Cisco Expo 2009

Новости из области сигурности рачунарских мрежа

Татјана Бошковић, Систем инжењер

tboskovi@cisco.com

Utorak, 10. novembar 2009.

Cisco Expo 2009

08.00 - 09.00	Registracija			
09.00 - 09.15	Svečano otvaranje i reč dobrodošlice - Goran Obradović, General manager, Cisco Srbija			
09.15 - 09.30	Planovi razvoja ICT u Srbiji - Jasna Matić, Ministarka, Ministarstvo telekomunikacija			
09.30 - 10.00	Razvoj uz pomoć ICT - Massimo Migliuolo, Vice President, Emerging Markets, Cisco			
10.00 - 10.45	Tehnologija za svet koji se menja - Axel Clauberg , Director System Engineering, Solutions and Technologies, Emerging Markets, Cisco			
10.45 - 11.15	Pauza	Sala A	Sala B	Sala C	Sala D
11.15-12.15	Nova generacija ISR rutera, Denis Zotov*	Data centar virtualizacija - Dizajn sesija, Višnja Milovanović	EANTC - Experience Provider Mega Test, Carsten Rossenhövel i Jason Sauviac*	Wireless novosti , Dragan Novaković
12.15-13.15	Novosti iz oblasti sigurnosti računarskih mreža, Tatjana Bošković	Unified Computing System, Višnja Milovanović	Cisco ASR 9000, Đorđe Vulović	Cisco rešenja za video na zahtev i online streaming, Jan Bogaert
13.15 - 14.00	Ručak			
14.00-15.00	Appocalypse Now? - Ivica Ostojić	Business Continuance & Disaster Recovery, Višnja Milovanović	CMTS i Docsis 3.0 novosti, Daniel Etman*	Cisco Services - Build and Optimize your Network, Hans Rill and Jan Bogaert*
15.00-16.00	Predstavljanje learning partnera Fast lane - Boris Ilovar, Fast lane	Rešenje za kontinulanu zaštitu i replikaciju podataka u heterogenim okruženjima - EMC Recover Point - Dejan Živanović, EMC	IBM/Cisco Unified Comminications solution - Petar Kovačević, IBM	Cisco UC – Platforma za poslovne aplikacije- Dejan Gavrilović, PSTech
16.00-17.00	Cisco Application eXtension Platform, Denis Zotov*	Unified Communications novosti, Aleksandar Vulović	Cisco 7600/ASR1000 novosti, Marko Vukadinović	Business Video, Ivan Zaklanovic

Sreda, 11. novembar 2009.

Cisco Expo 2009

	Sala A	Sala B	Sala C	Sala D
09.30 - 10.30	conf t:Cisco IPS u poslovnom okruzenju, Petr Ruzicka *	SIP trunk za PSTN pristup, Aleksandar Vulović	conf t: ISG - Intelligent Service Gateway, Đorđe Vulović	Cisco Borderless Network, Petr Pavlu*
10.30 - 11.30	conf t: Cisco IPSec VPN rešenja u mrežama poslovnih korisnika, Dragan Novaković	Cisco Unified Customer Voice Portal, Mario Gianni*	Najnovija dostignuća u BGP - Josef Ungerman*	IP Video Contribution for Broadcasters, Bojan Nedelčev
11.30 -11.45	Pauza			
11.45 - 12:45	Jedinstveni telefonski sistem Elektoprivrede Srbije - Jelena Bukelić i Bojana Pavlica, Saga i Ljiljana Čapalija, EPS	Cisco Storage Networking u virtualizovanim data centrima - Mladen Krivokuća, Pexim	Wireless security u realnom okruženju - Goran Josivljević, Siemens	Dizajn i implementacija digitalnog Headenda u KDS d.o.o, Novi Sad - Marko Radović, NIL
12.45 - 13.45	Primena DMVPN tehnologije u zaštiti komunikacije kroz javnu MPLS VPN mrežu- Marko Tanasković, MDS	IP TouchCall - Cisco based dispatcher solution of next generation networks - Tomass Mullet, TTC i Nenad Dimitrijević, Telefonija	DOCSIS 3.0 - Vežite se, polećemo! - Miodrag Radulović i Nemanja Potić, ComuTel	Cisco Wireless Mesh u realnom okruženju - Ivan Jovanović i Nenad Arsenijević, Konsing
13.45 -14.30	Ručak			
14.30 - 15.30	Email Security Appliance, Hrvoje Dogan	Cisco WebEx rešenja za poslovnu kolaboraciju, Slobodan Ivanović	Internet Peering za service providere - Dizajn sesija, Josef Ungerman*	Cisco Digital Headend rešenje, Bojan Nedelčev
15.30 - 16.30	Implementacija Web Security Appliance-a, Petr Ruzicka*	Prenos videa u mrežama poslovnih korisnika - Dizajn sesija, Tatjana Bošković	Cisco IP RAN arhitektura, Peter Gaspar*	Video transport preko IP, Marko Vukadinović
16.30 - 17.00	Svečana ceremonija zatvaranja			

* Prezentacija na engleskom

Cisco Expo 2009

Новости из области сигурности рачунарских мрежа

Татјана Бошковић, Систем инжењер

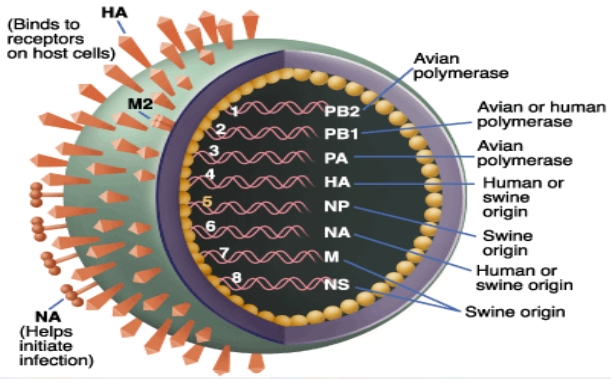
tboskovi@cisco.com

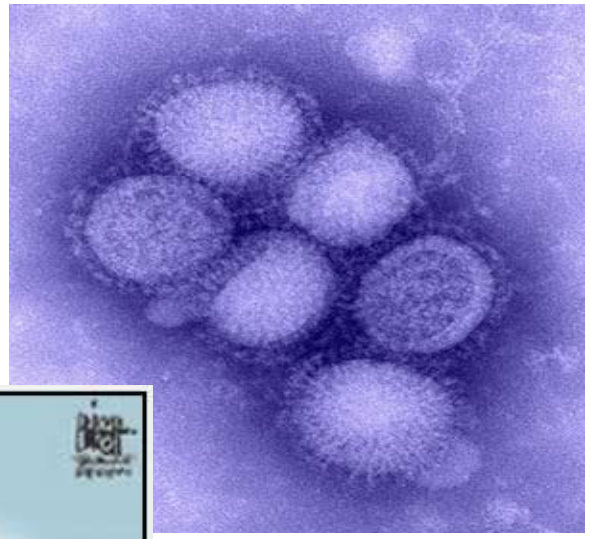
Агенда

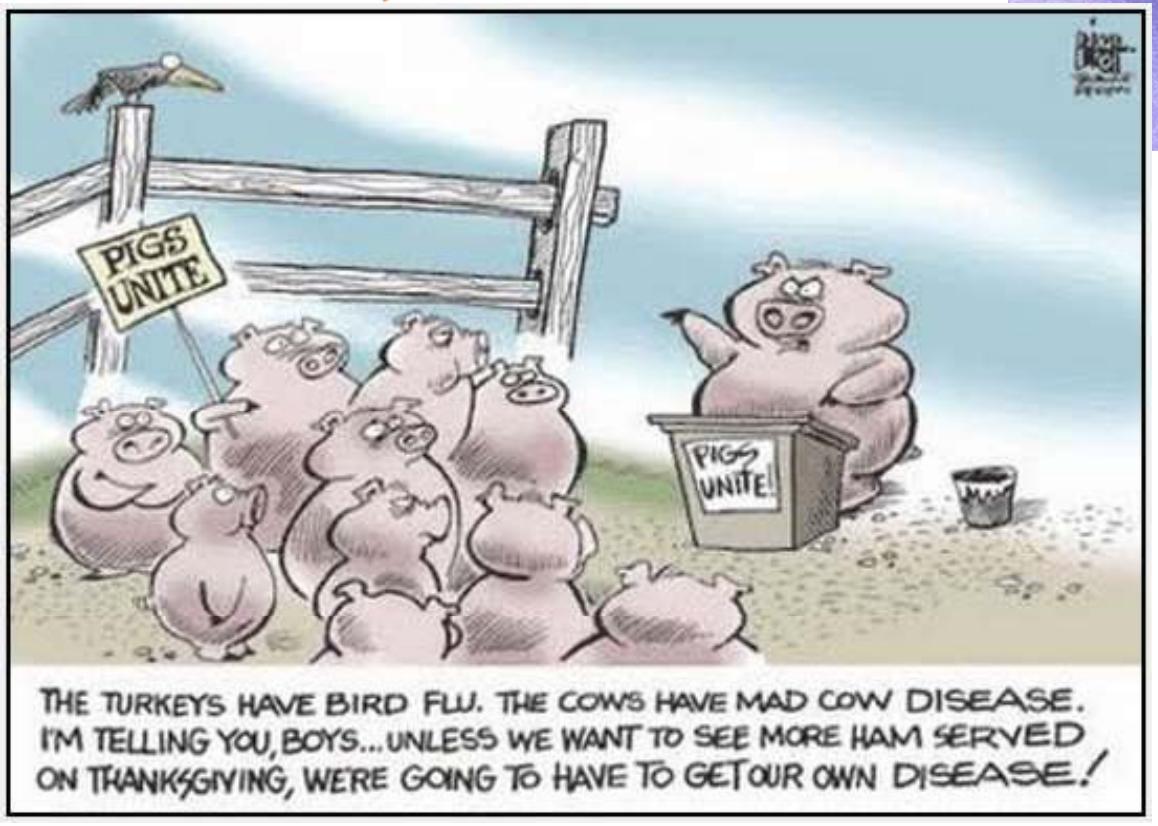
1. ASA 8.2 новости
2. IPS *Global correlation*
3. ACS 5.0
4. NAC новости
5. CSM и MARS - новости
6. Питања и одговори
7. Ручак ☺

ASA 8.2 новости

Ботнет мреже – H1N1 грип за рачунарске мреже?



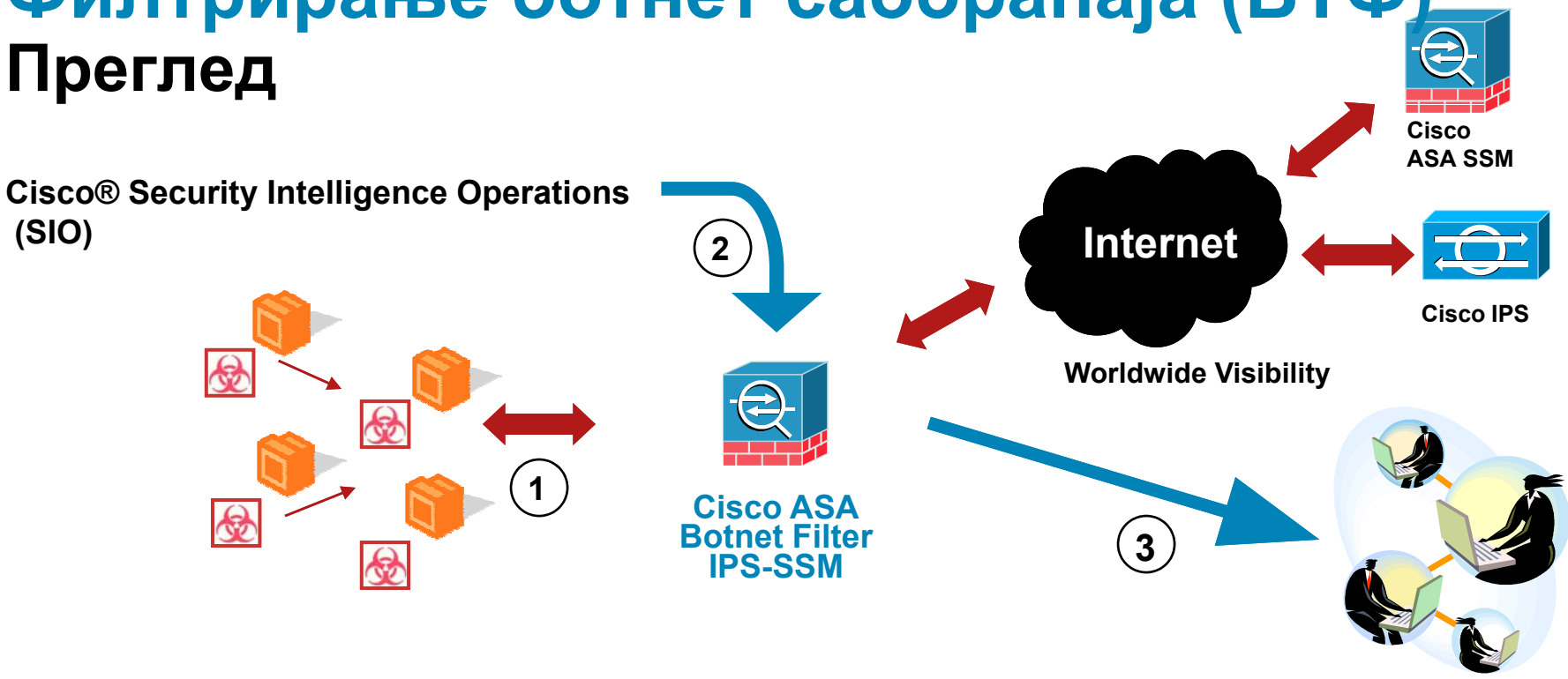




- Ботнети = мрежа компромитованих рачунара
- Напади су од типа спама и ДоС напада па све до напада на веб сајтове у циљу профита и уништавања конкурентске мреже

