ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ

Кафедра управління інформаційною безпекою

Освітня компонента “Інструменти кібербезпеки”

Л Е К Ц І Я

Політики firewall-у

План лекції:

1. Політика firewall-у.
2. Реалізація сукупності правил firewall-у.
3. Тестування політики firewall-у.
4. Супровід firewall-у і управління ним.
5. Фізична безпека оточення firewall-у.
6. Адміністрування firewall-у.
7. Стратегії відновлення після збоїв firewall-у

Інформаційні джерела

Основні

1. Курс дисципліни у віртуальному університеті

Додаткові

1. Chris Sanders. PRACTICAL PACKET ANALYSIS. 3-RD EDITION. Usng Wireshark to Solve Real-World Problems.San Francisco. 2017. 450 p.
2. James D. Miller Implementing Splunk 7. Third Edition. Effective operational intelligence to transform machine-generated data into valuable business insightr. Packt Publishing. 2018. 490 p.
3. Левин М. Библия хакера 2. Книга 1. - М.: Майор, 2003. - 640 с. 4. Левин М. Библия хакера 2. Книга 2. - М.: Майор, 2003. - 688 с.
Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – Київ.: BHV, 2009. – 607 с.

1 Політика брандмауера

Політика вже розглядалася в 2.4.1 , коли йшлося про політику мережного доступу та політику проектування брандмауера. У цій частині розглядаються дві ці політики у зв'язку із загальною безпековою політикою організації та іншими керівними документами, в яких описані завдання організації, ризики, що загрожують їй та політики безпеки.

Концептуальні рішення щодо використання технології ьбрандмауерів повинні прийматися спільно з рішеннями щодо безпеки всієї мережі. Вони включають рішення про безпеку самих машин в мережі, безпеку доступу через модеми, безпеку доступу до Інтернету, захист інформації, що знаходиться на машинах в мережі та інші рішення. Автономна політика, що описує лише брандмауер, неефективна; потрібна інтеграція її у загальну безпекову політику організації. У [RFC1244] є докладніша інформація про створення політики безпеки організації, орієнтована на організації, які мають з'єднання з Інтернетом.

1.1 Кроки під час створення політики мережного доступу

Брандмауер - це реалізація політики мережного доступу, що розглядалася в 2.4.1 . Існує низка варіантів цієї політики, які можна реалізувати, таких як заборона доступу ззовні, необмежений доступ до Інтернету або обмежений вхідний доступ та обмежений вихідний доступ. Політика проектування брандмауера визначає багато в чому політику мережного доступу: чим суворіша політика проектування брандмауера, тим суворішою буде і політика мережного доступу. Тому, перш за все, потрібно визначитися з політикою проектування брандмауера.

Як пояснювалося у розділі 2.4.1, типовими політиками проектування брандмауера є заборона всіх сервісів, крім явно дозволених, або дозвіл на доступ до всіх сервісів, крім тих, що явно заборонені. Перший тип безпечніший і тому кращий, але він також суворіший, у результаті при ньому допускається робота меншого числа сервісів. Розділ 3 містить кілька прикладів брандмауерів, і в ній наочно показано, що деякі типи брандмауерів можуть реалізовувати обидва види політики керування доступом, тоді як брандмауер на основі шлюзу з двома інтерфейсами призначений для реалізації політики "все, що не

дозволено - заборонено". Крім того, ці приклади показують, що системи, що вимагають забезпечення доступу до сервісів, які не пропускаються брандмауером, можуть бути розміщені в ізольованих підмережах окремо від інших внутрішніх систем. Ключовим моментом тут є те, що в залежності від вимог забезпечення безпеки та гнучкості, деякі типи брандмауерів більш кращі, ніж інші. Цей факт наголошує на важливості правильного вибору політики до початку створення брандмауера; інший порядок дій недоцільний.

