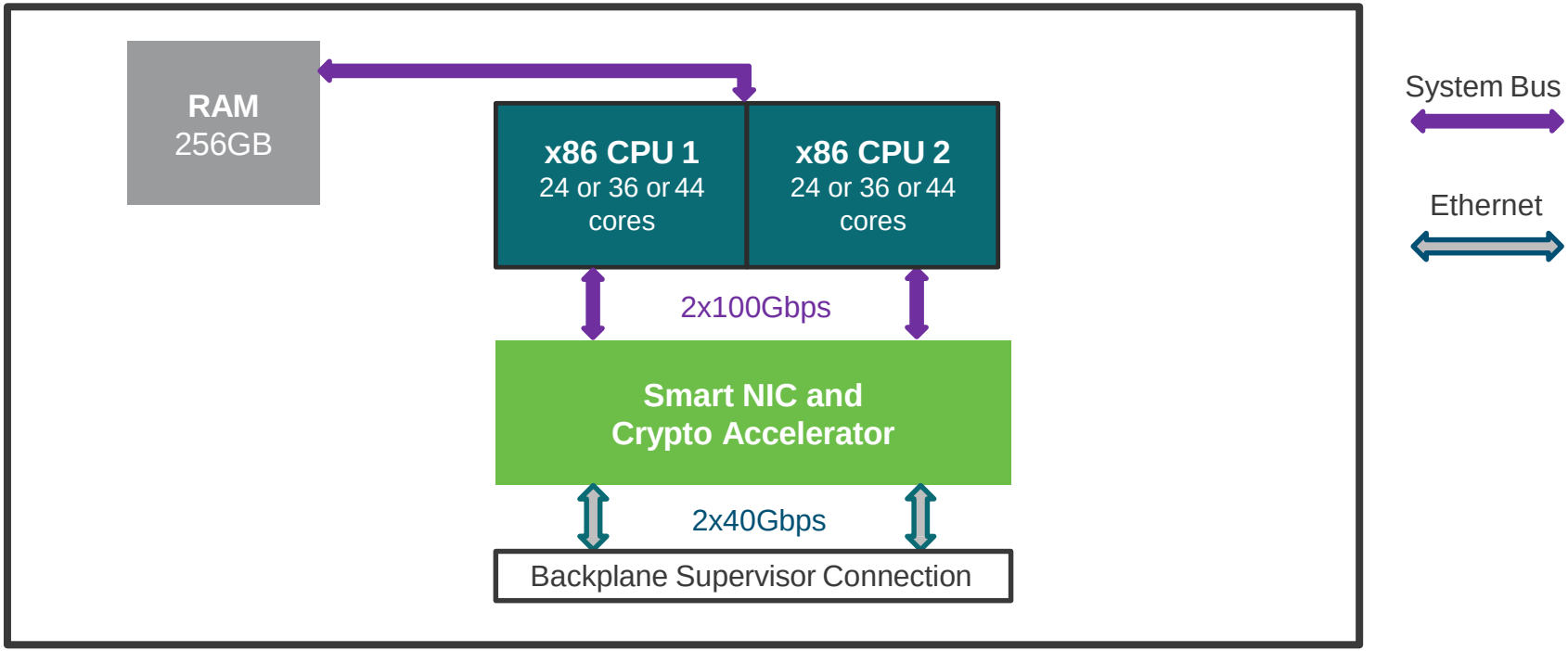
Supervisor Architecture



Firepower 9300 Security Modules

- Three configurations
  - **SM-44** : 88 x86 CPU cores (54Gbps **FTD** NGFW)
  - **SM-36** : 72 x86 CPU cores (42Gbps **FTD** NGFW)
  - **SM-24** : 48 x86 CPU cores (30Gbps **FTD** NGFW), NEBS Level 3 Certified
- Dual 800GB SSD in RAID1 by default
- Built-in hardware Smart NIC and Crypto Accelerator
  - Flow Offload
  - VPN connection acceleration
  - Transit TLS inspection with **FTD 6.2.3+**

Security Module Architecture



Firepower 4100 Overview

Built-in Supervisor and Security Module
- Same hardware and software architecture as 9300
- Fixed configurations (4110, 4120, 4140, 4150)
- Built-in 8*10GE Data Interfaces (SFP+)