Филтрирање ботнет саобраћаја (БТФ)

Преглед



Корак 1:

Сумњив саобраћај од клијената покушава да успостави везу споља ка лошим сајтовима

Корак 2:

Cisco SIO освежи Cisco ASA ботнет филтер базу података; дестинација је познат сумњив сајт

Корак 3:

Аларми се шаљу до тимова који се баве спречавањем, санацијом и оздрављењем

Филтрирање ботнет саобраћаја (БТФ) Преглед

- Користи Иронпорт технологију да идентификује потенцијални лош саобраћај
- Надгледа *phone-home* активност између унутрашњости и спољашњости корпоративне мреже
- Подржан у свим начинима рада: самостални, више-контексни, транспарентни и рутирани начин рада
- Постоји око 5-10% пада перформанси (доста зависи од величине DNSRC)
- Користити ову функцију само на интерфејсима ASA које су директно на Интернету
- Функционалност филтрирања ботнет саобраћаја се састоји из 3 главна дела:
  - Динамички и администраториски подаци на црној листи
  - Класификација саобраћаја и извештај
  - *DNS Snooping*

Филтрирање ботнет саобраћаја (БТФ)

Класификација саобраћаја

Класификуј саобраћај који подлеже БТФ-у

- Активирај специфичне мреже, интерфејсе или саобраћај који подлеже филтрирању ботнет саобраћаја
- Активирај интерфејс који је окренут Интернету

Категорије података за БТФ

- Црне листе: Познати *malware* сајтови
- Беле листе: Познате дозвољене адресе
- Сиве листе: двозначне адресе
- Непознате: Непозант и није ни на једној листи.

БТФ типови података

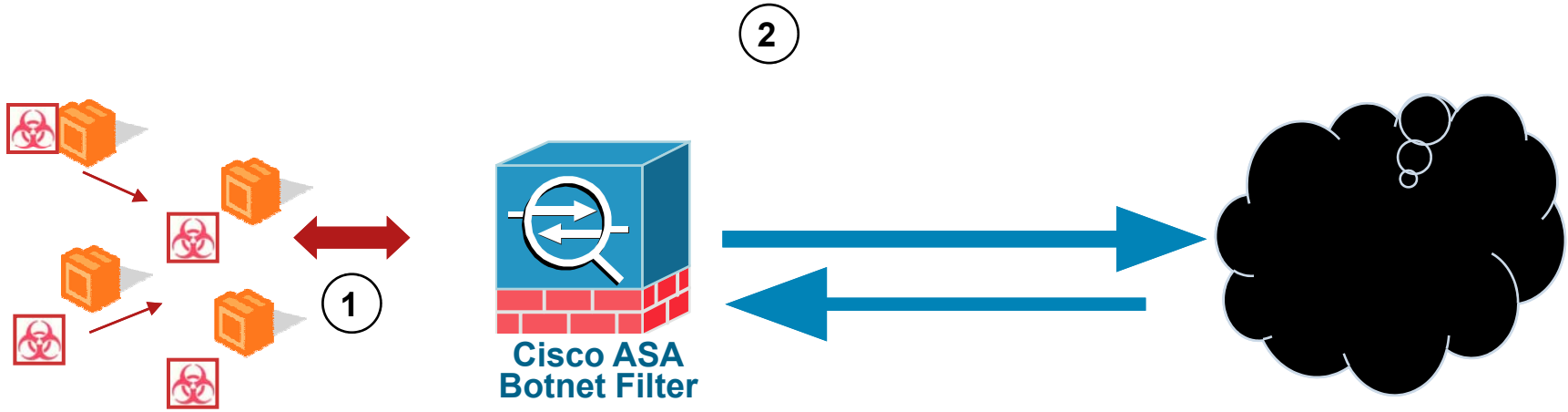
- Динамички : подаци скинути са CSIO
- Статички: подаци дефинисани од стране администатора који се баве сигурношћу мрежа

Напомена: БТФ база података не садржи атрибуте репутације

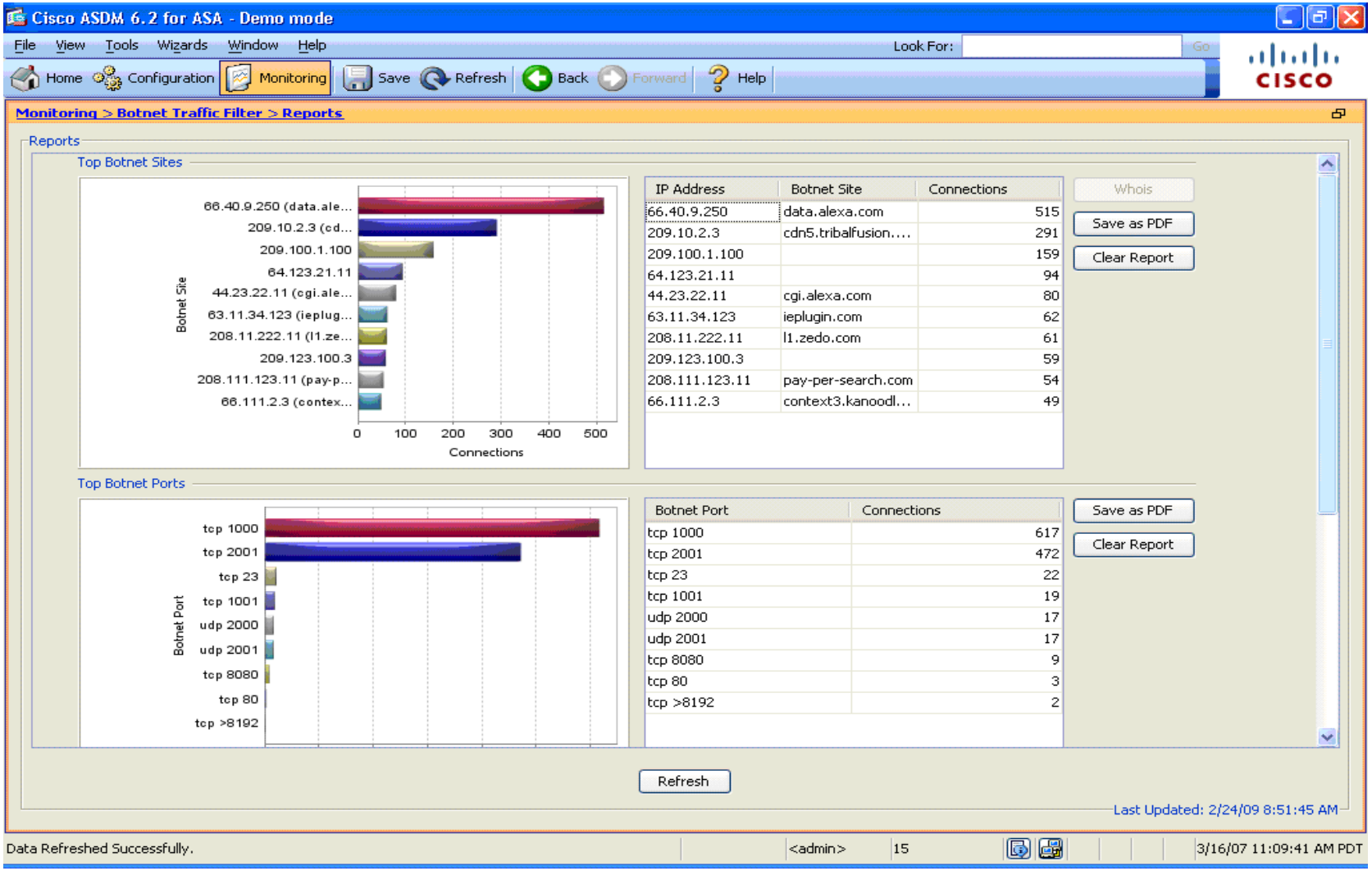
Филтрирање ботнет саобраћаја (БТФ)

Кораци за освежавање базе

1. Омогућити БТФ освежавање клијента
2. Сачекати 2 минута пре него се започне иницијални *download*
3. Контактирати сервер са кога се освежавање врши на https://update-manifests.ironport.com, почетна база података је ‘’скинута’’
4. Подесити ново време за пулинг
5. Покушај да се download-ујy нове информације освежене базе на 60-минутном интервалу
6. Освежи и потврди нове податке и учитај у меморију ако нови подаци постоје.



Извештај филтрирања ботнет саобраћаја
Најчешћи ботнет сајтови и портови



ASA VPN новости

Преглед

Enterprise class licensing

Usability

Security

Електронска испорука лиценци
(е-испорука)

HAPPY CUSTOMERS

GREEN

SAVE MONEY

HOW TO ORDER

Ново ASA VPN Лиценцирање

1. Флекс VPN Лиценца
   Пандемијска временски ограничена привремена лиценца

Ново

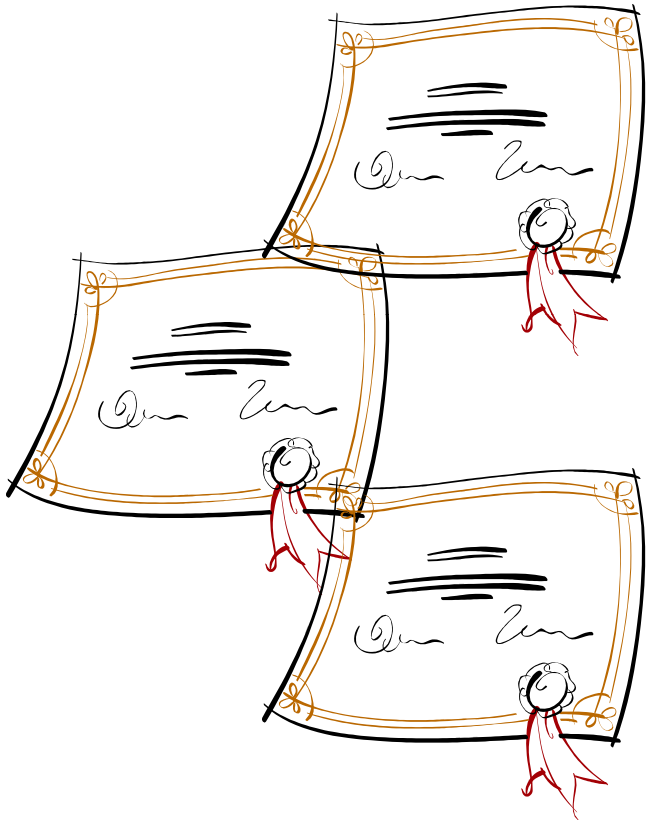
2. Мобилна VPN Лиценца
   Активира *Mobile VPN AnyConnect*

Ново

3. AnyConnect Essential
   Осиромашена AnyConnect Премиум лиценца. Нема лимита у капацитету

Ново

4. Дељена лиценца
   Пул лиценци које се деле између учесника



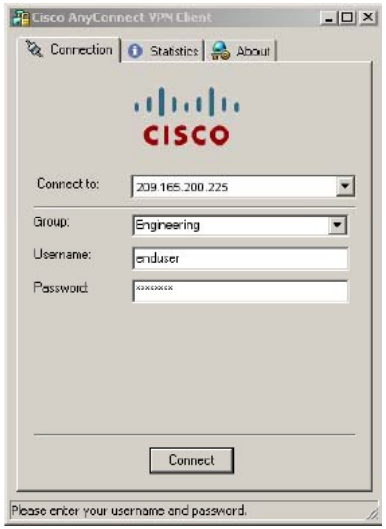
AnyConnect Побољшања

AnyConnect Essentials

AnyConnect Essentials

Могућ аутоматски даунлоад

- Приступ било којој апликацији или ресурсу
- Аутоматско освежавање
- Рубусан, неосетна веза
- Оптимизован за мобилне кориснике
- IPv4/IPv6 приступ мрежи
- Прилагођен гласу
- **Захтева ASA 8.2+**



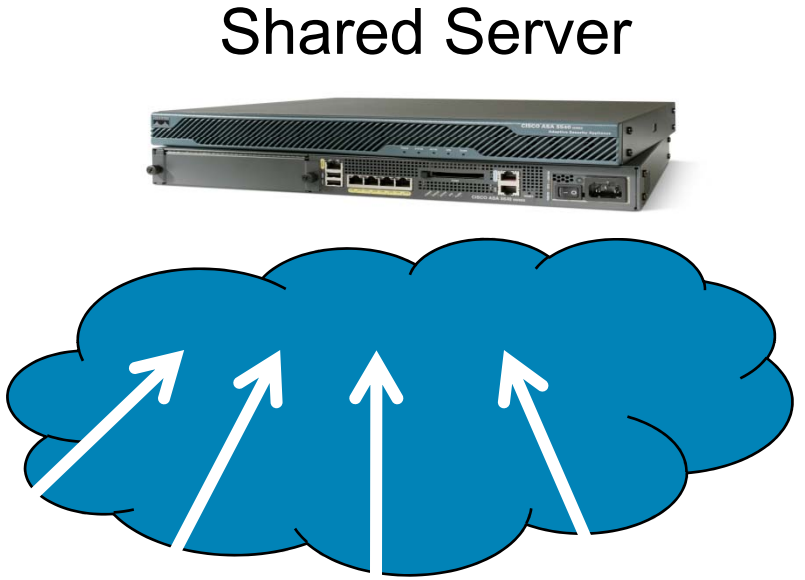
AnyConnect Premium

- Подршка за SSL приступ без клијента
- Cisco Сигурни Десктоп који омогућава сигуран приступ са неконтролисаних крајњих тачака
- Cisco Сигурни Десктоп *HostScan* функција за проверу стања у фази пре успоставе везе

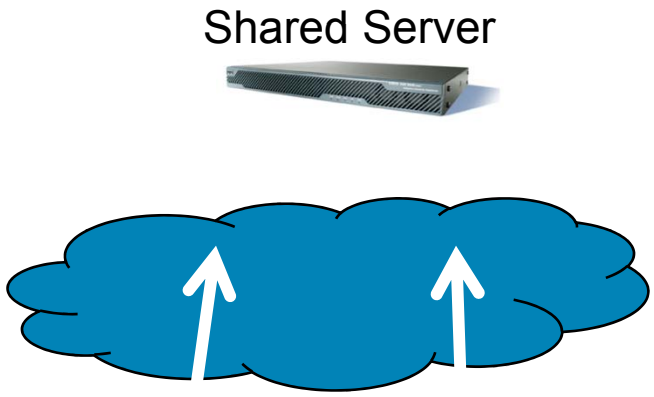
Essentials је природан пут миграције са Cisco VPN Client
Нове платформе захтевају AnyConnect.
Нема подршке за нове оперативне системе/платформе за Cisco VPN Client (укључујући x64, Windows 7, Mac OS X 10.6)

Шта је дељена лиценца?

