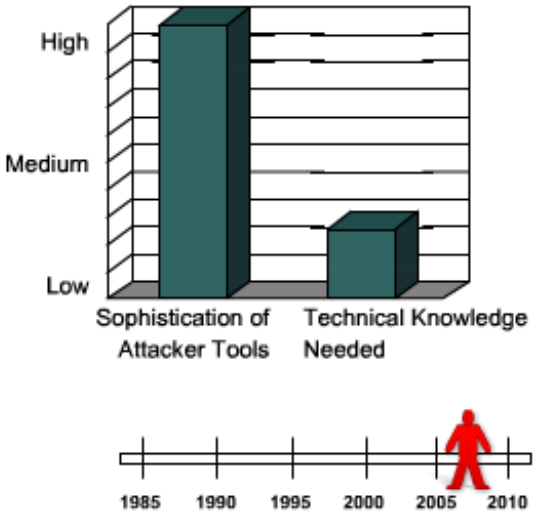
Networking Academy

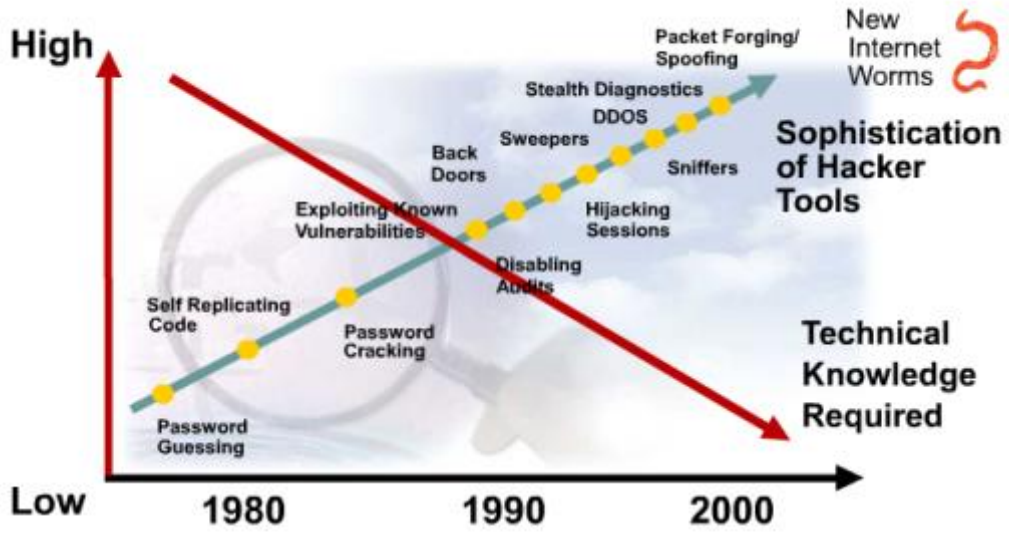
Фаєрволи. Організація захисту периметру мережі та фільтрування трафіку

ASC NULP

January 2020

Організація атак та необхідні технічні знання





Threats continue to become more sophisticated as the technical knowledge required to implement attacks deminishes.

© 2012 Cisco and/or its affiliates. All rights reserved.

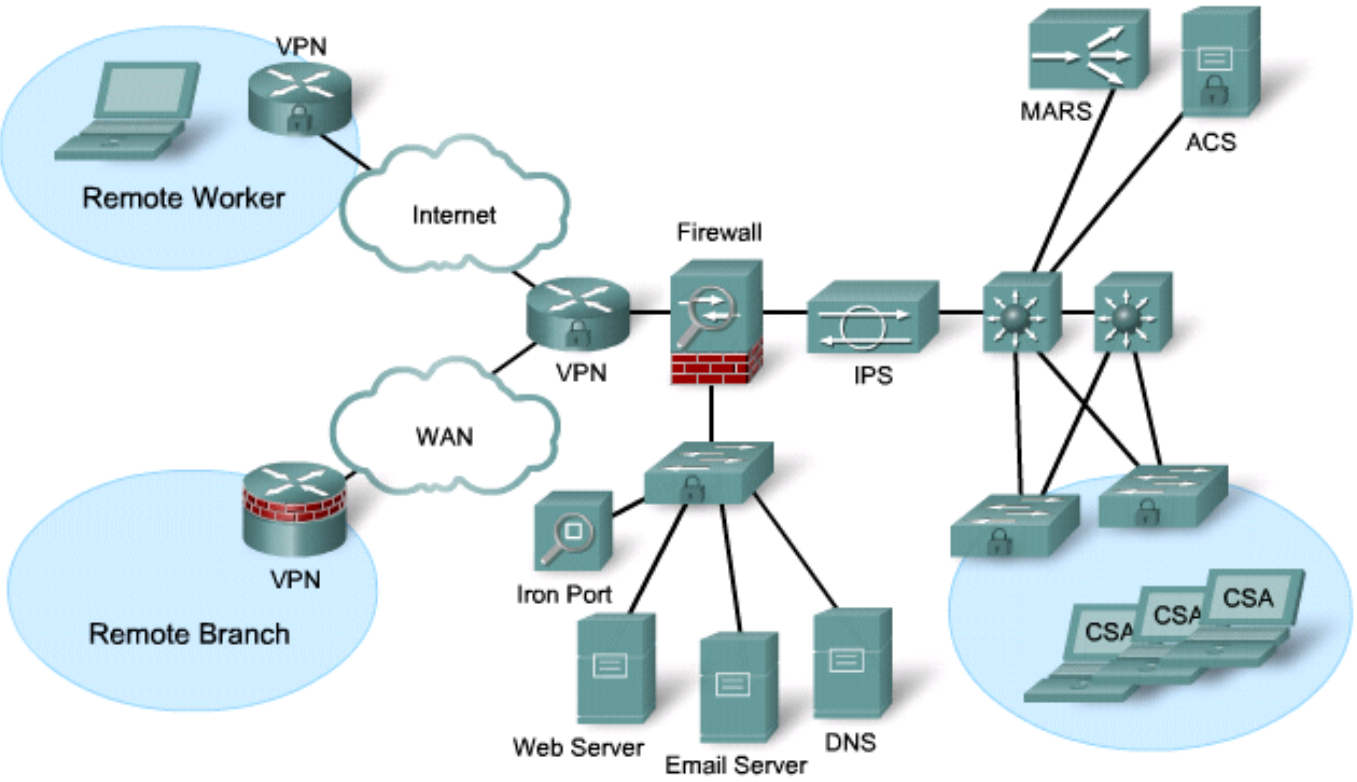
Захист периметра мережі

- **Периметр** - це укріплена границя корпоративної мережі, що може включати:
- маршрутизатори (routers);
- брандмауери (firewalls);
- проксі-сервери (proxy-servers);
- Системи виявлення та запобігання вторгнень (IDS/IPS);
- Засоби віртуальних приватних мереж (VPN);
- Засоби антивірусного захисту;
- Демілітаризовану зону (DMZ).

- Захист периметра вважається обов'язковим елементом системи безпеки, який забезпечує інформаційну безпеку, корпоративні мережі.

- Його реалізація залишається одна з основних задач ІБ та основа надійного функціонування критичних для компаній інформаційних систем.

Secure End-to-End Network



- Периметр мережі виконує захист на основі політик безпеки, які використовуються в організації/корпорації.

© 2012 Cisco and/or its affiliates. All rights reserved.

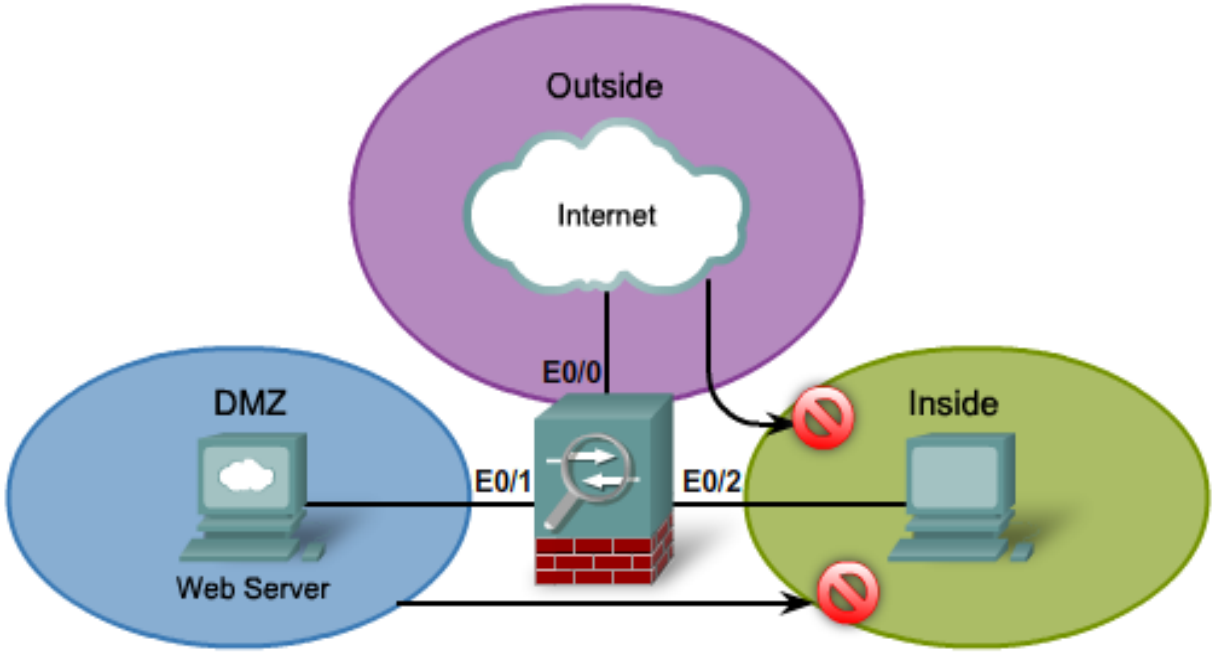
Найбільш поширені загрози для інформаційних ресурсів організації

- Мережні атаки, спрямовані на недоступність інформаційних ресурсів (Web-серверів, сервісів електронної пошти і т.д.) — атаки класу DoS і DDoS;
- Компрометація інформаційних ресурсів та ескалація привілеїв — як з боку внутрішніх, так і зовнішніх зловмисників, як з метою використання ваших ресурсів, так і з метою нанесення шкоди;
- Дії шкідливого програмного коду (віруси, мережні хробаки, трояни, програми-шпигуни і т.д.);
- Витік конфіденційної інформації і викрадення даних — як через мережу (e-mail, FTP, web тощо), так і через зовнішні носії;
- Різні мережні атаки на застосунки (application);
- Захист периметра інформаційної системи є обов’язковим елементом системи інформаційної безпеки організації.