Для того, щоб правильно розробити концептуальну політику брандмауера, а потім систему брандмауера, яка реалізує цю політику, NIST рекмоїдує, щоб спочатку було розроблено найбезпечніший варіант політики - тобто заборонити всі сервіси, окрім тих, що явно дозволені. Розробники політики повинні розумітися на таких питаннях і задокументувати їх:

- які послуги в Інтернеті організація планує використовувати (наприклад, TELNET, WWW, NFS)
- яким чином ці сервіси будуть використовуватися, тобто локально, через Інтернет, по модему з дому або з віддалених організацій
- додаткові потреби, такі як шифрування та забезпечення роботи з модему
- які ризики пов'язані з наданням цих сервісів
- яка вартість засобів захисту та які зміни у можливостях використання мережі при забезпеченні захисту
- пріоритети забезпечення безпеки при використанні тих чи інших сервісів по відношенню до можливості використовувати їх: чи надаватиметься сервіс, якщо він занадто ризикований, або його занадто дорого захищати

Відповіді на ці питання прості, але відповідати на них, швидше за все, доведеться кілька разів. Наприклад, організація може хотіти використовувати NFS між двома віддаленими мережами, але політика "забороняти все, що не дозволено" може забороняти доступ до NFS (як це пояснюється у пункті 2.4.1). Якщо ризик, пов'язаний з NFS, прийнятний для організації, то знадобиться переробка концептуальної політики брандмауера на менш сувору - дозвіл всіх сервісів, крім тих, які явно запрощені, і дозвіл пропускати NFS через брандмауер до внутрішніх систем. Або може знадобитися придбання

брандмауера, який може розмістити системи, яким потрібно NFS, в ізольованій підмережі, дозволяючи таким чином залишити політику "забороняти все, що не дозволено". Або ризик використання NFS може бути занадто великим; та NFS буде виключено зі списку сервісів, які дозволено використовувати віддаленим системам.

Для того, щоб допомогти в розробці політики брандмауера нижче описано ряд типових проблем, які потрібно вирішити під час створення брандмауера.

1.2 Гнучкість політики

Будь-яка політика безпеки, пов'язана з доступом з Інтернету, сервісами Інтернету та доступом до мережі взагалі має бути гнучкою. Ця гнучкість повинна бути з двох причин: сам Інтернет постійно змінюється і потреби організації можуть змінитися в міру появи нових сервісів в Інтернеті та нових способів виконання діяльності організації. З'являються нові протоколи та нові сервіси в Інтернеті, які надають нові можливості організаціям, які використовують Інтернет, але це може призвести до нових проблем з безпекою. Тому політика повинна мати можливості обліку та включення цих нових проблем із безпекою. Інша причина гнучкості полягає в тому, що ризики для організації також не статичні. Ризик може змінитися через великі зміни, такі як нові обов'язки, покладені на організацію,

1.3 Політика посиленої автентифікації віддалених користувачів

Віддалені користувачі - це користувачі, які встановлюють з'єднання з внутрішніми системами звідкись з Інтернету. Ці з'єднання можуть виходити від будь-якого місця в Інтернеті, модемних ліній, авторизованих користувачів, які працюють з дому. У будь-якому випадку для всіх таких сполук повинні використовуватися заходи посиленої аутентифікації брандмауера перед наданням дсотупа до внутрішніх систем. У політиці має бути зазначено, що видалені користувачі не можуть отримувати доступ до систем за допомогою неавторизованих модемів за брандмауером. Не повинно бути винятків для цього правила, оскільки навіть один перехоплений пароль або один неконтрольований модем може відкрити чорний вхід в обхід брандмауера.

Така політика має й недоліки: необхідно навчати користувачів користуватися засобами посиленої аутентифікації, витрачати кошти на пристрої аутентифікації користувачів та адмініструвати віддалений доступ. Але буде дурістю встановити брандмауер і не контролюватиме віддалений доступ.

1.4 Політика доступу через модеми

Корисною можливістю для авторизованих користувачів є віддалений доступ до внутрішніх систем, коли користувачі знаходяться поза мережею. Така можливість дозволяє їм здійснювати доступ до систем із місць, де Інтернет може бути недоступним. Але, як уже обговорювалося у частині 2.3.2 , ці можливості є одним із шляхів отримання доступу зловмисником.

Авторизовані користувачі можуть хотіти мати можливість вихідних дзвінків для доступу до систем в інших місцях, до яких неможливий доступ через Інтернет. Ці користувачі повинні розуміти, що можуть створити вразливі місця при недбалому поводженні з модемом. Можливість вихідних дзвінків легко може дозволити організувати і вхідні дзвінки, якщо не прийняти відповідні застереження.