- Дели сесије према потреби са осталим учесницима
- Компоненте укључују: Сервер, бекап сервер и Учеснике.
- Нема подршке за 5505



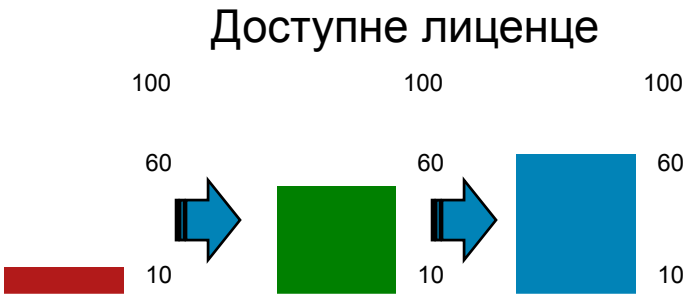
Механизам дељене лиценце



Shared backup Server/ participant

participant

- Сви учесници треба да се успешно региструју на сервер
- Кад број слободних лиценци падне испод 10, тражиће 50 нових лиценци
- Кад број расположивих лиценци достигне 60 и преко, ослободиће дељене лиценце
- Сервер надгледа коришћење лиценци и дели њихов статус са бекап сервером
- Подесив интервал комуникације (10-300 секунди)



Тражи 50

Ослобађа 50

Cisco AnyConnect VPN Клијент 2.4

Преглед

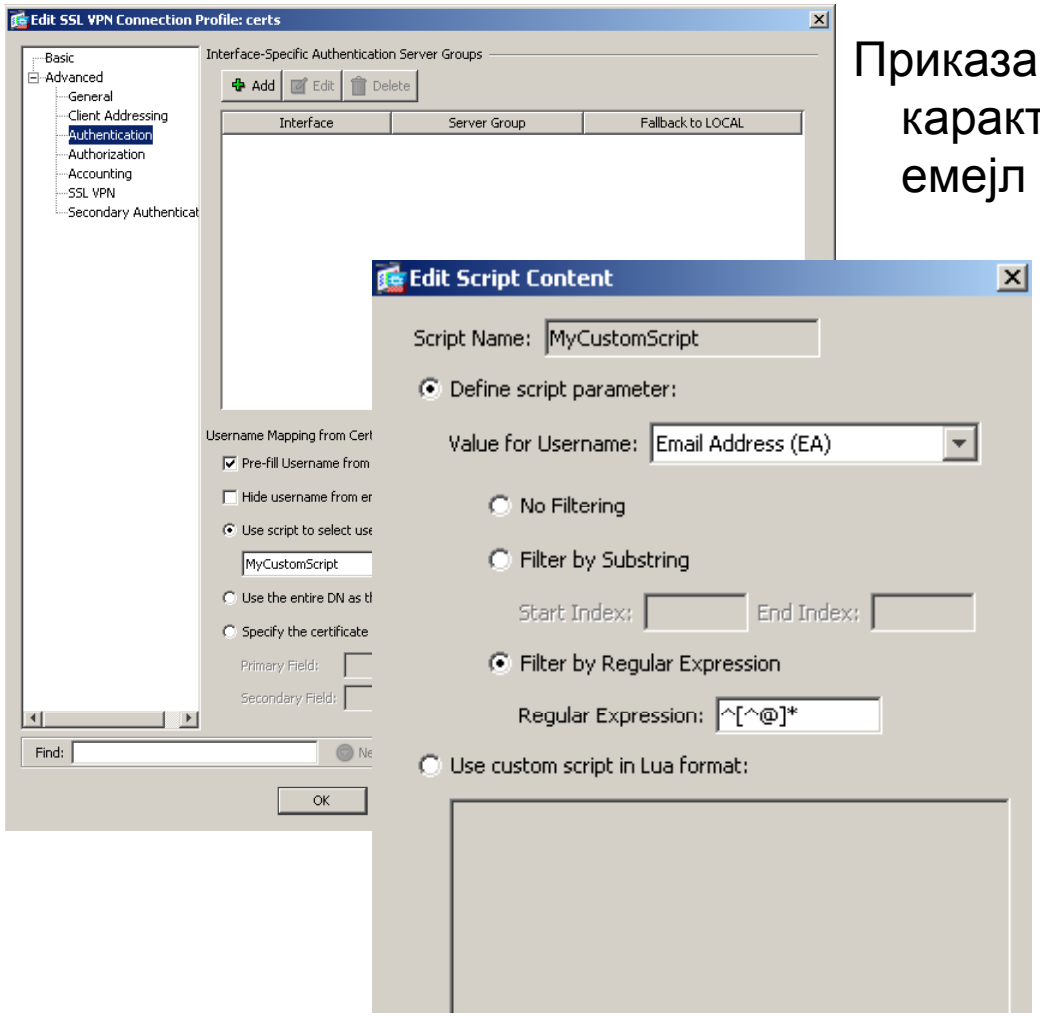
New OS Ready

Federal Enablement

Seamless and Simple VPN

Једноставно повезивање

Попуњено корисничко име из сертификата



Приказана скрипта ће вратити карактере пре @ знака у пољу емејл адресе

За “user@example.com” извучено корисничко име ће бити “user”

Може се такође специфицирати помоћни стринг за коришћење на почетку и на крају индекс карактера

Ако су опције за филтрирање неодговарајуће, могуће је написати прилагођени скрипт

Побољшање у имплементацији за фајервол

IPv6 адресирање за транспарентни фајервол

Обезбеђене нове функционалности за транспарентни фајервол

- Омогућава учешће у IPv6 рутирању
- Менаџмент адресе сада могу да буду IPv6
- Листе за право приступа сада могу да садрже IPv6 адресе

fdac:f83a:ec17:4d1e:xxxx:xxxx:xxxx:xxxx

vlan10

vlan11

fdac:f83a:ec17:4d1e:xxxx:xxxx:xxxx:xxxx

NetFlow логовање догађаја

Сада подржано на свим Cisco ASA платформама

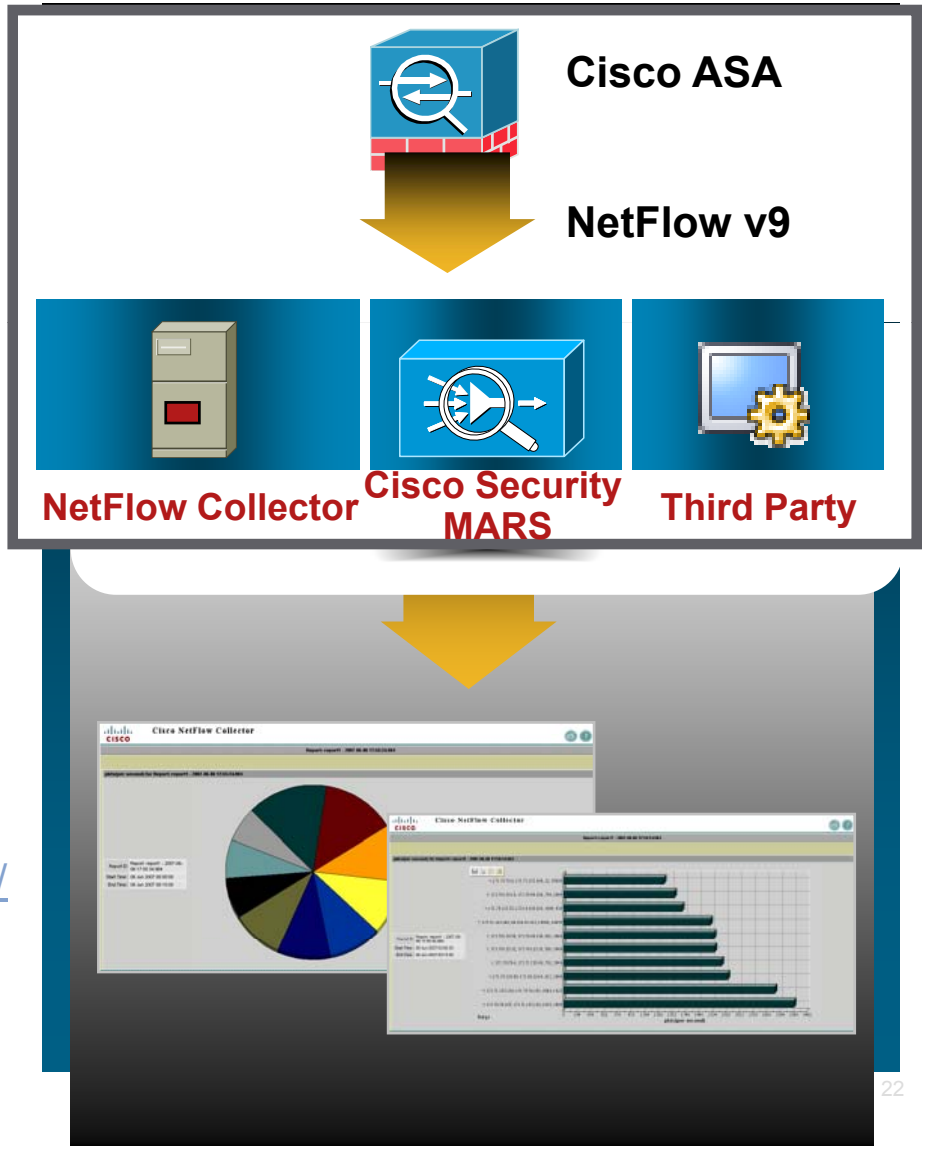
Корелација и смањивање обима сигурносних догађаја за мутигигабитни саобраћај

- Увођење NetFlow v9 могућности на све Cisco® ASA платформе
- Обезбеђује усклађеност са захтевима аудита

Записи засновани на догађајима:

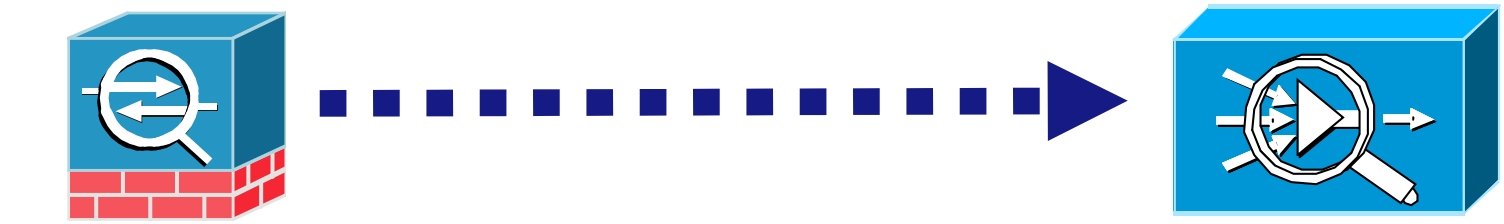
Токови генерисани на основу 3 статуса тока догађаја (стварање тока, заустављање и забрана), а не на основу временске активности тока саобраћаја.