Міжмережні екрани можуть забезпечувати різний функціонал

- Розмежування та контроль доступу, виконання аутентифікації користувачів, трансляція IP-адрес (NAT);
- Організація демілітаризованих зон;
- Побудова різних типів VPN (IPSec і SSL VPN);
- Функціонал контролю контенту. Аналіз трафіку на прикладному рівні, захист трафіку від вірусів і різних типів spyware і malware, захист від спаму, URL-фільтрація, антифішинг, та ін;
- Функціонал системи виявлення та запобігання мережевих атак і несанкціонованої мережевої активності;
- Високу доступність і кластеризацию;
- Балансування навантаження;
- Підтримка якості обслуговування (QoS);
- Інтеграцію з різними системами аутентифікації і авторизації (RADIUS, TACACS +, LDAP та ін);
- Керування списками контролю доступу маршрутизаторів;
- Ряд інших можливостей.

Використання Firewall в мережі



- Traffic originating from the Outside network going to the Inside network is denied.
- Traffic originating from the DMZ network going to the Inside network is denied.

© 2012 Cisco and/or its affiliates. All rights reserved.

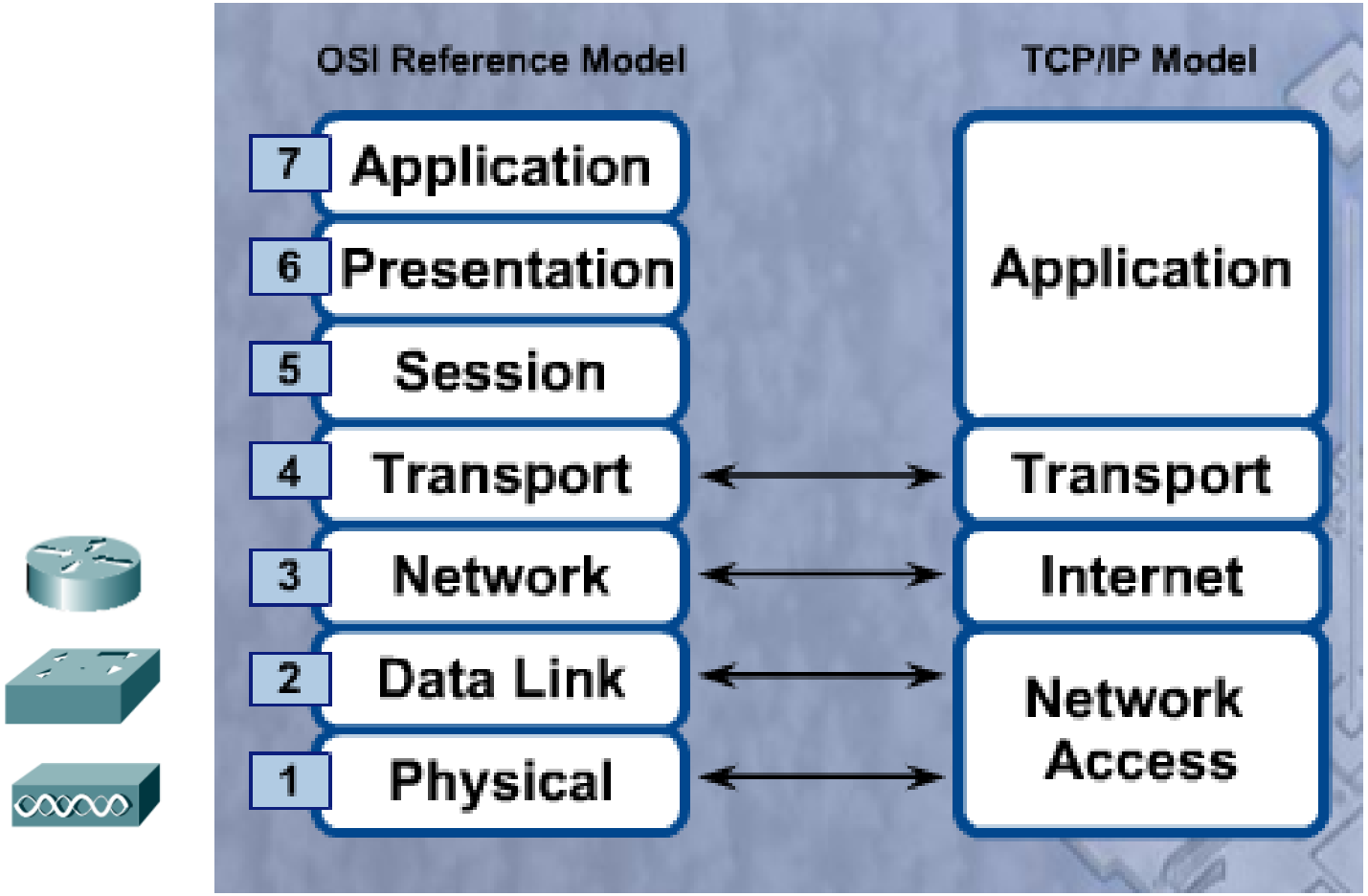
Міжмережні екрани (Firewalls)

Міжмережний екран розміщують між двома мережами. Він здійснює контроль трафіку та дозволяє здійснювати контроль трафіку та запобігти несанкціонованому доступу. несанкционированный доступ.

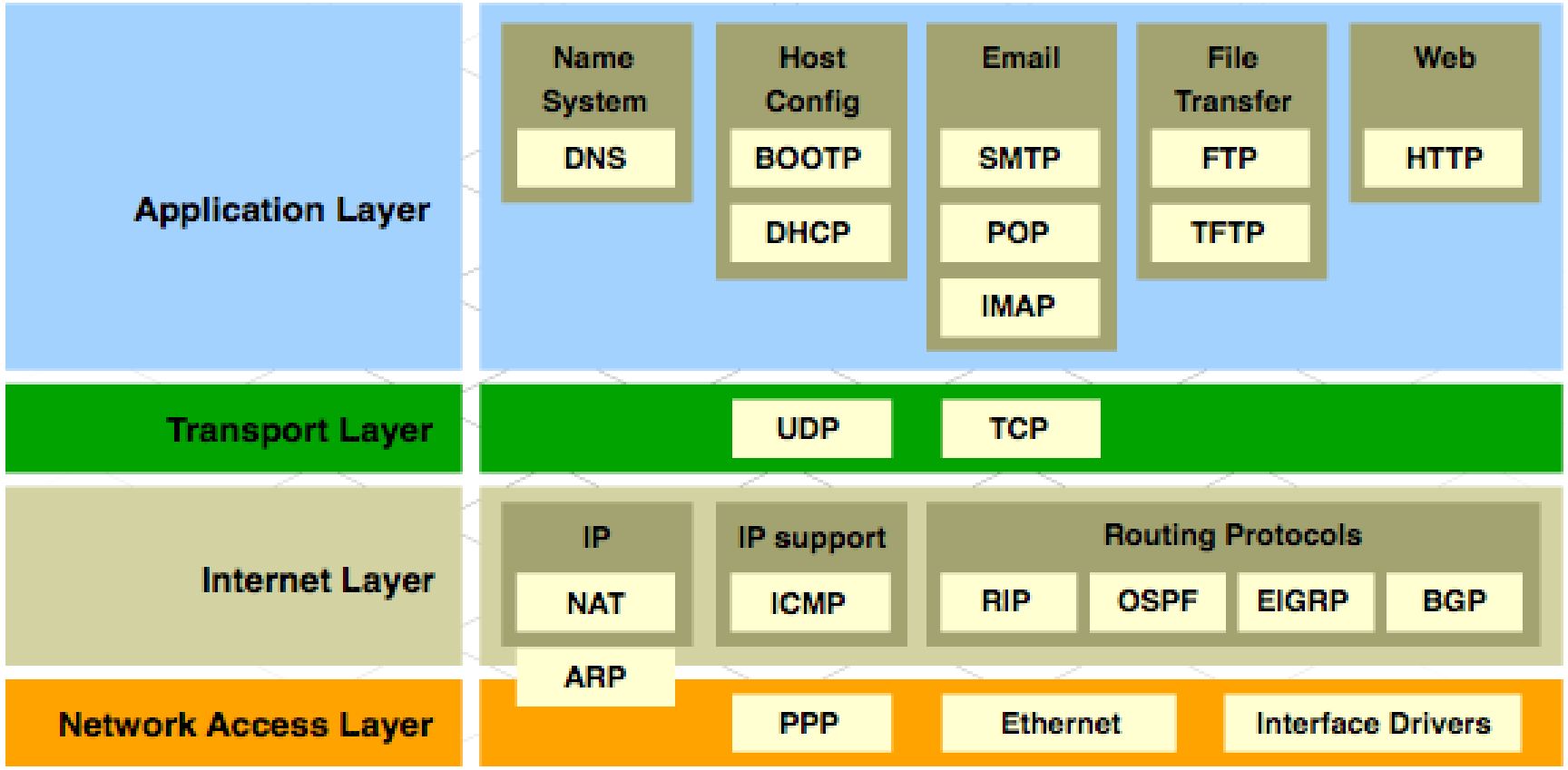
Використовуються наступні методи:

- фільтрація пакетів;
- фільтрація застосунків;
- фільтрація URL-адрес.
- динамічний аналіз пакетів (*Stateful Packet Inspection* -**SPI**): вхідні пакети можуть бути легітимними відгуками на запити внутрішніх вузлів.