Обидві ці можливості повинні враховуватись при розробці брандмауера та включені при необхідності до нього. Вимога обов'язковості застосування заходів посиленої аутентифікації при доступі через брандмауер має бути обов'язково відбито у політиці. Політика також може забороняти використання неавторизованих модемів, приєднаних до систем мережі, якщо доступ до модему обходить засоби захисту брандмауера. Сувора політика може обмежити кількість використовуваних модемів в мережі, зменшуючи таким чином її вразливість.

1.5 Віддалені з'єднання з мережею організації

Окрім з'єднань через модеми, політика повинна регламентувати використання з'єднань за допомогою протоколів SLIP та PPP. Користувачі можуть використовувати їх для створення нових з'єднань всередині захищеної мережі. Таке з'єднання потенційно є способом обходу брандмауера, і може виявитися навіть більш небезпечним, ніж з'єднання, що комутується.

У частині 3 є кілька прикладів розміщення засобів організації доступу модемам таким чином, що з'єднання проходять через брандмауер. Таке ж розміщення може бути використане і для протоколів SLIP і PPP, але їх слід заздалегідь описати в політиці. Зазвичай політика дуже суворо регламентує такі сполуки.

1.6 Політика для інформаційного сервера

Мережа, яка надає доступ до інформаційного сервера, повинна враховувати цей вид доступу під час проектування брандмауера. Хоча інформаційний сервер створює специфічні проблеми безпеки, він не повинен стати вразливим місцем для мережі. У політиці має бути відображено посилку, що безпека мережі не має постраждати через те, що потрібно мати інформаційний сервер.

Можна зробити важливий висновок про те, що трафік, пов'язаний з інформаційним сервером, відрізняється від трафіку, пов'язаного з роботою інших програм, таких як електронна пошта. З кожним із цих двох видів трафіку пов'язані свої ризики, і не слід змішувати їх.

У частині 3 описується, як врахувати наявність інформаційного сервера під час проектування брандмауера. Приклади брандмауерів з ізольованою підмережею та на основі шлюзу з двома інтерфейсами містять інформаційні сервери, які можуть бути розміщені в ізольованій підмережі та, по суті, ізольовані від інших систем мережі. Це зменшує шанс того, що спочатку буде скомпрометовано інформаційний сервер, а потім з нього буде зроблено атаку на внутрішні системи.

ЯК ВИБРАТИ ЕФЕКТИВНУ ПОЛІТИКУ БРАНДМАУЕРА

19 січня, 2018 12:00 пп 1 946 views |коментарів немає

Linux | Amber | Коментувати запис

Налаштування брандмауера переважно полягає у пошуку розумної політики. Брандмауери типу iptables можуть реалізувати політики, наслідуючи правила адміністратора. Однак для цього адміністратору потрібно знати, які типи правил потрібні його інфраструктурі.

Читайте також :

- Що таке брандмауер та як він працює?

- Налаштування фаєрволу за допомогою IPTables на Ubuntu 14.04

  У цій статті ви знайдете корисні поради щодо налаштування брандмауера. Ви дізнаєтесь, як вплинути на поведінку брандмауера та оцінити рівень захисту сервера. Як приклад у статті використовується iptables, але більшість описаних порад спрацюють і з іншими інструментами.

  Вибір політики за умовчанням

  При налаштуванні брандмауера одним із основних рішень, які ви повинні прийняти, є стандартна політика. Вона визначає, що відбувається, коли трафік не відповідає правилам брандмауера. За замовчуванням брандмауер може приймати будь-який трафік, що не відповідає його правилам, або скидати цей трафік.

  Політики за промовчанням drop та accept

  Політика accept за промовчанням означає, що будь-який трафік, який не відповідає правилам брандмауера, може потрапити на сервер. Цю політику зазвичай не рекомендується застосовувати, тому що це означає, що вам доведеться підтримувати чорний список. Чорним списком складно керувати, тому що для його налаштування ви повинні передбачати та заблокувати всі типи небажаного трафіку. Це ускладнює підтримку списку; більше, у чорних списках часто бувають помилки конфігурації та непередбачені відхилення від встановленої політики.

  Альтернативною політикою за промовчанням є drop. Ця політика скидає весь трафік, який не відповідає правилам. За цієї політики вам потрібно підтримувати білий список. Для цього потрібно явно дозволити всі необхідні послуги. Спершу здається, що для цього потрібно виконати велику роботу. Однак це забезпечить більш високу безпеку сервера. До того ж, ви точно знатимете, який трафік може оброблятися сервером.