- Потпуна листа поља подржаних NSEL:http://www.cisco.com/en/US/docs/security/asa/asa82/netflow/netflow.html



Netflow сигурносно логовање догађаја (NSEL)
Колектори

- Званични Cisco подржан NSEL колектор: MARS 6.0 и више
- Незванично подржани колектори: nfdump са NSEL модулом http://sourceforge.net/project/showfiles.php?group_id=119350
- Подршка за не-Cisco уређаје: Користити јавно доступно упутство за имплементацију http://www.cisco.com/en/US/docs/security/asa/asa82/netflow/netflow.html



ASA 5500 series

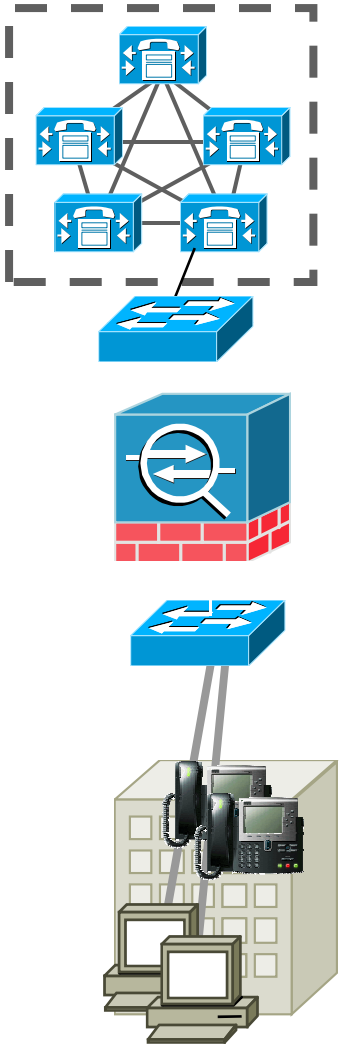
CS-MARS v6.0

Cisco ASA и скалабилност сигурних обједињених комуникација

SIP/SCCP Инспекција

- Опсежно тестирање перформанси са Cisco Communication Manager-ом
- Који фајервол ми је потребан?

Фајервол	Телефони
ASA 5505	Позиционира се за мала предузећа, радника на даљину
ASA 5510	Позиционира се за мала предузећа
ASA 5520	500-5,000 телефона
ASA 5540	5000-15,000 телефона
ASA 5550	15,000-30000 телефона
ASA 5580-20	30000-60000 телефона
ASA 5580--40	60000 – 130000 телефона



- Бројеви подразумевају:
  - Крајње тачке су SIP или SCCP
  - Nat конфигурација се користи
  - CPU испод 60% да заштити од џитера и кашњења
  - Подразумева 10% активних позива (пример – ASA 5550 подржава 3000 позива)
  - G.711 ulaw кодек

Cisco ASA и скалабилност сигурних обједињених комуникација

Максимални број UC Proxy сесија

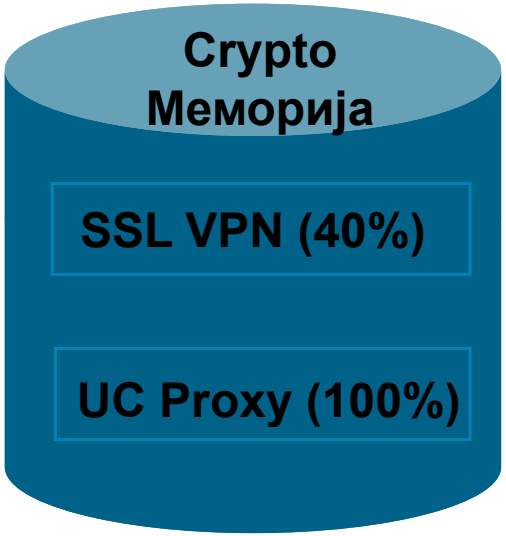
	UC Proxy сесије*	Доступност у софтверској верзији
ASA 5505	24	ASA 8.0.4
ASA 5510	100	ASA 8.0.4
ASA 5520	1000	ASA 8.0.4
ASA 5540	2000	ASA 8.0.4
ASA 5550	3000	ASA 8.0.4
ASA 5580	10,000 за TLS Proxy, Mobility Proxy, Presence Federation Proxy 5,000 за Phone Proxy	ASA 8.2(1)

***Proxy сесије = број регистрованих телефона**

Подржани број активних позива: 10% броја максималних сесија за позиве између телефона унутра и споља, а 30% за позиве између телефона споља

Cisco ASA и скалабилност сигурних обједињених комуникација

Комбиновање UC Proxy и SSL VPN



- **UC Proxy и SSL VPN користе исти скуп crypto меморијских ресурса**

  1 UC Proxy сесија ~ 2.5 SSL VPN сесија

- **Пример: ASA 5520**

  Корисник жели да имплементира 800 UC Proxy сесија

  Колико SSL VPN корисника може да буде?

Максимални UC Proxy капацитет на 5520	1000 сесија
Максимални број UC Proxy коришћених сесија	800 сесија
Преостали капацитет	200 сесија
Кад се ово преведе у SSL VPN сесије	200 * 2.5 = 500 SSL VPN

Повећање меморије

- ASA 5510 и 5505 долазе са предефинисаном DRAM меморијом од 256MB
- Сада је за ASA 5510 доступан *upgrade* меморије

Product Number	Product Description	List Price	Availability
ASA5510-MEM-512=	512 MB Memory for Cisco ASA 5510	USD $500	Now

- Када се препоручује повећање меморије?
  - Када се активира детекција напада путем скенирања

    http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/protect.html#wp1072953
  - За кориснике који разматрају прелаз на 8.2

    Ако је текућа “show mem” мања од 20%

    http://www.cisco.com/en/US/customer/docs/security/asa/asa82/release/notes/asarn82.html#wp37821

Cisco ASA 8.2 преглед

Фајервол и IPS

- Филтрирање ботнет саобраћаја
- Cisco® IPS SSC на Cisco ASA 5505
- IPV6 адресирање за транспарентни фајервол
- *Multicast group NAT*
- Cisco ASA подршка за Cisco IPS 6.2 и IPv6 саобраћај
- VLAN скалирање до 250 на Cisco ASA 5580
- TCP *state bypass*
- Unified communications proxy на Cisco ASA 5580
- H.239 подршка
- NAT за phone proxy media завршавање адреса

Удаљени приступ

- Дељене лиценце
- Cisco AnyConnect Essentials
- Попуњено корисничко име из сертификата
- Двострука аутентификација
- Ауторитет за сертификате по групи
- Cisco Secure Desktop по групи
- Web Microsoft SharePoint 2007 подршка
- Extended key usage (EKU) тунел група

Надгледање

- Cisco ASDM јавни сервер конфигурациони тоол
- Cisco ASDM подршка за једновремену лозинку за AAA
- SNMPv3
- Cisco ASDM подршка за кустомизацију Cisco Secure Desktop
- NetFlow логовање сигурносних догађаја на свим Cisco ASA моделима
- Cisco Security Manager и Monitoring, Analysis and Response System (MARS)

IPS Global correlation

Cisco Security Intelligence Operations

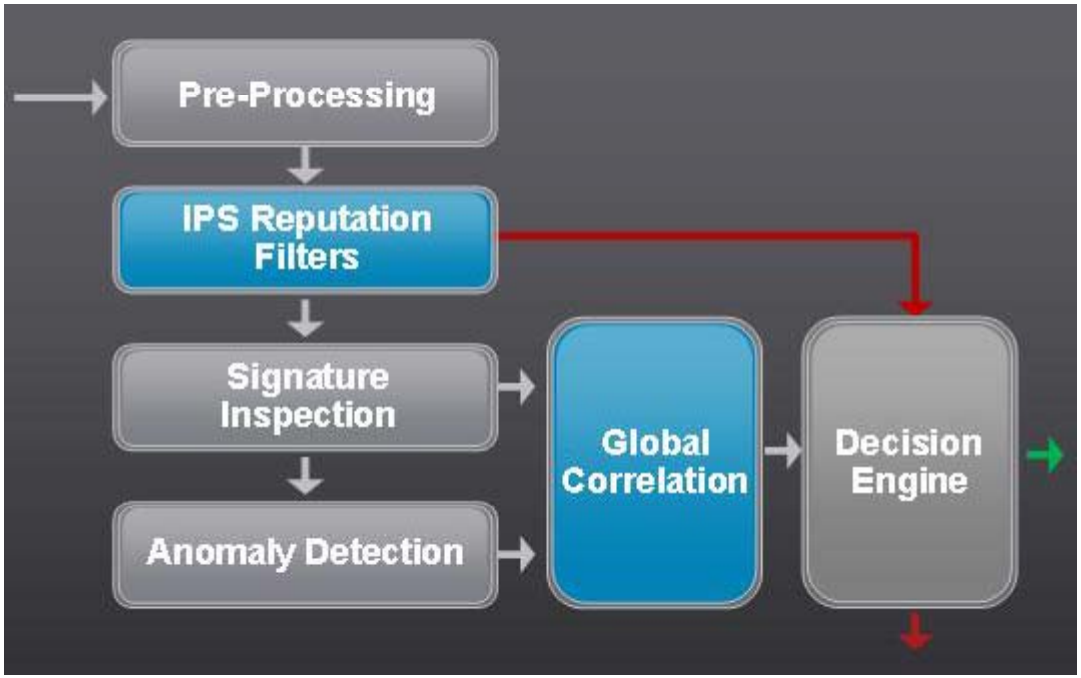
Сигурност на свакој локацији

Сигурност у сваком градивном елементу

Уређај | **Сигурносни модул** | ***Hybrid Hosted*** | **Сигурносни софтвер**

Пут пакета у IPS 7.0

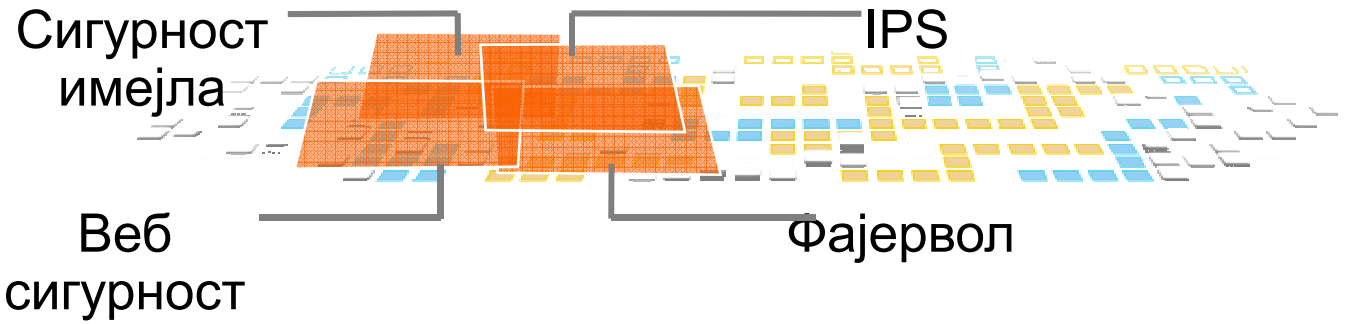
- IPS репутациони филтери блокирају приступ IP адресама које су на ‘зомби’ мрежама или мрежама које су потпуно контролисане од злонамерних организација



- Инспекција помоћу глобалне корелације повећава Risk Rating догађаја када нападач има негативну репутацију допуштајући тим догађајима да буду блокирани са већом сигурношћу и много чешће него догађај који нема негативну репутацију.

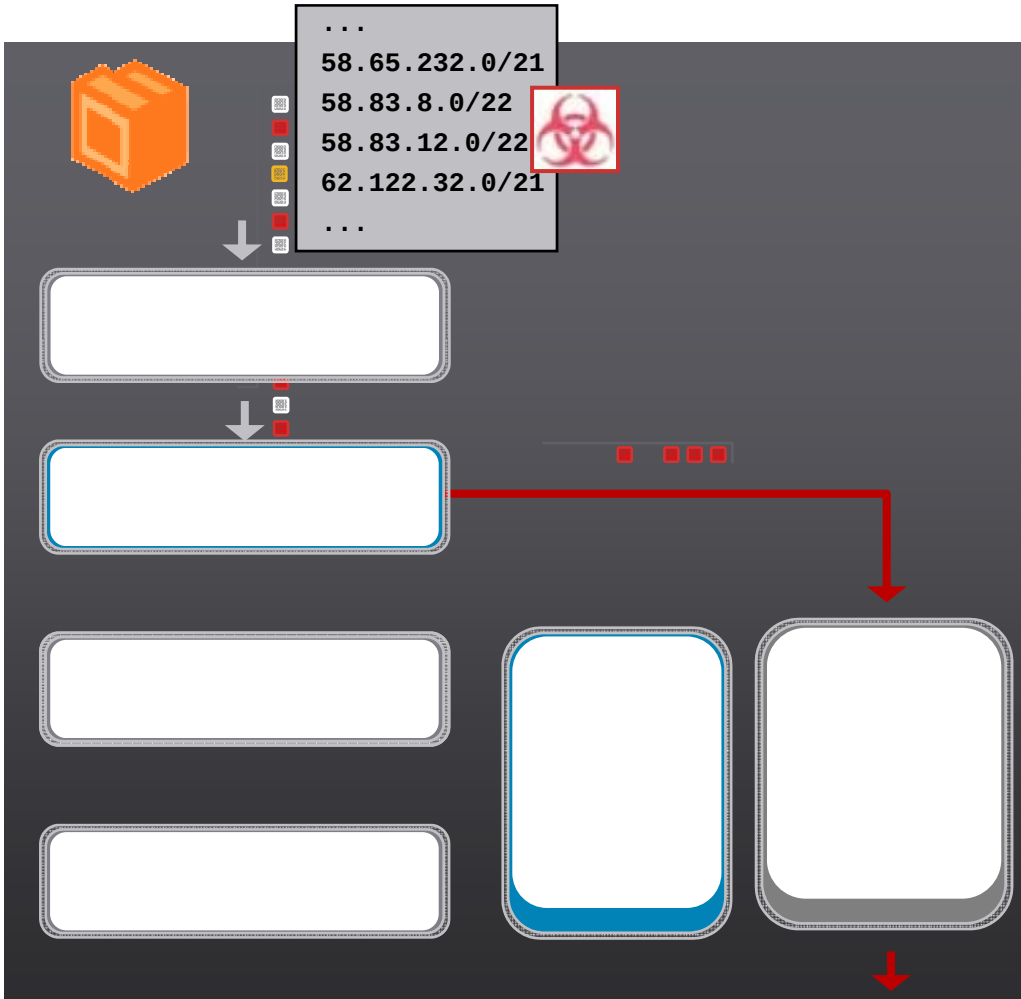
Шта је репутација?