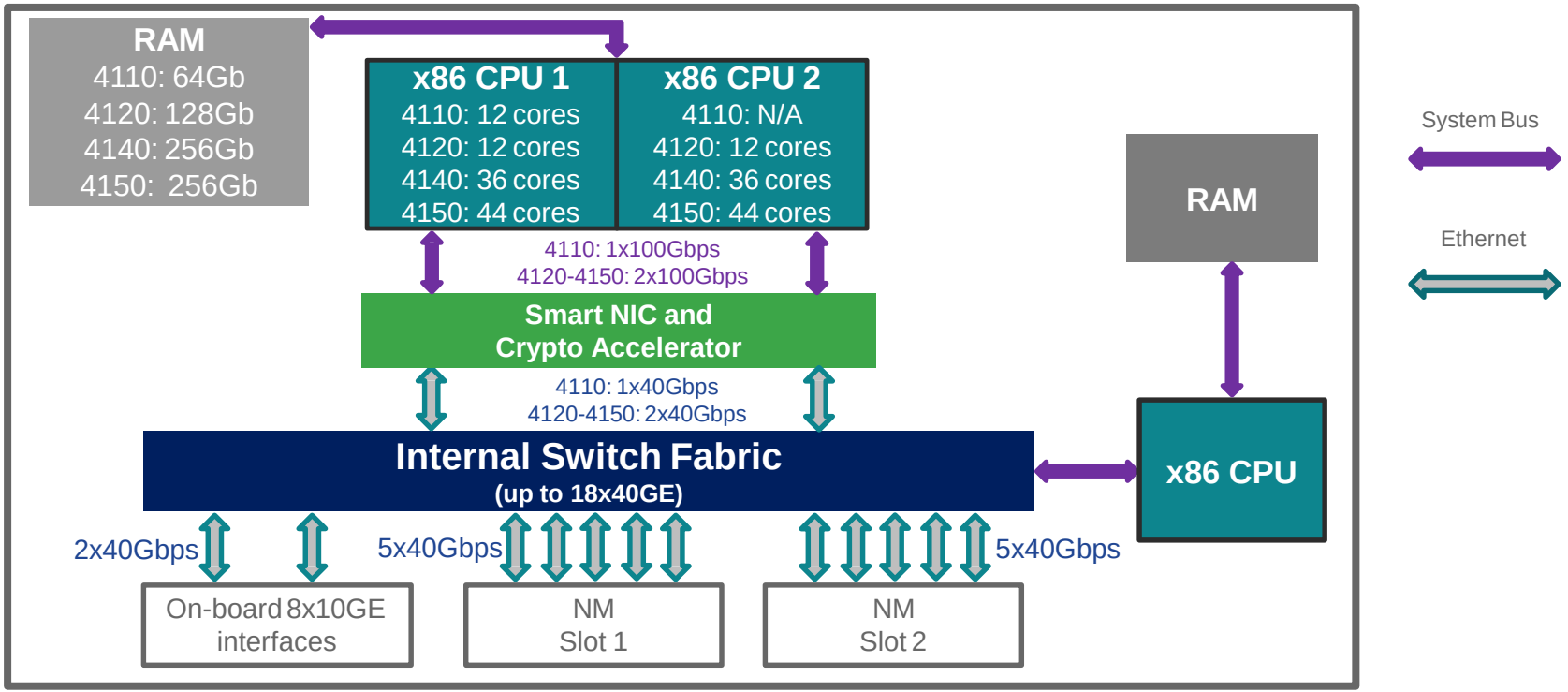
Solid State Drives
- Independent operation (no RAID)
- Slot 1 today provides limited AMP storage: 200GB for 4110, 4120 и 400GB for 4130, 4140
- Slot 2 future for AMP storage