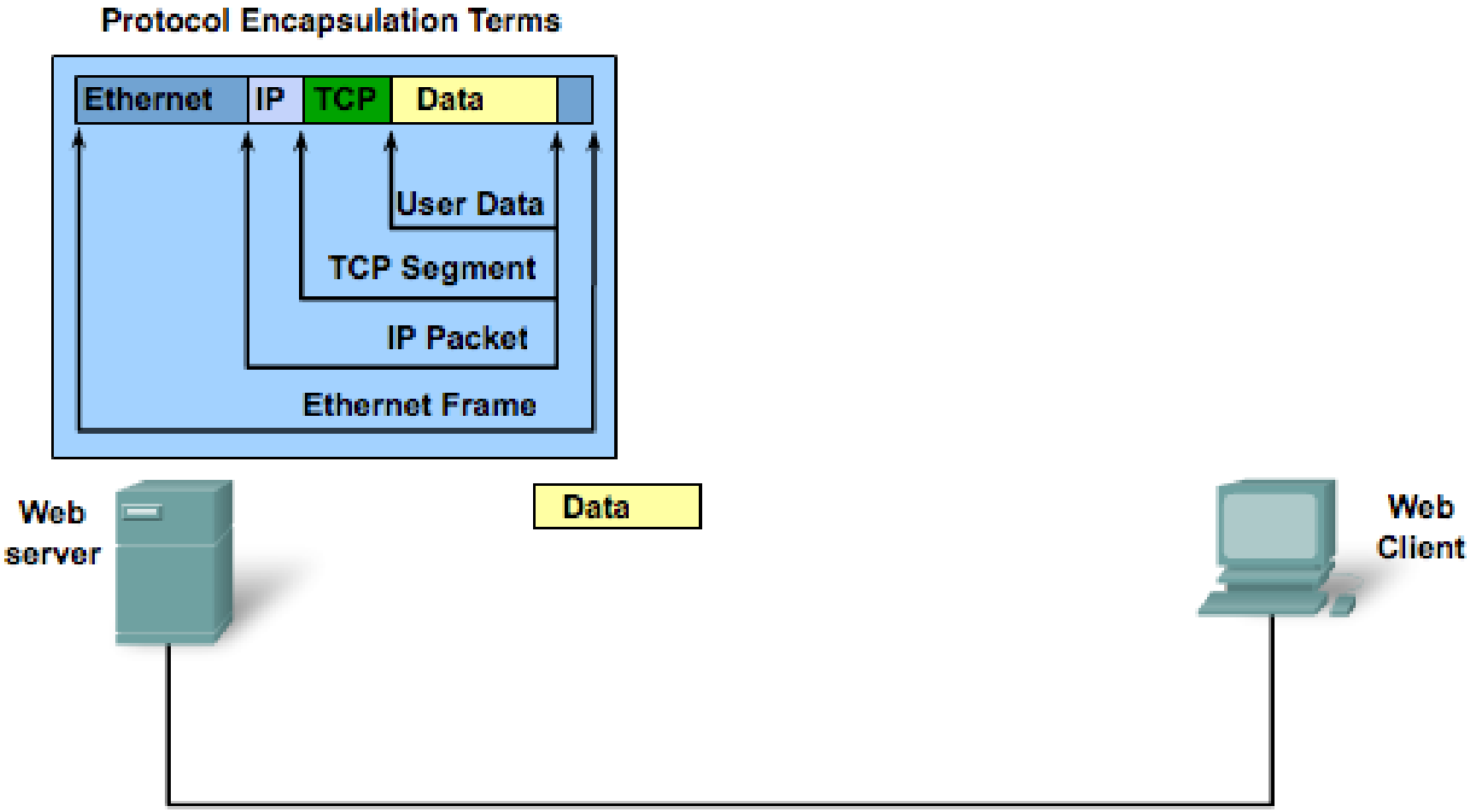
Порівняння моделей OSI і TCP/IP



TCP/IP Protocol



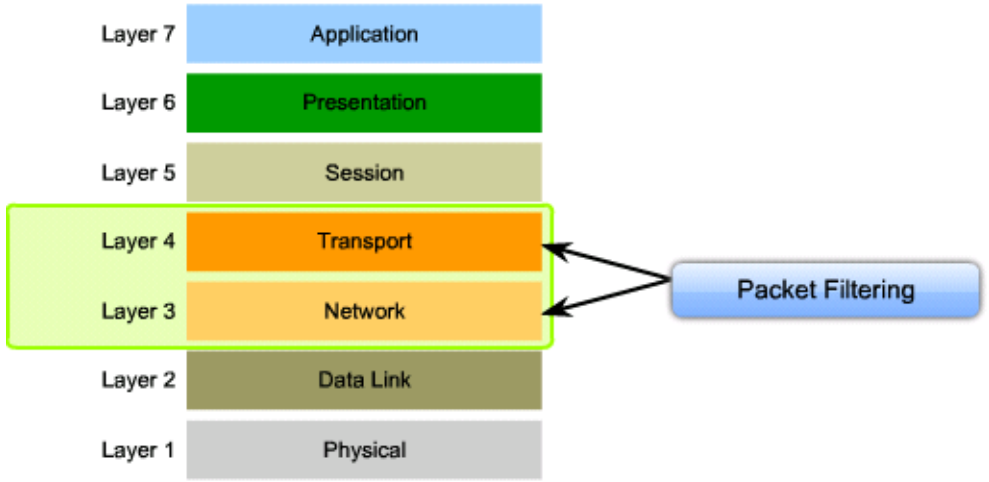
Інкапсуляція



Типи Firewalls

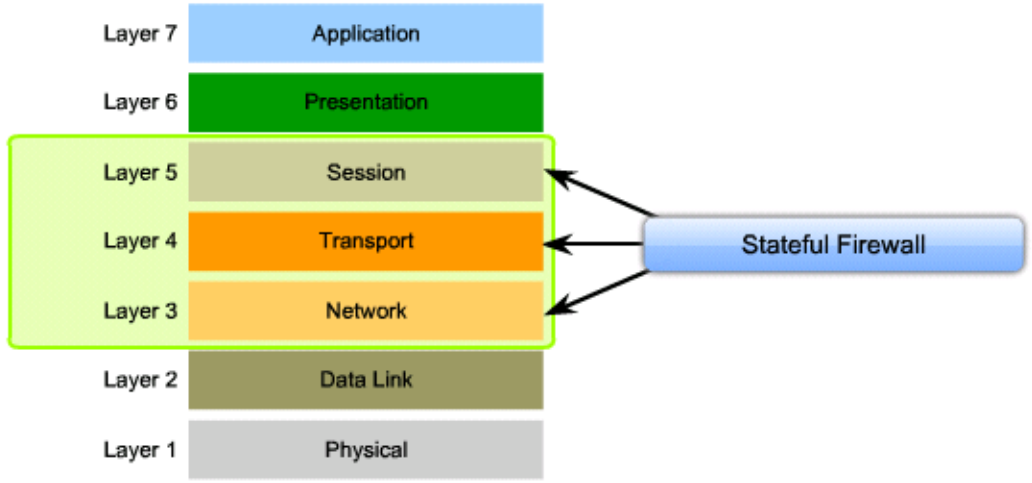
- Packet-filtering firewall

  (FW фільтрації пакетів)



- Stateful firewall

  (Повний FW)



Міжмережеві екрани (Firewalls)

Апаратний Firewalli	Програмні Firewall
Спеціалізований компонент обладнання	Програмне забезпечення вбудоване в ОС, або стороннього виробника.
Вартість оновлення обладнання і програмного забезпечення може бути дуже високою	Безкоштовна версія входить до складу операційної системи Windows. Інструменти ОС: Windows brandmauer (для ОС Windows) iptables (для ОС Linux)
Як правило, захищає периметр мережі	Як правило, захищає тільки той комп’ютер на якому встановлений
Не впливає на продуктивність кінцевого хоста	Використовує ЦП кінцевого хоста, може знижувати продуктивність комп’ютера

Фільтрація трафіку

Пристрої, що фільтрують трафік:

- Міжмережні екрани, що налаштовані в маршрутизаторах
- Спеціалізовані пристрої безпеки (апаратні firewalls)
- Маршрутизатори з інтегрованими сервісами (ISR)
- Інструменти ОС робочих станцій:
  - **Windows brandmauer** (для ОС Windows)
  - **iptables** (для ОС Linux)