Или “Јесу ли све репутације исте?”



- Репутација је историја активности и квалитета специфичне IP адресе или мреже. Она се рачуна користећи неколико стотина различитих типова података који се налазе у Сензорбази.
- За различите типове уређаја, различити параметри значе више или мање за саму репутацију уређаја
  - СПАМ је веома релевантан за имејл репутацију уређаја а мање за IPS сензор

IPS репутациони филтери:
Блокирање најгорих из скупа ‘лоших јабука’



- Репутациони филтер блокира приступ овим мрежама слично као листа за право приступа
- Појединачне IP адресе не иду на ову листу (Једна IP адреса не иде од -1 до -9 да би била на овој листи)

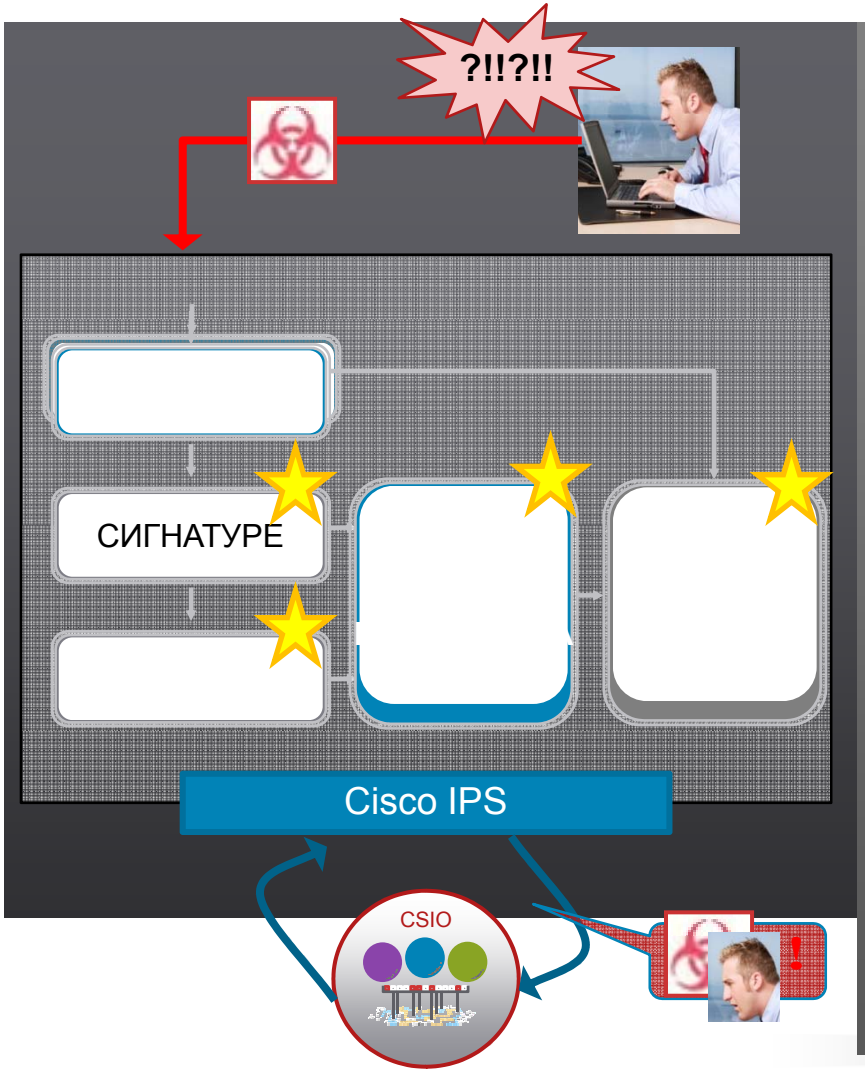
33

Локална провера је увек важна
Пример 1: Непознат нападач

1. Нови нападач ‘удари’ на IPS
2. Нападач нема репутацију
3. Сигнатуре или детекција аномалије идентификују неку активност
4. На напад ће се применити одговарајуће сигурносне полисе које су имплементиране на сензору (Одбиј уколико *Risk Rating* достигне праг)
5. Информације о нападачу се шаљу назад CSIO да би се пратила његова репутација (ако је конфигурисано)

Провера коришћењем глобалне корелације
Пример 2: Сумњив нападач

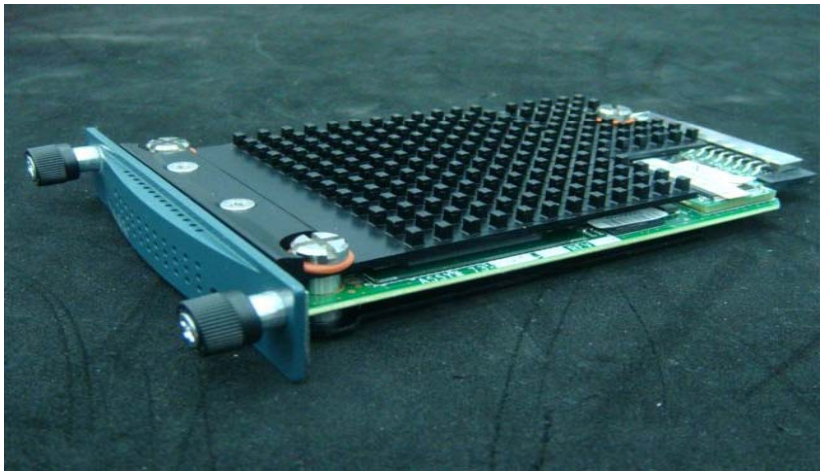
Идентификован кроз локалну проверу, забрањен кроз глобалну корелацију

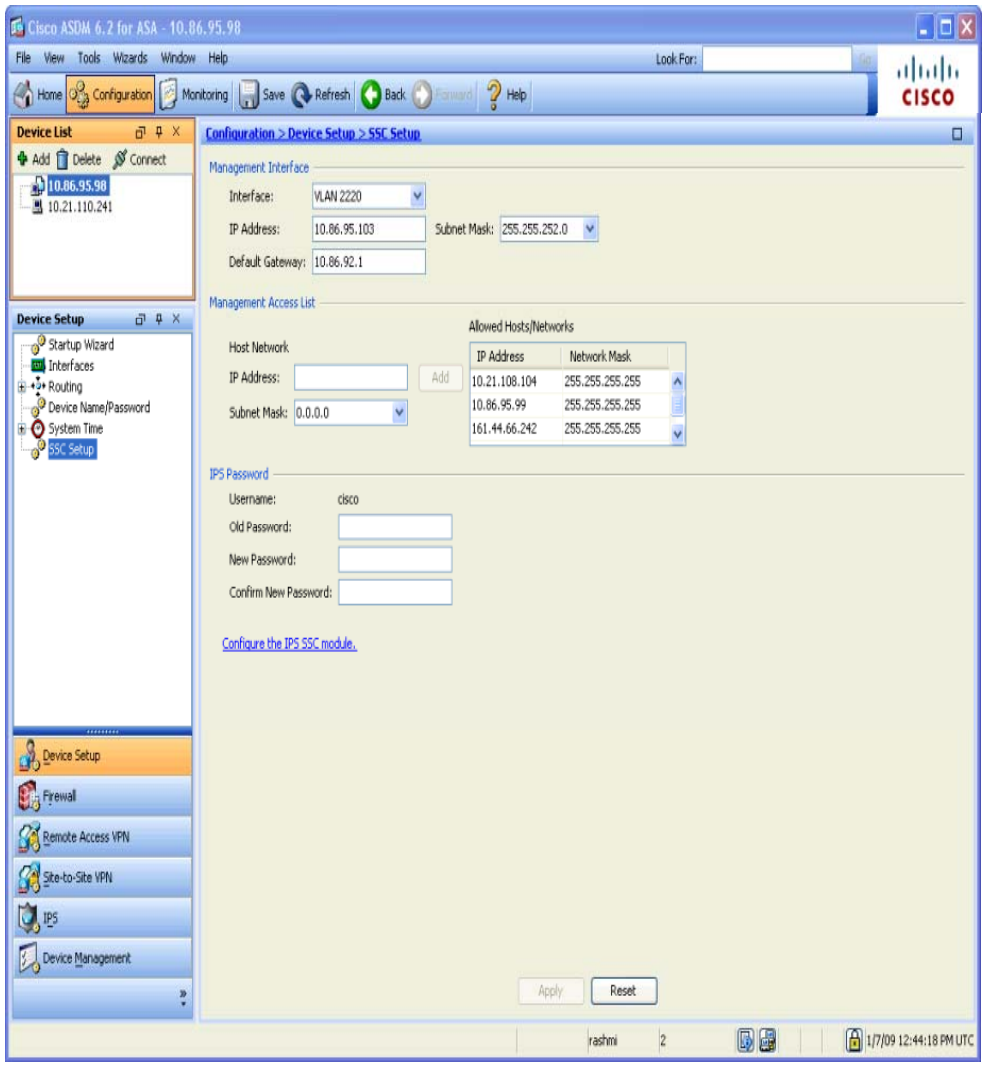


1. Сумњив нападач напада
2. Има средњу репутацију
3. Сигнатуре иденфитикују сумњиву активност и дају средњи Risk Rating
4. Глобална корелација дода и информацију о репутацији нападача на сам Risk Rating
5. Доносилац одлуке блокира
6. Информације о новој репутацији се шаљу назад CSIO.

IPS и Cisco ASA 5505

- Cisco® Secure Services Client (SSC) модул се у потпуности конфигурише кроз Cisco ASA 5505
- Њим се управља кроз backplane између Cisco ASA и SSC коришћењем екстерног свич порта на Cisco ASA
- Cisco ASDM може да се корсити да се конфигурише Cisco ASA SSM



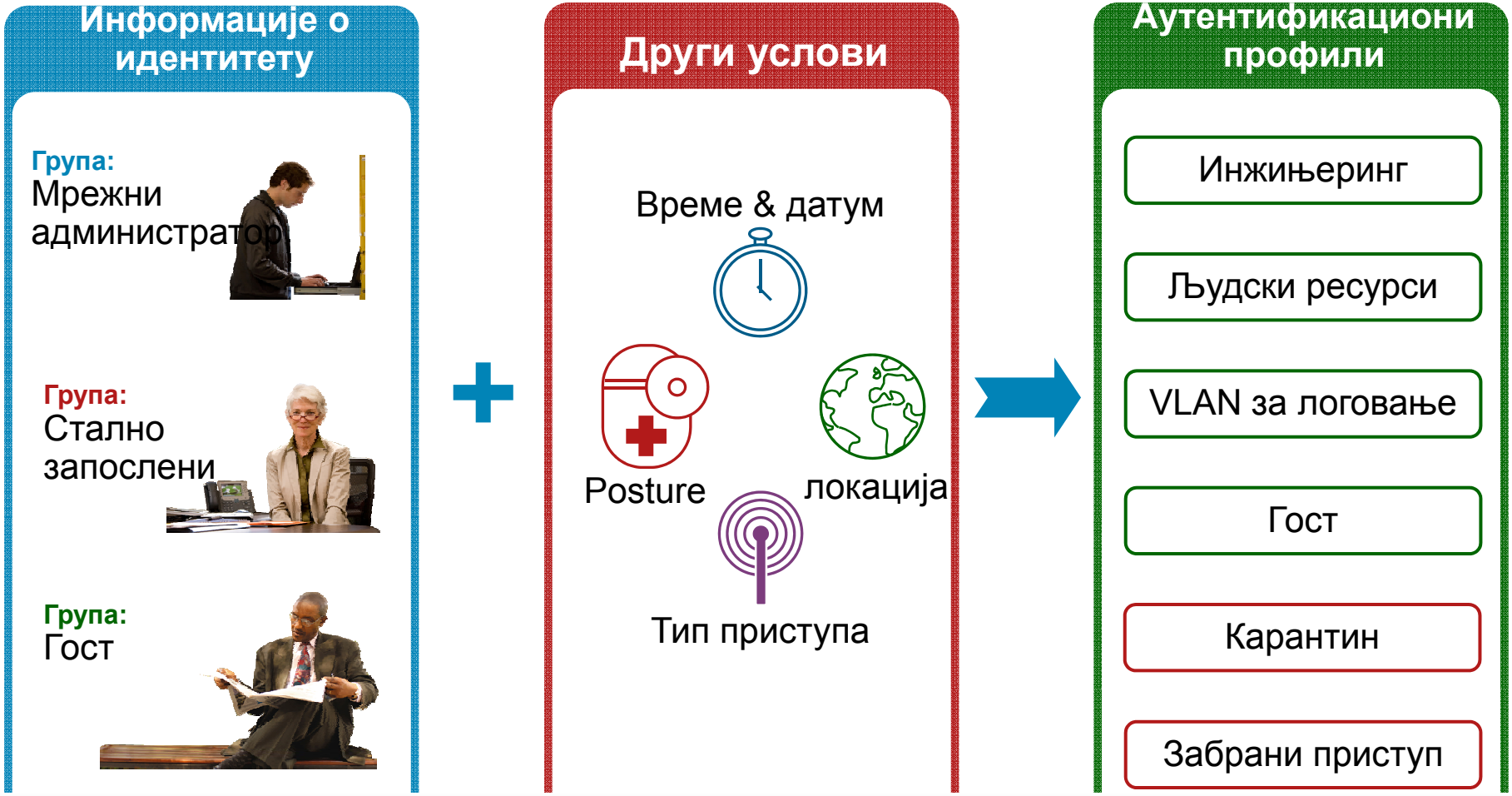


Cisco AIP SSC и AIP SSM упоредни приказ

Функција	Cisco® AIP SSC	Cisco AIP SSM-10/ 20/40
Максимални проток	75 Mbps	650 Mbps
Подржане платформе	Cisco ASA 5505	Cisco ASA 5510, 5520, и 5540
IPS инспекција	Потпуно подржано	Потпуно подржано
Anti-evasion	Потпуно подржано	Потпуно подржано
Стандардни IPS сет сигнатура	Потпуно подржано	Потпуно подржано
Risk rating	Потпуно подржано	Потпуно подржано
Глобална корелација	Није подржано	Потпуно подржано
Виртуелизација	Један виртуелни сензор	Потпуно подржано
Детекција аномалија	Није подржано	Да
Неугашене сигнатуре	Једно стандардне неугашене сигнатуре	Све
Направљене сигнатуре	Није подржано	Пхтпуно подржано
IP логовање	ограничено	Да