  В основному при налаштуванні брандмауера рекомендується блокувати весь трафік, який не було явно дозволено правилами. Тому зазвичай за умовчанням використовується політика drop.

  Політика drop та правило drop

У iptables та інших подібних брандмауерах політика за замовчуванням може бути задана за допомогою вбудованих функцій або реалізована шляхом додавання загального правила drop до кінця списку правил.
Відмінність між цими двома методами полягає в тому, що відбувається при скиданні правил брандмауера.
Якщо встановлено вбудовану політику брандмауера drop, то при скиданні правил (або видаленні деяких з них) сервіси миттєво стануть недоступними віддалено. Це часто використовується при налаштуванні політики не дуже важливих сервісів, щоб сервер не піддавався шкідливому трафіку, якщо правила були видалені.
Недоліком цього є те, що всі сервіси будуть повністю недоступні до тих пір, поки ви не встановите нові правила. Ви навіть можете заблокувати себе на власному сервері, якщо у вас немає локального або стороннього способу доступу, щоб усунути проблему. Якщо ж ви навмисно хочете скинути правила брандмауера, ви можете перед цим перейти на політику accept.
Замість використання політики drop, ви можете встановити політику accept і додати правило drop в кінець списку. Ви можете додати правило брандмауера в кінці свого ланцюжка, який збирає та скидає весь трафік, який не пройшов брандмауер.
У цьому випадку при скиданні правил брандмауера всі послуги будуть доступні, але не захищені.
Залежно від вашої ситуації, це може бути необхідним злом (що дозволить вам підключитися до сервера навіть після скидання правил). Якщо ви вирішите використати цей варіант, ви повинні пам'ятати, що загальне правило скидання завжди йде останнім у наборі правил.

Скидання та відхилення трафіку

Брандмауер може відмовити у прийомі пакетів кількома способами. Це впливає на те, як клієнт сприймає спробу підключення та як швидко клієнт зможе визначити, що запит не обслуговуватиметься.
Перший спосіб - це скидання пакетів або drop. Drop може використовуватися як стандартна політика. При цьому iptables просто відкидає пакет. Брандмауер не

надсилає відповідь клієнту і не дає жодних вказівок про те, що він колись отримував такі пакети. Це означає, що клієнти нічого не дізнаються про свої пакети.

TCP-з'єднання, які не пройшли брандмауер, чекатимуть обробки до досягнення межі таймууту. Оскільки UDP є протоколом без встановлення з'єднання, відсутність відповіді може заплутати клієнтів. По факту неповернення пакета може означати, що пакет було прийнято. Якщо клієнт UDP дбає про свої пакети, він повинен буде повторно відправити їх, щоб спробувати визначити, чи були вони прийняті. Це може збільшити кількість часу, який зловмиснику доведеться витратити, щоб отримати правильну інформацію про стан портів вашого сервера, але це також може викликати проблеми з трафіком звичайних користувачів.

Альтернативою скидання трафіку є явне відхилення пакетів. ICMP (або Internet Control Message Protocol) – це мета-протокол, який використовується для надсилання повідомлень про стан, діагностику та помилки як позасмуговий канал, який не покладається на звичайні протоколи зв'язку типу TCP або UDP. Коли ви використовуєте ціль reject, трафік відхиляється, і ICMP-пакет повертається відправнику, щоб повідомити, що трафік отримано, але не прийнято. Повідомлення про стан може підказати причину.

Це має низку наслідків. Припускаючи, що ICMP трафік може досягти клієнта, клієнт відразу ж дізнається, що його трафік заблокований. При цьому звичайні клієнти можуть зв'язатися з адміністратором або перевірити параметри підключення та переконатися, що вони звертаються до правильного порту. А зловмисникам це допоможе завершити сканування та виявити відкриті, закриті та відфільтровані порти за більш короткий період часу.

Вибираючи між скиданням та відхиленням трафіку, потрібно розуміти, що більшість шкідливого трафіку відправляється автоматизованими сценаріями. Оскільки сценарії можуть працювати скільки завгодно довго, скидання такого трафіку не допоможе, крім того, це матиме негативні наслідки для звичайних користувачів.

Ця таблиця покаже, як сервер реагує різні запити залежно від політики цільового порту.