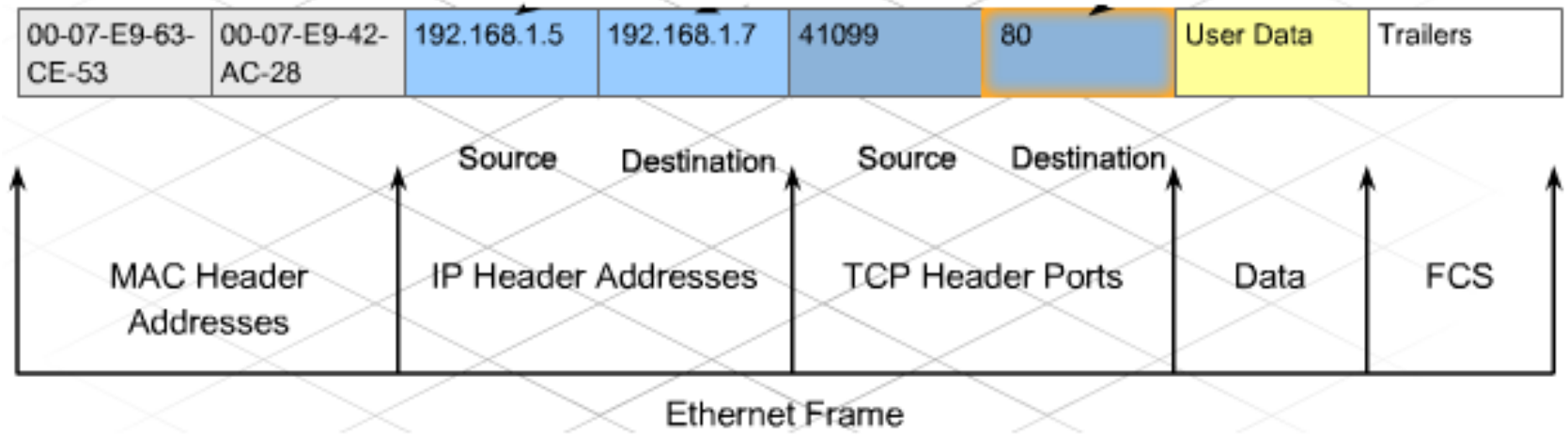
Cisco Router with IOS Firewall

Linksys Wireless Router with Integrated Firewall

Cisco Security Appliances

Алгоритм фільтрації трафіку

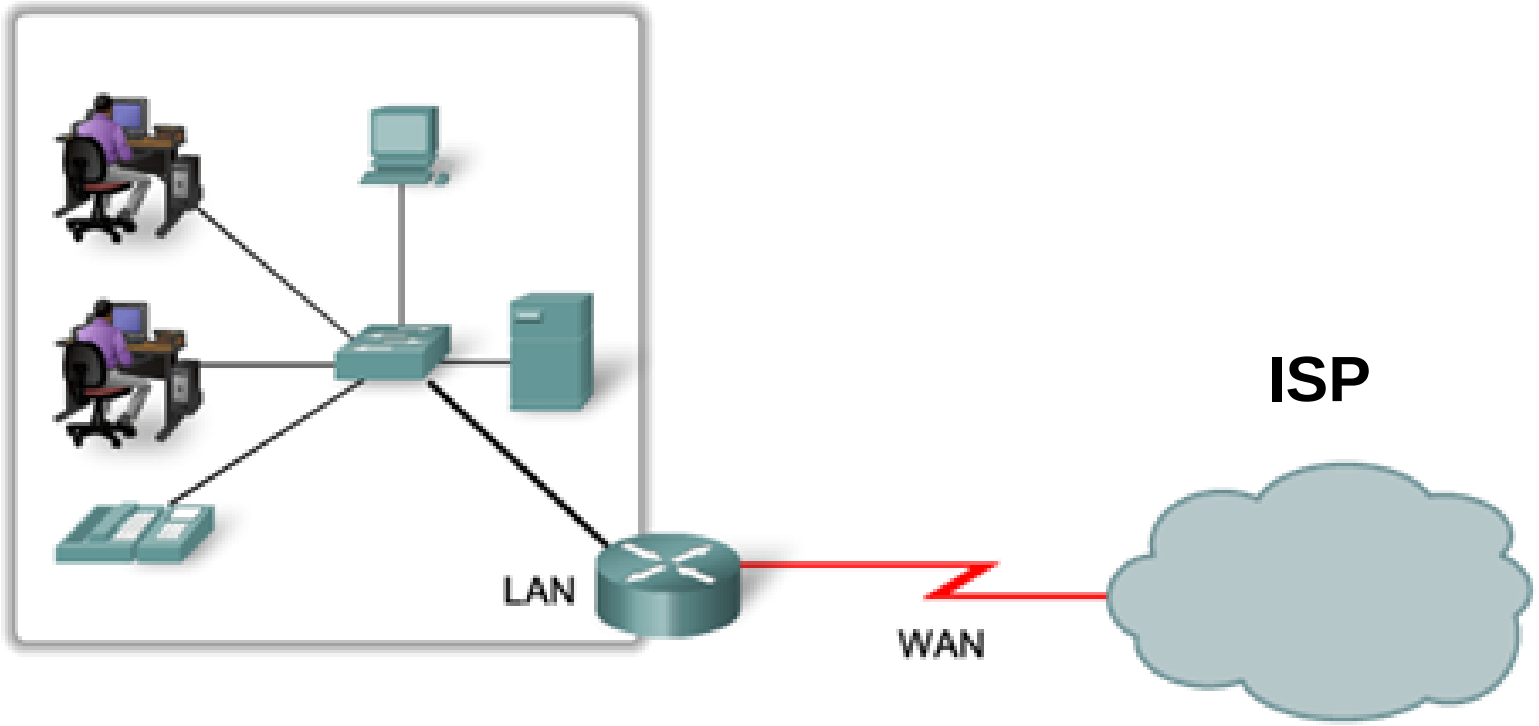
- Аналіз вмісту пакету
- Пропускання або блокування пакету
- Фільтрація за:
  - MAC адресою
  - IP адресою джерела
  - IP адресою призначення
  - Протоколом мережного рівня і вище
  - Типом сервісу прикладного рівня



Список контролю доступу (**ACL**) — це послідовний список дозвільних або забороняючих послідовно прописаних правил.

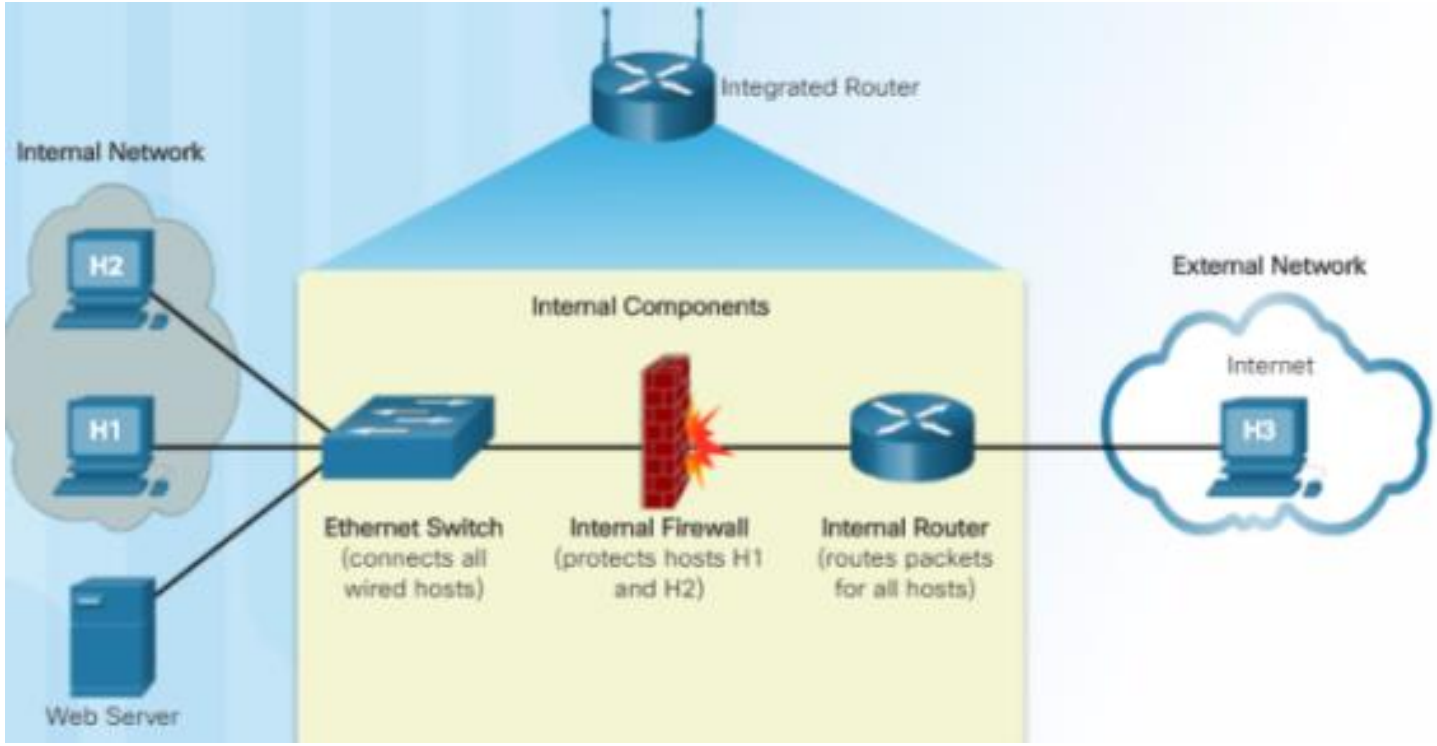
Топологія Small Network /Home Network (SOHO)

Типова топологія невеликих мереж



Маршрутизатор з інтегрованими сервісами

Еквівалентна схема



© Корпорация Cisco Systems, 2015. Все права защищены.
Конфиденциальная информация Cisco

Базовий рівень безпеки бездротової мережі

- Зміна усіх значень, що встановлені за замовчуванням в бездротовому маршрутизаторі з інтегрованими сервісами: логіну/паролю доступу до налаштувань
- Відключення можливості доступу до налаштувань через Wi-Fi
- Відключіть WPS
- Налаштування надійного паролю для підключення до Wi-Fi мережі
- Вибір безпечного типу шифрування (на сьогоднішній момент WPA2)
- Фільтрування MAC адрес бездротових пристроїв
- Фільтрування трафіку за допомогою вбудованого фаєрволу
- Відключення широкомовного розсилання ідентифікатора SSID (опційно)
- Оновлення вбудованого ПЗ маршрутизатора до актуальної версії з останніми виправленнями безпеки (patches).

© Корпорация Cisco Systems, 2015. Все права защищены.

Режими безпеки безпровідної мережі

- **Wired Equivalent Privacy (WEP)** – стандарт безпеки першого покоління для безпровідних мереж. Використовує заздалегідь визначені ключі для шифрування і розшифрування даних. На всіх безпровідних пристроях, для яких дозволений доступ до мережі, необхідно ввести один і той же ключ WEP. Зловмисники швидко виявили, що шифрування WEP є слабким і його легко зламати. НЕ Є БЕЗПЕЧНИМ!!!
- **Wi-Fi Protected Access (WPA) -** вдосконалена версія WEP, використовує більш стійке шифрування. НЕ Є БЕЗПЕЧНИМ!!!
- **Wi-Fi Protected Access 2 (WPA2)** – покращена версія WPA. WPA2 підтримує надійне шифрування, забезпечуючи урядовий рівень безпеки. WPA2 має дві версії: Personal (перевірка достовірності за допомогою пароля) і Enterprise (серверна перевірка достовірності).