ACS 5.0

ACS 5: Полиса заснована на правилима



Ауторизација заснована на индентитету и садржају

Услови су специфицирани као правила - IF <услов> THEN <услов>

ACS 5 : Преглед модела полиса

Полиса
Група правила полисе у циљу достизања одлуке полисе

Правило полисе
Услов који се састоји од елемената полисе који даје резултат

Елемент полисе
Услов (време/датум, локација) или дозвола (ауторизациони профил)

Полиса идентитета
Дефинише складиште ID-ја

Полиса ауторизације
Додељује ауторизационе атрибуте за захтеве за приступ

Ауторизациони профил
Основни “садржалац дозвола" за мрежни приступ (VLANs, ACLs, URL редирект, итд.)

Shell Профил
Основни “садржалац дозвола" за администрацију уређаја (IOS ниво привилегија, време истека сесија, итд.)

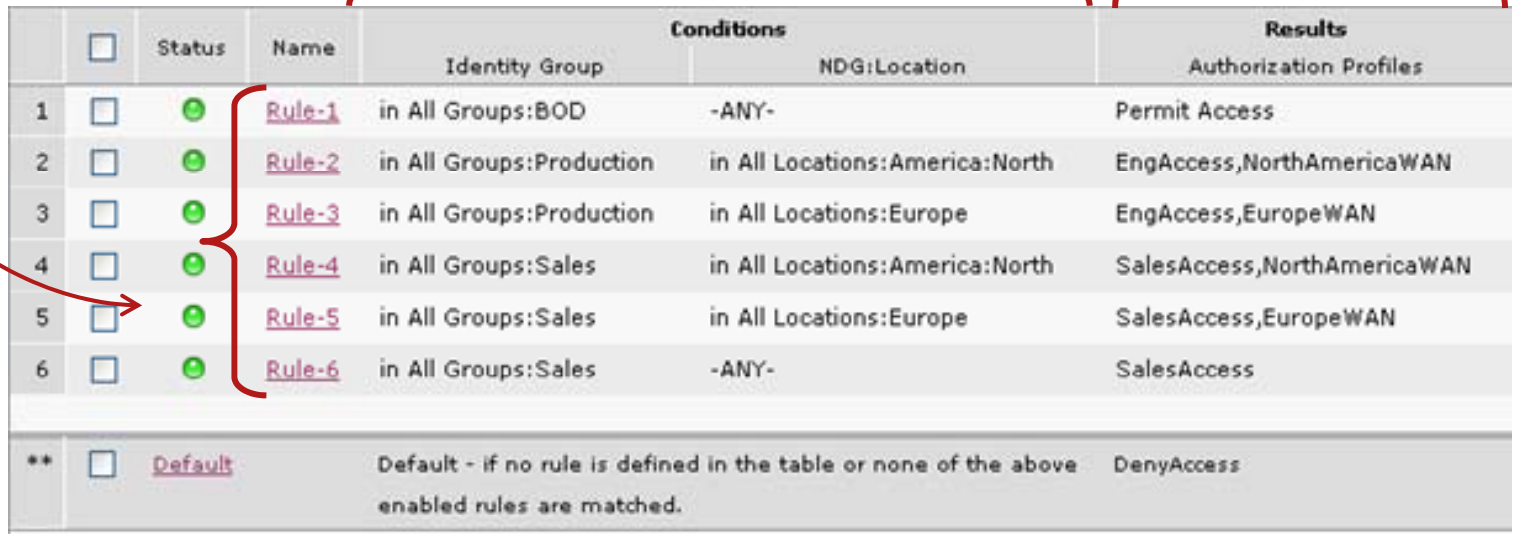
Захтеви за приступ
TACACS+, RADIUS захтев за приступ

Избор сервиса за приступ
Секвенцијални сет полиса који се користи за процесирање захтева за приступ

Резултати полисе
Дефинише дозволе засноване на правилима полисе: Ауторизациони профил за мрежни приступ; Shell профил за Администрацију уређаја

Табела полиса – структура

- Полиса је колекција правила који се процесирају секвенцијално
- Свако правило се састоји од услова и резултата
- Ако су услови у оквиру правила задовољени, резултати тог правила се примењују



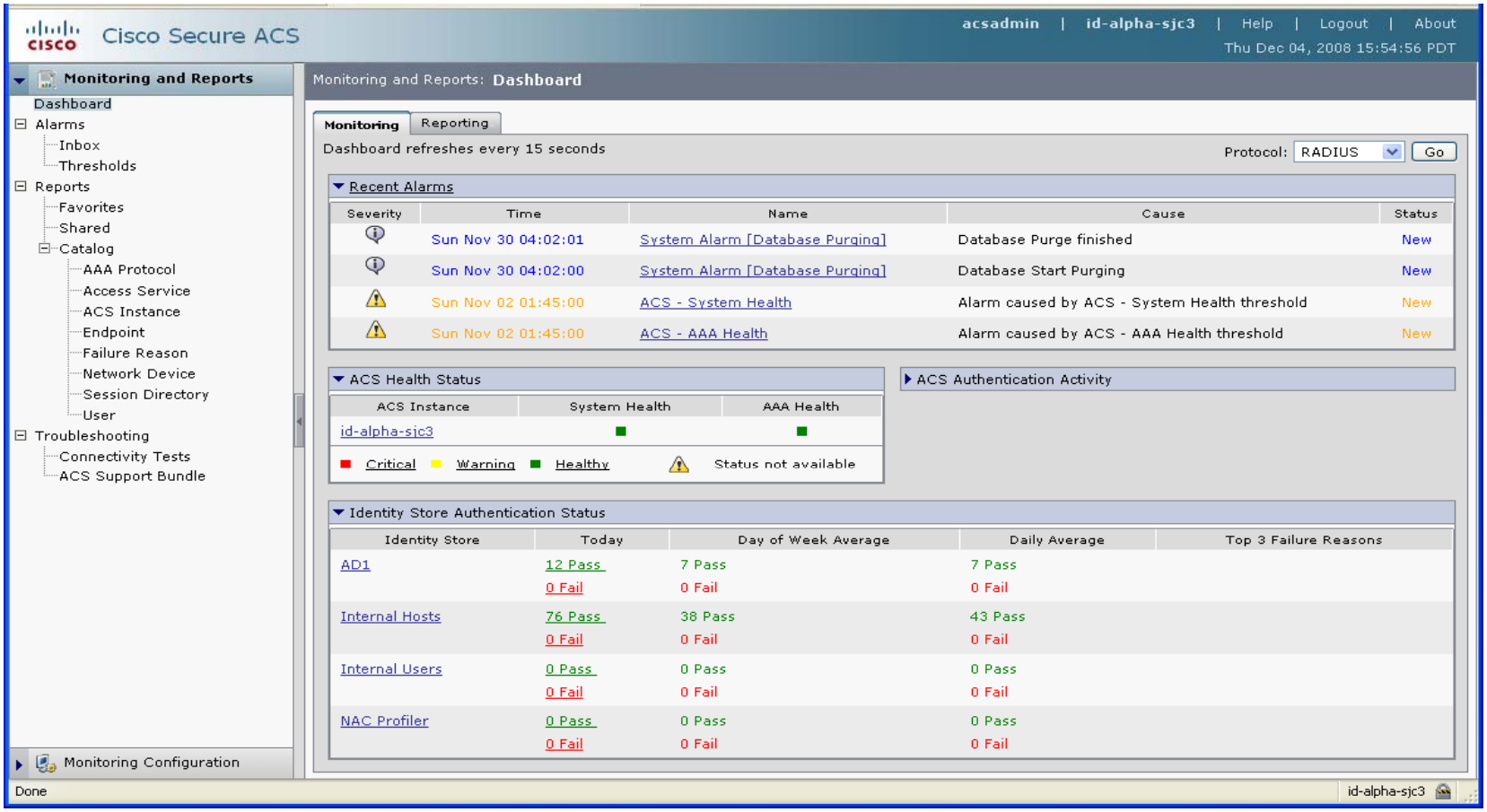
		Status	Name	Conditions		Results
				Identity Group	NDG:Location	Authorization Profiles
1	☐	●	Rule-1	in All Groups:BOD	-ANY-	Permit Access
2	☐	●	Rule-2	in All Groups:Production	in All Locations:America:North	EngAccess,NorthAmericaWAN
3	☐	●	Rule-3	in All Groups:Production	in All Locations:Europe	EngAccess,EuropeWAN
4	☐	●	Rule-4	in All Groups:Sales	in All Locations:America:North	SalesAccess,NorthAmericaWAN
5	☐	●	Rule-5	in All Groups:Sales	in All Locations:Europe	SalesAccess,EuropeWAN
6	☐	●	Rule-6	in All Groups:Sales	-ANY-	SalesAccess
**	☐		Default	Default - if no rule is defined in the table or none of the above enabled rules are matched.		DenyAccess

ACS 5.0 графички кориснички интерфејс

- Лак, сигуран, интуитиван и лак за коришћење веб заснован графички кориснички интерфејс
- Не захтева додатни клијентски софтвер за приступ графичком интерфејсу

ACS 5.0 Компоненте надгледања и извештавања

- Интегрисано напредно надгледање, извештавање и *troubleshooting* могућности за максималну контролу и транспарентност
  - КГИ лак за коришћење
  - флексибилни алати за презентовање



Надгледање и извештаји - преглед

Функције основне лиценце

- Табла
  - приказ система у реалном времену и AAA метрике исправности
- Извештаји
  - предефинисани & направљени извештаји
  - најчешће коришћени извештаји
  - Troubleshooting извештаји и алати
- Стандардни сториџ за чување логова података (1 месец)

Напредне фунције лиценце за надгледање и извештај

- Аларми
  - Дефинисати услове и лимите да би се генерисао аларм
  - Приказ аларма на табли за мониторинг
- Директориј сесије
  - Директориј свих сесија, приказ основних података (корисничко име, MAC адреса, IP адреса, идентификатор сесије, порт, одлука за полису, posture, итд).
  - AAA Accounting старт/стоп за сесију старт/стоп
- Алати за Troubleshooting
  - Тестови за конективност (ping/nslookup/traceroute) на било ком уређају
- Повећан сториџ за чување логова података (до 1 године)

Друге ACS 5.0 функционалност

- Напредне екстерне базе података и интеграција са сервером за полисе
  - – увођење спољњих (AD, LDAP) информација из полиса директно у правилима приступних полиса
  - – коришћење атрибута у условима или резултатима ауторизације
  - – проналажење података у реалном времену од екстерних сервера за полисе
- Дистрибуирани модел имплементације намењен великим
  - – један примарни и више секундарних сервера
  - – инкрементална репликација конфигурације
  - – централизован софтвер за *update*

ACS 5.0 опције за платформу

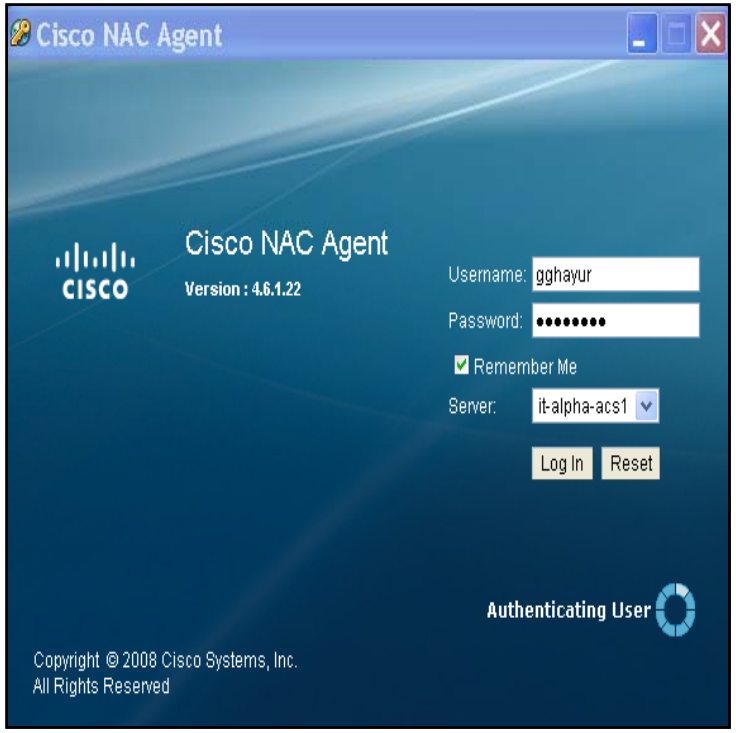
- Linux уређај
  - 1 рек-јединица, осигуран, уређај заснован на Linux-у
- VMWare верзија
  - софтверска апликација и имиџ за Linux оперативни систем за инсталацију VMware ESX 3.5