1RU

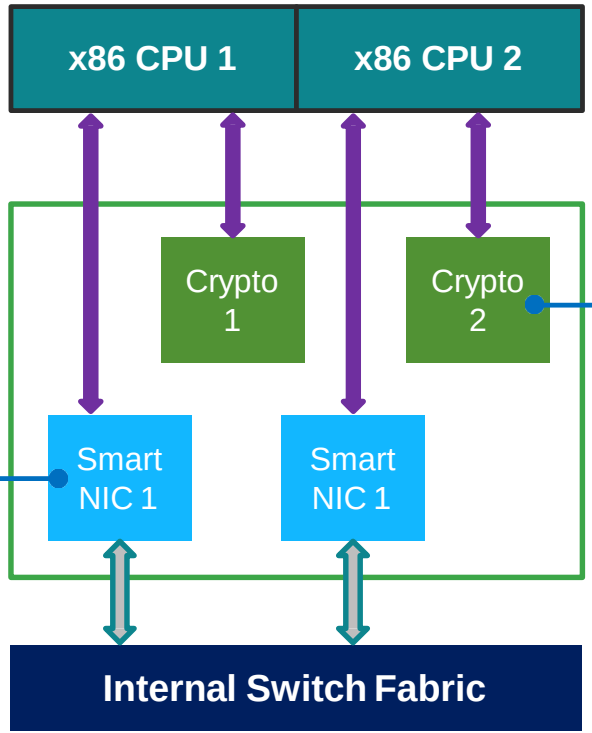
Redundant Power supplies and Fans

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

Firepower 4100 Architecture



Firepower 4100/9300 Smart NIC and Crypto



Crypto Accelerator
- Single on 4110, dual elsewhere
- Up to 20Gbps IPsec/TLS each
- Configurable core bias to IPsec/TLS
- IPsec S2S and RAVPN
- TLS/DTLS RAVPN
- TLS inspection assistance

Cisco Programmable NIC
- Single on 4110, dual elsewhere
- 40Gbps connectivity each
- Packet Matching and Rewrite
- Tracks **2M flows** for Offload

FXOS 2.3.1

System Bus

Ethernet

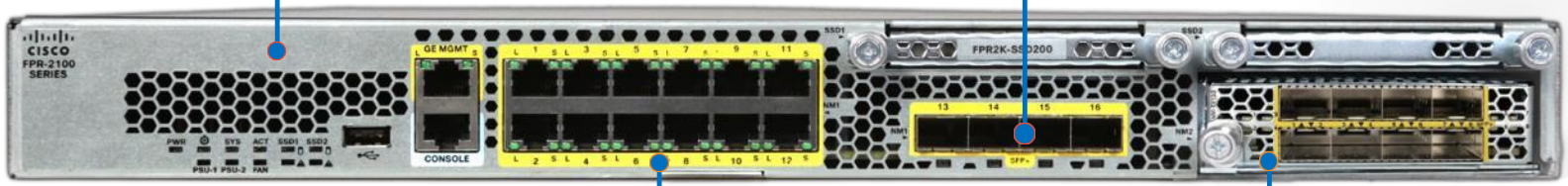
Firepower 2100 Overview

Redundant Power supplies and Fans
- only 4130, 4140

Integrated Security Platform for FTD or ASA Application
- Lightweight virtual Supervisor module
- Embedded x86 and NPU with Hardware Crypto Acceleration
- Fixed configurations (2110, 2120, 2130, 2140)
- Dual redundant power supplies on 2130 and 2140 only

SFP/SFP+ Data Interfaces
- 4x1GE on Firepower 2110 and 2120
- 4x10GE on Firepower 2130 and 2140