Тип пакету клієнта	**Команда NMap**	**Політика**	**Відповідь**	**Й п**
TCP	nmap [-sT | -sS] -Pn <server>	Accept	TCP SYN/ACK	В
TCP	nmap [-sT | -sS] -Pn <server>	Drop	(ні)	В
TCP	nmap [-sT | -sS] -Pn <server>	Reject	TCP RESET	З
UDP	nmap -sU -Pn <server>	Accept	(ні)	В ві
UDP	nmap -sU -Pn <server>	Drop	(ні)	В ві
UDP	nmap -sU -Pn <server>	Reject	ICMP Port Unreachable	З

У першому стовпці вказано тип пакета, надісланого клієнтом. У другому стовпці перелічені команди nmap, які можна використовуватиме тестування кожного сценарію. У третьому стовпці вказується політика порту. Четвертий стовпець – це відповідь, яку сервер відправить назад, а п'ятий стовпець – це те, що клієнт дізнається про порт на основі отриманої відповіді.

Політики ICMP

Також існує багато різних думок щодо того, чи варто приймати ICMP-пакети. Протокол ICMP використовується для різних цілей. Він часто надсилає відповіді, щоб надати інформацію про стан запитів, надісланих із використанням інших протоколів. Можливо, найбільш важливою його

функцією є надсилання та відповідь на мережеві пінги для перевірки можливості підключення до віддалених хостів.

ICMP-пакети організовані за типом, а потім за кодом». Тип визначає загальний зміст повідомлення. Наприклад, Type 3 означає, що пункт призначення недоступний. Код часто використовується для надання додаткової інформації про тип. Наприклад, ICMP Type 3 Code 3 означає, що цільовий порт недоступний, а ICMP Type 3 Code 0 – недоступна цільова мережа.

Типи, які можна заблокувати назавжди

Деякі типи ICMP застаріли, тому їх, можливо, слід блокувати беззастережно. Серед них – пригнічення ICMP (type 4 code 0) та альтернативний хост (type 6). Типи 1, 2, 7, 15 і вище застаріли, зарезервовані для майбутнього використання або є експериментальними.

Типи, які потрібно заблокувати в залежності від налаштувань мережі

Деякі типи ICMP корисні за певних конфігурацій мережі, але повинні блокуватися в інших випадках.

Наприклад, повідомлення про переадресацію ICMP (тип 5) можуть допомогти виявити неправильну структуру мережі. Переадресація ICMP використовується, коли клієнт має кращий маршрут. Тому якщо маршрутизатор отримує пакет, який має бути перенаправлений на інший хост у тій самій мережі, він надсилає повідомлення переадресації ICMP, щоб запропонувати клієнту надалі відправляти пакети через інший хост.

Це корисно, якщо ви довіряєте своїй локальній мережі та хочете підвищити ефективність своїх таблиць маршрутизації під час початкового налаштування (виправлення маршрутів – найкраще довгострокове рішення). Однак у ненадійній мережі зловмисник може надсилати ICMP-перенаправлення для керування таблицями маршрутизації на хостах.

Інші типи ICMP, які корисні в деяких мережах та потенційно шкідливі для інших, – це оголошення маршрутизатора ICMP (тип 9) та виклик маршрутизатор (тип 10). Ці пакети використовуються як частина системи IRDP (ICMP Internet Router Discovery Protocol), яка дозволяє хостам динамічно

виявляти доступні маршрутизатори під час завантаження чи підключення до мережі.

У більшості випадків хосту краще налаштувати статичні маршрути для шлюзів, які він використовуватиме. Ці пакети повинні прийматися у тих самих ситуаціях, як і пакети переадресації ICMP.

Типи, які можна не блокувати

Нижче наведено типи ICMP, які безпечно використовувати в більшості випадків (але ви можете вимкнути деякі з них, щоб підвищити безпеку).

- Тип 8 - луна-запит. Це пінг-запити, спрямовані на ваш сервер. Зазвичай можна не блокувати цей тип, але ви можете заблокувати ці пакети в разі потреби або обмежити список адрес, які можуть надсилати їх. Блокування цих пакетів не допоможе приховати ваш сервер - є ще багато способів дізнатися про існування вашого хоста.
- Тип 13 – запит тимчасової мітки. Ці пакети використовуються клієнтами для збирання інформації про затримку. Вони використовуються у контрольних сумах. Ви можете заблокувати ці пакети в разі потреби або обмежити список адрес, які можуть надсилати їх.