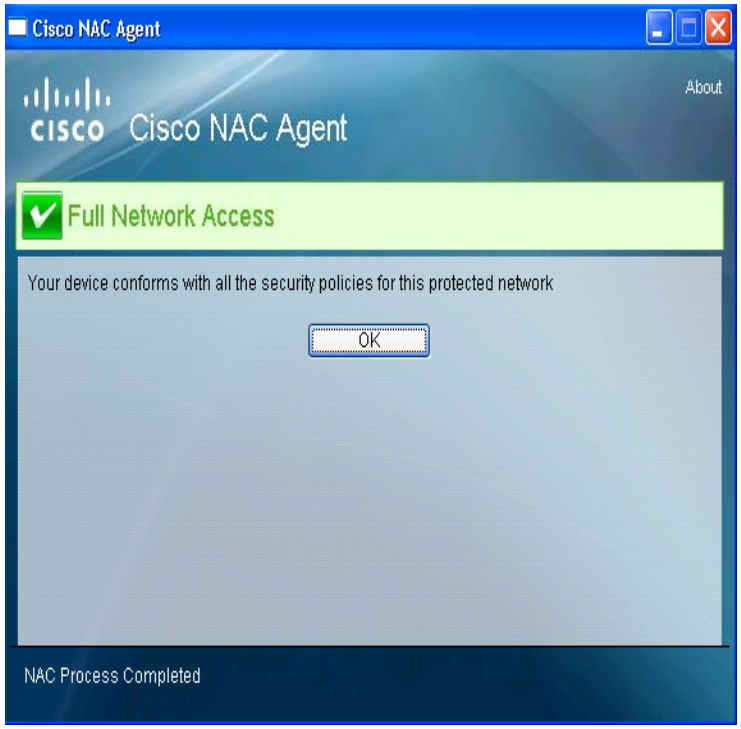
NAC новости

NAC Агент 4.6.1: Нови кориснички интерфејс

У складу је са новим Cisco правилима за кориснички интерфејс (CUES 6.0)

Локализација на више језика





NAC Агент

Инсталација и освежавање

- Администраторска права су неопходна да би се инсталирао нови агент
- Корисници са не-администраторским правима неће моћи да инсталирају агент преко CAS/CAM
- Корисници у великим предузећима треба да користе њихово Patch Менаџмент решење да дистрибуирају агент
- Када се нови агент 4.6 једном инсталира наредно освежавање верзије неће захтевати администраторске привилегије

Подржане платформе

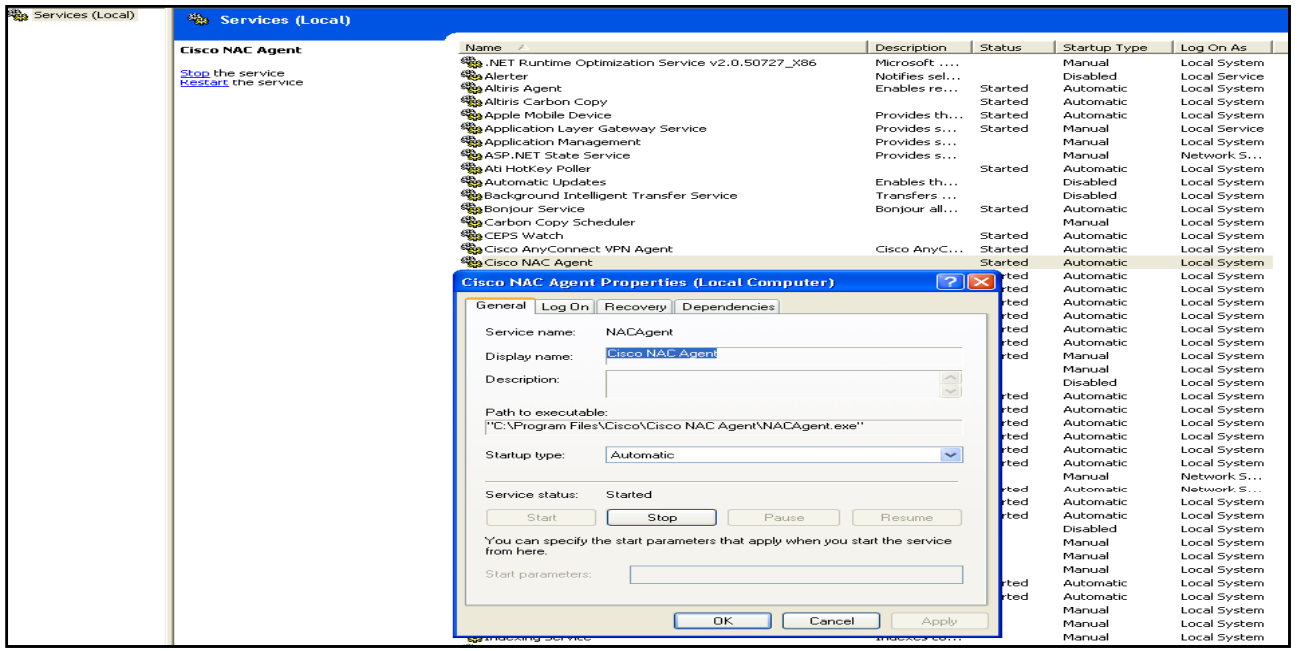
a) Windows XP (32 битни [SP2 и каснији] и 64 битни)

b) Windows Vista (32 битни и 64 битни)

c) Windows 2000 (SP4 и каснији)

Могућност управљања Агент сервисом са удаљене локације

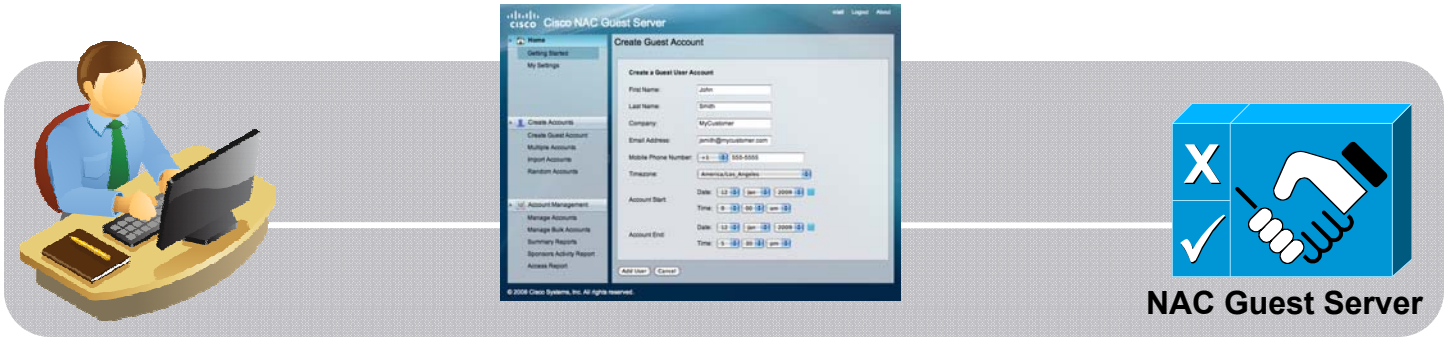
- 4.6.1 NAC агент има сервисну компоненту.
- Ово је кључно зарад контроле других старт-ап апликација у односу на NAC кроз будућа побољшања



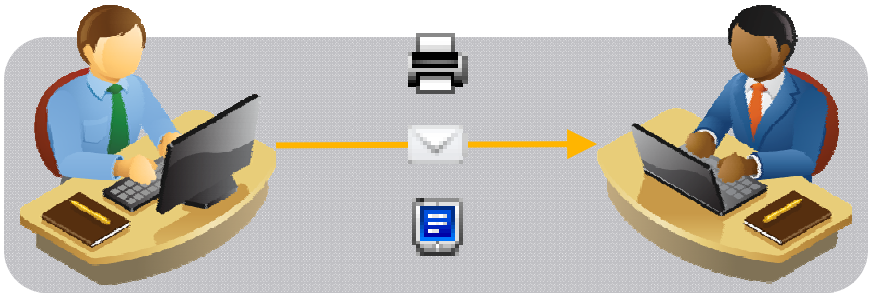
NAC 4.7.0 функције

- Нова хардверска платформа
- Подржана од 4.7.0 па на даље
- Стари модели: 3310, 3350, 3390
- Нови модели: 3315, 3355, 3395
- Цена се неће мењати
- Већи број корисника подржан на NAC серверима
- Постоји програм миграције на нову платформу

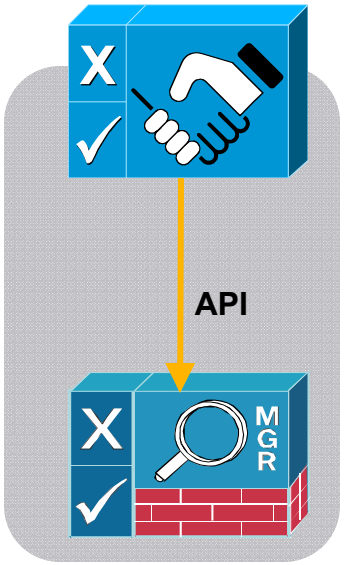
NAC Guest Сервер - приказ



1. Спонзор креира налог на NAC Guest серверу



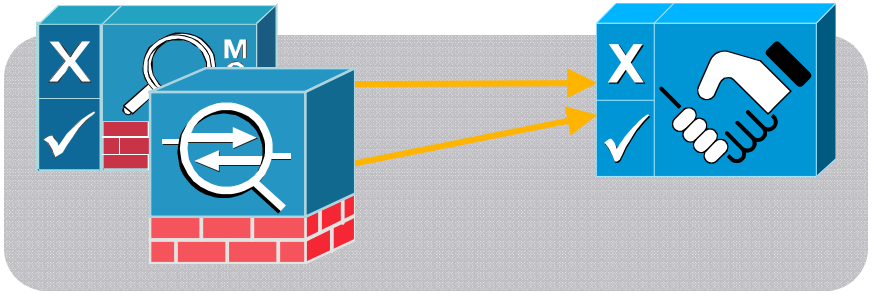
2. Спонзор даје права приступа госту кроз одштампани излистак, слањем имејла или смс-а



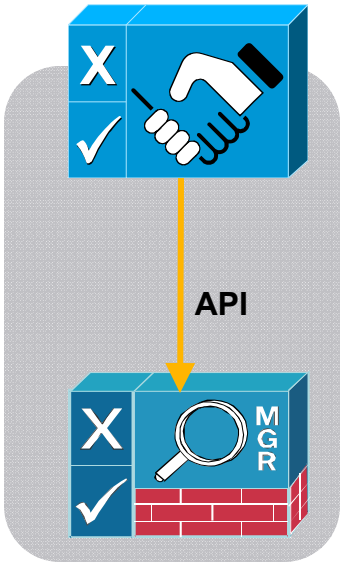
3. Када је налог активан NAC Guest сервер прави налог на NAC менаџеру

NAC Guest сервер - приказ

4. Гост се аутентификује кроз веб портал на NAC серверу и даје му се интернет приступ



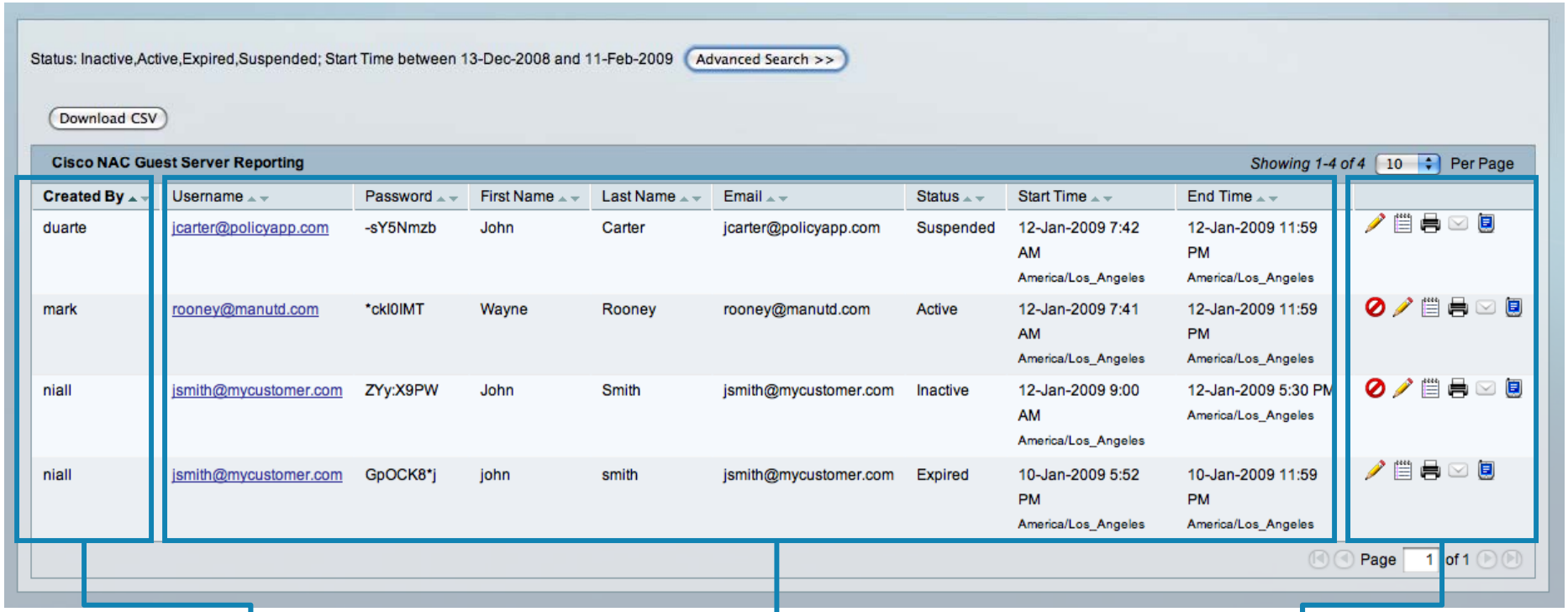
5. NAC и фајервол пружају аудит информације NAC Guest серверу