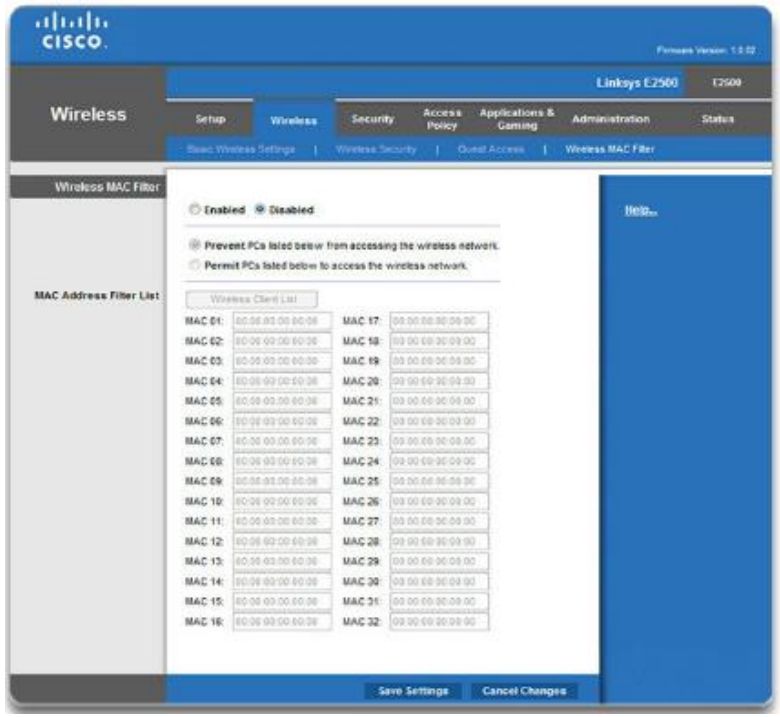
Бездротовий доступ. Процедури безпеки

- **Антени безпровідного зв'язку**
  - Уникайте передачу сигналів за межами області функціонування мережі, встановивши антена з діаграмою направленості, яка обслуговує користувачів вашої мережі. Діаграма поркиття у більшості SOHO маршрутизаторів має сферичну форму.
- **Доступ до мережих пристроїв**
  - Перед підключенням пристрою до мережі необхідно змінити ім'я користувача та пароль за замовчуванням для керування налаштуваннями**.**
- **Налаштування захисту Wi-Fi (Уникайте використання WPS)**
  - В технології WPS користувач підключається до безпровідного маршрутизатора використовуючи встановлений виробником PIN, який є або на наклейці або відображається на дисплеї.
  - Розроблено програмне забезпечення, яке може перехоплювати трафік і відновити PIN-коду WPS і попередньо узгодженого ключа шифрування. Рекомендується вимкнути WPS на бездротовому маршрутизаторі, якщо це можливо.

© 2008 Cisco Systems, Inc. All rights reserved.

Фільтрація MAC- адрес

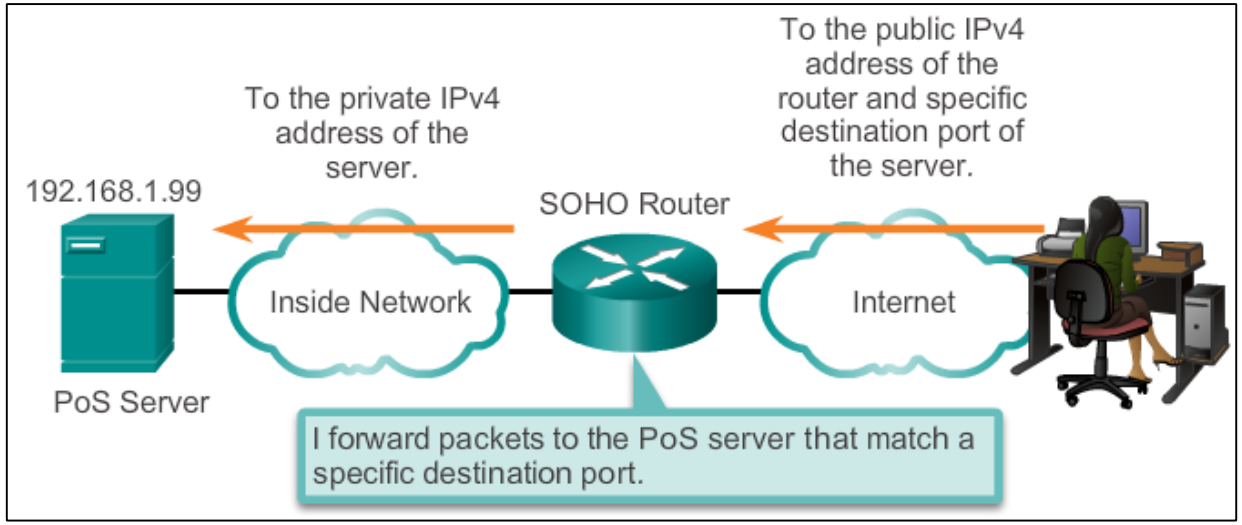
- Фільтрація по MAC адресах це метод, що використовується на рівні пристроїв, для безпечного доступу до бездротових локальних мереж.



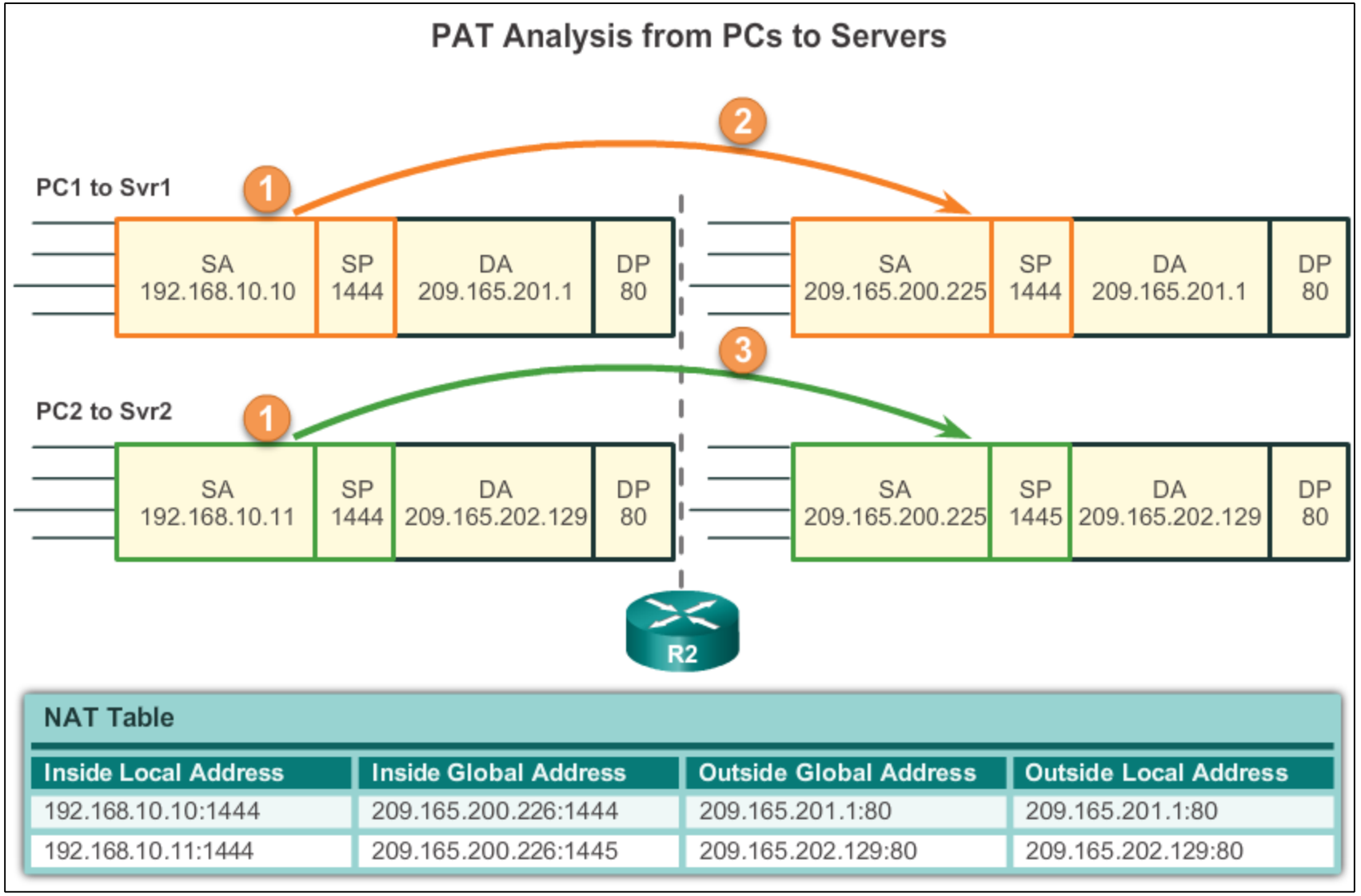
© 2008 Cisco Systems, Inc. All rights reserved.

Переадресація портів (Port Forwarding)

- Переадресація портів (також відоме, як **Port forwarding**) — це процес переадресації мережного порту від одного вузла мережі на інший вузол.
- Пакет, що надісланий на публічну IP-адресу та порт маршрутизатора, може бути перенаправлений на приватну IP-адресу та порт внутрішньої мережі відповідно.
- Даний процес корисний у випадку, коли сервери мають приватні адреси, що не доступні з зовнішніх мереж.