1RU



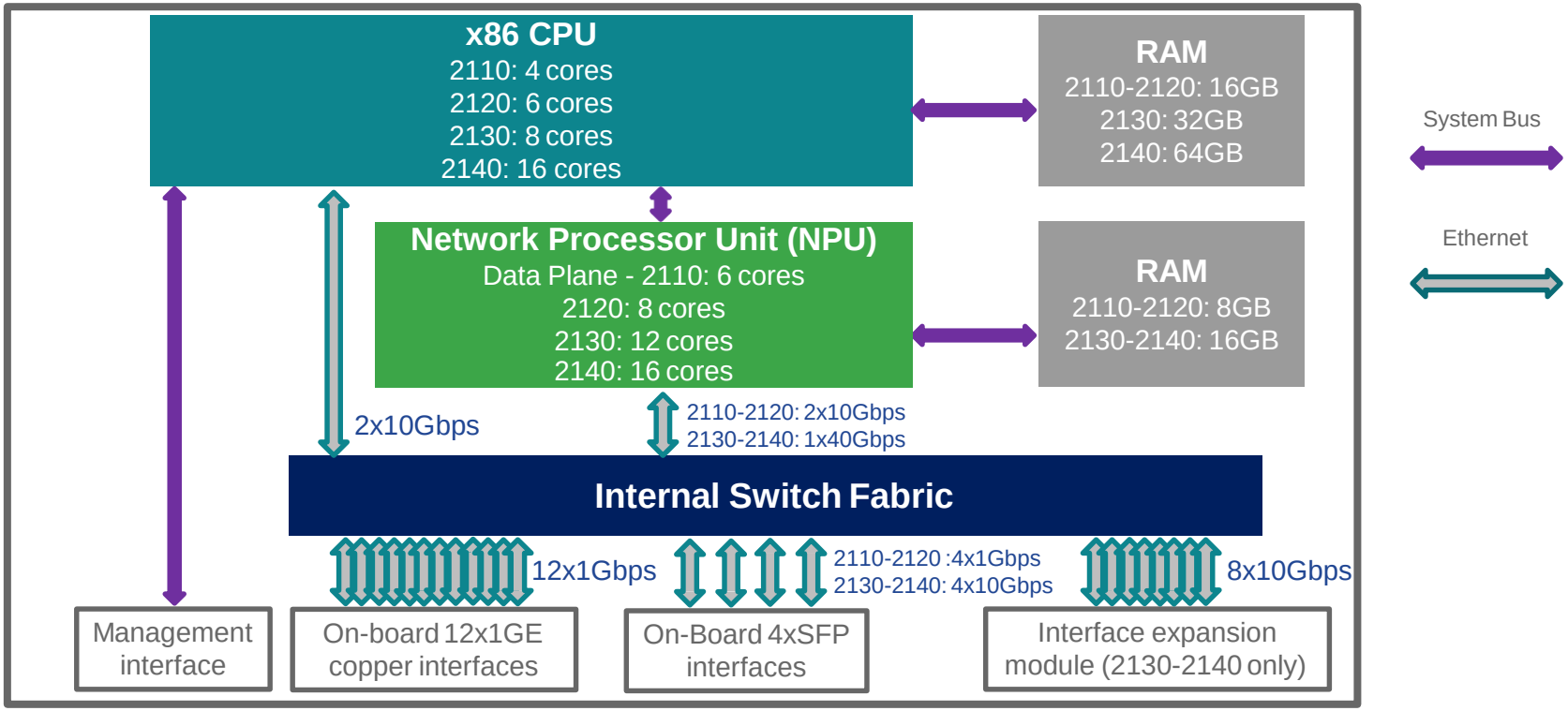
Copper Data Interfaces
- 12x1GE Ethernet

Network Module
- Firepower 2130 and 2140 only
- Same 8x10GE SFP module as on Firepower 4100/9300

Firepower 2100 Overview

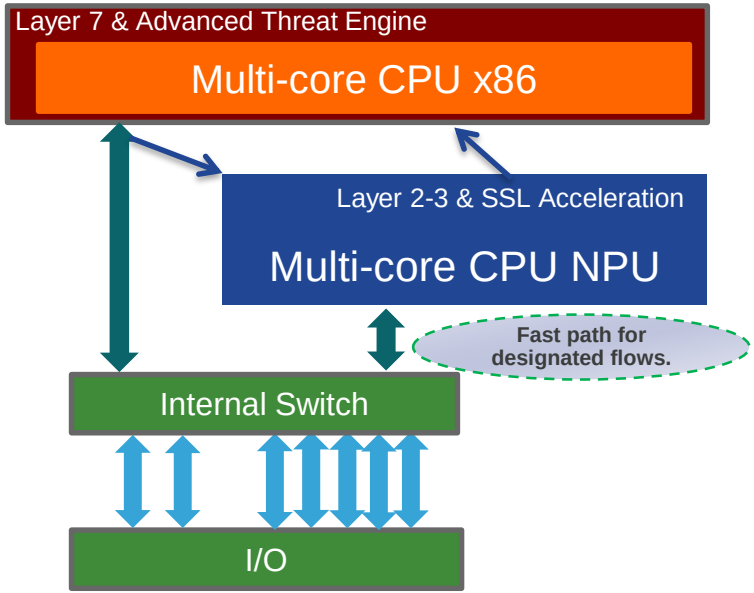
- Designed and optimized for **FTD** application
  - Data Plane runs on integrated NPU and crypto module
  - Threat-centric Advanced Inspection Modules run on x86
  - No separate Flow Offload engine
  - Supports **ASA** application as well
- Single point of management for chassis and application
  - Firepower Device Manager (FDM) for on-box
  - Firepower Management Center (FMC) for multi-device