  Наступні пакети можна підтримувати без спеціальних правил шляхом налаштування брандмауера для відповідей на запити, які він зробив (використовуючи модуль conntrack, щоб дозволити трафік ESTABLISHED та RELATED).
- Тип 0 – це відповідь на луна-запит.
- Тип 3 – ціль недоступна. Такі пакети – це відповіді на запити, створені сервером, які повідомляють, що пакет не може бути доставлений.
- Тип 11 – це діагностична помилка, яка видається, якщо згенерований сервером пакет був втрачений до того, як досяг призначення через перевищення його значення TTL.
- Тип 12 – проблема з параметрами: вихідний пакет із сервера був спотворений.
- Тип 14 – це відповіді на запити мітки часу, згенеровані сервером.

  Деякі експерти з безпеки, як і раніше, рекомендують повністю заблокувати трафік ICMP, проте багато користувачів підтримують його.

Обмеження швидкості та кількості з'єднань

Ви можете дозволити доступ до деяких сервісів та шаблонів трафіку, якщо клієнти не зловживатимуть цим доступом.

Обмеження кількості сполук

Обмеження кількості з'єднань можна реалізувати за допомогою розширень типу connlimit. Воно перевірить, скільки активних з'єднань створив клієнт. Ви можете обмежити кількість цих з'єднань. Для цього потрібно вирішити:

- Як обмежувати з'єднання: за адресою, мережею чи глобально?
- Обмежувати трафік лише для певного сервісу чи сервера в цілому?

З'єднання можна обмежити на основі хоста або сегменту мережі (за допомогою мережевого префікса). Ви також можете встановити глобальну максимальну кількість з'єднань для сервісу або всієї машини. Майте на увазі, що їх можна комбінувати для створення складніших політик.

Обмеження швидкості

Також можна створити правила, які керують частотою/швидкістю, з якою сервер обробляє трафік. І тому існує ряд розширень – limit, hashlimit і recent. Кожне з розширень управляє швидкістю по-своєму.

Розширення limit буде пропускати відповідний правилу трафік до тих пір, поки не буде досягнуто межі, після чого воно скидатиме пакети. Якщо ви встановите ліміт 5/sec, правило пропускатиме 5 пакетів в секунду, після чого воно буде недійсним. Це дозволяє настроїти глобальну швидкість сервісу.

Розширення hashlimit більш гнучке, воно дозволяє вказати деякі з значень, які iptables буде хешувати, щоб оцінити відповідність трафіку. Наприклад, для створення хеша кожного запису iptables може подивитися вихідну адресу та порт, цільову адресу та порт або довільну комбінацію цих чотирьох значень. Він може обмежуватись отриманими пакетами або байтами.

Розширення recent динамічно додає IP-адреси клієнта до списку або перевіряє існуючий список, якщо трафік відповідає правилу. Це дозволяє поширити логіку обмеження на кілька правил та створити складний шаблон. Це розширення дозволяє вказувати кількість збігів та часовий діапазон, але також може скинути часовий діапазон, якщо з'явиться додатковий трафік.

Управління iptables

Всі політики брандмауера iptables засновані на розширенні вбудованих ланцюжків. У простих брандмауерах це часто набуває форми зміни політики ланцюжків та додавання правил. У складніших брандмауерах часто буває корисно розширити структуру управління, створивши додаткові мережі. Користувальницькі ланцюжки успадковують ланцюжки, що викликаються ними. У ланцюжків користувача немає політики за умовчанням, тому якщо пакет проходить по такому ланцюжку, він повернеться в ланцюжок, що викликається, для подальшої перевірки. Ланцюжки користувача добре застосовувати в організаційних цілях і для підвищення надійності правил. Якщо ви повторюєте певну умову в багатьох правилах, можливо, доцільно замість цього створити правило переходу в новий ланцюжок. Всередині нового ланцюжка ви можете визначити цей набір правил із загальною для всіх умовою відповідності.

Такий підхід має багато переваг. Наприклад, розумне використання ланцюжків для дуже схожих наборів правил дозволяє спростити створення нових правил і зменшити кількість помилок. Крім того, таку політику легше сприймати.