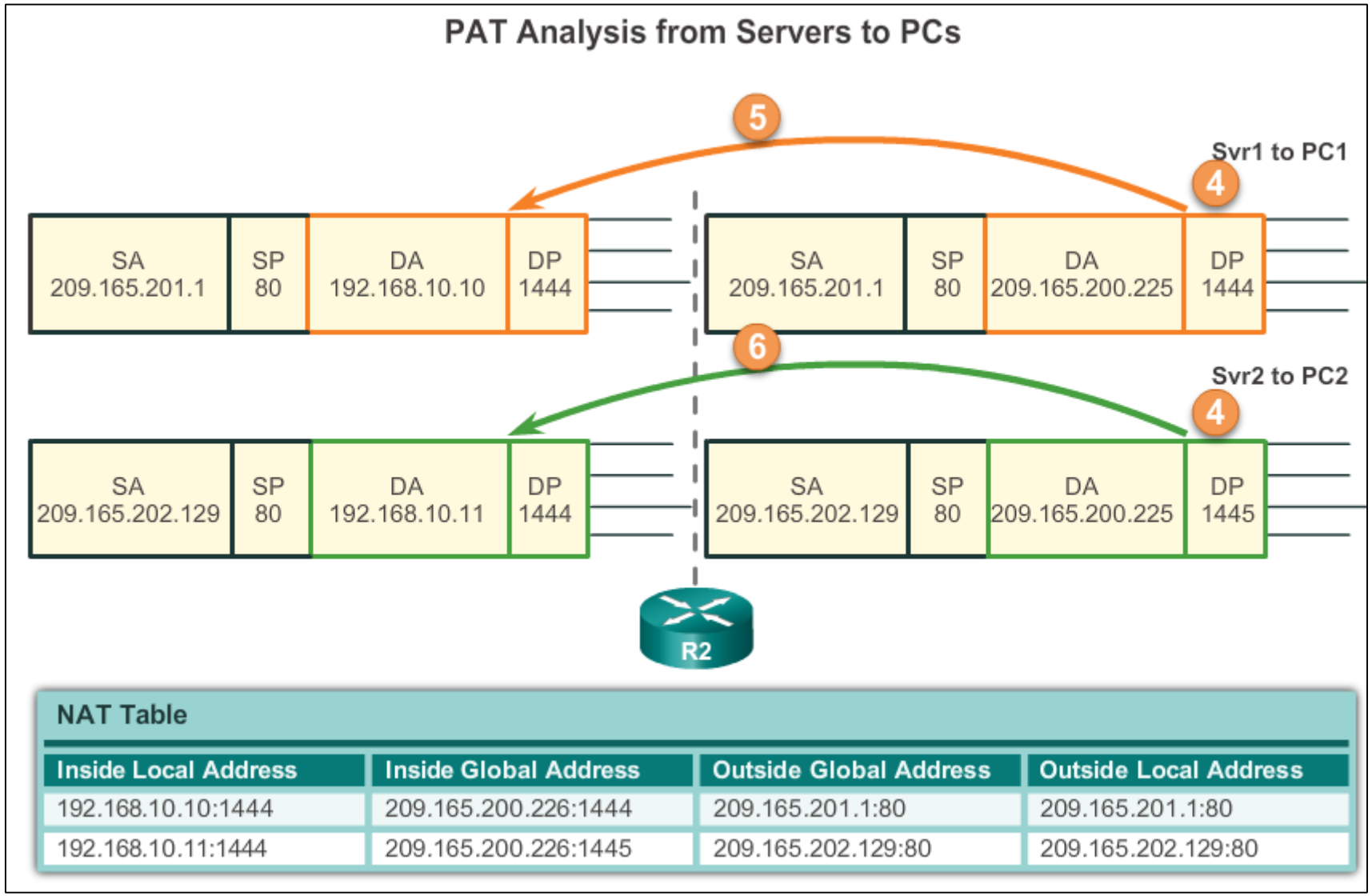
Аналіз роботи PAT



NAT Table

Inside Local Address	Inside Global Address	Outside Global Address	Outside Local Address
192.168.10.10:1444	209.165.200.226:1444	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1444	209.165.200.226:1445	209.165.202.129:80	209.165.202.129:80

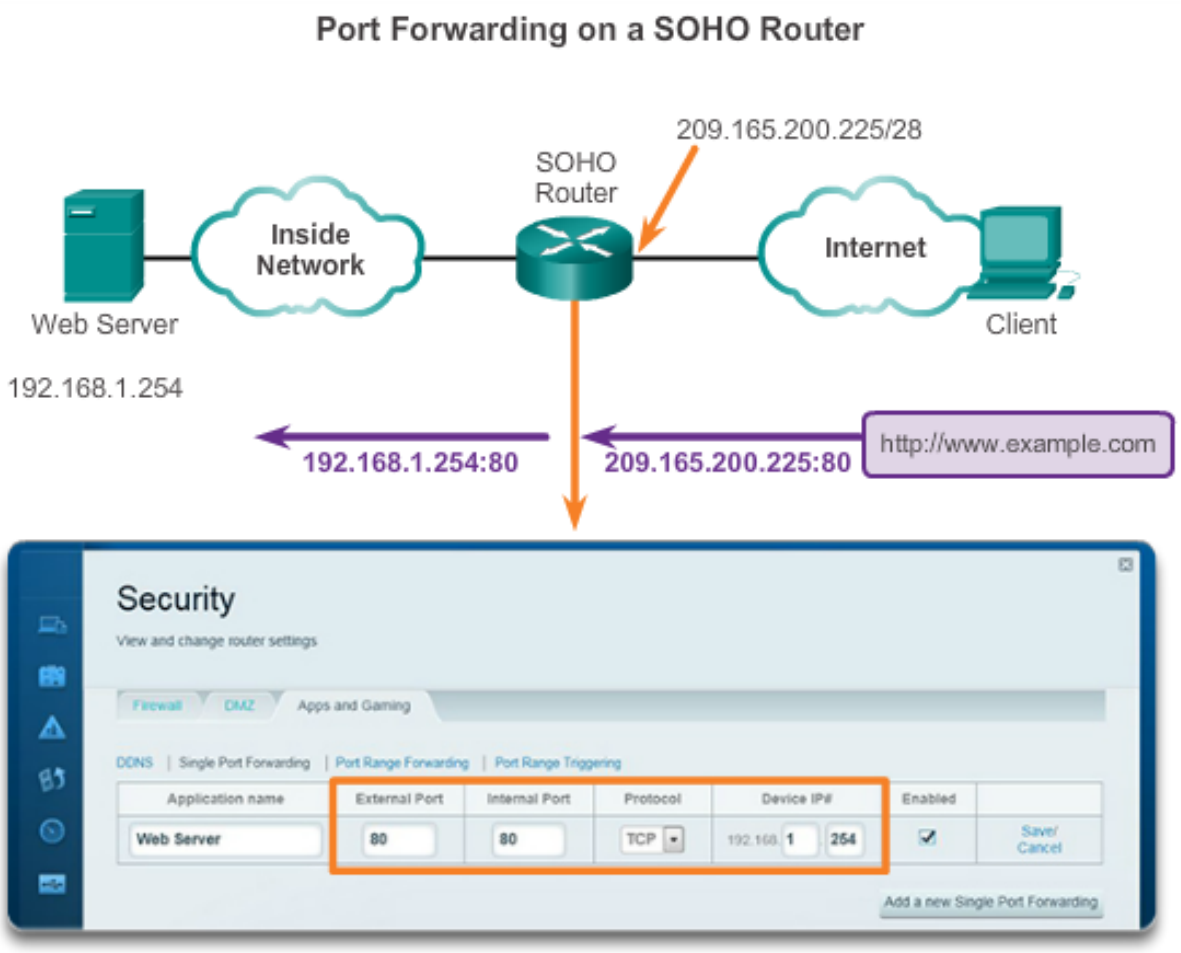
Аналіз роботи PAT



NAT Table

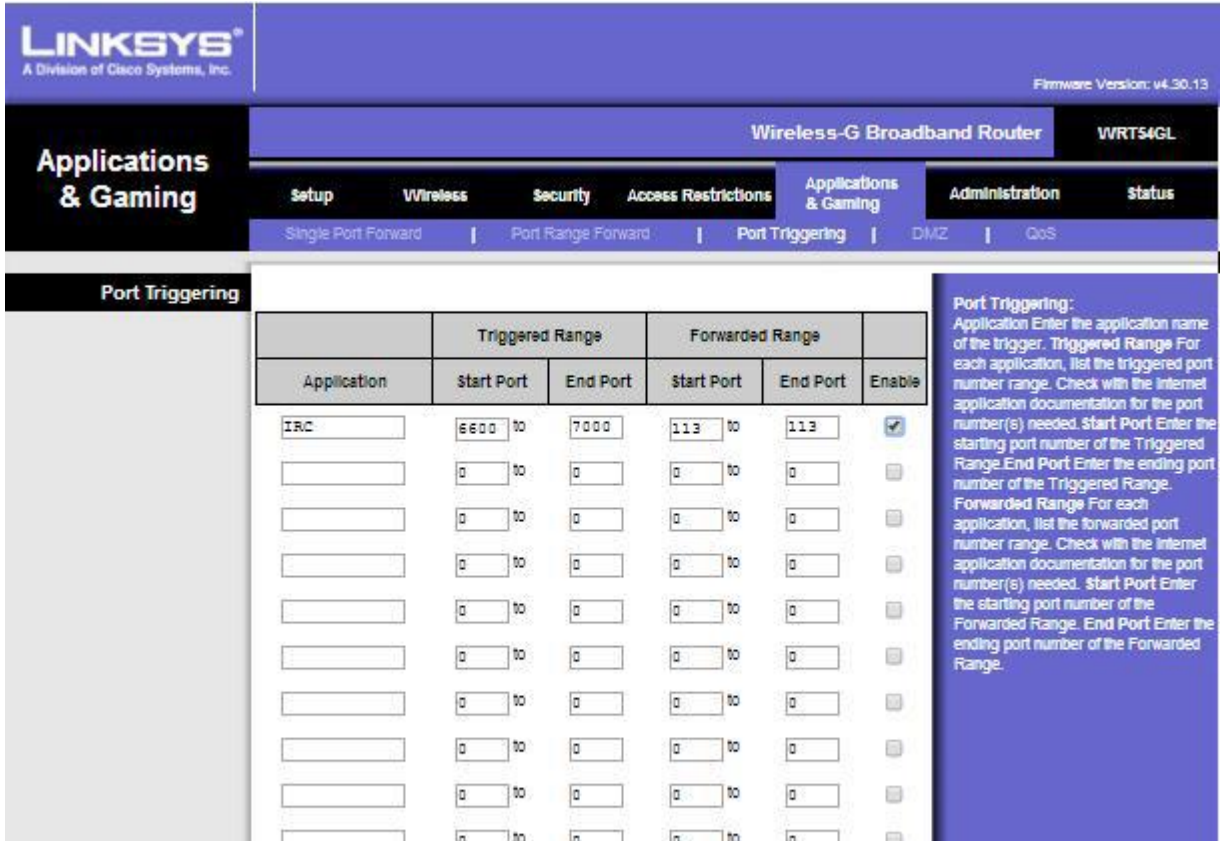
Inside Local Address	Inside Global Address	Outside Global Address	Outside Local Address
192.168.10.10:1444	209.165.200.226:1444	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1444	209.165.200.226:1445	209.165.202.129:80	209.165.202.129:80