Firepower 2100 Architecture



Benefits of Firepower 2100 Series NGFW
Dual Multi-core CPU Architecture

- **Sustained throughput performance,** when threat functions are enabled vs. competing designs
- **Flexibility and future-proofing** vs. ASIC-based designs that degrade as new defenses and functions are added
- **Fast Path** flows not requiring threat inspection, further enhancing performance



Standard Network Interfaces

- Supervisor attaches network modules to network
  - All interfaces are called “Ethernet” and 1-referenced (i.e. Ethernet1/1)
  - All external network ports require fiber or copper transceivers

8x10GE

- Firepower 2100, 4100, 9300
- Single width
- 1GE/10GE SFP
- OIR in **FXOS 2.3.1**

4x40GE

- Firepower 4100 and 9300
- Single width
- 4x10GE breakouts for each 40GE port
- OIR in **FXOS 2.3.1**

2x100GE

- Firepower 9300 only
- Double width
- QSFP28 connector
- No breakout support
- Future single-width 2x100GE and 4x100GE

Fail-to-Wire Network Modules

- Fixed interfaces, no removable SFP support
- NGIPS inline interfaces for standalone **FTD 6.1+** only
- Sub-second reaction time to application, software, or hardware failure
  - Designed to engage during unplanned failure or restart events
  - <90ms reaction time for Standby→Bypass with full power failure

8x1GE

- Firepower 2100, 4100
- Single width
- 10M/100M/1GE copper

6x1GE

- Firepower 2100, 4100
- Single width
- 1GE fiber SX

6x10GE

- Firepower 2100, 4100, 9300
- Single width
- 10GE SR or LR

2x40GE

- Firepower 4100 and 9300
- Single width
- 40GE SR4
- No 10GE breakout support

NGFW Competitive

Key Competitive Advantages

*No Performance Hit from NGIPS

2110	FW+AVC	FW+AVC+NGIPS
	2G	2G (NGFW)

2120	FW+AVC	FW+AVC+NGIPS
	3G	3G (NGFW)

2130	FW+AVC	FW+AVC+NGIPS
	4.5G	4.5G (NGFW)

2140	FW+AVC	FW+AVC+NGIPS
	8G	8G (NGFW)

	FW+AVC	FW+AVC+NGIPS
PA-3020	2G	1G (NGFW)
PA-3060	4G	2G (NGFW)

	FW-AVC	FW+AVC+NGIPS
FG-500D	3.5G	2G (NGFW)
	FW-Only	FW+AVC+NGIPS
FG-1000D	4.2G	3G (NGFW)

	FW-AVC	FW+AVC+NGIPS
CP-5600	2G	1G (NGFW)
	FW-AVC	FW+AVC+NGIPS
CP-5800	3G	1.5G (NGFW)

*Final Performance Values Subject to Change

Key Competitive Advantages

*No Performance Hit from NGIPS

***Up to 200% Performance vs. Price

2110

FW+AVC **2G**

FW+AVC+NGIPS **2G** (NGFW)

+106%

PA-3020 FW+AVC **2G** FW+AVC+NGIPS **1G** (NGFW)

PA-3060 FW+AVC **4G** FW+AVC+NGIPS **2G** (NGFW)

2120

FW+AVC **3G**

FW+AVC+NGIPS **3G** (NGFW)

+150%

FG-500D FW-AVC **3.5G** FW+AVC+NGIPS **2G** (NGFW)

FG-1000D FW-Only **4.2G** FW+AVC+NGIPS **3G** (NGFW)

2130

FW+AVC **4.5G**

FW+AVC+NGIPS **4.5G** (NGFW)

+200%

CP-5600 FW-AVC **2G** FW+AVC+NGIPS **1G** (NGFW)

CP-5800 FW-AVC **3G** FW+AVC+NGIPS **1.5G** (NGFW)

2140

FW+AVC **8G**

FW+AVC+NGIPS **8G** (NGFW)