6. Када налог истекне NAC Guest Сервер уклања налог и искључује госта са мреже

NAC Guest сервер
Аудит и извештај

Преглед и менаџмент посетиоца

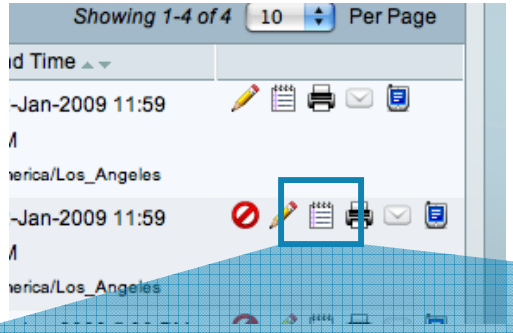


Информације о спонзору

Информације о посетиоцу

Управљање налозима

NAC Guest сервер
Детаљне аудит информације за посетиоца



- Када су се улоговали
- Где су се улоговали
- Адреса посетиоца

- Шта су радили
- Шта је било дозвољено
- Шта је било забрањено

Detailed Login Report for: jsmith@mycustomer.com *Showing 1-1 of 1* 10 Per Page

NAS IP Address	Users IP Address	Logged In	Logged Out	Duration
192.168.137.20	1.0.0.7	12:-Jan-2009 9:31 AM	12-Jan-2009 9:45 AM	14 Minute(s)

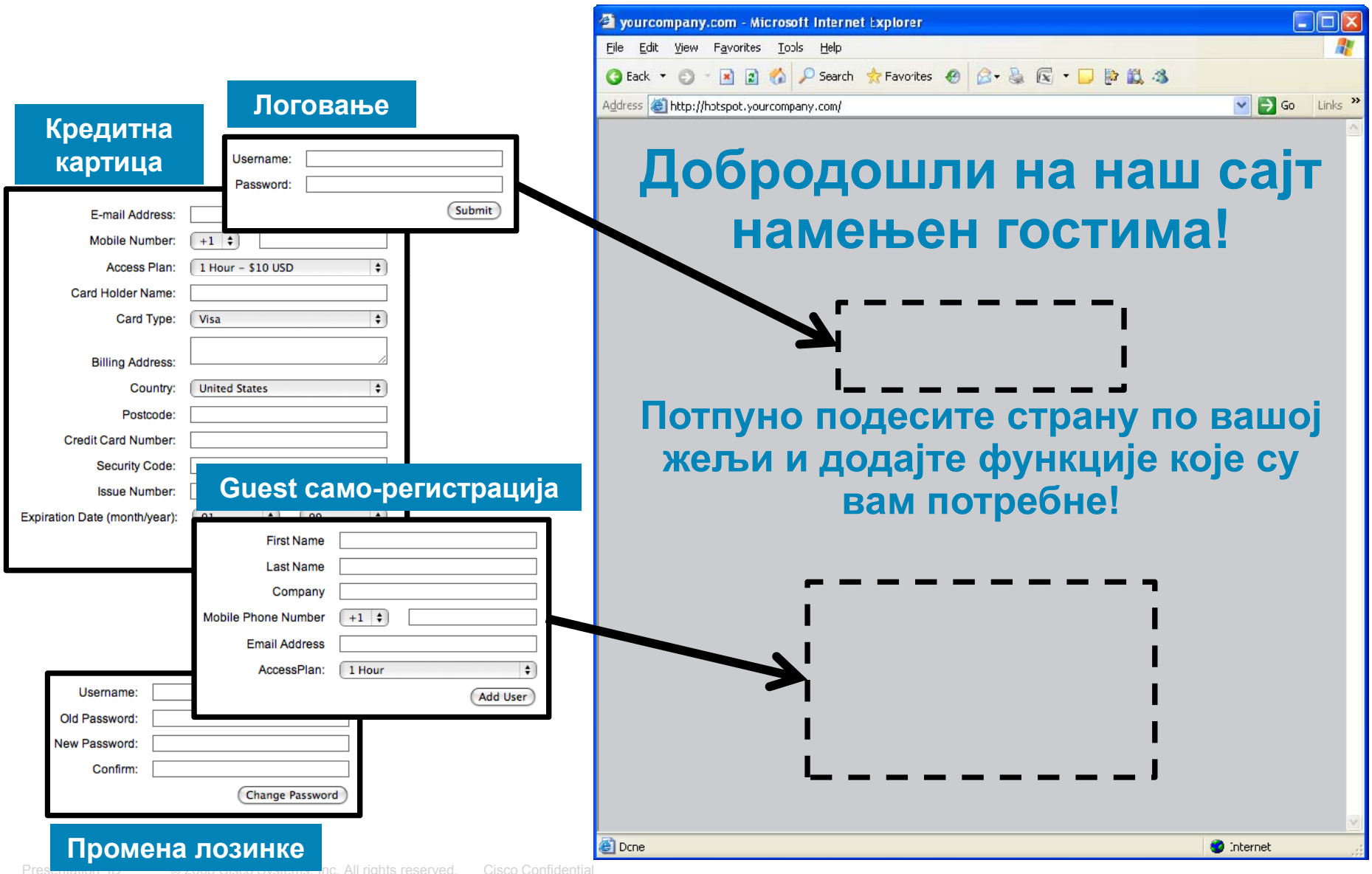
Page 1 of 1

Activity Log: jsmith@mycustomer.com *Showing 1-3 of 3* 10 Per Page

Date/Time	Device	Message
12-Jan-2009 9:31 AM	192.168.137.20	1.0.0.7 TCP connection permitted to 198.133.219.25:80
12-Jan-2009 9:31 AM	192.168.137.20	1.0.0.7 accessed URL http://www.cisco.com
12-Jan-2009 9:32 AM	192.168.137.20	1.0.0.7 TCP connection denied to 204.65.34.23:4662

Page 1 of 1

NAC *Guest* сервер
Подесиви портал



CSM и MARS - новости

Cisco Security Менаџер 3.3
Преглед

Карактеристике	Вредност за посао
Солидни оперативни алати	1. додавање балка, импорт и експорт функција за брзу имплементацију 2. брза имплементација коришћењем постојећих информација
Капацитет да подржи нове технологије	1.Потпуна подршка за фајервол заснован на зонама 2. побољшана GET VPN подршка и VPN коришћење
Ефикасност и перформансе	1. размена информација о инвенторију са системима у циљу боље интеграције 2. перформансе побољшане за свакодневне операције
Повећана подршка за уређаје	1. подршка за уређаје и оперативне системе уређаја у циљу бољег покривања Cisco® ASA 7.2.5, 8.0.5, и 8.1.2; Titan; IPS 6.2; collaborative IPS; FWSM 3.1(13), 3.1(14), 3.2(9), 3.2(10), 4.0(3), и 4.0(4); 861 to 892 Integrated Services Routers; ASR 1000 Release 3; и VSPA; и Cisco IOS® Software 12.4(15/20/22)T

MARS подршка за глобалну корелацију

новости

6.0.4

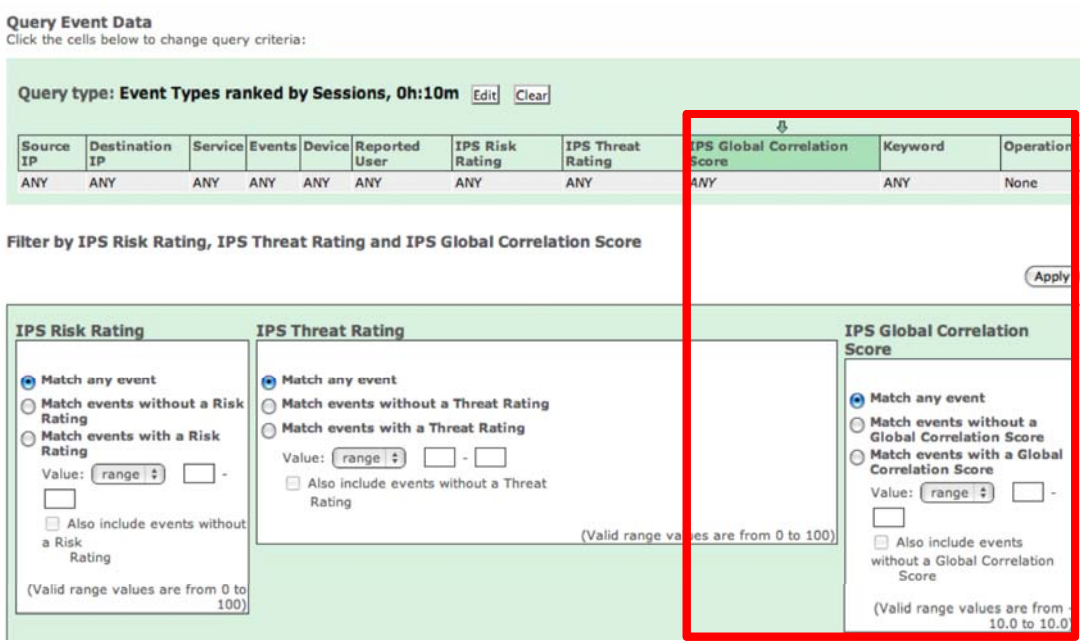
Софтверске карактеристике

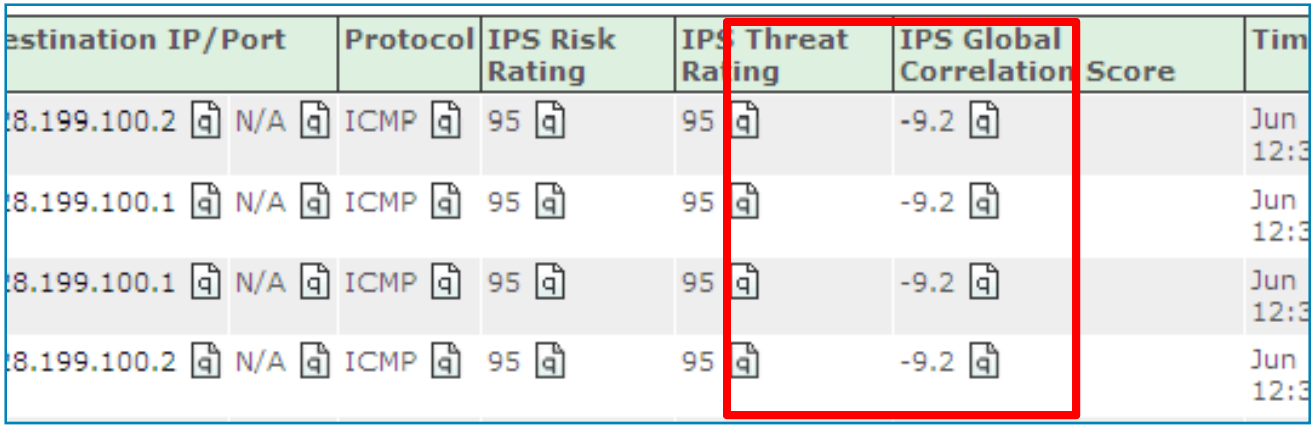
- БТФ – приказ и извештаји
- Глобална корелација – приказ и извештаји

Подржани уређаји

- ASA 8.2
- ASA 5505 IPS SSC
- IPS 7

Нови потписи





Презентације и демои на Експу посвећени сигурности рачунарских мрежа

Презентације

1. Апокалипса Сада? – Ивица Остојић – уторак, 14:00
2. conf t: Имплементација Cisco IPS решења – Петр Ружичка – среда 09:30
3. conf t: Cisco IPSec VPN решења – Драган Новаковић – среда 10:30
4. *E-mail security appliance* – Хрвоје Доган – среда, 14:30
5. Имплементација *web security appliance* – Петр Ружичка – среда, 15:30

Партнерске презентације

1. Сигурност бежичне мреже у реалном окружењу – среда, 11:45
2. Примена DMVPN технологије у заштити комуникације кроз јавну MPLS VPN мрежу – среда, 12:45

Демои на партнерским штандовима

- ASA 8.2 BTF, IPS 7.0, NSEL у интеграцији са MARS 6.0
- ACS 5.0 и 802.1x
- NAC guest сервер, сигурност у бежичним мрежама

Региструјте се за Cisco Networkers
25-28. јануар 2010. Барселона
28-31. март 2010. Бахреин