Приклад застосування переадресації портів



Включення групи портів

- **Включення групи портів (Port triggering)** дозволяє маршрутизатору тимчасово переадресовувати дані через вхідні порти певному пристрою.
  - Наприклад, відеогра може використовувати порти 27000 - 27100 для зв'язку з іншими гравцями.Це є порти ті порти, що включаються.

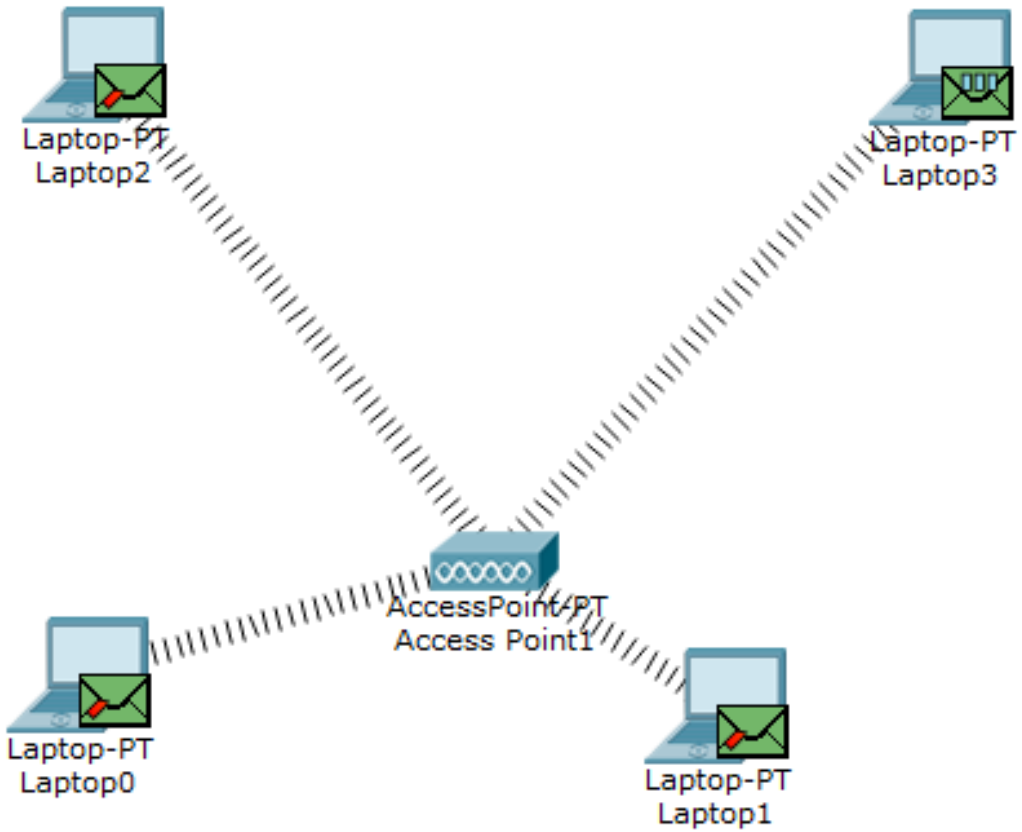


Методи забезпечення інформаційної безпеки в публічних Wi-Fi мережах

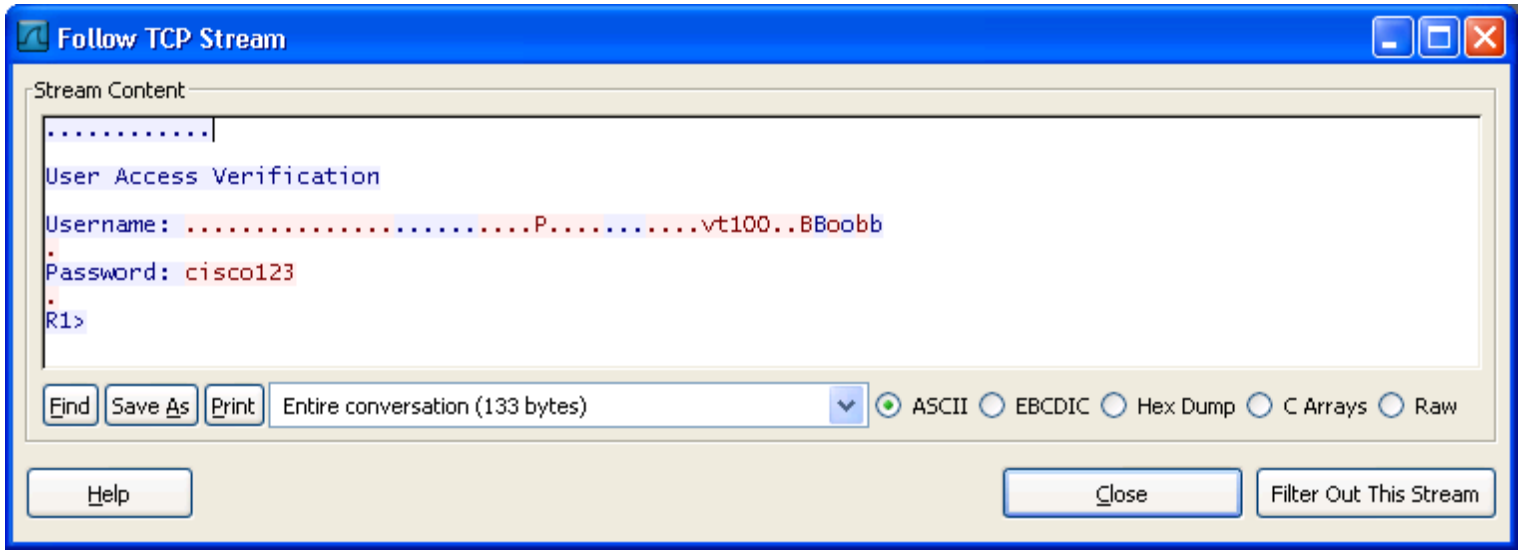
- Шифрування повідомлень між двома комп'ютерами, що взаємодіють, через зашифрований канал передачі даних, наприклад, через віртуальні приватні мережі (VPN).
- Для передавання конфіденційної інформації, за можливості, використовуйте мобільний Інтернет, а не публічні Wi-Fi мережі.

© Корпорация Cisco Systems, 2015. Все права защищены.

Робота AP

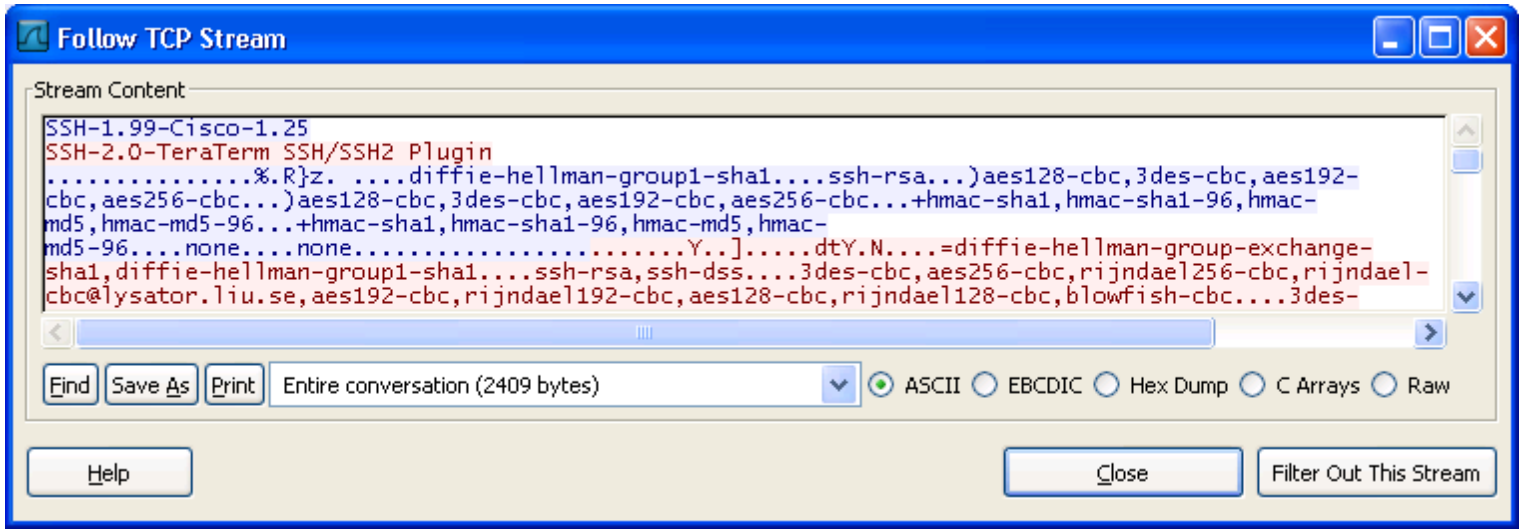

Laptop-PT
Laptop2
Laptop-PT
Laptop3
AccessPoint-PT
Access Point1
Laptop-PT
Laptop0
Laptop-PT
Laptop1

Follow the TCP Stream



- У TCP Telnet потоці можна виявити логін адміністратора (username - Bob) та пароль (password - cisco123).