*Final Performance Values Subject to Change

***HW Street Prices Compared

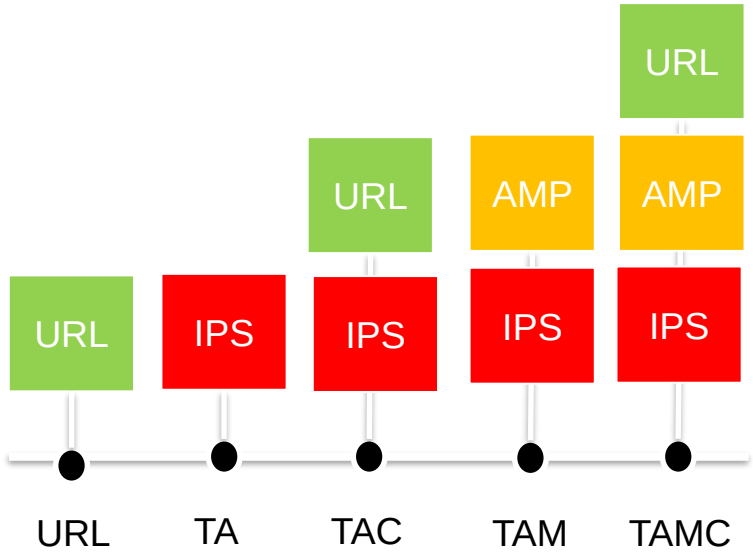
NSS Labs Releases 2017 NGFW Results

Product	Firewall	IPS	Stability & Reliability	Security Effectiveness
Barracuda Networks	100%	25.8%	100%	25.8%
Check Point	100%	89.6%	100%	89.6%
Cisco	100%	95.5%	100%	95.5%
Forcepoint	100%	99.9%	100%	99.9%
Fortinet 3200D	100%	78.6%	100%	78.6%
Fortinet 600D	100%	78.6%	100%	78.6%
Juniper Networks	100%	37.8%	100%	37.8%
Palo Alto Networks	100%	39.7%	100%	39.7%
SonicWall	100%	26.4%	100%	26.4%
Sophos	100%	90.4%	100%	90.4%
WatchGuard	100%	88.9%	100%	88.9%

NGFW Licenses

Лицензирование платформы ASA + Firepower
Classic licensing = PAK (привязка лицензии к устройству)

- Функционал FW, R&S, NAT, s2s VPN включен по умолчанию (постоянный)
- Включены также Control (AVC) and Protection (IPS+SI+File Control) лицензии - постоянные
- Обновления AVC включены в SMARTnet
- Обновления сигнатур IPS требуют отдельную подписку (TA-)
- Функционал URL, AMP, IPS – временные подписки на 1, 3, 5 (включая обновления) на каждое устройство
- RA VPN – AnyConnect (Plus, Apex and VPN Only) licenses are required (постоянные или временные)



PAK → http://www.cisco.com/web/go/license

Лицензирование платформы ASA + Firepower
Classic licensing = PAK (привязка лицензии к устройству)

- Security Plus Lic (опциональная только для ASA5506X) – HA, > сессии, > VLAN
- Security Context Lic – виртуализация FW (поддерживается начиная с ASA5508X)
  - ASA и ASA on the Firepower 2100 – 2 x Security Context включены по умолчанию
  - ASA on the Firepower 4100 и 9300 - 10 x Security Context включены по умолчанию
- Licenses required for both elements of HA pair
- DDOS Protection lic based on known legitimate traffic 200Mb – 30Gb (41xx-93xx) - - by Radware

PAK → http://www.cisco.com/web/go/license

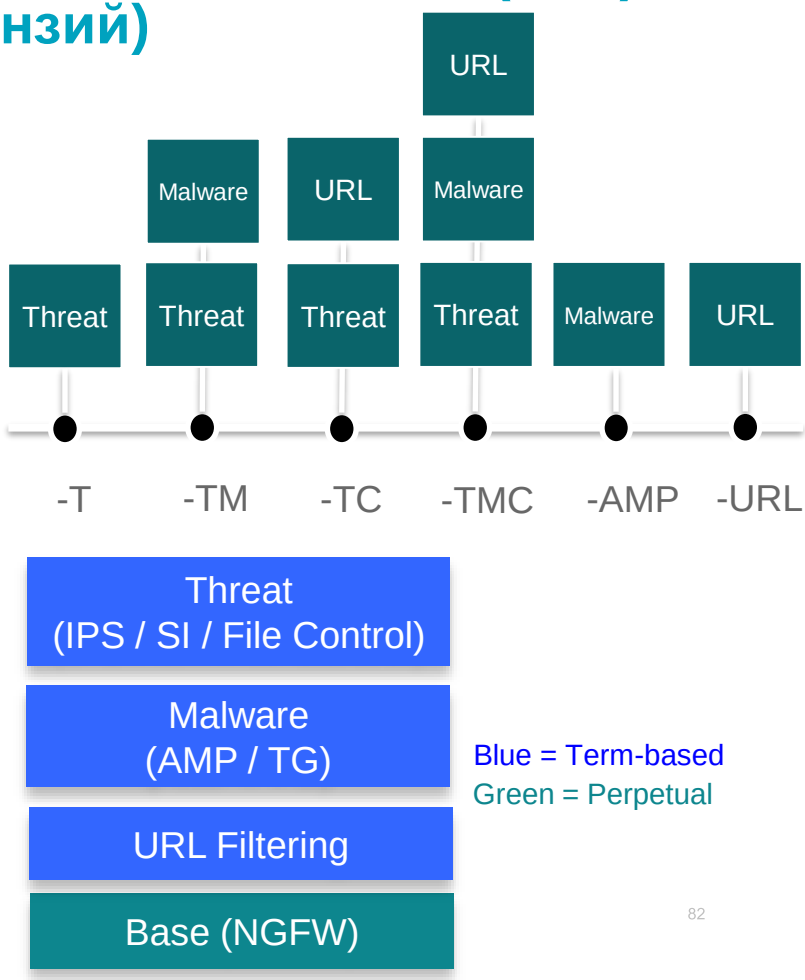
Лицензирование платформы Firepower Threat Defense (FTD) Smart licensing = SA (общий пул лицензий)

- Функционал FW, R&S, NAT, AVC, s2s VPN включен по умолчанию (постоянный)

- Обновления AVC включены в SMARTnet

- Необходима Strong Encryption License (3DES/AES) – дополнительная, постоянная
- Функционал URL, Malware, Threat – временные подписки на 1, 3, 5 (включая обновления) на каждое устройство
- RA VPN – AnyConnect (Plus, Apex and VPN Only) licenses are required (постоянные или временные)

Smart Account - https://software.cisco.com/



Лицензирование платформы Firepower Threat Defense (FTD) Smart licensing = SA (общий пул лицензий)

- Security Plus Lic включена в Base license для всех устройств
- Security Context Lic – виртуализация FW - feature is not available in Firepower 6.2.3
- Licenses required for both elements of HA pair
- High Availability bundle – минус 50% на подписки на второе устройство
- DDOS Protection lic based on known legitimate traffic 200Mb – 30Gb (41xx-93xx) - by Radware

Smart Account - https://software.cisco.com/
https://cisco.com/go/smartaccounts

Заключение

Cisco has an NGFW solution for every business

Small and Midsized Business

ASA 5506-X / 5506W-X / 5506H-X /
5508-X / 5516-X

NGFWs for SMBs and distributed enterprises with integrated threat defense, a low TCO, and simplified security management.

Midrange

ASA 5525-X/ ASA 5545-X/
ASA 5555-X

Firepower
2110/2120

Firepower
2130/2140

Enterprise-class security for the internet edge, with superior threat defense, sustained performance, and simple management.

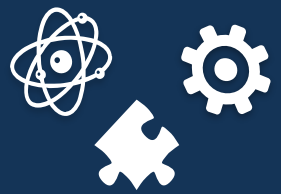
Enterprise

Firepower
4110/4120/4140/4150

Firepower 9300

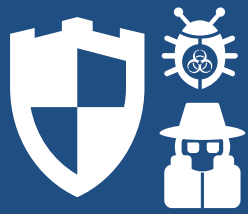
From the internet edge to carrier grade security for data centers and other high-performance settings, with multiservice security, flexible architecture, and unified management.

Cisco Firepower NGFW



Fully Integrated

- FW / AVC / IPS
- AMP – network / endpoint
- Analysis and remediation
- Cisco security solutions
- Application-aware DDoS



Threat Focused

- Networkwide visibility
- Industry-best threat protection
- Known and unknown threats
- Track / contain / recover

Unified Management

- Across attack continuum
- Manage, control, and investigate
- Automatically prioritize
- Automatically protect

Спасибо за внимание!

Максим Порицкий

инженер по направлению Cisco, CCIE R&S

m.poritsky@elcoregroup.com

14.04.2018