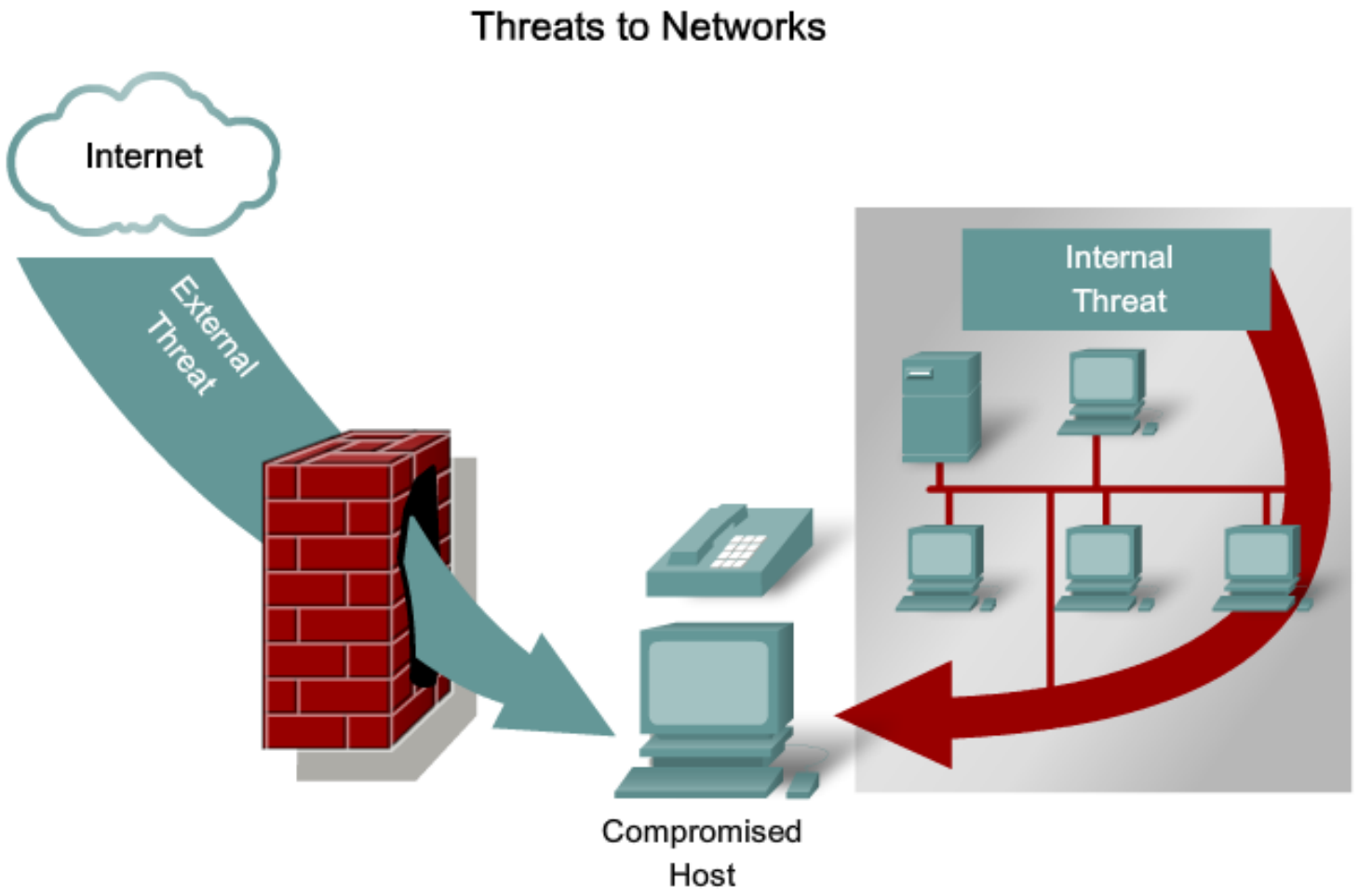
Follow the TCP Stream



- Нападник тільки бачить інформацію інкапсульовану у TCP – сегменті, але не може її прочитати – вміст SSH пакету зашифровано.

Мережна безпека

20%

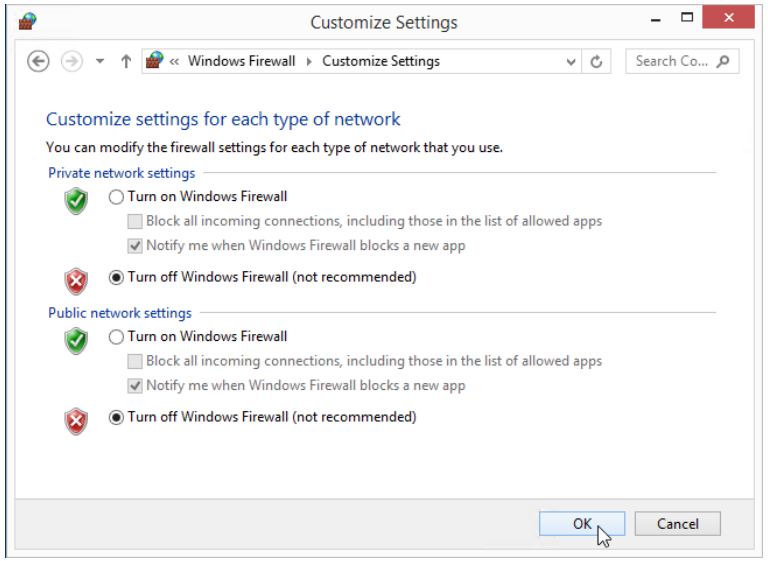


80%

Забезпечення безпеки

Забезпечення безпеки включає виконання наступних завдань:

- Встановлення актуальних виправлень безпеки і пакетів виправлень для операційної системи.
- Регулярне резервне копіювання даних.
- Встановлення, налаштування і включення програмного фаєрволу, наприклад брандмауер Windows.



© Корпорация Cisco Systems, 2015. Все права защищены.
Конфиденциальная информация Cisco

The Networking Academy Learning Portfolio

Current & Planned

Aligns to Certification

Instructor Training required

Self-paced

* Available within 12 months

Collaborate for Impact

Introduction to Packet Tracer | **Packet Tracer** | **Hackathons** | **Prototyping Lab** | **Internships**

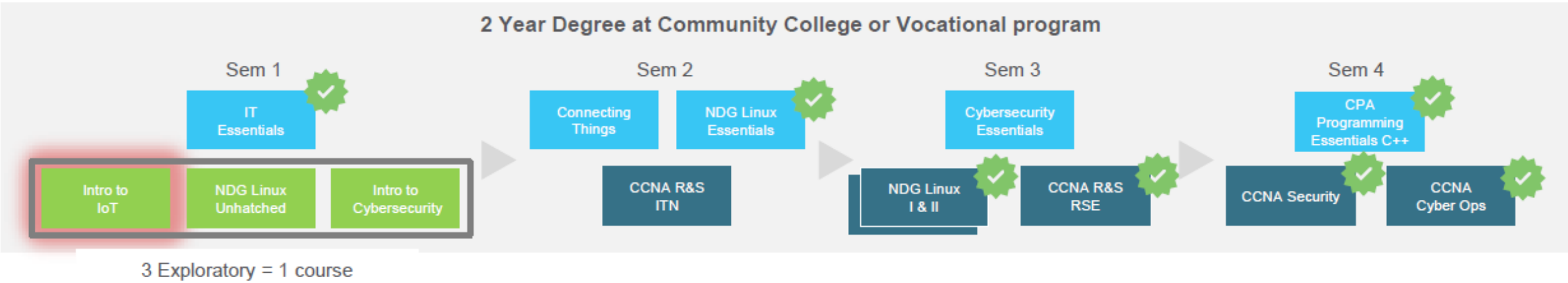
	Exploratory	Foundational	Career-Ready
Networking		**Networking Essentials** **Mobility Fundamentals**	**CCNA R&S:** Introduction to Networks, R&S Essentials, Scaling Networks, Connecting Networks **CCNP R&S:** Switch, Route, TShoot **Emerging Tech Workshop:** Network Programmability Using Cisco APIC-EM*
Security	**Introduction to Cybersecurity**	**Cybersecurity Essentials**	**CCNA Security** **CCNA Cyber Ops***
IoT & Analytics	**Introduction to IoT**	**IoT Fundamentals:** Connecting Things, Big Data & Analytics Hackathon Playbook, **IoT Security***	
OS & IT	**NDG Linux Unhatched**	**NDG Linux Essentials** **IT Essentials**	**NDG Linux I** **NDG Linux II**
Programming		**CLA: Programming Essentials in C** **CPA: Programming Essentials in C++** **PCA: Programming Essentials in Python*** **Emerging Tech Workshop:** Experimenting with REST APIs Using Cisco Spark*	**CLP: Advanced Programming in C*** **CPP: Advanced Programming in C++**
Business	**Be Your Own Boss**	**Entrepreneurship**	
Digital Literacy	**Get Connected**		

Cybersecurity Pathway

Program: Cybersecurity
Target Audience: 2-Year Post-Secondary or Secondary Vocational/Career Tech program

Considerations

- Networking + Programmability
- 3 self-paced in 1 semester = a “course”
- Variety of domains—building breadth
- Incorporate 6 IT certifications for stackable credentials—building depth



© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

День безпечного Інтернету

Подробиці на:
Instructor Training Center Lviv Polytechnic
@itc.nulp

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Ресурси

Сайти

www.cisco.com
www.netacad.com

Fb-сторінки

Instructor Training Center Lviv Polytechnic
@itc.nulp

Cisco Networking Academy Ukraine
@CiscoNetAcadUA

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential